

SINUMERIK

MindSphere Manage MyMachines /Remote - Installation in bestehende Steuerungsumgebungen

Anwendungsbeispiele

Vorwort

Grundlegende
Sicherheitshinweise **1**

Einleitung **2**

Installation/Konfiguration **3**

Anhang **A**

Gültig für Steuerung:
SINUMERIK 840D pl/ 840D sl/840DE sl


Software
HMI-Advanced, Version 6.4/7.6
SINUMERIK Operate, Version 2.7.3.10
Manage MyMachines /Remote, Version 01.03.00.00


03/2020
A5E45211403A AC


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 das Produkt "Manage MyMachines /Remote" bedeutet dies:

Informationen über Zeitraum und Teilnehmer an Fernzugriffssitzungen.

Das Produkt verarbeitet / speichert folgende personenbezogene Daten:

Es handelt sich nicht um Daten der Privat- oder Intimsphäre.

Die o. g. Daten werden für die Auswertung von Sitzungsinformationen benötigt. Die Speicherung der Daten ist zweckmäßig und auf das Notwendigste beschränkt, da diese zur Identifizierung der durchgeführten Sitzungen und deren Teilnehmer und zur weitergehenden Verrechnung zwischen Diensterbringer (OEM) und Endkunde unerlässlich sind.

Die o. g. Daten können nicht anonymisiert gespeichert werden, da der Zweck der Identifizierung des Bedienpersonals sonst nicht erreicht werden kann.

Wenn notwendig, können diese Sitzungsinformationen gelöscht werden. Dafür wenden Sie sich an den Kundensupport.

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".

Inhaltsverzeichnis

	Vorwort	3
1	Grundlegende Sicherheitshinweise	9
1.1	Allgemeine Sicherheitshinweise.....	9
1.2	Gewährleistung und Haftung für Applikationsbeispiele.....	10
1.3	Security-Hinweise	11
2	Einleitung.....	13
2.1	Übersicht.....	13
2.2	Systemvoraussetzungen.....	14
3	Installation/Konfiguration	19
3.1	SINUMERIK-Steuerung mit HMI-Advanced - SINUMERIK Integrate installieren	19
3.2	SINUMERIK-Steuerung mit SINUMERIK Operate - Proxy einstellen.....	26
3.3	SINUMERIK Integrate Client-Update über Remote-Zugriff mittels AMM (Linux).....	29
3.4	SINUMERIK Integrate Client-Update über Remote-Zugriff mittels AMM (Windows).....	32
3.5	Service Client Manage MyMachines /Remote unter Windows XP installieren	35
3.6	Service Client Manage MyMachines /Remote unter Windows XP nutzen.....	41
A	Anhang	45
A.1	Liste der Abkürzungen	45

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.

- 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.

- 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 SINUMERIK Powerline Steuerungen mit der Bedien-Software HMI-Advanced und SINUMERIK Operate mit der Applikation "Manage MyMachines /Remote" verbinden.

Die nachfolgende Beschreibung bezieht sich auf die Komponenten, die in folgendem Kapitel aufgeführt sind: Systemvoraussetzungen (Seite 14).

2.2 Systemvoraussetzungen

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

Voraussetzung

Für die Verbindung mit MindSphere benötigen Sie die aktuelle Version des SINUMERIK Integrate-Client und Service Client für Manage MyMachines /Remote. 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.

Bedien-Software und Hardware

Die nachfolgende Vorgehensweise ist beispielhaft mit folgenden Komponenten erstellt:

Tabelle 2-1 SINUMERIK 840D pl

Bedien-Software Version	SINUMERIK Integrate Client Software Version	Hardware Version	Betriebssystem
HMI-Advanced ^{*)} ^{***)} V06.04 V07.06	04.12.00.21 04.13.00.36	PCU 50.3B	WinXP SP3
SINUMERIK Operate ^{*)} ^{***)} V02.07.03.10			
FANUC 31i ^{**)}			Windows 7 Standard Embedded

- ^{*)} Die Verbindung erfüllt nicht die sicherheitstechnischen Anforderungen. Die Funktionalität wird garantiert, ist aber nicht Bestandteil der Produktfreigabe. Sie müssen eigenverantwortlich zusätzliche Sicherheitsmaßnahmen umsetzen.
- ^{**)} Für den SINUMERIK Integrate-Client ist der zusätzlicher Treiber "FANUCdriver 1.0" erforderlich. Die Funktionalität wird garantiert, ist aber nicht Bestandteil der Produktfreigabe. Die Anbindung ist nur über den IPC-Client auf dem IPC möglich, nicht über den in SINUMERIK Operate integrierten SINUMERIK Integrate-Client.
- ^{***)} Nur PCU

Hinweis

SINUMERIK Integrate Applikationen

Eine parallele Bearbeitung mit SINUMERIK Integrate Anwendungen ist nicht möglich.

Industrie-PC / 3rdPartyController

Prozessor	1-GHz Prozessor
RAM (GB)	4
Freier Plattenplatz (GB)	1
Betriebssysteme	Windows 7 SP1 (x64) Professional/Enterprise/Ultimate Windows 7 Standard Embedded Windows 10 (x64) Pro/Enterprise
Bildschirmauflösung	Mindestens 1980 x 1080

Hinweis**Nur eine VNC-Verbindung möglich**

Zur SINUMERIK-Steuerung ist nur eine VNC-Viewer-Verbindung zulässig.

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 Bestandteil des Produkts. 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 (Service-Ingenieur-Seite)

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 /Remote beim Maschinenbediener oder Endkunden verwendet werden.

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

Hinweis

Sicherung der SINUMERIK-Steuerung (Maschinenbediener-Seite)

Die notwendigen Sicherheitsmaßnahmen (z. B. Virusscanner, Firewalls, Betriebssystem Patching usw.) müssen auf den SINUMERIK-Steuerungen implementiert sein.

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

ACHTUNG

Missbrauch von Daten

Achten Sie beim Speichern Ihrer Daten - insbesondere bei vertraulichen Daten - unbedingt auf eine sichere Datenablage. Legen Sie diese Daten verschlüsselt lokal oder verschlüsselt auf dem Netzwerk ab. Tragen Sie dafür Sorge, dass diese Daten unbefugten Personen nicht zugänglich sind.

Das betrifft u. a. folgende Daten:

- Archiv-Dateien
- Image-Dateien
- Projekt-Dateien
- Trace-Dateien
- Safety-relevante Daten

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

ACHTUNG

Datenmanipulation möglich

Es besteht das Risiko, dass sich ein Angreifer innerhalb des Netzwerks Zugriff auf den Bedien-PC verschafft. Dort kann der Angreifer verschiedene Systembestandteile (z. B. Datenbankinhalte) lesen bzw. manipulieren. Dadurch kann der Angreifer, z. B. Werkzeugdaten, NC-Programme, Maschinenarchive oder die Anlagenstruktur verändern. Diese Form des Angriffs kann durch Manage MyMachines /Remote nicht unterbunden werden.

- Treffen Sie als Betreiber des Maschinennetzes Maßnahmen für die Industrial Security des Produktions-/Maschinennetzwerks.

Die Siemens AG übernimmt hierfür keine Haftung!

Hinweis**Erhobene Daten speichern**

Das Produkt "Manage MyMachines Remote" wurde von Siemens auch unter Berücksichtigung des Privacy By Design Grundsatzes entwickelt. Das bedeutet, dass es der Dienstbringer (OEM) selbst in der Hand hat zu entscheiden, wie lange die im Rahmen der Nutzung erhobenen Daten, wie Informationen über Zeitraum und Teilnahme an Fernzugriffssitzungen, gespeichert werden.

Lieferform

Der SINUMERIK Integrate Client, der Service Client für Manage MyMachines /Remote 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.

Weiterführende Literatur

- Weitere Informationen zur Bedien-Software "SINUMERIK Operate" finden Sie in folgender Literatur:
Inbetriebnahmehandbuch SINUMERIK Operate (IM9)
- Weitere Informationen zu "SINUMERIK Integrate" finden Sie in folgender Literatur:
Inbetriebnahmehandbuch SINUMERIK Integrate MMP, MMT, AMC, AMP, AMM/E, AMD

Weitere Informationen zu den Applikationen von MindSphere finden Sie unter folgenden Links:

MindSphere (<https://support.industry.siemens.com/cs/de/en/view/109742256>)

MindSphere-Dokumentation (<https://documentation.mindsphere.io/index.html#/kiosk/de>)

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 Fabriknetzwerkumgebung nicht angegriffen werden kann.

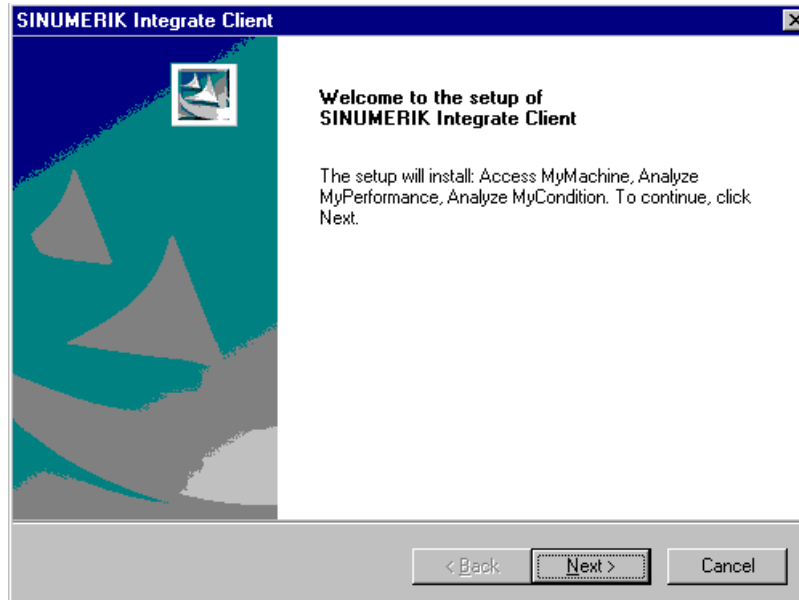
Dabei müssen die Richtlinien der kundenseitigen IT-Abteilung berücksichtigt werden.

Installation/Konfiguration

3.1 SINUMERIK-Steuerung mit HMI-Advanced - SINUMERIK Integrate installieren

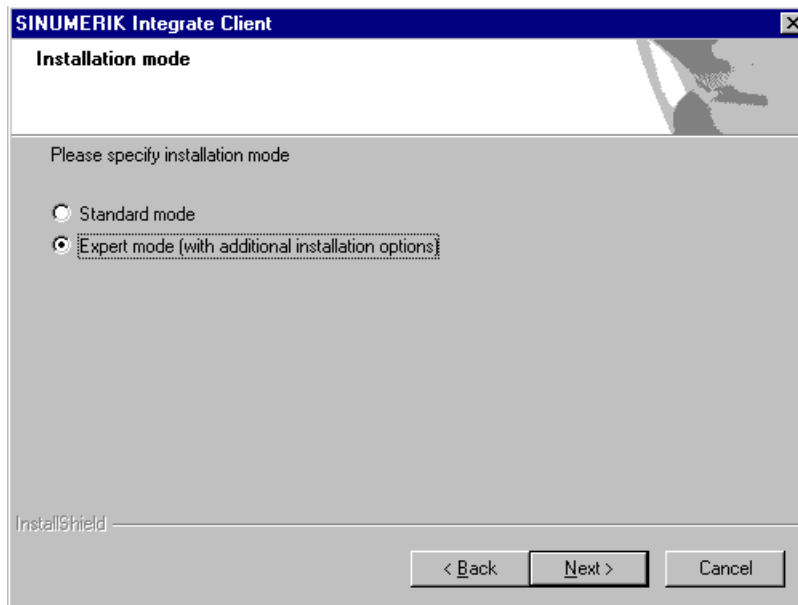
Vorgehensweise

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.

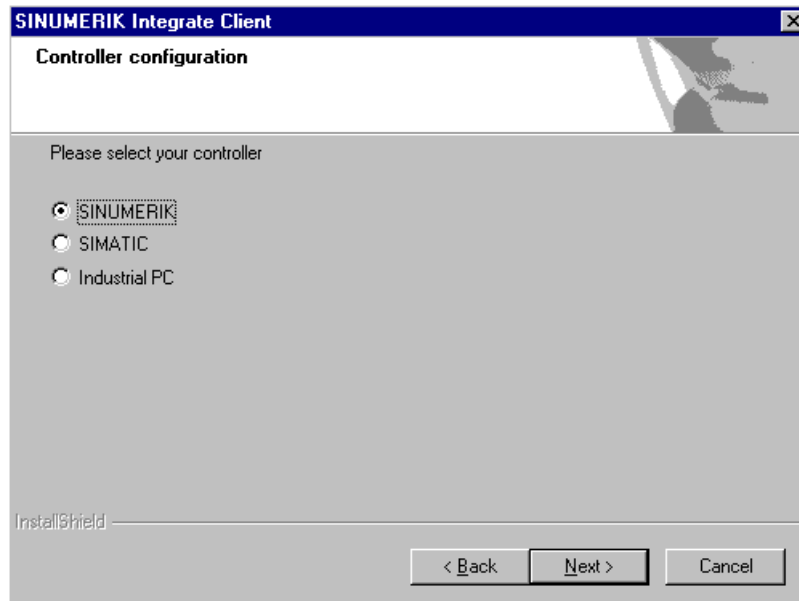


3.1 SINUMERIK-Steuerung mit HMI-Advanced - SINUMERIK Integrate installieren

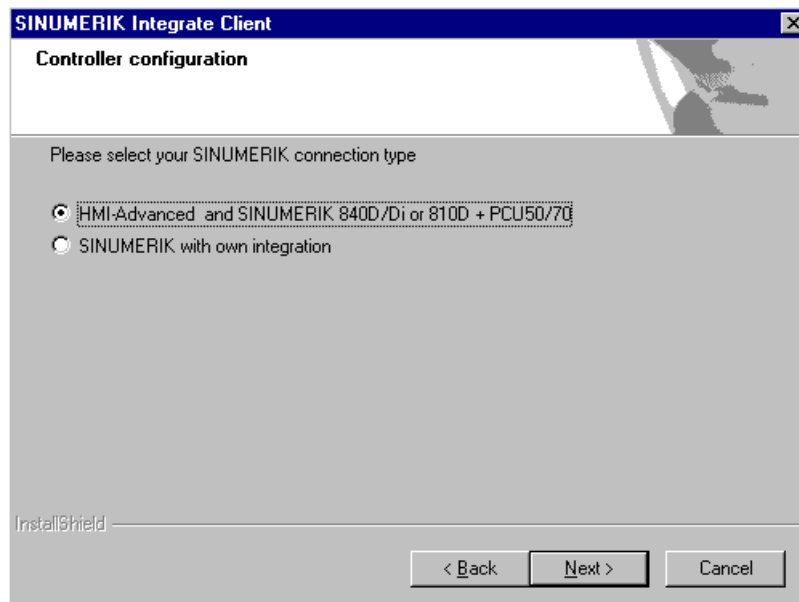
5. Das Fenster "License Agreement" wird geöffnet.
Lesen Sie die Lizenzvereinbarung.
 - Wenn Sie sich die Bedingungen ausdrucken möchten, klicken Sie auf die Schaltfläche "Print".
 - Aktivieren Sie anschließend das Optionsfeld "I accept the terms of the license agreement" und klicken Sie auf die Schaltfläche "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. Wählen Sie Ihren Controller.
 - Aktivieren Sie, z. B. das Optionsfeld "SINUMERIK".
 - Klicken Sie auf die Schaltfläche "Next >".

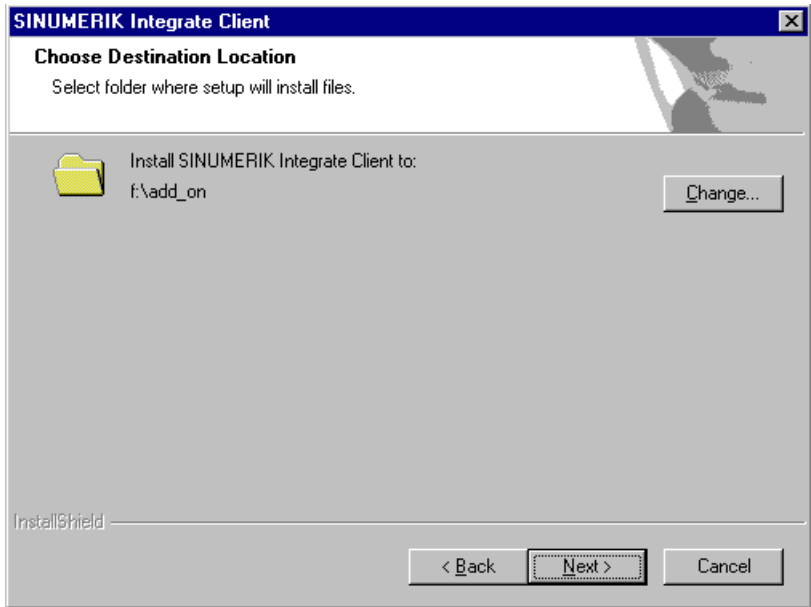


8. Wählen Sie im Fenster "Controller configuration" nun den SINUMERIK-Anschlusstyp.
 - Aktivieren Sie das Optionsfeld "HMI-Advanced and SINUMERIK 840D/Di or 810D + PCU50/70".
 - Klicken Sie auf die Schaltfläche "Next >".

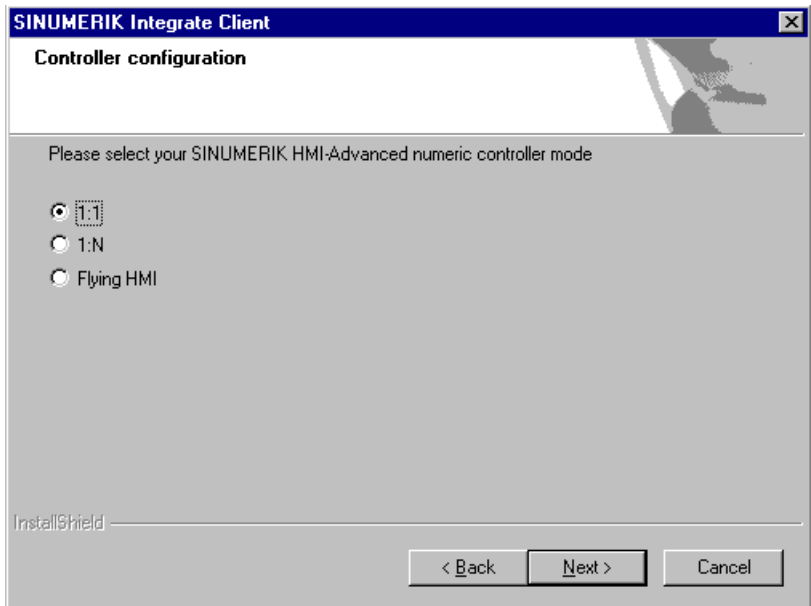


3.1 SINUMERIK-Steuerung mit HMI-Advanced - SINUMERIK Integrate installieren

- 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...".

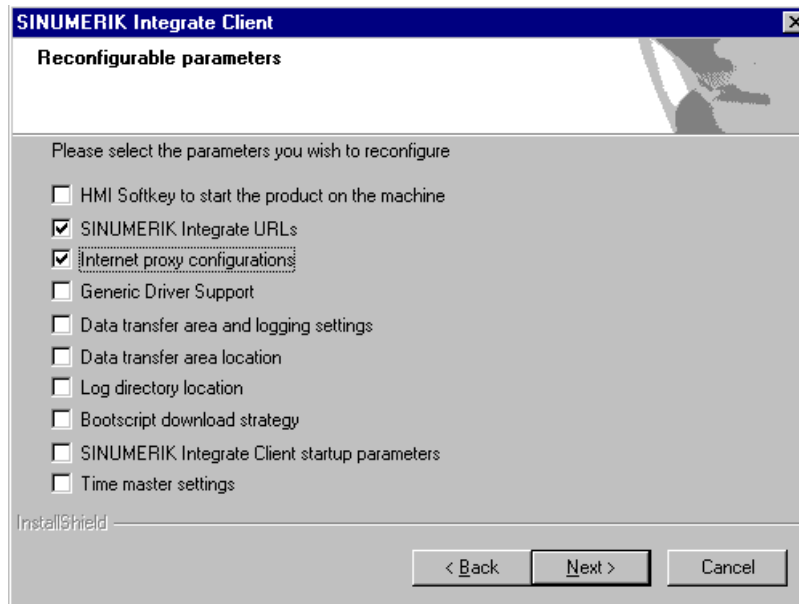


- 10. Das Fenster "Controller configuration" wird geöffnet.
 - Aktivieren Sie das Optionsfeld der Verbindung "1:1".
 - Klicken Sie anschließend auf die Schaltfläche "Next >".



11. Das Fenster "Reconfigurable parameters" wird geöffnet.

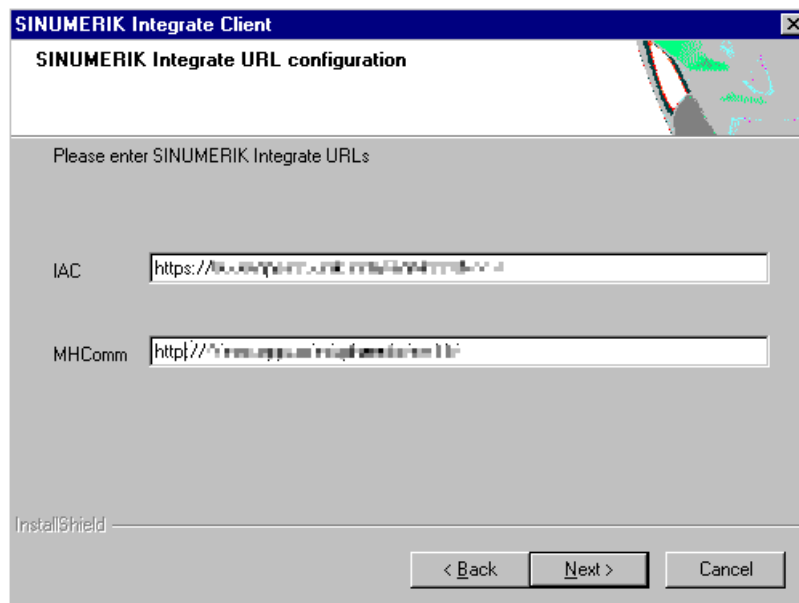
- Aktivieren Sie das Optionskästchen "SINUMERIK Integrate URLs" und "Internet proxy configurations".
- Klicken Sie auf die Schaltfläche "Next >".



12. Das Fenster "SINUMERIK Integrate URL configuration" wird geöffnet.

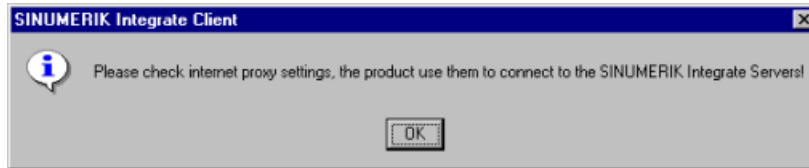
Der Proxy-Server wird für die Verbindung der Steuerung mit der MindSphere benötigt.

- Tragen Sie im Eingabefeld "MHComm" folgende Webservice URL für das MindSphere V3 Livesystem ein:
<https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/v3/ws11>
- Klicken Sie auf die Schaltfläche "Next >".

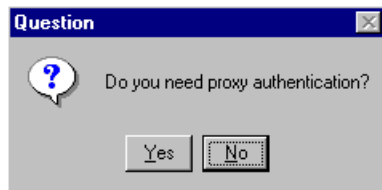


3.1 SINUMERIK-Steuerung mit HMI-Advanced - SINUMERIK Integrate installieren

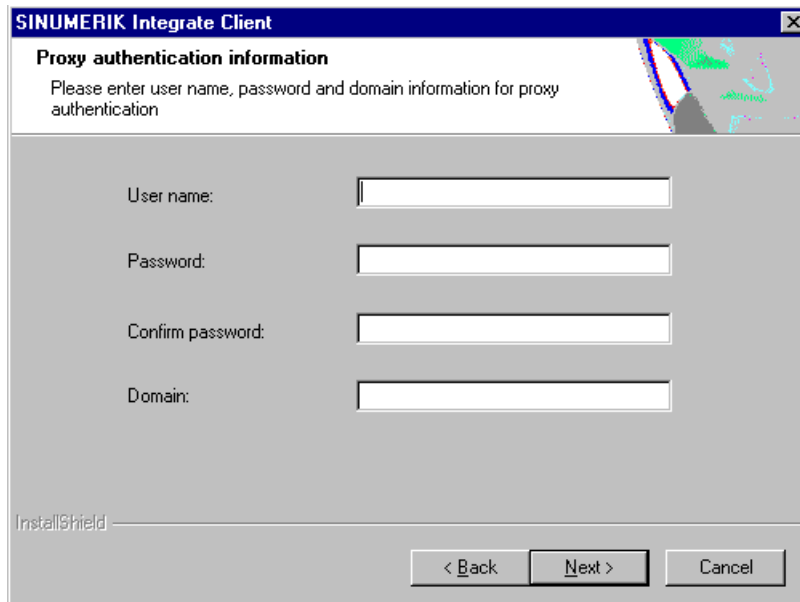
- 13. Folgende Meldung wird angezeigt: "Please check internet proxy settings, the product use them to connect to the SINUMERIK Integrate Servers!"
 - Klicken Sie auf die Schaltfläche "OK", um den Proxy-Server anzupassen.



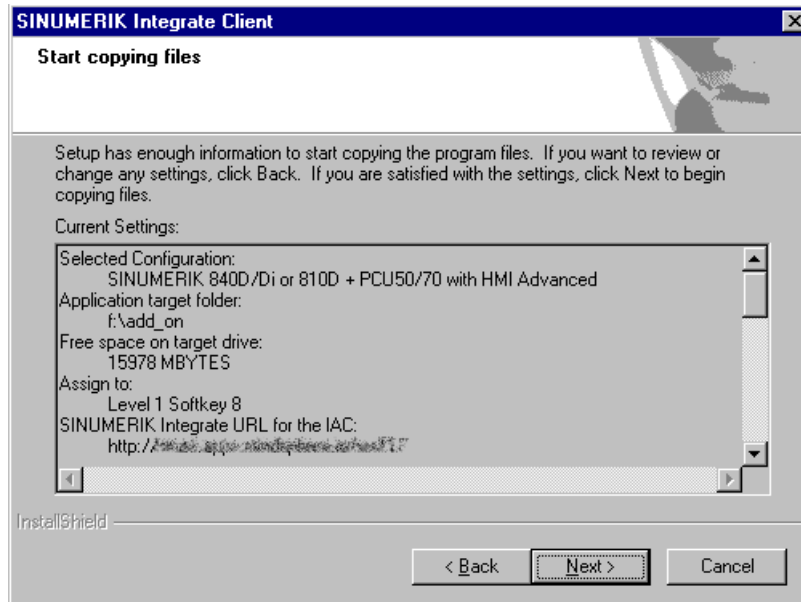
- 14. Das Fenster "Question" wird mit folgender Frage angezeigt: "Do you need proxy authentication?"
 - Wenn eine Authentifizierung für den Proxy benötigt wird, klicken Sie auf die Schaltfläche "Yes".



- 15. Das Fenster "SINUMERIK authentication information" wird angezeigt. Tragen Sie die Daten in die Eingabefelder:
 - User name:
 - Passwort:
 - Confirm passwort:
 - Domain:
 - 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. Nach erfolgter Installation, erhalten Sie die Meldung einen Neustart auszuführen. Klicken Sie dazu auf die Schaltfläche "OK".

3.2 SINUMERIK-Steuerung mit SINUMERIK Operate - Proxy einstellen

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.

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, z. B. für das MindSphere V3 Livesystem ein:
https://gateway.eu1.mindsphere.io/api/agentcom-mmmops/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 the following settings:

- Verzeichnis: User (selected in a dropdown menu)
- Anzeige Homepage: hier überschreiben
- RenderService: hier überschreiben
- Webservice URL: hier überschreiben
http://wslmac.apps.mindsphere.io/ws11
- Sende Timeout in ms: 20 hier überschreiben
- Empfang Timeout in ms: 20 hier überschreiben

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>".
Die hinterlegten Einstellungen werden 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:

automatik 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:

Workstation:

hier überschreiben

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

3.3 SINUMERIK Integrate Client-Update über Remote-Zugriff mittels AMM (Linux)

Um die Migration vom Produkt "Access MyMachines/Ethernet" auf das Produkt "Manage MyMachines /Remote" zu ermöglichen, sind folgende Schritte notwendig.

1. Löschen des vorhandenen SINUMERIK Integrate-Client
2. Übertragen des neuen SINUMERIK Integrate-Client
3. Power-On an der SINUMERIK-Steuerung

Softwareversionen

Im beschriebenen Beispiel wurde der SINUMERIK Integrate-Client im Softwarestand V4.7 SP2 HF4 auf den Stand V03.00.06 aktualisiert.

Diese Vorgehensweise lässt sich bei folgenden Softwareständen anwenden:

- In der Softwarelinie V4.5 ab Softwarestand V4.5 SP6 (Client größer V02.00.06)
- In der Softwarelinie V4.7 ab Softwarestand V4.7 SP2 HF1 (Client größer V03.00.06)

Nach dem gleichen Verfahren können auch andere Softwarestände aktualisiert werden. Allerdings besteht keine Garantie, dass die Vorgehensweise für jede Konfiguration innerhalb der Systemvoraussetzungen möglich ist.

Voraussetzung

- Die Systemzeit der SINUMERIK-Steuerung zeigt das aktuelle Datum.
- SINUMERIK Integrate Package V4.1 SP5
- Die Funktionalität und Bedienung von AMM/Ethernet und dessen Filetransfer-Funktionalität ist bekannt.
- Eine Verbindung zum Zielsystem wurde mittels AMM/Ethernet aufgebaut.
- Filetransfer ist aktiviert und sämtliche Zustimmungen seitens des Maschinenbedieners zum Übertragen einer Datei sind vorhanden.

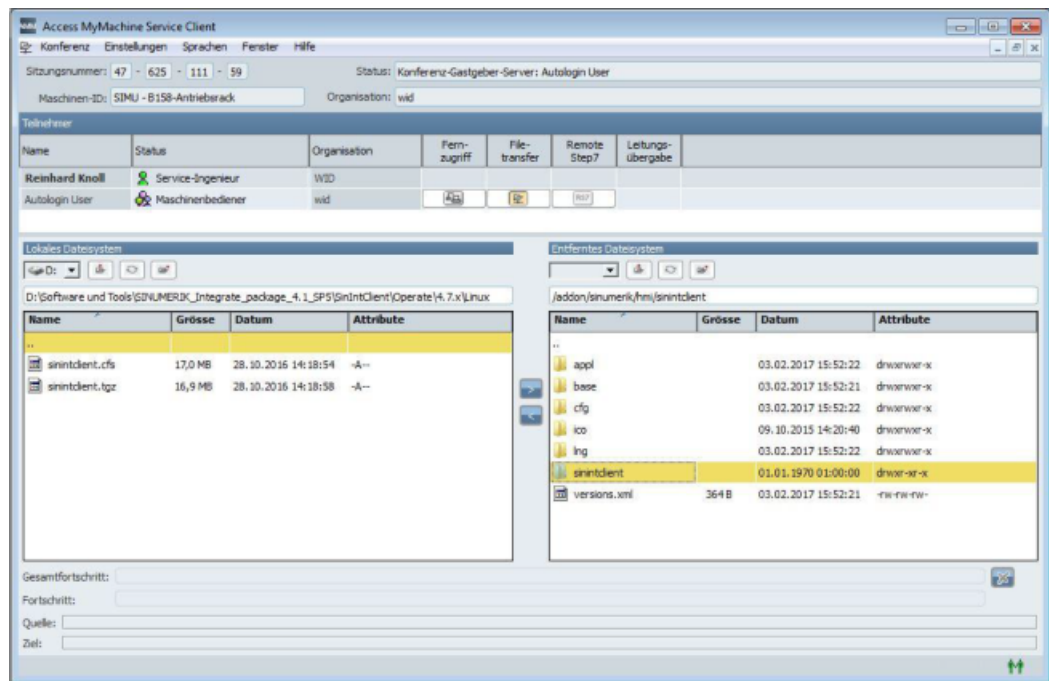
Löschen des vorhandenen SINUMERIK Integrate-Client

Damit der SINUMERIK Integrate-Client ersetzt werden kann, muss die Datei "sinintclient.cfs" auf der SINUMERIK-Steuerung gelöscht werden.

1. Navigieren Sie im entfernten Dateisystem in das Zielverzeichnis auf der CF-Card: /addon/sinumerik/hmi/sinintclient.
2. Wählen Sie die Datei "sinintclient.cfs".

3.3 SINUMERIK Integrate Client-Update über Remote-Zugriff mittels AMM (Linux)

3. Löschen Sie die Datei.
4. Bestätigen Sie die Sicherheitsabfrage mit "Ja".



Übertragen des neuen SINUMERIK Integrate-Client

Der SINUMERIK Integrate-Client aus dem SINUMERIK Integrate Package wird direkt in das Zielverzeichnis auf der SINUMERIK-Steuerung kopiert.

1. Navigieren Sie im lokalen Dateisystem in das Quellverzeichnis, z. B.:
SINUMERIK_Integrate_package_V04.01.05.00/SinIntClient/Operate/4.7.x/Linux/.
2. Wählen Sie die Datei "sinintclient.cfs".
3. Navigieren Sie im entfernten Dateisystem in das Zielverzeichnis auf der CF-Card: /addon/sinumerik/hmi/sinintclient.
4. Klicken Sie auf die Schaltfläche ">", um die Datei auf die SINUMERIK-Steuerung zu übertragen.
Während eines Kopiervorgangs können keine anderen Aktionen vorgenommen werden. Der Vorgang wird Ihnen in einer Fortschrittsanzeige angezeigt.

Aktivieren des SINUMERIK Integrate-Client

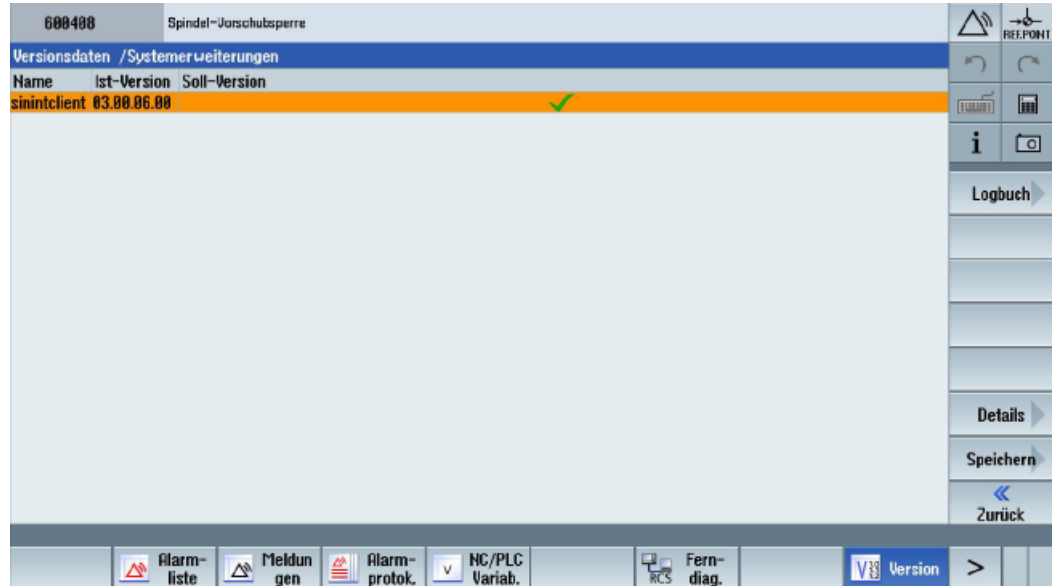
1. Beenden Sie den Fernzugriff an der SINUMERIK-Steuerung.
2. Führen Sie ein Power-On durch.

Hinweis

HMI-Neustart ist nicht ausreichend!

3.3 SINUMERIK Integrate Client-Update über Remote-Zugriff mittels AMM (Linux)

3. Treten Sie der Remote Session wieder bei.
4. Öffnen Sie den Bedienbereich Diagnose.
Prüfen Sie die Version des SINUMERIK Integrate-Client unter "/Version/
Systemerweiterungen".



- ODER -

Prüfen Sie die Version des SINUMERIK Integrate-Client im Dateisystem der CF-Card.
Öffnen Sie die Datei "version.xml" im Verzeichnis: /addon/sinumerik/hmi/sinintclient.

3.4 SINUMERIK Integrate Client-Update über Remote-Zugriff mittels AMM (Windows)

Um die Migration vom Produkt "Access MyMachines/Ethernet" auf das Produkt "Manage MyMachines /Remote" zu ermöglichen, sind folgende Schritte notwendig.

1. Übertragen des neuen SINUMERIK Integrate-Client
2. Client-Update und Power-On an der SINUMERIK-Steuerung

Softwareversionen

Im beschriebenen Beispiel wurde der SINUMERIK Integrate-Client im Softwarestand V4.7 SP2 HF4 auf den Stand V03.00.15 aktualisiert.

Diese Vorgehensweise lässt sich bei folgenden Softwareständen anwenden:

- In der Softwarelinie V4.5 ab Softwarestand V4.5 SP6 (Client größer V02.00.06)
- In der Softwarelinie V4.7 ab Softwarestand V4.7 SP2 HF1 (Client größer V03.00.06)

Nach dem gleichen Verfahren können auch andere Softwarestände aktualisiert werden. Allerdings besteht keine Garantie, dass die Vorgehensweise für jede Konfiguration innerhalb der Systemvoraussetzungen möglich ist.

Voraussetzung

- Die Systemzeit der SINUMERIK-Steuerung zeigt das aktuelle Datum.
- SINUMERIK Integrate Package V4.1 SP5
- Die Funktionalität und Bedienung von AMM/Ethernet und dessen Filetransfer-Funktionalität ist bekannt.
- Eine Verbindung zum Zielsystem wurde mittels AMM/Ethernet aufgebaut.
- Filetransfer ist aktiviert und sämtliche Zustimmungen seitens des Maschinenbedieners zum Übertragen einer Datei sind vorhanden.
- Zugriffsrechte auf das Zielverzeichnis: Lesen / Schreiben / Ausführen

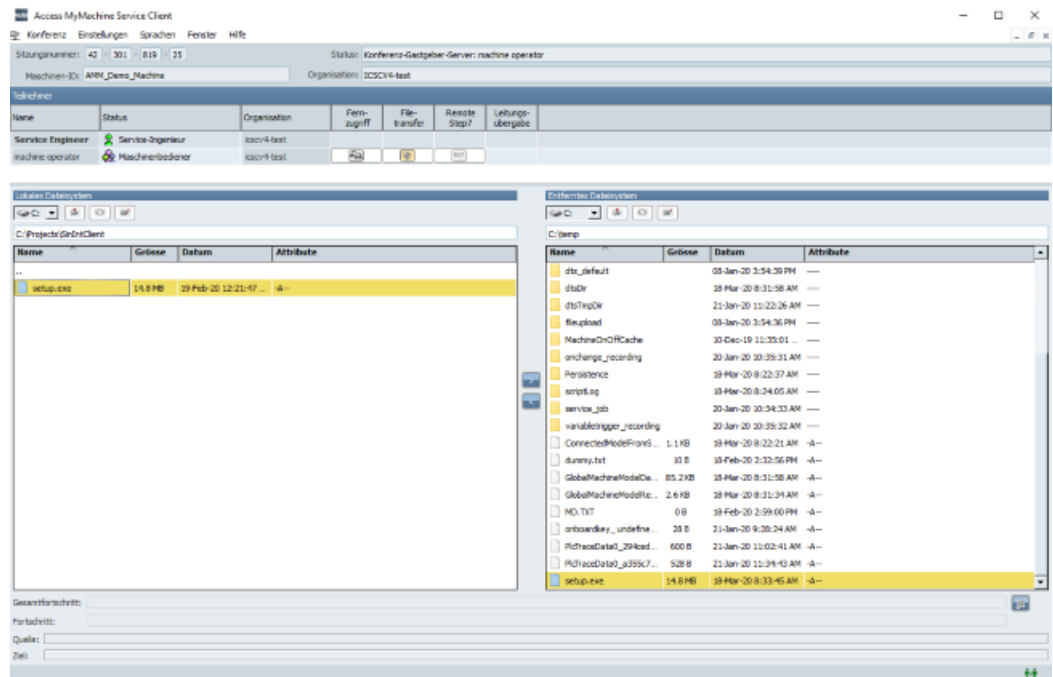
Übertragen des neuen SINUMERIK Integrate-Client

Der SINUMERIK Integrate-Client aus dem SINUMERIK Integrate Package wird direkt in das Zielverzeichnis auf der SINUMERIK-Steuerung kopiert.

1. Navigieren Sie im lokalen Dateisystem in das Quellverzeichnis, z. B.: C:\Projects \SinIntClient.
2. Wählen Sie die Datei "setup.exe".

3.4 SINUMERIK Integrate Client-Update über Remote-Zugriff mittels AMM (Windows)

3. Navigieren Sie im entfernten Dateisystem in das Zielverzeichnis: C:\temp.
4. Klicken Sie auf die Schaltfläche ">", um die Datei auf die SINUMERIK-Steuerung zu übertragen.
Während eines Kopiervorgangs können keine anderen Aktionen vorgenommen werden. Der Vorgang wird Ihnen in einer Fortschrittsanzeige angezeigt.



Aktivieren des SINUMERIK Integrate-Client

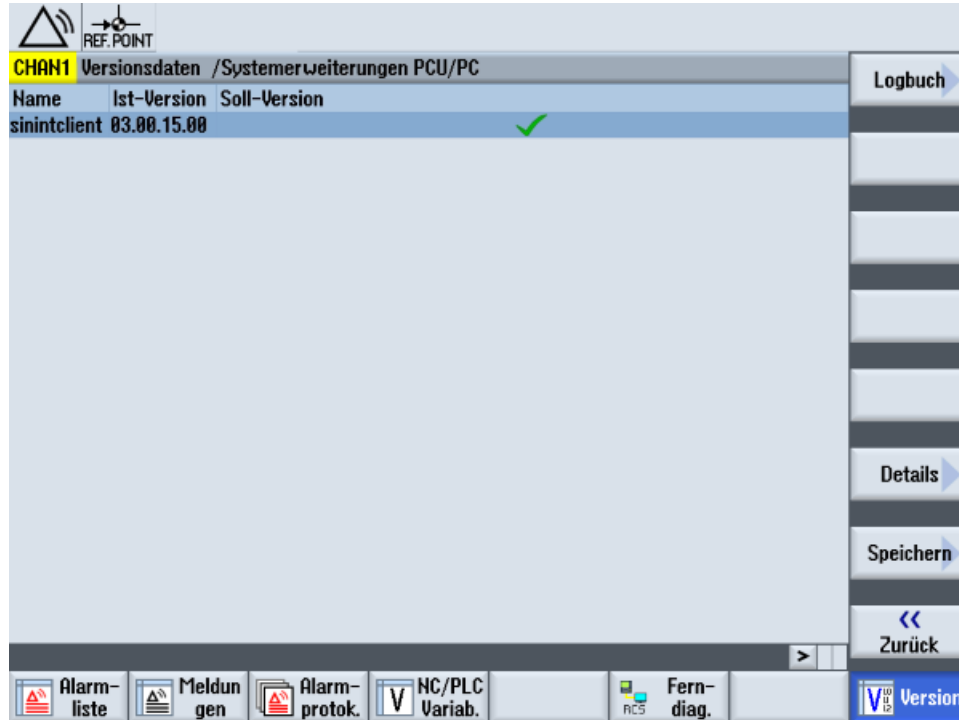
1. Beenden Sie den Fernzugriff an der SINUMERIK-Steuerung.
2. Aktualisieren Sie den SINUMERIK Integrate-Client.
Weitere Informationen zum Client-Update unter Windows finden Sie im Funktionshandbuch Manage MyMachines /Remote.
3. Führen Sie ein Power-On durch.

Hinweis

HMI-Neustart ist nicht ausreichend!

3.4 SINUMERIK Integrate Client-Update über Remote-Zugriff mittels AMM (Windows)

4. Treten Sie der Remote Session wieder bei.
5. Öffnen Sie den Bedienbereich Diagnose.
Prüfen Sie die Version des SINUMERIK Integrate-Client unter "/Version/
Systemerweiterungen PCU/PC".



- ODER -

Prüfen Sie die Version des SINUMERIK Integrate-Client im Dateisystem.

Öffnen Sie die Datei "version.xml" im Verzeichnis: <Installationspfad>\addon\sinumerik\hmi\sinintclient.

3.5 Service Client Manage MyMachines /Remote unter Windows XP installieren

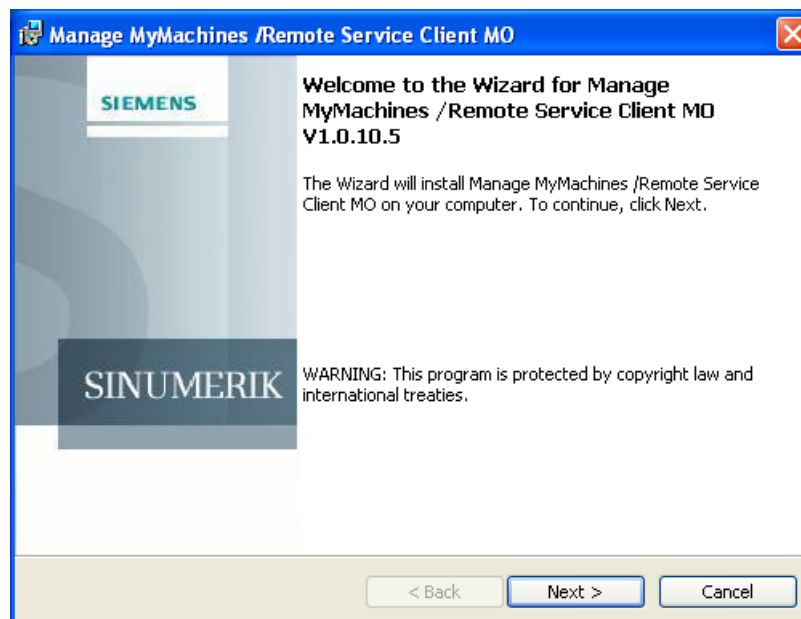
Voraussetzung

Sie haben sich von "Manage MyMachines /Remote" folgende Software heruntergeladen, z. B. auf einen USB-FlashDrive.

- Manage MyMachines /Remote Service Client for Machine Operators - PCU

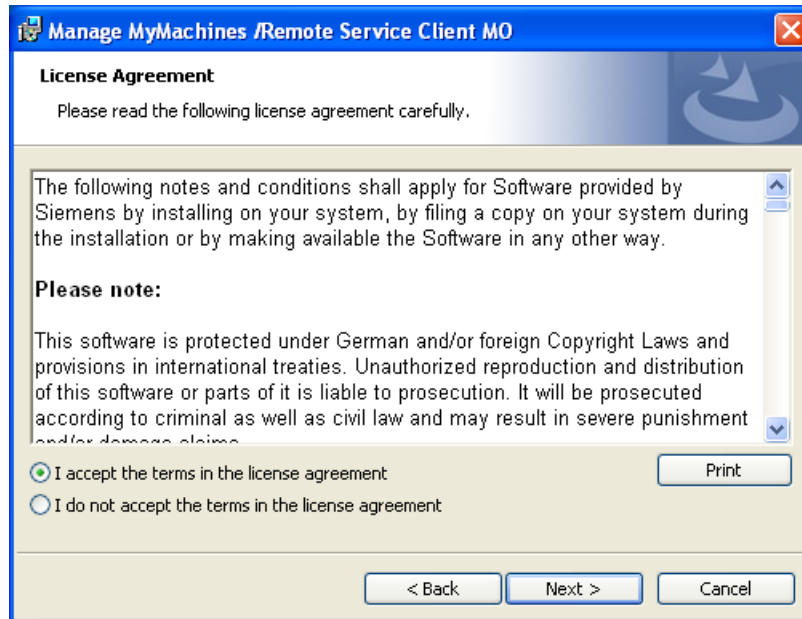
Vorgehensweise

1. Legen Sie die Software in das Installationsverzeichnis, z. B. unter "F".
2. Starten Sie die "setup.exe" mit Doppelklick.
Die Installationssprache ist Englisch.
3. "Manage MyMachines /Remote Service Client MO - InstallShield Wizard" wird geöffnet.
4. Der Willkommensdialog wird geöffnet und zeigt die aktuelle Version.
Klicken Sie auf die Schaltfläche "Next >", um mit der Installationsvorbereitung zu beginnen.

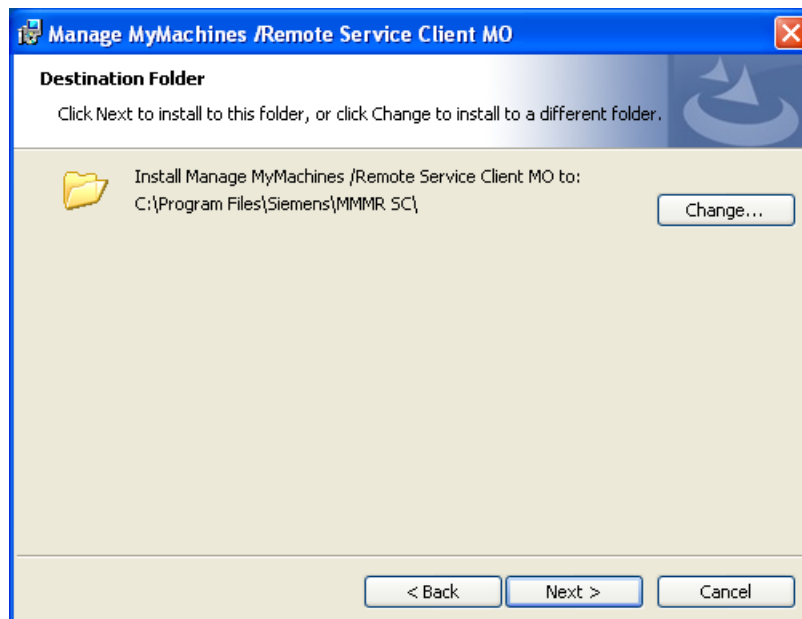


3.5 Service Client Manage MyMachines /Remote unter Windows XP installieren

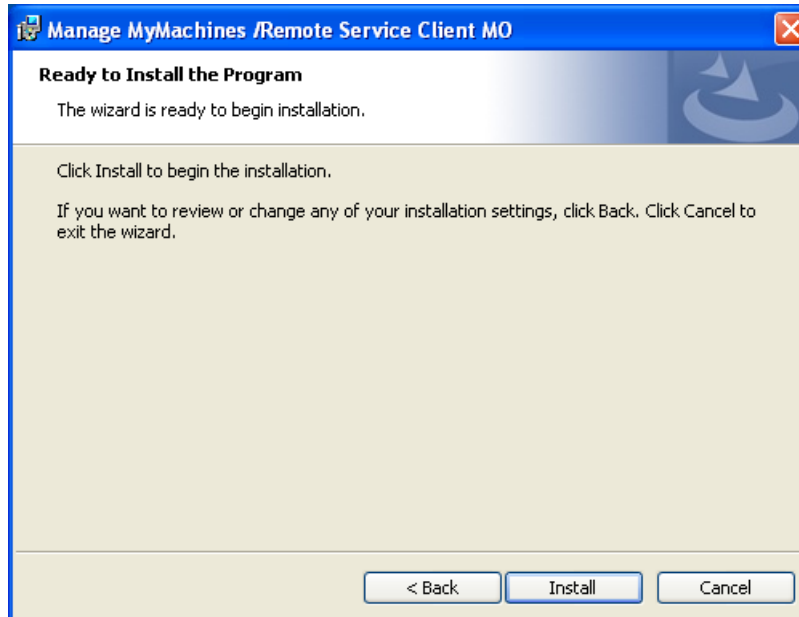
5. Das Fenster "License Agreement" wird geöffnet.
Lesen Sie die Lizenzvereinbarung.
 - Wenn Sie die Bedingungen ausdrucken möchten, klicken Sie auf die Schaltfläche "Print".
 - Aktivieren Sie das Optionsfeld "I accept the terms in the license agreement" und klicken Sie auf die Schaltfläche "Next >".



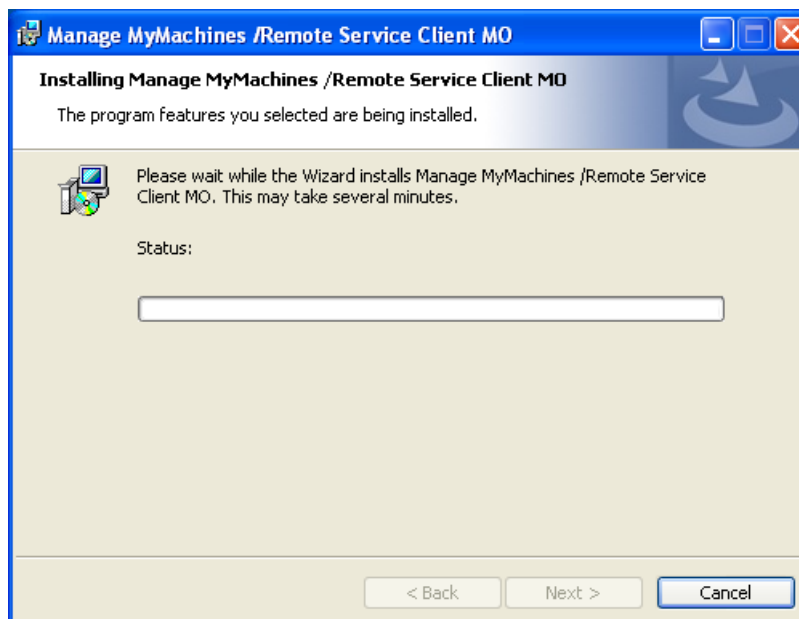
6. Das Fenster "Destination Folder" wird geöffnet und das Installationsverzeichnis wird angezeigt.
Klicken Sie auf die Schaltfläche "Next >".
- ODER -
Um das Verzeichnis zu wechseln, klicken Sie auf die Schaltfläche "Change...".



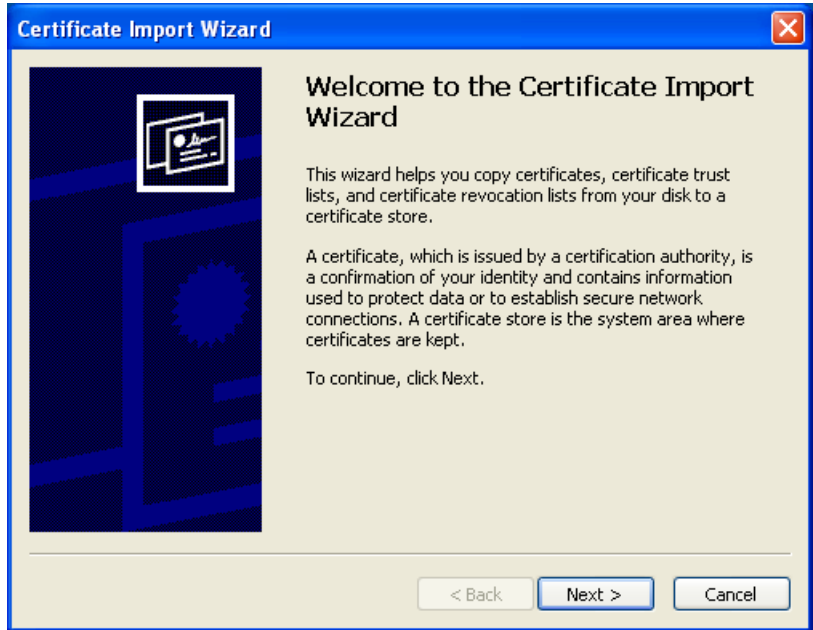
- Der Assistent ist bereit das Programm zu installieren.
Klicken Sie auf die Schaltfläche "Install", um die Installation zu starten.



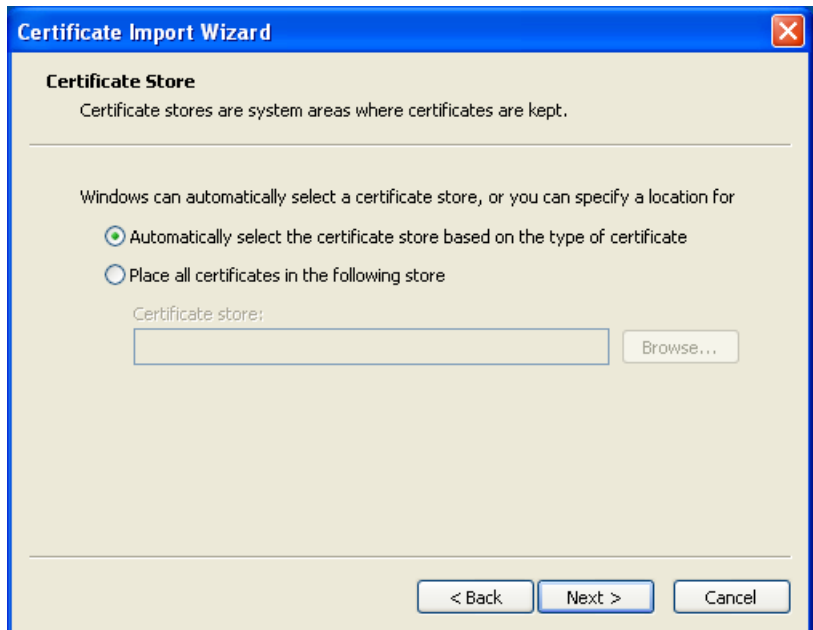
- Das Fenster "Installing Manage MyMachines /Remote Service Client MO" wird geöffnet und zeigt den Installationsfortschritt.



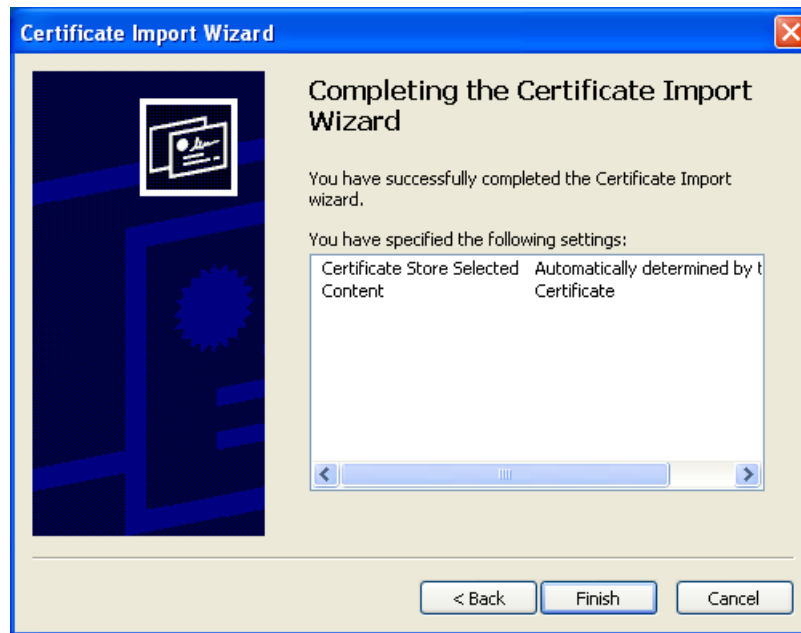
9. Das Fenster "Welcome to the Certificate Import Wizard" wird geöffnet.
Klicken Sie auf die Schaltfläche "Next >", um den Import der Zertifikate zu starten.
- ODER -
Wenn Sie auf die Schaltfläche "< Back" klicken, gelangen Sie jeweils in das vorherige Fenster.



10. Das Fenster "Certificate Store" wird geöffnet.
 - Aktivieren Sie das Optionsfeld "Automatically select the certificate store based on the type of certificate".
 - Klicken Sie auf die Schaltfläche "Next >".



11. Das Fenster "Completing the Certificate Import Wizard" wird geöffnet.
Sie sehen die gewählten Einstellungen.
Klicken Sie die Schaltfläche "Finish", um den Import der Zertifikate zu vervollständigen.

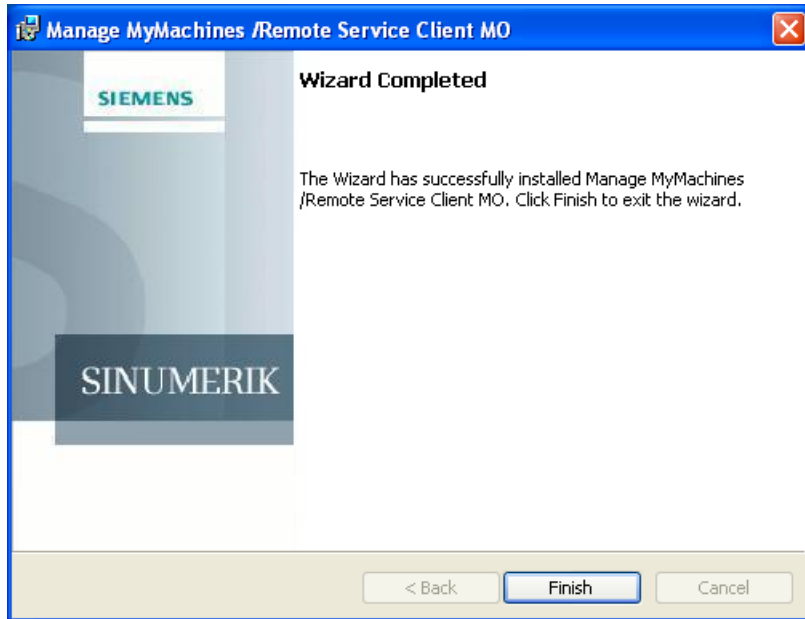


12. Sie erhalten eine Sicherheitswarnung.
Klicken Sie auf die Schaltfläche "Yes", um die Installation der Zertifikate fortzuführen.

13. Sie erhalten die Meldung, dass der Import erfolgreich durchgeführt wurde. Klicken Sie die Schaltfläche "OK", um den Import der Zertifikate zu beenden.



14. Das Fenster "Wizard Completed" wird geöffnet. Klicken Sie auf die Schaltfläche "Finish", um die Installation zu beenden.



3.6 Service Client Manage MyMachines /Remote unter Windows XP nutzen

Um Manage MyMachines /Remote unter Windows XP zu nutzen, steht Ihnen eine Autorisierungssoftware zur Verfügung. Mit dieser Software authentifizieren Sie eine SINUMERIK-Steuerung mit HMI-Advanced, bevor Sie einer Sitzung mit Manage MyMachines / Remote beitreten.

Das Programm ist eine Windows-.exe-Anwendung, welche die Autorisierung älterer SINUMERIK-Steuerungen mit dem Betriebssystem Windows XP ermöglicht. Verwenden Sie die Autorisierungssoftware zusätzlich zum "Manage MyMachines /Remote Service Client".

Standard-Konfiguration - vor der ersten Anwendung

Die Autorisierungssoftware öffnet eine Autorisierungsseite in Ihrem Standard-Webbrowser.

Hinweis

Webbrowser

- Verwenden Sie einen Webbrowser, der mit MindSphere und den nachfolgenden Funktionen von MindSphere kommuniziert.
 - Beachten Sie, dass die Kommunikation eventuell von der Art der Patches für das Betriebssystem abhängt, die auf dem Gerät installiert sind.
 - Beachten Sie auch, dass die Verwendung veralteter Browser und Betriebssysteme spezielle Implementierungsregularien der Sicherheit erfordert, z. B. Firewalls, die vor dem Zugriff von außen schützen. Diese Maßnahmen sind, z. B. im Anwendungshinweis und in der Standarddokumentation zur Sicherheit von SIEMENS beschrieben.
-

Wenn für die Anwendungen in MindSphere zusätzliche Proxy-Einstellungen verwendet werden, übernehmen Sie diese Einstellungen auch für die Autorisierungssoftware.

Weitere Informationen zu den Proxy-Einstellungen finden Sie im Anwendungsbeispiele MindSphere Manage MyMachines /Remote - Installation in bestehende Steuerungsumgebungen

Vorgehensweise

1. Wählen Sie im Startmenü: Start -> Alle Programme -> SIEMENS -> SINUMERIK Integrate.
2. Klicken Sie auf "XP_authorization".

3. Ihr Browser wird mit der Seite "Authorisation page" geöffnet.
 - Geben Sie den Tenantnamen und die Maschinen ID ein.
 - Klicken Sie auf die Schaltfläche "Submit".

SIEMENS

Authorisation page

Tenant Name

tenant name

Machine ID

machine ID

Submit

©2019 Siemens Digital Industries Software Privacy Terms Help

4. Das Fenster "Sign In" wird geöffnet. Geben Sie Ihr MindSphere-Login ein:
 - Geben Sie Ihre E-Mail-Adresse und Ihr Passwort ein.
 - Klicken Sie auf die Schaltfläche "Sign In".

SIEMENS

Sign In

[or create an account](#)

Sign In has changed. If you previously signed in with a username, please use your email. [Need help?](#)

Email

user@domain.com

Password [Show](#)

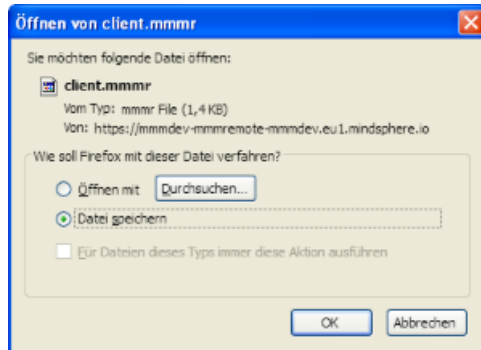
Enter your password

[Forgot your password?](#)

Sign In

©2019 Siemens Digital Industries Software Privacy Terms Help

- Das Standardfenster für das Herunterladen von Dateien wird geöffnet. Klicken Sie auf die Schaltfläche "OK", um die Client-Autorisierungsdatei "client.mmmr" zu speichern. Die Datei wird automatisch im richtigen Verzeichnis abgelegt.



- Starten Sie den "Manage MyMachines /Remote Service Client MO". Sie können nun an einer Sitzung teilnehmen, nachdem der Service Ingenieur die Sitzung initiiert hat.

Fehlerbehandlung - Daten für den Login-Prozess sichern

Die Autorisierungssoftware verwaltet nicht die Sitzung zwischen Benutzer und MindSphere.

Wenn Sie Daten für das Login sichern möchten, erfolgt dies in Ihrem Webbrowser, z. B. mit Cookies.

Hinweis

Daten im Browser merken

Der Browser kann sich eventuell die Daten merken, die Sie in Eingabefelder ausfüllen.

Wenn Daten wie Tenantname oder Maschinen ID nicht automatisch ausgefüllt werden, ändern Sie die Standardeinstellungen für den Datenschutz.

Anhang

A.1 Liste der Abkürzungen

Admin	Administrator (Benutzerrolle)
AMM /C	Analyze 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
VNC	Virtual Network Computing

