

Table of contents

- Eigenschaften
 - Verbindungseinstellungen
 - Security
 - Endpoints
 - Benutzer und Passwort
 - Zertifikatmanagement
 - Protokoll und Encoding
 - Unterstützte Dienste
 - Adressraum des ctrlX OPC UA Servers
 - Unterstützte Dienste für den Datenbereich Data Layer
 - OPC UA-Events

Eigenschaften

Eigenschaften

Verbindungseinstellungen

Der ctrlX OPC UA Server ist über alle TCP/IP-fähigen Netzwerkschnittstellen des ctrlX OS-Geräts erreichbar. Bei ctrlX CORE werden dementsprechend die Anschlüsse XF10, XF11, XF12 und XF51 vom OPC UA Server unterstützt.

Der OPC UA Server verwendet standardmäßig den Port 4840.

Aufbau der EndpointURL ist `opc.tcp://<hostnameDerSteuerung>:4840` oder `opc.tcp://<hostadresse>:4840`.

Mit der standardmäßigen IP-Adresse des ctrlX OS-Geräts (192.168.1.1) entspricht die EndpointURL `opc.tcp://192.168.1.1:4840`.

Security

Folgende Verfahren zum Verschlüsseln und Signieren (SecurityPolicies) sind standardmäßig aktiviert:

- SecurityPolicy [B] – Basic256Sha256
- SecurityPolicy [A] – Aes128-Sha256-RsaOaep
- SecurityPolicy – Aes256-Sha256-RsaPss



Bevorzugt sollte das Verfahren Aes256-Sha256-RsaPss verwendet werden, da es das sicherste Verfahren ist.



Eine unverschlüsselte Verbindung (SecurityPolicy None) kann über die Konfiguration aktiviert werden.

Eine unverschlüsselte Verbindung wird nur zu Diagnosezwecken empfohlen.

Im Regelbetrieb sollte die unverschlüsselte Verbindung nicht genutzt werden.

Endpoints

Folgende Endpoints mit den verschiedenen Verfahren zur Verschlüsselung und zum Signieren stehen standardmäßig zur Verfügung:

- Sign – Basic256Sha256
- Sign – Aes128-Sha256-RsaOaep
- Sign – Aes256-Sha256-RsaPss
- SignAndEncrypt – Basic256Sha256
- SignAndEncrypt – Aes128-Sha256-RsaOaep
- SignAndEncrypt – Aes256-Sha256-RsaPss

Benutzer und Passwort

Für eine Verbindung zum ctrlX OPC UA Server ist eine gültige Kombination aus Benutzername und Passwort nötig. Benutzername und Passwort können über den Identity-Manager des ctrlX OS (unter [Einstellungen](#) → [Benutzer & Berechtigungen](#) in der Web-Oberfläche) konfiguriert werden.

Dem Benutzer muss eine der folgenden Berechtigungen zugeordnet werden:

- OPC UA Scopes: OPC UA Server access
- Administration : Full access

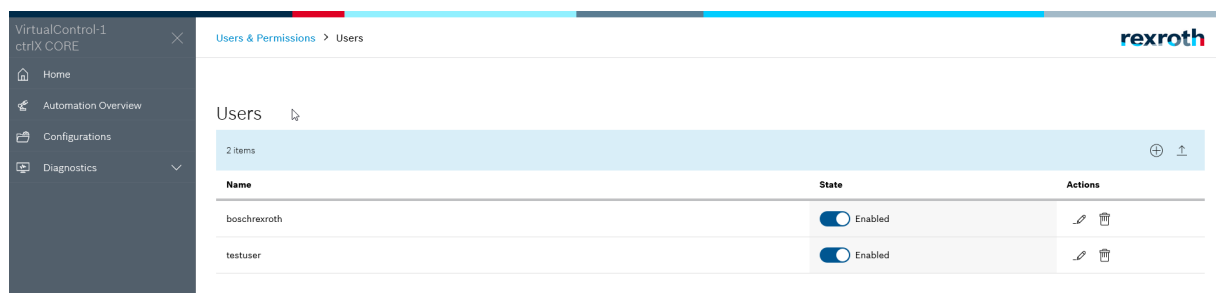


Abb. 10: Beispielkonfiguration eines Benutzers im Identity-Manager des ctrlX OS

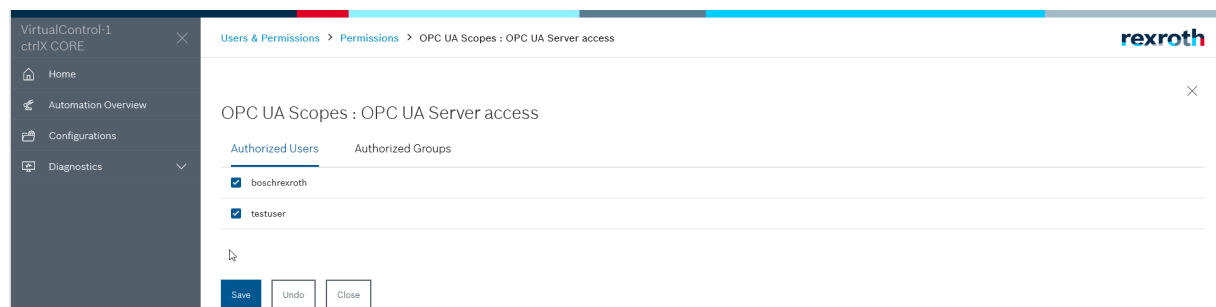


Abb. 11: Beispielkonfiguration der Berechtigungen in "OPC UA Scopes: OPC UA Server access"

Standardmäßig werden zum Übertragen des Passworts an die Steuerung folgende zwei UserNameIdentityToken angeboten:

- "Username_256_Token" mit SecurityPolicy BASIC256SHA256}
- "Username_256_RSAPSS_Token" mit SecurityPolicy Aes256-Sha256-RsaPss



Username_256_Token mit SecurityPolicy BASIC256SHA256 ist auch das Standardverfahren für SecurityPolicy Aes128-Sha256-RsaOaep.



Der AnonymousIdentityToken "Anonymous_Token" wird für die Dienste FindServer & Get Endpoint angeboten. Eine OPC UA Verbindung (Session) kann nur über Benutzer & Passwort hergestellt werden. Ein anonymer Zugriff ist nicht möglich.

Zertifikatsmanagement

Die sichere Verbindung zwischen OPC UA Server und Client basiert auf vertrauenswürdigen Zertifikaten. Hier wird zurzeit nur das selbstsignierte Zertifikatsmanagement unterstützt. Dies basiert auf einem manuellen Austausch der Zertifikate zwischen OPC UA Server und Client. Hierbei werden beim Verbindungsaufbau zwischen Server und Client die Zertifikate ausgetauscht. Sowohl Server als auch Client müssen manuell den Zertifikaten vertrauen.

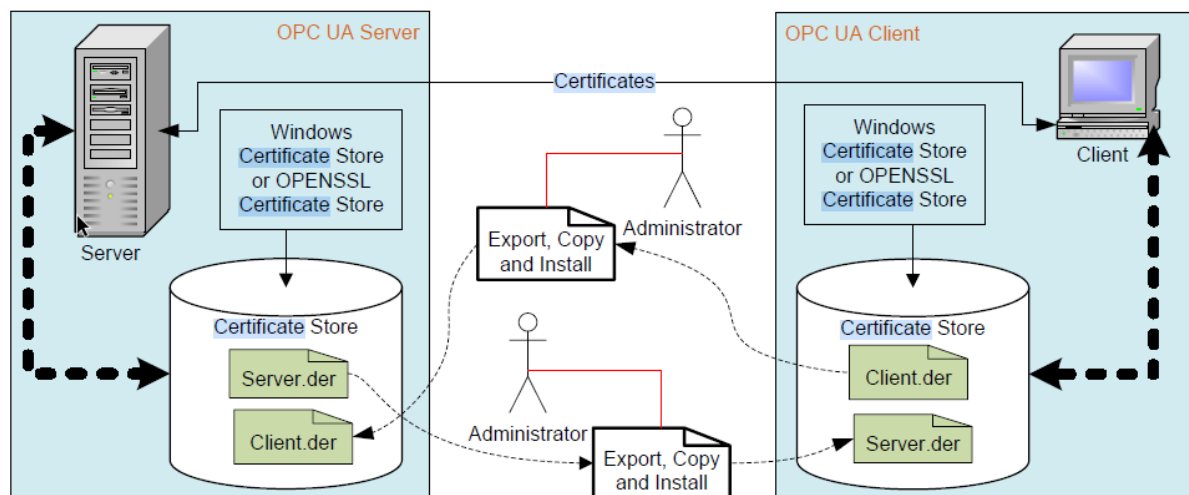


Abb. 12: Manuelles Zertifikatsmanagement aus "OPC UA Specification Part 2: Security"

Das Vertrauen der Zertifikate geschieht beim ctrlX OPC UA Server über den ctrlX OS Certificate Manager (unter [Einstellungen → Zertifikate & Schlüssel](#) in der Web-Oberfläche).

Folgende Schritte sind durchzuführen:

1. Zuerst muss eine sichere Verbindung (SecureChannel) per OpenSecureChannel aufgebaut werden. Hierbei wird das Zertifikat vom Client zum Server übertragen.
⇒ Der Server meldet den Fehler "BadSecurityChecksFailed" und trägt das Client-Zertifikat in seine Reject-Liste für Zertifikate ein.
2. Im Certificate Manager unter [Zertifikate & Schlüssel → OPC UA Server](#) wird das Zertifikat des Clients als rejected angezeigt. Dieses Zertifikat kann dort manuell getrustet werden. Auf Clientseite muss ebenfalls dem Server-Zertifikat vertraut werden.

3. Eine sichere OPC UA Verbindung kann jetzt vom Client zum Server hergestellt werden.

Als Alternative kann das Zertifikat des Clients auch direkt im Certificate Manager hochgeladen werden. Dadurch entfällt Schritt 1. Jedoch ist hierbei notwendig, das Zertifikat zuvor umzubenennen. Der Dateiname muss dem SHA1-Wert der Datei entsprechen. Dieser kann zum Beispiel aus dem Fingerabdruck des Zertifikats ermittelt werden. Bei der Benennung müssen alle Zeichen des SHA1 als Großbuchstaben dargestellt werden. Das Schema der Datei ist "[SHA1-Wert in Großbuchstaben].der".

Ab Version 2.2 kann das Laden von Zertifikaten auch über die App-Daten des OPC UA Servers geschehen. Hierzu müssen die Zertifikate und evtl. dazugehörige CRLs im Ordner "cert-import" in den OPC UA Server App-Daten (Pfad *opcuaserver*) abgelegt werden. Der Inhalt des Ordners "cert-import" wird zum Start der OPC UA Server App geprüft und gegebenenfalls darin befindliche Zertifikate überprüft und in die entsprechenden Ordner des OPC UA Server Certificate Store verschoben.

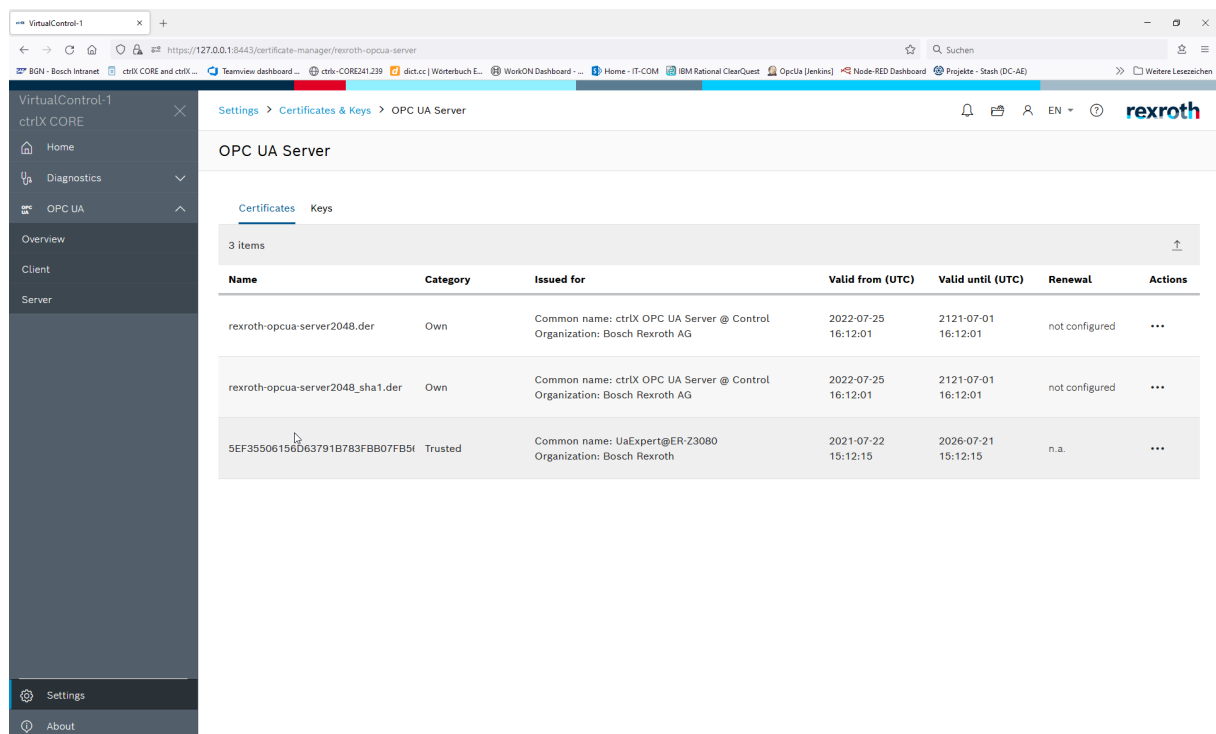


Abb. 13: Certificate Manager für ctrlX OPC UA Server

Technische Informationen zu Zertifikaten und privaten Schlüsseln

Die Zertifikate des ctrlX OPC UA Servers werden zurzeit selbst erzeugt und signiert und sind standardmäßig 36135 Tage (ca. 99 Jahre) gültig.

Die verwendeten Verschlüsselungsverfahren sind "sha256" und "sha1".

Der ctrlX OPC UA Server unterstützt DER-encodierte Zertifikate und CRLs (Certificate Revocation List) entsprechend der OPC UA Spezifikation. Der private Schlüssel muss ein PEM-encodierter RSA-privater Schlüssel sein.

Technische Informationen zur Ablage der Zertifikate

Ablage für die Zertifikate ist der Certificate Store.

Der Certificate Store liegt unter `$SNAP_COMMON/package-certificates/rexroth-opcua-server/rexroth-opcua-server/`.

Bei VirtualControl lautet der Pfad beispielsweise wie folgt:

`/var/snap/rexroth-opcua-server/common/package-certificates/rexroth-opcua-server/rexroth-opcua-server/`

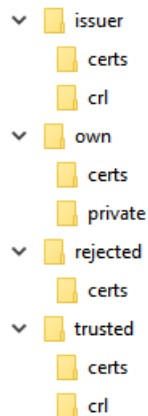


Abb. 14: Certificate Store - Ordner und Unterordner

Der Certificate Store besteht aus folgenden Ordnern:

- **issuer:**
Wird momentan nicht unterstützt
- **own:**
Beinhaltet das Application Instance Certificate vom OPC UA Server/Client und den dazugehörigen privaten Schlüsseln
- **rejected:**
Beinhaltet Zertifikate von UA Client bzw. Server, die eine Verbindung zum OPC UA Server bzw. Client aufbauen wollten, denen aber noch nicht vertraut worden ist
- **trusted:**
Beinhaltet die Zertifikaten der UA Clients bzw. Servers, denen der OPC UA Server bzw. Client vertraut
Die jeweiligen Unterordner "certs" beinhalten die zu den einzelnen Kategorien gehörenden Zertifikate, welchen zum Beispiel vertraut werden (unter Ordner "trusted") bzw. noch nicht vertraut werden (unter Ordner "rejected"). Eine Certificate Revocation List (CRL) wird im Unterordner "crl" geführt.

Protokoll und Encoding

Es wird entsprechend der Profile des OPC UA Standards Release 1.04 (Part 7 - Profiles) Folgendes unterstützt:

ctrlX OPC UA Server - Unterstützte Profile

Protocol and Encoding

Name	Description	From Profile
------	-------------	--------------

Protocol and Encoding		
Name	Description	From Profile
Protocol UA TCP	Support the UA TCP transport protocol defined in UA Part 6.	UA-TCP UA-SC UA-Binary
UA Secure Conversation	Support UA Secure Conversation specified in UA Part 6.	UA-TCP UA-SC UA-Binary
UA Binary Encoding	Support UA Binary Encoding. Values of these data types are encoded in compact binary formats, contiguously and without tagging. I.e. the receiver is assumed to understand the structure it is decoding.	UA-TCP UA-SC UA-Binary

Unterstützte Dienste

Es werden entsprechend der Profile des OPC UA Standards Release 1.04 (Part 7 - Profiles) folgende Dienste unterstützt:

ctrlX OPC UA Server - "Discovery Services"

Discovery Services		
Name	Description	From Profile
Discovery Get Endpoints	Support the GetEndpoints Service to obtain all Endpoints of the Server. This includes filtering based on Profiles.	Core 2017 Server Facet
Discovery Find Servers Self	Support the FindServers Service only for itself	Core 2017 Server Facet

ctrlX OPC UA Server - "Session Services"

Session Services			
Name	Description	From Profile	Comments
Session General Service Behaviour	Implement basic Service behaviour. This includes in particular: ■ checking the authentication token ■ returning the requestHandle in responses ■ returning available diagnostic information as requested with the 'returnDiagnostics' parameter ■ respecting a timeoutHint	Core 2017 Server Facet	
Session Base	Support the Session Service Set (CreateSession, ActivateSession, CloseSession) except the use of ActivateSession to change the Session user. This includes correct handling of all parameters that are provided. Note that for the CreateSession and ActivateSession services, if the SecurityMode = None then: 1) The Application Certificate and Nonce are optional. 2) The signatures are null/empty. The details of this are described in Part 4.	Core 2017 Server Facet	
Session Minimum 1	Support minimum 1 Session (total)	Core 2017 Server Facet	Max. 50 Sessions Max. 10 Sessions for Subscriptions
Session Minimum 2 Parallel	Support minimum 2 parallel Sessions (total for all Clients)	Micro Embedded Device 2017 Server Profile	Max. 50 Sessions Max. 10 Sessions for Subscriptions

ctrlX OPC UA Server - "View Services"

View Services

Name	Description	From Profile	Comments
View Basic	Support the View Service Set (Browse, BrowseNext)	Core 2017 Server Facet	
View TranslateBrowsePath	Support TranslateBrowsePathsToNodeIds Service	Core 2017 Server Facet	

ctrlX OPC UA Server - "Attribute Services"**Attribute Services**

Name	Description	From Profile
Attribute Read	Supports the Read Service to read one or more Attributes of one or more Nodes. This includes support of the IndexRange parameter to read a single element or a range of elements when the Attribute value is an array	Core 2017 Server Facet
Attribute Write Values	Supports writing to values to one or more Attributes of one or more Nodes	Core 2017 Server Facet

ctrlX OPC UA Server- "Supscription Services"**Subscription Services**

Name	Description	From Profile	Comments
Subscription Basic	Support the following Subscription Services: CreateSubscription, ModifySubscription, DeleteSubscriptions, Publish, Republish and SetPublishingMode	Embedded DataChange Subscription Server Facet	

Subscription Services

Name	Description	From Profile	Comments
Subscription Minimum 05	Support at least 5 Subscriptions per Session. This number has to be supported for at least half of the minimum required sessions.	Enhanced DataChange Subscription 2017 Server Facet	Max 150. Subscriptions per Session
Subscription Publish Min 10	Support at least 10 Publish Service requests per Session. This number has to be supported for at least half of the minimum required sessions. Support, as a minimum, the number of Publish requests per session as the size of the NotificationMessage retransmission queue for Republish.	Enhanced DataChange Subscription 2017 Server Facet	Max 10. Publish Service requests per Session
Subscription Publish Discard Policy	Respect the specified policy for discarding Publish Service requests. If the maximum number of Publish Service requests has been queued and a new Publish Service request arrives, the "oldest" Publish request has to be discarded by returning the proper error.	Embedded DataChange Subscription Server Facet	

ctrlX OPC UA Server- "Monitored Item Services"**Monitored Item Services**

Name	Description	From Profile	Comments
Monitor Basic	Support the following MonitoredItem Services: CreateMonitoredItems, ModifyMonitoredItems, DeleteMonitoredItems and SetMonitoringMode	Embedded DataChange Subscription Server Facet	

Monitored Item Services

Name	Description	From Profile	Comments
Monitor Value Change	Support creation of MonitoredItems for Attribute value changes. This includes support of the IndexRange to select a single element or a range of elements when the Attribute value is an array	Embedded DataChange Subscription Server Facet	
Monitor Items 500	Support at least 500 MonitoredItems per Subscription. This number has to be supported for at least half of the required Subscriptions for half of the required Sessions.	Enhanced DataChange Subscription 2017 Server Facet	Max 500 pro Session. 5000 across all 10 Sessions
Monitor MinQueueSize_05	Support at least 5 queue entries for MonitoredItems. Servers often will adapt the queue size to the number of currently MonitoredItems. However, it is expected that Servers support this minimum queue size for at least one third of the supported MonitoredItems.	Enhanced DataChange Subscription 2017 Server Facet	Max Queue size: 100

ctrlX OPC UA Server- "Method Services"**Method Services**

Name	Description	From Profile	Test Cases	Comments
Method Call	Support the Call Service to call (invoke) a Method which includes support for Method Parameters.	Standard DataChange Subscription 2017 Server Facet	Open	Nur teilweise im Datenbereich des Data Layers unterstützt

Adressraum des ctrlX OPC UA Servers

Zurzeit gibt es insgesamt 10 Namespaces innerhalb des ctrlX OPC UA Servers:

ctrlX OPC UA Server - Namespaces

Namespace Index	Namespace URI
0	http://opcfoundation.org/UA/
1	urn:Control@Rexroth:ctrlX:AUTOMATION:Server
2	http://www.boschrexroth.com/OpcUa/Datalayer
3	http://www.boschrexroth.com/OpcUa/DatalayerTypes
4	http://www.boschrexroth.com/OpcUa/DatalayerEncoding
5	http://www.boschrexroth.com/OpcUa/DatalayerEventTypes
6	http://www.boschrexroth.com/OpcUa/DatalayerMethod
7	http://www.boschrexroth.com/OpcUa/DatalayerEnumeration
8	http://www.boschrexroth.com/OpcUa/DatalayerObjects
9	http://www.boschrexroth.com/OpcUa/DatalayerInputArguments
10	http://www.boschrexroth.com/OpcUa/DatalayerOutputArguments

Namespace 2 bis 10 liefern die Daten für den Data Layer, dessen Typen und das Encoding von Strukturen innerhalb des Data Layer.



Die Namespace URI kennzeichnet eindeutigen Namensraum (Namespace) als Ressource innerhalb des OPC UA-Adressraums und sollte nicht mit einer URL einer Webseite verwechselt werden.

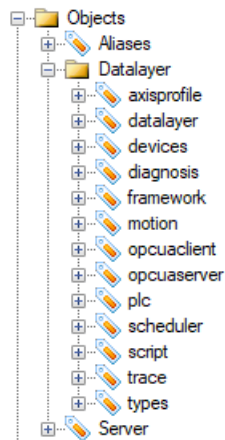


Abb. 15: ctrlX OPC UA Server - Adressraum unter "Objects"

Die Nutzdaten der Steuerung befinden sich alle unter dem Knoten *Objects/DataLayer/*. Die darunterliegenden Daten werden direkt auf dem Data Layer gemappt. Dieser Bereich wird dynamisch, je nach installierten Snaps, angepasst.

In **Abb. 15** sind zum Beispiel alle Daten der installierten Apps Automation Core, Motion, OPC UA Server und OPC UA Client vorhanden.

Unterstützte Dienste für den Datenbereich Data Layer

Es werden folgende Dienste für den Datenbereich des Data Layer unterstützt:

- Browse und TranslateBrowsePathsToNodeIds
- Read
- Write
- Subscription
- Call
- Events

OPC UA-Events

Der ctrlX Data Layer bietet einen Event-Mechanismus. Events bilden Ereignisse ab. Dies kann z.B. eine Fehlermeldung der Maschine sein. Die Data Layer-Events können auch über den ctrlX OPC UA Server übertragen werden. Mit einer OPC UA-Subscription auf die Data Layer-Knoten können entsprechende OPC UA-Events empfangen werden.

In der folgenden Abbildung ist beispielhaft eine OPC UA-Event-Subscription dargestellt. Hier werden Events vom Data Layer-Knoten *framework/bundles* empfangen. Dieser Knoten liefert Events bei Änderungen der App-Installationen. Im Beispiel wurde die ctrlX Motion App installiert. Diese Installation liefert mehrere Events, die über die installierten Bundles informiert.

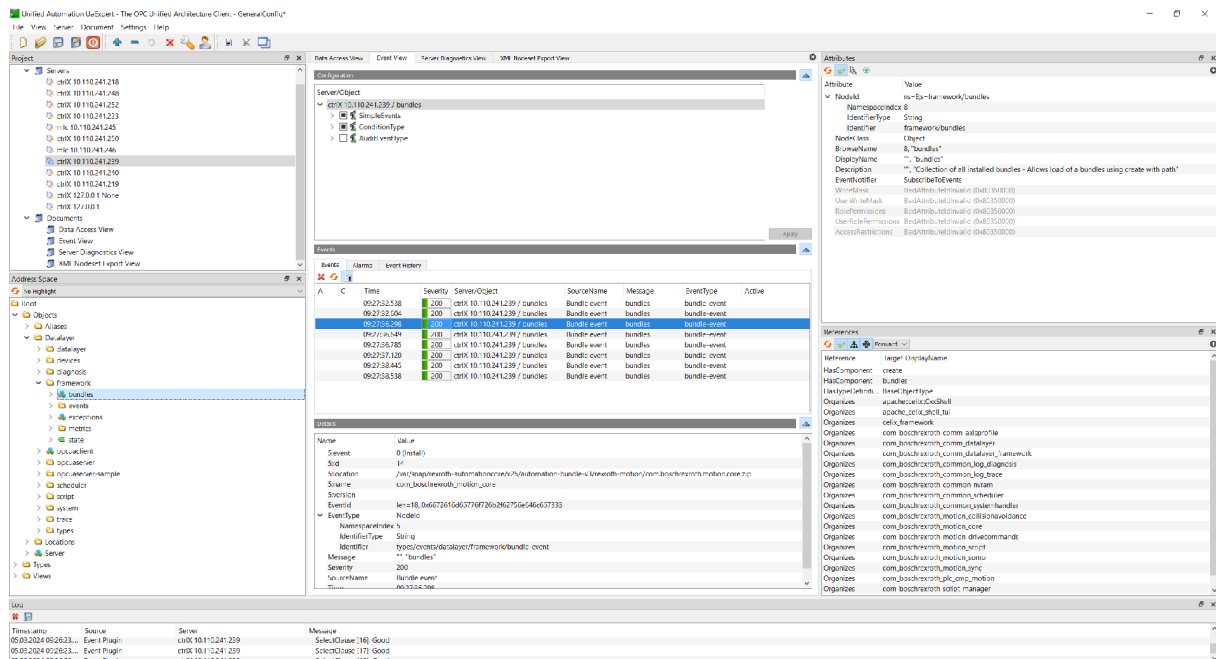


Abb. 16: Beispielhafte OPC UA-Event-Subscription

Aktuelle Einschränkungen der OPC UA-Events:

- Beim erstmaligen Hinzufügen eines Knotens zur Event-Subscription wird dies mit einem Fehler quittiert. Erst beim zweiten Hinzufügen des Knotens wird dies erfolgreich durchgeführt.
- Das Attribut "EventNotifier" liefert zunächst den Wert "None" für alle Data Layer-Knoten. Erst nach dem Hinzufügen des Knotens zur Event-Subscription wird der Wert "SubscribeToEvents" geliefert, falls der Knoten Events bereitstellen kann.
- Der OPC UA Client selektiert die Event-Felder über "selectClause", welche als "SimpleAttributeOperand" definiert werden.
Hierbei wird aktuell nur folgende Kombination von "typeDefinitionId" und "browsePath" unterstützt:
 - typeDefinitionId: ns=0;i=2041 (BaseEventType)
 - browsePath: BrowseName des Event-Feldes, z.B.: 5, "name"

Verbindungseinstellungen

Verbindungseinstellungen

Der ctrlX OPC UA Server ist über alle TCP/IP-fähigen Netzwerkschnittstellen des ctrlX OS-Geräts erreichbar. Bei ctrlX CORE werden dementsprechend die Anschlüsse XF10, XF11, XF12 und XF51 vom OPC UA Server unterstützt.

Der OPC UA Server verwendet standardmäßig den Port 4840.

Aufbau der EndpointURL ist **opc.tcp://<hostnameDerSteuerung>:4840** oder **opc.tcp://<hostadresse>:4840**.

Mit der standardmäßigen IP-Adresse des ctrlX OS-Geräts (192.168.1.1) entspricht die EndpointURL **opc.tcp://192.168.1.1:4840**.

Security

Security

Folgende Verfahren zum Verschlüsseln und Signieren (SecurityPolicies) sind standardmäßig aktiviert:

- SecurityPolicy [B] – Basic256Sha256
- SecurityPolicy [A] – Aes128-Sha256-RsaOaep
- SecurityPolicy – Aes256-Sha256-RsaPss



Bevorzugt sollte das Verfahren Aes256-Sha256-RsaPss verwendet werden, da es das sicherste Verfahren ist.



Eine unverschlüsselte Verbindung (SecurityPolicy None) kann über die Konfiguration aktiviert werden.

Eine unverschlüsselte Verbindung wird nur zu Diagnosezwecken empfohlen.

Im Regelbetrieb sollte die unverschlüsselte Verbindung nicht genutzt werden.

Endpoints

Endpoints

Folgende Endpoints mit den verschiedenen Verfahren zur Verschlüsselung und zum Signieren stehen standardmäßig zur Verfügung:

- Sign –Basic256Sha256
- Sign – Aes128-Sha256-RsaOaep
- Sign – Aes256-Sha256-RsaPss
- SignAndEncrypt –Basic256Sha256
- SignAndEncrypt – Aes128-Sha256-RsaOaep
- SignAndEncrypt – Aes256-Sha256-RsaPss

Benutzer und Passwort

Benutzer und Passwort

Für eine Verbindung zum ctrlX OPC UA Server ist eine gültige Kombination aus Benutzername und Passwort nötig. Benutzername und Passwort können über den Identity-Manager des ctrlX OS (unter [Einstellungen](#) → [Benutzer & Berechtigungen](#) in der Web-Oberfläche) konfiguriert werden.

Dem Benutzer muss eine der folgenden Berechtigungen zugeordnet werden:

- OPC UA Scopes: OPC UA Server access
- Administration : Full access

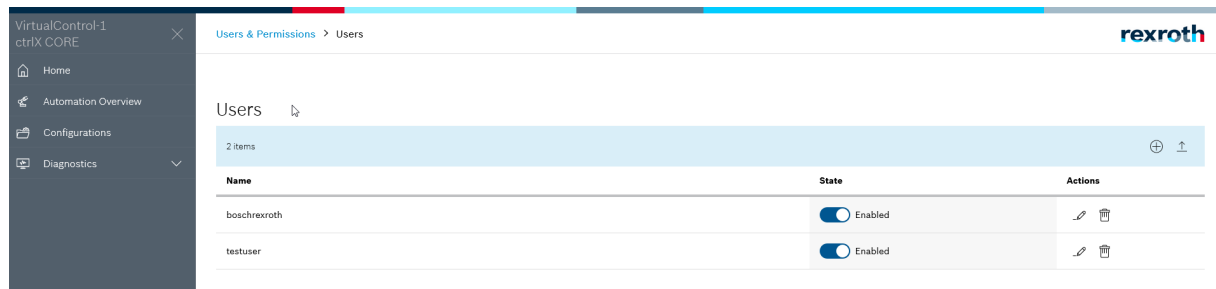


Abb. 10: Beispielkonfiguration eines Benutzers im Identity-Manager des ctrlX OS

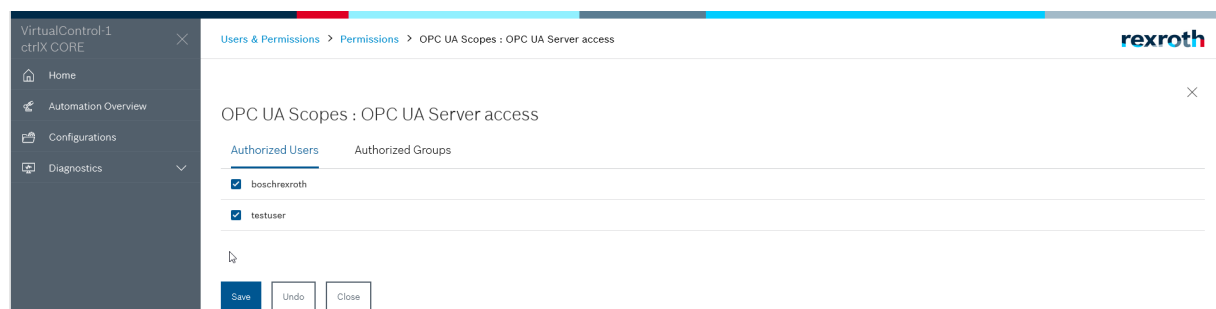


Abb. 11: Beispielkonfiguration der Berechtigungen in "OPC UA Scopes: OPC UA Server access"

Standardmäßig werden zum Übertragen des Passworts an die Steuerung folgende zwei UserNameIdentityToken angeboten:

- "Username_256_Token" mit SecurityPolicy BASIC256SHA256}
- "Username_256_RSAPSS_Token" mit SecurityPolicy Aes256-Sha256-RsaPss



Username_256_Token mit SecurityPolicy BASIC256SHA256 ist auch das Standardverfahren für SecurityPolicy Aes128-Sha256-RsaOaep.



Der AnonymousIdentityToken "Anonymous_Token" wird für die Dienste FindServer & Get Endpoint angeboten. Eine OPC UA Verbindung (Session) kann nur über Benutzer & Passwort hergestellt werden. Ein anonymer Zugriff ist nicht möglich.

Zertifikatmanagement

Zertifikatmanagement

Die sichere Verbindung zwischen OPC UA Server und Client basiert auf vertrauenswürdigen Zertifikaten. Hier wird zurzeit nur das selbstsignierte Zertifikatsmanagement unterstützt. Dies basiert auf einem manuellen Austausch der Zertifikate zwischen OPC UA Server und Client. Hierbei werden beim Verbindungsaufbau zwischen Server und Client die Zertifikate ausgetauscht. Sowohl Server als auch Client müssen manuell den Zertifikaten vertrauen.

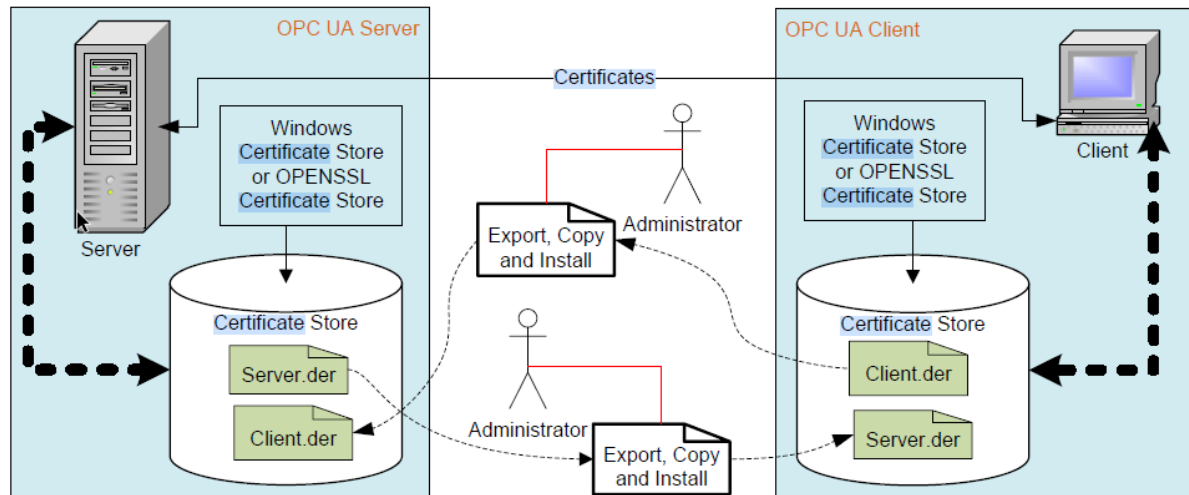


Abb. 12: Manuelles Zertifikatsmanagement aus "OPC UA Specification Part 2: Security"

Das Vertrauen der Zertifikate geschieht beim ctrlX OPC UA Server über den ctrlX OS Certificate Manager (unter [Einstellungen → Zertifikate & Schlüssel](#) in der Web-Oberfläche).

Folgende Schritte sind durchzuführen:

1. Zuerst muss eine sichere Verbindung (SecureChannel) per OpenSecureChannel aufgebaut werden. Hierbei wird das Zertifikat vom Client zum Server übertragen.
 ⇒ Der Server meldet den Fehler "BadSecurityChecksFailed" und trägt das Client-Zertifikat in seine Reject-Liste für Zertifikate ein.
2. Im Certificate Manager unter [Zertifikate & Schlüssel → OPC UA Server](#) wird das Zertifikat des Clients als rejected angezeigt. Dieses Zertifikat kann dort manuell getrustet werden. Auf Clientseite muss ebenfalls dem Server-Zertifikat vertraut werden.
3. Eine sichere OPC UA Verbindung kann jetzt vom Client zum Server hergestellt werden.

Als Alternative kann das Zertifikat des Clients auch direkt im Certificate Manager hochgeladen werden. Dadurch entfällt Schritt 1. Jedoch ist hierbei notwendig, das Zertifikat zuvor umzubenennen. Der Dateiname muss dem SHA1-Wert der Datei entsprechen. Dieser kann zum Beispiel aus dem Fingerabdruck des Zertifikats ermittelt werden. Bei der Benennung müssen alle Zeichen des SHA1 als Großbuchstaben dargestellt werden. Das Schema der Datei ist "[SHA1-Wert in Großbuchstaben].der".

Ab Version 2.2 kann das Laden von Zertifikaten auch über die App-Daten des OPC UA Servers geschehen. Hierzu müssen die Zertifikate und evtl. dazugehörige CRLs im Ordner "cert-import" in den OPC UA Server App-Daten (Pfad *opcuaserver*) abgelegt werden. Der Inhalt des Ordners "cert-import" wird zum Start der OPC UA Server App geprüft und gegebenenfalls darin befindliche Zertifikate überprüft und in die entsprechenden Ordner des OPC UA Server Certificate Store verschoben.

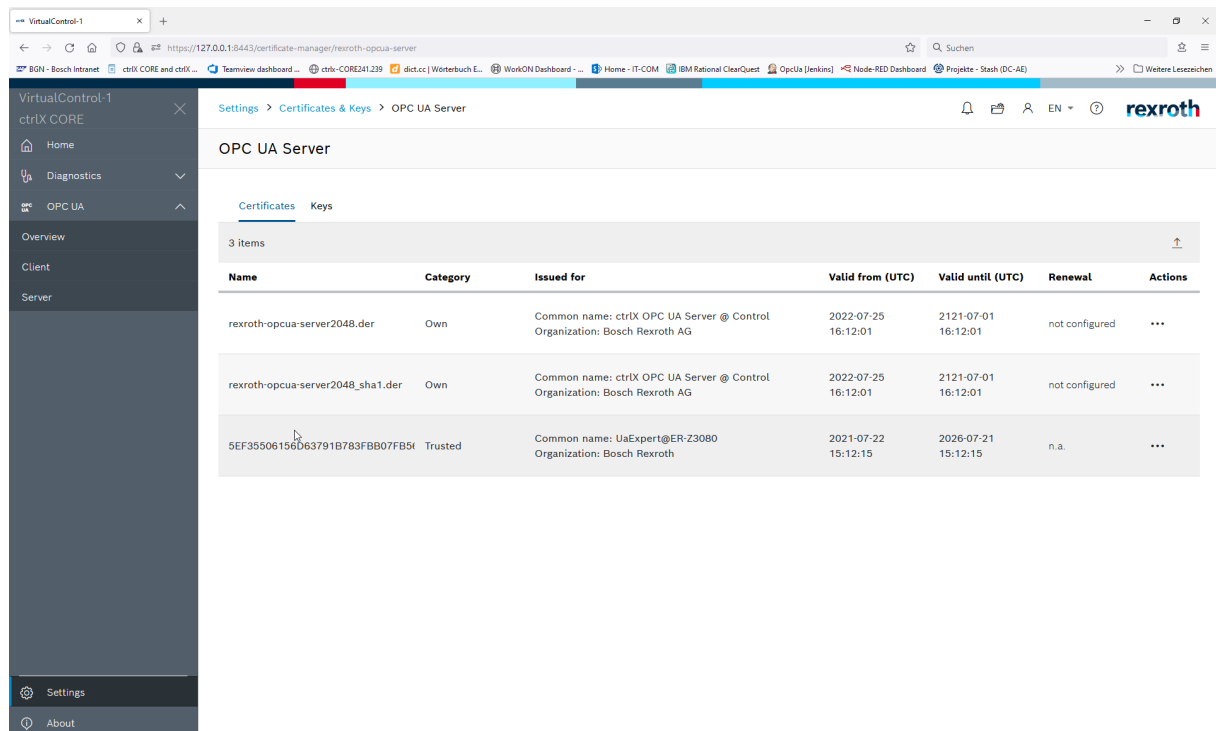


Abb. 13: Certificate Manager für ctrlX OPC UA Server

Technische Informationen zu Zertifikaten und privaten Schlüsseln

Die Zertifikate des ctrlX OPC UA Servers werden zurzeit selbst erzeugt und signiert und sind standardmäßig 36135 Tage (ca. 99 Jahre) gültig.

Die verwendeten Verschlüsselungsverfahren sind "sha256" und "sha1".

Der ctrlX OPC UA Server unterstützt DER-encodierte Zertifikate und CRLs (Certificate Revocation List) entsprechend der OPC UA Spezifikation. Der private Schlüssel muss ein PEM-encodierter RSA-privater Schlüssel sein.

Technische Informationen zur Ablage der Zertifikate

Ablage für die Zertifikate ist der Certificate Store.

Der Certificate Store liegt unter `$SNAP_COMMON/package-certificates/rexroth-opcua-server/rexroth-opcua-server/`.

Bei VirtualControl lautet der Pfad beispielsweise wie folgt:

`/var/snap/rexroth-opcua-server/common/package-certificates/rexroth-opcua-server/rexroth-opcua-server/`

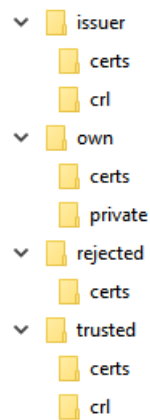


Abb. 14: Certificate Store - Ordner und Unterordner

Der Certificate Store besteht aus folgenden Ordnern:

- issuer:
Wird momentan nicht unterstützt
- own:
Beinhaltet das Application Instance Certificate vom OPC UA Server/Client und den dazugehörigen privaten Schlüsseln
- rejected:
Beinhaltet Zertifikate von UA Client bzw. Server, die eine Verbindung zum OPC UA Server bzw. Client aufbauen wollten, denen aber noch nicht vertraut worden ist
- trusted:
Beinhaltet die Zertifikaten der UA Clients bzw. Servers, denen der OPC UA Server bzw. Client vertraut
Die jeweiligen Unterordner "certs" beinhalten die zu den einzelnen Kategorien gehörenden Zertifikate, welchen zum Beispiel vertraut werden (unter Ordner "trusted") bzw. noch nicht vertraut werden (unter Ordner "rejected"). Eine Certificate Revocation List (CRL) wird im Unterordner "crl" geführt.

Protokoll und Encoding

Protokoll und Encoding

Es wird entsprechend der Profile des OPC UA Standards Release 1.04 (Part 7 - Profiles) Folgendes unterstützt:

ctrlX OPC UA Server - Unterstützte Profile

Protocol and Encoding		
Name	Description	From Profile
Protocol UA TCP	Support the UA TCP transport protocol defined in UA Part 6.	UA-TCP UA-SC UA-Binary

Protocol and Encoding		
Name	Description	From Profile
UA Secure Conversation	Support UA Secure Conversation specified in UA Part 6.	UA-TCP UA-SC UA-Binary
UA Binary Encoding	Support UA Binary Encoding. Values of these data types are encoded in compact binary formats, contiguously and without tagging. I.e. the receiver is assumed to understand the structure it is decoding.	UA-TCP UA-SC UA-Binary

Unterstützte Dienste

Unterstützte Dienste

Es werden entsprechend der Profile des OPC UA Standards Release 1.04 (Part 7 - Profiles) folgende Dienste unterstützt:

ctrlX OPC UA Server - "Discovery Services"

Discovery Services		
Name	Description	From Profile
Discovery Get Endpoints	Support the GetEndpoints Service to obtain all Endpoints of the Server. This includes filtering based on Profiles.	Core 2017 Server Facet
Discovery Find Servers Self	Support the FindServers Service only for itself	Core 2017 Server Facet

ctrlX OPC UA Server - "Session Services"

Session Services			
Name	Description	From Profile	Comments

Session Services

Name	Description	From Profile	Comments
Session General Service Behaviour	Implement basic Service behaviour. This includes in particular: ■ checking the authentication token ■ returning the requestHandle in responses ■ returning available diagnostic information as requested with the 'returnDiagnostics' parameter ■ respecting a timeoutHint	Core 2017 Server Facet	
Session Base	Support the Session Service Set (CreateSession, ActivateSession, CloseSession) except the use of ActivateSession to change the Session user. This includes correct handling of all parameters that are provided. Note that for the CreateSession and ActivateSession services, if the SecurityMode = None then: 1) The Application Certificate and Nonce are optional. 2) The signatures are null/empty. The details of this are described in Part 4.	Core 2017 Server Facet	
Session Minimum 1	Support minimum 1 Session (total)	Core 2017 Server Facet	Max. 50 Sessions Max. 10 Sessions for Subscriptions
Session Minimum 2 Parallel	Support minimum 2 parallel Sessions (total for all Clients)	Micro Embedded Device 2017 Server Profile	Max. 50 Sessions Max. 10 Sessions for Subscriptions

ctrlX OPC UA Server - "View Services"

View Services

Name	Description	From Profile	Comments
View Basic	Support the View Service Set (Browse, BrowseNext)	Core 2017 Server Facet	
View TranslateBrowsePath	Support TranslateBrowsePathsToNodeIds Service	Core 2017 Server Facet	

ctrlX OPC UA Server - "Attribute Services"**Attribute Services**

Name	Description	From Profile
Attribute Read	Supports the Read Service to read one or more Attributes of one or more Nodes. This includes support of the IndexRange parameter to read a single element or a range of elements when the Attribute value is an array	Core 2017 Server Facet
Attribute Write Values	Supports writing to values to one or more Attributes of one or more Nodes	Core 2017 Server Facet

ctrlX OPC UA Server- "Subscription Services"**Subscription Services**

Name	Description	From Profile	Comments
Subscription Basic	Support the following Subscription Services: CreateSubscription, ModifySubscription, DeleteSubscriptions, Publish, Republish and SetPublishingMode	Embedded DataChange Subscription Server Facet	

Subscription Services

Name	Description	From Profile	Comments
Subscription Minimum 05	Support at least 5 Subscriptions per Session. This number has to be supported for at least half of the minimum required sessions.	Enhanced DataChange Subscription 2017 Server Facet	Max 150. Subscriptions per Session
Subscription Publish Min 10	Support at least 10 Publish Service requests per Session. This number has to be supported for at least half of the minimum required sessions. Support, as a minimum, the number of Publish requests per session as the size of the NotificationMessage retransmission queue for Republish.	Enhanced DataChange Subscription 2017 Server Facet	Max 10. Publish Service requests per Session
Subscription Publish Discard Policy	Respect the specified policy for discarding Publish Service requests. If the maximum number of Publish Service requests has been queued and a new Publish Service request arrives, the "oldest" Publish request has to be discarded by returning the proper error.	Embedded DataChange Subscription Server Facet	

ctrlX OPC UA Server- "Monitored Item Services"**Monitored Item Services**

Name	Description	From Profile	Comments
Monitor Basic	Support the following MonitoredItem Services: CreateMonitoredItems, ModifyMonitoredItems, DeleteMonitoredItems and SetMonitoringMode	Embedded DataChange Subscription Server Facet	

Monitored Item Services

Name	Description	From Profile	Comments
Monitor Value Change	Support creation of MonitoredItems for Attribute value changes. This includes support of the IndexRange to select a single element or a range of elements when the Attribute value is an array	Embedded DataChange Subscription Server Facet	
Monitor Items 500	Support at least 500 MonitoredItems per Subscription. This number has to be supported for at least half of the required Subscriptions for half of the required Sessions.	Enhanced DataChange Subscription 2017 Server Facet	Max 500 pro Session. 5000 across all 10 Sessions
Monitor MinQueueSize_05	Support at least 5 queue entries for MonitoredItems. Servers often will adapt the queue size to the number of currently MonitoredItems. However, it is expected that Servers support this minimum queue size for at least one third of the supported MonitoredItems.	Enhanced DataChange Subscription 2017 Server Facet	Max Queue size: 100

ctrlX OPC UA Server- "Method Services"**Method Services**

Name	Description	From Profile	Test Cases	Comments
Method Call	Support the Call Service to call (invoke) a Method which includes support for Method Parameters.	Standard DataChange Subscription 2017 Server Facet	Open	Nur teilweise im Datenbereich des Data Layers unterstützt

Adressraum des ctrlX OPC UA Servers

Adressraum des ctrlX OPC UA Servers

Zurzeit gibt es insgesamt 10 Namespaces innerhalb des ctrlX OPC UA Servers:

ctrlX OPC UA Server - Namespaces

Namespace Index	Namespace URI
0	http://opcfoundation.org/UA/
1	urn:Control@Rexroth:ctrlX:AUTOMATION:Server
2	http://www.boschrexroth.com/OpcUa/Datalayer
3	http://www.boschrexroth.com/OpcUa/DatalayerTypes
4	http://www.boschrexroth.com/OpcUa/DatalayerEncoding
5	http://www.boschrexroth.com/OpcUa/DatalayerEventTypes
6	http://www.boschrexroth.com/OpcUa/DatalayerMethod
7	http://www.boschrexroth.com/OpcUa/DatalayerEnumeration
8	http://www.boschrexroth.com/OpcUa/DatalayerObjects
9	http://www.boschrexroth.com/OpcUa/DatalayerInputArguments
10	http://www.boschrexroth.com/OpcUa/DatalayerOutputArguments

Namespace 2 bis 10 liefern die Daten für den Data Layer, dessen Typen und das Encoding von Strukturen innerhalb des Data Layer.



Die Namespace URI kennzeichnet eindeutigen Namensraum (Namespace) als Ressource innerhalb des OPC UA-Adressraums und sollte nicht mit einer URL einer Webseite verwechselt werden.

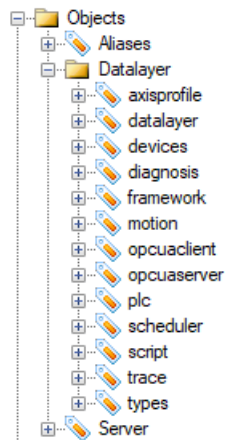


Abb. 15: ctrlX OPC UA Server - Adressraum unter "Objects"

Die Nutzdaten der Steuerung befinden sich alle unter dem Knoten *Objects/DataLayer/*. Die darunterliegenden Daten werden direkt auf dem Data Layer gemappt. Dieser Bereich wird dynamisch, je nach installierten Snaps, angepasst.

In **Abb. 15** sind zum Beispiel alle Daten der installierten Apps Automation Core, Motion, OPC UA Server und OPC UA Client vorhanden.

Unterstützte Dienste für den Datenbereich Data Layer

Unterstützte Dienste für den Datenbereich Data Layer

Es werden folgende Dienste für den Datenbereich des Data Layer unterstützt:

- Browse und TranslateBrowsePathsToNodeIds
- Read
- Write
- Subscription
- Call
- Events

OPC UA-Events

OPC UA-Events

Der ctrlX Data Layer bietet einen Event-Mechanismus. Events bilden Ereignisse ab. Dies kann z.B. eine Fehlermeldung der Maschine sein. Die Data Layer-Events können auch über den ctrlX OPC UA Server übertragen werden. Mit einer OPC UA-Subscription auf die Data Layer-Knoten können entsprechende OPC UA-Events empfangen werden.

In der folgenden Abbildung ist beispielhaft eine OPC UA-Event-Subscription dargestellt. Hier werden Events vom Data Layer-Knoten *framework/bundles* empfangen. Dieser Knoten liefert Events bei Änderungen der App-Installationen. Im Beispiel wurde die ctrlX Motion App installiert. Diese Installation liefert mehrere Events, die über die installierten Bundles informiert.

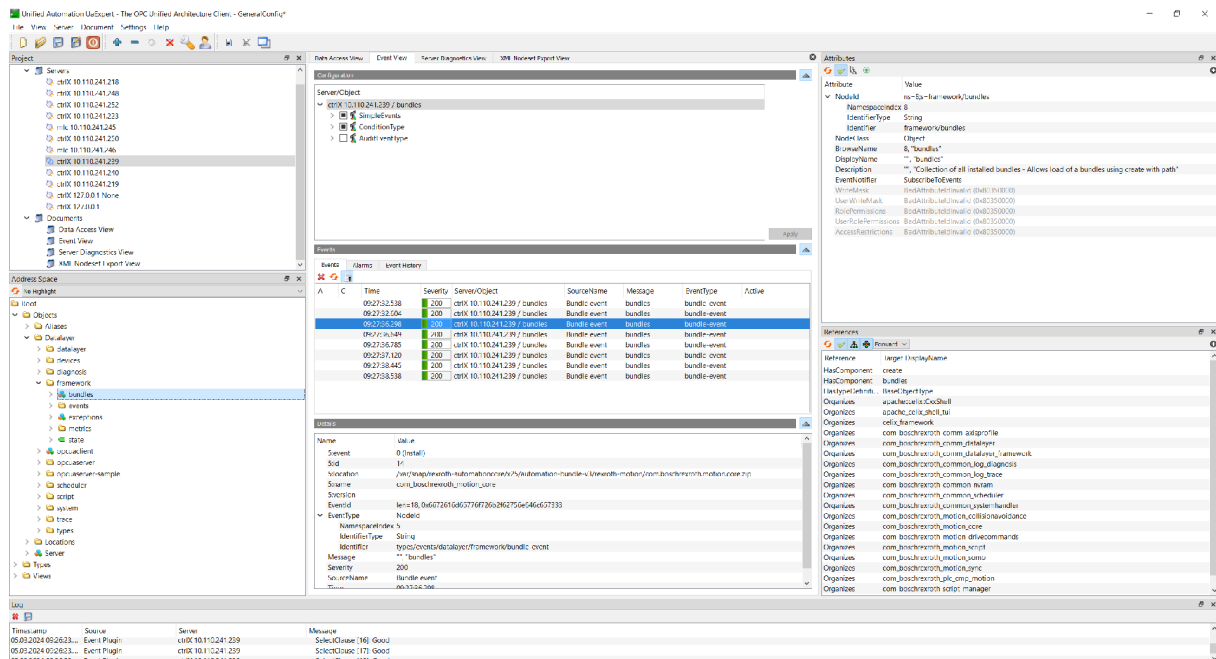


Abb. 16: Beispielhafte OPC UA-Event-Subscription

Aktuelle Einschränkungen der OPC UA-Events:

- Beim erstmaligen Hinzufügen eines Knotens zur Event-Subscription wird dies mit einem Fehler quittiert. Erst beim zweiten Hinzufügen des Knotens wird dies erfolgreich durchgeführt.
- Das Attribut "EventNotifier" liefert zunächst den Wert "None" für alle Data Layer-Knoten. Erst nach dem Hinzufügen des Knotens zur Event-Subscription wird der Wert "SubscribeToEvents" geliefert, falls der Knoten Events bereitstellen kann.
- Der OPC UA Client selektiert die Event-Felder über "selectClause", welche als "SimpleAttributeOperand" definiert werden.
Hierbei wird aktuell nur folgende Kombination von "typeDefinitionId" und "browsePath" unterstützt:

- typeDefinitionId: ns=0;i=2041 (BaseEventType)
- browsePath: BrowseName des Event-Feldes, z.B.: 5, "name"