SIEMENS

SIMATIC WinCC

Unified SCADA Certificate Manager

Manual del usuario

11/2019
A5E48696577-AA

Notas jurídicas

Filosofía en la señalización de advertencias y peligros

Este manual contiene las informaciones necesarias para la seguridad personal así como para la prevención de daños materiales. Las informaciones para su seguridad personal están resaltadas con un triángulo de advertencia; las informaciones para evitar únicamente daños materiales no llevan dicho triángulo. De acuerdo al grado de peligro las consignas se representan, de mayor a menor peligro, como sigue.

⚠ PELIGRO
Significa que si no se adoptan las medidas preventivas adecuadas **se producirá** la muerte o bien lesiones corporales graves.

⚠ ADVERTENCIA
Significa que si no se adoptan las medidas preventivas adecuadas **puede producirse** la muerte o bien lesiones corporales graves.

⚠ PRECAUCIÓN
Significa que si no se adoptan las medidas preventivas adecuadas pueden producirse lesiones corporales.

ATENCIÓN
Significa que si no se adoptan las medidas preventivas adecuadas pueden producirse daños materiales.

Si se dan varios niveles de peligro se usa siempre la consigna de seguridad más estricta en cada caso. Si en una consigna de seguridad con triángulo de advertencia de alarma de posibles daños personales, la misma consigna puede contener también una advertencia sobre posibles daños materiales.

Personal cualificado

El producto/sistema tratado en esta documentación sólo deberá ser manejado o manipulado por **personal cualificado** para la tarea encomendada y observando lo indicado en la documentación correspondiente a la misma, particularmente las consignas de seguridad y advertencias en ella incluidas. Debido a su formación y experiencia, el personal cualificado está en condiciones de reconocer riesgos resultantes del manejo o manipulación de dichos productos/sistemas y de evitar posibles peligros.

Uso previsto de los productos de Siemens

Considere lo siguiente:

⚠ ADVERTENCIA
Los productos de Siemens sólo deberán usarse para los casos de aplicación previstos en el catálogo y la documentación técnica asociada. De usarse productos y componentes de terceros, éstos deberán haber sido recomendados u homologados por Siemens. El funcionamiento correcto y seguro de los productos exige que su transporte, almacenamiento, instalación, montaje, manejo y mantenimiento hayan sido realizados de forma correcta. Es preciso respetar las condiciones ambientales permitidas. También deberán seguirse las indicaciones y advertencias que figuran en la documentación asociada.

Marcas registradas

Todos los nombres marcados con ® son marcas registradas de Siemens AG. Los restantes nombres y designaciones contenidos en el presente documento pueden ser marcas registradas cuya utilización por terceros para sus propios fines puede violar los derechos de sus titulares.

Exención de responsabilidad

Hemos comprobado la concordancia del contenido de esta publicación con el hardware y el software descritos. Sin embargo, como es imposible excluir desviaciones, no podemos hacernos responsable de la plena concordancia. El contenido de esta publicación se revisa periódicamente; si es necesario, las posibles correcciones se incluyen en la siguiente edición.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
ALEMANIA

A5E48696577-AA
℗ 03/2020 Sujeto a cambios sin previo aviso

Índice

Funciones del Certificate Manager

1

Uso de los certificados

Para defender las instalaciones, sistemas y redes frente a amenazas cibernéticas, es necesario proteger la comunicación dentro de la instalación. Esto se consigue utilizando protocolos de comunicación cifrados entre los dispositivos WinCC Unified. A cada uno de los interlocutores se le asigna un certificado único que se usará para la autenticación y el cifrado.

WinCC Unified Certificate Manager

El Certificate Manager sirve para crear y distribuir los certificados para los componentes WinCC Unified que utilizan la comunicación cifrada.

Encontrará más información sobre el uso de certificados en el archivo de ayuda "Léame de runtime", en "AUTOHOTSPOT".

Funciones del Certificate Manager:

- Creación de un certificado raíz para la instalación (Certificate Authority o CA)
- Creación centralizada de certificados para dispositivos WinCC Unified en la red
- Creación de certificados para los siguientes componentes WinCC Unified:
  - WinCC Unified Runtime (servidor web (IIS))
  - WinCC Unified OPC UA Server
  - WinCC Unified OPC UA Exporter
  - WinCC Unified Collaboration
- Exportación cifrada de los certificados para su distribución manual entre los dispositivos WinCC Unified
- Importación e instalación de los certificados configurados en un dispositivo WinCC Unified
- Exportación e importación cifradas del certificado raíz junto con la clave y todos los certificados de dispositivo para copias de seguridad y restauración de datos

Uso de los certificados

2

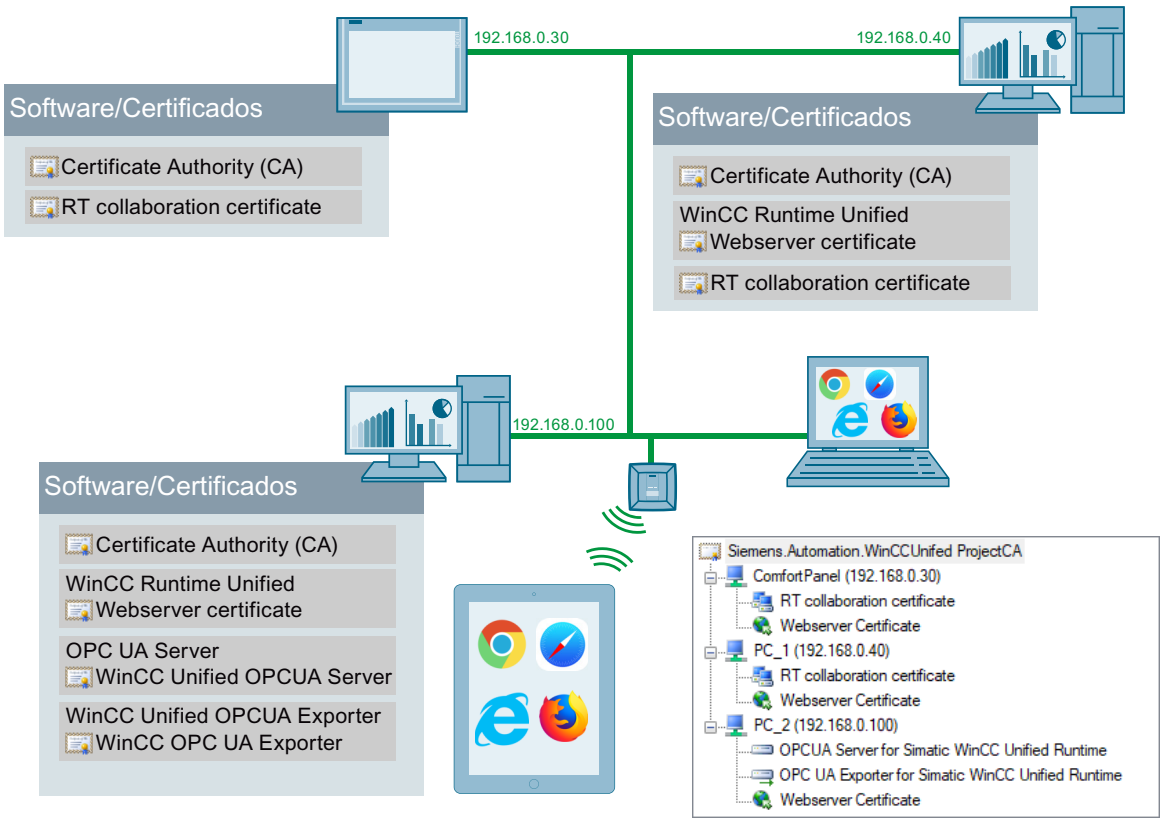
Certificados necesarios

En los dispositivos WinCC Unified se deben crear certificados para las siguientes aplicaciones:

- Si un dispositivo cuenta con un servidor web (IIS), se necesita un certificado "WebServer" para permitir el acceso a WinCC Unified a través de sitios web.
- Si los dispositivos WinCC deben intercambiar datos entre sí (WinCC Unified Collaboration), se necesita un certificado "RT collaboration" en cada uno de los dispositivos implicados.
- Si se utiliza el OPC UA Server en un dispositivo, se necesita un certificado específico del dispositivo para el OPC UA Server y el OPC UA Exporter.
- Todos los certificados mencionados debe emitirlos una entidad de certificación (CA) común para facilitar la relación de confianza entre los interlocutores de la comunicación.
- El certificado raíz de la CA se clasifica como "de confianza" en todos los dispositivos y para todas las aplicaciones.
- En caso de acceder a WinCC Unified Runtime a través de sitios web, será necesario configurar una vez en el navegador que el certificado raíz es de confianza.

Ejemplo

- En el ejemplo ilustrado, se utiliza un panel y dos equipos PC WinCC Unified.
- Los equipos PC proporcionan sitios web para la visualización del runtime, por lo que necesitan un "WebServer certificate".
- En un equipo PC (192.168.0.100) se ejecuta un OPC UA Server. Por este motivo necesita los certificados "WinCC Unified OPC UA Server" y "WinCC OPC UA Exporter".
- Se pretende intercambiar datos runtime entre un panel (192.168.0.30) y un PC (192.168.0.40). Así pues, los dos dispositivos requieren un "RT collaboration certificate".
- El certificado raíz se instala en todos los dispositivos y se clasifica como "de confianza".
- Si se pretende acceder a las páginas web de runtime desde navegadores de dispositivos externos, se deberá instalar el certificado raíz en la memoria de certificados del navegador. En la página de inicio de WinCC Runtime se ofrece un enlace de descarga a tal efecto. Encontrará más información sobre el uso de certificados en el archivo de ayuda "Léame de runtime", en "AUTOHOTSPOT".

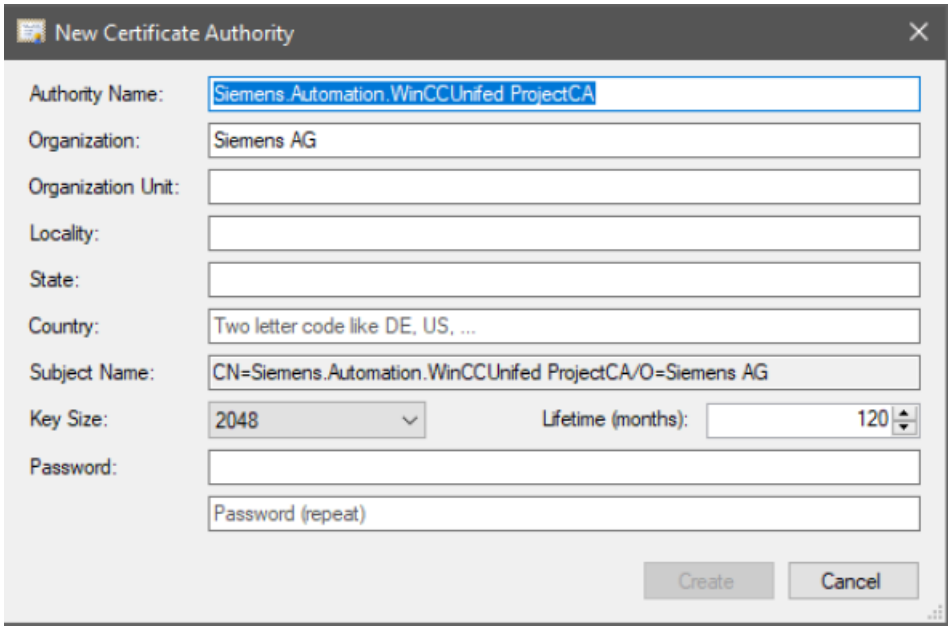

192.168.0.30
192.168.0.40
Software/Certificados
Certificate Authority (CA)
RT collaboration certificate
Software/Certificados
Certificate Authority (CA)
WinCC Runtime Unified
Webserver certificate
RT collaboration certificate
192.168.0.100
Software/Certificados
Certificate Authority (CA)
WinCC Runtime Unified
Webserver certificate
OPC UA Server
WinCC Unified OPCUA Server
WinCC Unified OPCUA Exporter
WinCC OPC UA Exporter
Siemens.Automation.WinCCUnifed ProjectCA
ComfortPanel (192.168.0.30)
RT collaboration certificate
Webserver Certificate
PC_1 (192.168.0.40)
RT collaboration certificate
Webserver Certificate
PC_2 (192.168.0.100)
OPCUA Server for Simatic WinCC Unified Runtime
OPC UA Exporter for Simatic WinCC Unified Runtime
Webserver Certificate

Creación de certificados

3

Crear un certificado raíz

1. Seleccione un equipo PC WinCC Unified en la red que deba actuar como entidad de certificación.
   El certificado raíz y la clave correspondiente solo están disponibles en este dispositivo. La configuración de certificados de aplicación adicionales para otros dispositivos solo es posible en este dispositivo.
2. Abra el "WinCC Unified Certificate Manager" en este dispositivo.
3. Cree un nuevo certificado raíz para la instalación. Para ello, haga clic con el botón derecho del ratón en el punto "No certificate authority configured ..." y seleccione "Create new certificate authority..." en el menú contextual.
4. Introduzca las propiedades del certificado raíz en el cuadro de diálogo. Los campos pueden editarse libremente.



   Campos obligatorios:

   – "Authority Name"
   – "Password" para la clave privada

   Si es necesario, modifique la longitud de la clave y el periodo de vigencia del certificado.
5. Haga clic en "Create".

El certificado raíz y la clave correspondiente se guardan en el dispositivo y se utilizarán para crear certificados de dispositivo.

Nota

Cuando el "WinCC Certificate Manager" vuelva a iniciarse en este dispositivo, se cargarán automáticamente el certificado raíz y los certificados de dispositivo creados con él.

Agregar dispositivos

1. Haga clic con el botón derecho del ratón en el certificado raíz y seleccione "Add device ...".
2. En el cuadro de diálogo "New Device", introduzca el nombre correcto y la dirección IP del dispositivo.
   Para los paneles, basta con introducir la dirección IP.
   En el caso de dispositivos con direcciones IP dinámicas, introduzca solo el nombre de host.

   Nota

   Nombres permitidos

   Como nombre se puede utilizar el nombre de host o el "fully qualified domain name". El nombre se inserta en los certificados creados para el dispositivo y se utiliza para la validación. Se debe utilizar el "fully qualified domain name" dentro de un dominio para evitar errores de validación al acceder a los sitios web.

   No se permite el uso del nombre "localhost": el Certificate Manager lo sustituirá automáticamente por el nombre del dispositivo local.

Agregar certificados

1. Haga clic con el botón derecho del ratón en el dispositivo y seleccione "Add <tipo de certificado> ...".
2. Introduzca las propiedades del certificado en el cuadro de diálogo.
   Si es necesario, modifique la longitud de la clave y el periodo de vigencia del certificado.

   Nota

   Periodo de vigencia

   El periodo de vigencia de los certificados web está limitado a 27 meses como máximo. Algunos navegadores no aceptan periodos de vigencia superiores.

   Nota

   Para los certificados de servidor web se debe utilizar el "fully qualified domain name".

Distribución e instalación de certificados para equipos PC

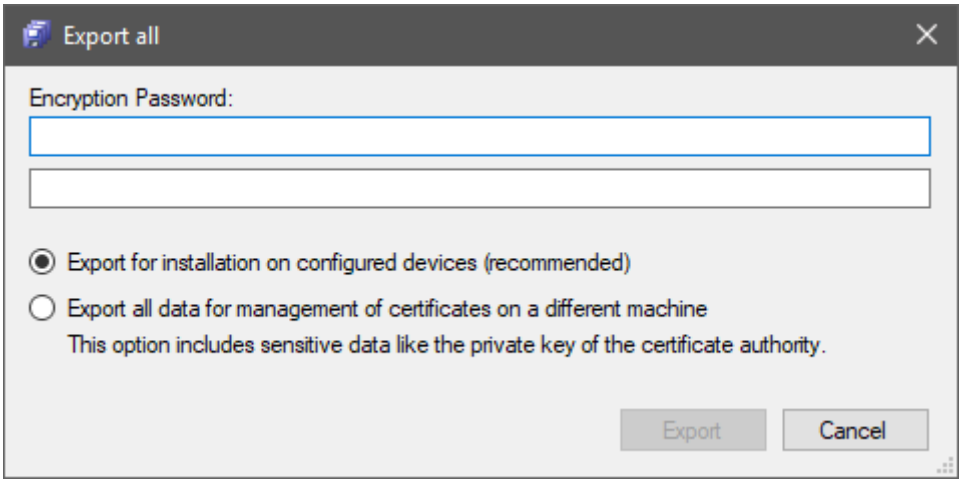
4

Introducción

Los certificados configurados se deben exportar a un archivo de almacenamiento seguro para poder distribuirlos entre los dispositivos correspondientes. Este archivo se debe transferir manualmente a cada dispositivo para importarlo desde allí. El procedimiento es distinto para los equipos PC y para los paneles.

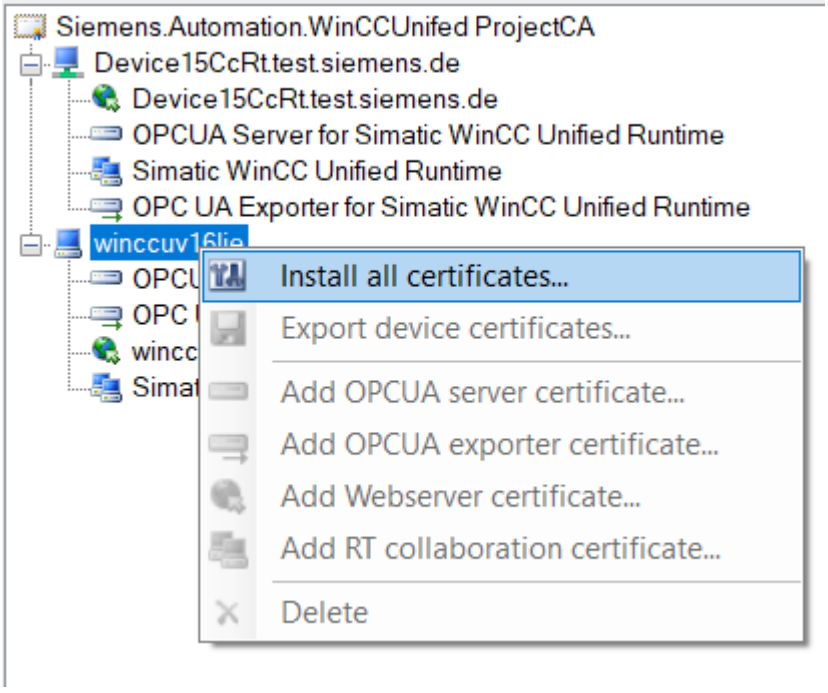
Distribución e instalación en equipos PC

1. Exporte la configuración de certificados completa a un archivo cifrado. Haga clic con el botón derecho del ratón en el certificado raíz y seleccione "Export all" en el menú.



2. Asigne una contraseña y seleccione "Export for installation…" (ajuste predeterminado).
3. Haga clic en "Export" y seleccione la ubicación y el nombre del archivo.
   Los datos se guardan cifrados con la contraseña indicada.
4. Copie el archivo de exportación en el dispositivo que va a instalar.
5. Abra WinCC Certificate Manager en el dispositivo que va a instalar.
6. Haga clic con el botón derecho del ratón en "No certificate authtority configured ..." y seleccione "Open configuration..." en el menú contextual.
7. Abra el archivo exportado e introduzca la contraseña.

8. Verá la configuración completa de todos los dispositivos, pero solo podrá instalar un certificado para el dispositivo local.
   Los certificados de los otros dispositivos solo se pueden visualizar, la configuración no se puede editar.
9. Para instalar certificados para el dispositivo local, seleccione el dispositivo local con el botón derecho del ratón (instala todos los certificados disponibles) o bien elija un solo certificado del dispositivo y seleccione la opción "Install…" en el menú.



Ejecute los pasos 4 a 9 en cada uno de los equipos PC que desee instalar.

Resultado

- Se instalan los certificados en las memorias de certificados definidas para cada aplicación.
- El certificado raíz público de la CA se clasifica como "de confianza" en todas las memorias de certificados.
- Si se instala un certificado web, se vinculará automáticamente al sitio web de WinCC Unified. El certificado web sustituye a otro posible certificado seleccionado durante la instalación de Runtime.
  A continuación, se reinicia el sitio web para aplicar el nuevo certificado. Al hacerlo, si hay navegadores conectados, se desconectarán y deberán registrarse de nuevo.

Nota

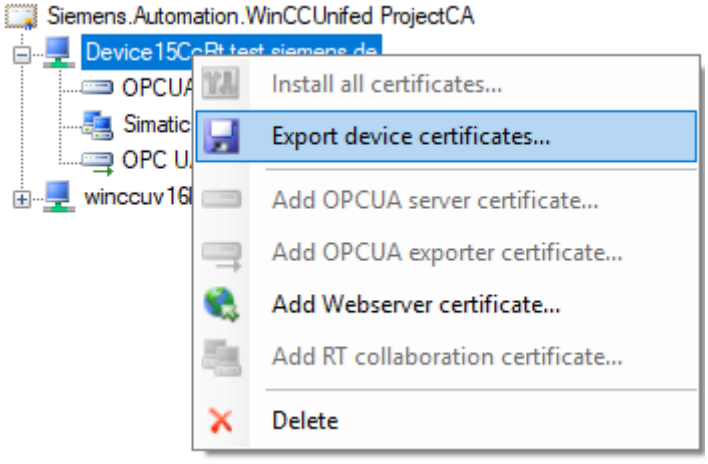
Los nuevos certificados para el OPC UA Server se harán efectivos solo después de reiniciar WinCC Unified Runtime.

Distribución e instalación de certificados para paneles HMI

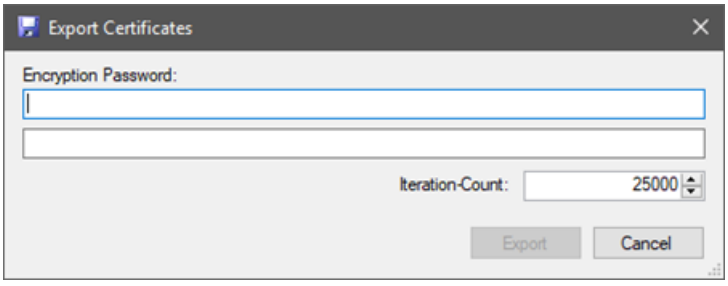
5

Exportar la configuración de certificados

1. Exporte la configuración de certificados del panel a un archivo cifrado. Para ello, haga clic con el botón derecho del ratón en el dispositivo en cuestión y seleccione la opción "Export device certificates…" del menú.



2. Asigne una contraseña. Si lo desea, puede adaptar el recuento de iteración para el cifrado. Confirme haciendo clic en "Export".



3. Seleccione la ubicación y el nombre del archivo.

Los datos se guardan en un fichero TAR y se cifran con la contraseña.

Descomprimir la configuración de certificados

Copie el archivo de exportación en el panel que va a instalar. Para descifrar el archivo se necesita OpenSSL.

```
openssl enc -d -aes256 -salt -iter <25000> -in <exportfilename> -out
<tarfilename.tar> -k <password>
```

- El valor del parámetro `-iter` debe coincidir con el recuento de iteración indicado durante la exportación.
- El fichero TAR descifrado contiene los certificados configurados en la estructura de carpetas específica de cada aplicación.
- Distribuya los certificados manualmente en las ubicaciones de almacenamiento específicas de cada aplicación.

Instalación del certificado raíz en el navegador 6

Uso de los certificados web

Para que un navegador web pueda establecer una conexión segura con WinCC Unified, dicho navegador web debe reconocer el certificado raíz actual de WinCC Runtime como entidad de certificación de confianza.

Al instalar el certificado web en el equipo PC, el certificado raíz público aparece en la página de inicio de WinCC Unified para su descarga e instalación en navegadores web.

El procedimiento de instalación del certificado raíz depende de cada navegador web.

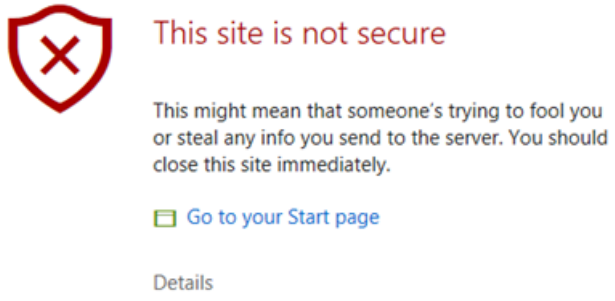
Instalación del certificado raíz en Chrome y Microsoft Edge

Chrome y Microsoft Edge usan la memoria de certificados (almacén de certificados en la nomenclatura de Microsoft) de sistema de Windows.

- En los dispositivos **con instalación de WinCC Unified** que se hayan configurado con el Certificate Manager, estos navegadores pueden establecer de inmediato una conexión segura con los sitios web de WinCC Unified, ya que el certificado raíz ya está instalado en los almacenes de certificados de sistema.
- En los dispositivos **sin instalación de WinCC Unified**, se debe instalar el certificado raíz manualmente.

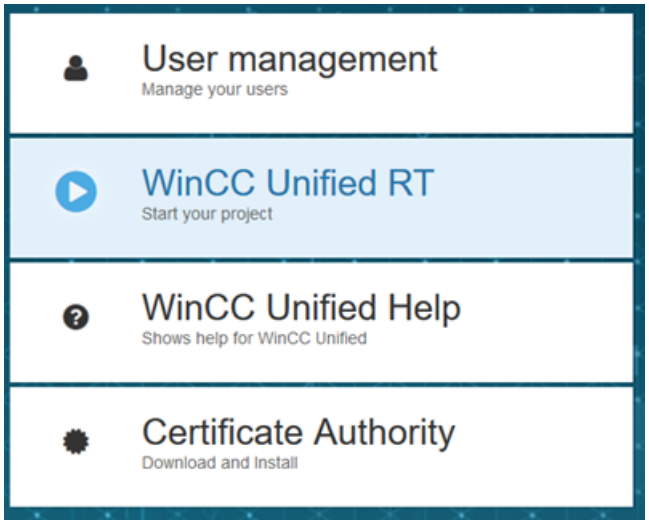
Realice los siguientes pasos para la instalación manual (ejemplo en Microsoft Edge):

1. Abra la página de inicio de WinCC Unified con la URL https://<nombre de host>
   En primer lugar aparece un mensaje de error:

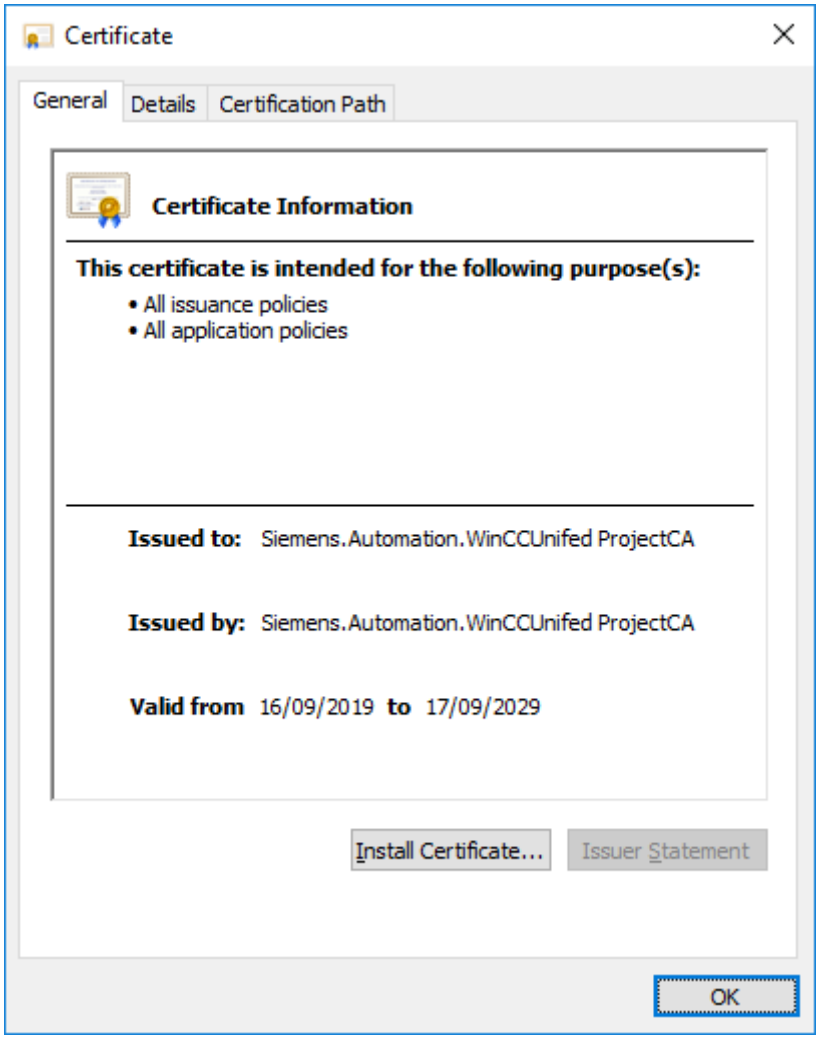


2. Abra el campo de detalles del error y confirme que desea abrir el sitio web.

3. En la página de inicio de WinCC Unified, seleccione el campo "Certificate Authority" y confirme con "Open file" en el diálogo de descarga.



4. El certificado raíz "ca.cer" se abre con el formulario estándar de Windows.

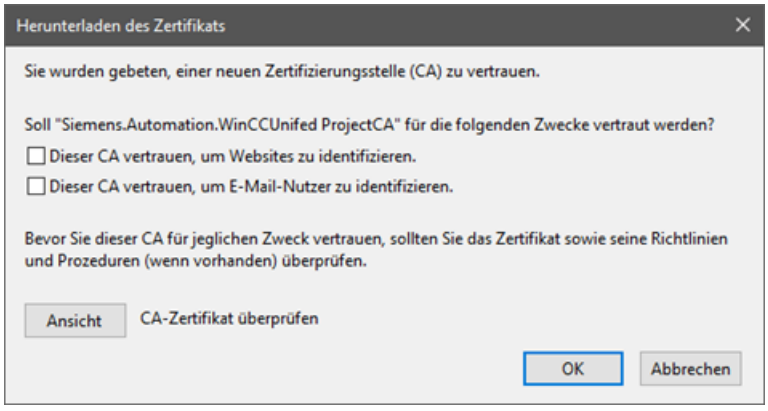


5. Seleccione "Install Certificate" para importar el certificado raíz en Windows.
6. En el asistente de importación, seleccione "Local Machine" como ubicación y "Trusted Root Certification Authority" como almacén de certificados, e inicie el proceso de importación.

Instalación del certificado raíz en Firefox

Firefox utiliza su propia memoria de certificados y por eso debe configurarse manualmente una vez en cada dispositivo. Al abrir la página de inicio de WinCC Unified, aparece también un mensaje de error.

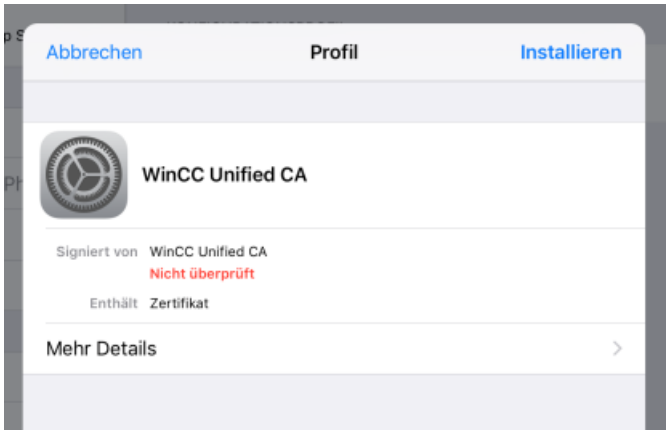
1. Abra el campo "Advanced" y confirme el campo "Accept the Risk and Continue".
2. En la página de inicio de WinCC Unified, seleccione el campo "Certificate Authority".
3. En el siguiente diálogo de Firefox, active la casilla "Trust this CA to identify websites" y confirme.



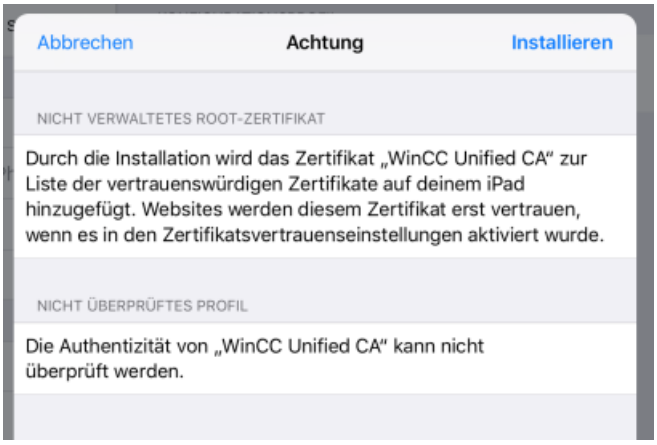
Instalación del certificado raíz en dispositivos iOS

iOS utiliza su propia memoria de certificados y por eso debe configurarse manualmente una vez en cada dispositivo. Al abrir la página de inicio de WinCC Unified, aparece también un mensaje de error.

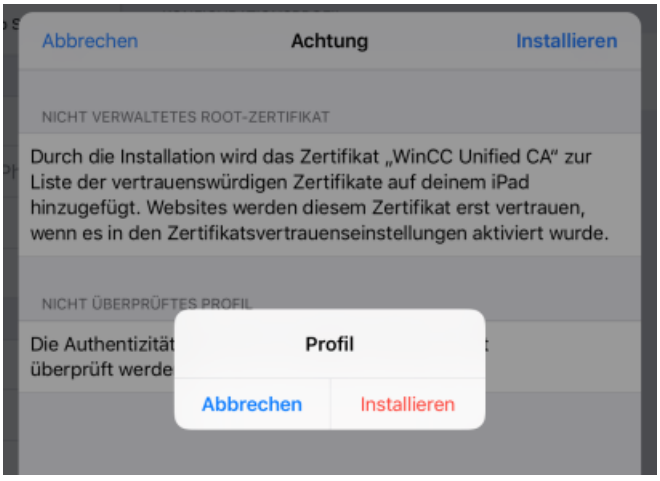
1. Abra el campo "Advanced" y confirme el campo "Accept the Risk and Continue".
2. En la página de inicio de WinCC Unified, seleccione el campo "Certificate Authority".



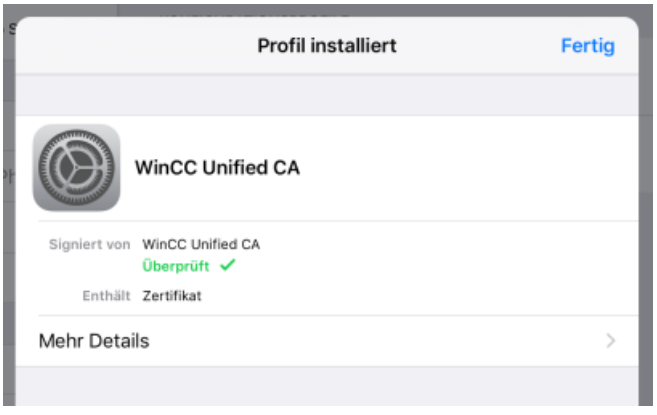
3. Seleccione "Install".



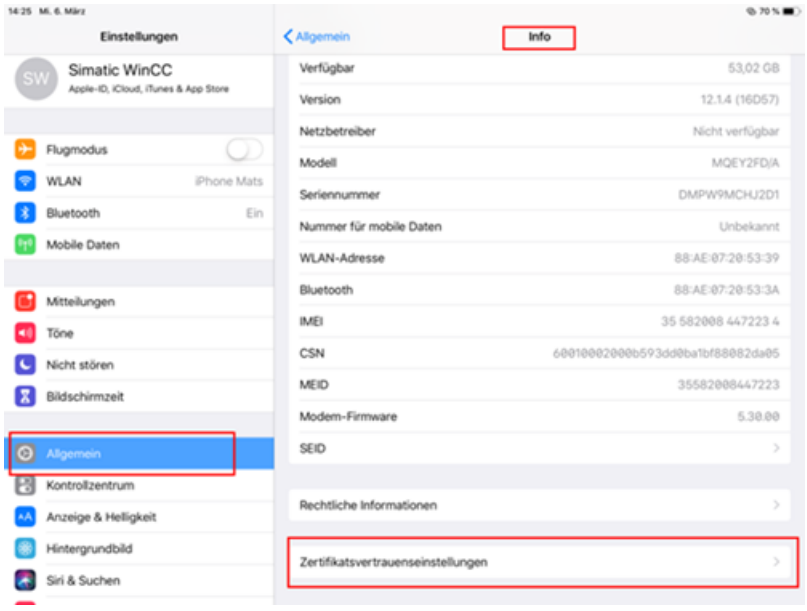
4. Vuelva a seleccionar "Install".



Verá la entrada "Trusted".



5. Seleccione "General > Information > Certificate Trust Settings".



6. Active "WinCC Unified CA" y seleccione "Next".