

Industry Online Support

NEWS

Erstellung einer Zertifikatsstruktur mit WinCC Unified

WinCC Unified V17

https://support.industry.siemens.com/cs/ww/de/view/109777591

Siemens Industry Online Support



Dieser Beitrag stammt aus dem Siemens Industry Online Support. Es gelten die dort genannten Nutzungsbedingungen (<u>www.siemens.com/nutzungsbedingungen</u>).

Securityhinweise Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen

Konzepts. Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter <u>http://www.siemens.com/industrialsecurity</u>.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter <u>http://www.siemens.com/industrialsecurity</u>.

Inhaltsverzeichnis

Einfüł	nrung	3
Allgen	neine Informationen	3
Vorge	hensweise	4
3.1 3.2 3.3 3.4 3.5 3.6	Certificate Authority Geräte anlegen Webserver-Zertifikat OPC UA Zertifikate (Server, Client, Exporter) Runtime Collaboration Zertifikat Audit Trail System Zertifikat	4 5 6 7 10 10
Install	ation von Zertifikaten auf verschiedenen Geräten	11
4.1 4.2 4.3 4.4 4.5	Unified Comfort Panel Android-Clients IOS-Clients Browser mit eigenem Zertifikatsspeicher (Mozilla Firefox) Browser ohne eigenen Zertifikatsspeicher (Chrome, Edge,)	11 11 12 14 14
	Einfül Allger Vorge 3.1 3.2 3.3 3.4 3.5 3.6 Install 4.1 4.2 4.3 4.4 4.5	Einführung Allgemeine Informationen Vorgehensweise 3.1 Certificate Authority 3.2 Geräte anlegen 3.3 Webserver-Zertifikat 3.4 OPC UA Zertifikate (Server, Client, Exporter) 3.5 Runtime Collaboration Zertifikat 3.6 Audit Trail System Zertifikat Installation von Zertifikaten auf verschiedenen Geräten 4.1 Unified Comfort Panel 4.2 Android-Clients 4.3 IOS-Clients 4.4 Browser mit eigenem Zertifikatsspeicher (Mozilla Firefox) 4.5 Browser ohne eigenen Zertifikatsspeicher (Chrome, Edge,)

1 Einführung

Dieses Dokument liefert Ihnen Hinweise zur Erstellung einer Zertifikatsstruktur für WinCC Unified-Systeme zur verschlüsselten Kommunikation zwischen Endgeräten und Runtime.

2 Allgemeine Informationen

Damit WinCC Unified Geräte sich mit vertrauenswürdigen Zertifikaten authentifizieren können, muss eine Root Certificate Authority (Stammzertifizierungsstelle) erstellt werden. Diese müssen Sie erstellen und anschließend an sämtliche Endgeräte verteilen, welche später mit den Unified Geräten kommunizieren sollen.

Für folgende Funktionen der WinCC Unified Geräte werden Zertifikate benötigt:

- OPC UA Server
- OPC UA Client
- OPC UA Exporter
- Webserver
- RT Collaboration
- Audit Trail System

Die Verwaltung und Erstellung der Zertifikate geschieht mit dem WinCC Unified Certificate Manager. (Sie finden den Certificate Manager bei einer Standardinstallation unter "C:\Program Files\Siemens\Automation\WinCCUnified\ WebConfigurator\WinCC_CertManager.exe".)

Abbildung 2-1



3 Vorgehensweise

3.1 Certificate Authority

- Erstellen Sie im WinCC Unified Certificate Manager eine neue "Certificate Authority". Die voreingestellte "Key Size" und "Lifetime" können Sie beibehalten. "Lifetime" bestimmt die Gültigkeitsdauer der Zertifikate. Ist diese Dauer überschritten, müssen die "Certificate Authority" und die zugehörigen Zertifikate neu generiert werden. Die maximale Gültigkeitsdauer beträgt 150 Monate (12,5 Jahre).
- 2. Mit Rechtsklick auf die CA ist ein Export der kompletten CA (CA inkl. aller unterlagerten Zertifikate) möglich.

WinCC Unified Certificate Manager – C × SIEMENS Totally Integrated Automation Deutsch © Stemens Automation.WinCCUnifed ProjectCA CA-Zertifikat anzeinen CA-Zertifikat exportieren Gerät hinzufügen Alle exportieren X Löschen	Abbildung 3-1					
SIEMENS	WinCC Unified Certificate Mar	nager		to − .0		×
Deutsch vinCCUnifed ProjectCA	SIEMENS	Totally	y Integr	ated Au	ıtoma	tion
Siemens Automation WinCCUnifed ProjectCA Certificate Revocation List CA-Zertifikat exportieren Gerät hinzufügen Alle exportieren Cöschen			Deutsch		\sim	0
Schließen	Siemens Automation WinCCUnife	 d ProjectCA CA-Zertifikat anzeigen CA-Zertifikat exportieren Gerät hinzufügen Alle exportieren X Löschen 			Schl	ießen

Diese Exportdatei kann dann im Zertifikatemanager auf anderen Unified Runtime-PCs verwendet werden.

3.2 Geräte anlegen

Alle Geräte, für die ein Zertifikat benötigt wird, müssen auch als entsprechendes Gerät im Certificate Manager hinzugefügt werden.

Wählen Sie im WinCC Unified Certificate Manager "Add device" (über das Kontextmenü der zuvor erstellten CA) und fügen Sie das Gerät hinzu.

Beim Anlegen der Geräte können Sie zwischen folgenden Möglichkeiten wählen:

- Hostname & IP-Adresse (normale Konfiguration)
- Hostname & Domäne (in der Form [Domain-Name].[Hostname])
- IP-Adresse

Wenn sich Ihr Gerät in einer Domäne befindet, müssen Sie zwingend den Domänen-Namen mit angeben.

Hat Ihr Gerät eine dynamische IP-Adresse, lassen Sie die IP-Adresse bei dieser Angabe weg.

Abbildung 3-2					
WinCC Unified Certif	ïcate Manager				×
SIEMENS	Total	ly Integra	ted Au	tomat	tion
		Deutsch		\sim	0
Siemens.Automation.W	/inCCUnifed ProjectCA				
🛄 🛄 Neues Gerät	×				
Computername: IP-Adresse:	Galaxy_S10]			
	Erstellen Abbrechen				
				Schlie	eßen

Nachdem Sie (wie in den nächsten Kapiteln beschrieben) alle benötigten Zertifikate erstellt haben, können Sie alle Zertifikate auf einmal über das Kontextmenü des Geräts installieren. Die CA wird hierbei automatisch mit installiert.

Im Kapitel "<u>Installation von Zertifikaten auf verschiedenen Geräten</u>" wird beschrieben, wie Sie die Zertifikate auf ein Unified Comfort Panel übertragen können.

Vorgehen bei fehlendem DNS-Server

Sie können ab TIA Portal Unified V16 Update 2 die Runtime auf IP-Adresszugriff umstellen, sodass keine Namensauflösung benötigt wird. Starten Sie dazu die "WinCC Unified Configuration" und setzen Sie unter "User Administration" den Haken bei der Option "Die IP-Adresse für den Identity Provider…" ("Use the IP address for the Identity Provider…").



WinCC Unified Configuration	
SIEMENS	Totally Integrated Automation
WinCC Unified	Konfiguration der Benutzerverwaltung Bestehende Konfiguration übernehmen
Zertifikatsverwaltung	Aus dem TIA Portal deladene Konfiguration verwenden
 Benutzerverwaltung 	IP-Adresse für Identity Provider und Website verwenden
O Archiv-Einstellungen	
Reporting	UMC-Serveradresse
O Sicheres Herunterladen	Identity Provider-Adresse
Einstellungen anwenden	✓ Identity Provider-Adresse vom UMC-Server erzeugen.
	Die Konfiguration der Verbindung zum Benutzerverwaltungs-Server kann nach der Installation durch den TIA-Administrator erfolgen.
Deutsch 🗸	
	Abbrechen < Zurück Weiter >

3.3 Webserver-Zertifikat

Das Webserver-Zertifikat wird beim Aufruf der Unified Website automatisch an den Client geschickt, wird allerdings standardmäßig abgelehnt, da der Client die CA zuerst als nicht vertrauenswürdig einstuft.

Wurden alle Einstellungen richtig getroffen erscheint beim Aufruf der "WinCC

Unified" Startseite mittels "https://[Hostname]" nun der Punkt "Certificate Authority". Mithilfe dieser Schaltfläche können Sie die "Certificate Authority" auf den Clients installieren.

Abbildung 3-4

¥		¥	18	сж.	<u> </u>	1
۵	User n Manage your	nana	gen	nent		
0	WinCC Start your proj	Uni	fied	RT		
0	WinCC Shows help fo	Uni	fied	Hel	р	
٠	Certific Download and	ate /	Auth	ority	/	

Im Kapitel "Installation von Zertifikaten auf verschiedenen Geräten" wird beschrieben, wie Sie die CA auf den Clients installieren.

3.4 OPC UA Zertifikate (Server, Client, Exporter)

Damit Geräte eine verschlüsselte OPC UA Verbindung aufbauen können, müssen entsprechende Zertifikate zwischen Server und Client ausgetauscht werden.

Server-Zertifikat erstellen

Mithilfe des Server-Zertifikats weist sich der Server gegenüber den Clients aus.

Das Zertifikat kann über das Kontextmenü des Geräts erstellt werden und hat eine maximale Gültigkeitsdauer von 600 Monaten.

Abbildung 3-5	
📟 Neues OPC UA-Ze	rtifikat ×
Name:	OPCUA Server for Simatic WinCC Unified Runtime
Organisation:	Siemens AG
Organisationseinheit:	
Stadt:	
Bundesland:	
Land:	Zwei-Buchstaben-Code wie DE, US,
Antragstellername:	CN=OPCUA Server for Simatic WinCC Unified Runtime/O=Siemens AG/DC=WinCCUr
Schlüssellänge:	2048 ▼ Lebensdauer (Monate): 600 ◆
	Erstellen Abbrechen

Ab TIA V17 ist es möglich, eingehende Client-Zertifikate am Server über den Simatic Runtime Manager als vertrauenswürdig einzustufen.

Starten Sie hierzu den SIMATIC Runtime Manager und öffnen Sie die Einstellungen. Wechseln Sie in den Einstellungen in den Reiter Certificates. Dort

können Sie alle Zerifikate von Clients, die eine Verbindung mit dem OPC Server aufbauen möchten, als vertrauenswürdig einstufen.

Abbildung 3-6

eneral OPC UA Export Certificates Script	Debugger				
-5					
Subject	Issuer	Valid from	Valid until	Status	File name
OPC UA Exporter for Simatic WinCC U	OPC UA Exporter for	2021-01-08	2025-12-13	Trusted	OPC UA Export
OPCUA Server for Simatic WinCC Unifi	OPCUA Server for Sim	2021-01-08	2025-12-13	Trusted	OPCUA Server
UA Local Discovery Server	UA Local Discovery Se	2021-01-07	2024-01-07	Trusted	UA Local Discov
UaExpert@WINCCUNIF	"Expert@WINCCUN	2020-11-17	2025-11-16	Untrusted	UaExpert@WIN
😢 Reject					
Show.					
Delete					
E+ Export					

Client-Zertifikat erstellen

Mithilfe des Client-Zertifikats weist sich der Client gegenüber dem Server aus.

Das Zertifikat kann über das Kontextmenü des Geräts erstellt werden und hat eine maximale Gültigkeitsdauer von 600 Monaten.

Abbild	una	3-7

₽ Neues OPC UA Client-Instanz-Zertifikat ×						
Name:	OPC UA Client for Sin	natic WinCO	CUnified Runtime			
Organisation:	Siemens AG					
Organisationseinheit:						
Stadt:						
Bundesland:						
Land:	Zwei-Buchstaben-Co	de wie DE,	US,			
Antragstellername:	CN=OPC UA Client fo	or Simatic W	/inCC Unified Runtim	ie/O=Siemens AG/l	DC=WinCCUn	
Schlüssellänge:	2048	-	Lebensdauer (Mor	nate):	600 🖨	
				Erstellen	Abbrechen	

Exporter-Zertifikat erstellen

Mithilfe des Exporter-Zertifikats kann über den Runtime Manager das OPC Interface exportiert werden.

Dieser Export kann dann verwendet werden, um das Interface auf anderen OPC Clients (z.B. auf einer S7-1500 CPU) zu verwenden. So können Sie z.B. alle Variablen auf einen Client bringen, ohne auf den Server browsen zu müssen.

Das Zertifikat kann über das Kontextmenü des Geräts erstellt werden und hat eine maximale Gültigkeitsdauer von 600 Monaten.

Abbi	ldung	3-8
------	-------	-----

The Neues OPC UA Exporter-Zertifikat						
Name:	OPC UA Exporter for	Simatic Wi	nCC Unified Runtime			
Organisation:	Siemens AG					
Organisationseinheit:						
Stadt:						
Bundesland:						
Land:	Zwei-Buchstaben-Co	de wie DE,	US,			
Antragstellername:	CN=OPC UA Exporte	r for Simati	ic WinCC Unified Rur	ntime/O=Siemens	AG/DC=WinCC	
Schlüssellänge:	2048	•	Lebensdauer (Mor	nate):	600 🌩	
				Erstellen	Abbrechen	

Nachdem Sie das Exporter-Zertifikat erstellt haben können Sie, wenn der OPC Server läuft, über den Runtime Manager einen Export des Interfaces erstellen.

Öffnen Sie hierzu die Settings und wechseln Sie in den Reiter "OPC UA Export". Hier können Sie die Exportdatei erstellen.

.

Abbildung 3-9							
Settings						2	×
General OPC UA export	User management	Certificates	Script Debug	jer			
Settings							
Output file:	C:\User	s (Admin \Docu	iments\OPCExp	ort			
User name:	Admin						
Password:	•••••	••••					
Port:	4890						
					Exp	port	
Status							
					ОК	Exit	

3.5 Runtime Collaboration Zertifikat

Mit Unified Runtime Collaboration haben Sie die Möglichkeit auf Unified Runtime-Objekte, wie zum Beispiel Bilder eines anderen Bediengerätes, zuzugreifen. Sie können diese Bilder anzeigen und bedienen.

Da es sich hier um eine verschlüsselte Verbindung handelt, müssen Zertifikate ausgetauscht werden.

Ein Runtime Collaboration-Zertifikat kann über das Kontextmenü des Geräts erstellt werden und hat eine maximale Gültigkeit von 150 Monaten.

Damit die Zertifikate auf allen beteiligten Unified Runtimes akzeptiert werden, muss die CA auf allen Runtime-Systemen bekannt sein.

Der Export der CA ist im Kapitel Certificate Authority beschrieben.

Im Kapitel <u>"Installation von Zertifikaten auf verschiedenen Geräten</u>" wird beschrieben, wie Sie die Zertifikate auf ein Unified Comfort Panel übertragen können.

3.6 Audit Trail System Zertifikat

Mit dem Audit Trail System Zertifikat signieren Sie die Einträge des Audit Trails. Das Zertifikat kann über das Kontextmenü des Geräts angelegt werden und ist 150 Monate gültig.

4 Installation von Zertifikaten auf verschiedenen Geräten

4.1 Unified Comfort Panel

Um angelegte Zertifikate auf ein Unified Comfort Panel zu übertragen wählen Sie den Punkt "Alle Gerätezertifikate exportieren" über das Kontextmenü des Geräts im Certificate Manager aus und vergeben Sie ein Passwort für die Exportdatei.

Die Iterationsanzahl (Standard = 25000) kann beibehalten werden.

Übertragen Sie sich die erstellte Datei im Anschluss auf ein Speichermedium und schließen Sie es ans Panel an.

- 1. Öffnen Sie die Einstellungen
- 2. Wählen Sie "Security > Certificates"
- Klicken Sie auf "Import" Hier können Sie die Exportdatei auswählen und das Passwort und die Iterationsanzahl einstellen
- 4. Klicken Sie auf "Import". Im Anschluss werden die Zertifikate automatisch dem richtigen Zertifikatsspeicher zugeordnet.

Abbildung 4-1

-24	 SIMATIC HMI Unified Comfort
_	Security \ Certificates
0	Certificates on the device
	Certificate store: Certificate Authorities
O	Import certificate
	Select storage media X64 (Size:3.72 GB/Free: 🗸
- 660	Win10-20H2.enc
•	
3	Password: *****
Ŧ٨	Iteration: 25000 Delete
A	Import Cancel
	Certificate details
	Certificate name
	Status:

4.2 Android-Clients

- 1. Rufen Sie die "WinCC Unified" Startseite mittels "https://[Hostname]" auf und wählen Sie den Punkt "Certificate Authority" aus.
- 2. Öffnen Sie die Datei "ca.cert", benennen Sie das Zertifikat und wählen Sie bei Verwendung der Anmeldedaten "VPN und Apps" aus.

Abbildung 4-2



Dieses Vorgehen wurde beispielhaft für die Gesamtheit der Android Geräte auf einem Smartphone mit Android-Version 9 getestet und kann von Gerät zu Gerät abweichen.

4.3 IOS-Clients

- 1. Rufen Sie die "WinCC Unified" Startseite mittels "https://[Hostname]" auf und wählen Sie den Punkt "Certificate Authority" aus.
- 2. Klicken Sie bei "Laden eines Konfigurationsprofils" auf "zulassen" ("Allow").

Abbildung 5-3



Öffnen Sie nun die Einstellungen des iOS-Gerätes und wählen Sie im Reiter "Allgemein" den Punkt "Profil" aus. Wählen Sie nun in der aberen rechten Ecke "Instellioren" an

Wählen Sie nun in der oberen rechten Ecke "Installieren" an.

Abbildung 4-3			
13:20 Wed 15. Jan	Cancel Ins	stall Profile	≈ 89 % ■
Settings			
Q Search	Siemens.A	utomation.WinCCUr	nifed Proj
F: Har n 4 dd Apple ID, iCloud, iTunes & App St	Signed by Siemens.Autor Not Verified Contains Certificate	nation.WinCCUnifed Projec	tCA
	More Details		>
Profile Downloaded >			
	Remove D	ownloaded Profile	
Airplane Mode			
🛜 Wi-Fi			
Bluetooth On			
Mobile Data Off			
Notifications			
Sounds			
C Do Not Disturb			
Screen Time			
😥 General			
Control Centre			

- 3. Wählen Sie nun im Reiter "Allgemein" den Punkt "Info" aus und wählen Sie dort den Punkt "Zertifikatsvertrauenseinstellungen" aus.
- 4. Erteilen Sie der "WinCCUnifiedProjectCA" das "Volle Vertrauen für RootZertifikate".

Abbildung 5-5



Dieses Vorgehen ist beispielhaft für die Gesamtheit der iOS Geräte auf einem Tablet mit iOS Version 12 entstanden und kann von Gerät zu Gerät abweichen.

4.4 Browser mit eigenem Zertifikatsspeicher (Mozilla Firefox)

Firefox nutzt nicht den windowseigenen Zertifikatsspeicher, sondern legt einen separaten eigenen Zertifikatsspeicher an.

- 1. Rufen Sie die "WinCC Unified" Startseite mittels "https://[Hostname]" auf.
- 2. Wählen Sie den Punkt "Certificate Authority" ("CA") aus. Es erscheint das Fenster "Herunterladen des Zertifkats".
- 3. Wählen Sie "Dieser CA vertrauen, um Websites zu identifizieren" an.

Abbildung 4-1

Downloading Certificate	\times
You have been asked to trust a new Certificate Authority (CA).	
Do you want to trust "Siemens.Automation.WinCCUnifed ProjectCA" for the following pu	rposes?
✓ Trust this CA to identify websites.	
Trust this CA to identify email users.	
Before trusting this CA for any purpose, you should examine its certificate and its policy ar procedures (if available).	nd
View Examine CA certificate	
ОК	Cancel

 Sie erhalten beim Aufruf der "WinCC Unified" Startseite ein gelbes Ausrufezeichen neben dem Schloss-Symbol.
 Klicken Sie auf das Symbol und wählen Sie bei den Verbindungsdetails "Ausnahme entfernen".

Abbildung 4-2



4.5 Browser ohne eigenen Zertifikatsspeicher (Chrome, Edge, ...)

1. Rufen Sie die "WinCC Unified" Startseite mittels "https://[Hostname]" auf und wählen Sie den Punkt "Certificate Authority" aus.

- 2. Öffnen Sie die Datei "ca.cert" und akzeptieren Sie die Sicherheitswarnung.
- 3. Fügen Sie anschließend analog zu Schritt 3 in Kap. <u>4.4</u> die Stammzertifizierungsstelle hinzu.

Abbildung 5-1

pen File -	Security Warn	ing	×
Do you v	vant to open	this file?	
_	Name: Publisher: Type: From:	C:\Users\ Downloads\ca.crt Unknown Publisher Security Certificate C:\Users\ Downloads\ca.crt	
⊡ Al <u>w</u> ay	while files from your co	opening this file	itially this