


The Siemens logo is displayed in a bold, teal, sans-serif font.

Ingenuity for life

A man in a light blue shirt is seen from the side, looking at a tablet. The background is a blurred industrial setting with a clock and various machinery. Overlaid on the image are several digital graphics: a '24/7' icon with a circular arrow, a 'NEWS' section with a person icon, a 'Home' button, and a network diagram with three people icons connected by lines. The text 'Industry Online Support' is also visible in a stylized font.

**How do I have to
proceed with the
encrypted access of
end devices to WinCC
Unified Runtime
(certificate
handling)?**

WinCC Unified V17

<https://support.industry.siemens.com/cs/ww/en/view/109777591>

Siemens
Industry
Online
Support



This entry originates from Siemens Industry Online Support. The conditions of use specified there apply (www.siemens.com/nutzungsbedingungen).

Security Informa-tion

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customers are responsible to prevent unauthorized access to their plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <http://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase the customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <http://www.siemens.com/industrialsecurity>.

Contents

1	Introduction	3
2	General information.....	3
3	Settings for WinCC Unified Runtime	4
4	Installation of certificates on various terminal devices.....	5
4.1	Android Clients	5
4.2	iOS clients	6
4.3	Browser with own certificate store (Mozilla Firefox)	8
4.4	Browser without own certificate store (Chrome, Edge, ...)	8
5	Revision history	9

1 Introduction

This document provides information on how to create a certificate structure for WinCC Unified systems. The certificate structure is used for encrypted access from terminal devices to the runtime device.

Note on mobile terminal devices

Access from mobile devices to WinCC Unified Runtime is only possible via the IP address, not via the computer name.

2 General information

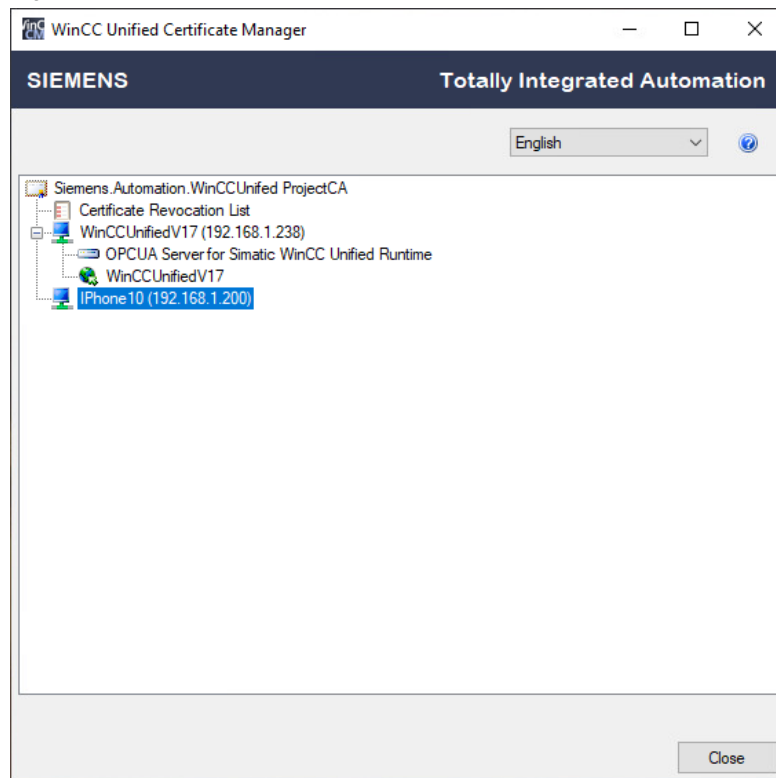
Communication between WinCC Unified devices is encrypted and uses a trusted certificate. In particular, you need to create a Root Certificate Authority (CA) for this purpose (see point 3). You then install this CA on all WinCC Unified terminal devices that are to communicate with the Unified Runtime device (see point 4) so that the terminal devices can authenticate themselves.

Certificates are required for the following functions of the WinCC Unified devices:

- OPC UA Server
- OPC UA Client
- OPC UA Exporter
- Web server
- Unified Collaboration
- Audit Trail System

You use the WinCC Unified Certificate Manager to manage and create the certificates. You can find the Certificate Manager in a standard installation under "C:\Program Files\Siemens\Automation\WinCCUnified\WebConfigurator\WinCC_CertManager.exe".

Figure 2-1



3 Settings for WinCC Unified Runtime

The settings for accessing WinCC Unified Runtime via an internet browser are described in the following entry:

Which settings do I have to make for the communication with WinCC Unified Runtime on the runtime device?

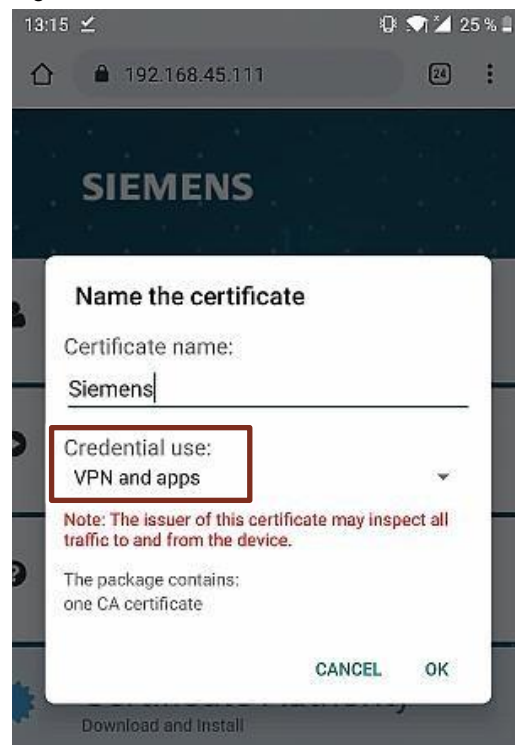
<https://support.industry.siemens.com/cs/ww/en/view/109806850>

4 Installation of certificates on various terminal devices

4.1 Android Clients

1. Call the "WinCC Unified" start page via "https://[Host name]" and select the "Certificate Authority" item.
2. Open the "ca.cert" file, name the certificate and select "VPN and Apps" using the login data.

Figure 4-1

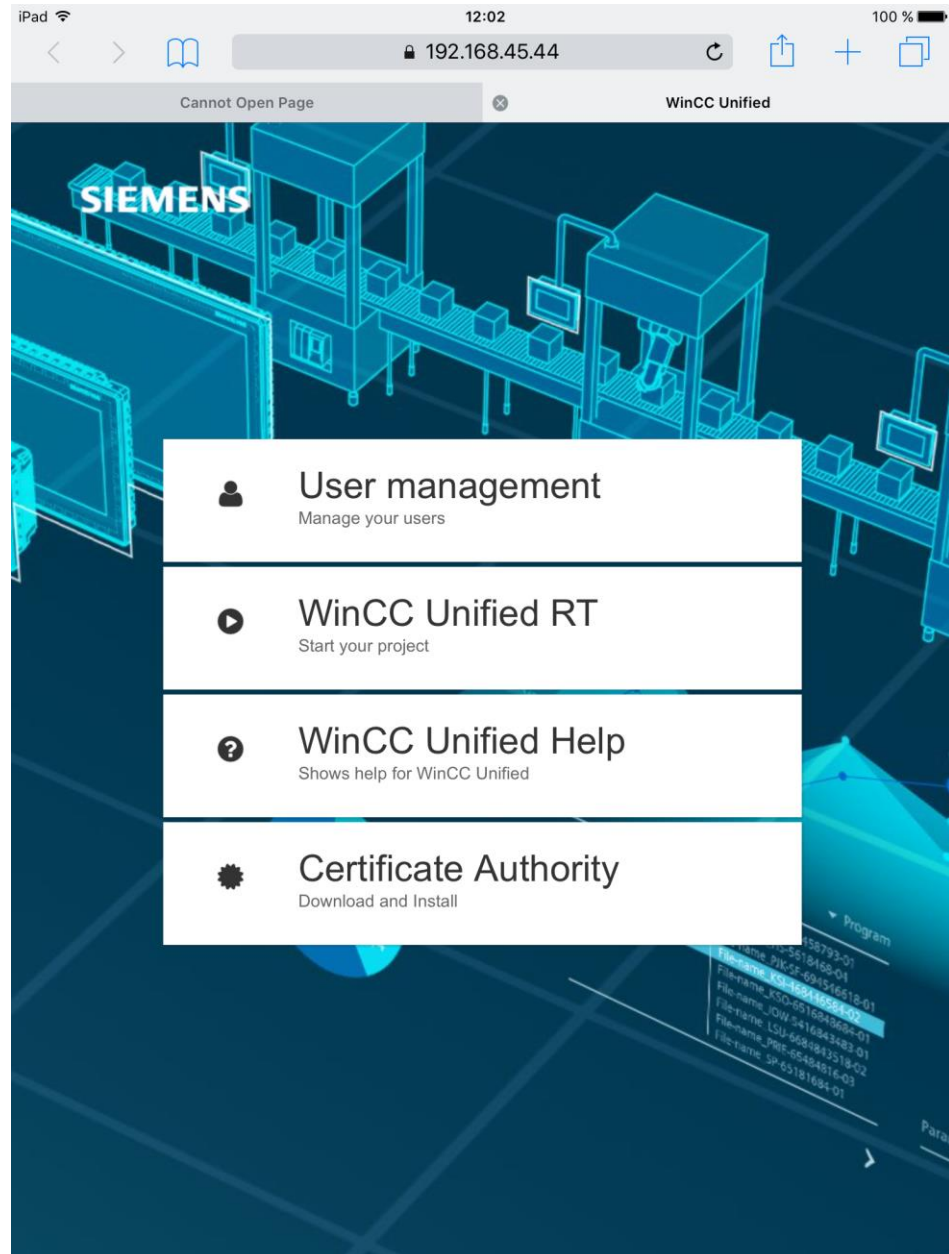


This procedure was tested on a smartphone with Android version 9 as an example for all Android devices and may vary from device to device.

4.2 iOS clients

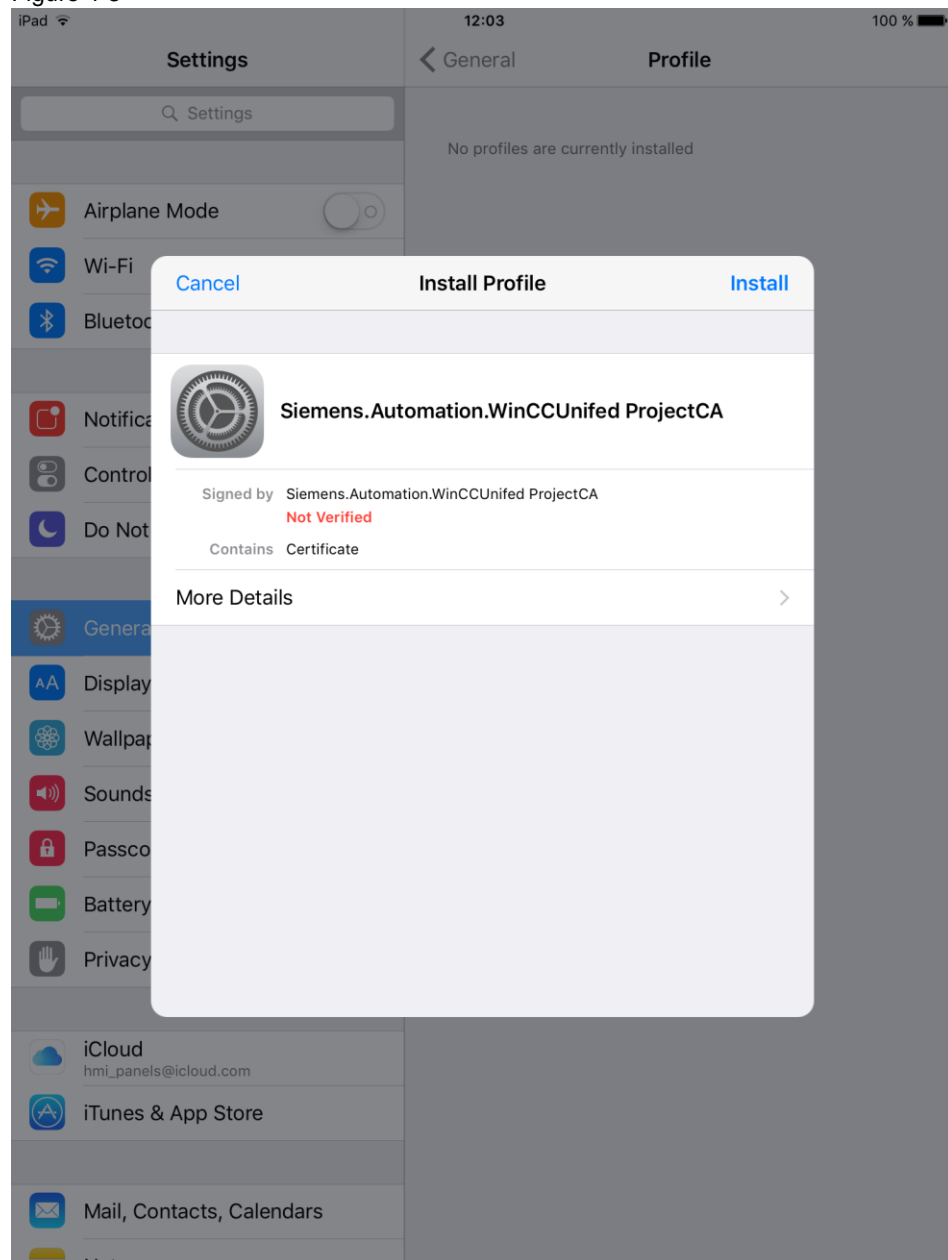
1. Call the "WinCC Unified" start page via [https://\[IP address\]](https://[IP address]) and select the "Certificate Authority" item:

Figure 4-2



2. The Settings dialog opens:

Figure 4-3



3. Go to General > Profile and the installed CA is displayed, and you can now access the Unified RT.

This procedure was done on a tablet with iOS version 15.0.2 as an example for all iOS devices and may vary from device to device.

4.3 Browser with own certificate store (Mozilla Firefox)

Firefox uses its own certificate store, not the Windows certificate store. The procedure is documented here in the WinCC Unified Runtime System manual V17:

Installing a certificate in the browser when accessing via web client (Unified PC)
<https://support.industry.siemens.com/cs/ww/en/view/109803796/142577146507>

Installing the root certificate for Firefox

4.4 Browser without own certificate store (Chrome, Edge, ...)

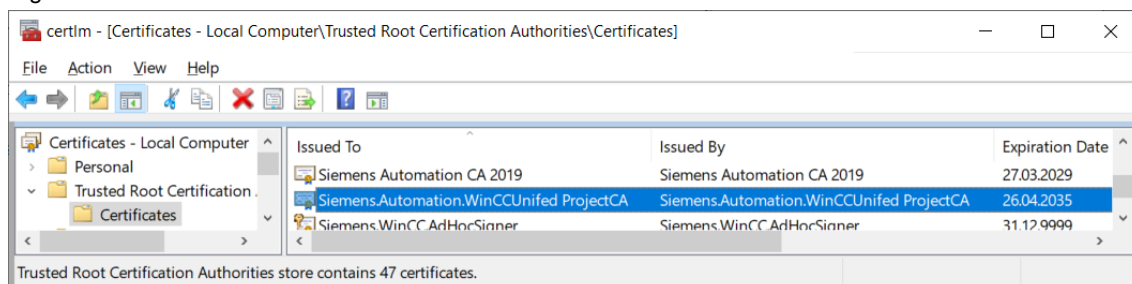
The procedure is documented here in the WinCC Unified Runtime System manual V17:

Installing a certificate in the browser when accessing via web client (Unified PC)
<https://support.industry.siemens.com/cs/ww/en/view/109803796/142577146507>

Installing the root certificate for Chrome and Microsoft Edge

Finally, check via Windows > Search "Manage computer certificates" whether the CA has been installed under "Certificates - Local Computer" > "Trusted Root Certification Authorities" > "Certificates": "Siemens.Automation.WinCCUnified ProjectCA"

Figure 4-4



5 Revision history

10/2022 Version 2.1

1. Title modified
2. Handling added to point 2.1 (certificate created via IP address)
3. Content removed from item 3. and linked to entry 109806850. The remaining topics are now documented in the V17 manual.
4. Points 4.2, 4.3 and 4.4 updated