SIEMENS

Projektierungsbeispiel • 09/2014

Einrichtung einer gesicherten VPN-Verbindung zwischen dem TS Adapter IE Advanced und Windows 7

TS Adapter IE Advanced

http://support.automation.siemens.com/WW/view/de/99681037

Gewährleistung und Haftung

Hinweis

Die Applikationsbeispiele sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit hinsichtlich Konfiguration und Ausstattung sowie jeglicher Eventualitäten. Die Applikationsbeispiele stellen keine kundenspezifischen Lösungen dar, sondern sollen lediglich Hilfestellung bieten bei typischen Aufgabenstellungen. Sie sind für den sachgemäßen Betrieb der beschriebenen Produkte selbst verantwortlich. Diese Applikationsbeispiele entheben Sie nicht der Verpflichtung zu sicherem Umgang bei Anwendung, Installation, Betrieb und Wartung. Durch Nutzung dieser Applikationsbeispiele erkennen Sie an, dass wir über die beschriebene Haftungsregelung hinaus nicht für etwaige Schäden haftbar gemacht werden können. Wir behalten uns das Recht vor, Änderungen an diesen Applikationsbeispielen jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in diesem Applikationsbeispiel und anderen Siemens Publikationen, wie z.B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.

Für die in diesem Dokument enthaltenen Informationen übernehmen wir keine Gewähr.

Unsere Haftung, gleich aus welchem Rechtsgrund, für durch die Verwendung der in diesem Applikationsbeispiel beschriebenen Beispiele, Hinweise, Programme, Projektierungs- und Leistungsdaten usw. verursachte Schäden ist ausgeschlossen, soweit nicht z.B. nach dem Produkthaftungsgesetz in Fällen des Vorsatzes, der groben Fahrlässigkeit, wegen der Verletzung des Lebens, des Körpers oder der Gesundheit, wegen einer Übernahme der Garantie für die Beschaffenheit einer Sache, wegen des arglistigen Verschweigens eines Mangels oder wegen Verletzung wesentlicher Vertragspflichten zwingend gehaftet wird. Der Schadensersatz wegen Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegt oder wegen der Verletzung des Lebens, des Körpers oder der Gesundheit zwingend gehaftet wird. Eine Änderung der Beweislast zu Ihrem Nachteil ist hiermit nicht verbunden.

Security-hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter http://support.automation.siemens.com.

Inhaltsverzeichnis

1 Aufgabenstellung und Lösung

1.1 Aufgabe

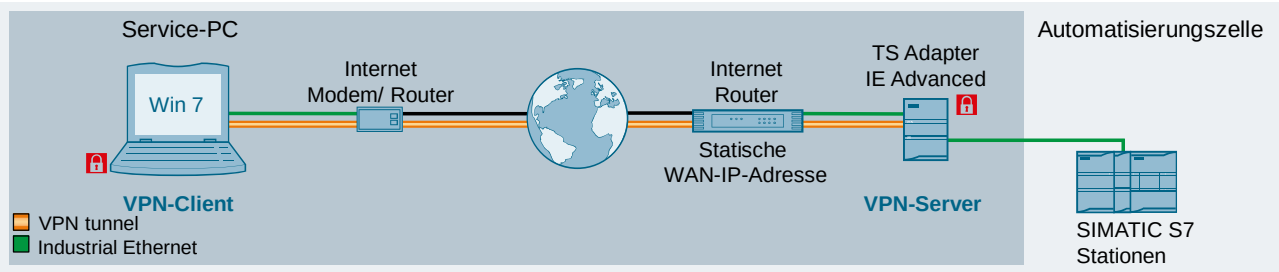
Die Aufgabe besteht darin, eine sichere Verbindung zwischen zwei Netzen (z. B. Automatisierungsnetzwerken oder einzelnen Geräten) über Internet oder ein firmeninternes Netzwerk zu errichten.
Dabei sind folgende Kundenanforderungen zu berücksichtigen:

- Absicherung gegen Spionage und Datenmanipulation.
- Verhindern von unerlaubtem Zugriff.
- Unkomplizierte Handhabung und Integration.
- Verwendung vorhandener Adressen und Adressierungsschemata.
- Transparenz (bzw. einfache Anwendung) für Benutzer.

1.2 Lösungsmöglichkeit

Gesamtübersicht

Die folgende Grafik zeigt eine Möglichkeit, die Kundenanforderung umzusetzen:



Die Verbindung zwischen dem Service-PC und der Automatisierungszelle (wie z.B. SIMATIC Stationen, Panel, Antriebe, PCs) wird durch einen VPN-Tunnel abgesichert.

Der Service-PC und der TS Adapter IE Advanced bilden in diesem Beispiel die beiden Tunnelendpunkte für die gesicherte Verbindung. Der TS Adapter IE fungiert als VPN-Server, der PC als VPN-Client.

Der Zugang zum TS Adapter IE (VPN-Server) aus dem WAN ist über die Nutzung einer statischen WAN-IP-Adresse fest definiert.

Der WAN-Zugang auf Clientseite ist flexibel; die IP-Adresse des WAN-Zugangs ist nicht relevant.

Die Rollenverteilung beim Aufbau des VPN-Tunnels wird wie folgt festgelegt:

Tabelle 1-1

Komponente	VPN-Rolle
Service-PC	Initiator (VPN-Client); startet die VPN-Verbindung
TS Adapter IE Advanced	Responder (VPN-Server); wartet auf VPN-Verbindung

TS Adapter IE Advanced

Der TS Adapter IE Advanced ermöglicht den Zugriff über das Internet auf alle Automatisierungskomponenten - z.B. S7-CPUs - die auf der Anlage am Industrial Ethernet angeschlossen sind.

Mit einem PG/PC mit mind. Windows 7 oder Windows Server 2008 ist die Fernwartung einer Anlage über das Internet komfortabel und inklusiver verbesserter Sicherheitsmechanismen möglich.

Sie bieten folgende Funktionen:

- SSTP-VPN (Datenverschlüsselung und Authentifizierung) zur Fernwartung.
- IPv4- und IPv6-Unterstützung an der WAN-Schnittstelle (IPv6 ab Firmware-Version 1.1.0).
- Zeitgesteuerte WAN-Konnektivität.
- Paketfilter-Konfiguration.
- Freigeben- und Sperren von Verbindungswegen (VPN-Tunnel, Internetzugang).
- Router-Funktionalität (Port-Forwarding, NAT, DynDNS (mit IPv6)).

1.3 Merkmale der Lösung

- Hoher Sicherheitsstandard durch
  - VPN,
  - Zertifikate,
  - in Hardware gebildete Zufallszahlen
  - Berücksichtigung der hohen Siemens Security Richtlinien.
- Maßgeschneiderte Lösung für die Fernwartung im Automatisierungsumfeld.
- Gleicher Funktionsumfang (STEP 7-Funktionen, Diagnose) wie vor Ort ohne zusätzlich zu installierende Programme.
- Problemlose Integration in vorhandene Netzwerke und Schutz von Geräten ohne eigene Security Funktionen.
- In der Regel kein Freischalten oder Konfiguration durch die IT Administratoren notwendig.

2 Konfiguration und Projektierung

2.1 Einrichten der Umgebung

2.1.1 Erforderliche Komponenten und IP-Adressenübersicht

Softwarepakete

Für das Arbeiten mit dem TS Adapter IE Advanced benötigen Sie einen PC mit einem Betriebssystem „Windows 7“ (oder höher) und der Software“ Primary Setup Tool“ (PST) (ab V4.1).

Installieren Sie diese Softwarepakete auf einen PC/PG.

Hinweis Das Primary Setup Tool wird für die Einstellung der LAN-Schnittstelle des TS Adapter IE Advanced verwendet.
Dieses Tool kann kostenlos unter der BeitragsID:19440762 im Online Support heruntergeladen werden.

Erforderliche Geräte/Komponenten:

Für den Aufbau verwenden Sie folgende Komponenten:

- Einen TS Adapter IE Advanced (optional: eine entsprechend montierte Hutschienen mit Montagematerial).
- Eine 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker.
- Einen DSL-Zugang mit dynamischer WAN-IP-Adresse und einen DSL-Router (z.B. SCALANCE M81x-1).
- Einen DSL-Zugang mit statischer WAN-IP-Adresse und einen DSL-Router (z.B. SCALANCE M81x-1).
- Ein PC, auf dem „Windows 7“ und das „PST“ installiert ist.
- Die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet.

Hinweis Sie können auch einen anderen Internet-Zugang (z.B. UMTS) verwenden.
Die nachfolgend beschriebene Projektierung bezieht sich explizit nur auf die im Abschnitt „Erforderliche Geräte/Komponenten“ erwähnten Komponenten.

IP-Adressen

Die Zuordnung der IP-Adressen ist für dieses Beispiel wie folgt festgelegt:

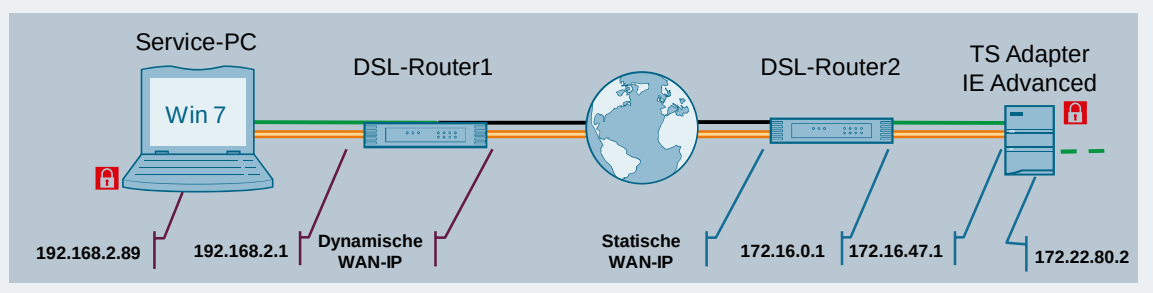


Tabelle 2-1

Komponente	Port	IP-Adresse	Router	Subnetzmaske
Service-PC	LAN-Port	192.168.2.89	192.168.2.1	255.255.255.0
DSL-Router1	LAN-Port	192.168.2.1	-	255.255.255.0
DSL-Router1	WAN-Port	Dynamische IP-Adresse vom Provider	-	Vom Provider zugewiesen
DSL-Router2	WAN-Port	Statische IP-Adresse vom Provider	-	Vom Provider zugewiesen
DSL-Router2	LAN-Port	172.16.0.1	-	255.255.0.0
TS Adapter IE	WAN-Port	172.16.47.1	172.16.0.1	255.255.0.0
TS Adapter IE	LAN-Port	172.22.80.2	-	255.255.255.0

2.1.2 Service-PC

Installierte Software

Auf dem Service-PC sind folgende Softwarepakete relevant:

- PC mit dem Betriebssystem Windows 7 als Gegenstelle für die VPN-Verbindung zum TS Adapter IE Advanced.
- Web-Browser für die Parametrierung des TS Adapters IE Advanced.
- Primary Setup Tool zum Einstellen der IP-Adresse.

CA-Zertifikat löschen

Falls der Verdacht besteht, dass ein CA-Zertifikat missbraucht wird, sollten Sie zur Sicherheit ein neues CA-Zertifikat generieren. Stellen Sie sicher, dass das neue CA-Zertifikat bei allen beteiligten Service-PCs ausgetauscht wird (Löschen des alten und Importieren des neuen CA-Zertifikats).

Aus Sicherheitsgründen sollten Sie die CA-Zertifikate in regelmäßigen Abständen neu generieren.

Orientieren Sie sich zum Löschen an der Anleitung aus Kapitel 4 (Anhang: Umgang mit CA-Zertifikaten).

CA-Zertifikat installieren

Die Erstkonfiguration des TS Adapter IE Advanced erfolgt über eine lokale HTTPS-Verbindung. Da zu diesem Zeitpunkt noch kein CA-Zertifikat für diesen TS Adapter IE Advanced auf dem Service-PC installiert ist, erscheint eine Sicherheitswarnung. Sie können diese Sicherheitswarnung quittieren oder vor der Erstinbetriebnahme das auf der CD mitgelieferte CA-Zertifikat im Windows Zertifikatsspeicher installieren. Orientieren Sie sich hierbei an der Anleitung aus Kapitel 4 (Anhang: Umgang mit CA-Zertifikaten).

Hinweis Zum Verwalten von CA-Zertifikaten benötigen Sie Administrator-Rechte.

Web-Interface des TS Adapter IE Advanced

Sie haben folgende Möglichkeiten das Web-Interface zu öffnen:

- Web-Browser im Direktanschluss mit TIA-Portal öffnen.
- Web-Browser über Fernverbindung mit dem TIA-Portal öffnen.
- Standard Web-Browser im Direktanschluss.

Für dieses Beispiel wird die Methode „ Standard Web-Browser im Direktanschluss“ verwendet.

Hinweis Nähere Informationen über die Möglichkeiten zum Öffnen des Web-Interfaces finden Sie im entsprechende Kapitel im Handbuch des TS Adapters unter diesem Link:
https://www.automation.siemens.com/mdm/default.aspx?DocVersionId=65739502731&Language=de-DE&TopicId=65449369483

2.1.3 DSL-Zugang beim TS Adapter IE Advanced (DSL-Router2)

Statische IP-Adresse bei DSL-Router2

Der WAN-Zugriff des Service-PCs (VPN-Client) auf den TS Adapter IE Advanced (VPN-Server) erfolgt über eine fest zugewiesene, öffentliche IP-Adresse. Diese muss beim Provider beantragt und anschließend im DSL-Router2 hinterlegt werden.

Portforwarding am DSL-Router2

Durch die Nutzung eines DSL-Routers als Internet-Gateway müssen Sie folgenden Port am DSL-Router2 freischalten und die Datenpakete an den TS Adapter IE Advanced (VPN-Server; IP-Adresse am WAN-Port) weiterleiten:

- TCP Port 443 (HTTPS)

Hinweis

Einige Router erlauben den Fernzugriff über eine Internet-Verbindung (HTTPS-Port 443). In diesem Fall ist es nicht möglich, den Port 443 über das Portforwarding an den TS Adapter IE Advanced weiterzuleiten. Sie müssen für den Fernzugriff auf den Router einen anderen Port verwenden (z. B. Port 5443).

Der Port 443 ist für VPN-Verbindungen (SSTP) in Windows und somit auch für den TS Adapter IE fest definiert und kann nicht geändert werden.

2.1.4 TS Adapter IE Advanced

Zurücksetzen auf Werkseinstellung

Um sicherzugehen, dass keine alten Konfigurationen und Zertifikate im TS Adapter IE Advanced gespeichert sind, setzen Sie das Modul auf Werkseinstellung zurück. Das entsprechende Kapitel im Handbuch des TS Adapters finden Sie unter diesem Link:

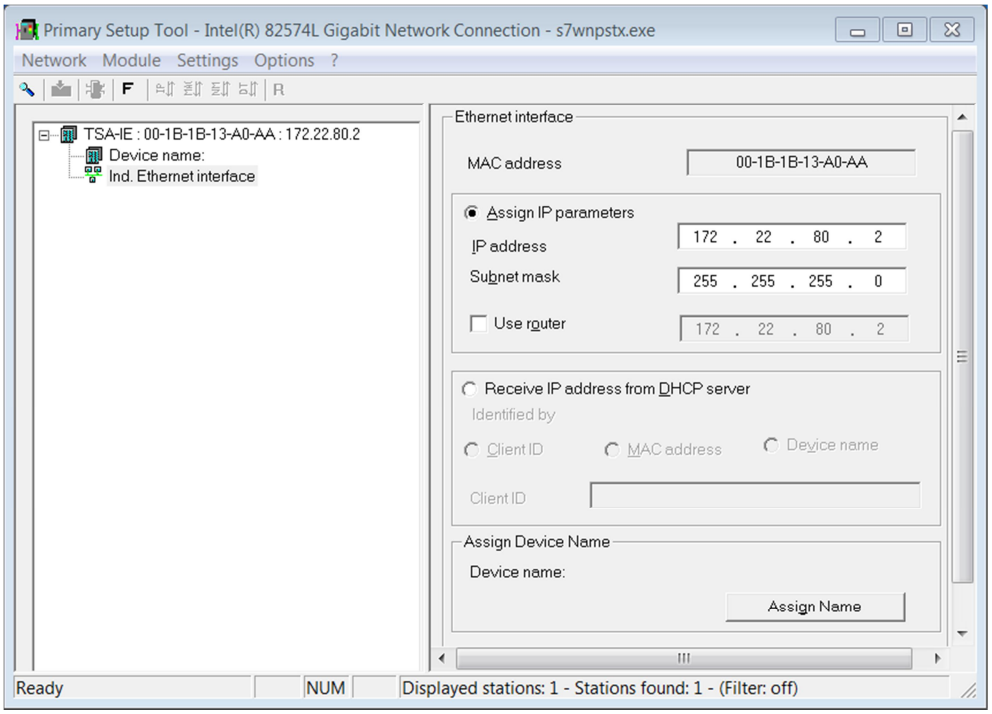
https://www.automation.siemens.com/mdm/default.aspx?DocVersionId=65739502731&Language=de-DE&TopicId=49826068875

Physikalische Verbindung zwischen PC und TS Adapter IE Advanced

Verbinden Sie den PC mit einem LAN-Port des TS Adapter IE Advanced.

IP-Adresse zuweisen

Im Auslieferungszustand und nach Rücksetzen der Parameter hat der TS Adapter IE Advanced keine gültige IP-Adresse. Um mit dem Modul arbeiten zu können, müssen Sie zuerst seine IP-Parameter gemäß Tabelle 2-1 einstellen. Verwenden Sie dafür das Primary Setup Tool.



Hinweis Informationen zu dem Primary Setup Tool wie Installation, Konfiguration und Handhabung finden Sie im Handbuch unter der BeitragsID:19440762.

2.1.5 Aufbau der Infrastruktur

Verbinden Sie alle teilnehmenden Komponenten dieser Lösung miteinander.

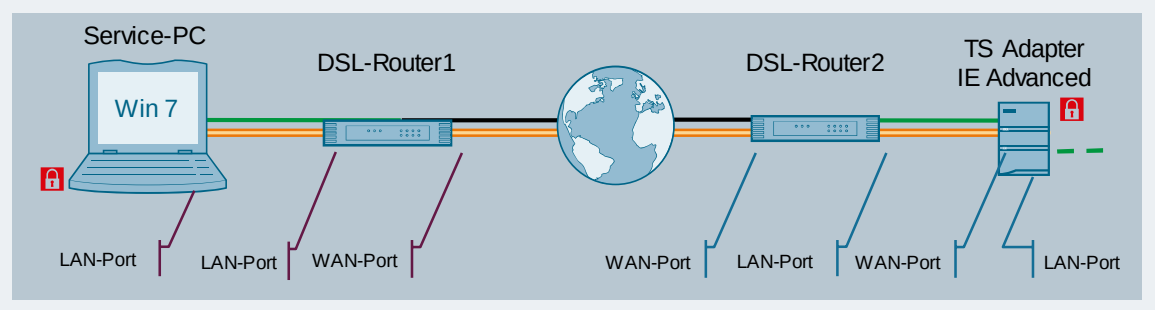


Tabelle 2-2

Komponente	Lokaler Port	Partner	Partner Port
Service-PC	LAN-Port	DSL- Router1	LAN-Port
TS Adapter IE	WAN-Port	DSL- Router2	LAN-Port
TS Adapter IE	LAN-Port	z. B. ein Automatisierungsnetzwerk (in dieser Lösung nicht vorhanden)	

2.2 Inbetriebnahme der Fernwartung

2.2.1 Vorbereitung

Verwendete Komponenten

Für diese Lösung werden die Komponenten TS Adapter IE Advanced und ein Standard Internet Browser verwendet.

Physikalische Verbindung zwischen PC und TS Adapter IE Advanced

Verbinden Sie den Service-PC mit einem freien LAN-Port des TS Adapter IE Advanced und ändern Sie die Netzeinstellung am Service-PC wie folgt:

IP-Adresse: 172.22.80.100

Subnetzmaske: 255.255.255.0

Öffnen des Web-Interface

Die Parametrierung des TS Adapters IE Advanced erfolgt im Direktanschluss mit einem Standard Internet Browser.

1. Geben Sie im Adressfeld des Browsers in der Form **https://172.22.80.2:5443** die IP-Adresse des TS Adapter IE Advanced an. Achten Sie speziell darauf, den Port 5443 anzugeben, unter dem das Web-Interface erreichbar ist.

2. Geben Sie Benutzernamen und Kennwort an. Wenn Sie sich das erste Mal oder nach Setzen auf Werkeinstellung anmelden, sind die Login-Daten wie folgt festgelegt:
   Name: **Administrator**
   Password: **admin**

3. Klicken Sie auf „Login".

Ergebnis:
Das Web-Interface des TS Adapters wird geöffnet.

2.2.2 Erstkonfiguration des TS Adapter IE Advanced

Bei der Erstanmeldung werden Sie anhand einer Guided Tour durch alle Einstellungen geführt, die zur Inbetriebnahme des TS Adapter IE Advanced erforderlich sind.

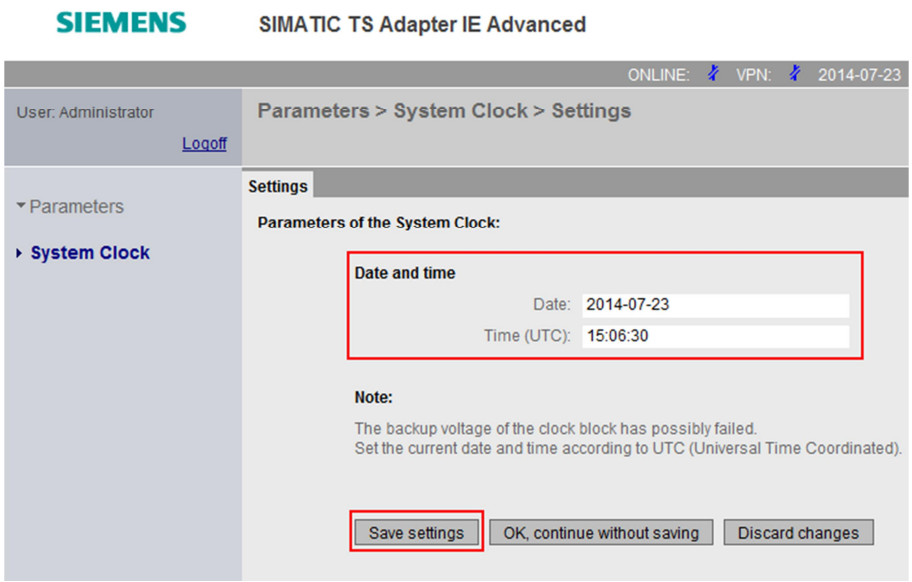
Im Folgenden finden Sie die einzelnen Schritte der Guided Tour aufgelistet und erklärt.

Systemzeit

Die Systemzeit wird u. a. zur Generierung von Zertifikaten verwendet. Stellen Sie die Uhrzeit wie folgt ein:

1. Tragen Sie die Parameter der Systemzeit ein. Die Uhrzeit muss im UTC-Format eingegeben werden.

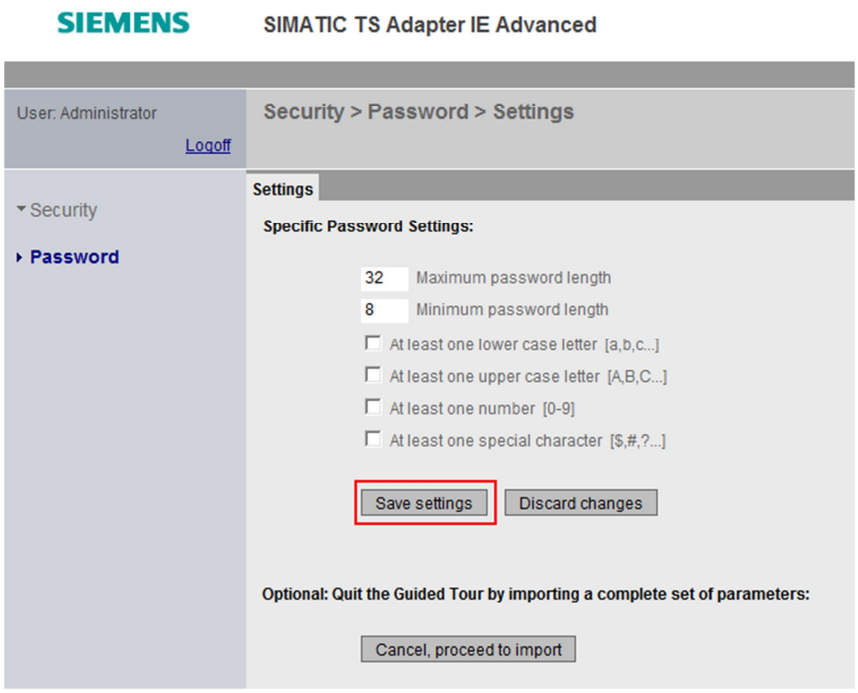
2. Übernehmen Sie die Einstellungen mit „Einstellungen übernehmen“ („Save Settings“).



Spezifische Kennwortregeln

Jedes Kennwort, dass im TS Adapter neu angelegt oder geändert wird, muss bestimmten Richtlinien entsprechen. Diese Regeln wie z.B. die Mindestlänge und die Mindestanzahl von Kennwortbestandteilen können Sie im Web-Interface des TS Adapter IE Advanced selbst festlegen.

1. Definieren Sie die Vorgaben für die Kennworteingabe.

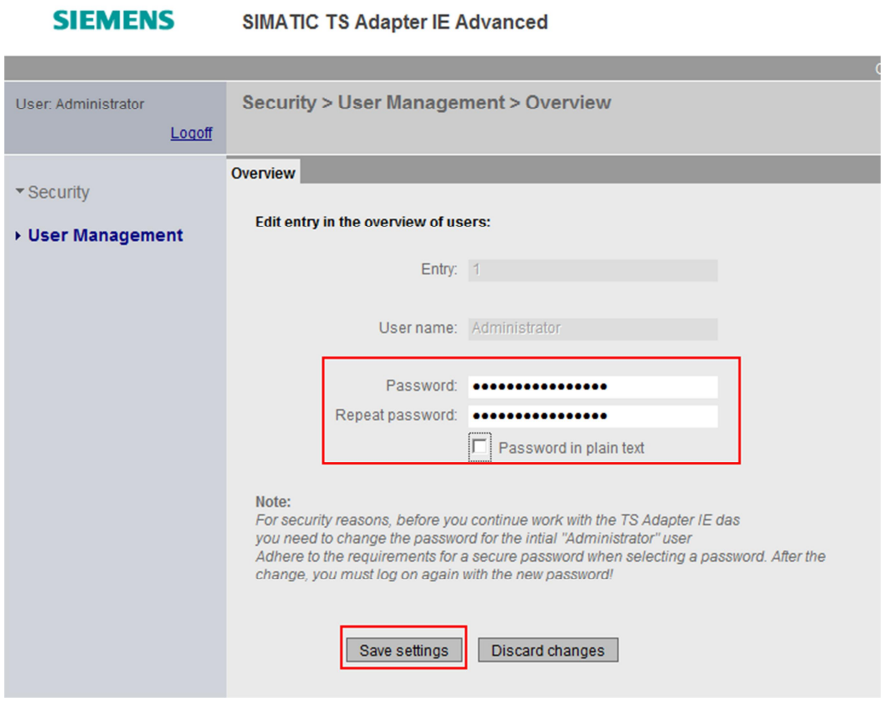


2. Übernehmen Sie die Einstellungen mit „Einstellungen übernehmen“ („Save Settings“).

Administrator-Passwort ändern

Bei der ersten Anmeldung werden Sie aufgefordert, das voreingestellte Kennwort des Standard-Benutzers „Administrator" durch ein neues Kennwort zu ersetzen.

1. Tragen Sie im Feld „Passwort“ ein neues Administrator-Passwort ein und bestätigen dieses durch erneute Eingabe.
   Beachten Sie bei der Kennwortwahl, dass das Kennwort den Regeln für die Kennwortprüfung ("Spezifische Kennwortregeln") entspricht.

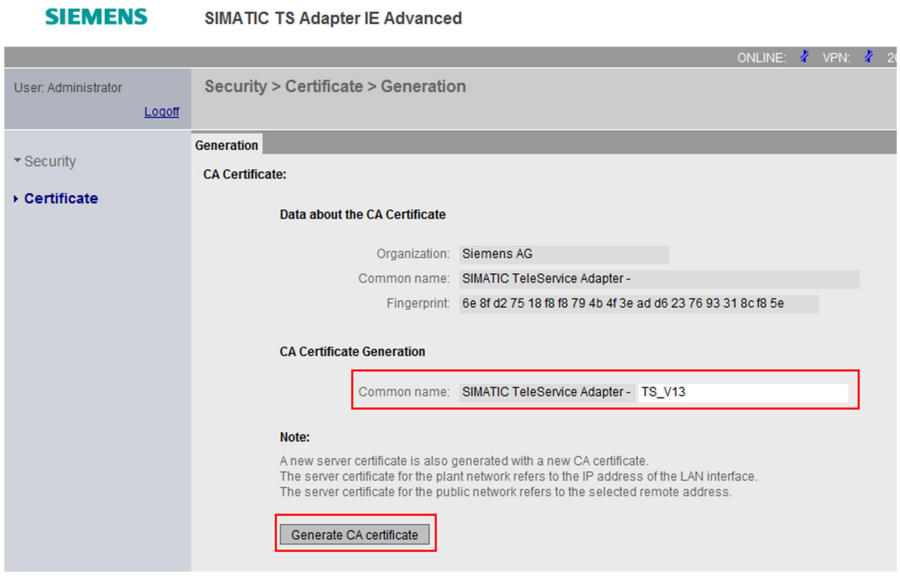


2. Übernehmen Sie die Einstellungen mit „Einstellungen übernehmen“ („Save Settings“).

CA-Zertifikatgenerierung

Als letzten Schritt der Guided Tour werden Sie aufgefordert, ein neues CA-Zertifikat zu generieren. Das voreingestellte CA-Zertifikat wird dadurch überschrieben.

1. Ergänzen Sie unter „Allgemeiner Name“ („Common Name“) den Namen bei „SIMATIC TeleServiceAdapter“. Dieser Name wird im CA-Zertifikat als Antragsteller und Ausstellerinformation hinterlegt.



2. Generieren Sie das CA-Zertifikat über die Schaltfläche „CA Zertifikat generieren“ („Generate CA certificate“).

Ergebnis

Die Erstkonfiguration des TS Adapters ist abgeschlossen.

2.2.3 Parametrierung des Fernzugriffs

Vorbereitung

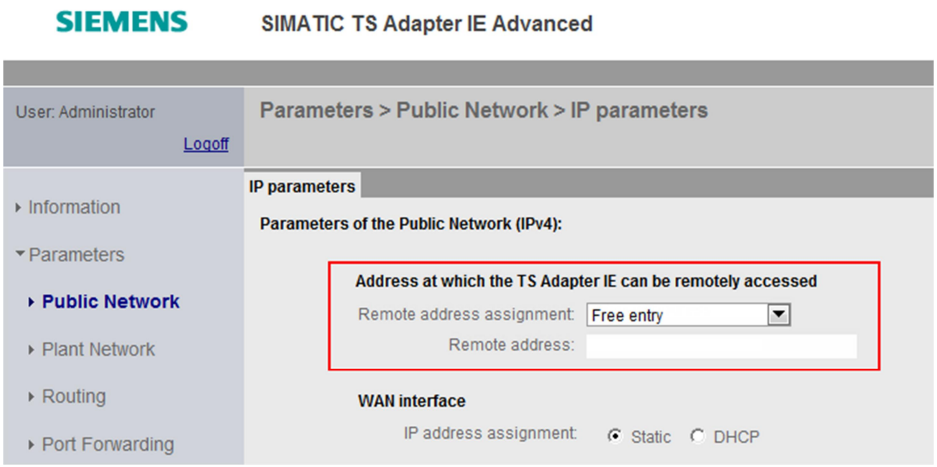
Öffnen Sie das Web-Interface des TS Adapter IE Advanced.
Orientieren Sie sich hierbei an der Anleitung aus Kapitel 2.2.1 (Vorbereitung).

Melden Sie sich als Administrator und mit dem neuen Passwort (siehe Kapitel 2.2.2) an.

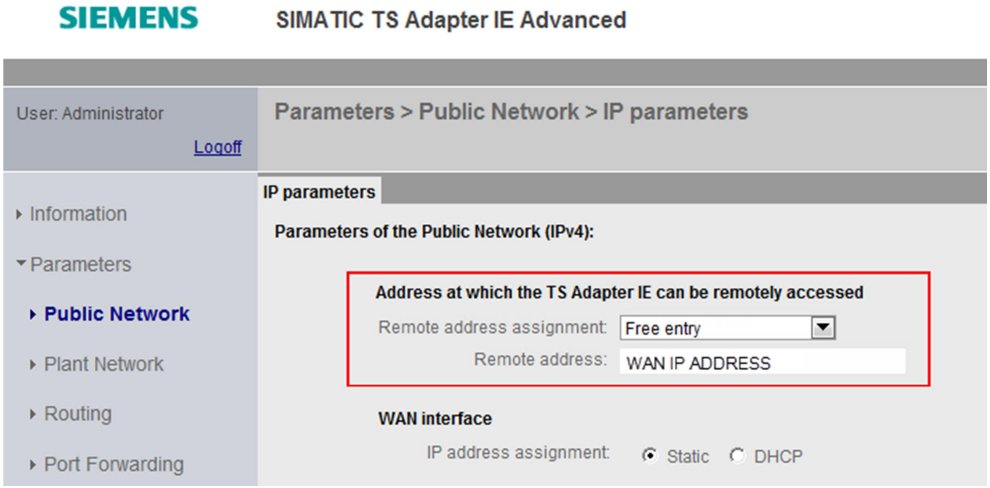
IP Parameter Öffentliches Netz

Im Folgenden wird festgelegt, wie der TS Adapter IE Advanced aus der Ferne erreicht werden kann.

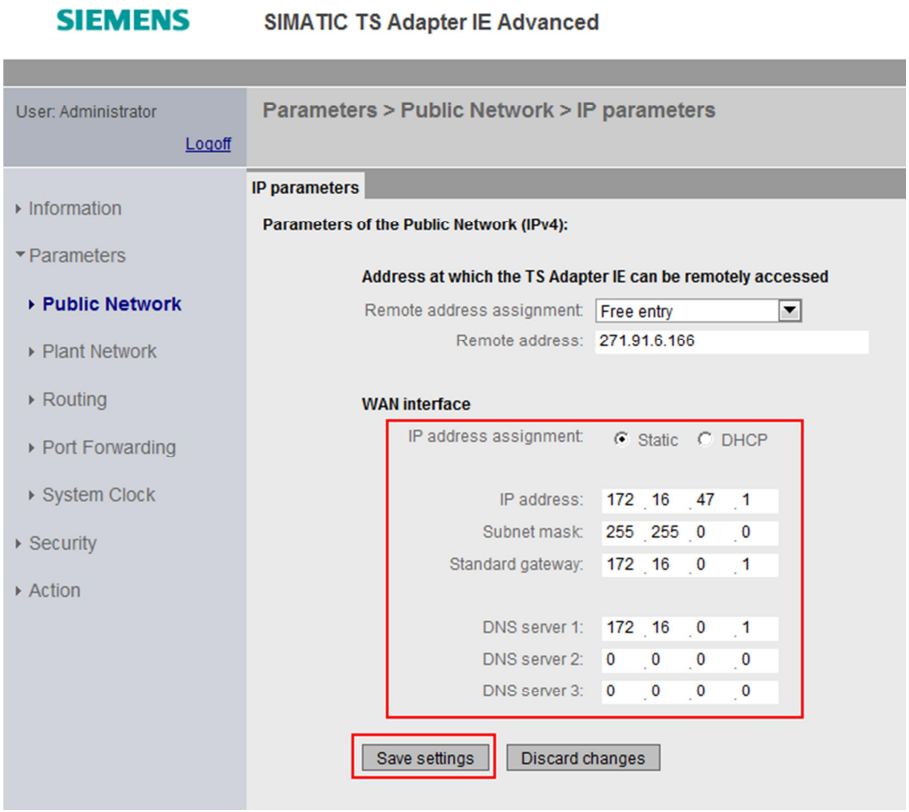
1. Gehen Sie in der Navigationsleiste zu „Parameter“ > „Öffentliches Netzwerk“ („Parameters“ > „Public Network“). Wählen Sie als Remote-Zugang „Freie Eingabe“ („Free Entry“).



2. Tragen Sie bei „Remote-Adresse“ („Remote-Address“) die **statische WAN-IP-Adresse** Ihres DSL-Zugangs ein.



3. Wählen Sie für die WAN-Schnittstelle bei „IP-Adressvergabe“ („IP address assignment“) „statisch“ („static“) und tragen Sie die **IP-Adresse für die WAN-Schnittstelle** gemäß Tabelle 2-1 ein.
   Als DNS-Server verwenden Sie die IP-Adresse der LAN-Schnittstelle des DSL-Routers.

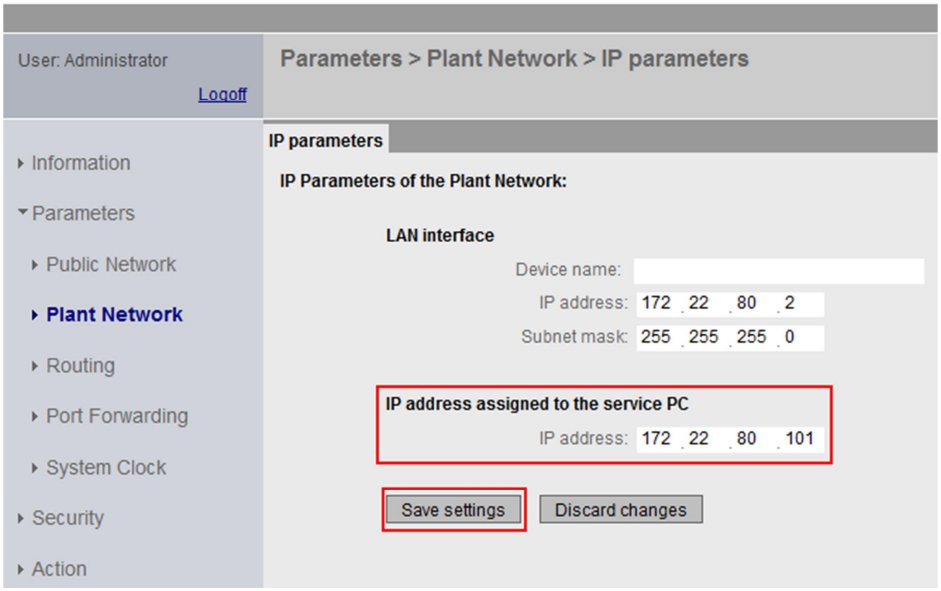


4. Übernehmen Sie die Einstellungen mit „Einstellungen übernehmen“ („Save Settings“).

IP Parameter Anlagennetz

Im Folgenden wird festgelegt, welche IP-Adresse der Service-PC beim Aufbau der VPN-Verbindung zugewiesen bekommt.

1. Gehen Sie in der Navigationsleiste zu „Parameter“ > „Anlagennetz“ > „IP Parameter“ („Parameters“ > „Plant Network“ > „IP parameters“). Tragen Sie eine beliebige, freie IP-Adresse ein, die sich im gleichen Subnetz wie das Anlagennetz (Automatisierungsnetz an der LAN-Schnittstelle des TS Adapters) befindet.

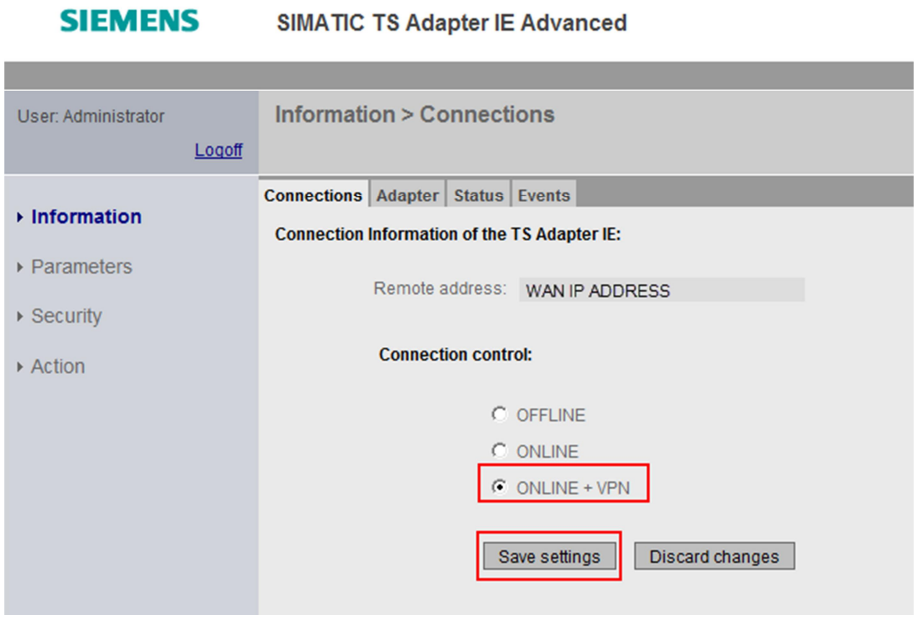


2. Übernehmen Sie die Einstellungen mit „Einstellungen übernehmen“ („Save Settings“).

Verbindungsparameter

Der Zugriff auf den TS Adapter über die WAN-Schnittstelle kann - je nach Anwendung - unterschiedlich projektiert werden. Für dieses Beispiel wird eine Fernwartung über VPN gewünscht.
Gehen Sie zur Freigabe wie folgt vor:

1. Gehen Sie in der Navigationsleiste zu „Information“ > „Verbindungen“ („Information“ > „Connections“). Ändern Sie die Verbindungssteuerung für die WAN-Schnittstelle auf „Online+VPN“.



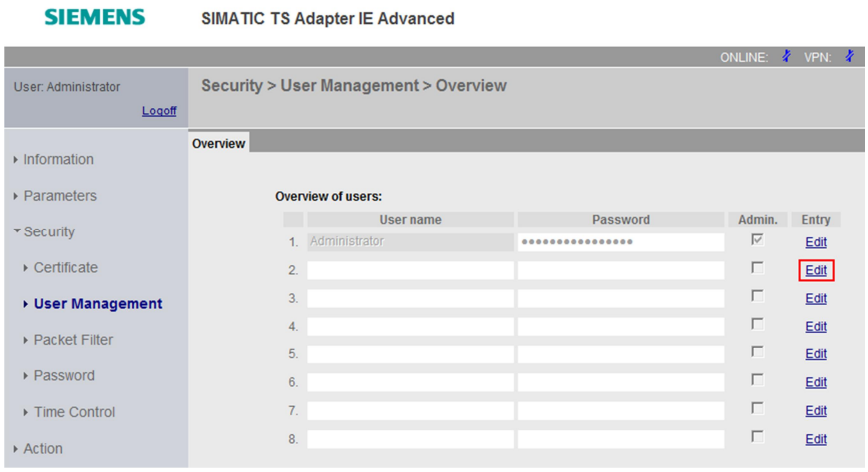
2. Übernehmen Sie die Einstellungen mit „Einstellungen übernehmen“ („Save Settings“).

Benutzer anlegen

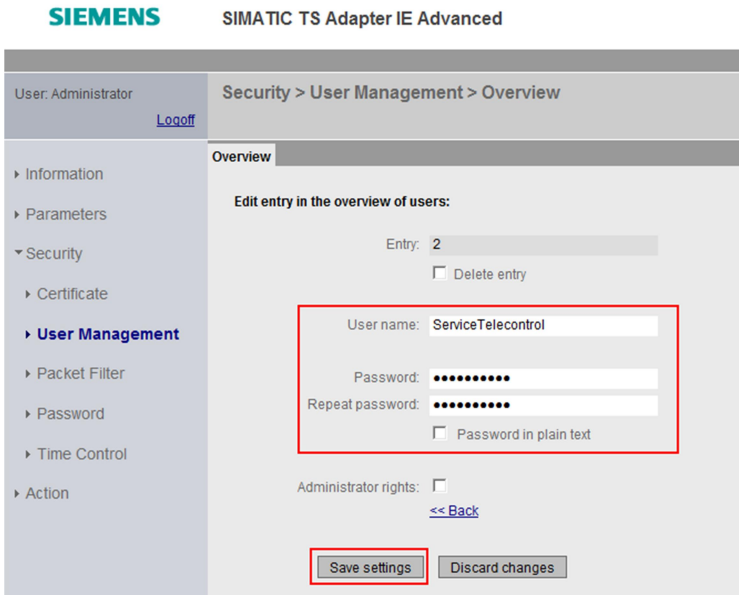
Damit der Service-PC eine VPN-Verbindung zum TS Adapter IE Advanced aufbauen kann, ist ein Login mit einem Benutzername und einem Kennwort nötig. Bei der Erstkonfiguration ist lediglich der Benutzer „Administrator“ im TS Adapter eingetragen. Da dieser keine VPN-Verbindung aufbauen kann, ist ein weiterer Benutzereintrag nötig.

Gehen Sie für das Anlegen eines neuen Benutzers wie folgt vor:

1. Gehen Sie in der Navigationsleiste zu „Sicherheit“ > „Benutzerverwaltung“ („Security“ > „User Management“). Legen Sie einen weiteren Benutzer über „Bearbeiten“ („Edit“) an.



2. Tragen Sie in die entsprechenden Eingabefelder einen Benutzername und ein Kennwort ein. Bestätigen Sie das Kennwort.
Beachten Sie bei der Kennwortwahl, dass das Kennwort den Regeln für die Kennwortprüfung ("Spezifische Kennwortregeln") entspricht.



3. Übernehmen Sie die Einstellungen mit „Einstellungen übernehmen“ („Save Settings“).

Ergebnis
Ein neuer Benutzer mit der Berechtigung zum Aufbau eine VPN-Verbindung wurde angelegt.

CA-Zertifikat exportieren

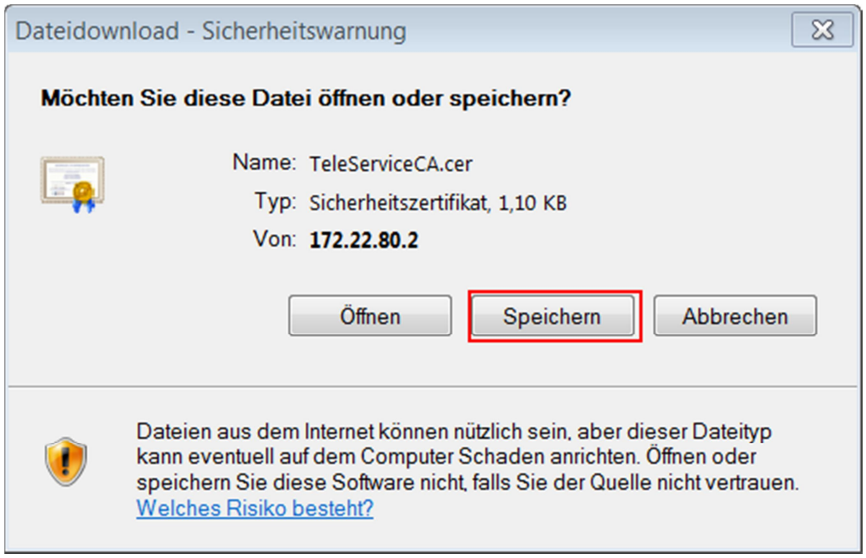
Um den TS Adapter IE Advanced als Verbindungspartner gegenüber dem Service-PC eindeutig zu identifizieren, wird vom TS Adapter IE Advanced ein CA-Zertifikat mit einem eindeutigen Fingerabdruck generiert
(siehe Kapitel 2.2.2 (Erstkonfiguration des TS Adapter IE Advanced).

Für den Aufbau einer VPN-Verbindung ist es zwingend erforderlich, dieses CA-Zertifikat im Windows-Zertifikatsspeicher (Lokaler Computer) zu hinterlegen.

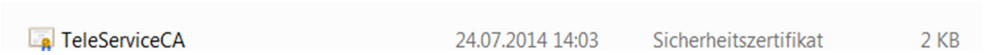
Gehen Sie für den Export des Zertifikats wie folgt vor:

1. Gehen Sie in der Navigationsleiste zu „Sicherheit“ > „Zertifikate“ („Security“ > „Certificates“). Exportieren Sie das Zertifikat über die Schaltfläche „CA Zertifikat exportieren“ („Exporting CA certificate“).

2. Speichern Sie das Zertifikat in Ihrem Projektordner ab.



3. Das CA-Zertifikat des TS Adapters IE Advanced wird im Projektordner abgelegt.



Ergebnis
Die Parametrierung des TS Adapters für die Fernwartung ist abgeschlossen.

2.2.4 Abschlussarbeiten

Service-PC

Für den Aufbau einer VPN-Verbindung ist es zwingend erforderlich, das vom TS Adapter generierte CA-Zertifikat im Windows-Zertifikatsspeicher (Lokaler Computer) zu hinterlegen. Orientieren Sie sich hierbei an der Anleitung aus Kapitel 4 (Anhang: Umgang mit CA-Zertifikaten).

Infrastruktur

1. Verbinden Sie den Service-PC mit der LAN-Schnittstelle des DSL-Router1.

2. Vergeben Sie der Netzwerkkarte die benötigte Netzkonfiguration nach Tabelle 2-1.

3. Tragen Sie in allen Geräten, die sich am LAN-Port des TS Adapter IE Advanced befinden, das Standard-Gateway (IP-Adresse des LAN-Ports) ein.

2.3 Aufbau der VPN-Verbindung

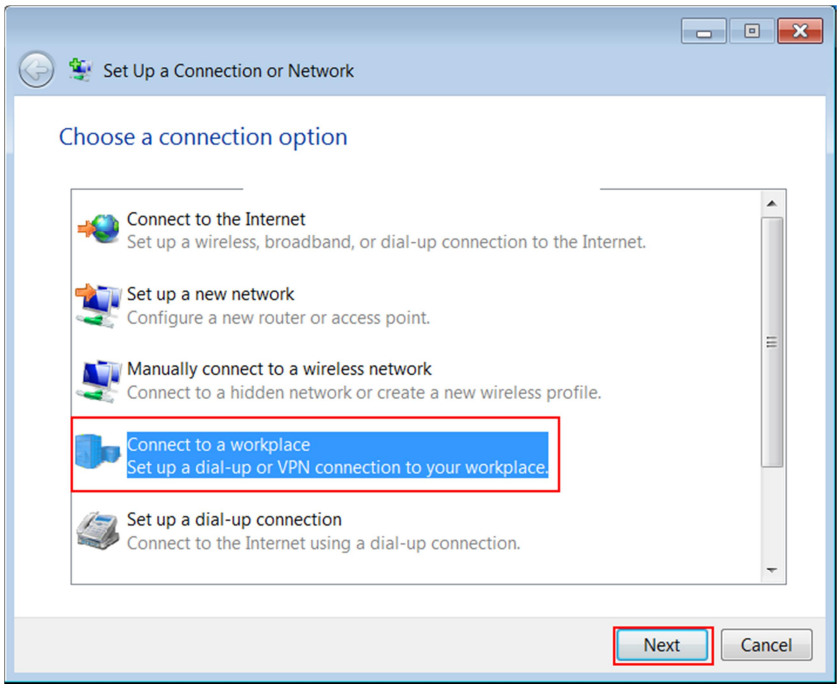
Ist der TS Adapter IE Advanced für die Fernwartung parametriert und die Infrastruktur gemäß Tabelle 2-2 verbunden, kann der Service-PC (VPN-Client) den VPN-Tunnel zum TS Adapter IE Advanced (VPN-Server) initialisieren.

Gehen Sie für den Aufbau einer Fernverbindung zum TS Adapter IE Advanced folgendermaßen vor:

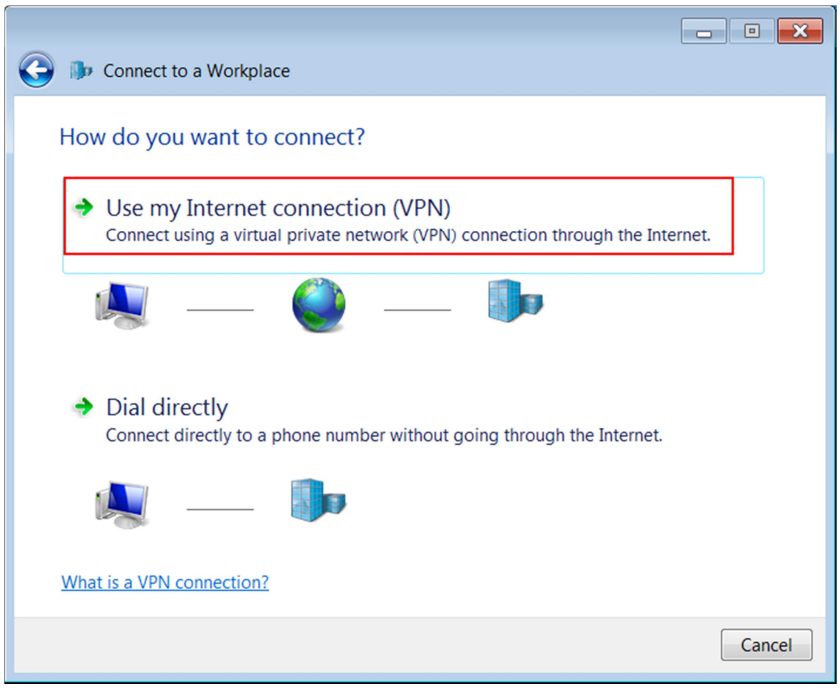
1. Öffnen Sie auf dem Service-PC (Windows 7) die Systemsteuerung (Control Panel).

2. Geben Sie in der Suchleiste „Netzwerk" („network) ein und wählen Sie „Eine Verbindung oder ein Netzwerk einrichten" („Set up a new connection or network").

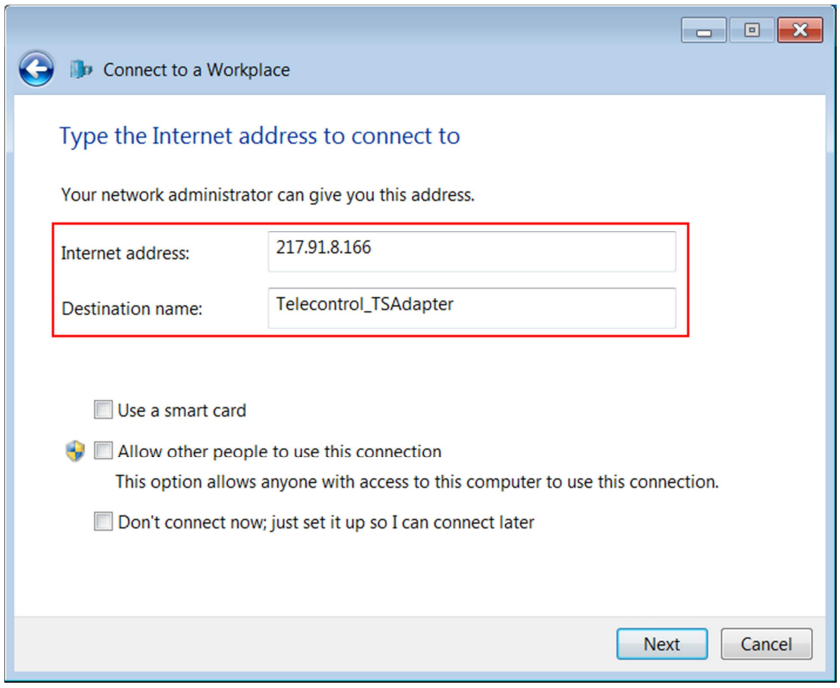
3. Wählen Sie die Option „Verbindung mit einem Arbeitsplatz herstellen" („Connect to a workplace") und klicken Sie auf („Weiter") („Next").



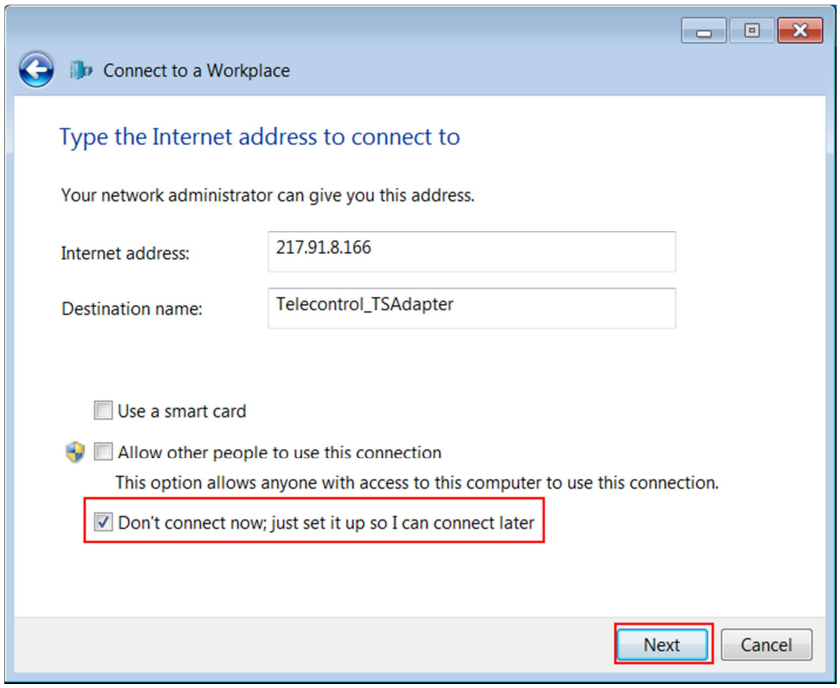
4. Wählen Sie „Die Internetverbindung (VPN) verwenden“ („Use my Internet connection (VPN)“).



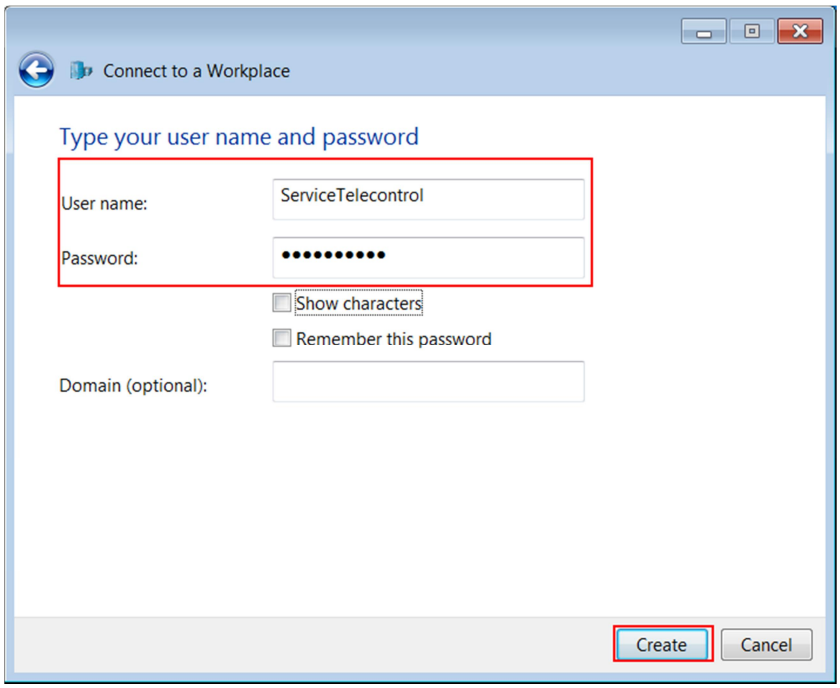
5. Tragen Sie die statische WAN-IP-Adresse des DSL-Routers2 (DSL-Router des zu kontaktierenden TS Adapter IE Advanced) sowie ein Namen für die Verbindung in die entsprechenden Eingabefelder ein.



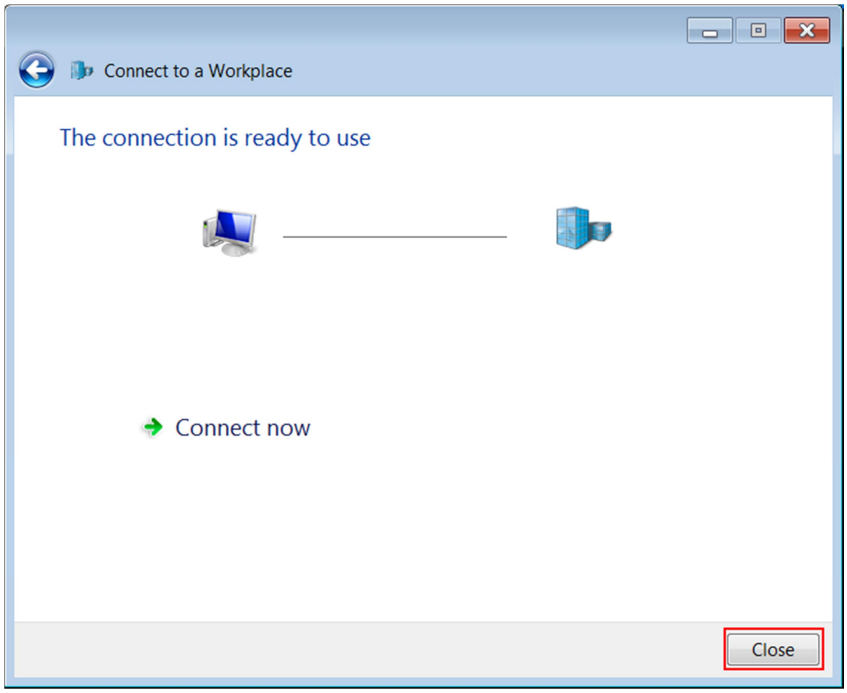
6. Aktivieren Sie die Option „Jetzt nicht verbinden, nur für spätere Verwendung einrichten“) („Don't connect; just set it up so I can connect later“) und klicken Sie auf („Weiter“) („Next).



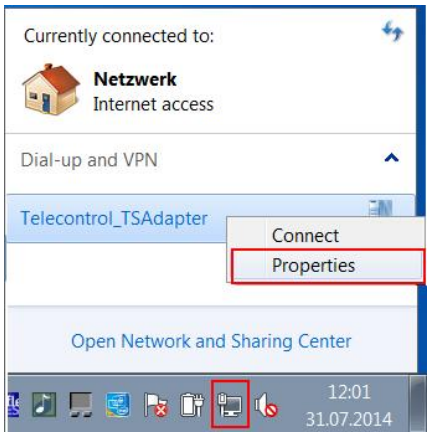
7. Geben Sie den Benutzername und das zugehörige Kennwort des neu angelegten Benutzers (siehe Seite 21) in die entsprechenden Eingabefelder ein.
Klicken Sie auf „Erstellen“ („Create“).



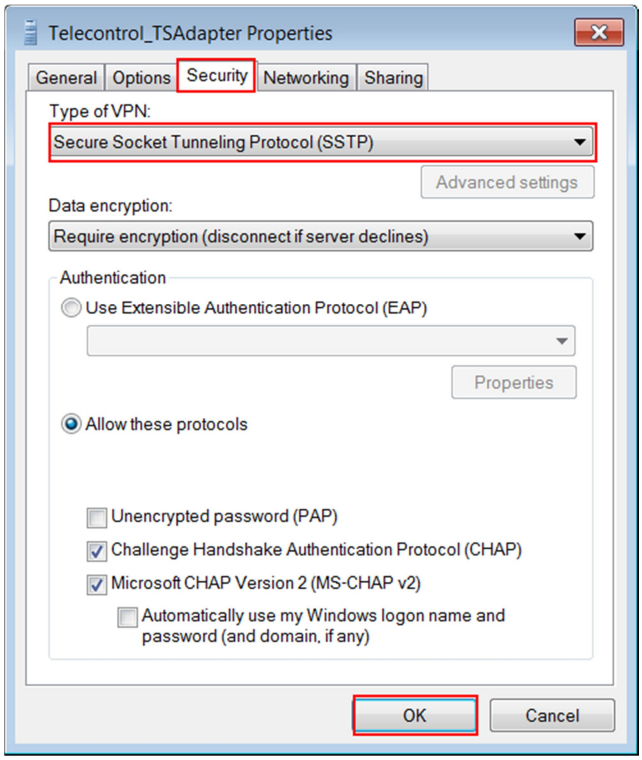
8. Schließen Sie den Dialog mit „Schließen“ („Close“).



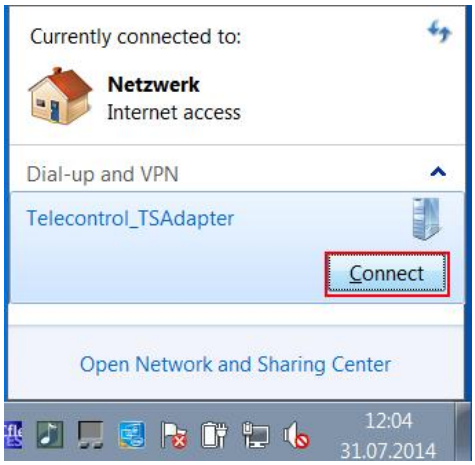
9. Klicken Sie auf das Netzwerk-Symbol im SysTray. Die neue Verbindung wird unter „Einwähl- und VPN-Netzwerke“ („Dial-up and VPN“) angezeigt.
Markieren Sie die neue Verbindung und öffnen Sie über „Rechte Maustaste“ > „Eigenschaften“ („Properties“) den entsprechenden Dialog.



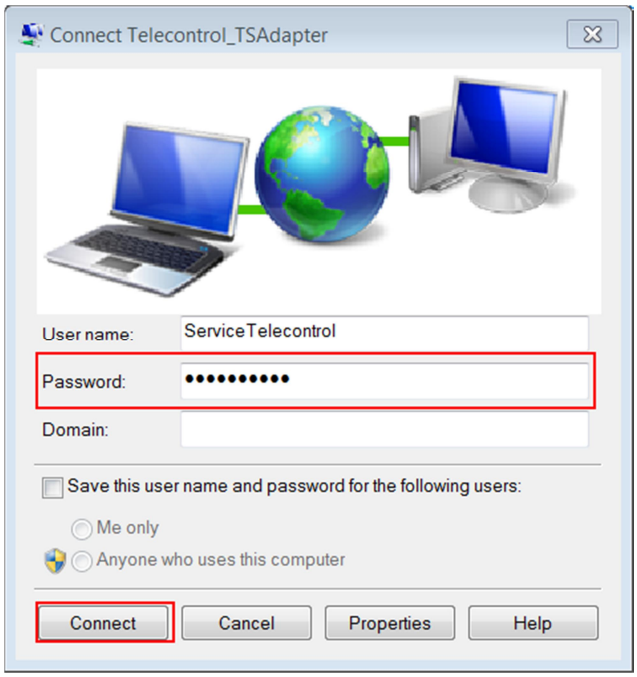
10. Wechseln Sie in das Register „Sicherheit“ („Security“) und wählen Sie als VPN-Typ das „Secure Socket Tunnelling-Protokoll (SSTP)“ („Secure Socket Tunneling Protocol (SSTP)“).
Schließen Sie die Eigenschaften mit „OK“.



11. Klicken Sie erneut auf das Netzwerk-Symbol im SysTray und markieren Sie die neue Verbindung. Klicken Sie auf „Verbinden“ („Connect“), um die Fern-Verbindung zum TS Adapter IE Advanced aufzubauen.



12. Geben Sie das Kennwort für den Benutzer (siehe Seite 21) ein und starten Sie den Verbindungsaufbau mit „Verbinden“ („Connect“).



Ergebnis

Die VPN-Verbindung zum TS Adapter wird aufgebaut. Sobald die VPN-Verbindung zustande gekommen ist, wird der Dialog geschlossen. Als Status erscheint die Meldung: „Verbunden" („Connected“).

Hinweis

Ist kein Verbindungsaufbau möglich, versuchen Sie, die Fehlerursache zu ermitteln.

Nähere Informationen und Hilfestellung zur Fehlersuche finden Sie im entsprechende Kapitel im TIA-Handbuch unter diesem Link:

https://www.automation.siemens.com/mdm/default.aspx?DocVersionId=63972520715&Language=de-DE&TopicId=58521033355

3 Tunnelfunktion testen

Nach Kapitel 2 ist die Inbetriebsetzung der Konfiguration abgeschlossen und der Service-PC und der TS Adapter IE Advanced haben einen VPN-Tunnel zur sicheren Kommunikation aufgebaut.

Die aufgebaute Tunnelverbindung können Sie - wie nachfolgend beschrieben - mit einem Ping-Kommando an einen internen Teilnehmer durchführen.

Alternativ können Sie auch andere Methoden für den Test der Konfiguration verwenden (z. B. durch Öffnen der internen Webseite bei Verwendung einer PROFINET-CPU).

1. Rufen Sie auf dem Service-PC in der Startleiste den Menübefehl „Start" > „Alle Programme" > „Zubehör" > „Eingabeaufforderung" auf.

2. Geben Sie in die Kommandozeile des aufgeblendeten Fensters „Eingabeaufforderung", an der Cursor-Position, den Befehl „ping <IP-Adresse des internen Teilnehmers der Gegenstelle>" ein.

Ergebnis
Sie erhalten eine positive Antwort des internen Teilnehmers.

Hinweis Bei Windows kann die Firewall standardmäßig so eingestellt sein, dass Ping-Kommandos nicht passieren können. Sie müssen ggf. die ICMP-Dienste vom Typ „Request" und „Response" freischalten.

4 Anhang: Umgang mit CA-Zertifikaten

4.1 CA-Zertifikate löschen

Gehen Sie zum Löschen vorhandener CA-Zertifikate folgendermaßen vor:

1. Melden Sie sich als Administrator am System an.

2. Öffnen Sie die Windows-Zertifikatsverwaltung auf Ihrem PG/PC mit Hilfe der Microsoft® Management Console.

3. Klicken Sie dazu auf „Start", tragen Sie im Suchfeld **mmc** ein und drücken Sie die EINGABETASTE.
   Die Konsole öffnet sich.

4. Klicken Sie im Menü „Datei" („File“) auf „Snap-In hinzufügen/entfernen..." („Add/Remove Snap-In…“).
   Das Dialogfeld zur Snap-In-Auswahl öffnet sich.

5. Doppelklicken Sie in der Liste „Snap-In" auf „Zertifikate" (“Certificates“) und wählen Sie im anschließenden Dialog „Computerkonto" („Computer account“) aus.

6. Wählen Sie im folgenden Dialog den Eintrag „Lokaler Computer" („Local Computer“) aus und klicken Sie auf „Fertig stellen" („Finish“) und auf „OK".
   Der Konsolenstamm öffnet sich und zeigt den Ordner „Zertifikate (Lokaler Computer)" („Certificates (Local Computer)“) an.

7. Öffnen Sie den angezeigten Ordner „Zertifikate (Lokaler Computer)" („Certificates (Local Computer)“) und klicken Sie auf „Vertrauenswürdige Stammzertifizierungsstellen" („Trusted Root Certification Authorities“).

8. Öffnen Sie den Ordner „Zertifikate" („Certificates“), wählen Sie das gewünschte CA-Zertifikat aus klicken Sie im Kontextmenü auf „Löschen" („Delete“).

9. Bestätigen Sie die nachfolgende Abfrage mit „Ja" („Yes“).

Ergebnis
Das ausgewählte CA-Zertifikat wird aus der Liste der verfügbaren Zertifikate gelöscht.

4.2 CA-Zertifikaten installieren

Gehen Sie für die Installation eines CA-Zertifikats folgendermaßen vor:

1. Melden Sie sich als Administrator am System an.

2. Öffnen Sie die Windows-Zertifikatsverwaltung auf Ihrem PG/PC mit Hilfe der Microsoft® Management Console.

3. Klicken Sie auf „Start", tragen Sie im Suchfeld **mmc** ein und drücken Sie die EINGABETASTE.
   Die Konsole öffnet sich.

4. Klicken Sie im Menü „Datei" („File“) auf „Snap-In hinzufügen/entfernen..." („Add/Remove Snap-In…“).
   Das Dialogfeld zur Snap-In-Auswahl öffnet sich.

5. Doppelklicken Sie in der Liste „Snap-In" auf „Zertifikate" (“Certificates“) und wählen Sie im anschließenden Dialog „Computerkonto" („Computer account“) aus.

6. Wählen Sie im folgenden Dialog den Eintrag „Lokaler Computer" („Local Computer“) aus und klicken Sie auf „Fertig stellen" („Finish“) und auf „OK".
   Der Konsolenstamm öffnet sich und zeigt den Ordner „Zertifikate (Lokaler Computer)" („Certificates (Local Computer)“) an.

7. Öffnen Sie den angezeigten Ordner „Zertifikate (Lokaler Computer)" („Certificates (Local Computer)“) und klicken Sie auf „Vertrauenswürdige Stammzertifizierungsstellen" („Trusted Root Certification Authorities“).

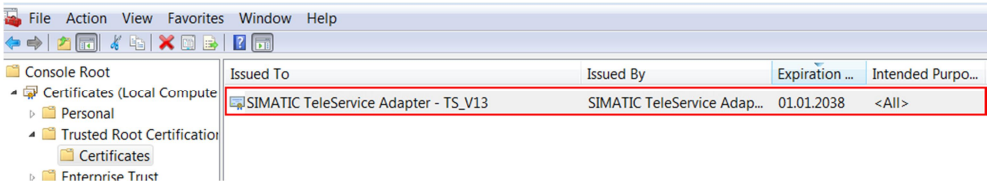
8. Klicken Sie auf den Ordner „Zertifikate" („Certificates“) und rufen Sie über das Kontextmenü den Befehl „Aktion“ > „Alle Aufgaben" > „Importieren..." („Action“ > „All Tasks“ > „Import…“) auf.

9. Beachten Sie die im Dialog „Zertifikat - Import-Assistent" („Certificate - Import-Assistent") angezeigten Informationen und klicken Sie auf „Weiter" („Next“).

10. Klicken Sie im nachfolgenden Dialog auf „Durchsuchen ..." („Search…“), wählen Sie das gewünschte CA-Zertifikat aus und übernehmen Sie dieses mit „Öffnen“ („Open“).

11. Klicken Sie zwei Mal auf „Weiter" („Next“) und anschließend auf „Fertig stellen" („Finish“), um das CA-Zertifikat zu installieren.

Ergebnis
Das ausgewählte CA-Zertifikat wird an der angegebenen Stelle im Windows-Zertifikatsspeicher installiert.



5 Historie

Tabelle 5-1

Version	Datum	Änderung
V1.0	09/2014	Erste Ausgabe