

SINUMERIK

MindSphere Manage MyMachines /Remote

Liesmich

Gültig für Steuerung:
SINUMERIK 840D sl, 840DE sl, 828D
SINUMERIK ONE

Software
Manage MyMachines /Remote, Version 01.03.00.00

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.

Inhaltsverzeichnis

1	Grundlegende Sicherheitshinweise	5
1.1	Allgemeine Sicherheitshinweise.....	5
1.2	Gewährleistung und Haftung für Applikationsbeispiele.....	6
1.3	Security-Hinweise	7
2	Systemvoraussetzungen	9
3	Produktinformation / Technische Aktualisierung	17
3.1	Randbedingungen.....	17

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.

Systemvoraussetzungen

Hardware und Bedien-Software

Die Anbindung erfolgt über den "Manage MyMachines /Remote Service Client".

Der SINUMERIK Integrate Client wird benötigt, wenn Sie den integrierten Manage MyMachines /Remote Client im SINUMERIK Integrate Client nutzen wollen. Diese Komponente muss bei Bedarf hochgerüstet werden.

SINUMERIK 840D sl, SINUMERIK ONE

SINUMERIK Integrate Client-Software Version	Bediensoftware SINUMERIK Operate Version	Hardware Version	Betriebssystem
2.0.13 2.0.14 2.0.16	4.5 SP4, HF1, 2, 3, 4	NCU 7x0.3 (B) PN	Linux
	4.5 SP5, HF1, 3, 5 4.5 SP6, HF2, 3, 5, 7, 8, 10, 11, 13 14, 15, 16, 17, 18	PCU 50.5 IPC 427E IPC 477E	Windows 7 Windows 10
	4.5 SP4, HF1, 2, 3, 4 4.5 SP6, HF1, 3, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18	NCU 7x0.3 (B) PN	Linux
3.0.13 3.0.14 3.0.16	4.7 SP1, HF1 4.7 SP2, HF1, 3, 4 4.7 SP3, HF1, 2, 3 4.7 SP4, HF1, 4, 5, 6 4.7 SP5, HF1 4.7 SP6, HF1, 3, 4, 5, 6, 7 4.8 SP1, HF1, 2, 3 4.8 SP2, HF1, 3 4.8 SP3, HF1 4.8 SP4, HF1, 3, 4, 6, 8 4.8 SP5, HF5, 6	NCU 7x0.3 (B) PN PCU 50.5 IPC 427E IPC 477E	Linux Windows 7 Windows 10
4.0.16	4.92, HF3 4.93, HF1	NCU 7x0.3 (B) PN PCU 50.5 IPC 427E IPC 477E	Linux Windows 7 Windows 10
	6.13, HF1	SINUMERIK ONE 1750/ 1760	Linux

SINUMERIK 828D

SINUMERIK Integrate Client-Software Version	Bediensoftware SINUMERIK Operate Version	Hardware Version	Betriebssystem
2.0.13	4.5 SP4	PPU 281.3	Linux
2.0.14	4.5 SP5, HF1, 2	PPU 261.3	
2.0.16	4.5 SP6, HF1, 2, 3, 4	PPU 241.3	
3.0.13	4.7 SP2, HF1 4.7 SP3, HF2 4.7 SP4, HF1, 2 4.7 SP5 4.7 SP6, HF1		Linux
3.0.13	4.8 SP4, HF1	PPU 271.4	
3.0.14 3.0.16	4.7 SP2, HF1 4.7 SP3, HF2 4.7 SP4, HF1, 2 4.7 SP5 4.7 SP6, HF1, 2 4.7 SP7, HF1, 3	PPU 290.3 PPU 28x.3 PPU 26x.3 PPU 24x.3	
3.0.14	4.8 SP4, HF1, 2, 3, 4,5	PPU 27x.4 PPU 290.4	Linux

SINUMERIK-Steuerung

Bildschirmauflösung	800 x 600 1280 x 1024 1366 x 768 1440 x 900 1600 x 1200 1680 x 1050 1920 x 1200 1920 x 1080
---------------------	------------------------------------------------------------------------------------------------------------------

Webbrowser

Sie können folgende Webbrowser einsetzen:

- Chrome
Version ab 65.0.3325.18 (64 bit) bis zur aktuellen Version
- Firefox
Version ab 59.0.2 (64 bit) bis zur aktuellen Version

Bedien-PC

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

Industrie-PC

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.

Remote STEP 7

- SIMATIC Manager Versionen:
 - 5.4
 - 5.5
 - 5.6
- TIA Portal Versionen:
 - 15.0
 - 15.1
 - 16.0
 - 16.1

- TCU und Remote Step 7 unterstützen folgende SINUMERIK Integrate Client Versionen:
 - 2.0.13
 - 2.0.14
 - 3.0.13
 - 3.0.14
- SINUMERIK Operate läuft unter PCU oder IPC mit folgenden SINUMERIK Integrate Client Versionen:
 - 2.0.16
 - 3.0.16
 - 4.0.16

Hinweis

"Remote STEP 7"

"Remote STEP 7" steht in folgenden Konfigurationen zur Verfügung:

- SINUMERIK Operate unter Linux (NCU)
- SINUMERIK Operate auf PCU oder IPC

"Remote STEP 7" wird von SINUMERIK 828D **nicht** unterstützt.

Hinweis

SINUMERIK Integrate Applikationen

Eine parallele Bearbeitung mit SINUMERIK Integrate Anwendungen ist nicht möglich.

Weitere Informationen

Weitere Informationen zur Anbindung von Fremdsteuerungen finden Sie in folgendem Handbuch:

"Manage MyMachines /Remote - Installation in bestehende Steuerungsumgebungen" und "SIMATIC IoT2040".

Security-Hinweise

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 Netz 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, z. B. bei der Übertragung der Asset-Daten.

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

ACHTUNG

Datenmanipulation möglich

Es besteht das Risiko, dass sich ein Angreifer innerhalb des Netzes 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 Dienstleister (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.

ACHTUNG

Fernzugriff auf der SINUMERIK-Steuerung erlauben

Erlauben Sie eine Fernzugriffssitzung nur, wenn Ihnen Folgendes bekannt ist:

- Sind Sie über eine Fernzugriffssitzung informiert worden?
- Ist Ihnen die Person bekannt und vertrauenswürdig, die die Sitzung ausführt?

Lieferform

Der "Manage MyMachines /Remote Service Client" ist über die Applikation "Manage MyMachines /Remote" verfügbar.

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.

Hinweis

Vertrauenswürdige Software aus dem Internet

Wenn Sie Clients über das Internet herunterladen, installieren Sie nur die von Siemens signierte Software.

Produktinformation / Technische Aktualisierung

3.1 Randbedingungen

Manage MyMachine /Remote auf PCU

Fehlerbeschreibung:

Wenn Sie Manage MyMachine /Remote auf PCU nutzen, haben Sie als Maschinenbediener 2 Möglichkeiten einer Fernzugriffssitzung beizutreten:

- Über SINUMERIK Integrate Client im SINUMERIK Operate
- Über Manage MyMachine /Remote Service Client

Wenn Sie versuchen, einer Sitzung mit beiden Clients beizutreten, können Fehler auftreten.

Abhilfe:

Treten Sie einer bestehenden Fernzugriffssitzung nur mit einem Client bei: Entweder mit dem SINUMERIK Integrate Client oder mit dem Manage MyMachine /Remote Service Client.

Komplette Verzeichnisse mit der Funktion "Datenübertragung" kopieren

Fehlerbeschreibung:

Die Funktion "Datenübertragung" im Remote Service Client unterstützt nicht das Kopieren von kompletten Verzeichnissen.

Abhilfe:

Öffnen Sie das Verzeichnis und kopieren Sie die einzelnen Dateien.

Installation des Access MyMachine SMC SE Client wird zerstört

Fehlerbeschreibung:

Eine existierende Installation des Access MyMachine SMC SE Client wird durch die Installation des Manage MyMachines /Remote Service Client für Serviceingenieure zerstört.

Abhilfe:

1. Deinstallieren Sie den AMM SMC SE Client.
2. Installieren Sie den Manage MyMachines /Remote Service Client für Serviceingenieure.
3. Installieren Sie den AMM SMC SE Client.

Zeitweise Löschen durch den Service-Ingenieur nicht möglich

Fehlerbeschreibung:

Sporadisch kann der Fehler auftreten, dass eine Datei nicht gelöscht werden kann. In diesem Fall wird keine Fehlermeldung angezeigt, der Status der Operation ist "Unknown".

Abhilfe:

Schließen Sie die Sitzung und starten Sie eine neue Sitzung, um Dateien zu löschen.

Teilnahme eines zweiten Service-Ingenieurs an einer Sitzung

Fehlerbeschreibung:

Ein zweiter Service-Ingenieur kann nicht an einer Sitzung beitreten, die durch einen Service-Ingenieur geleitet wird.

Abhilfe:

Warten Sie, bis der Maschinenbediener der Sitzung beigetreten ist.

Meldung "Zugriff verweigert" bei der Übertragung von Dateien

Fehlerbeschreibung:

Wenn Sie eine bereits gelöschte Datei aus dem Remote-System ins lokale Dateisystem oder umgekehrt übertragen möchten, kommt die Meldung "Zugriff verweigert".

Abhilfe:

Stellen Sie sicher, dass die Datei im lokalen Dateisystem verfügbar ist.

Löschvorgang abbrechen

Fehlerbeschreibung:

Der Maschinenbediener kann den Löschvorgang von Dateien nicht abbrechen, nachdem der Löschvorgang eingeleitet wurde.

Abhilfe:

Der Service-Ingenieur kann die Dateien des Maschinenbedieners sowie alle anderen Dateien löschen, wenn der Maschinenbediener dem Service-Ingenieur die Rechte für alle Aktivitäten in der Sitzung übertragen hat.

Datenübertragung vom mehr als 300 Dateien

Fehlerbeschreibung:

Eine Datenübertragung von mehr als 300 Dateien kann zu Anwendungsproblemen führen.

Abhilfe:

Beachten Sie, dass die Datenmenge nicht mehr als maximal 300 Dateien beträgt.

Beitreten der Sitzung als beobachtender Ingenieur

Fehlerbeschreibung:

Sie können als beobachtender Ingenieur einer Sitzung nicht beitreten, wenn die Bildschirmfreigabe aktiv ist.

- ODER -

Sie können einer Sitzung nicht beitreten, während eine Datenübertragung läuft.

Abhilfe:

Warten Sie, bis die Bildschirmfreigabe gestoppt wird.

- ODER -

Warten Sie, bis die Datenübertragung abgeschlossen ist.

Sitzungsinformationen unvollständig bei Übertragung mehrerer Dateien

Fehlerbeschreibung:

Wenn mehrere Dateien parallel übertragen werden, können Sitzungsinformationen unvollständige Informationen enthalten, z. B. können Dauer und Endzeitpunkt fehlen.

Abhilfe:

Übertragen Sie Daten hintereinander.

Logs sind sporadisch unvollständig

Fehlerbeschreibung:

Es kann vorkommen, dass Logs unvollständige Daten enthalten.

Sender und Empfänger werden nicht korrekt angezeigt

Fehlerbeschreibung:

Es kann vorkommen, dass Sender und Empfänger in den Logs nicht korrekt angezeigt werden.

Fehlender Speicherplatz

Fehlerbeschreibung:

Wenn der Speicherplatz auf dem Zielsystem eingeschränkt ist, werden die Dateien nicht korrekt übertragen.

Abhilfe:

Prüfen Sie, ob ausreichend Speicherplatz vorhanden ist.

Beendigung der Sitzung, wenn der leitende Service-Ingenieur die Sitzung verlässt

Fehlerbeschreibung:

Wenn der leitende Service-Ingenieur die Sitzung verlässt, wird die Sitzung geschlossen.

Abhilfe:

Übertragen Sie die Leitung der Sitzung an einen anderen Service-Ingenieur, bevor Sie die Sitzung verlassen.

Dateien auf D:\ löschen

Fehlerbeschreibung:

Der Service-Ingenieur kann Dateien im Verzeichnis D:\ nicht löschen. Der Zugriff wird vom System verweigert.

Datenübertragung abbrechen

Fehlerbeschreibung:

Der Maschinenbediener kann die Datenübertragung von mehreren Dateien mit geringen Dateigrößen nicht abbrechen, wenn er die Option "Für alle nachfolgenden akzeptieren" gewählt hat.

Abhilfe:

Prüfen, ob die Option "Für alle nachfolgenden akzeptieren" abgewählt ist.

Dateien umbenennen

Fehlerbeschreibung:

Wenn der Service-Ingenieur die Aktion "Dateien umbenennen" abbricht, bekommt der Maschinenbediener eine Abfrage, ob er die Datenübertragung wirklich abbrechen möchte.

Abhilfe:

Verwenden Sie den Dialog, um die Anfrage zu bestätigen bzw. abubrechen.

Verbindungsunterbrechung während einer Sitzung

Fehlerbeschreibung:

Wenn die Verbindung zum Client für länger als 1 Minute unterbrochen wurde, werden Sie nach dem Wiederherstellen der Verbindung durch einen Dialog darüber informiert, dass die Verbindung zur jeweiligen IP-Adresse nicht hergestellt werden kann.

Abhilfe:

Bestätigen Sie den Dialog mit der Schaltfläche "OK".

Klicken Sie in der Abfrage, ob Sie die Session verlassen möchten, auf die Schaltfläche "Nein".

Sie bleiben in der Sitzung.

Das Systemverhalten kann je nach Dauer der Verbindungsunterbrechung variieren.

Verbindungsunterbrechung von mehr als 1 Minute

Fehlerbeschreibung:

Nach einer Verbindungsunterbrechung von mehr als 1 Minute und einer anschließenden Wiederherstellung der Verbindung, wird die noch laufende Sitzung als beendet angezeigt.

Abhilfe:

Keine Abhilfe möglich, denn aufgrund von fehlenden Schaltflächen können keine weiteren Teilnehmer dieser Session beitreten.

Deinstallation von Manage MyMachines /Remote Service Client

Fehlerbeschreibung:

Bei der Deinstallation des "Manage MyMachines /Remote Service Clients" erhalten Sie eine Meldung, dass die Deinstallation des Zertifikats fehlgeschlagen ist.

Abhilfe:

Klicken Sie auf die Schaltfläche "OK".

Beitreten der Sitzung mit der Datei "client.mmmr"

Fehlerbeschreibung:

Mit einer gültigen Datei "client.mmmr" ist es nicht möglich, eine Sitzung zu starten oder einer Sitzung beizutreten.

Abhilfe:

Wählen Sie in Windows den "Manage MyMachines /Remote Service Client" als Standardprogramm für das Öffnen der Datei "*.mmm".

Mozilla Firefox

Fehlerbeschreibung:

Es ist nicht möglich, in Mozilla Firefox die Standardanwendung "MMM /Remote Service Client" zu wählen.

Abhilfe:

Wählen Sie in Windows den "Manage MyMachines /Remote Service Client" als Standardprogramm für das Öffnen der Datei "*.mmm".

Subtenant-Benutzer startet Manage MyMachines /Remote

Fehlerbeschreibung:

Es ist nicht möglich, mit einem Subtenant-Benutzer eine Sitzung für "Manage MyMachines / Remote" zu starten.

Abhilfe:

Vergeben Sie Administratorrechte.

Der Softkey "Manage MyMachines /Remote" wird nach dem Update des SINUMERIK Integrate Clients nicht angezeigt

Der Softkey "Manage MyMachines /Remote" wird nach dem Update des SINUMERIK Integrate Clients nicht angezeigt, wenn das Base Setup bereits auf dem SINUMERIK Integrate Client installiert wurde.

Vorgehensweise 1: Das Update des SINUMERIK Integrate Client ist noch nicht durchgeführt

1. Deinstallieren Sie das Base Setup.
2. Starten Sie HMI neu.
3. Führen Sie das Update des SINUMERIK Integrate Client durch.
4. Installieren Sie das Base Setup.
5. Starten Sie HMI neu.

Vorgehensweise 2: Das Update des SINUMERIK Integrate Client ist bereits durchgeführt

1. Deinstallieren Sie das Base Setup.
2. Starten Sie HMI neu.
3. Installieren Sie das Base Setup.
4. Starten Sie HMI neu.

Der Softkey "Manage MyMachines /Remote" wird wieder angezeigt.

Zertifikat mehrfach installieren

Vorgehensweise

Während der Installation von Manage MyMachines /Remote Service Client werden Sie mehr als einmal aufgefordert den Zertifikats-Installationsprozess abzuschließen.

Hinweis:

Die Aufforderung Zertifikate mehr als einmal zu installieren, stellt sicher, dass alle relevanten Zertifikate enthalten sind. Folgen Sie der Aufforderung.