

SINUMERIK

MindSphere Application Manage MyMachines - Installation in bestehende Steuerungsumgebungen

Anwendungsbeispiele

Vorwort

Grundlegende
Sicherheitshinweise **1**

Einleitung **2**

Installation/Konfiguration **3**

Fehlerbehandlung **4**


Anhang **A**


Gültig für Steuerung:
SINUMERIK 840D pl/ 840D sl/ 840DE sl
Software
Manage MyMachines, Version 02.00.01.00


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.

Vorwort

SINUMERIK-Dokumentation

Die SINUMERIK-Dokumentation ist in folgende Kategorien gegliedert:

- Allgemeine Dokumentation/Kataloge
- Anwender-Dokumentation
- Hersteller-/Service-Dokumentation

Weiterführende Informationen

Unter folgender Adresse (<https://support.industry.siemens.com/cs/de/de/view/108464614>) finden Sie Informationen zu den Themen:

- Dokumentation bestellen/Druckschriftenübersicht
- Weiterführende Links für den Download von Dokumenten
- Dokumentation online nutzen (Handbücher/Informationen finden und durchsuchen)

Bei Fragen zur technischen Dokumentation (z. B. Anregungen, Korrekturen) senden Sie eine E-Mail an folgende Adresse (<mailto:docu.motioncontrol@siemens.com>).

mySupport/Dokumentation

Unter folgender Adresse (<https://support.industry.siemens.com/My/ww/de/documentation>) finden Sie Informationen, wie Sie Ihre Dokumentation auf Basis der Siemensinhalte individuell zusammenstellen und für die eigene Maschinendokumentation anpassen.

Training

Unter folgender Adresse (<http://www.siemens.de/sitrain>) finden Sie Informationen zu SITRAIN - dem Training von Siemens für Produkte, Systeme und Lösungen der Antriebs- und Automatisierungstechnik.

FAQs

Frequently Asked Questions finden Sie in den Service&Support-Seiten unter Produkt Support (<https://support.industry.siemens.com/cs/de/de/ps/faq>).

SINUMERIK

Informationen zu SINUMERIK finden Sie unter folgender Adresse (<http://www.siemens.de/sinumerik>).

Zielgruppe

Die vorliegende Druckschrift wendet sich an:

- Projektueure
- Technologen (von Maschinenherstellern)
- Inbetriebnehmer (von Systemen/Maschinen)
- Programmierer
- Anwender

Nutzen

Das Funktionshandbuch beschreibt die Funktionen, so dass die Zielgruppe die Funktionen kennen und auswählen kann. Es ist dazu geeignet die Zielgruppe zu befähigen, die Funktionen in Betrieb zu nehmen.

Standardumfang

In der vorliegenden Dokumentation ist die Funktionalität des Standardumfangs beschrieben. Ergänzungen oder Änderungen, die durch den Maschinenhersteller vorgenommen werden, werden vom Maschinenhersteller dokumentiert.

Es können in der Steuerung weitere, in dieser Dokumentation nicht erläuterte Funktionen ablauffähig sein. Es besteht jedoch kein Anspruch auf diese Funktionen bei der Neulieferung bzw. im Servicefall.

Ebenso enthält diese Dokumentation aus Gründen der Übersichtlichkeit nicht sämtliche Detailinformationen zu allen Typen des Produkts und kann auch nicht jeden denkbaren Fall der Aufstellung, des Betriebes und der Instandhaltung berücksichtigen.

Hinweis zur Datenschutzgrundverordnung

Siemens beachtet die Grundsätze des Datenschutzes, insbesondere die Gebote der Datenminimierung (privacy by design). Für dieses Produkt bedeutet dies:

Das Produkt verarbeitet/speichert keine personenbezogenen Daten, lediglich technische Funktionsdaten (z. B. Zeitstempel). Verknüpft der Anwender diese Daten mit anderen Daten (z. B. Schichtpläne) oder speichert er personenbezogene Daten auf dem gleichen Medium (z. B. Festplatte) und stellt so einen Personenbezug her, hat er die Einhaltung der datenschutzrechtlichen Vorgaben selbst sicherzustellen.

Technical Support

Landesspezifische Telefonnummern für technische Beratung finden Sie im Internet unter folgender Adresse (<https://support.industry.siemens.com/sc/ww/de/sc/2090>) im Bereich "Kontakt".

Um eine technische Frage zu stellen, nutzen Sie das Online-Formular im Bereich "Support Request".


Inhaltsverzeichnis


	Vorwort	3
1	Grundlegende Sicherheitshinweise	7
1.1	Allgemeine Sicherheitshinweise.....	7
1.2	Gewährleistung und Haftung für Applikationsbeispiele.....	8
1.3	Security-Hinweise	9
2	Einleitung.....	11
2.1	Übersicht.....	11
2.2	Systemvoraussetzungen.....	12
3	Installation/Konfiguration	15
3.1	SINUMERIK-Steuerung mit HMI-Advanced.....	15
3.2	SINUMERIK-Steuerung mit SINUMERIK Operate.....	23
3.3	SINUMERIK-Steuerung mit MindSphere verbinden	26
3.4	SIMATIC IoT2040	27
3.4.1	SIMATIC IoT2000 SD-Karten Beispiel Image auf IoT2040.....	27
3.4.2	Infrastruktur	31
3.4.3	Apache http.....	35
3.4.4	Apache http konfigurieren	39
3.4.5	SINUMERIK-Steuerungen konfigurieren.....	68
3.4.5.1	Übersicht.....	68
3.4.5.2	SINUMERIK-Steuerung mit HMI-Advanced - Proxy einstellen	69
3.4.5.3	SINUMERIK-Steuerung mit SINUMERIK Operate - Proxy einstellen.....	78
3.4.6	Root Zugang zur IoT2040 Box sichern - optional.....	81
3.4.6.1	Passwort für den Root Benutzer setzen.....	81
3.4.6.2	SSH Schlüsselpaare generieren	82
3.4.6.3	Private Key im Putty Format generieren	83
3.4.6.4	Mit Private Key an den IoT2040 anbinden	85
3.5	Inbetriebnahme 3rdPartyController/ FANUC/ MTConnect.....	88
3.5.1	Übersicht.....	88
3.5.2	SINUMERIK Integrate Client installieren.....	89
3.5.3	Installation mit dem 3rdPartyController	99
3.5.4	Aktuellen Treiber mit dem Fanuc Treiber ersetzen	101
3.5.5	Aktuellen Treiber mit dem MTConnect Treiber ersetzen	102
3.5.6	FanucModule und MindSphere konfigurieren	105
3.5.7	MTConnect und MindSphere konfigurieren	106
3.5.8	Variable einbinden	108
3.5.9	MTConnect - Beispiel: Variable einbinden	111
3.5.10	3rdPartyController deinstallieren.....	116
4	Fehlerbehandlung.....	117
4.1	SINUMERIK Integrate/ePS-Client Log Files	117

4.2	FanucModule Service und Logs.....	118
4.3	Alarmmeldung	120
A	Anhang	121
A.1	Liste der Abkürzungen	121
	Index.....	123

Grundlegende Sicherheitshinweise

1.1 Allgemeine Sicherheitshinweise

 WARNUNG
Lebensgefahr bei Nichtbeachtung von Sicherheitshinweisen und Restrisiken
Bei Nichtbeachtung der Sicherheitshinweise und Restrisiken in der zugehörigen Hardware-Dokumentation können Unfälle mit schweren Verletzungen oder Tod auftreten.
<ul style="list-style-type: none">• Halten Sie die Sicherheitshinweise der Hardware-Dokumentation ein.• Berücksichtigen Sie bei der Risikobeurteilung die Restrisiken.

 WARNUNG
Fehlfunktionen der Maschine infolge fehlerhafter oder veränderter Parametrierung
Durch fehlerhafte oder veränderte Parametrierung können Fehlfunktionen an Maschinen auftreten, die zu Körperverletzungen oder Tod führen können.
<ul style="list-style-type: none">• Schützen Sie die Parametrierung vor unbefugtem Zugriff.• Beherrschen Sie mögliche Fehlfunktionen durch geeignete Maßnahmen, z. B. NOT-HALT oder NOT-AUS.

1.2 Gewährleistung und Haftung für Applikationsbeispiele

Applikationsbeispiele sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit hinsichtlich Konfiguration und Ausstattung sowie jeglicher Eventualitäten.

Applikationsbeispiele stellen keine kundenspezifischen Lösungen dar, sondern sollen lediglich Hilfestellung bieten bei typischen Aufgabenstellungen.

Als Anwender sind Sie für den sachgemäßen Betrieb der beschriebenen Produkte selbst verantwortlich. Applikationsbeispiele entheben Sie nicht der Verpflichtung zu sicherem Umgang bei Anwendung, Installation, Betrieb und Wartung.

1.3 Security-Hinweise

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 einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter:

<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie 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:

<https://www.siemens.com/industrialsecurity> (<https://new.siemens.com/global/en/products/services/cert.html#Subscriptions>)

Weitere Informationen finden Sie im Internet:

Projektierungshandbuch Industrial Security (<https://support.industry.siemens.com/cs/ww/de/view/108862708>)

WARNUNG

Unsichere Betriebszustände durch Manipulation der Software

Manipulationen der Software, z. B. Viren, Trojaner oder Würmer, können unsichere Betriebszustände in Ihrer Anlage verursachen, die zu Tod, schwerer Körperverletzung und zu Sachschäden führen können.

- Halten Sie die Software aktuell.
- Integrieren Sie die Automatisierungs- und Antriebskomponenten in ein ganzheitliches Industrial Security-Konzept der Anlage oder Maschine nach dem aktuellen Stand der Technik.
- Berücksichtigen Sie bei Ihrem ganzheitlichen Industrial Security-Konzept alle eingesetzten Produkte.
- Schützen Sie die Dateien in Wechselspeichermedien vor Schadsoftware durch entsprechende Schutzmaßnahmen, z. B. Virens Scanner.
- Prüfen Sie beim Abschluss der Inbetriebnahme alle security-relevanten Einstellungen.
- Schützen Sie den Antrieb vor unberechtigten Änderungen, indem Sie die Umrichterfunktion "Know-How-Schutz" aktivieren.

Einleitung

2.1 Übersicht

Dieses Dokument informiert Sie darüber, wie Sie bestehende Steuerungsumgebungen mit der Applikation "Manage MyMachines" verbinden.

- SINUMERIK-Steuerung mit HMI-Advanced (Seite 15)
- SINUMERIK-Steuerung mit SINUMERIK Operate (Seite 23)
- SINUMERIK-Steuerung mit MindSphere verbinden (Seite 26)
- SIMATIC IoT2040 (Seite 27)
- Inbetriebnahme 3rdPartyController/ FANUC/ MTConnect (Seite 88)

2.2 Systemvoraussetzungen

Wenn Sie "Manage MyMachine" mit einer bereits bestehenden Steuerungsumgebung verbinden möchten, beachten Sie folgende Voraussetzungen.

Voraussetzung

Für die Verbindung mit MindSphere benötigen Sie eine neue Version des SINUMERIK Integrate-Clients. Installieren und konfigurieren Sie den Client nachträglich.

Hinweis

Windows XP

Windows XP und ältere Windows Versionen unterstützen zur sicheren Datenübertragung das TLS1.2 Verschlüsselungsprotokoll nicht, das zwingend nötig ist für eine Verbindung zur MindSphere.

Hardware und Bediensoftware

Die nachfolgende Vorgehensweise ist beispielhaft mit folgenden Komponenten erstellt:

Tabelle 2-1 SINUMERIK 840D pl

Bediensoftware Version	SINUMERIK Integrate Client-Software Version	Hardware Version	Operating System
HMI-Advanced V07.06.02.05	V4.12.0.21	PCU 50.3B	WinXP SP3
		PCU Base 8.6	
HMI-Advanced V07.06	V4.12.0.21	PCU 50.1	
		PCU 50.3B	
HMI-Advanced V06.04	V4.12.0.21	PCU 50.1	
		PCU 50.3B	
HMI-Advanced V06.04.28.00	V4.12.0.21	PCU 50.2 mit 566 MHz	WinNT 4.0
		PCU Base 7.3.5	
SINUMERIK Operate V2.7.3.10	V4.12.0.21	PCU 50.3	WinXP ab V8.6 SP3
		PCU 50.5	WinXP ab V1.3

Voraussetzung für MTConnect und Fanuc

Folgende Voraussetzungen müssen für die Installation erfüllt sein:

- ePS-Client
- .NET 4.0 oder eine höhere Version
- Visual C++ (redistributable für Visual Studio 2015 oder eine höhere Version)
- Windows Update auf dem neuesten Stand

Sicherheitshinweise

ACHTUNG

Sicherheitsstandards für SINUMERIK-Steuerungen an MindSphere

Die Anbindung von SINUMERIK-Steuerungen an MindSphere über TLS 1.2 /https genügt höchsten Sicherheitsstandards.

SINUMERIK-Versionen, die diese Standards nicht erfüllen, sind nicht Produktbestandteil. Für diese Versionen sind zusätzliche sicherheitstechnische Maßnahmen erforderlich.

Sie sind dafür verantwortlich, unbefugten Zugriff auf Ihre 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.

ACHTUNG

Datenmissbrauch durch ungeschützte Internet-Verbindung

Durch uneingeschränkte Internet-Verbindung kann es zu Datenmissbrauch kommen.

Beachten Sie, dass Sie vor Aufbau einer Netzwerk-Verbindung sicherstellen, dass Ihr PC ausschließlich über eine geschützte Verbindung mit dem Internet verbunden ist. Achten Sie dabei auf die sicherheitsrelevanten Hinweise.

Weitere Informationen über die Kommunikationssicherheit finden Sie im Projektierungshandbuch: Industry Security (<https://support.industry.siemens.com/cs/ww/de/view/108862708>).

Hinweis

Sicherung des Bedien-PCs

Die notwendigen Sicherheitsmaßnahmen (z. B. Virusscanner, Firewalls, OS Patching usw.) müssen auf den PCs implementiert sein, die für die Visualisierung und Konfiguration von Manage MyMachines beim Maschinenbediener oder Endkunden verwendet werden.

Weitere Informationen zum PC im Industrieumfeld finden Sie im Projektierungshandbuch: Industry Security (<https://support.industry.siemens.com/cs/ww/de/view/108862708>).

Hinweis

Sicherung der SINUMERIK-Steuerung

Die notwendigen Sicherheitsmaßnahmen (z. B. Virusscanner, Firewalls, OS Patching usw.) müssen auf den PCUs/IPCs implementiert sein.

Weitere Informationen über die Kommunikationssicherheit finden Sie im Projektierungshandbuch: Industry Security (<https://support.industry.siemens.com/cs/ww/de/view/108862708>).

Software

Die Anbindung erfolgt über den integrierten SINUMERIK Integrate Client.

Benutzen Sie immer die aktuellste Version.

Hinweis

Parallelbetrieb mit SINUMERIK Integrate Anwendungen

Der Parallelbetrieb mit den Anwendungen von SINUMERIK Integrate ist nicht möglich.

Lieferform

Der SINUMERIK Integrate-Client sowie neueste Updates und weitere Informationen zu den Anwendungen und Produkten, werden auf PridaNet abgelegt und können direkt von dort heruntergeladen werden.

- ODER -

Sie kontaktieren Ihren Maschinenhersteller.

- ODER -

Sie wenden sich an den Siemens Service&Support.

Weitere Informationen

Weitere Informationen zu SINUMERIK Integrate finden Sie im Inbetriebnahmehandbuch SINUMERIK Integrate MMP, MMT, AMC, AMP, AMM/E, AMD

Zusätzliche Informationen

Bei Anbindungen von SINUMERIK-Steuerungen, die nicht der aktuellen Generation entsprechen, müssen Sicherheitsanforderungen besonders berücksichtigt werden.

Die Sicherheitsanforderungen der MindSphere nach aktuellem Stand der Technik müssen für solche Steuerungen entsprechend betrachtet und durch weitere Maßnahmen und Netzwerk-Komponenten innerhalb der lokalen IT-Umgebung sichergestellt werden.

- Es muss sichergestellt sein, dass die Kommunikation zwischen Fabriknetzwerk und MindSphere den aktuellen Sicherheitsstandards genügt, z. B. TLS 1.2.
- Es muss sichergestellt sein, dass unbefugter Zugriff auf die Steuerung in der Firmennetz- / Fabriknetzwerkumgebung sowie Angriffe auf die Firewall vor Steuerung nicht möglich sind.
- Es muss sichergestellt sein, dass die Kommunikation innerhalb der Fabriknetzumgebung nicht angegriffen werden kann.

Dabei müssen die Richtlinien der kundenseitigen IT-Abteilung berücksichtigt werden.

Installation/Konfiguration

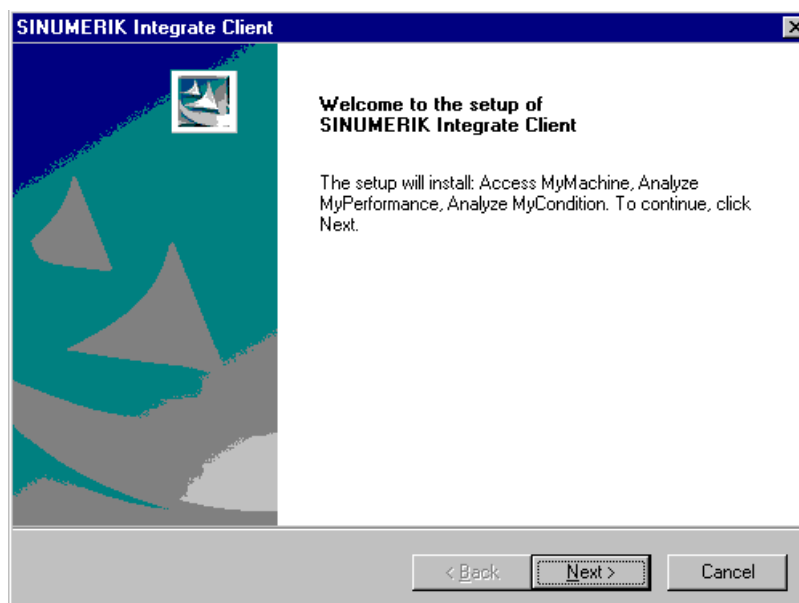
3.1 SINUMERIK-Steuerung mit HMI-Advanced

Voraussetzung

Um eine Verbindung zu MindSphere herzustellen, muss der TLS 1.2 Support aktiviert sein. Die Beschreibung finden Sie in folgendem Handbuch: Installationshandbuch SINUMERIK Integrate

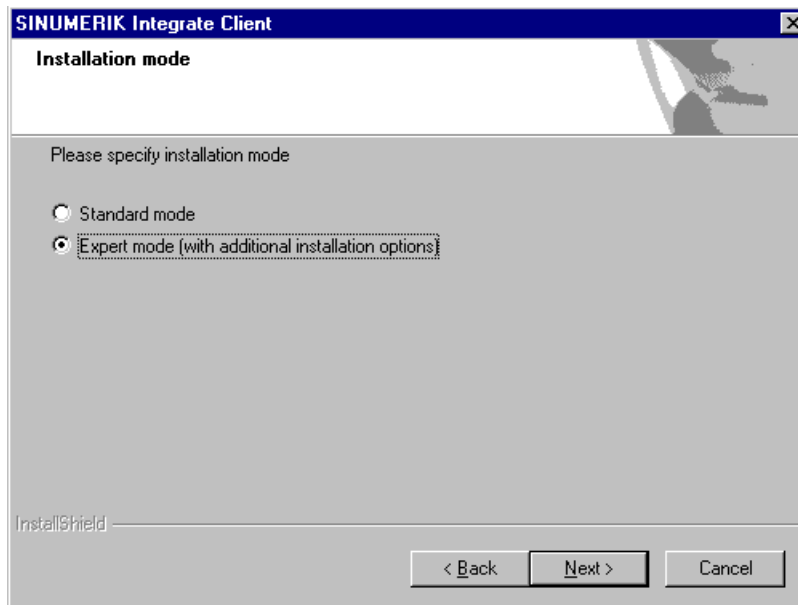
Vorgehensweise

1. Starten Sie die SINUMERIK-Steuerung im Windows Servicemodus.
2. Öffnen Sie das Installationsverzeichnis.
3. Starten Sie die Setup-Datei "setup.exe" mit Doppelklick.
 - Wenn Sie nicht den passenden Internet Explorer installiert haben, erhalten Sie eine entsprechende Meldung, z. B. "Das Programm benötigt den Internet Explorer 6 oder höher".
Die Installation wird abgebrochen und Sie müssen zuerst den entsprechenden Internet Explorer installieren.
Anschließend starten Sie die Client-Installation erneut.
4. Der Willkommensdialog wird geöffnet.
Die Installationssprache ist Englisch.
Klicken Sie auf die Schaltfläche "Next >", um mit der Installationsvorbereitung zu beginnen.

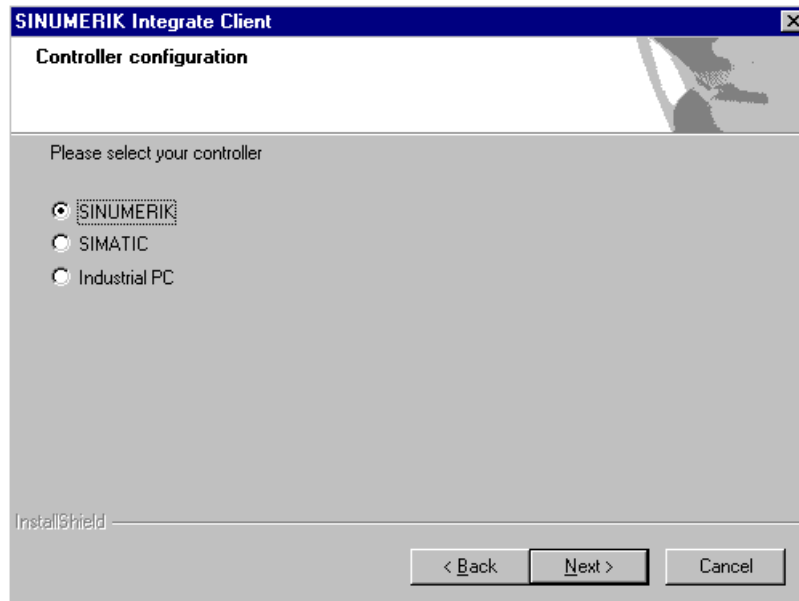


3.1 SINUMERIK-Steuerung mit HMI-Advanced

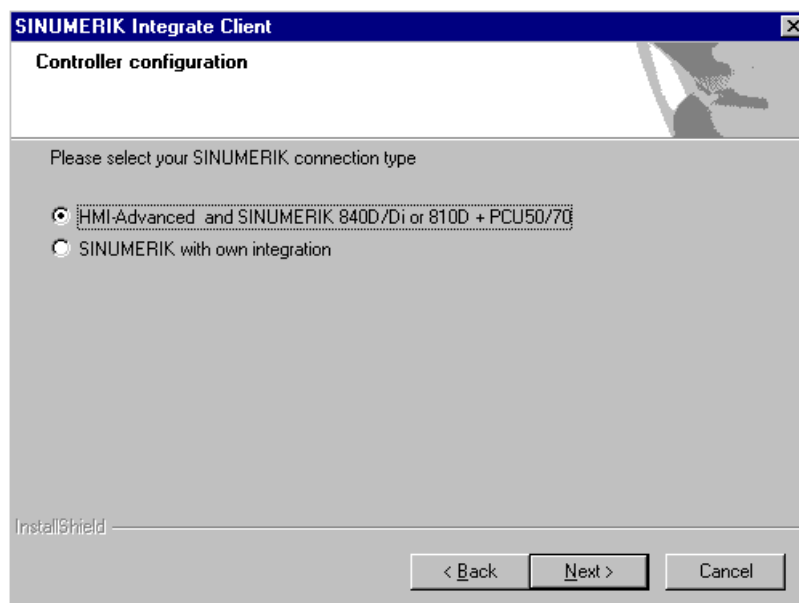
5. Das Fenster "License Agreement" wird geöffnet.
Lesen Sie die Lizenzvereinbarung.
 - Wenn Sie sich die Bedingungen ausdrucken möchten, klicken Sie auf die Schaltfläche "Print".
 - Aktivieren Sie anschließend das Optionsfeld "I accept the terms of the license agreement" und klicken Sie auf die Schaltfläche "Next >".
 - ODER -
Wenn Sie auf die Schaltfläche "< Back" klicken, gelangen Sie jeweils in das vorherige Fenster.
6. Das Fenster "Installation mode" wird geöffnet.
 - Aktivieren Sie das Optionsfeld "Expert mode (with additional installation options)".
 - Klicken Sie auf die Schaltfläche "Next >".



7. Das Fenster "Controller configuration" wird geöffnet.
 - Aktivieren Sie, z. B. das Optionsfeld "SINUMERIK".
 - Klicken Sie auf die Schaltfläche "Next >".

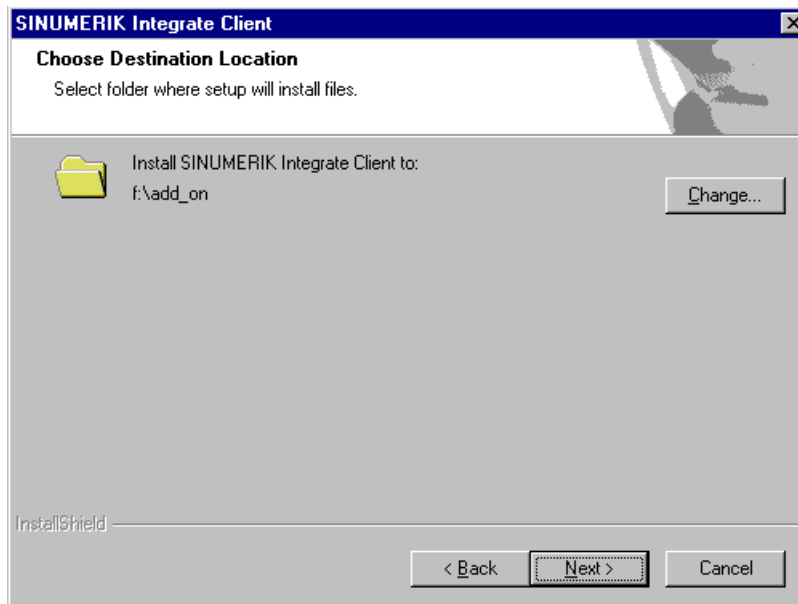


8. Im Fenster "Controller configuration" werden Ihnen die SINUMERIK-Verbindungstypen angezeigt.
 - Aktivieren Sie das Optionsfeld "HMI-Advanced and SINUMERIK 840D/Di or 810D + PCU50/70".
 - Klicken Sie auf die Schaltfläche "Next >".

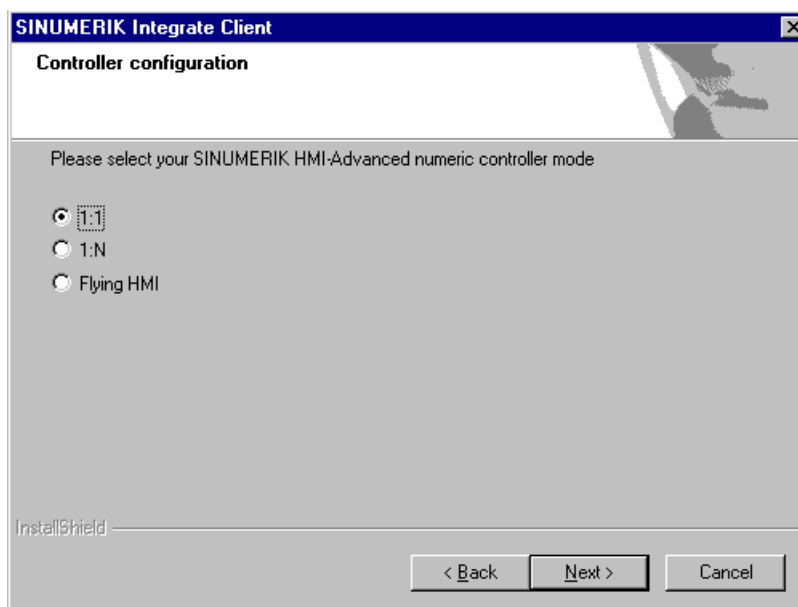


3.1 SINUMERIK-Steuerung mit HMI-Advanced

- 9. Das Fenster "Choose Destination Location" wird geöffnet und das Installationsverzeichnis wird angezeigt.
 - Klicken Sie auf die Schaltfläche "Next >".
 - ODER -
 - Um das Verzeichnis zu wechseln, klicken Sie auf die Schaltfläche "Change...".

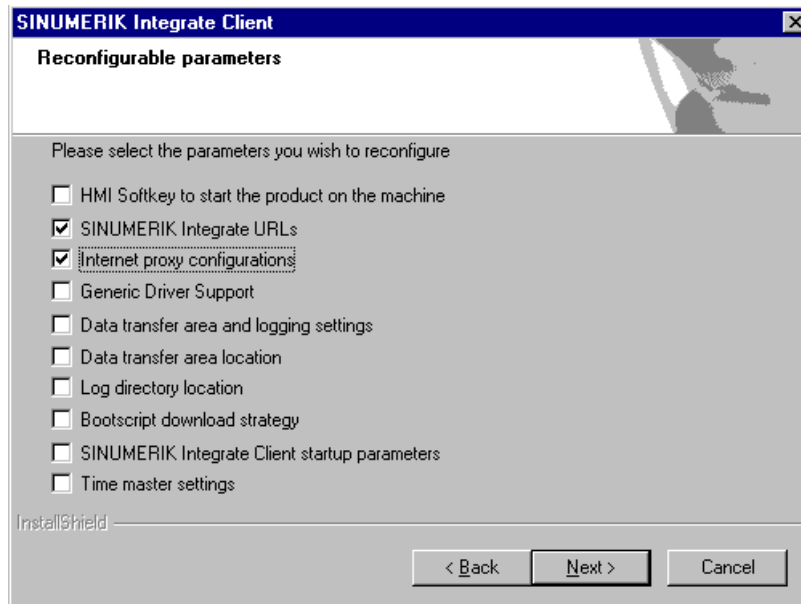


- 10. Das Fenster "Controller configuration" wird geöffnet.
 - Aktivieren Sie das Optionsfeld der Verbindung "1:1".
 - Klicken Sie anschließend auf die Schaltfläche "Next >".



11. Das Fenster "Reconfigurable parameters" wird geöffnet.

- Aktivieren Sie das Optionskästchen "SINUMERIK Integrate URLs" und "Internet proxy configurations".
- Klicken Sie auf die Schaltfläche "Next >".

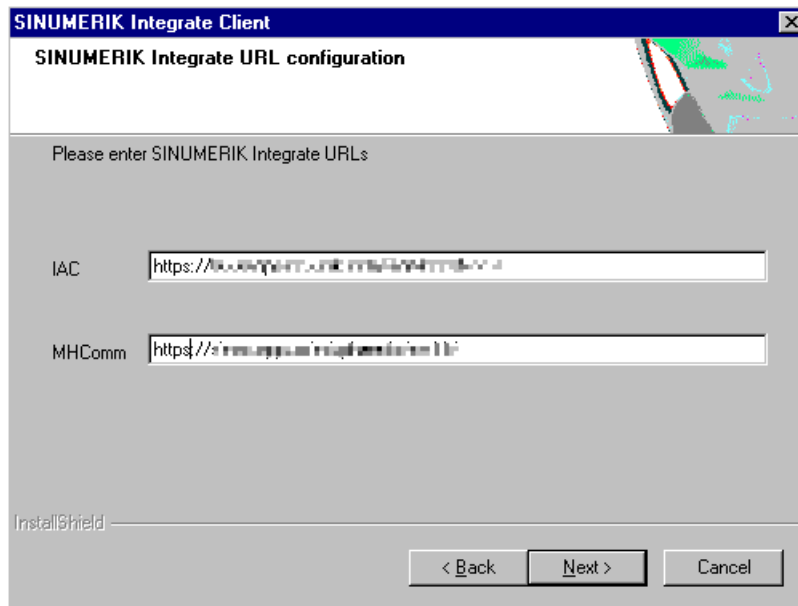


3.1 SINUMERIK-Steuerung mit HMI-Advanced

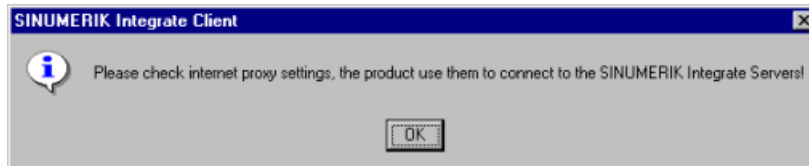
12. Das Fenster "SINUMERIK Integrate URL configuration" wird geöffnet.
Der Proxy-Server wird für die Verbindung der Steuerung mit der MindSphere benötigt.
Tragen Sie folgende Webservice URL ein, je nachdem mit welchem MindSphere-System Sie verbunden sind:

- MindSphere V3 Livesystem (<https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11>)
- MindSphere Alibaba (<https://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11>)

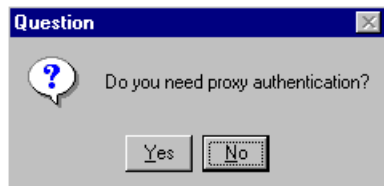
Klicken Sie auf die Schaltfläche "Next >".



13. Folgende Meldung wird angezeigt.
Klicken Sie auf die Schaltfläche "OK", um den Proxy-Server anzupassen.

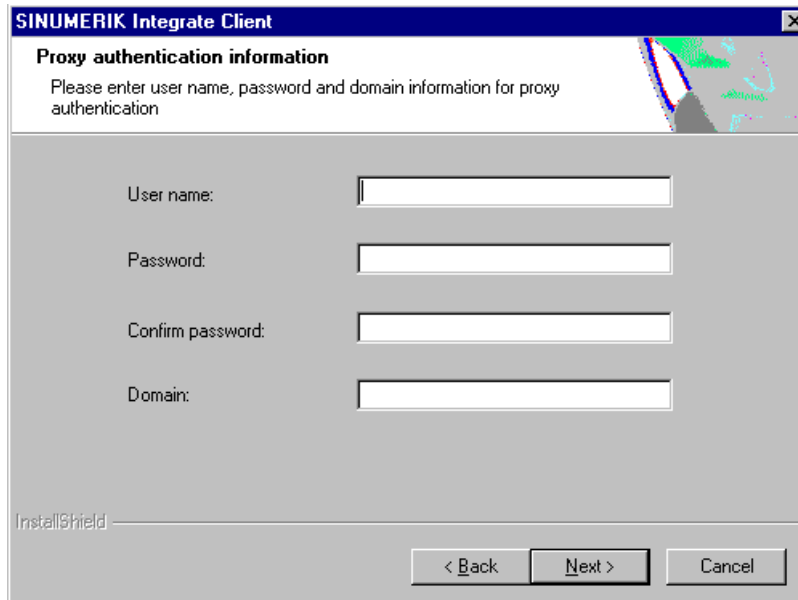


14. Wenn eine Authentifizierung für den Proxy benötigt wird, klicken Sie auf die Schaltfläche "Yes".



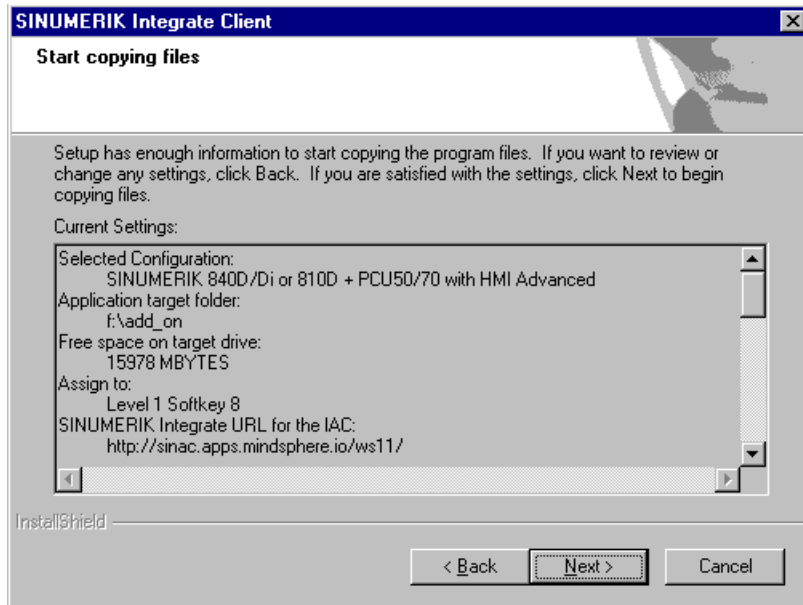
15. Tragen Sie die Daten in die Eingabefelder:

- User name:
- Passwort:
- Confirm passwort:
- Domain:
- Klicken Sie auf die Schaltfläche "Next >".



The screenshot shows a dialog box titled "SINUMERIK Integrate Client" with a close button (X) in the top right corner. The main heading is "Proxy authentication information". Below the heading, there is a text instruction: "Please enter user name, password and domain information for proxy authentication". The dialog contains four input fields, each with a label to its left: "User name:", "Password:", "Confirm password:", and "Domain:". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog area.

16. Das Fenster "Start copying files" wird geöffnet und die vorgenommenen Einstellungen angezeigt.
- Klicken Sie auf die Schaltfläche "Next >", um die Daten auf die SINUMERIK-Steuerung zu kopiert.



17. Nach erfolgter Installation, erhalten Sie die Meldung einen Neustart auszuführen. Klicken Sie dazu auf die Schaltfläche "OK".

3.2 SINUMERIK-Steuerung mit SINUMERIK Operate

Die Bedien-Software SINUMERIK Operate wird bereits mit der Client-Software SINUMERIK Integrate ausgeliefert.

Ein Update ist nicht möglich.

Hinweis

SINUMERIK-Daten auf MindSphere-Plattform übermitteln

Die Durchführung der nachfolgenden Schritte dient dazu, Ihnen die Übermittlung der SINUMERIK-Daten auf die MindSphere-Plattform zu ermöglichen.

In dem Sie die unten beschriebenen Schritte durchführen. Insbesondere durch Eingabe und Bestätigung der Webservice URL, werden Prozesse automatisiert durchgeführt, bei denen Softwareskripte auf die SINUMERIK-Steuerung geladen werden.

Voraussetzung

Die Nutzung von SINUMERIK Integrate ist freigeschaltet.

Integrate-Client mit Windows XP/PCU

Achten Sie darauf, dass die verwendeten Laufwerke ausreichend Speicherplatz zur Verfügung stellen.

Ist dies nicht der Fall, weil das Laufwerk C:\ in der Größe beschränkt ist, verfahren Sie wie folgt.

1. Stellen Sie sicher, dass SINUMERIK Operate nicht gestartet ist.
2. Öffnen Sie die Datei "epsconfig.user.xml" unter <SINUMERIKInstallDir>\user\sinumerik\hmi\cfg.
3. Ersetzen Sie in allen Einträgen "C:\" durch "F:\".
Damit verlegen Sie die Verzeichnisse für die temporären Dateien auf das Laufwerk "F:\".

Vorgehensweise

1. Das Fenster "Einstellungen" ist geöffnet.
Drücken Sie den Softkey "URLs>".
2. Drücken Sie den Softkey "Editieren" und wählen Sie folgende Einstellungen:
 - Verzeichnis: Wählen Sie aus der Klappliste "Verzeichnis" den Eintrag "User".
 - Anzeige Homepage: Aktivieren Sie das Optionskästchen "hier überschreiben".
 - RenderService: Aktivieren Sie das Optionskästchen "hier überschreiben".
 - Webservice URL: Aktivieren Sie das Optionskästchen "hier überschreiben".
 - Tragen Sie folgende Webservice URL ein, je nachdem mit welchem MindSphere-System Sie verbunden sind:
MindSphere V3 Livesystem (<https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11>)
MindSphere Alibaba (<https://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11>)
 - Tragen Sie im Eingabefeld "Sende Timeout in ms" den gewünschten Wert ein (Standardwert ist 200). Für MindSphere wird der Wert "20" empfohlen und aktivieren Sie das Optionskästchen "hier überschreiben".
 - Tragen Sie im Eingabefeld "Empfang Timeout in ms" den gewünschten Wert ein (Standardwert ist 200). Für MindSphere wird der Wert "20" empfohlen und aktivieren Sie das Optionskästchen "hier überschreiben".

The screenshot shows a configuration window with the following fields and options:

- Verzeichnis:** A dropdown menu with "User" selected.
- Anzeige Homepage:** A checkbox labeled "hier überschreiben" which is checked.
- RenderService:** A checkbox labeled "hier überschreiben" which is checked.
- Webservice URL:** A text input field containing "http://wslmac.apps.mindsphere.io/ws11" and a checkbox labeled "hier überschreiben" which is checked.
- Sende Timeout in ms:** A text input field containing "20" and a checkbox labeled "hier überschreiben" which is checked.
- Empfang Timeout in ms:** A text input field containing "20" and a checkbox labeled "hier überschreiben" which is checked.

3. Drücken Sie den Softkey "OK".
Eine Syntaxprüfung wird durchgeführt und die Zugangsdaten werden gespeichert.
4. Um aus dem Kundennetz eine Verbindung herzustellen, müssen Sie die Einstellungen vom Proxy anpassen.
 - Drücken Sie den Softkey "Proxys>".
Es werden die hinterlegten Einstellungen angezeigt.

5. Drücken Sie den Softkey "Editieren" und wählen Sie folgende Einstellungen:
 - Aktivieren Sie das Optionskästchen "nutze fix Proxy".
 - Tragen Sie in die Eingabefelder "Proxy 1" bis "Proxy 3" Ihre Proxies ein.
 - Aktivieren Sie die Optionskästchen "hier überschreiben", auch dann, wenn Sie nur einen Proxy eintragen, um den neuen Eintrag zu übernehmen.
 - Drücken Sie den Softkey "OK", um die Einstellungen zu speichern.

Verzeichnis:

automatisch hier überschreiben

nutze Proxy Script hier überschreiben

URL (Proxy Script)

nutze fix Proxy hier überschreiben

Proxy 1:

Proxy 2:

Proxy 3:

direkt hier überschreiben

6. Wenn für den Proxy eine Authentifizierung notwendig ist, drücken Sie den Softkey "Berechtigung".
 - Aktivieren Sie das Optionskästchen "hier überschreiben", um den neuen Eintrag zu übernehmen.
 - Geben Sie die Benutzerdaten in den Eingabefeldern "Domäne", "Benutzername" und "Passwort" ein.
 - Drücken Sie den Softkey "OK", um die Einstellungen zu speichern.

Verzeichnis:

hier überschreiben

Domäne:

Benutzername:

Passwort:

hier überschreiben

Workstation:

7. Damit die Zugangsdaten wirksam werden, starten Sie die Steuerung erneut.

3.3 SINUMERIK-Steuerung mit MindSphere verbinden

Durch das Aktivieren von SINUMERIK Integrate, dem Einrichten der URL/Proxy und dem Neustart, wird im Verzeichnis "/var/tmp/" der Ordner "boot_job" erzeugt. Wenn das Verzeichnis nicht eingerichtet wird, erstellen Sie es manuell.

Sie haben zwei Möglichkeiten den "onboard.key" auf die SINUMERIK-Steuerung zu kopieren:

- Über die Bedienoberfläche der Bedien-Software
- Mit Hilfe von WinSCP

Voraussetzung

Der Onboard Key wurde erzeugt

Der Ordner "boot_job" ist auf der Steuerung unter einem der folgenden Pfade angelegt:

- Linux (SINUMERIK 840/828): /var/tmp/boot_job
- Win7 PCU 50: C:\Temp\boot_job
- WinXP PCU 50: F:\tmp\boot_job

Vorgehensweise

1. Starten Sie an der Steuerung die Bedien-Software im Service-Modus.
2. Stecken Sie den USB-FlashDrive mit der Datei "onboard.key" in die PCU.
Der USB-FlashDrive wird im Verzeichnisbaum angezeigt.
3. Kopieren Sie die Datei "onboard.key", z. B. in folgendes Verzeichnis: C:\temp\boot_job.
4. Nach dem Verbinden, wird die Datei "onboard.key" gelöscht und die Datei "cert.key" erstellt.
Im Manage MyMachine Dashboard wird die SINUMERIK-Steuerung (Maschine) als online dargestellt.

3.4 SIMATIC IoT2040

Übersicht

Dieses Kapitel informiert Sie darüber, wie Sie SIMATIC IoT2040 zur Installation eines Proxy verwenden.

Mit IoT2040 verbinden Sie SINUMERIK Maschinen, die TLS 1.2 nicht unterstützen, mit MindSphere.

TLS 1.2 ist Bedingung für die Anbindung an IoT2040.

Hardware einrichten

SIMATIC IoT2040 (6ES7647-0AA00-1YA2) wird verwendet, um diese Konfiguration einzurichten.

Produkte (<https://mall.industry.siemens.com/mall/de/WW/Catalog/Products/10321262>)

Welche weiteren Voraussetzungen notwendig sind, lesen Sie im folgenden Kapitel: Systemvoraussetzungen (Seite 12), Absatz "SIMATIC IoT2040".

3.4.1 SIMATIC IoT2000 SD-Karten Beispiel Image auf IoT2040

Vorgehensweise

Laden Sie das SIMATIC IoT2000 SD-Karten Beispiel Image von folgendem Pfad:

SD-Karten Beispiel Image (<https://support.industry.siemens.com/cs/document/109741799/simatic-iot2000-sd-card-example-image?dti=0&lc=en-WWW>)

- ODER -

Von der .zip-Datei:

Example Image Zip (https://support.industry.siemens.com/cs/attachments/109741799/Example_Image_V2.2.0.zip)

Roadkil's Disk Image

1. Verwenden Sie "Roadkil's Disk Image", um das Image zu installieren.
Laden Sie sich die Standalone-Version unter folgendem Pfad herunter:
Roadkil (<http://www.roadkil.net/program.php/P12/Disk%20Image>)

Hinweis

Löschen aller Laufwerke

Um Fehlfunktionen zu vermeiden, löschen Sie vor dem Start alle existierenden Laufwerke auf der SD-Karte.

2. Wählen Sie den "Write Image" Tab.

3. Wählen Sie "Physical Disk", um das Image darauf zu schreiben.

Hinweis

Auswahl der Physical Disk

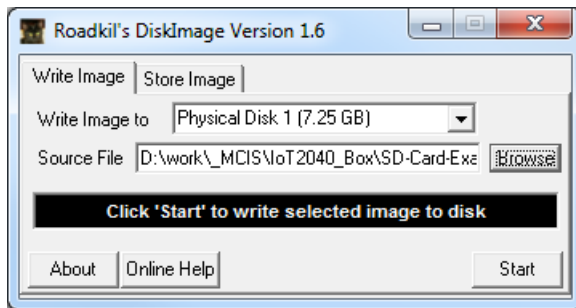
Achten Sie darauf die SD-Karte auszuwählen.

4. Wählen Sie das Image File "example-V2.2.0.wic".
5. Klicken Sie auf die Schaltfläche "Start".

Hinweis

SD-Karte vorbereiten

Löschen Sie alle vorhandenen Laufwerke auf Ihrer SD-Karte, bevor Sie starten.



dd

Parameter	Beschreibung
if	Eingabe File
of	Ausgabe Disk/Laufwerke
bs	Blockierter Platz (10 MB sind empfohlen)
--progress	Zeigt den Fortschritt

Vorgehensweise

1. Verwenden Sie "dd" um das Image zu installieren.
Laden Sie "dd" unter folgendem Pfad herunter:
dd (<http://www.chrysocome.net/dd>)
- ODER -
Von der zip.-Datei:
dd zip (<http://www.chrysocome.net/downloads/dd-0.6beta3.zip>
<//XmlEditor.InternalXmlClipboard:0b34d906-6791-2de3-57fd-5a19fdca7b37>)

Hinweis

Löschen aller Laufwerke

Um Fehlfunktionen zu vermeiden, löschen Sie vor dem Start alle existierenden Laufwerke auf der SD-Karte.

2. Führen Sie, z. B. folgenden Befehl aus.
Hinweis: Führen Sie die folgende Zeilen als einen Befehl aus:
dd if=D:\temp\example-V2.2.0.wic of=\\?\Device
\Harddisk1\Partition0 bs=10M --progress

Windows Rechner

1. Öffnen Sie Windows "CMD" als Administrator.
2. Öffnen Sie das Verzeichnis, in dem Sie die "dd.exe" gespeichert haben.
3. Schreiben Sie "dd --list".
Sie erhalten eine Liste aller eingebundenen Laufwerke.
4. Suchen Sie das korrekte Laufwerk, das Sie verwenden wollen. Beachten Sie den Warnhinweis.
5. Laden Sie das Image File und das Ziellaufwerk in das "dd Tool".
Die Prozedur dauert etwa 3-5 Minuten.
Der Erfolg wird angezeigt.
6. Nächster Schritt: Ausgabe

```
dd --list
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.
Win32 Available Volume Information
\\.\Volume{7994290d-4b77-11e2-b265-c01885b5e329}\
  link to \\?\Device\HarddiskVolume2
  fixed media
  Not mounted
\\.\Volume{afccbe56-4bb9-11e2-8a23-2cd444b4b548}\
  link to \\?\Device\HarddiskVolume1
  fixed media
  Mounted on \\.\c:
```

```
\\.\Volume{049b1544-4b77-11e2-a26b-806e6f6e6963}\
  link to \\?\Device\HarddiskVolume3
  fixed media
  Mounted on \\.\d:
\\.\Volume{66f507b7-c527-11e7-8975-005056c00008}\
  link to \\?\Device\HarddiskVolume7
  removeable media
  Mounted on \\.\f:
\\.\Volume{049b1547-4b77-11e2-a26b-806e6f6e6963}\
  link to \\?\Device\CdRom0
  CD-ROM
  Mounted on \\.\e:
NT Block Device Objects
  \\?\Device\CdRom0
    size is 2147483647 bytes
  \\?\Device\Harddisk0\Partition0
    link to \\?\Device\Harddisk0\DR0
    Fixed hard disk media. Block size = 512
    size is 500107862016 bytes
  \\?\Device\Harddisk0\Partition1
    link to \\?\Device\HarddiskVolume1
  \\?\Device\Harddisk0\Partition2
    link to \\?\Device\HarddiskVolume2
  \\?\Device\Harddisk0\Partition3
    link to \\?\Device\HarddiskVolume3
  \\?\Device\Harddisk1\Partition0
    link to \\?\Device\Harddisk1\DR4
    Removable media other than floppy. Block size = 512
    size is 7780433920 bytes
  \\?\Device\Harddisk1\Partition1
    link to \\?\Device\HarddiskVolume7
    Removable media other than floppy. Block size = 512
    size is 7780433920 bytes
Virtual input devices
  /dev/zero          (null data)
  /dev/random        (pseudo-random data)
  -                  (standard input)
Virtual output devices
  -                  (standard output)
  /dev/null          (discard the data)
```

- Nächster Schritt: Befehl
Hinweis:Führen Sie die folgenden Zeilen als einen Befehl aus:

```
dd if=D:\temp\example-V2.2.0.wic of=\\?\Device  
\Harddisk1\Partition0 bs=10M --progress
```

Fehlerkorrektur beim Schreiben des Image auf die SD Karte

Wenn Sie beim Schreiben des Image auf die SD Karte Schwierigkeiten erwarten:

- Trennen Sie die Internetverbindung.
- Stoppen Sie die Antivirus Software.

Ebenso kann eine lokale Sicherheitsvorschrift die Ausführung von Disk Werkzeugen verhindern.

- Versuchen Sie das Image mit einem Computer auf die SD Karte zu schreiben, der die Sicherheitsvorschriften weniger restriktiv handhabt.

3.4.2 Infrastruktur

Überblick

Dieses Kapitel gibt Ihnen Hinweise und Tipps zur Konfiguration des IoT2040 in Ihrem Netzwerk. Großenteils ist die Installation mit der Linux-Installation identisch. Beachten Sie aber einige spezifische Themen zum hier genutzten Yocto-Image.

Voreingestellte Netz-Konfiguration

Im Folgenden sehen Sie die Konfiguration, für die Installation des "Default-Image".

Die Standard Netz-Konfiguration des IoT2000 ist:

- X1 P1 LAN (eth0)
 - DHCP: no
 - IP: 192.168.200.1
 - Subnet Mask: 255.255.255.0
- X2 P1 LAN (eth1)
 - DHCP: yes

Die Netz-Konfiguration wird gespeichert unter: **/etc/network/interfaces**

```
# /etc/network/interfaces -- configuration file for ifup(8),  
ifdown(8)  
# The loopback interface  
auto lo  
iface lo inet loopback  
# Wired interfaces
```

3.4 SIMATIC IoT2040

```
auto eth0
iface eth0 inet static
    address 192.168.200.1
    netmask 255.255.255.0
auto eth1
iface eth1 inet dhcp
```

Beachten Sie beim ersten Zugang zu IoT2040 folgende Punkte:

- Port "X1 P1" ist konfiguriert mit der festen IP-Adresse 192.168.200.1
 - Für den Zugriff von diesem Port, setzen Sie Ihre IP-Adresse zu einer Adresse im Bereich 92.168.200.2 - 192.168.0.254
- Port "X2 P1" ist als DHCP konfiguriert
 - Für den Zugriff von diesem Port vernetzen Sie zu einem Netz mit DHCP-Server.
 - Sie müssen die IP-Adresse Ihres IoT2040 kennen.

Netz-Konfiguration ändern

Ändern Sie die Sektion "# Wired interfaces" in "/etc/network/interfaces":

DHCP an einem Port konfigurieren, z. B. X2 P1 LAN (eth1)

```
auto eth1
iface eth1 inet dhcp
```

Statischen (festen) IP an einem Port konfigurieren, z. B. X1 P1 LAN (eth0)

```
auto eth0
iface eth0 inet static
    address 192.168.200.1
    netmask 255.255.255.0
    gateway 192.168.200.252
```

Der Parameter "gateway" ist optional.

Hinweis

Probleme mit der Netz-Konfiguration

- Konfigurieren Sie nicht beide Netz-Ports als DHCP!
 - Setzen Sie nicht beide Netz-Ports als "Default" Gateways!
 - Bei Problemen mit der Netz-Konfiguration, versuchen Sie beide Netz-Ports als statische IP-Adressen zu konfigurieren!
 - Lassen sich die Netzprobleme nicht beheben, kontaktieren Sie Ihren lokalen Netzwerk-Administrator.
-

IoT2040 anbinden

Sie binden IoT2040 an X1 P1 an, entweder mit fester IP-Adresse oder mit DHCP.

X1 P1 mit fester IP-Adresse anbinden

Die Default-IP-Adresse an Port "X1 P1" ist 192.168.200.1.

- Verbinden Sie den Computer direkt mit einem Ethernet Kabel an diesen Port.
- Setzen Sie Ihre lokale IP-Adresse in das gleiche Subnetz, z. B. "192.168.200.2".
- Verbinden Sie IoT2000 mit den voreingestellten Daten.

X2 P1 mit DHCP anbinden

Der Port "X2 P1" des IoT2040 ist für DHCP konfiguriert.

- Verbinden Sie IoT2040 mit einem DHCP Router, der eine IP-Adresse bereitstellt. Diese IP-Adresse muss bekannt sein, um IoT2040 zu verbinden.
- Verbinden Sie IoT2000 mit den voreingestellten Daten.

User Name und Passwort

User Name und Passwort sind voreingestellt:

- User name: root
- Passwort: iot2000

Proxy Verbindung setzen

Benötigen Sie einen Proxy-Server für die Internetanbindung, verfahren Sie, wie in den nächsten Abschnitten beschrieben. Die Internetanbindung benötigen Sie, z. B. um die Pakete herunterzuladen, die für die folgenden Schritte notwendig sind.

Sie haben 2 Möglichkeiten eine Proxy-Verbindung aufzusetzen:

- Temporär, die Verbindung ist bis zum nächsten Start gültig
- Permanent, die Verbindung bleibt permanent erhalten

In den folgenden Abschnitten wird folgendes Beispiel verwendet:

Beispiel:

Proxy: 123.124.125.126

Proxy-Port: 4321

Für die Umsetzung in Ihrem Netzwerk, verwenden Sie die aktuellen Daten Ihrer Firma.

Hinweis

Apache Web Server

- Der Apache Web Server übernimmt die Einstellungen nicht.
 - Sie müssen die Proxy-Verbindung in der Apache Konfiguration zusätzlich aufsetzen.
-

Temporäre Proxy-Verbindung

Die Proxy-Verbindung ist temporär. Die Verbindung ist bis zum nächsten Start oder Reboot gültig.

Für die folgenden Befehle werden die Beispieldaten verwendet, passen Sie Ihre Eingaben mit den Firmendaten an.

- Proxy: 123.124.125.126
- Proxy-Port: 4321

Für die Umsetzung in Ihrem Netzwerk, verwenden Sie die aktuellen Daten Ihrer Firma.

Firmen Proxy mit Benutzer Authentifizierung

Führen Sie folgende Befehle im PuTTY aus:

- `export http_proxy="http://123.124.125.126:4321"`
- `export https_proxy="https://123.124.125.126:4321"`

Der folgende Befehl listet alle Umgebungsvariablen auf, so haben Sie die Möglichkeit Ihre Einstellungen zu prüfen:

- `export`

Ports für die Proxy Verbindung

In der aktuellen Dokumentation sind einige Listener Ports für Apache 80xxx festgelegt.

Hinweis

Verwendung anderer Ports

Wenn Sie aufgrund von Vorgaben andere Ports verwenden müssen, ist dies jederzeit möglich.

Passen Sie den Proxy-Port überall an.

Folgende Einstellungen sind gültig:

- `/usr/local/apache2/conf/httpd.conf`
- `/usr/local/apache2/conf/extra/httpd-vhosts.conf`
- Alle Einstellungen, die Sie mit Ihrer, z. B. SINUMERIK-Steuerung konfiguriert haben.

Permanente Proxy Verbindung

Die Proxy-Verbindung ist permanent und bleibt auch nach einem Neustart, oder Reboot erhalten.

Für die folgenden Befehle werden die Beispieldaten verwendet, passen Sie Ihre Eingaben mit den Firmendaten an.

1. Navigieren Sie zu dem Verzeichnis "etc".
2. Öffnen Sie die Datei "profile".
3. Fügen Sie die folgenden Zeilen hinzu:

```
export http_proxy="http://123.124.125.126:4321"  
export https_proxy="https://123.124.125.126:4321"
```
4. Fügen Sie die folgende Zeile am Ende der Datei, als vorletzte Zeile ein:

```
"umask 022"
```

Firmen-Proxy mit Benutzer-Authentifizierung

Wenn Ihr Firmen Proxy eine Benutzer Authentifizierung benötigt, verfahren Sie wie folgt:

1. Navigieren Sie zu dem Verzeichnis "etc".
2. Öffnen Sie die Datei "profile".
3. Fügen Sie die folgenden Zeilen hinzu:

```
export http_proxy="http://username:password@123.124.125.126:4321"  
export https_proxy="https://  
username:password@123.124.125.126:4321"
```

Ersetzen Sie "username" mit Ihrem Benutzernamen, und "password" mit Ihrem Passwort.
4. Fügen Sie die folgende Zeile am Ende der Datei, als vorletzte Zeile ein:

```
"umask 022"
```

Firmen Proxy Fehlerkorrektur

Wenn Probleme mit Ihrer speziellen Umgebung auftreten:

- Versuchen Sie eine Lösung zu finden, die für Linux funktioniert, insbesondere im Yocto-Project.

Da jedes Firmennetz individuell reagiert, ist es nicht möglich, für jeden möglichen Fall eine Lösung anzubieten.

3.4.3 Apache http

Abläufe und Downloads

Die folgenden Abläufe und Download Pakete benötigen Sie für die Einrichtung des Apache httpd.

Hinweis

Sicherheit der Installation

Achten Sie darauf immer die aktuelle Version für die Installation zu verwenden.

1. Laden Sie die folgenden Datenpakete:
 - Apache HTTP Server (httpd) (<http://httpd.apache.org>)
 - Apache APR & APR-util (<https://apr.apache.org/>)
 - PCRE (<https://www.pcre.org/>)

Wenn Ihr IoT2040 über eine Internetverbindung verfügt, verwenden Sie "wget" und laden die Datenpakete direkt herunter.

- ODER -

- Laden Sie die Datenpakete manuell herunter.
 - Kopieren Sie die Datenpakete in folgendes Verzeichnis: /usr/downloads.
2. Erstellen Sie das Verzeichnis "/usr/downloads":

```
cd /usr
mkdir downloads
cd downloads
```

3. Um alle benötigten Pakete herunterzuladen, führen Sie die folgenden Befehle aus:
Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:

```
wget http://mirror.netcologne.de/apache.org//httpd/
httpd-2.4.33.tar.gz wget http://mirror.23media.de/apache//apr/
apr-1.6.3.tar.gz wget http://mirror.23media.de/apache//apr/apr-
util-1.6.1.tar.gz
```

Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:

```
wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/
pcre-8.42.tar.gz
```

Pakete öffnen

Um die Pakete zu öffnen, führen Sie die folgenden Befehle im Verzeichnis "/usr/downloads/" aus:

```
tar xzf httpd-2.4.33.tar.gz
tar xzf apr-1.6.3.tar.gz
tar xzf apr-util-1.6.1.tar.gz
tar xzf pcre-8.42.tar.gz
```

Pakete in den entsprechenden Ordnern ablegen

Um die Pakete in den entsprechenden Ordnern abzulegen und diese richtig zu benennen, führen Sie die folgenden Befehle im Verzeichnis "/usr/downloads/" aus:

```
mkdir --parents /usr/local
mv httpd-2.4.33 apache2
mv apache2 /usr/local/
mv apr-1.6.3 apr
mv apr /usr/local/apache2/src/lib/
mv apr-util-1.6.1 apr-util
mv apr-util /usr/local/apache2/src/lib/
mv pcre-8.42 pcre
mv pcre /usr/local/
```

"opkg" und "pcre" installieren

1. Laden und installieren Sie "opkg".
`opkg install make`
2. Kompilieren und installieren Sie "pcre".
Führen Sie dazu die folgenden Befehle im Verzeichnis "/usr/local/pcre/" aus:
`./configure --prefix=/usr/local/pcre`
`make`
`make install`

Apache APR - kompilieren und installieren

Hinweis

Fehler im APR V1.6.3

Wegen eines Fehlers in APR V1.6.3 erzeugt das Kompilieren des APR einen Fehler. Editieren Sie die Datei manuell, um diesen Fehler zu vermeiden.

Weitere Details finden Sie unter: APR (<https://stackoverflow.com/questions/18091991/error-while-compiling-apache-apr-make-file-not-found>).

- Führen Sie die folgenden Anweisungen aus.
 - Prüfen Sie in künftigen APR Versionen ob der Fehler noch vorhanden ist.
-

1. Führen Sie den folgenden Befehl aus:
`cd /usr/local/apache2/src/lib/apr/`
2. Erstellen Sie eine Kopie der Originaldatei, bevor Sie mit der Bearbeitung beginnen.
`cp configure configure.original`
3. Ersetzen Sie die Zeile
`$RM "$cfgfile"`
durch
`$RM -f "$cfgfile"`
4. Speichern Sie die Änderung.
5. Wechseln Sie den Ordner: `cd /usr/local/apache2/src/lib/apr/`
Führen Sie die folgenden Befehle aus:
`./configure --prefix=/usr/local/apr/`
`make`
`make install`
`/usr/local/apache2/src/lib/apr/libtool --finish /usr/local/apr/lib/`

Apache APR-util kompilieren und installieren

1. Wechseln Sie den Ordner: `cd /usr/local/apache2/src/lib/apr-util/`
2. Führen Sie folgende Befehle aus:
`./configure --prefix=/usr/local/apr-util --with-apr=/usr/local/apr`
`make`
`make install`

Apache HTTP Server (httpd) kompilieren und installieren

1. Wechseln Sie den Ordner: `cd /usr/local/apache2/`
2. Führen Sie den folgenden Befehl aus:
Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:
`./configure --prefix=/usr/local/apache2 --with-apr=/usr/local/apr/bin --with-apr-util=/usr/local/apr-util/bin --with-pcre=/usr/local/pcre/bin/pcre-config`

Hinweis

Zeilenumbrüche

Achten Sie auf die Zeilenumbrüche - die vorhergehenden Zeilen bilden einen Befehl.

```
make
make install
```

Apache Web Server (httpd) starten und stoppen

- Manueller Start:
`/usr/local/apache2/bin/apachectl start`
- Manueller Stopp:
`/usr/local/apache2/bin/apachectl -k stop`
- Manueller Neustart:
`/usr/local/apache2/bin/apachectl -k graceful`

Apache Web Server (httpd) - Autostart konfigurieren

Startdatei erstellen

1. Wechseln Sie in das Verzeichnis `"/etc/init.d"`.
2. Erstellen Sie die Datei `"apache2"`.
3. Geben Sie den folgenden Text in die Datei ein:

```
#!/bin/bash
#
# apache2      Startup script for the Apache HTTP Server
#
chkconfig:    3 85 15
#             Apache is a World Wide Web server.
description:  It is used to serve \
              HTML files and CGI.
/usr/local/apache2/bin/apachectl $@
```

Dateieigenschaften bearbeiten

1. Geben Sie ein:

```
chmod 755 /etc/init.d/apache2
```
2. Führen Sie folgenden Befehl aus:

```
update-rc.d -f apache2 defaults
```

Weitere Details finden Sie unter: Apache Autostart (<https://serverfault.com/questions/16839/how-do-i-get-apache-to-startup-at-boottime-on-linux>)

3.4.4 Apache http konfigurieren

Dieses Kapitel beschreibt, wie Sie die erforderlichen Zertifikate erstellen. Sie benötigen die Zertifikate für:

- Die Nutzung der https Verbindung
- Die Konfiguration des Apache http als Proxy für ältere SINUMERIK-Steuerungen
- Die Anbindung an das MindSphere V3 Livesystem bei älteren SINUMERIK-Steuerungen

Im Folgenden wird eine Minimalkonfiguration beschrieben, die für die Verbindung ausreicht. Ausschließlich die benötigten Module werden geladen. Für die SSL-Verbindung ist nur TLS 1.2 erlaubt. Es werden nur die Ciphers freigeschaltet, die MindSphere für die Funktion benötigt.

Zertifikat für SSL-Verbindung erstellen

1. Erstellen Sie das Verzeichnis für das Zertifikat:

```
mkdir /usr/local/apache2/ssl_cert
```
2. Wechseln Sie in das Zertifikat Verzeichnis:

```
cd /usr/local/apache2/ssl_cert
```

3. Erstellen Sie das Zertifikat und das entsprechende Schlüssel-File mit dem folgenden Befehl:
Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem
```

Hinweis

Gültigkeit des Zertifikats

Das Zertifikat hat eine Gültigkeit von 1 Jahr (365 Tagen).

Um die Gültigkeit zu erweitern, fügen Sie den Parameter "-days 365" an.

4. Folgen Sie den Anweisungen und geben Sie die erforderlichen Informationen ein:

```
Generating a 2048 bit RSA private key
```

```
.....+++
```

```
.....+++
```

```
writing new private key to 'key.pem'
```

```
-----
```

```
You are about to be asked to enter information that will be incorporated
```

```
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Country Name (2 letter code) [AU]:DE
```

```
State or Province Name (full name) [Some-State]:Bavaria
```

```
Locality Name (eg, city) []:Nuremberg
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Siemens
```

```
Organizational Unit Name (eg, section) []:Mindsphere
```

```
Common Name (e.g. server FQDN or YOUR name) []:IoT2040
```

```
Email Address []:
```

Apache http Konfigurationsdateien bearbeiten

In der folgenden Konfiguration ist der Proxy für die Verbindung folgender Systeme konfiguriert.

- MindSphere V3 Livesystem (<https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11>)
- MindSphere Alibaba (<https://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11>)

Folgende Möglichkeiten stehen für die Bearbeitung der Konfigurationsdateien zur Verfügung:

- Über die Verbindung mit WinSCP
- Über die Verbindung mit PuTTY oder einen anderen SSH-Client, und der Benutzung des integrierten Linux Befehlszeileneditor "nano", der im aktuellen Image integriert ist
- Auf jede andere gewünschte Weise

Die folgenden Dateien werden bearbeitet:

- /usr/local/apache2/conf/httpd.conf
- /usr/local/apache2/conf/extra/httpd-ssl.conf
- /usr/local/apache2/conf/extra/httpd-vhosts.conf

httpd.conf bearbeiten

Geben Sie die folgenden Zeilen ein:

```
Listen 8080
Listen 8081
Listen 8082
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule autoindex_module modules/mod_autoindex.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule dir_module modules/mod_dir.so
#ServerAdmin you@example.com
ServerName localhost
Include conf/extra/httpd-vhosts.conf
Include conf/extra/httpd-ssl.conf
```

Zusatz für den Firmen-Proxy einfügen

Wird in Ihrer Firma ein Firmen-Proxy genutzt, müssen Sie eine zusätzliche Zeile in die Konfiguration einfügen.

Beispiel:

- Proxy: 123.124.125.126
- Proxy-Port: 4321

Fügen Sie folgende Zeile am Ende der Datei ein:

- httpd.conf:
ProxyRemote * http://123.124.125.126:4321

Hinweis

Proxy-Autorisierung im Proxy-Remote

In der aktuellen Apache Version wird die Benutzung der Proxy-Autorisierung im Proxy-Remote nicht unterstützt. In einem künftigen Release könnte es von Apache implementiert werden.

Wenn Sie diese Funktion für Ihre Anwendung benötigen, finden Sie eine mögliche Lösung unter dem folgenden Link, der einen Lösungsansatz verfolgt:

Proxy-Autorisierung (https://bz.apache.org/bugzilla/show_bug.cgi?id=37355)

extra\httpd-ssl.conf bearbeiten

Geben Sie die folgenden Zeilen ein:

```
#Listen 443
```

```
#SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
```

```
#SSLProxyCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
```

Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:

```
SSLCipherSuite ECDHE-RSA-AES128-CBC-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES128-SHA256
```

Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:

```
SSLProxyCipherSuite ECDHE-RSA-AES128-CBC-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES128-SHA256
```

```
SSLProtocol -all +TLSv1.2
```

```
SSLProxyProtocol -all +TLSv1.2
```

```
#ServerName www.example.com:443
```

```
#ServerAdmin you@example.com
```

```
ServerName IoT2040:443
```

```
SSLCertificateFile "/usr/local/apache2/ssl_cert/certificate.pem"
```

```
SSLCertificateKeyFile "/usr/local/apache2/ssl_cert/key.pem"
```

extra\httpd-vhosts.conf bearbeiten

Geben Sie die folgenden Zeilen ein:

```
#<VirtualHost *:80>
```

```
# ServerAdmin webmaster@dummy-host.example.com
```

```
# DocumentRoot "/usr/local/apache2/docs/dummy-host.example.com"
```

```
# ServerName dummy-host.example.com
```

```
# ServerAlias www.dummy-host.example.com
```

```
# ErrorLog "logs/dummy-host.example.com-error_log"
```

```
# CustomLog "logs/dummy-host.example.com-access_log" common
```

```
#</VirtualHost>
```

```
#<VirtualHost *:80>
```

```
# ServerAdmin webmaster@dummy-host2.example.com
```

```
# DocumentRoot "/usr/local/apache2/docs/dummy-host2.example.com"
```

```
# ServerName dummy-host2.example.com
```

```
# ServerAlias www.dummy-host2.example.com
```

```
# ErrorLog "logs/dummy-host2.example.com-error_log"
```

```
# CustomLog "logs/dummy-host2.example.com-access_log" common
```

```
#</VirtualHost>
```

```
<VirtualHost *:8080>
```

```
ServerName sinac.apps.mindsphere.io/
```

```
SSLProxyEngine On
```

```
RequestHeader set Front-End-Https "On"
```

```
ProxyPass / https://sinac.apps.mindsphere.io/
```

```
ProxyPassReverse / https://sinac.apps.mindsphere.io/
```

```
</VirtualHost>
```

```
<VirtualHost *:8081>
  ServerName sinumerikagentcom-dev.apps.mindsphere.io/
  SSLProxyEngine On
  RequestHeader set Front-End-Https "On"
  ProxyPass / https://sinumerikagentcom-dev.apps.mindsphere.io/
```

Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:

```
ProxyPassReverse / https://sinumerikagentcom-
dev.apps.mindsphere.io/
</VirtualHost>
```

Konfigurationsdateien - Export

httpd.conf

```
#
# This is the main Apache HTTP server configuration file. It
# contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed
# information.
# In particular, see # <URL:http://httpd.apache.org/docs/2.4/mod/
# directives.html>
# for a discussion of each configuration directive.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are
# unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for
# many
# of the server's control files begin with "/" (or "drive:/" for
# Win32), the
# server will use that explicit path. If the filenames do *not*
# begin
# with "/", the value of ServerRoot is prepended -- so "logs/
# access_log"
# with ServerRoot set to "/usr/local/apache2" will be interpreted by
# the
# server as "/usr/local/apache2/logs/access_log", whereas "/logs/
# access_log"
# will be interpreted as '/logs/access_log'.
```

```
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on
the
# Mutex directive, if file-based mutexes are used. If you wish to
share the
# same ServerRoot for multiple httpd daemons, you will need to
change at
# least PidFile.
#
ServerRoot "/usr/local/apache2"
#
# Mutex: Allows you to set the mutex mechanism and mutex file
directory
# for individual mutexes, or change the global defaults
#
# Uncomment and change the directory if mutexes are file-based and
the default
# mutex file directory is not on a local disk or is not appropriate
for some
# other reason.
#
# Mutex default:logs
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 8080
Listen 8081
```

```
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as
a DSO you
# have to place corresponding `LoadModule' lines at this location so
the
# directives contained in it are actually available before they
are used.
# Statically compiled modules (those listed by `httpd -l') do not
need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
```

```
LoadModule authn_file_module modules/mod_authn_file.so
#LoadModule authn_dbm_module modules/mod_authn_dbm.so
#LoadModule authn_anon_module modules/mod_authn_anon.so
#LoadModule authn_dbd_module modules/mod_authn_dbd.so
#LoadModule authn_socache_module modules/
#mod_authn_socache.so
LoadModule authn_core_module modules/mod_authn_core.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_groupfile_module modules/
mod_authz_groupfile.so
LoadModule authz_user_module modules/mod_authz_user.so
#LoadModule authz_dbm_module modules/mod_authz_dbm.so
#LoadModule authz_owner_module modules/
#mod_authz_owner.so
#LoadModule authz_dbd_module modules/mod_authz_dbd.so
LoadModule authz_core_module modules/mod_authz_core.so
LoadModule access_compat_module modules/
mod_access_compat.so
LoadModule auth_basic_module modules/mod_auth_basic.so
#LoadModule auth_form_module modules/mod_auth_form.so
#LoadModule auth_digest_module modules/
#mod_auth_digest.so
#LoadModule allowmethods_module modules/
#mod_allowmethods.so
#LoadModule file_cache_module modules/mod_file_cache.so
#LoadModule cache_module modules/mod_cache.so
#LoadModule cache_disk_module modules/mod_cache_disk.so
#LoadModule cache_socache_module modules/
#mod_cache_socache.so
LoadModule socache_shmcb_module modules/
#mod_socache_shmcb.so
#LoadModule socache_dbm_module modules/
#mod_socache_dbm.so
#LoadModule socache_memcache_module modules/
#mod_socache_memcache.so
#LoadModule watchdog_module modules/mod_watchdog.so
LoadModule macro_module modules/mod_macro.so
#LoadModule dbd_module modules/mod_dbd.so
#LoadModule dumpio_module modules/mod_dumpio.so
#LoadModule buffer_module modules/mod_buffer.so
#LoadModule ratelimit_module modules/mod_ratelimit.so
LoadModule reqtimeout_module modules/mod_reqtimeout.so
#LoadModule ext_filter_module modules/mod_ext_filter.so
#LoadModule request_module modules/mod_request.so
```

```
#LoadModule include_module modules/mod_include.so
LoadModule filter_module modules/mod_filter.so
#LoadModule substitute_module modules/mod_substitute.so
#LoadModule sed_module modules/mod_sed.so
#LoadModule deflate_module modules/mod_deflate.so
LoadModule mime_module modules/mod_mime.so
LoadModule log_config_module modules/mod_log_config.so
#LoadModule log_debug_module modules/mod_log_debug.so
#LoadModule logio_module modules/mod_logio.so
LoadModule env_module modules/mod_env.so
#LoadModule expires_module modules/mod_expires.so
LoadModule headers_module modules/mod_headers.so
#LoadModule unique_id_module modules/mod_unique_id.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule version_module modules/mod_version.so
#LoadModule remoteip_module modules/mod_remoteip.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/
mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
#LoadModule proxy_uwsgi_module modules/
#mod_proxy_uwsgi.so
#LoadModule proxy_fdpass_module modules/
#mod_proxy_fdpass.so
#LoadModule proxy_wstunnel_module modules/
#mod_proxy_wstunnel.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/
#mod_proxy_balancer.so
#LoadModule proxy_express_module modules/
#mod_proxy_express.so
#LoadModule proxy_hcheck_module modules/
#mod_proxy_hcheck.so
#LoadModule session_module modules/mod_session.so
#LoadModule session_cookie_module modules/
#mod_session_cookie.so
#LoadModule session_dbd_module modules/
#mod_session_dbd.so
#LoadModule slotmem_shm_module modules/
#mod_slotmem_shm.so
LoadModule ssl_module modules/mod_ssl.so
```

```
#LoadModule lbmethod_byrequests_module modules/  
#mod_lbmethod_byrequests.so  
#LoadModule lbmethod_bytraffic_module modules/  
#mod_lbmethod_bytraffic.so  
#LoadModule lbmethod_bybusyness_module modules/  
#mod_lbmethod_bybusyness.so  
#LoadModule lbmethod_heartbeat_module modules/  
#mod_lbmethod_heartbeat.so  
LoadModule unixd_module modules/mod_unixd.so  
#LoadModule dav_module modules/mod_dav.so  
#LoadModule status_module modules/mod_status.so  
#LoadModule autoindex_module modules/mod_autoindex.so  
#LoadModule info_module modules/mod_info.so  
#LoadModule cgid_module modules/mod_cgid.so  
#LoadModule dav_fs_module modules/mod_dav_fs.so  
LoadModule vhost_alias_module modules/  
mod_vhost_alias.so  
#LoadModule negotiation_module modules/  
#mod_negotiation.so  
#LoadModule dir_module modules/mod_dir.so  
#LoadModule actions_module modules/mod_actions.so  
#LoadModule speling_module modules/mod_speling.so  
#LoadModule userdir_module modules/mod_userdir.so  
LoadModule alias_module modules/mod_alias.so  
#LoadModule rewrite_module modules/mod_rewrite.so  
  
<IfModule unixd_module>  
#  
# If you wish httpd to run as a different user or group, you must  
run  
# httpd as root initially and it will switch.  
#  
# User/Group: The name (or #number) of the user/group to run httpd  
as.  
# It is usually good practice to create a dedicated user and group  
for  
# running httpd, as with most system services.  
#  
User daemon  
Group daemon  
</IfModule>
```



```
# 'Main' server configuration
#
# The directives in this section set up the values used by the
'main'
# server, which responds to any requests that aren't handled by a
# <VirtualHost> definition. These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
# All of these directives may appear inside <VirtualHost>
containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#
#
# ServerAdmin: Your address, where problems with the server should
be
# e-mailed. This address appears on some server-generated pages,
such
# as error documents. e.g. admin@your-domain.com
#
#ServerAdmin you@example.com
#
# ServerName gives the name and port that the server uses to identify
itself.
# This can often be determined automatically, but we recommend you
specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP
address here.
#
#ServerName www.example.com:80
ServerName localhost
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>
```

```
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working
# as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory,
# but
# symbolic links and aliases may be used to point to other
# locations.
#
DocumentRoot "/usr/local/apache2/htdocs"
<Directory "/usr/local/apache2/htdocs">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    # Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI
    MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options
    All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important. Please
    # see
    # http://httpd.apache.org/docs/2.4/mod/core.html
    #options
    # for more information.
    # Options Indexes FollowSymLinks
    #
    # AllowOverride controls what directives may be placed
    # in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    # AllowOverride FileInfo AuthConfig Limit
    # AllowOverride None
    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>
```

```
#
# DirectoryIndex: sets the file that Apache will serve if a
# directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>
#
# The following lines prevent .htaccess and .htpasswd files from
# being
# viewed by Web clients.
#
<Files ".ht*">
    Require all denied
</Files>
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error logfile for a
# <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"
#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn
<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use
    # with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"
    \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
</IfModule logio_module>
```

```
# You need to enable mod_logio.c to use %I and %O
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \
\"{%User-Agent}i\" %I %O"
combinedio
</IfModule>
#
# The location and format of the access logfile (Common Logfile
Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here. Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
CustomLog "logs/access_log" common
#
# If you prefer a logfile with access, agent, and referer
information
# (Combined Logfile Format) you can use the following directive.
#
#CustomLog "logs/access_log" combined
</IfModule>
<IfModule alias_module>
#
# Redirect: Allows you to tell clients about documents that used
to
# exist in your server's namespace, but do not anymore. The client
# will make a new request for the document at its new location.
# Example:
# Redirect permanent /foo http://www.example.com/bar
#
# Alias: Maps web paths into filesystem paths and is used to
# access content that does not live under the DocumentRoot.
# Example:
# Alias /webpath /full/filesystem/path
#
# If you include a trailing / on /webpath then the server will
# require it to be present in the URL. You will also likely
# need to provide a <Directory> section to allow access to
# the filesystem path.
```

```
#
# ScriptAlias: This controls which directories contain server
# scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the target directory are treated as applications
# and
# run by the server when requested rather than as documents sent
# to the
# client. The same rules about trailing "/" apply to ScriptAlias
# directives as to Alias.
#
ScriptAlias /cgi-bin/ "/usr/local/apache2/cgi-bin/"
</IfModule>
<IfModule cgid_module>
#
# ScriptSock: On threaded servers, designate the path to the UNIX
# socket used to communicate with the CGI daemon of mod_cgid.
#
#Scriptsock cgisock
</IfModule>
#
# "/usr/local/apache2/cgi-bin" should be changed to whatever your
ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/usr/local/apache2/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>
<IfModule headers_module>
# Avoid passing HTTP_PROXY environment to CGI's on this or any
# proxied
# backend servers which have lingering "httproxy" defects.
# 'Proxy' request header is undefined by the IETF, not listed by
IANA
#
RequestHeader unset Proxy early
</IfModule>
<IfModule mime_module>
```

```
#
# TypesConfig points to the file containing the list of mappings
# from
# filename extension to MIME-type.
#
TypesConfig conf/mime.types
#
# AddType allows you to add to or override the MIME configuration
# file specified in TypesConfig for specific file types.
#
#AddType application/x-gzip .tgz
#
# AddEncoding allows you to have certain browsers uncompress
# information on the fly. Note: Not all browsers support this.
#
#AddEncoding x-compress .Z
#AddEncoding x-gzip .gz .tgz
#
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media
# types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
#
# AddHandler allows you to map certain file extensions to
# "handlers":
# actions unrelated to filetype. These can be either built into
# the server
# or added with the Action directive (see below)
#
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add "ExecCGI" to the "Options"
# directive.)
#
#AddHandler cgi-script .cgi
# For type maps (negotiated resources):
#AddHandler type-map var
```

```
#
# Filters allow you to process content before it is sent to the
# client.
#
# To parse .shtml files for server-side includes (SSI):
# (You will also need to add "Includes" to the "Options"
# directive.)
#
#AddType text/html .shtml
#AddOutputFilter INCLUDES .shtml
</IfModule>
#
# The mod_mime_magic module allows the server to use various hints
# from the
# contents of the file itself to determine its type. The
# MIMEMagicFile
# directive tells the module where the hint definitions are
# located.
#
#MIMEMagicFile conf/magic
#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
#
# MaxRanges: Maximum number of Ranges in a request before
# returning the entire resource, or one of the special
# values 'default', 'none' or 'unlimited'.
# Default setting is to accept 200 Ranges.
#MaxRanges unlimited
```

```
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
#EnableSendfile on
# Supplemental configuration
#
# The configuration files in the conf/extra/ directory can be
# included to add extra features or to modify the default
# configuration of
# the server, or you may simply copy their contents here and change
# as
# necessary.
# Server-pool management (MPM specific)
#Include conf/extra/httpd-mpm.conf
# Multi-language error messages
#Include conf/extra/httpd-multilang-errordoc.conf
# Fancy directory listings
#Include conf/extra/httpd-autoindex.conf
# Language settings
#Include conf/extra/httpd-languages.conf
# User home directories
#Include conf/extra/httpd-userdir.conf
# Real-time info on requests and configuration
#Include conf/extra/httpd-info.conf
# Virtual hosts
Include conf/extra/httpd-vhosts.conf
# Local access to the Apache HTTP Server Manual
#Include conf/extra/httpd-manual.conf
# Distributed authoring and versioning (WebDAV)
#Include conf/extra/httpd-dav.conf
# Various default settings
#Include conf/extra/httpd-default.conf
```



```
# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include conf/extra/proxy-html.conf
</IfModule>
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
# starting without SSL on platforms with no /dev/random equivalent
# but a statically compiled-in mod_ssl.
#
  <IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
#ProxyRemote * http://123.124.125.126:4321
```

extra\httpd-ssl.conf

```
#
# This is the Apache server configuration file providing SSL
# support.
# It contains the configuration directives to instruct the server
# how to
# serve pages over an https connection. For detailed information
# about these
# directives see <URL:http://httpd.apache.org/docs/2.4/mod/
# mod_ssl.html>
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are
# unsure
# consult the online docs. You have been warned.
#
# Required modules: mod_log_config, mod_setenvif, mod_ssl,
# socache_shmcb_module (for default value of SSLSessionCache)
#
# Pseudo Random Number Generator (PRNG):
# Configure one or more sources to seed the PRNG of the SSL library.
# The seed data should be of good random quality.
# WARNING! On some platforms /dev/random blocks if not enough
# entropy
# is available. This means you then cannot use the /dev/random
# device
# because it would lead to very long connection times (as long as
# it requires to make more entropy available). But usually those
# platforms additionally provide a /dev/urandom device which
# doesn't
# block. So, if available, use this one instead. Read the mod_ssl
# User
# Manual for more details.
#
#SSLRandomSeed startup file:/dev/random 512
#SSLRandomSeed startup file:/dev/urandom 512
#SSLRandomSeed connect file:/dev/random 512
#SSLRandomSeed connect file:/dev/urandom 512
#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
#Listen 443
```

```
##
## SSL Global Context
##
## All SSL configuration in this context applies both to
## the main server and all SSL-enabled virtual hosts.
##
# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate,
# and that httpd will negotiate as the client of a proxied server.
# See the OpenSSL documentation for a complete list of ciphers, and
# ensure these follow appropriate best practices for this
# deployment.
# httpd 2.2.30, 2.4.13 and later force-disable aNULL, eNULL and EXP
# ciphers,
# while OpenSSL disabled these by default in 0.9.8zf/1.0.0r/1.0.1m/
# 1.0.2a.
#SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
#SSLProxyCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:
SSLCipherSuite ECDHE-RSA-AES128-CBC-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES128-SHA256
Hinweis: Führen Sie die folgenden Zeilen als einen Befehl aus:
SSLProxyCipherSuite ECDHE-RSA-AES128-CBC-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES128-SHA256
# By the end of 2016, only TLSv1.2 ciphers should remain in use.
# Older ciphers should be disallowed as soon as possible, while the
# kRSA ciphers do not offer forward secrecy. These changes inhibit
# older clients (such as IE6 SP2 or IE8 on Windows XP, or other
# legacy
# non-browser tooling) from successfully connecting.
#
# To restrict mod_ssl to use only TLSv1.2 ciphers, and disable
# those protocols which do not support forward secrecy, replace
# the SSLCipherSuite and SSLProxyCipherSuite directives above with
# the following two directives, as soon as practical.
# SSLCipherSuite HIGH:MEDIUM:!SSLv3:!kRSA
# SSLProxyCipherSuite HIGH:MEDIUM:!SSLv3:!kRSA
```

3.4 SIMATIC IoT2040

```
# User agents such as web browsers are not configured for the user's
# own preference of either security or performance, therefore this
# must be the prerogative of the web server administrator who
# manages
# cpu load versus confidentiality, so enforce the server's cipher
# order.
SSLHonorCipherOrder on
# SSL Protocol support:
# List the protocol versions which clients are allowed to connect
# with.
# Disable SSLv3 by default (cf. RFC 7525 3.1.1). TLSv1 (1.0) should
# be
# disabled as quickly as practical. By the end of 2016, only the
# TLSv1.2
# protocol or later should remain in use. #SSLProtocol all -SSLv3
#SSLProxyProtocol all -SSLv3
SSLProtocol -all +TLSv1.2
SSLProxyProtocol -all +TLSv1.2
```

```
# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is an internal
# terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog builtin
# Inter-Process Session Cache:
# Configure the SSL Session Cache: First the mechanism
# to use and second the expiring timeout (in seconds).
#SSLSessionCache "dbm:/usr/local/apache2/logs/ssl_scache"
SSLSessionCache "shmcb:/usr/local/apache2/logs/ssl_scache(512000)"
SSLSessionCacheTimeout 300
# OCSP Stapling (requires OpenSSL 0.9.8h or later)
#
# This feature is disabled by default and requires at least
# the two directives SSLUseStapling and SSLStaplingCache.
# Refer to the documentation on OCSP Stapling in the SSL/TLS
# How-To for more information.
#
# Enable stapling for all SSL-enabled servers:
#SSLUseStapling On
# Define a relatively small cache for OCSP Stapling using
# the same mechanism that is used for the SSL session cache
# above. If stapling is used with more than a few certificates,
# the size may need to be increased. (AH01929 will be logged.)
#SSLStaplingCache "shmcb:/usr/local/apache2/logs/
ssl_stapling(32768)"
# Seconds before valid OCSP responses are expired from the cache
#SSLStaplingStandardCacheTimeout 3600
# Seconds before invalid OCSP responses are expired from the cache
#SSLStaplingErrorCacheTimeout 600
##
## SSL Virtual Host Context
##
<VirtualHost _default_:443>
```

```
# General setup for the virtual host DocumentRoot "/usr/local/
apache2/htdocs"
#ServerName www.example.com:443
#ServerAdmin you@example.com ServerName IoT2040:443
ErrorLog "/usr/local/apache2/logs/error_log"
TransferLog "/usr/local/apache2/logs/access_log"
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "/usr/local/apache2/ssl_cert/certificate.pem"
#SSLCertificateFile "/usr/local/apache2/conf/server-dsa.crt"
#SSLCertificateFile "/usr/local/apache2/conf/server-ecc.crt"
# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "/usr/local/apache2/ssl_cert/key.pem"
#SSLCertificateKeyFile "/usr/local/apache2/conf/server-dsa.key"
#SSLCertificateKeyFile "/usr/local/apache2/conf/server-ecc.key"
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile "/usr/local/apache2/conf/server-ca.crt"
```

```
# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
# Note: Inside SSLCACertificatePath you need hash symlinks
# to point to the certificate files. Use the provided
# Makefile to update the hash symlinks after changes.
#SSLCACertificatePath "/usr/local/apache2/conf/ssl.crt"
#SSLCACertificateFile "/usr/local/apache2/conf/ssl.crt/ca-
bundle.crt"

# Certificate Revocation Lists (CRL):
# Set the CA revocation path where to find CA CRLs for client
# authentication or alternatively one huge file containing all
# of them (file must be PEM encoded).
# The CRL checking mode needs to be configured explicitly
# through SSLCAREvocationCheck (defaults to "none" otherwise).
# Note: Inside SSLCAREvocationPath you need hash symlinks
# to point to the certificate files. Use the provided
# Makefile to update the hash symlinks after changes.
#SSLCARevocationPath "/usr/local/apache2/conf/ssl.crl"
#SSLCARevocationFile "/usr/local/apache2/conf/ssl.crl/ca-
bundle.crl"

#SSLCARevocationCheck chain

# Client Authentication (Type):
# Client certificate verification type and depth. Types are
# none, optional, require and optional_no_ca. Depth is a
# number which specifies how deeply to verify the certificate
# issuer chain before deciding the certificate is not valid.
#SSLVerifyClient require
#SSLVerifyDepth 10

# TLS-SRP mutual authentication:
# Enable TLS-SRP and set the path to the OpenSSL SRP verifier
# file (containing login information for SRP user accounts).
# Requires OpenSSL 1.0.1 or newer. See the mod_ssl FAQ for
# detailed instructions on creating this file. Example:
# "openssl srp -srpvfile /usr/local/apache2/conf/passwd.srpv -add
username"
#SSLSRPVerifierFile "/usr/local/apache2/conf/passwd.srpv"
```

```
# Access Control:
# With SSLRequire you can do per-directory access control based
# on arbitrary complex boolean expressions containing server
# variable checks and other lookup directives. The syntax is a
# mixture between C and Perl. See the mod_ssl documentation
# for more details.
#<Location />

#SSLRequire %{SSL_CIPHER} !~ m/^(EXP|NULL)/ \
(
    and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd." \
    and %{SSL_CLIENT_S_DN_OU} in {"Staff", "CA", "Dev"} \
    and %{TIME_WDAY} >= 1
    and %{TIME_WDAY} <= 5 \
    and %{TIME_HOUR} >= 8
    and %{TIME_HOUR} <= 20 ) \
    or %{REMOTE_ADDR} =~ m/^192\.76\.162\.[0-9]+$/
#</Location>

# SSL Engine Options:
# Set various options for the SSL engine.

# o FakeBasicAuth:
# Translate the client X.509 into a Basic Authorisation. This
# means that
# the standard Auth/DBMAuth methods can be used for access
# control. The
# user name is the `one line' version of the client's X.509
# certificate.
# Note that no password is obtained from the user. Every entry
# in the user
# file needs this password: `xxj3lZMTZzkVA'.

# o ExportCertData:
# This exports two additional environment variables:
# SSL_CLIENT_CERT and
# SSL_SERVER_CERT. These contain the PEM-encoded certificates of
# the
# server (always existing) and the client (only existing when
# client
# authentication is used). This can be used to import the
# certificates
# into CGI scripts.
```



```
# o StdEnvVars:
# This exports the standard SSL/TLS related `SSL_*' environment
# variables.
# Per default this exportation is switched off for performance
# reasons,
# because the extraction step is an expensive operation and is
# usually
# useless for serving static content. So one usually enables
# the
# exportation for CGI and SSI requests only.
# o StrictRequire:
# This denies access when "SSLRequireSSL" or "SSLRequire"
# applied even
# under a "Satisfy any" situation, i.e. when it applies access
# is denied
# and no other module can change it.
# o OptRenegotiate:
# This enables optimized SSL connection renegotiation handling
# when SSL
# directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory "/usr/local/apache2/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
# SSL Protocol Adjustments:
# The safe and default but still SSL/TLS standard compliant
# shutdown
# approach is that mod_ssl sends the close notify alert but doesn't
# wait for
# the close notify alert from client. When you need a different
# shutdown
# approach you can use one of the following variables:
# o ssl-unclean-shutdown:
# This forces an unclean shutdown when the connection is closed,
# i.e. no
# SSL close notify alert is sent or allowed to be received. This
# violates
# the SSL/TLS standard but is needed for some brain-dead
# browsers. Use
# this when you receive I/O errors because of the standard
# approach where
# mod_ssl sends the close notify alert.
```

```
# o ssl-accurate-shutdown:
#   This forces an accurate shutdown when the connection is
#   closed, i.e. a
#   SSL close notify alert is send and mod_ssl waits for the close
#   notify
#   alert of the client. This is 100% SSL/TLS standard compliant,
#   but in
#   practice often causes hanging connections with brain-dead
#   browsers. Use
#   this only for browsers where you know that their SSL
#   implementation
#   works correctly.
# Notice: Most problems of broken clients are also related to the
# HTTP
# keep-alive facility, so you usually additionally want to disable
# keep-alive for those clients, too. Use variable "nokeepalive" for
# this.
# Similarly, one has to force some clients to use HTTP/1.0 to
# workaround
# their broken HTTP/1.1 implementation. Use variables
# "downgrade-1.0" and
# "force-response-1.0" for this.
BrowserMatch "MSIE [2-5]" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
# Per-Server Logging:
# The home of a custom SSL log file. Use this when you want a
# compact non-error SSL logfile on a virtual host basis.
CustomLog "/usr/local/apache2/logs/ssl_request_log" \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

extra/httpd-vhosts.conf

```
# Virtual Hosts
#
# Required modules: mod_log_config
# If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most
# configurations
# use only name-based virtual hosts so the server doesn't need to
# worry about
# IP addresses. This is indicated by the asterisks in the directives
# below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs/2.4/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual
# host
# configuration.
#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for all requests that do not
# match a ServerName or ServerAlias in any <VirtualHost> block.
#
#<VirtualHost *:80>
#   ServerAdmin webmaster@dummy-host.example.com
#   DocumentRoot "/usr/local/apache2/docs/dummy-host.example.com"
#   ServerName dummy-host.example.com
#   ServerAlias www.dummy-host.example.com
#   ErrorLog "logs/dummy-host.example.com-error_log"
#   CustomLog "logs/dummy-host.example.com-access_log" common
#</VirtualHost>
#
#<VirtualHost *:80>
#   ServerAdmin webmaster@dummy-host2.example.com
#   DocumentRoot "/usr/local/apache2/docs/dummy-host2.example.com"
#   ServerName dummy-host2.example.com
#   ErrorLog "logs/dummy-host2.example.com-error_log"
#   CustomLog "logs/dummy-host2.example.com-access_log" common
#</VirtualHost>
```

```
<VirtualHost *:8080>
    ServerName sinac.apps.mindsphere.io/
    SSLProxyEngine On
    RequestHeader set Front-End-Https "On"
    ProxyPass / https://sinac.apps.mindsphere.io/
    ProxyPassReverse / https://sinac.apps.mindsphere.io/
</VirtualHost>
<VirtualHost *:8081>
    ServerName sinumerikagentcom-dev.apps.mindsphere.io/
    SSLProxyEngine On RequestHeader set Front-End-Https "On"
    ProxyPass / https://sinumerikagentcom-dev.apps.mindsphere.io/
    ProxyPassReverse / https://sinumerikagentcom-
dev.apps.mindsphere.io/
</VirtualHost>
<VirtualHost *:8082>
    ServerName gateway.eul.mindsphere.io/
    SSLProxyEngine On RequestHeader set Front-End-Https "On"
    ProxyPass / https://gateway.eul.mindsphere.io/
    ProxyPassReverse / https://gateway.eul.mindsphere.io/
</VirtualHost>
```

3.4.5 SINUMERIK-Steuerungen konfigurieren

3.4.5.1 Übersicht

Einleitung

Dieses Kapitel beschreibt die Konfiguration von folgenden SINUMERIK-Steuerungen für die Verwendung eines Apache Proxy auf einem IoT2040.

- SINUMERIK-Steuerung mit HMI-Advanced - Proxy einstellen (Seite 69)
- SINUMERIK-Steuerung mit SINUMERIK Operate - Proxy einstellen (Seite 78)

Folgende Ports werden für die verschiedenen MindSphere-Systeme verwendet:

- Port 8082 ist konfiguriert für das MindSphere V3 Livesystem

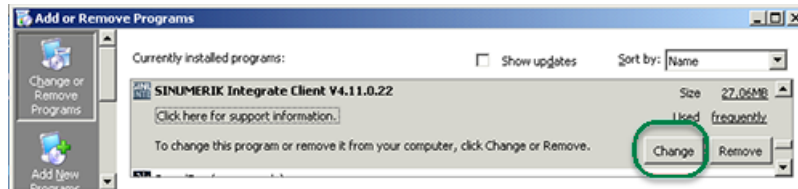
Konfigurieren Sie die URL, für die Anbindung an MindSphere mit **http**, nicht mit **https**.

- MindSphere V3 Livesystem (<http://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11>)
- MindSphere Alibaba (<http://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11>)

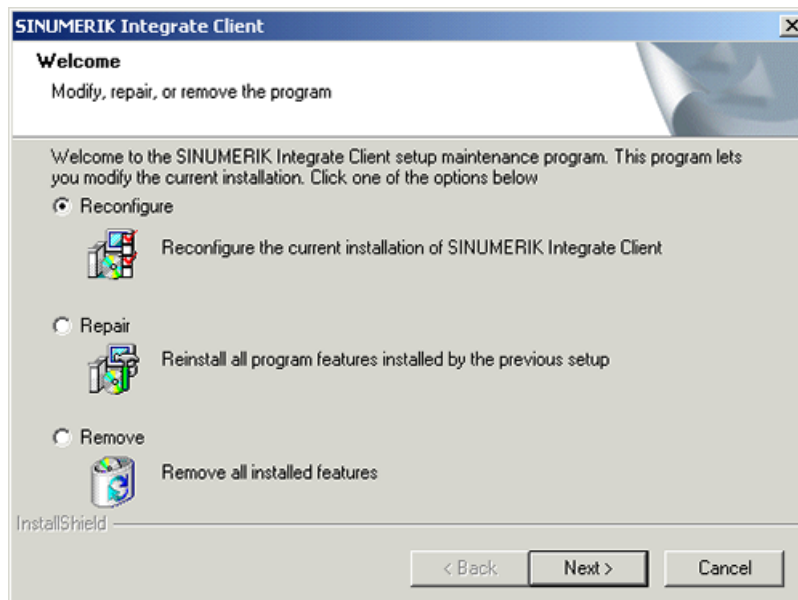
3.4.5.2 SINUMERIK-Steuerung mit HMI-Advanced - Proxy einstellen

Vorgehensweise

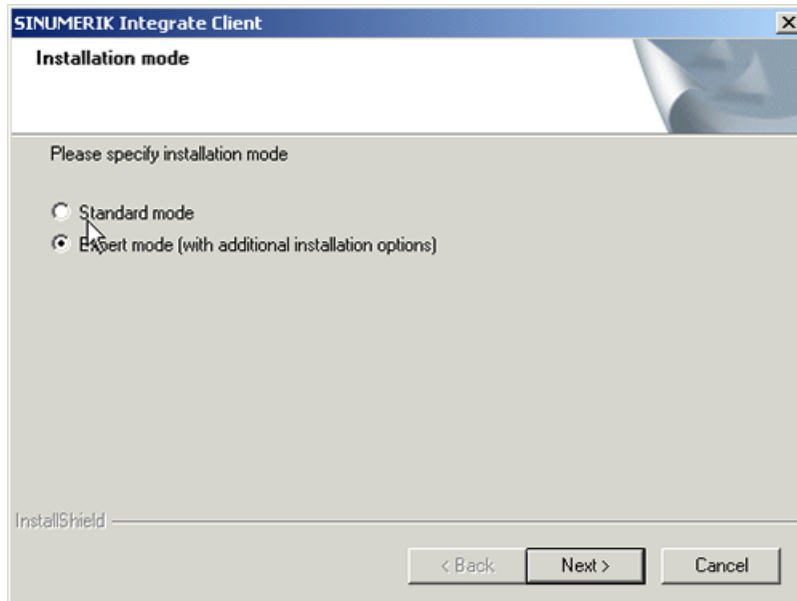
1. Starten Sie die PCU im Servicemodus.
2. Öffnen Sie in Windows "Add or Remove programs" und wählen Sie "SINUMERIK Integrate Client".
Klicken Sie auf die Schaltfläche "Change".



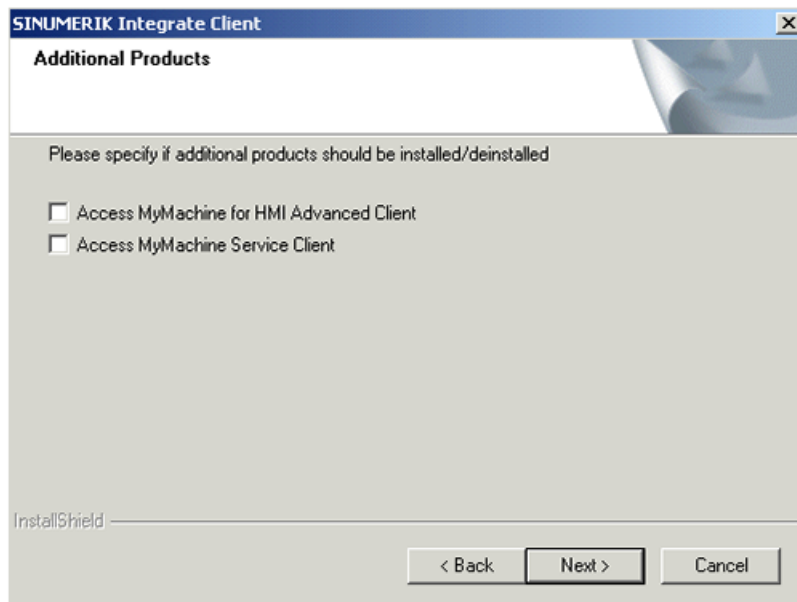
3. Das Fenster "Welcome" wird geöffnet.
 - Um die Konfiguration zu bearbeiten, aktivieren Sie das Optionsfeld "Reconfigure".
 - Um das Setup des "SINUMERIK Integrate Client" auszuführen, klicken Sie auf die Schaltfläche "Next >".



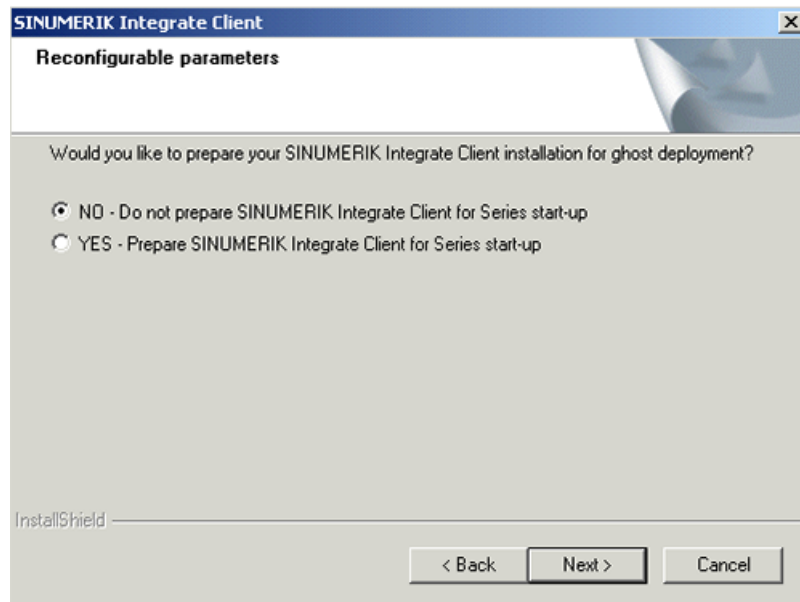
- 4. Das Fenster "Installation mode" wird geöffnet.
 - Aktivieren Sie das Optionsfeld "Expert mode (with additional installation options)".
 - Klicken Sie auf die Schaltfläche "Next >".



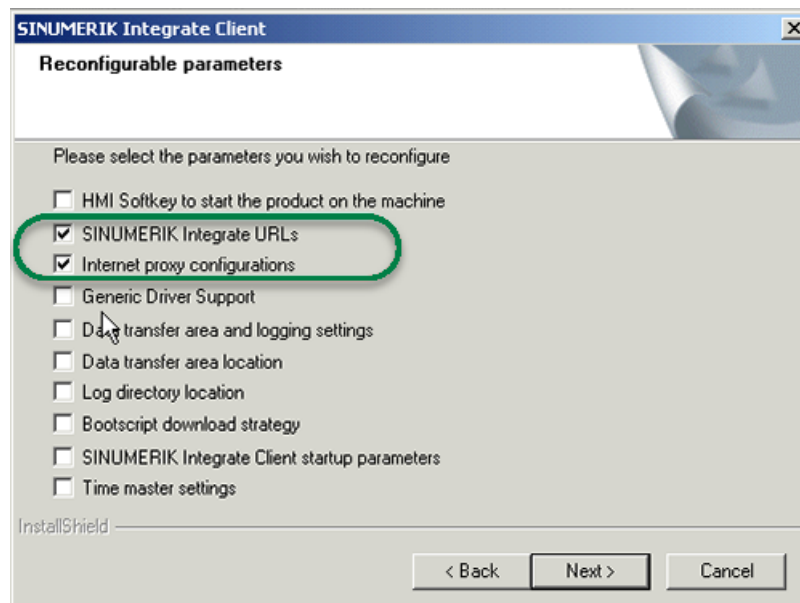
- 5. Das Fenster "Additional Products" wird geöffnet.
 - Klicken Sie auf die Schaltfläche "Next >".



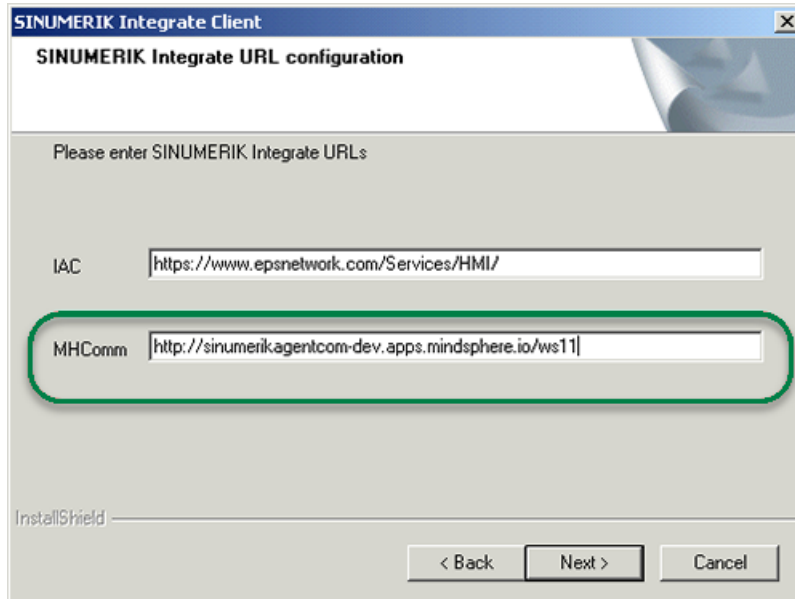
6. Das Fenster "Reconfigurable parameter" wird geöffnet.
 - Aktivieren Sie das Optionsfeld "NO - Do not prepare SINUMERIK Integrate Client for Series start-up".
 - Klicken Sie auf die Schaltfläche "Next >".



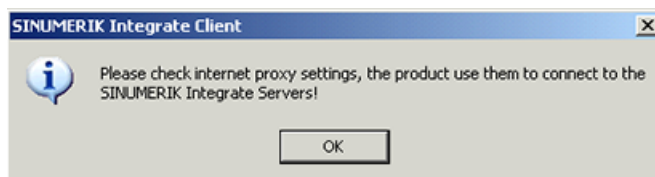
7. Aktivieren Sie folgende Optionskästchen:
 - "SINUMERIK Integrate URLs"
 - "Internet proxy configurations"
 - Klicken Sie auf die Schaltfläche "Next >".



- 8. Das Fenster SINUMERIK Integrate URL configuration wird geöffnet.
 - Konfigurieren Sie die URL, für die Anbindung an MindSphere mit **http**, nicht mit **https**. Tragen Sie im Eingabefeld "MHComm" folgende URL ein, je nachdem mit welchem MindSphere-System Sie verbunden sind:
MindSphere V3 Livesystem (<http://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11>)
MindSphere Alibaba (<http://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11>)
 - Klicken Sie auf die Schaltfläche "Next >".

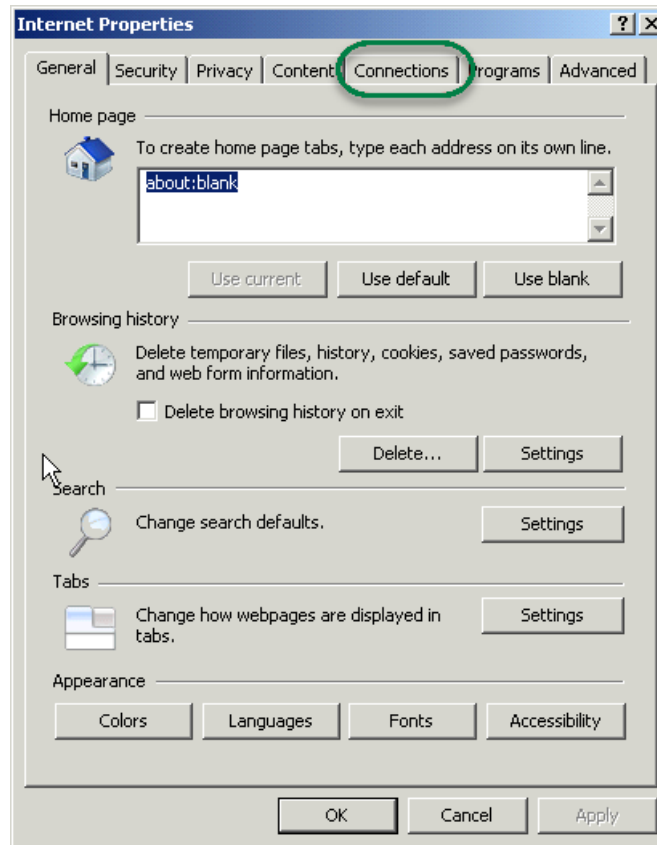


- 9. Sie erhalten folgende Aufforderung: "Please check internet proxy setting, the product use them to connect to the SINUMERIK Integrate Servers!".
 - Klicken Sie auf "OK".



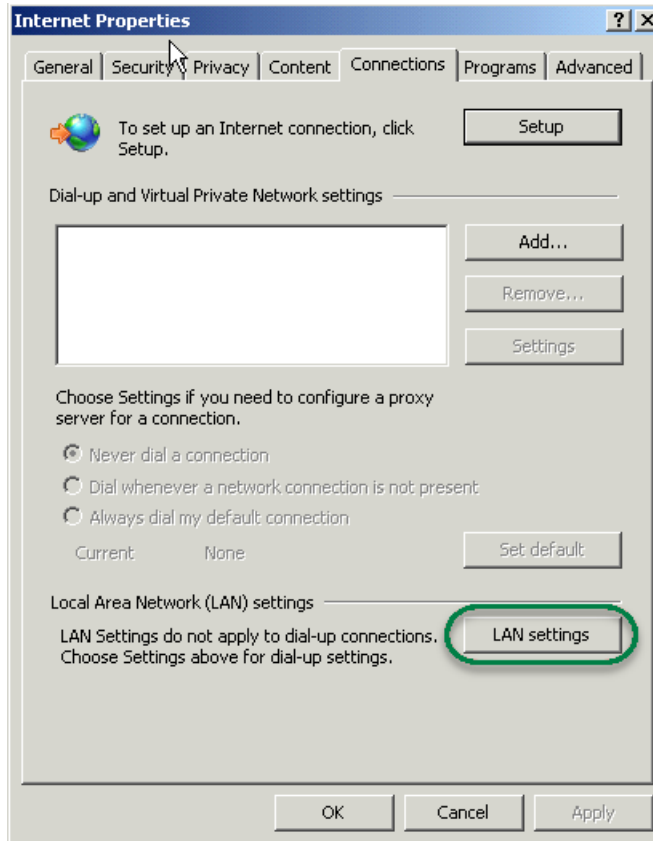
10. Das Fenster "Internet Properties" > "General" wird geöffnet.

- Öffnen Sie das Register "Connections".



11. Das Fenster "Connections" wird geöffnet.

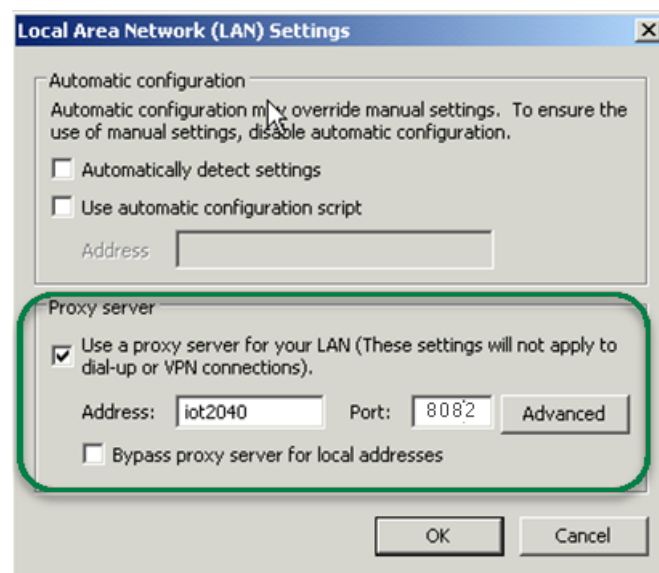
- Im Bereich "Local Area Network (LAN) settings", klicken Sie auf die Schaltfläche "LAN settings".



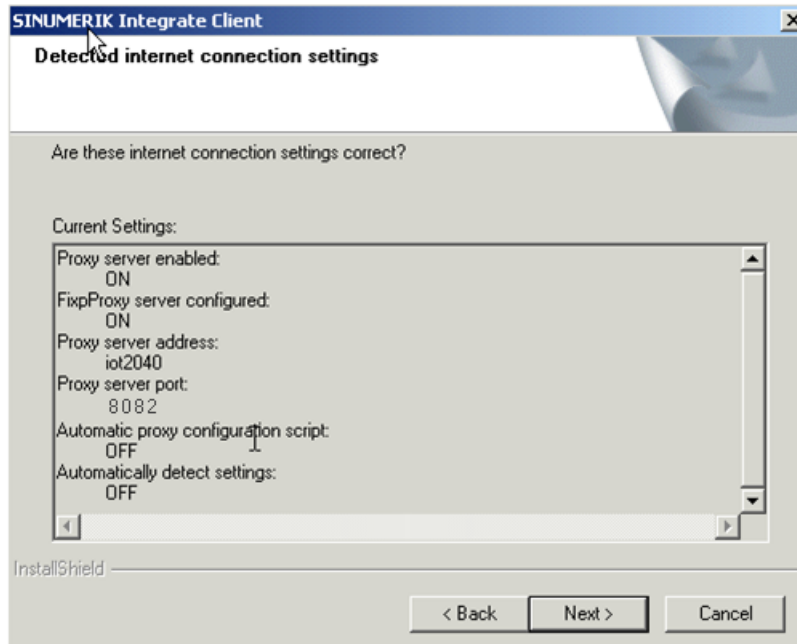
12. Das Fenster "Local Area Network (LAN) Settings" wird geöffnet.

Geben Sie die Proxy-Einstellungen ein:

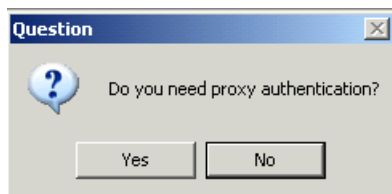
- Deaktivieren Sie das Optionskästchen "Automatically detect settings".
- Deaktivieren Sie das Optionskästchen "Use automatic configuration script".
- Im Bereich "Proxy server" aktivieren Sie das Optionskästchen "Use a proxy server for your LAN"
- Address: iot2040
- Port (wie in Apache konfiguriert), z. B.: 8082
- Deaktivieren Sie das Optionskästchen "Bypass proxy server for local addresses"
- Klicken Sie auf die Schaltfläche "OK".



- 13. Das Fenster "Detected internet connection settings" wird geöffnet.
Die festgelegten Proxyeinstellungen werden zur Überprüfung angezeigt.
 - Klicken Sie auf die Schaltfläche "Next >".

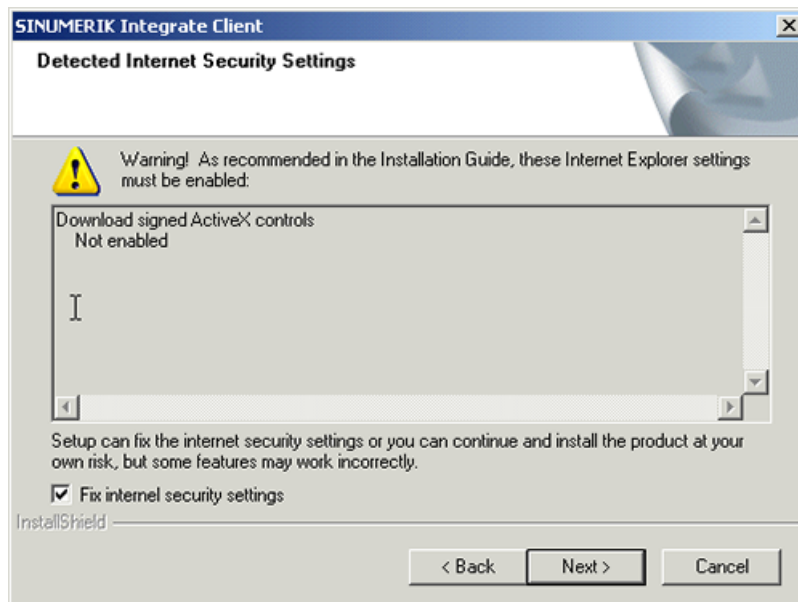


- 14. Folgende Frage wird angezeigt: "Do you need proxy authentication?".
 - Klicken Sie auf die Schaltfläche "No".

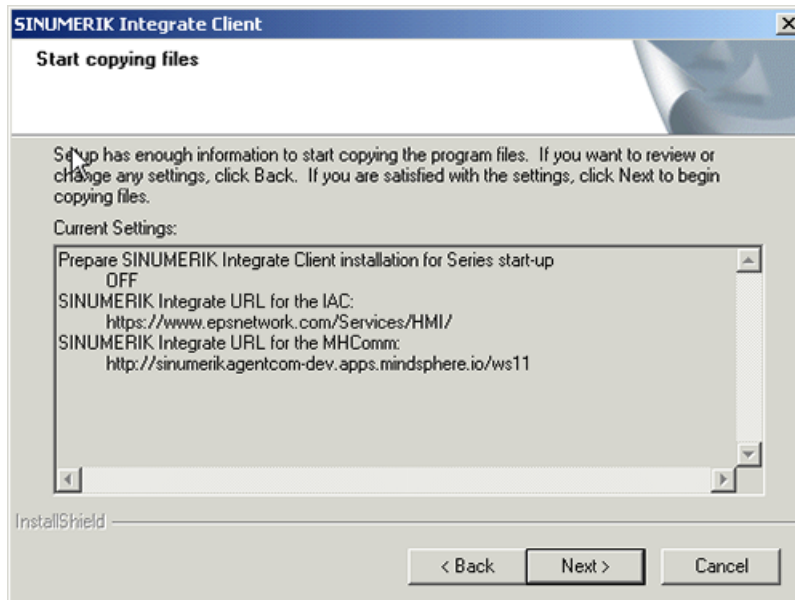


15. Aktivieren Sie das Optionskästchen "Fix internal security settings".

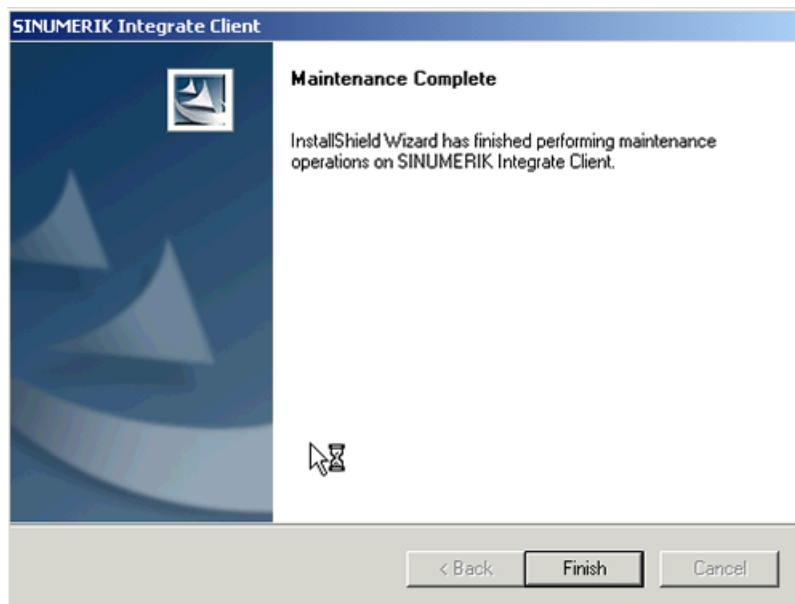
- Klicken Sie auf die Schaltfläche "Next >".



- 16. Das Fenster "Start copying files" wird geöffnet.
Die festgelegten URL-Einstellungen werden zur Überprüfung angezeigt.
 - Klicken Sie auf die Schaltfläche "Next >".



- 17. Das Fenster "Maintenance Complete" wird angezeigt.
 - Klicken Sie auf die Schaltfläche "Finish>", um die Installation abzuschließen.

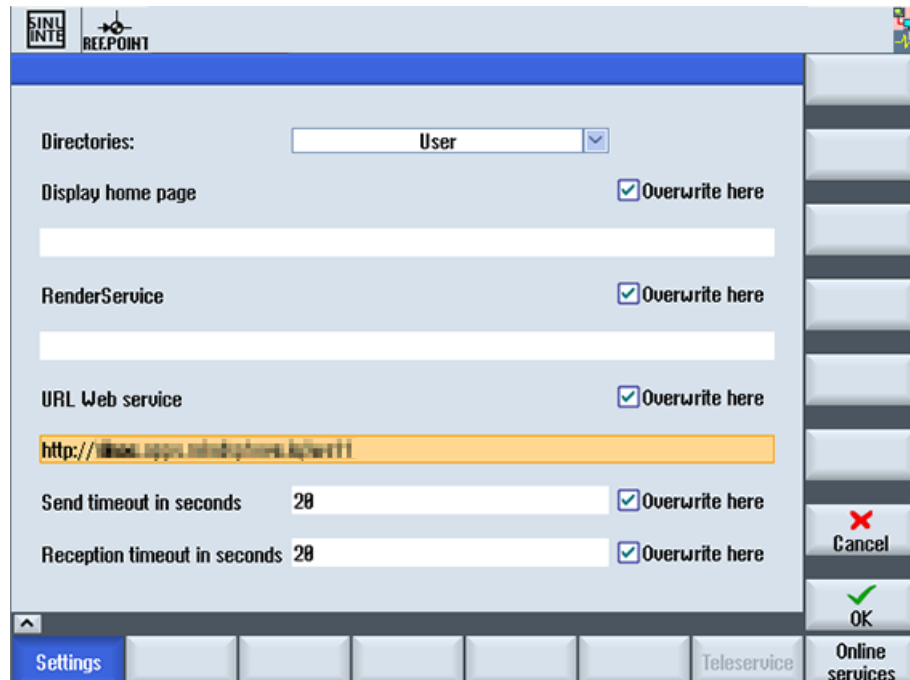


3.4.5.3 SINUMERIK-Steuerung mit SINUMERIK Operate - Proxy einstellen

In diesem Kapitel ist die Konfiguration des SINUMERIK Integrate Client für SINUMERIK Operate beschrieben.

Vorgehensweise

1. Das Fenster "Einstellungen" ist geöffnet.
Drücken Sie den Softkey "URLs>".
2. Drücken Sie den Softkey "Settings" und wählen Sie folgende Einstellungen:
 - Verzeichnis: Wählen Sie aus der Klappliste "Directories" den Eintrag "User".
 - Display home page: Aktivieren Sie das Optionskästchen "Overwrite here".
 - RenderService: Aktivieren Sie das Optionskästchen "Overwrite here".
 - URL Web service: Aktivieren Sie das Optionskästchen "Overwrite here".
 - Konfigurieren Sie die URL, für die Anbindung an MindSphere mit **http**, nicht mit **https**. Tragen Sie folgende Webservice URL ein, je nachdem mit welchem MindSphere System Sie verbunden sind:
MindSphere V3 Livesystem (<http://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11>)
MindSphere Alibaba (<http://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11>)
 - Tragen Sie im Eingabefeld "Send timeout in seconds" den gewünschten Wert ein (Standardwert ist 200). Für MindSphere wird der Wert "20" empfohlen und aktivieren Sie das Optionskästchen "Overwrite here".
 - Tragen Sie im Eingabefeld "Receptions timeout in seconds" den gewünschten Wert ein (Standardwert ist 200). Für MindSphere wird der Wert "20" empfohlen und aktivieren Sie das Optionskästchen "Overwrite here".



3. Konfigurieren Sie den festen Proxy in SINUMERIK in folgendem Format:
<ip-address>:<port>
 <ip-address>: IP Adresse des IoT2040
 <port>: von Apache genutzter Port:

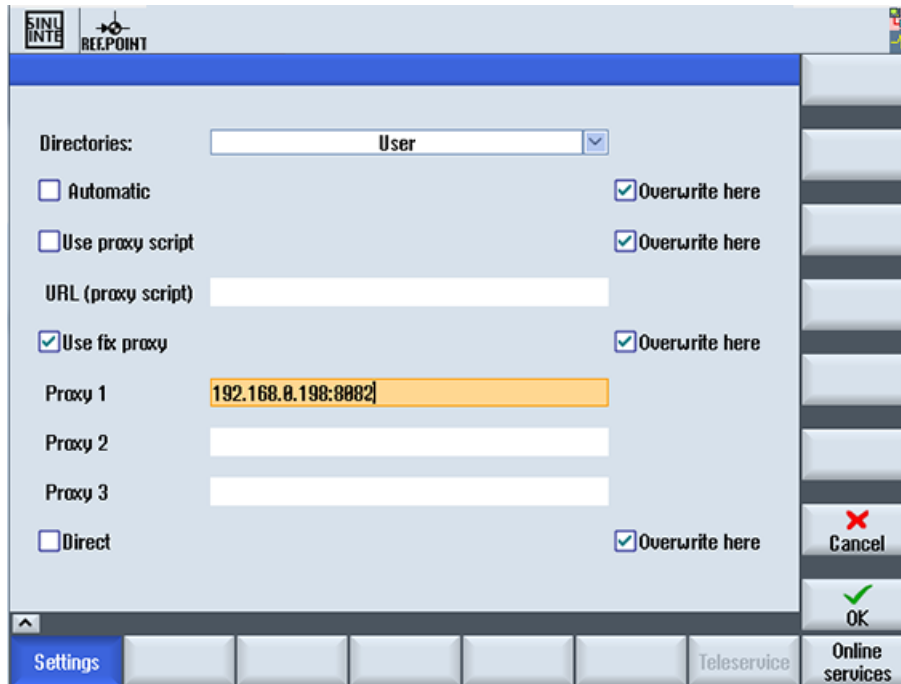
- Port 8082

Drücken Sie den Softkey "OK".

Beispiel

Die IP-Adresse des IoT2040 ist 192.168.0.198, daraus ergibt sich folgende Konfiguration:

- MindSphere V3 Livesystem: 192.168.0.198:8082

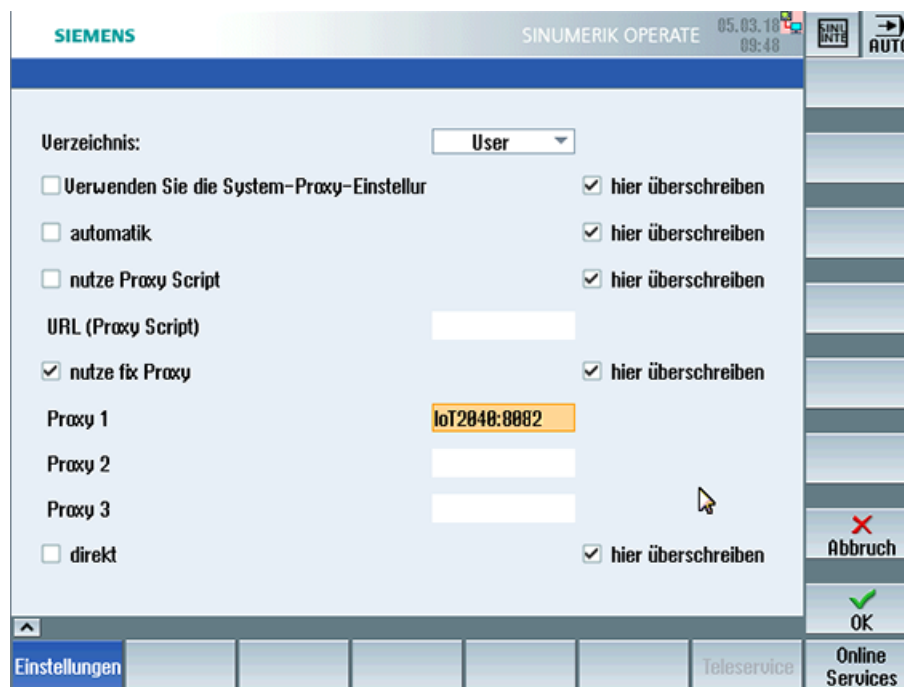


Fehlerkorrektur bei der Proxy-Verbindung

Das Zertifikat wird mit dem allgemeinen Namen IoT2040 erzeugt. Es kann notwendig sein, dass Sie statt der IP-Adresse den FQDN: IoT2040 verwenden müssen, um den Proxy zu erreichen.

Wird der IoT2040 mit der DNS erreicht, ist keine weitere Aktion notwendig.

1. Wenn Sie keine DNS verwenden, erweitern Sie die Host Dateien mit der IP und dem Namen des IoT2040.
In der PCU 50 ist die Datei in folgendem Verzeichnis gespeichert:
C:\Windows\System32\drivers\etc\hosts
2. Im folgenden Beispiel fügen Sie die folgende Datei zu dem "Host" hinzu:
192.168.0.198 IoT2040
3. Tragen Sie im Eingabefeld "Proxy 1" die gewünschte Einstellung ein, z: B.: "IoT2040:8082".



3.4.6 Root Zugang zur IoT2040 Box sichern - optional

Dieser Schritt ist optional, aus Sicherheitsgründen wird empfohlen diese Konfiguration durchzuführen.

3.4.6.1 Passwort für den Root Benutzer setzen

Grundsätzlich ist kein Root Password gesetzt.

Aus Sicherheitsgründen wird empfohlen das Root Password möglichst zeitnah zu setzen.

Vorgehensweise

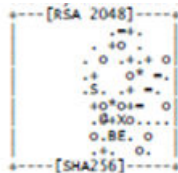
1. Öffnen Sie eine Remote Session mit PuTTY und geben Sie folgenden Befehl ein:
passwd
2. Sie werden nach einem neuen Passwort gefragt.
Geben Sie das neue Passwort entsprechend der Vorgaben ein:
Changing password for root
Enter the new password (minimum of 5 characters)
Please use a combination of upper and lower case letters and numbers.
New password:

3. Wiederholen Sie das Passwort:
Re-enter new password:
4. Sie erhalten folgende Anzeige:
passwd: password changed.
root@iot2000:~#
Das Passwort ist gesetzt.

3.4.6.2 SSH Schlüsselpaare generieren

Vorgehensweise

1. Erstellen Sie das Verzeichnis, in dem die Schlüssel gespeichert werden:
mkdir -p ~/.ssh
2. Erstellen Sie die Schlüsselpaare:
ssh-keygen -t rsa
 - Generieren Sie das Schlüsselpaar "public/private rsa".
 - Geben Sie den Speicherplatz des Schlüssels ein, z. B. /home/root/.ssh.
 - Geben Sie das Passwort ein.
Wenn Sie kein Passwort eingeben, lassen Sie die Eingabe leer.
 - Wiederholen Sie das Passwort.
Ihre Identifikation wird in folgendem Verzeichnis gespeichert: /home/root/.ssh/id_rsa.
Ihr Public Key ist in folgendem Verzeichnis gespeichert: /home/root/.ssh/id_rsa.pub.
Der Fingerabdruck des Schlüssels wird angezeigt:
SHA256:vN0y+nIMQ0Nb5UOBkZ8upyVa4wwf/8Z1IDg7TJcMvrg root@iot2000
Das Randomart Image des Schlüssels ist:



3. Kopieren Sie den Public Key mit dem Befehl "ssh-copy-id" in die Autorisierungsdateien der neuen SINUMERIK-Steuerung.
4. Stellen Sie sicher, dass Sie den Beispielnamen und die IP-Adresse ersetzt haben:
cat ~/.ssh/id_rsa.pub | ssh root@192.168.0.198 "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
 - Sie erhalten folgende Anzeige:
The authenticity of host '192.168.0.198 (192.168.0.198)' can't be established.
ECDSA key fingerprint is
SHA256:KwhYZhX1APiulK0WXUkTmzF35S9VDhqv0YcFo5/KSWg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.198' (ECDSA) to the list of known hosts.
DISPLAY "(null)" invalid; disabling X11 forwarding

Weitere Informationen zu Schlüsselpaaren finden Sie unter

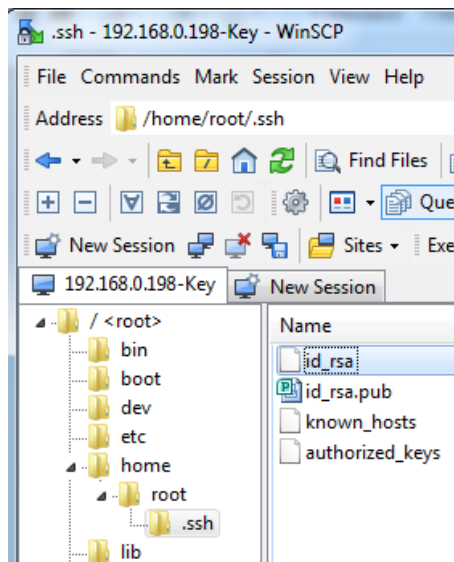
ssh key (<https://www.yoctobe.com/servers/setting-up-ssh-keys/>)

3.4.6.3 Private Key im Putty Format generieren

PuTTY SSH und der WinSCP Client für Microsoft Windows verwenden nicht das gleiche Schlüsselformat wie der OpenSSH Client. Aus diesem Grund ist es notwendig einen neuen SSH öffentlichen und privaten Schlüssel unter der Verwendung des PuTTYgen Tools zu erstellen, oder einen bereits vorhandenen OpenSSH privaten Schlüssel zu konvertieren.

Vorgehensweise

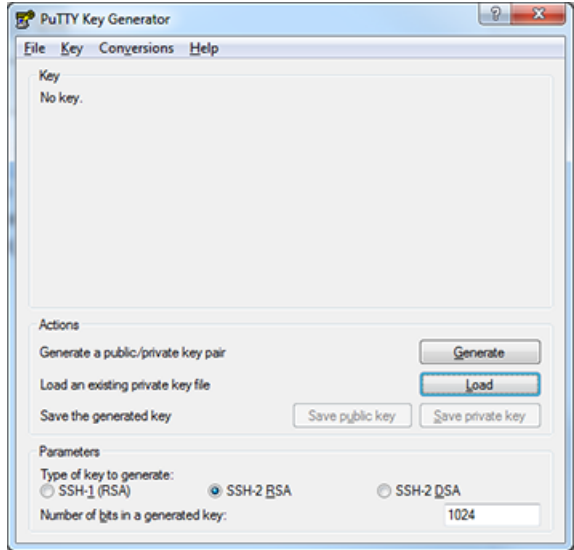
1. Laden Sie den generierten Private Key vom IoT2040 in die lokale SINUMERIK-Steuerung in folgendes Verzeichnis: /home/root/.ssh/id_rsa.



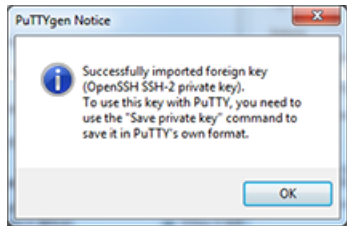
2. Starten Sie den Putty Key Generator mit einem Doppelklick auf "PuTTYgen".



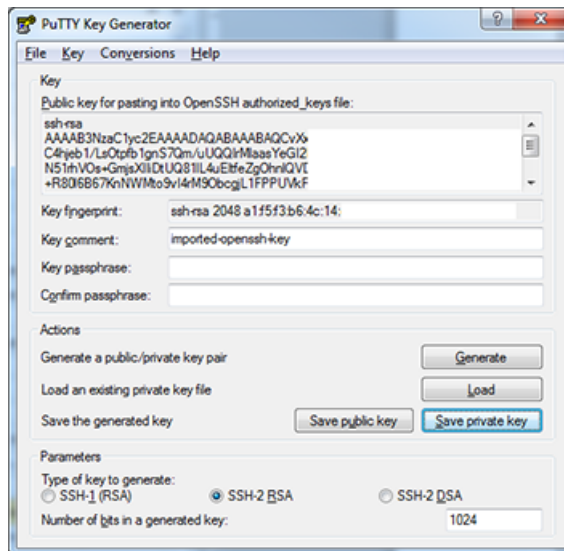
- 3. Das Fenster "PuTTY Key Generator" wird geöffnet.
Es ist noch kein Key vorhanden.
 - Klicken Sie im Bereich "Actions" auf die Schaltfläche "Load".
Laden Sie die Datei mit dem Private Key "id_rsa".



- 4. Das Fenster "PuTTYgen Notice" wird geöffnet und Sie erhalten eine Erfolgsmeldung.
Klicken Sie auf die Schaltfläche "OK".



5. Das Fenster "PuTTY Key Generator" wird geöffnet.
Der Key wird angezeigt.
 - Klicken Sie im Bereich "Actions" auf die Schaltfläche "Save private key".



6. Die neue Datei, z. B. "id_rsa_PUTTY.ppk" ist jetzt erstellt.

3.4.6.4 Mit Private Key an den IoT2040 anbinden

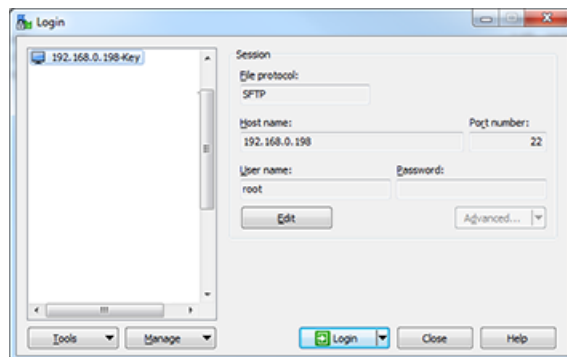
Voraussetzung

Erstellen Sie die Verbindung zu IoT2040 entweder mit WinSCP oder mit PUTTY, nachdem Sie den Private Key, z. B. "id_rsa_PUTTY.ppk" installiert haben.

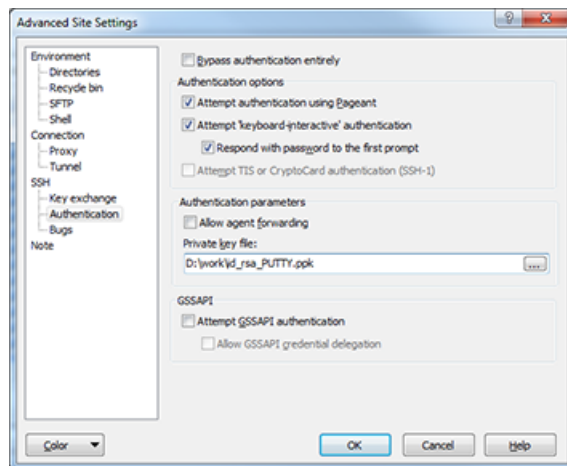
Weitere Informationen finden Sie unter: Private Key im Putty Format generieren (Seite 83).

Vorgehensweise

1. Loggen Sie sich in WinSCP ein.



2. Wählen Sie Edit > Advanced > SSH > Authentication > Authentication parameters > Private key file.



3. Deaktivieren Sie das Login mit Benutzernamen und Passwort.

Hinweis

Login sicherstellen

Führen Sie diesen Schritt nur aus, wenn Sie sicher wissen, dass Sie sich mit dem erstellten Private Key einloggen können! Sonst können Sie sich nicht mehr am IoT2040 einloggen und müssen die Firmware neu installieren.

- Erstellen Sie ein Backup, bevor Sie die nächsten Schritte durchführen.
- Öffnen Sie die Datei `"/etc/ssh/sshd_config"`.
- Ändern Sie den Parameter: `PermitRootLogin without-password`.
- Ändern Sie den Parameter: `PermitEmptyPasswords no`.
- Entfernen Sie die nicht benötigten Pakete vom Yokto Image (optional).
Aus Sicherheitsgründen wird empfohlen die nicht benötigten Pakete und Binaries zu löschen, die im voreingestellten Image des IoT2040 zur Verfügung gestellt werden.
- `opkg remove gdbserver --force-removal-of-dependent-packages`
- `opkg remove gdb-dev`

- `opkg remove gdb`

3.5 Inbetriebnahme 3rdPartyController/ FANUC/ MTConnect

3.5.1 Übersicht

Voraussetzung

- Windows 7 SP1
- Die aktuellen Windows Patches müssen installiert sein
- .NET Framework 4.x muss installiert sein
- MicrosoftEasyFix51044 muss installiert sein, damit der TLS 1.2 funktioniert
Weitere Informationen zu MicrosoftEasyFix51044 finden Sie unter: Support Microsoft (<https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in#easy>)
Der direkte Download Link ist: Download microsoftEasyFix51044 (<https://aka.ms/easyfix51044>)
- Visual C++ (freie Software für Visual Studio 2015 oder höher) muss installiert sein
- SINUMERIK Integrate Client Version 4.12.0.21
- Um eine Verbindung zu MindSphere herzustellen, muss der TLS 1.2 Support aktiviert sein.
Weitere Informationen zu MindSphere finden Sie im
Installationshandbuch SINUMERIK Integrate MMP, MMT, AMC, AMP, AMM/E, AMD

Einleitung

Um ManageMyMachines mit FANUC-Steuerungen zu nutzen, müssen Sie folgende Installationen und Konfigurationen durchführen:

1. SINUMERIK Integrate-/ ePS-Client installieren
Informationen zum SINUMERIK Integrate-/ ePS-Client finden Sie unter: SINUMERIK Integrate Client installieren (Seite 89)
2. FanucModule installieren
Informationen zur Installation finden Sie unter: Installation mit dem 3rdPartyController (Seite 99)
3. FanucModule in SINUMERIK Integrate-/ ePS-Client einbinden
Informationen zur Einbindung finden Sie unter: Aktuellen Treiber mit dem Fanuc Treiber ersetzen (Seite 101)
4. MTConnect in SINUMERIK Integrate-/ ePS-Client einbinden
Informationen zur Einbindung finden Sie unter: Aktuellen Treiber mit dem MTConnect Treiber ersetzen (Seite 102)
5. FanucModule und MindSphere konfigurieren
Informationen zur Konfiguration finden Sie unter: FanucModule und MindSphere konfigurieren (Seite 105)

6. MTConnect und MindSphere konfigurieren
Informationen zur Konfiguration finden Sie unter: MTConnect und MindSphere konfigurieren (Seite 106)

7. Benutzerdefinierte Einstellungen in MindSphere konfigurieren
Informationen zur Konfiguration finden Sie unter: Variable einbinden (Seite 108)

Wenn Sie den 3rdPartyController nicht mehr nutzen, deinstallieren Sie die Software.
Informationen zur Deinstallation finden Sie unter: 3rdPartyController deinstallieren (Seite 116)

Hinweis

Datei-Upload

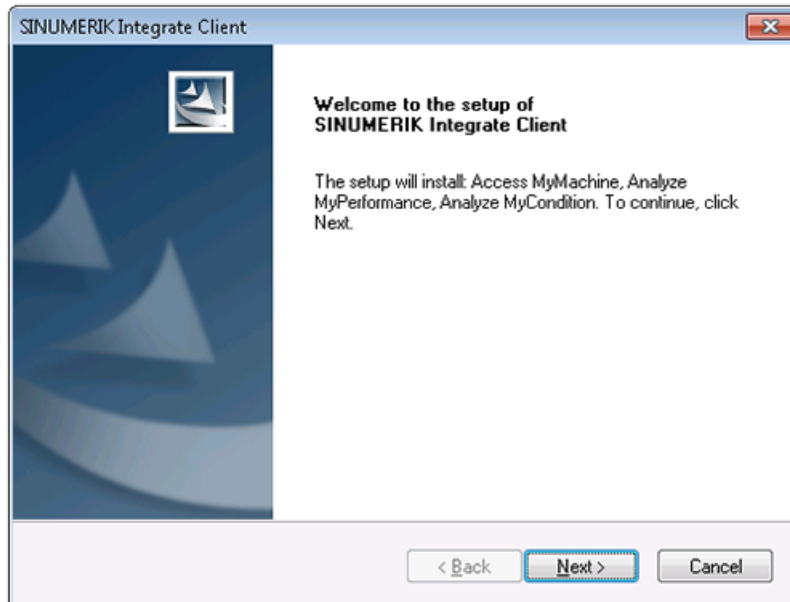
Wegen fehlender Treiber wird derzeit der Datei-Upload auf FANUC-Steuerungen nicht unterstützt.

3.5.2 SINUMERIK Integrate Client installieren

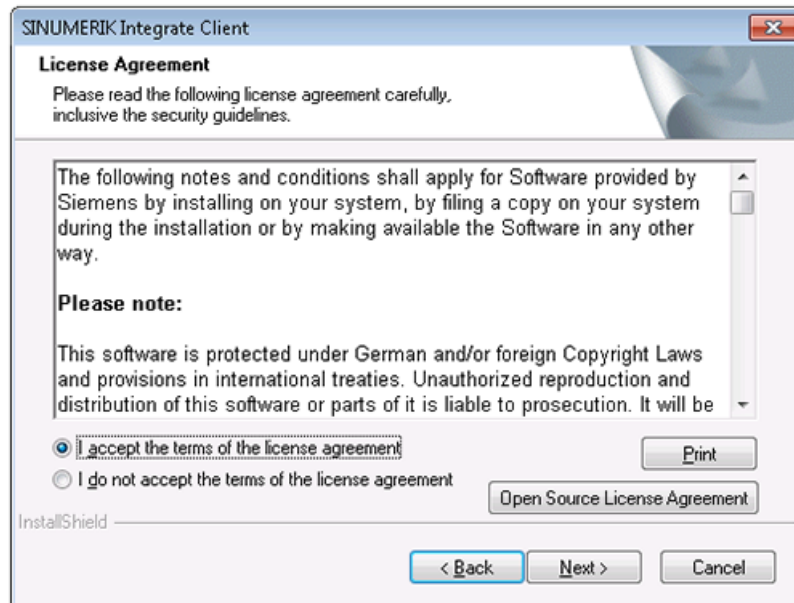
Vorgehensweise

1. Starten Sie die SINUMERIK-Steuerung im Windows Servicemodus.
2. Öffnen Sie das Installationsverzeichnis.
3. Starten Sie die Setup-Datei "setup.exe" mit Doppelklick.
 - Wenn Sie nicht den passenden Internet Explorer installiert haben, erhalten Sie eine entsprechende Meldung, z. B. "Das Programm benötigt den Internet Explorer 6 oder höher".
Die Installation wird abgebrochen und Sie müssen zuerst den entsprechenden Internet Explorer installieren.
Anschließend starten Sie die Client-Installation erneut.

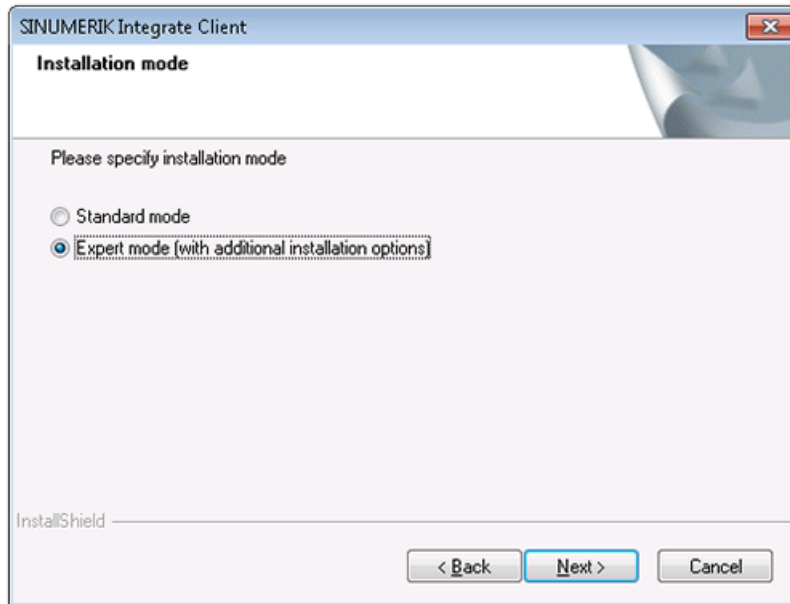
4. Der Willkommensdialog wird geöffnet.
Die Installationssprache ist Englisch.
Klicken Sie auf die Schaltfläche "Next >", um mit der Installationsvorbereitung zu beginnen.



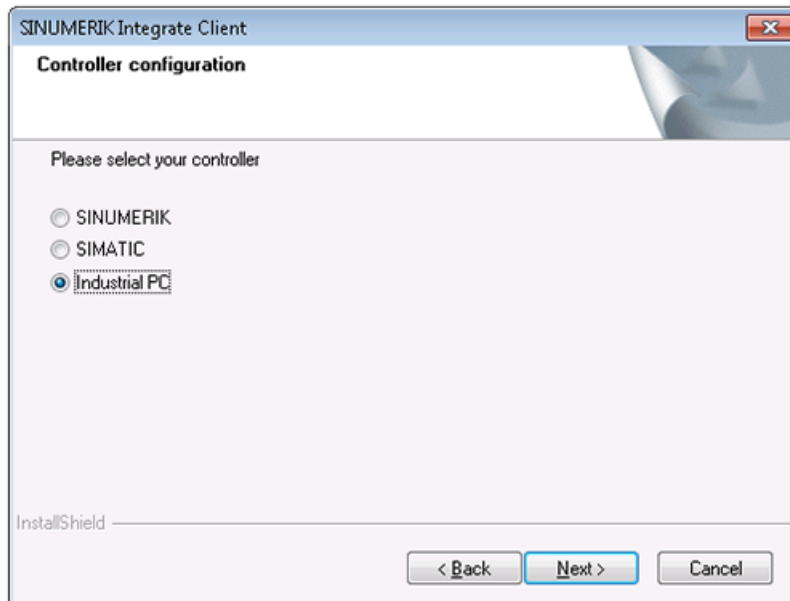
5. Das Fenster "License Agreement" wird geöffnet.
Lesen Sie die Lizenzvereinbarung.
 - Wenn Sie sich die Bedingungen ausdrucken möchten, klicken Sie auf die Schaltfläche "Print".
 - Aktivieren Sie anschließend das Optionsfeld "I accept the terms of the license agreement" und klicken Sie auf die Schaltfläche "Next >".
 - ODER -Wenn Sie auf die Schaltfläche "< Back" klicken, gelangen Sie jeweils in das vorherige Fenster.



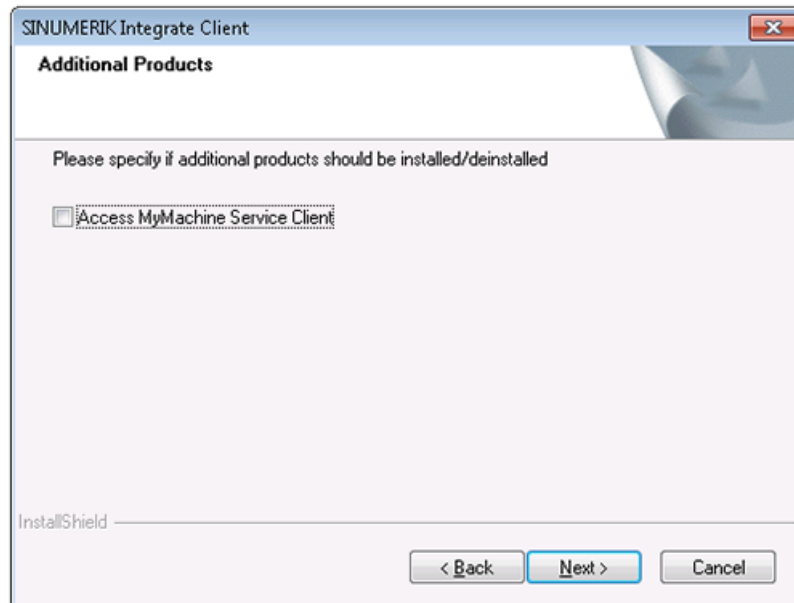
6. Das Fenster "Installation mode" wird geöffnet.
 - Aktivieren Sie das Optionsfeld "Expert mode (with additional installation options)".
 - Klicken Sie auf die Schaltfläche "Next >".



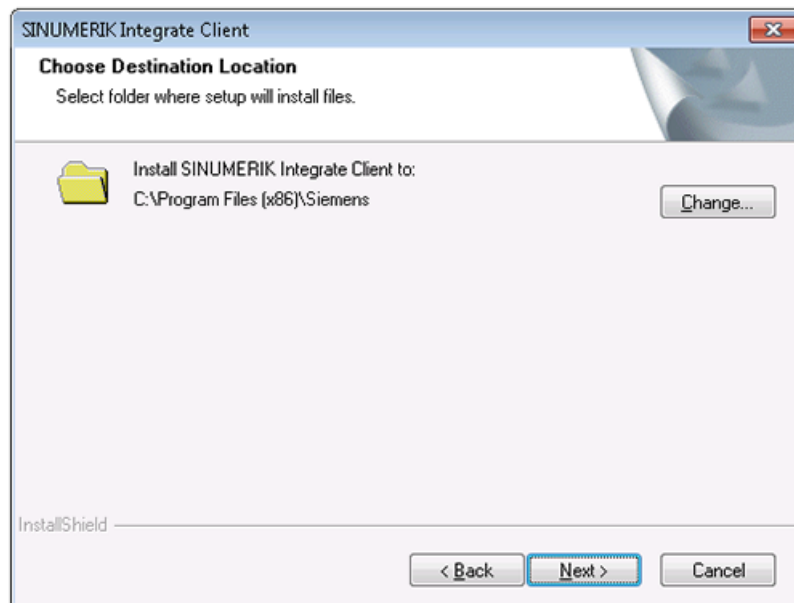
7. Das Fenster "Controller configuration" wird geöffnet.
 - Aktivieren Sie das Optionsfeld "Industrial PC".
 - Klicken Sie auf die Schaltfläche "Next >".



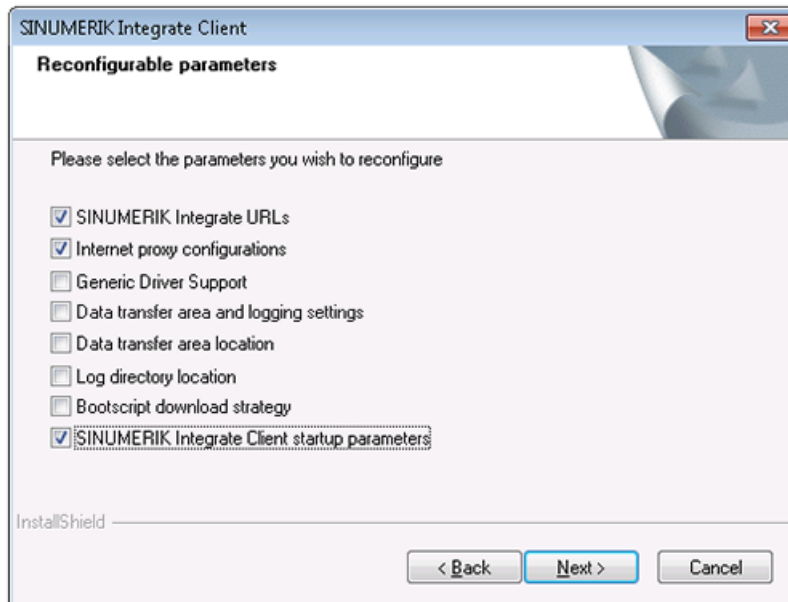
8. Das Fenster "Additional Products" wird geöffnet.
 - Klicken Sie auf die Schaltfläche "Next >".



9. Das Fenster "Choose Destination Location" wird geöffnet und das Installationsverzeichnis angezeigt.
 - Klicken Sie auf die Schaltfläche "Next >".
 - ODER -
 - Um das Verzeichnis zu wechseln, klicken Sie auf die Schaltfläche "Change...".



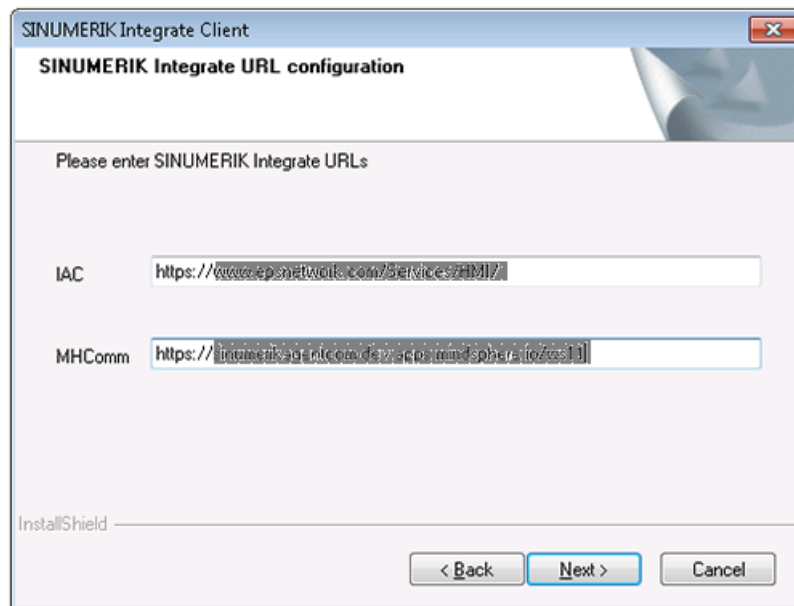
10. Das Fenster "Reconfigurable parameters" wird geöffnet.
Aktivieren Sie die Optionskästchen:
- "SINUMERIK Integrate URLs"
 - "Internet proxy configurations"
 - "SINUMERIK Integrate Client startup parameters"
 - Klicken Sie auf die Schaltfläche "Next >".



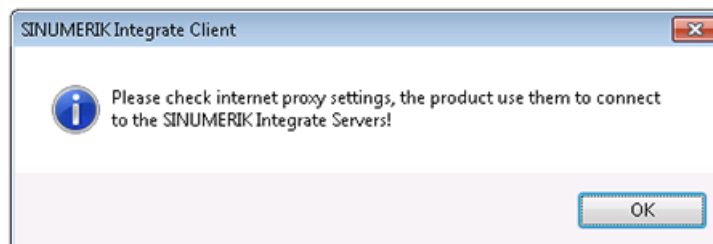
11. Das Fenster "SINUMERIK Integrate URL configuration" wird geöffnet.
Der Proxy-Server wird für die Verbindung der Steuerung mit der MindSphere benötigt.
Tragen Sie im Eingabefeld "MHComm" folgende Webservice URL ein, je nachdem mit welchem MindSphere-System Sie verbunden sind:

- MindSphere V3 Livesystem (<https://gateway.eu1.mindsphere.io/api/agentcommmops/v3/ws11>)
- MindSphere Alibaba (<https://gateway.cn1.mindsphere-in.cn/api/agentcom-dimcopt/v3/ws11>)

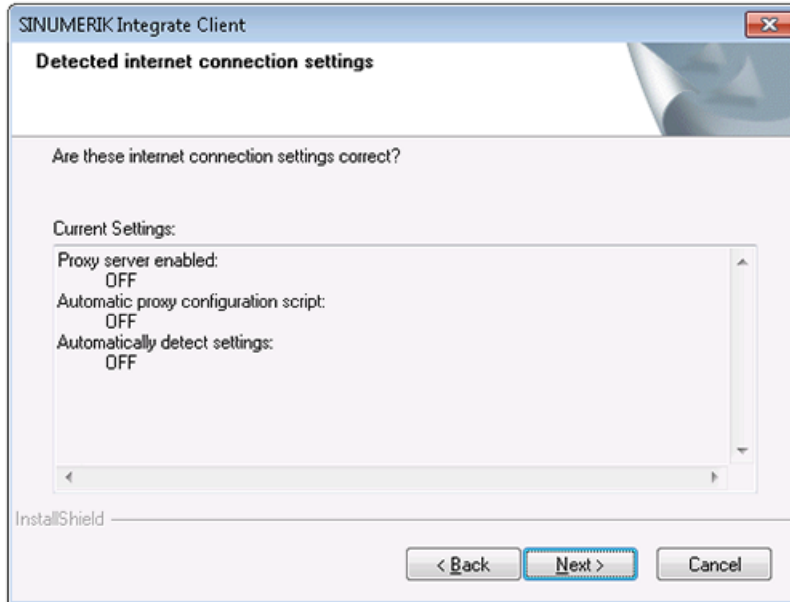
Klicken Sie auf die Schaltfläche "Next >".



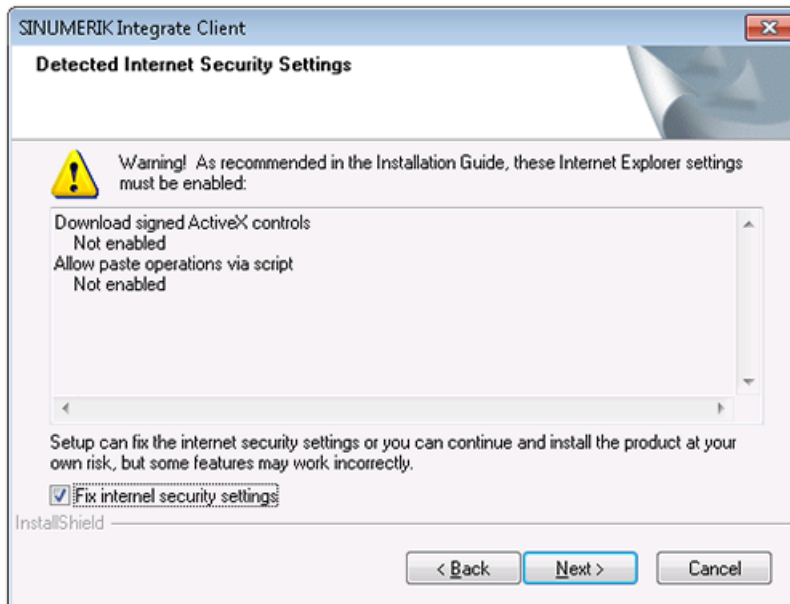
12. Folgende Meldung wird angezeigt.
Klicken Sie auf die Schaltfläche "OK", um den Proxy-Server anzupassen.



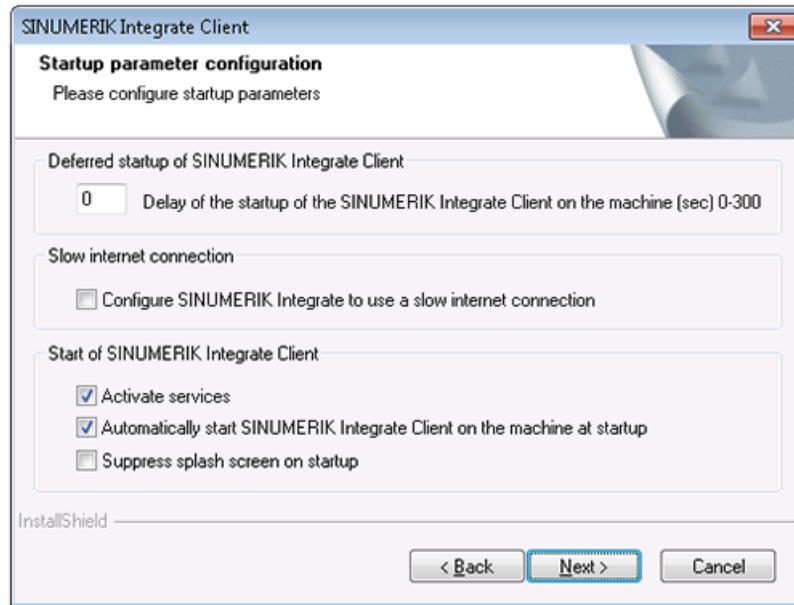
13. Das Fenster "Detected internet connection settings" wird angezeigt. Klicken Sie auf die Schaltfläche "Next >".



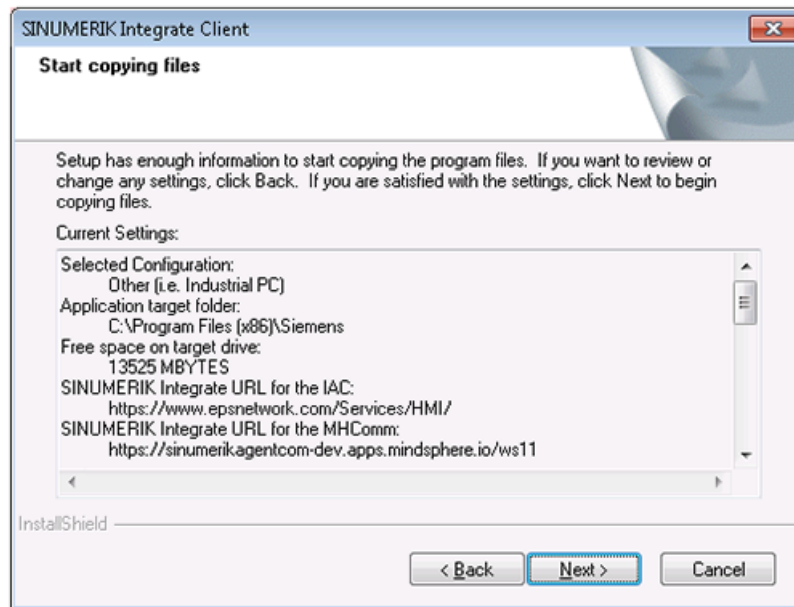
14. Das Fenster "Detected Internet Security Settings" wird angezeigt.
- Aktivieren Sie das Kontrollkästchen "Fix internet security settings".
 - Klicken Sie auf die Schaltfläche "Next >".



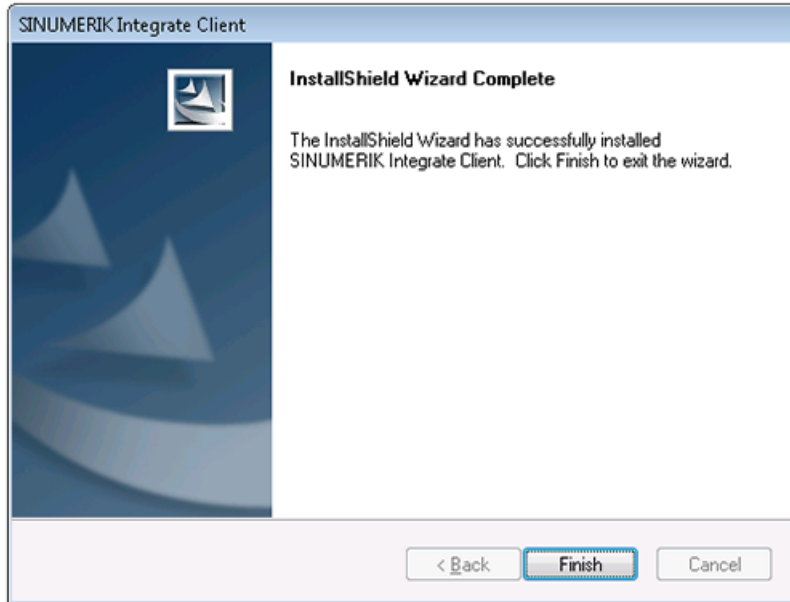
15. Das Fenster "Startup parameter configuration" wird geöffnet.
Aktivieren Sie die Optionskästchen:
- "Activate services"
 - "Automatically start SINUMERIK Integrate Client on the machine at startup"
 - Klicken Sie auf die Schaltfläche "Next >".



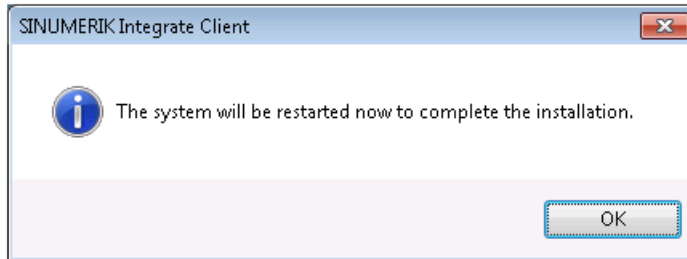
16. Das Fenster "Start copying files" wird geöffnet und die vorgenommenen Einstellungen angezeigt.
- Klicken Sie auf die Schaltfläche "Next >", um die Daten auf die SINUMERIK-Steuerung zu kopiert.



- 17. Das Fenster "InstallShield Wizard Complete" wird geöffnet. Klicken Sie auf die Schaltfläche "Finish".



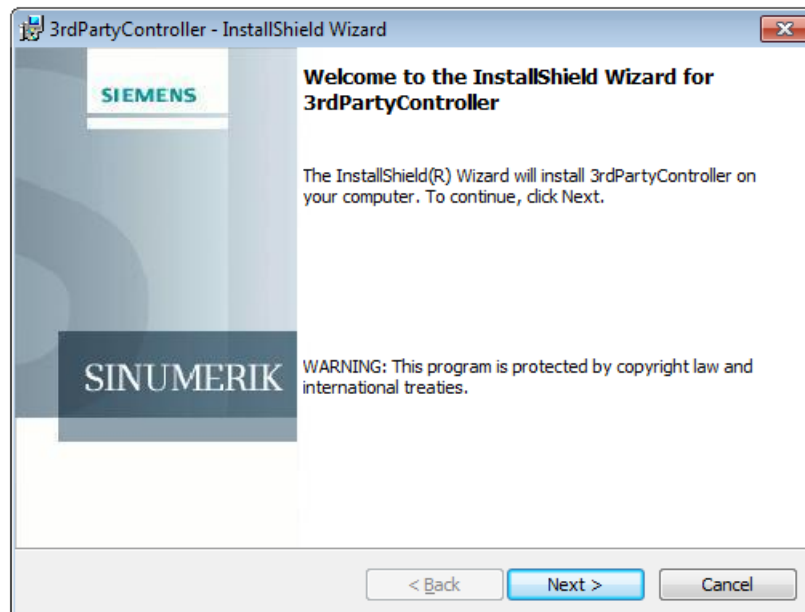
- 18. Sie erhalten die Meldung, einen Neustart auszuführen. Klicken Sie dazu auf die Schaltfläche "OK".



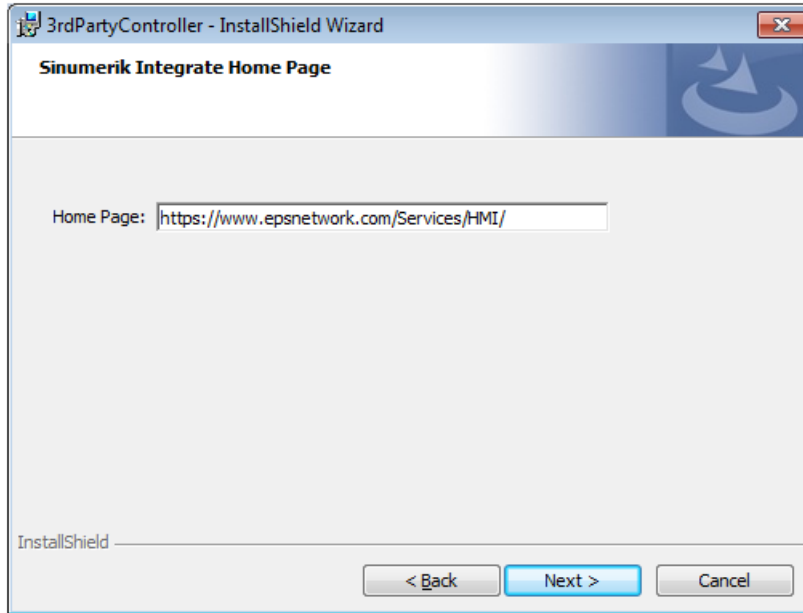
3.5.3 Installation mit dem 3rdPartyController

Vorgehensweise

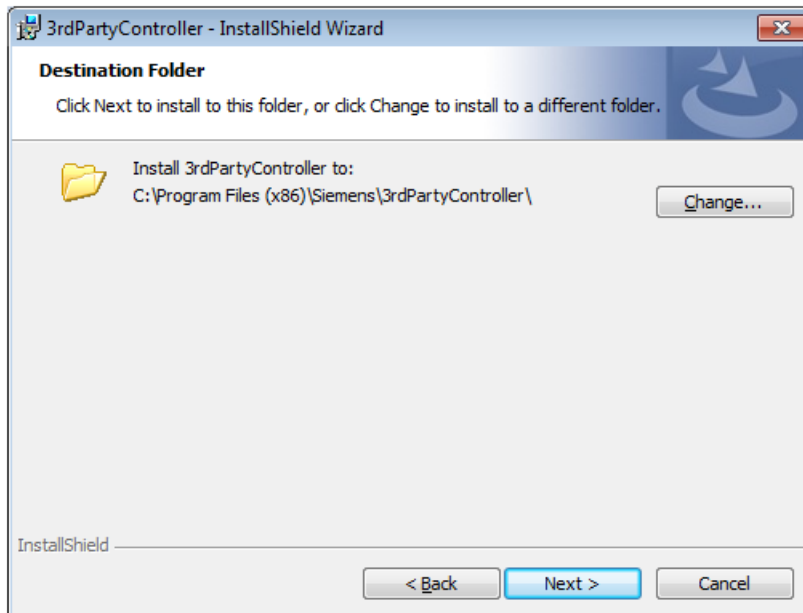
1. Doppelklicken Sie auf die Datei "3rdPartyControllerSetup.exe".
 - Wenn Sie nicht den passenden Internet Explorer installiert haben, erhalten Sie eine entsprechende Meldung, z. B. "Das Programm benötigt den Internet Explorer 6 oder höher".
Die Installation wird abgebrochen und Sie müssen zuerst den entsprechenden Internet Explorer installieren.
Anschließend starten Sie die Client-Installation erneut.
2. Der Willkommensdialog wird geöffnet.
Die Installationssprache ist Englisch.
Klicken Sie auf die Schaltfläche "Next >".



3. Verwenden Sie den vorgeschlagenen Installationsordner für die Installation des 3rdPartyController.



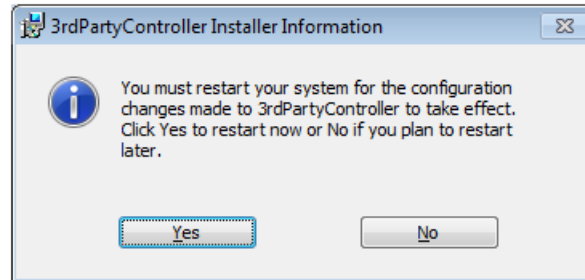
4. Klicken Sie auf die Schaltfläche "Next>". Die Installation wird durchgeführt.



5. Nach Beendigung der Installation erhalten Sie die Meldung einen Neustart durchzuführen. Klicken Sie auf die Schaltfläche "No", um die Einstellungen zu editieren und die aktuellen Treiber mit Ihren Treibern zu ersetzen.

Aktuell sind im 3rdPartyController Paket 2 Treiber verfügbar:

- Fanuc Treiber
- MTConnect Treiber



6. Nachdem Sie Ihre Treiber eingesetzt haben, führen Sie einen Neustart durch.

3.5.4 Aktuellen Treiber mit dem Fanuc Treiber ersetzen

Vorgehensweise

Um "FanucModule" einzubinden, müssen Sie den aktuellen Treiber mit dem Fanuc Treiber ersetzen. Dazu passen Sie die Konfigurationsdatei des Clients "settings.ini" manuell an.

Wenn der Client im Standard-Verzeichnis installiert wurde, dann liegt die Datei "settings.ini" in folgendem Verzeichnis:

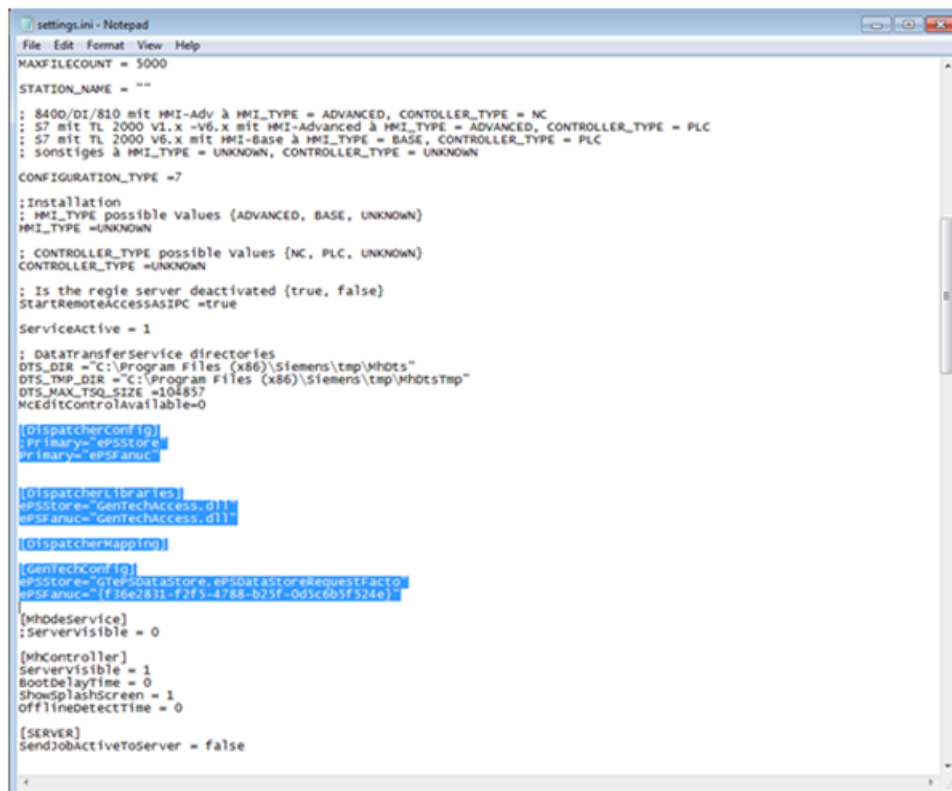
```
C:\Program Files (x86)\Siemens\MH\settings.ini
```

1. Öffnen Sie die Datei mit einem beliebigen Editor.
2. Suchen Sie folgende Einträge:
 - [DispatcherConfig],
 - [DispatcherLibraries]
 - [GenTechConfig]

3.5 Inbetriebnahme 3rdPartyController/ FANUC/ MTConnect

3. Ändern Sie diese Bereiche wie folgt:

```
[DispatcherConfig]
;Primary="ePSStore"
Primary="ePSFanuc"
[DispatcherLibraries]
ePSStore="GenTechAccess.dll"
ePSFanuc="GenTechAccess.dll"
[DispatcherMapping]
[GenTechConfig]
ePSStore="GTePSDataStore.ePSDataStoreRequestFacto"
ePSFanuc="{f36e2831-f2f5-4788-b25f-0d5c6b5f524e}"
```



4. Speichern Sie ihre Änderungen und starten Sie den Rechner neu, um die Änderungen zu aktivieren.

3.5.5 Aktuellen Treiber mit dem MTConnect Treiber ersetzen

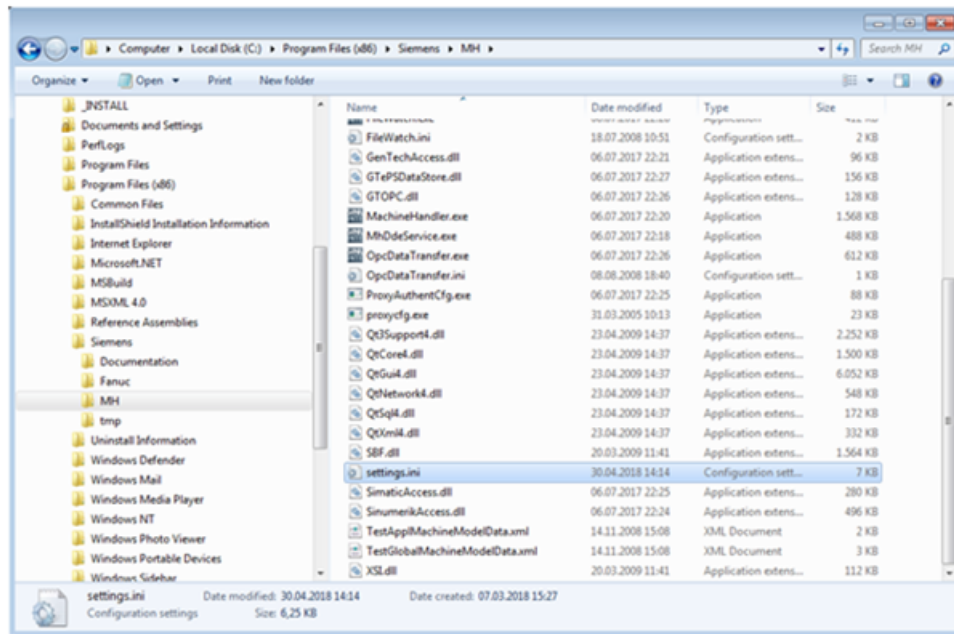
Vorgehensweise

Um "MTConnect" einzubinden, müssen Sie den aktuellen Treiber mit dem MTConnect Treiber ersetzen. Dazu passen Sie die Konfigurationsdatei des Clients "settings.ini" manuell an.

Wenn der Client im Standard-Verzeichnis installiert wurde, dann liegt die Datei "settings.ini" in folgendem Verzeichnis:

C:\Program Files (x86)\Siemens\MH\settings.ini

1. Öffnen Sie die Datei mit einem beliebigen Editor.



2. Suchen Sie folgende Einträge:

- [DispatcherConfig],
- [DispatcherLibraries]
- [GenTechConfig]

3.5 Inbetriebnahme 3rdPartyController/ FANUC/ MTConnect

- Ändern Sie diese Bereiche wie folgt:

```
[DispatcherConfig]
;Primary="ePSStore"
Primary="ePSMTConnect"
[DispatcherLibraries]
ePSStore="GenTechAccess.dll"
ePSMTConnect="GenTechAccess.dll"
[DispatcherMapping]
[GenTechConfig]
ePSStore="GTePSDataStore.ePSDataStoreRequestFacto"
ePSMTConnect="{ f36e2831-f2f5-4788-b25f-0d5c6b5f524e} "
```



- Ersetzen Sie den Inhalt der Beispieldatei mit der richtigen Maschinendatei:
C:\Program Files (x86)\Siemens\cppagent_bin\bin\agent.cfg
Weitere Informationen zur Dateisyntax finden Sie auf der Seite des Cppagent Projekt:
Syntax Github (<https://github.com/mtconnect/cppagent>)

- Klicken Sie mit der rechten Maustaste auf die folgende Datei:
Program Files (x86)\Siemens\MH\registerMTConnectModule.bat

6. Wählen Sie die Option "Run as Administrator".
7. Führen Sie einen Neustart durch.

3.5.6 FanucModule und MindSphere konfigurieren

Voraussetzung

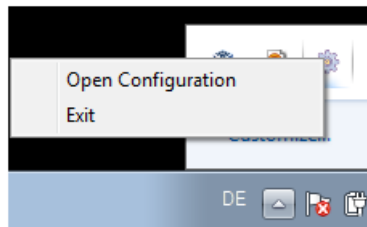
Um die IP-Adresse der zu verbindenden Maschine im "FanucModule" zu konfigurieren, führen Sie einen Neustart durch.

FanucModule konfigurieren – Verbindung zur Maschine

1. Klicken Sie mit der rechten Maustaste auf das Symbol "FanucConfig" im Infobereich der Taskleiste "system tray".



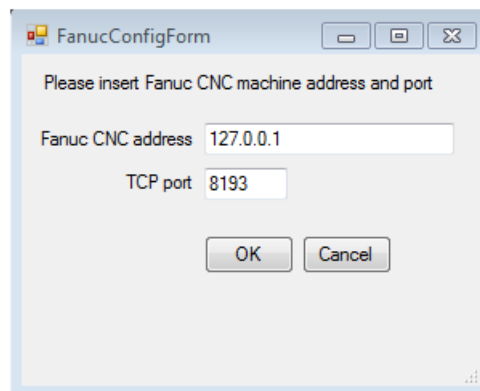
2. Wählen Sie "Open Configuration".



3. Konfigurieren Sie die IP-Adresse der FANUC-Steuerung, z. B.:
 - Fanuc CNC address: 127.0.0.1
 - Der TCP-Port sollte in den meisten Fällen nicht geändert werden.

Klicken Sie auf die Schaltfläche "OK".

Die Konfiguration ist aktiviert und das FanucModule ist zur Datenerfassung bereit.



3.5.7 MTConnect und MindSphere konfigurieren

Vorgehensweise

1. Stellen Sie sicher, dass MTConnect auf der Maschinenseite ordnungsgemäß installiert ist. Weitere Informationen hierzu finden Sie unter: MTConnect-Projektseite
2. Starten Sie die Konfiguration auf der IPC Seite.
3. Navigieren Sie zu
C:\Program Files\Siemens\cppagent_bin\bin
4. Öffnen Sie die Datei "agent.cfg" in einem Editor. Sie sehen den folgenden Inhalt.

```
1 Devices = ../simulator/VMC-3Axis.xml
2 AllowPut = true
3 ReconnectInterval = 1000
4 BufferSize = 17
5 SchemaVersion = 1.4
6
7 Adapters {
8     VMC-3Axis {
9         Host = 127.0.0.1
10        Port = 7878
11    }
12 }
13
14 Files {
15     schemas {
16         Path = ../schemas
17         Location = /schemas/
18     }
19     styles {
20         Path = ../styles
21         Location = /styles/
22     }
23     Favicon {
24         Path = ../styles/favicon.ico
25         Location = /favicon.ico
26     }
27 }
28
29 StreamsStyle {
30     Location = /styles/Streams.xml
31 }
32
33 # Logger Configuration
34 logger_config
35 {
36     logging_level = debug
37     output = cout
38 }
```

5. Geben Sie die IP-Adresse Ihrer Maschine ein, z. B.:

```

6  Adapters
7  {
8      Adapter_1
9      {
10         Host = 172.27.33.128
11         Port = 7878
12     }
13 }

```

6. Konfigurieren Sie eine XML-Datei, die Ihre Maschine definiert.

```

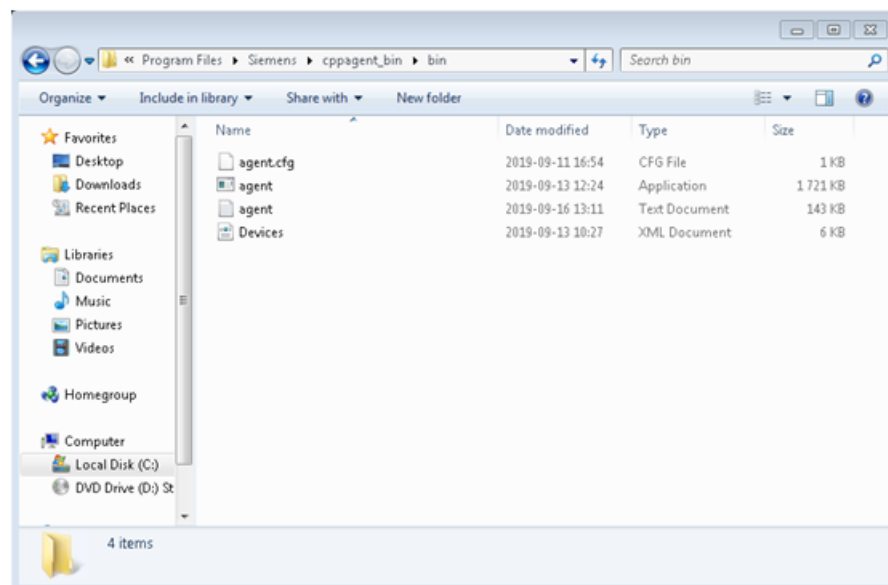
<Controller id="controllerv1" name="v1">
  <DataItem>
    <DataItem category="EVENT" id="/Bag/State/opMode[u1]" name="op_mode" type="CONTROLLER_MODE"/>
    <DataItem category="SAMPLE" id="/Nck/Configuration/accessLevel" name="accessLevel" type="PERCENT"/>
  </DataItem>
  <Component>
    <Path id="path1" name="p1">
      <DataItem>
        <DataItem category="SAMPLE" id="/Channel/State/progStatus[u1]" name="pl_status" type="EXECUTION"/>
        <DataItem category="EVENT" id="/Channel/State/stopCond[u1]" name="pl_status_stop" type="CONTROLLER_MODE_OVERRIDE" #dtType="OPTIONAL_STOP"/>
        <DataItem category="SAMPLE" id="/Channel/ProgramPointer/programName[u1]" name="pl_program" type="PROGRAM"/>
        <DataItem category="SAMPLE" id="/Channel/State/feedRateOvr[u1]" name="pl_feedrate_override" type="DATA_FEEDRATE_OVERRIDE" #dtType="PROGRAMMED" units="PERCENT"/>
        <DataItem category="SAMPLE" id="/Channel/Spindle/speedOvr[u1]" name="pl_spindle_override" type="ROTARY_VELOCITY_OVERRIDE" units="PERCENT"/>
      </DataItem>
    </Path>
  </Component>
</Controller>

```

Die XML-Datei muss folgende IDs enthalten:

- /Bag/State/opMode[u1]
- /Nck/Configuration/accessLevel
- /Channel/State/progStatus[u1]
- /Channel/State/stopCond[u1]
- /Channel/ProgramPointer/programName[u1,1]
- /Channel/State/feedRateIpoOvr[u1]
- /Channel/Spindle/speedOvr[u1,1]

Nach der Konfiguration sollte das Verzeichnis aussehen wie folgt:



7. Starten Sie Ihren PC neu.

Prüfen der Konfiguration

1. Um die Konfiguration zu prüfen, geben Sie die folgende Adresse ein:
`http://127.0.0.1:5000/current`
Wird die Seite nicht angezeigt, prüfen Sie die Logdateien des Agent. Der Speicherort der Logdateien wird in der Agent .cfg-Datei festgelegt.
2. Werden die Werte auf dem Dashboard nicht ordnungsgemäß angezeigt, prüfen Sie die folgende Datei:
`C:\Program Files\Siemens\3rdPartyController\mapMTConnect.xml`
Hier werden alle Eingaben an MindSphere angezeigt.
3. Sendet Ihre Maschine im aktiven Status die Nachricht "Running?", dann geben Sie ein anderes Alias ein, z. B. "OFF", oder "UNAVAILABLE" im Bereich `"/Channel/State/stopCond[u1]"` ein.
Die Applikation wird dann dem neuen Mapping folgen.

Hinweis

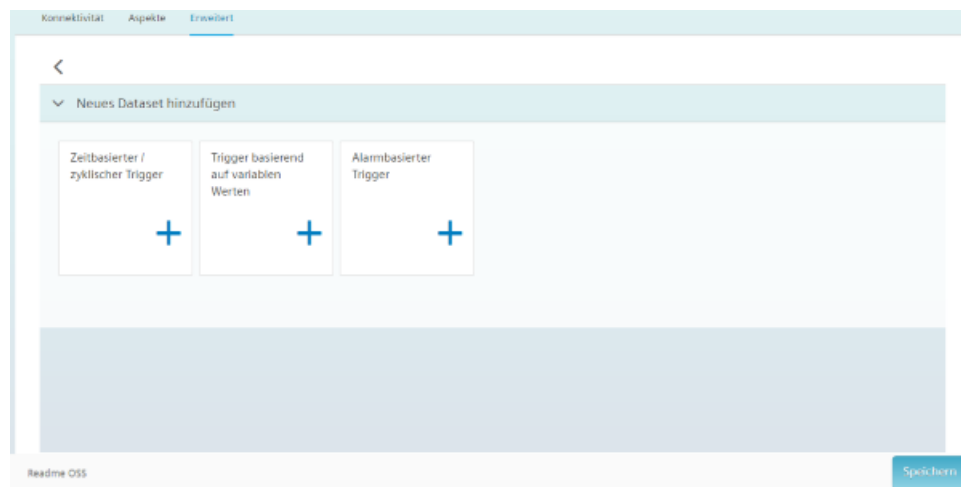
Gültige XML-Datei

Prüfen Sie, ob Sie nach den Änderungen eine gültige XML-Datei erzeugt haben.

3.5.8 Variable einbinden

Benutzerdefinierte Variable und Alarme

1. Wählen Sie im "MTA Asset Config" das Register "Erweitert".
2. Klicken Sie auf die Schaltfläche "Variablen hinzufügen".
Sie erhalten eine Eingabezeile für die neue Variable
3. Klicken Sie auf den kleinen Pfeil > links neben dem Eingabefeld.
4. Klicken Sie auf die Schaltfläche "Konfiguration hinzufügen".
Die Auswahl der Trigger wird angezeigt.
5. Wählen Sie mit Mausclick den gewünschten Trigger.



Zeitbasierter / zyklischer Trigger

Die zeitbasierte / zyklische Erfassung erfolgt in MindSphere ähnlich wie bei SINUMERIK-Steuerungen.

Die Adressen sind jedoch unterschiedlich.

The screenshot shows the 'Erweitert' (Advanced) configuration page for a time-based trigger. At the top, there are tabs for 'Konnektivität', 'Aspekte', and 'Erweitert'. Below the tabs, there is a back arrow and a dropdown menu for 'Aspektname *'. To the right of this dropdown is an 'Abbrechen' button. Below the dropdown is a 'Lesezyklus' field with a value of '5 Sekunde(n)' and a unit dropdown menu. Underneath is a table with columns: 'Name', 'Adresse', 'Datentyp', and 'Einheit'. The table content shows 'Keine Daten'. Below the table is a 'Variable hinzufügen' button. At the bottom left, it says 'Readme OSS', and at the bottom right, there is a blue 'Speichern' button.

Trigger basierend auf variablen Werten

1. Definieren Sie den neuen Aspekt.
Geben Sie die entsprechenden Werte ein.
2. Klicken Sie auf die Schaltfläche "Speichern".

The screenshot shows the 'Erweitert' (Advanced) configuration page for a variable-based trigger. At the top, there are tabs for 'Konnektivität', 'Aspekte', and 'Erweitert'. Below the tabs, there is a back arrow and a dropdown menu for 'Wenn die Variable'. To the right of this dropdown is an 'Abbrechen' button. Below the dropdown are several input fields: 'Datenerfassungsname *', 'Variablenadresse *', a 'DOUBLE' dropdown, a 'Größer als' dropdown, and 'Variablenwert'. Below these is the text 'Mit der folgenden Konfiguration'. Underneath are 'Entprellzeit *' with a 'min' dropdown, a 'Hysterese' checkbox, a 'Hysterese' input field, and radio buttons for 'Relativ' and 'Absolut' (which is selected). Below this is a 'Dann' dropdown menu. Underneath are 'Folgenden Wert aufzeichnen' dropdown, 'Variablenadresse *', and a 'DOUBLE' dropdown. At the bottom left, it says 'Readme OSS', and at the bottom right, there is a blue 'Speichern' button.

Variablentypen

In der folgenden Tabelle sehen Sie einige Beispiele zur Erfassung von Variablen aus der FANUC-Steuerung.

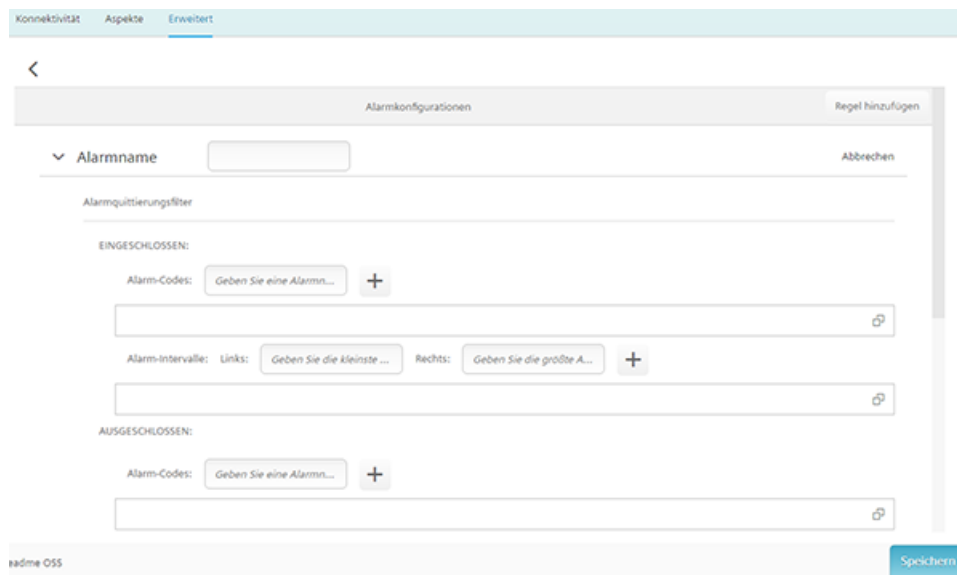
Weitere Variablen, die von der FOCAS-Library unterstützt werden, sind möglich.

Weitere Informationen zur Einbindung der Variablen in MindSphere finden Sie im Kapitel: MTConnect - Beispiel: Variable einbinden (Seite 111)

Name	Datentyp	Adresse
AxisAbs1	DOUBLE	/TPC/focas/cnc/dynamic2/pos/absolute[1]
AxisAbs2	DOUBLE	/TPC/focas/cnc/dynamic2/pos/absolute[2]
AxisAbs3	DOUBLE	/TPC/focas/cnc/dynamic2/pos/absolute[3]
AxisRel1	DOUBLE	/TPC/focas/cnc/dynamic2/pos/relative[1]
AxisRel2	DOUBLE	/TPC/focas/cnc/dynamic2/pos/relative[2]
AxisRel3	DOUBLE	/TPC/focas/cnc/dynamic2/pos/relative[3]
Axis1_dist	DOUBLE	/TPC/focas/cnc/dynamic2/pos/distance[1]
Axis2_dist	DOUBLE	/TPC/focas/cnc/dynamic2/pos/distance[2]
Axis3_dist	DOUBLE	/TPC/focas/cnc/dynamic2/pos/distance[3]
Axis1	STRING	/TPC/focas/cnc/axisname[1]
Axis2	STRING	/TPC/focas/cnc/axisname[2]
Axis3	STRING	/TPC/focas/cnc/axisname[3]
Spindle1	STRING	/TPC/focas/cnc/spdlname[1]
ActFeedRate	DOUBLE	/TPC/focas/cnc/dynamic2/actf
SequenceNr	DOUBLE	/TPC/focas/cnc/dynamic2/seqnum
feedRate-poOvr	DOUBLE	/TPC/focas/pmc/pmcrng/G/byte[1,12](mmm_fanuc_feedoverride)
speedOvr	DOUBLE	/TPC/focas/pmc/pmcrng/G/byte[1,30](mmm_fanuc_spindleoverride)

Alarmbasierter Trigger

Für die FANUC-Steuerung müssen Sie den zu erfassenden Alarmbereich konfigurieren. Die Erfassung der Alarme erfolgt in MindSphere ähnlich wie bei SINUMERIK-Steuerungen. Sie müssen mindestens einen "Alarmbasierten Trigger" einrichten.



Alarmtypen

FANUC-Steuerungen unterstützen 16 Alarmtypen. Jeder Alarmtyp kann wiederum bis zu 10.000 numerische Werte haben.

In der folgenden Tabelle sehen Sie eine Auflistung aller möglichen Alarme:

Fanuc Alarm Typ	Fanuc Alarm Namensbereich	Numerischer Alarm ID Bereich
SW	SW0000 – SW9999	100000 – 109999
PW	PW0000 – PW9999	110000 – 119999
IO	IO0000 – IO9999	120000 – 129999
PS	PS0000 – PS9999	130000 – 139999
OT	OT0000 – OT9999	140000 – 149999
OH	OH0000 – OH9999	150000 – 159999
Sv	Sv0000 – Sv9999	160000 – 169999
SR	SR0000 – SR9999	170000 – 179999
MC	MC0000 – MC9999	180000 – 189999
SP	SP0000 – SP9999	190000 – 199999
DS	DS0000 – DS9999	200000 – 209999
IE	IE0000 – IE9999	210000 – 219999
BG	BG0000 – BG9999	220000 – 229999
SN	SN0000 – SN9999	230000 – 239999
EX	EX0000 – EX9999	240000 – 249999
PC	PC0000 – PC9999	250000 – 259999

- Konfigurieren Sie entweder jeweils einzelne Subbereiche oder alle Alarme auf einmal.
- Um alle Alarme zu erfassen, konfigurieren Sie den Bereich 100.000 bis 260.000.

Beispiel

Sie wollen die Anzeige aller SW-Alarme sehen:

Geben Sie ein:

- Links: 100.000
- Rechts: 260.000

3.5.9 MTConnect - Beispiel: Variable einbinden

Sie haben die Möglichkeit weitere Variable in MindSphere einzubinden.

Voraussetzung

- Variable müssen von der FOCAS-Library unterstützt werden.
- Datei "Devices.xml".

VariableA anlegen

1. Öffnen Sie MindSphere.
2. Erstellen Sie im "Asset Manager" ein Asset.
3. Öffnen Sie das Asset und wählen Sie "MTA Asset Config".
4. Erstellen Sie die Variable, z. B. "VariableA".
5. Legen Sie den Pfad und Dateiname "Devices.xml" in der Datei "agent.cfg" fest.
Die Datei liegt in folgendem Verzeichnis: C:\Program Files\Siemens\cppagent_bin\bin\agent.cfg

6. Im Beispiel sehen Sie folgenden Dateninhalt der Datei "agent.cfg":

```
ServiceName = MTConnect Agent 840D
BufferSize = 17
Devices = Devices.xml
Port = 5000
Adapters
{
Adapter_1
  {
    Host = 172.27.33.128
    Port = 7878
  }
}
# Logger Configuration
logger_config
{
  logging_level = info
  output = file agent.log
}
```

- Zeile "Devices = Devices.xml": Hier legen Sie fest, wo sich die xml-Datei befindet und wie sie heißt:
Beispiel: Devices = D:\MyMachine.xml

7. In der Datei "MyMachine.xml" tragen Sie alle Änderungen ein:

Beispiel: Die Steuerung soll Informationen in folgendem Format senden:

```
<DataItems>
<DataItem category="SAMPLE" id="x2" name="Xact"
nativeUnits="MILLIMETER" subType="ACTUAL" type="POSITION"
units="MILLIMETER"/>
<DataItem category="SAMPLE" id="x3" name="Xcom"
nativeUnits="MILLIMETER" subType="COMMANDED" type="POSITION"
units="MILLIMETER"/>
<DataItem category="SAMPLE" id="n3" name="Xload"
nativeUnits="PERCENT" type="LOAD" units="PERCENT"/> <DataItem
category="CONDITION" id="Xloadc" type="LOAD"/> <DataItem
category="CONDITION" id="Xsystem" type="SYSTEM"/>
</DataItems>
```

– Xact ist die erstellte Variable in MindSphere, z. B. "VariableA".

– Passen Sie folgende Zeile an:

```
<DataItem category="SAMPLE" id="x2" name="Xact"
nativeUnits="MILLIMETER" subType="ACTUAL" type="POSITION"
units="MILLIMETER"/>
```

Ändern Sie id="x2" in id="VariableA"

8. Führen Sie am PC einen Neustart aus, damit die Konfiguration neu geladen wird.

Variable für Vorschubkorrektur

1. Prüfen Sie, ob Ihre Steuerung diese Art von Variablen an MindSphere sendet.
2. Prüfen Sie die Konfiguration im MTConnect Agent.
Im Beispiel sehen Sie folgenden Dateninhalt:

```
<DataItems>
<DataItem category="EVENT" id="path2_execution" name="p2_execution"
 type="EXECUTION"/>
<DataItem category="EVENT" id="path2_dry_run" name="p2_dry_run" subType="DRY_RUN"
 type="CONTROLLER_MODE_OVERRIDE"/>
<DataItem category="EVENT" id="path2_single_block" name="p2_single_block"
 subType="SINGLE_BLOCK" type="CONTROLLER_MODE_OVERRIDE"/>
<DataItem category="EVENT" id="path2_axis_lock" name="p2_axis_lock"
 subType="MACHINE_AXIS_LOCK" type="CONTROLLER_MODE_OVERRIDE"/>
<DataItem category="EVENT" id="path2_optional_stop" name="p2_optional_stop"
 subType="OPTIONAL_STOP" type="CONTROLLER_MODE_OVERRIDE"/>
<DataItem category="EVENT" id="path2_toolid" name="p2_tool_id" type="TOOL_ASSET_ID"/>
<DataItem category="EVENT" id="path2_part_count" name="p2_part_count"
 type="PART_COUNT"/>
<DataItem category="EVENT" id="path2_active_axes" name="p2_active_axes"
 type="ACTIVE_AXES"/>
<DataItem category="EVENT" id="path2_program" name="p2_program" type="PROGRAM"/>
<DataItem category="EVENT" id="path2_message" name="p2_message" type="MESSAGE"/>
<DataItem category="EVENT" id="path2_feedrate_ovr" name="p2_feedrate_override"
 nativeUnits="PERCENT" subType="PROGRAMMED" type="PATH_FEEDRATE_OVERRIDE"
 units="PERCENT"/>
<DataItem category="EVENT" id="path2_rapid_ovr" name="p2_rapid_override"
 nativeUnits="PERCENT" subType="RAPID" type="PATH_FEEDRATE_OVERRIDE"
 units="PERCENT"/>
<DataItem category="EVENT" id="path2_spindle_ovr" name="p2_spindle_override"
 nativeUnits="PERCENT" type="ROTARY_VELOCITY_OVERRIDE" units="PERCENT"/>
</DataItems>
```

3. Nachfolgend sehen Sie die Konfiguration von Steuerung und MTConnect: Feedoverride wird über das Element `<DataItem>` gesendet:

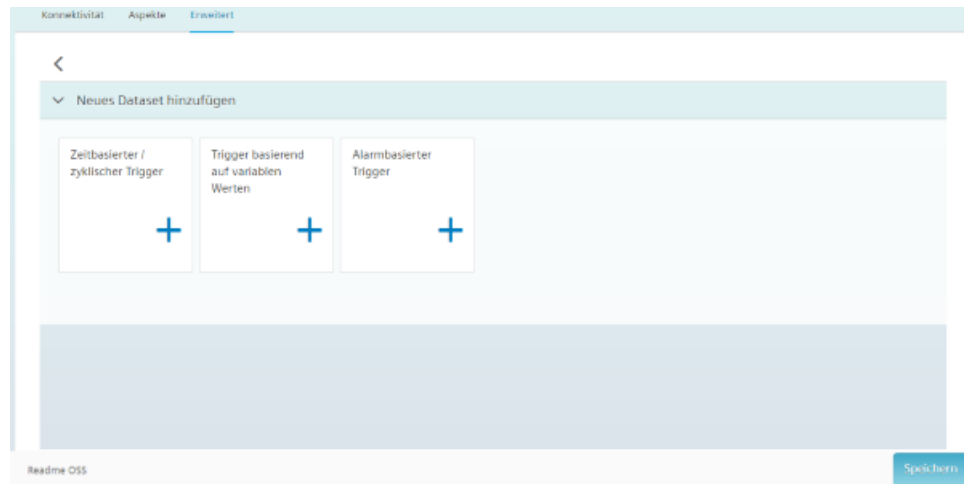
```
<DataItem category="EVENT" id="path2_feedrate_ovr" name="p2_feedrate_override"
 nativeUnits="PERCENT" subType="PROGRAMMED" type="PATH_FEEDRATE_OVERRIDE"
 units="PERCENT"/>
```

4. Kopieren Sie den Inhalt von folgendem ID-Element: `id="path2_feedrate_ovr"`.

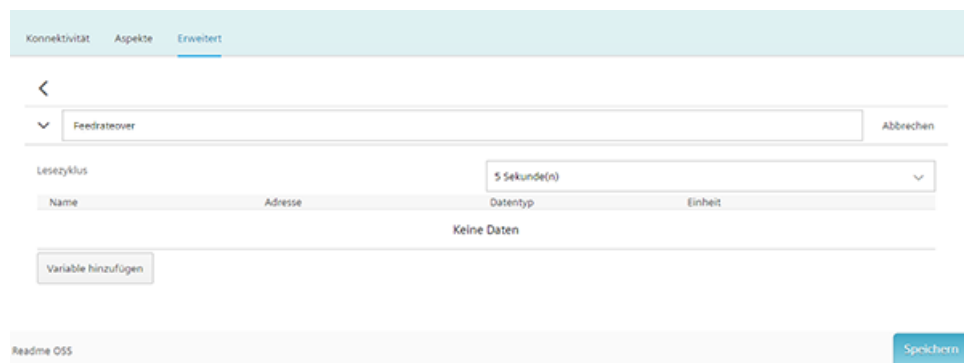
In MindSphere

1. Loggen Sie sich in MindSphere ein.
2. Wählen Sie den Asset-Manager.
3. Öffnen Sie Ihr Asset.

4. Wählen Sie im "MTA Asset Config" das Register "Erweitert".
 - Klicken Sie auf die Schaltfläche "Konfiguration hinzufügen". Die Auswahl der Trigger wird angezeigt.
 - Wählen Sie mit Mausklick den gewünschten Trigger.



5. Wählen Sie, z. B. den zeitbasierten / zyklischen Trigger.
 - Geben Sie den Aspektnamen ein, z. B. "Feedrateover"
 - Wählen Sie den Lesezyklus.
 - Klicken Sie auf die Schaltfläche "Variable hinzufügen".



6. Sie erhalten eine Eingabezeile für die neue Variable. Definieren Sie die Variable, z. B.:
 - Name: FeedRateOver
 - Adresse: path2_feedrate_ovr
 - Datentyp: DOUBLE
 - Einheit: %
7. Klicken Sie auf die Schaltfläche "Speichern".

3.5.10 3rdPartyController deinstallieren

3rdPartyController deinstallieren

Verwenden Sie das Control Panel um den 3rdPartyController zu deinstallieren.

1. Klicken Sie auf die Schaltfläche "Uninstall".
2. Führen Sie einen Neustart durch.

ePS-Client Einstellungsdatei

Führen Sie nach einer Deinstallation des ePS-Clients einen Restore der Einstellungsdatei durch.

Dies verhindert, dass die Maschine den Fanuc Treiber laden will, der nach der Deinstallation des 3rdPartyControllers nicht mehr vorhanden ist.

Fehlerbehandlung

4.1 SINUMERIK Integrate/ePS-Client Log Files

Sie haben die Möglichkeit in der Datei "setting.ini" den Log-Level zu erhöhen.

Sie finden die Log-Files vom SINUMERIK Integrate-/ePS-Client in folgendem Verzeichnis:

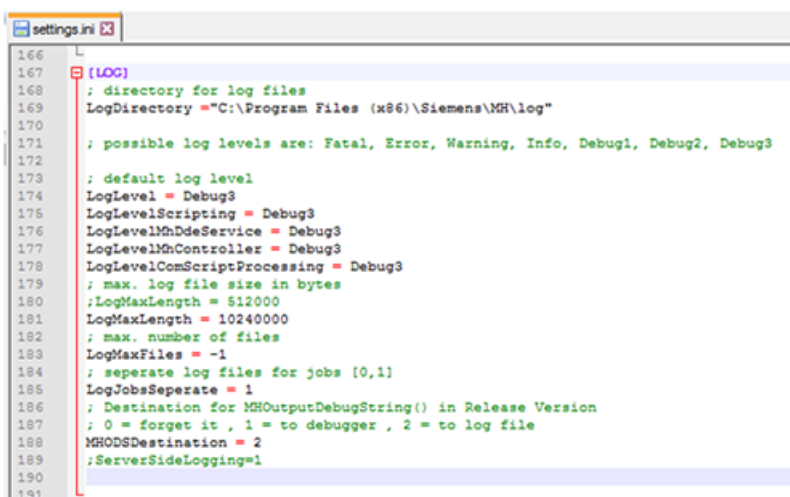
C:\Program Files (x86)\Siemens\MH\log\

- ODER -

C:\Users\YourUserName\AppData\Local\VirtualStore\Program Files (x86)\Siemens\MH\log\

Vorgehensweise

1. Öffnen Sie die Datei "settings.ini".
2. Suchen Sie den Bereich [LOG].
3. Setzen Sie Log-Level "Debug3".
Der Standard Log-Level ist "Error".
4. Starten Sie den Client neu, um die Änderungen zu aktivieren.

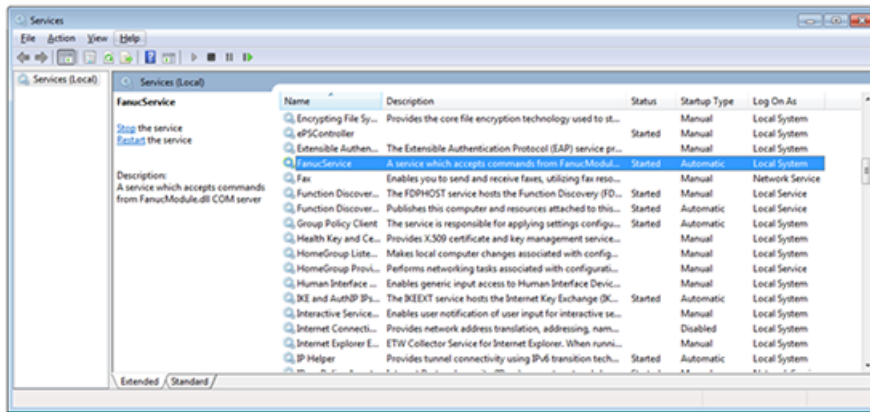


```
166 L
167 [LOG]
168 ; directory for log files
169 LogDirectory = "C:\Program Files (x86)\Siemens\MH\log"
170
171 ; possible log levels are: Fatal, Error, Warning, Info, Debug1, Debug2, Debug3
172
173 ; default log level
174 LogLevel = Debug3
175 LogLevelScripting = Debug3
176 LogLevelMhDdeService = Debug3
177 LogLevelMhController = Debug3
178 LogLevelComScriptProcessing = Debug3
179 ; max. log file size in bytes
180 ;LogMaxLength = 512000
181 LogMaxLength = 10240000
182 ; max. number of files
183 LogMaxFiles = -1
184 ; separate log files for jobs {0,1}
185 LogJobsSeperate = 1
186 ; Destination for MHOutputDebugString() in Release Version
187 ; 0 = forget it , 1 = to debugger , 2 = to log file
188 MHODSDestination = 2
189 ;ServerSideLogging=1
190
191
```

4.2 FanucModule Service und Logs

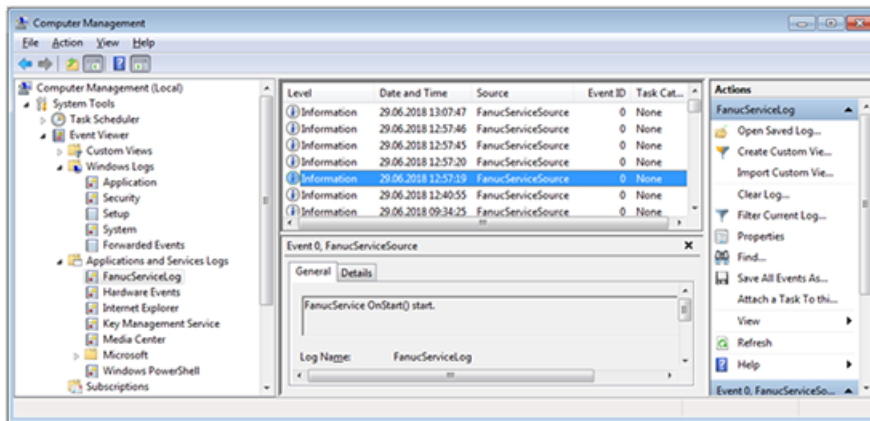
Voraussetzung

- Prüfen Sie, ob "FanucModule" korrekt installiert wurde.
- Prüfen Sie, ob der Windows Service "FanucService" installiert ist und gestartet wurde.



FanucService Logs

"FanucService Logs" werden in das Windows EventLog geschrieben:



FanucModule Logs

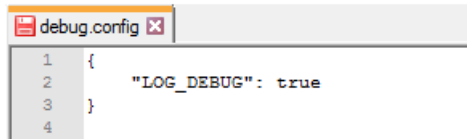
"FanucModule Logs" liegen in folgendem Verzeichnis:

C:\ProgramData\Siemens\Fanuclogs

- ODER -

C:\Users\YourUserName\AppData\Local\VirtualStore\ProgramData\Siemens\Fanuclogs

Der Log-Level des FanucModule passen Sie unter obigem Verzeichnis in der Datei "debug.config" an.
Mögliche Werte sind "true" oder "false":



```
1 {  
2   "LOG_DEBUG": true  
3 }  
4
```

Fanuc Informations Logs

Üblicherweise werden Logs nur geschrieben, wenn ein Fehler auftritt. Wenn Sie Informationslogs benötigen, muss die Datei "JSON" geändert werden.

Geben Sie folgende Zeilen ein:

```
{  
"LOG_FILE_SIZE": 1048576,  
"LOG_LEVEL": 5,  
"SEPARATE_ERROR": true  
}
```

Folgende Loglevel stehen zur Verfügung:

- 0 - Information
- 1 - Fehler
- 2 - Warnungen
- 3 - Debug1
- 4 - Debug2
- 5 - Debug3

Nachdem Sie die Änderungen durchgeführt haben, ist ein Neustart erforderlich.

4.3 Alarmmeldung

Alarm: Bootscript wurde nicht gefunden

Kontrollieren Sie die Verbindungseinstellungen:

- Prüfen Sie die URL.
Wenn Sie die Adresse ändern, starten Sie die Installationsdatei erneut und passen Sie die URL an.
- Prüfen Sie die Funktionalität von TLS1.2 – Kommunikation zwischen Proxy und MindSphere.
- Wenn sich die Maschine nicht mit der MindSphere verbindet, prüfen Sie den Ablageort der Datei "onboard.key". Das richtige Verzeichnis ist: F:\tmp\boot_job

Anhang

A.1 Liste der Abkürzungen

Admin	Administrator (Benutzerrolle)
AMM /C	Analyse MyMachine /Condition
CNC	Computerized Numerical Control: Computerunterstützte numerische Steuerung
COM	Communication
DIR	Directory: Verzeichnis
FAQ	Frequently Asked Questions
h	Stunde
HTTP	Hypertext Transfer Protocol, Hypertext-Übertragungsprotokoll
HTTPS	HyperText Transfer Protocol Secure, Sicheres Hypertext-Übertragungsprotokoll
IB	Inbetriebnehmer (Benutzerrolle)
ID	Identifikationsnummer
IE	Internet Explorer
IFC	Interface Client
IoT	Internet of Things
IPC	Industrie-PC
MB	Megabyte
MFA	Multi Factor Authentication
MLFB	Maschinenlesbare Fabrikatbezeichnung
MMM	Manage MyMachines
MMM /R	Manage MyMachines /Remote
MO	Maschinenbediener
MSTT	Maschinensteuertafel
NC	Numerical Control: Numerische Steuerung
NCU	Numerical Control Unit: Hardware Einheit des NC
OEM	Original Equipment Manufacturer
OP	Operation Panel: Bedieneinrichtung
PC	Personal Computer
PCU	PC Unit: Rechneinheit
PLC	Programmable Logic Control: speicherprogrammierbare Steuerung
SE	Service-Ingenieur
SI	SINUMERIK Integrate
SK	Softkey
SW	Software
URL	Uniform Resource Locator, einheitlicher Ressourcenzeiger
UTC	Universal Time Coordinated, koordinierte Weltzeit

Index

3

3rdPartyController
Deinstallieren, 116
Installieren, 99

A

Alarmer, 108
Anbinden
 IoT204, 33
 X1 P1 mit fester Adresse, 33
 X2 P1 mit DHCP, 33
Apache APR
 Installieren, 37
 Kompilieren, 37
Apache APR-util
 Installieren, 37
 Kompilieren, 37
Apache http konfigurieren, 39
Apache HTTP Server
 Autostart, 38
 Kompilieren und installieren, 38
 Starten und stoppen, 38
Apache httpd
 Downloadpakete, 35

D

Deaktivieren
 Login mit Benutzernamen, 86

E

Export - Konfigurationsdateien, 43

F

FanucModule
 Einbinden, 101
 Konfigurieren, 105

H

Hardware einrichten, 27

Hinzufügen, 115
HMI-Advanced Installation, 15
httpd.conf, 43

I

installation
 SIMATIC IoT2040, 27
Installation, 23
 Mit MindSphere verbinden, 26
Installation HMI-Advanced, 15
Installieren
 Apache APR, 37
 Apache APR_util, 37
 Apache HTTP Server, 38
 opkg, 37
 pcre, 37
 SINUMERIK Integrate Client, 89
IoT2000 SD-Karte installieren, 27
IoT2040
 Anbindung Private Key, 86
IoT2040
 Anbinden, 33

K

Kompilieren
 Apache APR, 37
 Apache APR-util, 37
 Apache HTTP Server, 38
Konfigurationsdateien
 Export, 43
Konfigurieren
 Apache http, 39
 Proxy, 79

M

MindSphere Verbindung, 26
MTConnect
 Einbinden, 102
 Konfigurieren, 106

N

Netz Konfiguration, 31

Netz-Konfiguration

Ändern, 32

O

opkg installieren, 37

P

Passwort, 33

Private Key

Anbindung an lot2040, 86

Putty Format, 83

Proxy konfigurieren, 79

Proxy Verbindung, 33

S

SIMATIC IoT2040, 27

Hardware einrichten, 27

SINUMERIK Integrate Client installieren, 89

SINUMERIK Operate, 23

SINUMERIK Operate Installation, 23

SSH Schlüsselpaare generieren, 82

SSL-Verbindung - Zertifikat, 39

Steuerung mit Mindsphere verbinden, 26

Systemvoraussetzung, 12

U

Übersicht, 27

User Name, 33

V

Variable, 108, 115

Einbinden, 111

Voraussetzung, 12

Voraussetzung FanucModule, 88

X

X1 P1

Anbinden mit fester Adresse, 33

X2 P1

Anbinden mit DHCP, 33

Z

Zertifikat

SSL-Verbindung, 39