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.

Weitergabe oder Vervielfältigung dieser Applikationsbeispiele oder Auszüge daraus sind nicht gestattet, soweit nicht ausdrücklich von Siemens Industry Sector zugestanden.

Securityhinweise 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 <u>http://support.automation.siemens.com</u>.

Inhaltsverzeichnis

Gewä	Gewährleistung und Haftung2					
1	Aufgabe	enstellung und Lösung	4			
	1.1 1.2 1.3	Aufgabe Lösungsmöglichkeit Merkmale der Lösung	4 4 5			
2	Konfigu	ration und Projektierung	6			
	2.1 2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.2 2.2.1 2.2.2 2.2.2 2.2.3 2.2.4 2.3	Einrichten der Umgebung Erforderliche Komponenten und IP-Adressenübersicht Service-PC DSL-Zugang beim TS Adapter IE Advanced (DSL-Router2) TS Adapter IE Advanced Aufbau der Infrastruktur Inbetriebnahme der Fernwartung Vorbereitung. Erstkonfiguration des TS Adapter IE Advanced Parametrierung des Fernzugriffs Abschlussarbeiten Aufbau der VPN-Verbindung	6 7 9 . 10 . 11 . 12 . 12 . 13 . 13 . 23 . 24			
3	Tunnelf	unktion testen	. 30			
4	Anhang	: Umgang mit CA-Zertifikaten	. 31			
	4.1 4.2	CA-Zertifikate löschen CA-Zertifikaten installieren	. 31 . 32			
5	Historie		. 33			

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.

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 f
 ür 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.

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:<u>19440762</u> im Online Support heruntergeladen werden.

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 f
 ür 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=6573950 2731&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=65739502 731&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.

▲ ▲ ▲ ► ▲ ▲ 조감 포감 노감 ► ►	Ethernet interface	
□- TSA-IE : 00-1B-1B-13-A0-AA : 172.22.80.2 Device name: T'''''''''''''''''''''''''''''''''	MAC address	00-1B-1B-13-A0-AA
	Assign IP parameter IP address	s
	Su <u>b</u> net mask	255 . 255 . 255 . 0
	Use router	172 . 22 . 80 . 2
	C C Client ID	
	Client ID	My to dudiess
	-Assign Device Name- Device name:	
		Assign Name
	•	4

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

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 dies 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.
- 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

SIEMENS

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").

SIMATIC TS Adapter IE Advanced

	ONLINE: 🥻 VPN: 🦧 2014-07-23
User: Administrator	Parameters > System Clock > Settings
Logoff	
	Settings
▼ Parameters	Parameters of the System Clock:
System Clock	Date and time
	Date: 2014-07-23
	Time (UTC): 15:06:30
	Note: The backup voltage of the clock block has possibly failed.
	Set the current date and time according to UTC (Universal Time Coordinated).
	Save settings OK, continue without saving Discard changes

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.

SIMATIC TS Adapter IE Advanced

1. Definieren Sie die Vorgaben für die Kennworteingabe.

SIEMENS

User: Administrator	Security	y > Password > Settings
<u>L</u>	ogoff	
	Settings	
▼ Security	Settings	
,	Specific P	assword Settings:
▶ Password		
		32 Maximum password length
		8 Minimum password length
		At least one lower case letter [a,b,c]
		At least one upper case letter [A,B,C]
		At least one number [0-9]
		At least one special character [\$,#,?]
		Save settings Discard changes
	Optional: (Quit the Guided Tour by importing a complete set of parameters:
		Cancel, proceed to import

Administrator-Passwort ändern

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

 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.

SIEMENS	SIMATIC	TS Adapter IE A	dvanced	
User: Administrator	Security	> User Manager	nent > Overview	
<u>Loqoff</u>				
▼ Security	Overview			
• User Management	Edit entry i	in the overview of us	ers:	
		Entry:	1	
		User name:	Administrator	
		Password:	•••••	
		Repeat password:	•••••	
			Password in plain text	
	Note: For securit you need t Adhere to l change, yo	y reasons, before you o change the passwo the requirements for a ou must log on again Save settings	continue work with the TS Adapter IE of rd for the intial "Administrator" user secure password when selecting a pa with the new password! Discard changes	das ssword. After the

SIEMENS SIMATIC TS Adapter IE Advanced

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.

	SIEMENS	SIMATIC TS Adapter IE Advanced				
				ONLINE:	🕴 VPN:	4 2
ι	Jser: Administrator	Security > Certificate > Generation				
	Logoff					
		Generation				
	Security	CA Certificate:				
•	Certificate	Data shout the CA Cartificate				
		Data about the CA Certificate				
		Organization: Sie	emens AG			
		Common name: SIM	IATIC TeleService Adapter -			
		Fingerprint: 6e a	8f d2 75 18 f8 f8 79 4b 4f 3e ad	d6 23 76 93 31 8c f8 5e		
		CA Cortificate Constation				
		CA Ceruncale Generation				-
		Common name: SIM	ATIC TeleService Adapter - TS	3_V13		
						Ē
		Note:				
		A new server certificate is also gener The server certificate for the plant ne	rated with a new CA certificate. etwork refers to the IP address o	f the LAN interface.		
		The server certificate for the public ne	etwork refers to the selected rer	mote address.		
		Generate CA certificate				
		Generale OA certificate				

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.

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

User: Administrator	Parameters > Public Network > IP parameters
<u>Loqoff</u>	
	IP parameters
 Information 	Parameters of the Public Network (IPv4):
▼Parameters	
Build in Madeurals	Address at which the TS Adapter IE can be remotely accessed
Public Network	Remote address assignment: Free entry
Plant Network	Remote address:
	WAN interface
▶ Port Forwarding	IP address assignment: IP Static C DHCP

SIEMENS SIMATIC TS Adapter IE Advanced

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



SIEMENS SIMATIC TS Adapter IE Advanced

 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.

User: Administrator	Parameters > Public Network > IF	P parameters
<u>Logoff</u>		
	IP parameters	
Information	Parameters of the Public Network (IPv4):	
 Parameters 		
Public Network	Address at which the TS Adap	Trace can be remotely accessed
	Remote address:	271.91.6.166
Plant Network		
▶ Routing	WAN interface	
Port Forwarding	IP address assignment:	Static C DHCP
 System Clock 	IP address:	172 16 47 1
 Security 	Subnet mask:	255 255 0 0
Action	Standard gateway:	172 16 0 1
ACTION	DNO second (470 46 0 4
	DNS server 1.	172,10,0,1
		0 0 0
	DNO SCIVEL 2.	0 0 0 0

SIEMENS SIMATIC TS Adapter IE Advanced

IP Parameter Anlagennetz

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

 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.

User: Administrator	Parameters > Plant Network > IP	parameters
Logoff		
. Information	IP parameters	
Information	IP Parameters of the Plant Network:	
▼Parameters		
	LAN interface	
Public Network	Device name:	
Plant Network	IP address:	172 22 80 2
	Subnet mask:	255 255 255 0
 Routing 		
Port Forwarding	IP address assigned to the service	vice PC
. Tortronarang	IP address:	172 22 80 101
System Clock		
▹ Security	Save settings Discard ch	nanges
► Action		

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:

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

User: Administrator	Information > Connections
Logoff	
	Connections Adapter Status Events
Information	Connection Information of the TS Adapter IE:
Parameters	Devile diferent
 Security 	Remote address: WAN IP ADDRESS
► Action	Connection control:
	C OFFLINE
	C ONLINE
	ONLINE + VPN
	Save settings Discard changes

SIEMENS SIMATIC TS Adapter IE Advanced

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:

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

SIEMENS	SIMATIC TS A	dapter IE Advanced			
				ONLINE: 🦨	VPN: 🠇
User: Administrator	Security > Us	er Management > Overvi	ew		
Logoff					
	Overview				
 Information 					
 Parameters 	Over	view of users:			
▼ Security		User name	Password	Admin.	Entry
oodanty	1.	Administrator	•••••		Edit
 Certificate 	2.			Г	Edit
• User Management	3.				Edit
 Dasket Filter 	4.				Edit
Packet Filler	5.				Edit
Password	6.				Edit
Time Control	7.			Г	Edit
Action	8.			Г	Edit
▶ Action					

 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.

Security > User Management > Overview User: Administrator <u>Loqoff</u> Overview Information Edit entry in the overview of users: Parameters Entry: 2 Security Delete entry ▶ Certificate User name: ServiceTelecontrol User Management Packet Filter Password: •••••••• Repeat password: •••••••• Password Password in plain text Time Control Administrator rights: 🗖 Action << Back Save settings Discard changes

SIMATIC TS Adapter IE Advanced

SIEMENS

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).

SIMATIC 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:

SIEMENS

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

		ONLINE: 4 VPN: 4
User: Administrator	Security > Certificate > Generation	
Logoff		
	Generation	
Information	CA Certificate:	
 Parameters 	Data about the CA Cartificate	
▼ Security		
	Organization: Siemens A	AG
Certificate	Common name: SIMATIC T	eleService Adapter - TS_V13
 User Management 	Fingerprint: 0c 2c 29 0	a 1b a7 b8 b9 62 29 a7 81 81 02 08 51 c4 1f d9 66
 Packet Filter 	CA Certificate Export	
Password	Exporting CA certificate	
► Time Control		
► Action	CA Certificate Generation	
	Common name: SIMATIC T	eleService Adapter - TS_V13

2. Speichern Sie das Zertifikat in Ihrem Projektordner ab.



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

🔄 TeleServiceCA	24.07.2014 14:03	Sicherheitszertifikat	2 KB
-----------------	------------------	-----------------------	------

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.

		[- • ×
G	🌗 🕪 Connect to a Workpl	ace	
	Type the Internet ad	dress to connect to	
	Your network administrate	or can give you this address.	
	Internet address:	217.91.8.166	
	Destination name:	Telecontrol_TSAdapter	
	Use a smart card		
	Allow other people This option allows	e to use this connection anyone with access to this computer to use this connec	tion.
	Don't connect now	; just set it up so I can connect later	
		Next	Cancel

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).

		- • 🗙
G 🐌 Connect to a Wor	kplace	
Type the Internet	address to connect to	
Your network administr	ator can give you this address.	
Internet address:	217.91.8.166]
Destination name:	Telecontrol_TSAdapter	
Use a smart card	t.	
😽 🔲 Allow other peo	pple to use this connection	
This option allow	ws anyone with access to this computer to use this conne	ection.
Don't connect n	ow; just set it up so I can connect later	
	Nex	t Cancel

 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").

_		
Ip Connect to a Work	kplace	
Type your user na	me and password	
User name:	ServiceTelecontrol	
Password:	•••••	
L	Show characters	
	Remember this password	
Domain (optional):		
		Create Cancel

8. Schließen Sie den Dialog mit "Schließen" ("Close").



 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.

Currently connected to: Netzwerk Internet access	47
Dial-up and VPN	^
Telecontrol_TSAdapter	Connect Properties
Open Network and S	Sharing Center
u Di 💻 🥶 😼 🖬 🗄	12:01

 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".

🖥 Telecontrol_TSAdapter Properties
General Options Security Networking Sharing
Type of VPN:
Secure Socket Tunneling Protocol (SSTP)
Advanced settings
Require encryption (disconnect if server declines)
Authentication
O Use Extensible Authentication Protocol (EAP)
•
Properties
Allow these protocols
Unencounted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and
password (and domain, if any)
OK Cancel

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").

Connect Tele	econtrol_TSAdapter
User name:	ServiceTelecontrol
Password:	•••••
Password: Domain:	•••••
Password: Domain: Save this us Me only	ser name and password for the following users:

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").

Currently connected to:	47
Netzwerk Internet access	
Dial-up and VPN	^
Telecontrol_TSAdapter	Connected
Open Network and S	haring Center
1 D 🗐 🗐 🚱 Gr ta	12:07 31.07.2014

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=6397252 0715&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.
- 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.

H:\>ping 172.2	2.80.6			_	
Ping wird aus Antwort von	geführt für 172 172.22.80.6:]	22.80.6 Bytes=32	mit 32 B∪ Zeit<1ms	ıteş Daten TTL=128	=
Antwort von	172.22.80.6: 1	Bytes=32	Zeit<1ms	TTL=128	
Antwort von	172.22.80.6:]	Bytes=32	Zeit<1ms	TTL = 128 TTL = 128	
HILWOPC VOI	172.22.00.0.1	byces-32	2610/11/12	116-120	
Ping-Statisti	k für 172.22.80	0.6:			
Pakete: G	esendet = 4, Er	npfangen	= 4, Ver]	loren = Ø	
Cos veriu	SC/,	-			

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

🍒 File Action View Favorites	Window Help			
🗢 🔿 💋 🐻 🐇 🐚 🗟				
Console Root	Issued To	Issued By	Expiration	Intended Purpo
Certificates (Local Compute Personal	SIMATIC TeleService Adapter - TS_V13	SIMATIC TeleService Adap	01.01.2038	<all></all>
🔺 🚞 Trusted Root Certification				
Certificates				
Enternrise Trust				

5 Historie

Tabelle 5-1

Version	Datum	Änderung
V1.0	09/2014	Erste Ausgabe