SIEMENS

SIMATIC

Industrie-PC

Konfiguration DiagMonitor OPC UA Server

Produktinformation

Inhaltsverzeichnis

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 nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z. B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter:

Industrial Security (http://www.siemens.de/industrialsecurity)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates 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:

Technical Support (https://support.industry.siemens.com)

Disclaimer für Fremdsoftware-Updates

Dieses Produkt beinhaltet Fremdsoftware. Für Updates/Patches an der Fremdsoftware übernimmt die Siemens AG die Gewährleistung nur, soweit diese im Rahmen eines Siemens Software Update Servicevertrags verteilt oder von der Siemens AG offiziell freigegeben wurden. Andernfalls erfolgen Updates/Patches auf eigene Verantwortung. Mehr Informationen rund um unser Software Update Service Angebot erhalten Sie im Internet unter:

Software Update Service (http://www.automation.siemens.com/mcms/automation-software/de/software-update-service).

Hinweise zur Absicherung von Administrator-Accounts

Einem Benutzer mit Administratorrechten stehen an dem System weitreichende Zugriffs- und Manipulationsmöglichkeiten zur Verfügung.

Achten Sie daher auf eine angemessene Absicherung der Administrator-Accounts, um unberechtigte Veränderungen zu verhindern. Verwenden Sie dazu sichere Passwörter und nutzen einen Standard-Benutzer-Account für den regulären Betrieb. Weitere Maßnahmen wie beispielsweise der Einsatz von Security-Richtlinien sind nach Bedarf anzuwenden.

OPC UA Funktionalität mit DiagMonitor

OPC UA (Open Platform Communications; Unified Architecture) ist die Nachfolgetechnologie von OPC. Sie ermöglicht eine zuverlässige und sichere Datenerfassung und Datenmodellierung sowie Kommunikation zwischen Geräten. OPC UA ist plattformunabhängig und kann verschiedene Protokolle als Kommunikationsmedium verwenden. Diese Funktionalität vereinfacht den Datenaustausch zwischen unterschiedlichen Produkten.

Industrie-PCs können mit Hilfe der OPC UA Funktionalität des DiagMonitors zur Überwachung in SIMATIC-Applikationen eingebunden werden. Jede SIMATIC-Station kann als ein OPC UA Server betrachtet werden. Damit haben Sie die Möglichkeit, Daten des DiagMonitor in eine andere OPC UA-Anwendung zu übertragen, beispielsweise in:

- SIMATIC WinAC
- SIMATIC WinCC
- SIMATIC NET

Die Daten können mit Hilfe dieser Programme dann anwendungsspezifisch visualisiert werden.

OPC UA Server starten oder stoppen

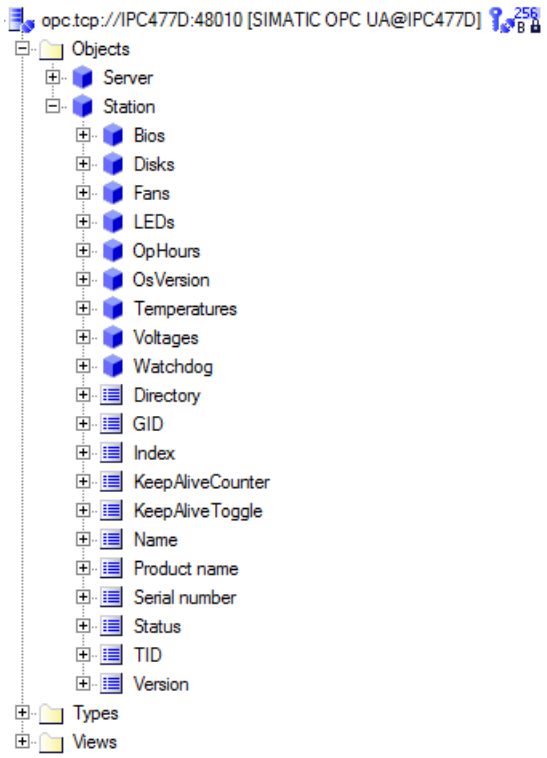
1. Wählen Sie im Management Explorer den Menüpunkt "Extras > OPC UA".
   Der OPC UA Server ist gestartet bzw. gestoppt.

Die Adresse des OPC UA Servers ist wie folgt voreingestellt:

`opc.tcp://[Computername]:48010`

Lautet der Computername der SIMATIC-Station z. B. "IPC477D“ ist der OPC UA Server über die Adresse "opc.tcp://IPC477D:48010“ erreichbar.

Der OPC UA Server stellt die Daten der SIMATIC-Station als Objekt im Ordner "Objects“ bereit.



Hinweis

Wenn Sie einen signierten oder verschlüsselten Sicherheitsmodus für die Verbindung zum OPC UA Server verwenden, stellen Sie sicher, dass die Zertifikate der OPC UA Clients in der Zertifikatsvertrauensliste des OPC UA Servers eingetragen sind.

Weitere Informationen zur Konfiguration des OPC UA Servers, zu Sicherheitsrichtlinien und Zertifikaten finden Sie im Kapitel "OPC UA Server konfigurieren (Seite 3)".

OPC UA Server konfigurieren

Konfigurationsdatei öffnen

1. Wählen Sie aus dem Installationsverzeichnis des DiagMonitor die Konfigurationsdatei des OPC UA Servers "OpcUaConfig.xml“.
2. Öffnen Sie die Konfigurationsdatei mit einem Texteditor.
   Sie benötigen dazu Administrator-Rechte.

Alle im Nachfolgenden beschriebenen Einstellungen sind bereits mit sinnvollen Werten voreingestellt und sollten nur bei Bedarf angepasst werden.

Kommunikationsendpunkt konfigurieren

1. Öffnen Sie die Konfigurationsdatei (Seite 3).
   Als Kommunikationsprotokoll wird nur das Binärprotokoll unterstützt.
   Der entsprechende Kommunikationsendpunkt und dessen Sicherheitseinstellungen sind im XML-Element "`<UaEndpoint>`“ beschrieben.

XML-Element	Beschreibung
`SerializerType`	Zu verwendendes Übertragungsprotokoll. Es wird nur „Binary“ unterstützt.
`Url`	Adresse des Endpunkts. „`[NodeName]`“ kann als Platzhalter für den Computernamen verwendet werden. Folgende Adressen sind möglich: • `opc.tcp://[NodeName]:48010` voreingestellt; der OPC UA Server wird an alle IP Adressen (aller Netzwerkschnittstellen) gebunden. Beispiel: Lautet der Windows Computername der SIMATIC- Station "MB427D-1“ ist der OPC UA Server erreichbar über die Adresse: "opc.tcp:// MB427D-1:48010“ . • `opc.tcp://[IP-Adresse]` Der OPC UA Server wird nur an die angegebene IP Adresse gebunden. Ist die IP-Adresse z. B. "192.168.0.15" so lautet die Adresse: "opc.tcp://192.168.0.15:48010".

<table>
<tr><th>XML-Element</th><th>Beschreibung</th></tr>
<tr><td>SecuritySetting</td><td>
Unterstützte Sicherheitsrichtlinie.
Jede Sicherheitsrichtlinie muss in einem eigenen Element "<SecuritySetting>“ angegeben werden.
<table>
<tr><th>Element</th><th>Beschreibung</th></tr>
<tr><td>SecurityPolicy</td><td>Gibt das zu verwendende Verfahren zum Signieren und Verschlüsseln an. Es sind folgende Werte möglich:
#None
#Basic128Rsa15
#Basic256</td></tr>
<tr><td>MessageSecurityMode</td><td>Gibt an, ob die Verbindung signiert oder signiert und verschlüsselt wird. Die möglichen Werte sind von der Sicherheitsrichtlinie abhängig.
<table>
<tr><th>SecurityPolicy</th><th>Mode</th></tr>
<tr><td>#None</td><td>None</td></tr>
<tr><td>#Basic128Rsa15</td><td>Sign,
SignAndEncrypt</td></tr>
<tr><td>#Basic256</td><td>Sign,
SignAndEncrypt</td></tr>
</table>
</td></tr>
</table>
Beispiel für die Sicherheitsrichtlinie #Basic256 mit Sign und SignAndEncrypt:

<pre>
<SecuritySetting>
 <SecurityPolicy>
 http://opcfoundation.org/UA/SecurityPolicy#Basic256
 </SecurityPolicy>
 <MessageSecurityMode>Sign</MessageSecurityMode>
 <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
</SecuritySetting>
</pre>
Es sind alle momentan unterstützten Sicherheitsrichtlinien voreingestellt.
Möchten Sie eine Richtlinie deaktivieren, müssen Sie die entsprechenden Elemente "<SecuritySetting>“ aus der Konfigurationsdatei entfernen.
</td></tr>
<tr><td>IsVisible</td><td>Gibt an, ob der Endpunkt für OPC UA Clients sichtbar ist.</td></tr>
<tr><td>AutomaticallyTrustAllClientCertificates</td><td>Ist diese Option auf "true“ gesetzt, werden alle Client-Zertifikate automatisch akzeptiert und nicht gespeichert.
Hinweis: Diese Option sollte nur bei aktivierter Benutzerauthentifizierung aktiviert werden.</td></tr>
<tr><td>SecurityCheckOverwrites</td><td>Manche Sicherheitsprüfungen sind in OPC UA optional und werden ggf. von älteren OPC UA Clients nicht unterstützt.
Unter diesem XML-Element können Sie bestimmte Sicherheitsprüfungen deaktivieren. Details zu den einzelnen Optionen finden Sie direkt in der Konfigurationsdatei (Seite 3).</td></tr>
</table>

Speicherung der Zertifikate konfigurieren

Die Pfade für die Speicherung von Zertifikaten werden für jeden Endpunkt über das Element "<`CertificateStore`>" konfiguriert.

Der OPC UA Server des DiagMonitor generiert beim ersten Start automatisch ein Server-Zertifikat. Möchten Sie ein eigenes Zertifikat verwenden oder den Ablagepfad der Zertifikate ändern, können Sie das Element "`<CertificateStore>`" anpassen.

<table>
<tr><th>XML-Element</th><th colspan="2">Beschreibung</th></tr>
<tr><td rowspan="8"><code>OpenSSLStore</code></td><td colspan="2">Datei-basierter Zertifikatspeicher von OpenSSL.
Zertifikate müssen im DER-Format (*.der) gespeichert werden.
Der private Schlüssel muss im PEM-Format (*.pem) gespeichert werden.
Zertifikatsperrlisten müssen im DER-Format (*.crl) oder im PEM-Format (*.pem) gespeichert werden.</td></tr>
<tr><td>Element</td><td>Beschreibung</td></tr>
<tr><td><code>CertificateTrustListLocation</code></td><td>In diesem Ordner kann eine Zertifikatsvertrauensliste gespeichert werden.</td></tr>
<tr><td><code>CertificateRevocationListLocation</code></td><td>In diesem Ordner kann eine Zertifikatsperrliste gespeichert werden.</td></tr>
<tr><td><code>IssuersCertificatesLocation</code></td><td>In diesem Ordner können Ausstellerzertifikate gespeichert werden.</td></tr>
<tr><td><code>IssuersRevocationListLocation</code></td><td>In diesem Ordner können Sperrlisten für Zertifizierungsstellen gespeichert werden.</td></tr>
<tr><td><code>ServerCertificate</code></td><td>Das Zertifikat des Servers im DER-Format. Diese Datei wird beim ersten Start des Servers automatisch generiert. Sie können die Datei auch durch ein eigenes Zertifikat ersetzen.</td></tr>
<tr><td><code>ServerPrivateKey</code></td><td>Der private Schlüssel des Servers im PEM-Format. Diese Datei wird beim ersten Start des Servers automatisch generiert. Wenn Sie ein eigenes Zertifikat nutzen, müssen Sie diese Datei durch den zu Ihrem Zertifikat passenden privaten Schlüssel ersetzen.</td></tr>
</table>

Zusätzlich kann der Ordner für abgelehnte Client-Zertifikate über das Element "`<RejectedCertificatesDirectory>`" angegeben werden.

In diesem Ordner werden alle abgelehnten Zertifikate von OPC-Clients abgelegt und können vom Administrator in die Zertifikatsvertrauensliste kopiert werden.

Benutzeranmeldung konfigurieren

Die unterstützten Anmeldearten für Benutzer werden über das Element "`<UserIdentityTokens>`“ konfiguriert.

XML-Element	Beschreibung
`EnableAnonymous`	Voreingestellt; Benutzer können sich ohne Kennung und Passwort anmelden.
`EnableUserPw`	Voreingestellt; Benutzer können sich über ein Windows-Benutzerkonto anmelden.
`EnableCertificate`	Wird nicht unterstützt.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Konfiguration DiagMonitor OPC UA Server
A5E38926068-AA, 08/2016

SIEMENS

SIMATIC

Industrial PC

Configuration of DiagMonitor OPC UA server

Product Information

Table of contents

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the Internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit:

Industrial Security (http://www.siemens.com/industrialsecurity)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under:

Technical Support (https://support.industry.siemens.com)

Disclaimer for third-party software updates

This product includes third-party software. Siemens AG only provides a warranty for updates/patches of the third-party software, if these have been distributed as part of a Siemens software update service contract or officially released by Siemens AG. Otherwise, updates/patches are undertaken at your own risk. You can find more information about our Software Update Service offer on the Internet at

Software Update Service (http://www.automation.siemens.com/mcms/automation-software/en/software-update-service).

Notes on protecting administrator accounts

A user with administrator privileges has extensive access and manipulation options in the system.

Therefore, ensure there are adequate safeguards for protecting the administrator accounts to prevent unauthorized changes. To do this, use secure passwords and a standard user account for normal operation. Other measures, such as the use of security policies, should be applied as needed.

OPC UA functionality with DiagMonitor

OPC UA (Open Platform Communications; Unified Architecture) is the successor technology of OPC. It enables reliable and secure data acquisition and data modeling as well as communication between devices. OPC UA is platform-independent and can use different protocols as communications medium. This functionality simplifies data exchange between different products.

Industry PCs can be integrated in SIMATIC applications with the help of OPC UA functionality of the DiagMonitor for monitoring. Each SIMATIC station can be seen as an OPC UA server. This enables you to transfer data from the DiagMonitor to a different OPC UA application, for example:

- SIMATIC WinAC
- SIMATIC WinCC
- SIMATIC NET

The data can be visualized for a specific application with the help of these programs.

Starting or stopping the OPC UA server

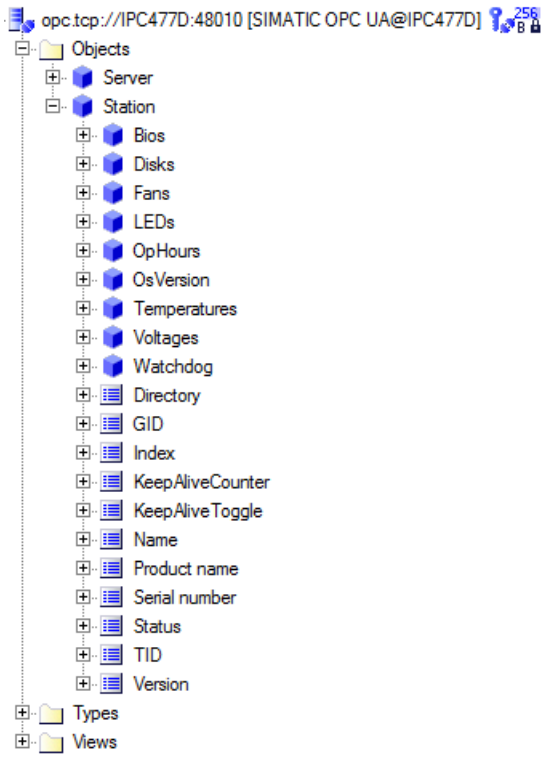
1. Select the menu command "Options > OPC UA" in the Management Explorer.
   The OPC UA server has been started or stopped.

The address of the OPC UA server is preset as follows:

```
opc.tcp://[Computername]:48010
```

If the computer name of the SIMATIC station is e.g. "IPC477D", the OPC UA server can be reached via the address "opc.tcp://IPC477D:48010".

The OPC UA server provides the data of the SIMATIC station as an object in the "Objects" folder.



Note

If you are using a signed or encrypted security mode for the connection to the OPC UA server, ensure that the certificates of the OPC UA clients are entered in the certificate trust list of the OPC UA server.

You can find additional information on the configuration of the OPC UA server, safety policies and certificates in section "Configuring the OPC UA server (Page 9)".

Configuring the OPC UA server

Opening the configuration file

1. Select the configuration file of the OPC UA server "OpcUaConfig.xml" from the installation directory of the DiagMonitor.
2. Open the configuration file with a text editor.
   You need administrator rights for this.

All the settings described in the following are preset with appropriate values and should only be changed if necessary.

Configuring a communications endpoint

1. Open the configuration file (Page 9).
   Only the binary protocol is used as the communications protocol.
   The corresponding communications endpoint and its security settings are described in the XML element "`<UaEndpoint>`".

XML element	Description
`SerializerType`	Transmission protocol to be used. Only "binary" is supported.
`Url`	Address of the end point: "`[NodeName]`" can be used as a wildcard for the computer name. The following addresses are possible: • `opc.tcp://[NodeName]:48010` default: The OPC UA server is linked to all IP addresses (all network interfaces). Example: If the Windows computer name of the SIMATIC station is "MB427D-1", the OPC UA server can be reached via the address: "opc.tcp:// MB427D-1:48010" . • `opc.tcp://[IP-Adresse]` The OPC UA server is only linked to the specified IP address. If the IP address is "192.168.0.15", for example, the address is: "opc.tcp://192.168.0.15:48010".

<table>
<tr><th>XML element</th><th>Description</th></tr>
<tr><td>SecuritySetting</td><td>Supported security policy
Every security policy must be specified in a separate "<SecuritySetting>" element.
<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>SecurityPolicy</td><td>Specifies the signing and encryption methods to be used. The following values are possible:
• #None
• #Basic128Rsa15
• #Basic256</td></tr>
<tr><td>MessageSecurityMode</td><td>Specifies whether the connection is signed or signed and encrypted. The possible values depend on the security policy.
<table>
<tr><th>SecurityPolicy</th><th>Mode</th></tr>
<tr><td>#None</td><td>None</td></tr>
<tr><td>#Basic128Rsa15</td><td>Sign,
SignAndEncrypt</td></tr>
<tr><td>#Basic256</td><td>Sign,
SignAndEncrypt</td></tr>
</table></td></tr>
</table>
Example of the security policy #Basic256 withSign and SignAndEncrypt:

<SecuritySetting>
<SecurityPolicy>
http://opcfoundation.org/UA/SecurityPolicy#Basic256
</SecurityPolicy>
<MessageSecurityMode>Sign</MessageSecurityMode>
<MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
</SecuritySetting>
All currently supported security policies are preset.
If you would like to deactivate a policy, you must remove the corresponding elements <SecuritySetting>" from the configuration file.</td></tr>
<tr><td>IsVisible</td><td>Specified whether the endpoint is visible for OPC UA clients.</td></tr>
<tr><td>AutomaticallyTrustAllClientCertificates</td><td>If this option is set to "true", all the client certificates are automatically accepted and not saved.
Note: This option should only be selected if user authentication is enabled.</td></tr>
<tr><td>SecurityCheckOverwrites</td><td>Some security checks are optional in OPC UA and are possibly not supported by older OPC UA clients.
You can deactivate certain security checks under this XML element. You can find details on the individual options directly in the configuration file (Page 9).</td></tr>
</table>

Configuring saving of certificates

The paths for saving certificates are configured for each endpoint via the "<`CertificateStore`>" element.

The OPC UA server of the DiagMonitor automatically generates a server certificate on the first start. If you would like to use your own certificate or change the storage path, you can change the "`<CertificateStore>`" element.

<table>
<tr><th>XML element</th><th colspan="2">Description</th></tr>
<tr><td rowspan="8"><code>OpenSSLStore</code></td><td colspan="2">File-based certificate store from OpenSSL.
Certificates must be saved in the DER format (*.der).
The private key must be saved in the PEM format (*.pem).
Certificate revocation lists must be saved in the DER (*.crl) or the PEM format (*.pem).</td></tr>
<tr><td>Element</td><td>Description</td></tr>
<tr><td><code>CertificateTrustListLocation</code></td><td>A certificate trust list can be saved in this folder.</td></tr>
<tr><td><code>CertificateRevocationListLocation</code></td><td>A certificate revocation list can be saved in this folder.</td></tr>
<tr><td><code>IssuersCertificatesLocation</code></td><td>Issuer certificates can be saved in this folder.</td></tr>
<tr><td><code>IssuersRevocationListLocation</code></td><td>Revocation lists for certificate authorities can be saved in this folder.</td></tr>
<tr><td><code>ServerCertificate</code></td><td>The certificate of the server in DER format. This file is automatically generated the first time the server is started. You can also replace the file with your own certificate.</td></tr>
<tr><td><code>ServerPrivateKey</code></td><td>The private key of the server in PEM format. This file is automatically generated the first time the server is started. If you are using your own certificate, you must replace this file with a private key that matches your certificate.</td></tr>
</table>

In addition, the folder for rejected client certificates can be specified via the element "`<RejectedCertificatesDirectory>`".

All the rejected certificates from OPC clients are stored in this folder and can be copied to the certificate trust list by the administrator.

Configuring user logon

The supported logon types for users are configured via the "<UserIdentityTokens>" element.

XML element	Description
EnableAnonymous	Preset; users can log on without an ID and password.
EnableUserPw	Preset; users can log on using a Windows user account.
EnableCertificate	Not supported.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

Configuration of DiagMonitor OPC UA server
A5E38926068-AA, 08/2016