SIEMENS

SIMATIC HMI

WinCC (TIA Portal) Liesmich Runtime Professional

Liesmich

Online-Dokumentation

06/2022
Online-Dokumentation

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠ **GEFAHR**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **WARNUNG**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **VORSICHT**
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠ **WARNUNG**
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokumentbestellnummer: Online-Dokumentation
Ⓟ 06/2022 Änderungen vorbehalten

Inhaltsverzeichnis

Gültigkeit

1

Gültigkeit

Dieses Update ist für folgende Produkte gültig:

- WinCC Runtime Professional V17

Hinweis

Wenn Sie nach der Installation des Updates Ihr System mit der Produkt-DVD modifizieren, müssen Sie das Update erneut ausführen.

Wichtige Hinweise

2

Diese Seite beinhaltet wichtige Hinweise zu Produkt-Eigenschaften

Hinweis

Wenn die Runtime im Kioskmodus mit deaktivierten Shortcut-Tasten im Fullscreen betrieben wird, sollten Sie die Zugriffe auf die Online-Hilfe in ActiveX-Controls unterbinden, da ansonsten der Bediener Zugriff auf das Betriebssystem erlangen kann.

Zeichensätze nach Windows 10-Update

Seit dem Windows 10-Update Version 1809 bietet Windows die Möglichkeit Zeichensätze entweder mit Administratorrechten für jeden Benutzer (Befehl "Für alle Benutzer installieren" im Kontextmenü) oder benutzerspezifisch zu installieren. Um in WinCC Zeichensätze uneingeschränkt nutzen und auf ein Bediengerät laden zu können, müssen Zeichensätze immer mit Administratorrechten installiert werden.

Bitte beachten Sie, dass die Schaltfläche "installieren" in der Ansicht eines Zeichensatzes nur eine benutzerspezifische Installation durchführt.

NTLMv1 und SMBv1 deaktivieren

Die Protokolle NTLMv1 und SMBv1 können deaktiviert werden. Die Deaktivierung der Protokolle hat keinen Einfluss auf den Betrieb von WinCC Runtime Professional.

Hinweis

Sicherheitsrisiko durch NTLMv1 und SMBv1

Die Verwendung der Protokolle NTLMv1 und SMBv1 stellt ein erhebliches Sicherheitsrisiko dar. Die Kommunikation im Netzwerk kann z. B. durch Man-in-the-Middle-Angriffe kompromittiert werden.

Abhängig vom Betriebssystem unterscheidet sich das Vorgehen zur Deaktivierung der Protokolle.

Verbesserungen in Update 4 SR1

3

Dieses Update enthält folgende Verbesserungen und Änderungen:

Stabilität und Performance

Stabilität und Performance wurden u. a. auf Basis von Rückmeldungen verbessert.

Verhalten der Bildschirmtastatur

Das Verhalten der Bildschirmtastatur wurde verbessert. Um diese Verbesserungen auch für das Anmelden über SIMATIC Logon nutzen zu können, benötigen Sie zusätzlich SIMATIC Logon V1.6 Update 5. Sie finden dieses Update im Industry Online Support (https://support.industry.siemens.com/cs/ww/de/view/109794407) unter der Beitrags-ID 109794407.

Bilder und Bildobjekte

Werte, die mit der Bildschirmtastatur in ein EA-Feld eingegeben werden, werden immer korrekt übernommen.

Die Bedienung des Mausrads an einem Symbolischen EA-Feld führt nicht zu einer ungewollten Veränderung von Werten.

Der Zustand einer Schaltfläche wird wieder korrekt dargestellt, auch wenn linke und rechte Maustaste gleichzeitig gedrückt werden.

Archivierung

Meldearchive benötigen wieder genauso viel Speicherplatz wie in V16.

Scripting

Änderungen, die mit einem VB-Skript am Text eines editierbaren Textfeldes vorgenommen werden, werden korrekt angezeigt.

Rezepturen

Die Darstellung von Datum und Uhrzeit in niederländischem Format wurde korrigiert..

Bildschirmtastatur

Die Bildschirmtastatur unterstützt japanisches Layout.

Redundante Systeme

Die Stabilität während der Redundanzumschaltung des Tag Logging wurde verbessert.

Web Navigator

Die Darstellung von Bildfenstern wurde verbessert.

Data Monitor

Die Ausgabe von Daten im Excel-Workbook wurde verbessert.

Information Server

Die Diagnose des Information Servers kann wieder gestartet werden.

Verbesserungen in Update 4

4

Dieses Update enthält folgende Verbesserungen und Änderungen:

Setzen der Hintergrundfarbe über VB-Skript

Die Eigenschaft Hintergrundfarbe kann bei folgenden Objekten auch über VB-Skript korrekt gesetzt werden: Linie, Polygonzug, Kreisbogen, Ellipsenbogen, Verbinder

Verbesserungen in Update 3 SR1

5

5.1 Verbesserungen in Update 3 SR1

Dieses Update enthält folgende Verbesserungen und Änderungen:

Stabilität und Performance

Stabilität und Performance wurden u. a. auf Basis von Rückmeldungen verbessert.

Bildschirmtastatur

Bei der Bildschirmtastatur wurde die Reaktionszeit beim Öffnen und das Verhalten beim Beenden von Runtime verbessert.

Symbolisches EA-Feld

Wenn die Sichtbarkeit von z. B. Objektgruppen geändert wird, hat sich das Verhalten von verwendeten symbolischen EA-Feldern verbessert.

Bildfenster bei Multi-Monitor-Betrieb

Die Darstellung von unabhängigen Bildfenstern im Multi-Monitor-Betrieb wurde verbessert.

Startverhalten der Runtime

Wenn keine Netzwerkverbindung besteht, wurde das Startverhalten der Runtime verbessert.

ALARM_DQ Meldungen

Alarm_DQ Meldungen werden in der Meldeanzeige korrekt angeziegt.

Allen-Bradley

Wenn nicht konfigurierte Variablen verwendet werden, ist die Kommunikation über den Allen-Bradley-Kanals verbessert.

WebNavigator

WebNavigator-Clients V17 können sich auch mit WebNavigator-Servern anderer Versionen verbinden.

5.2 Sichere Kommunikation über Zertifikate

Die zertifikatbasierte Kommunikation von Runtime Professional wurde erweitert.

Übersicht

Unterstützte S7-Steuerungen

Runtime Professional V17 kann nun mit folgenden S7-Steuerungen über Zertifikate kommunizieren:

- S7-1500 Steuerungen ab der Firmware 2.9
- S7-1200 Steuerungen ab der Firmware 4.5

Hinweis

Alle folgenden Aussagen gelten nur für S7-Steuerungen mit dieser Firmware.

Erweiterungen

Die zertifikatbasierte Kommunikation zwischen Runtime Professional und S7-Steuerungen wurde folgendermaßen erweitert:

- Die Kommunikation zwischen HMI-Geräten und S7-Steuerungen mit einer nicht-integrierten Verbindung unterstützt nun selbstsignierte Zertifikate.
- Das Hochrüsten von S7-Steuerungen wurde vereinfacht. Ein Hochrüsten in TIA Portal ist nicht mehr zwingend notwendig.
  Eine S7-Steuerung, die nur im Feld hochgerüstet wurde, kommuniziert nun über ein selbstsigniertes Zertifikat mit dem HMI-Gerät. Das selbstsignierte Zertifikat wird automatisch aus der Steuerung in den Zertifikatsspeicher des HMI-Geräts geladen.

Um diese Funktionen zu nutzen, aktivieren Sie an dem HMI-Gerät die Option "ForceSecure".

Einsatz von selbstsignierten Zertifikaten

Beim Einsatz von selbstsignierten Zertifikaten haben Sie die folgenden Möglichkeiten:

- Verwenden Sie ein in TIA Portal erzeugtes selbstsigniertes Zertifikat.
  Verwenden Sie das beim Hinzufügen einer S7-Steuerung oder Hochrüsten einer existierenden S7-Steuerung automatisch angelegte Zertifikat. Oder wählen Sie Zertifikatseinstellungen, die von den Standardeinstellungen abweichen, und erzeugen Sie selber ein selbstsigniertes Zertifikat.
  Beim Laden wird das Zertifikat in den Runtime-Projektordner geladen.
- Verwenden Sie ein selbstsigniertes Default-Zertifikat.
  Stellen Sie in TIA Portal für eine Steuerung kein Zertifikat bereit und aktivieren Sie an dem HMI-Gerät für den Verbindungstyp der Steuerung die Option "ForceSecure".
  Beim Laden in die Steuerung wird ein selbstsigniertes Zertifikat erzeugt. Das Zertifikat wird beim ersten Verbindungsversuch zwischen Steuerung und HMI-Gerät in den Zertifikatsspeicher des HMI-Geräts kopiert. Nach dem Umkopieren des Zertifikats in den Ordner mit den vertrauenswürdigen Zertifikaten wird dieses Zertifikat für die Kommunikation verwendet.

Option "ForceSecure" aktivieren oder deaktivieren

Einleitung

Die Option "ForceSecure" stellt für folgende Verbindungen sicher, dass die Kommunikation zwischen HMI-Gerät und S7-Steuerung durch ein Zertifikat geschützt wird:

- Nicht-integrierte Verbindungen
- Verbindungen, für die in TIA Portal kein Zertifikat konfiguriert wurde

Wenn die Option aktiviert ist und im Runtime-Projektordner kein PLC-Zertifikat gefunden wird, sucht Runtime im Zertifikatsspeicher des HMI-Geräts im Ordner "trusted" nach einem passenden Zertifikat.

Hinweis

Die Option wirkt sich nicht auf die Kommunikation mit S7-Steuerungen aus, die keine Zertifikate unterstützen.

Voreinstellung

Die Option ist in der Standardeinstellung für integrierte Verbindungen, nicht-integrierte Verbindungen und Geräte-Proxys deaktiviert.

Vorgehen

Hinweis

Es wird empfohlen, die Option für alle Verbindungstypen zu aktivieren.

Um die Option für ein HMI-Gerät zu konfigurieren, gehen Sie folgendermaßen vor:

1. Legen Sie die Datei "ForceSecure.xml" an.
2. Kopieren Sie die folgende XML-Struktur in die Datei:
```
<?xml version="1.0"?>
   <root>
   <NonIntegrated>true</NonIntegrated>
   <Integrated>true</Integrated>
   <IntegratedProxy>true</IntegratedProxy>
   </root>
```
3. Um die Auswertung des Zertifikatsspeichers für einen der Verbindungstypen zu deaktivieren, setzen Sie seinen Knoten auf "false".

   Hinweis

   Für nicht-integrierte Verbindungen ist in dem Fall keine zertifikatgeschützte Kommunikation möglich.

   Für integrierte Verbindungen und Geräte-Proxy ist eine zertifikatgeschützte Kommunikation nur nach dem Hochrüsten der Steuerungen in TIA Portal möglich.

4. Kopieren Sie die Datei auf dem Engineering-Gerät in das TIA-Projektverzeichnis des Projekts, dem das HMI-Gerät hinzugefügt wurde, in den folgenden Ordner:
"...\AdditionalFiles\Rdp"
5. Übersetzen und Laden Sie das HMI-Gerät.
Ihre Einstellungen werden auf die Kommunikation zwischen dem HMI-Gerät und seine verbundenen S7-Steuerungen angewendet.

Um die Option "ForceSecure" für alle in TIA Portal erstellten Projekte zentral zu konfigurieren, gehen Sie folgendermaßen vor:

1. Führen Sie Schritt 1 bis 3 aus wie oben beschrieben.
2. Kopieren Sie die Datei auf dem Engineering-Gerät in das Programmverzeichnis "C:\ProgramData\Siemens\Automation\ConfigFiles\RDP".
3. Um für einzelne Projekte eine abweichende Konfiguration zu verwenden, gehen Sie wie oben in Schritt 1 bis 4 beschrieben vor.

Wenn die XML-Datei im Programmverzeichnis und im TIA Projektverzeichnis liegt, greift die Konfiguration aus dem Projektverzeichnis.

S7-Steuerungen hochrüsten

Für den Einsatz von selbstsignierten Zertifikaten haben Sie die hier beschriebenen Möglichkeiten.

Hochrüsten im Feld ohne Hochrüsten der S7-Steuerung in TIA Portal

Voraussetzung:
An dem mit einer S7-Steuerung verbundenen HMI-Gerät ist die Option „ForceSecure" für den Verbindungstyp der S7-Steuerung aktiviert.

Vorgehen:

1. Rüsten Sie in TIA Portal das HMI-Gerät hoch.
2. Tauschen Sie die S7-Steuerung und das HMI-Gerät im Feld aus.
3. Laden Sie die S7-Steuerung und das HMI-Gerät.
Nach dem Laden enthält der Runtime-Projektordner kein Zertifikat für diese S7-Steuerung.
4. Starten Sie Runtime.
Beim ersten Verbindungsversuch wird das selbstsignierte Zertifikat automatisch aus der S7-Steuerung geladen. Es landet im Zertifikatsspeicher des HMI-Geräts im folgenden Ordner:
`%PROGRAMDATA%\Siemens\Automation\device-certificate-store\untrusted`
5. Kopieren Sie das PLC-Zertifikat im Zertifikatsspeicher des HMI-Geräts händisch oder per Script in den Ordner mit den vertrauenswürdigen Zertifikaten:
`%PROGRAMDATA%\Siemens\Automation\device-certificate-store\trusted\certs`

Hochrüsten im Feld und Hochrüsten in TIA Portal

Vorgehen für integrierte Verbindungen und Geräte-Proxy:

1. Rüsten Sie in TIA Portal die S7-Steuerung und das HMI-Gerät hoch.
2. Tauschen Sie die S7-Steuerung und das HMI-Gerät im Feld aus.

3. Laden Sie die S7-Steuerung und das HMI-Gerät.
   Der Runtime-Projektordner enthält nach dem Laden das Zertifikat dieser S7-Steuerung.
4. Starten Sie Runtime.
   HMI-Gerät und Steuerung vertrauen gegenseitig ihren Zertifikaten. Für Sie fallen keine weiteren Schritte an.

Vorgehen für nicht-integrierte Verbindungen:

1. Rüsten Sie in TIA Portal die S7-Steuerung und das HMI-Gerät hoch.
2. Aktivieren Sie für das HMI-Gerät die Option "ForceSecure" für den Verbindungstyp nicht-integrierte Verbindung.
3. Tauschen Sie die Steuerung und das HMI-Gerät im Feld aus.
4. Laden Sie die Steuerung und das HMI-Gerät.
   Nach dem Laden enthält der Runtime-Projektordner kein Zertifikat dieser S7-Steuerung.
5. Starten Sie Runtime.
   Beim ersten Verbindungsversuch wird das selbstsignierte Zertifikat automatisch aus der S7-Steuerung geladen. Es landet im Zertifikatsspeicher des HMI-Geräts im folgenden Ordner:
   `%PROGRAMDATA%\Siemens\Automation\device-certificate-store\untrusted`
6. Kopieren Sie das PLC-Zertifikat im Zertifikatsspeicher des HMI-Geräts händisch oder per Script in den Ordner mit den vertrauenswürdigen Zertifikaten:
   `%PROGRAMDATA%\Siemens\Automation\device-certificate-store\trusted\certs`
   HMI-Gerät und Steuerung vertrauen gegenseitig ihren Zertifikaten.

Alternativ können Sie das PLC-Zertifikat vorab aus TIA Portal exportieren und vor dem Start von Runtime in den Ordner "`...\trusted\certs`" kopieren. Die Zertifikatsdatei muss den folgenden Namen haben:

"S7PlusChannel_<PLC_IP>.der", z. B. "S7PlusChannel_192.168.0.1.der"

Verbesserungen in Update 3

6

Inhalt

Dieses Update enthält keine für WinCC Runtime Professional relevanten Verbesserungen oder Änderungen.

Verbesserungen in Update 2

7

Dieses Update enthält folgende Verbesserungen und Änderungen:

Stabilität und Performance

Stabilität und Performance wurden u. a. auf Basis von Rückmeldungen verbessert.

Verbesserungen in Update 1

8

Dieses Update enthält folgende Verbesserungen und Änderungen:

Stabilität und Performance

Stabilität und Performance wurden u. a. auf Basis von Rückmeldungen verbessert.