M212325EN-B

EN
DE
FR
ES
PT
ZH
JA

Vaisala OPC UA Server Software

Setup and Configuration

for use with Vaisala viewLinc 5.1

VAISALA

PUBLISHED BY

Vaisala Oyj
Vanha Nurmijärventie 21, FI-01670 Vantaa, Finland
P.O. Box 26, FI-00421 Helsinki, Finland
+358 9 8949 1

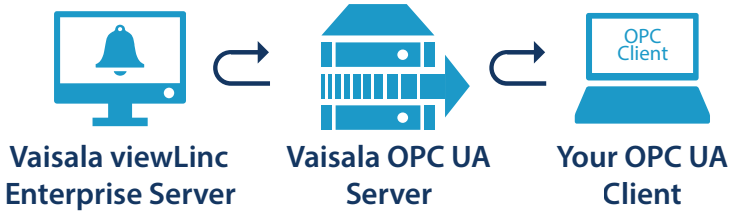
Visit our Internet pages at www.vaisala.com.

Table of contents

About Vaisala OPC UA Server

Vaisala OPC UA Server software supports the retrieval of real-time and historical data from Vaisala viewLinc Enterprise Server by third-party applications running on an OPC UA client machine.

When the Vaisala OPC UA Server receives a data request from an OPC UA client, it utilizes Vaisala API calls to retrieve data from viewLinc Enterprise Server. After authorizing the request, viewLinc Enterprise Server sends data via a secure transfer to the Vaisala OPC UA Server, which then transfers the data to the requesting OPC UA client.



System requirements

Availability	Dedicated server available 24 hours a day, 7 days a week
Server management	Recommended: Connected to an uninterruptible power supply (UPS)
	Recommended: Backup solution with support for open file backup
Operating System	Windows Server® 2019 (64-bit) Windows Server® 2016 (64-bit) Windows Server® 2012 R2 (64-bit) Windows® 10 Enterprise (64-bit)
Application disk space required	2 GB
Security certificate for web interface	Authorized TLS certificate and key
License key	OPC UA Server license key (on USB drive).

1) Vaisala OPC UA Server-signed certificate and key can be generated during installation.

License requirements

The Vaisala OPC UA Server software is shipped with a license key (found on the installation USB) to enable the OPC feature in viewLinc Enterprise Server. The matching license key must be entered in the Vaisala OPC UA Server Installation Wizard.

The OPC UA Server license must support an equal or greater number of devices as the viewLinc Enterprise Server license key.

To upgrade the Vaisala OPC UA Server software licensing size, you are only required to enter the new license key in viewLinc.

Security requirements

The Vaisala OPC UA Server can be set up with strict or relaxed levels of certificate authentication with viewLinc Enterprise Server, and strict or relaxed user authentication between Vaisala OPC UA Server and OPC UA clients. The decision to use strict or relaxed security depends on your company's security policy.

- **Certificate authentication**: If your security policy requires the use of trusted certificates, **strict** certificate authentication must be selected during installation. Certificate authentication refers to a security process which checks the level of security between viewLinc and the Vaisala OPC UA Server. **Relaxed** certificate authentication allows for the use of self-signed certificates.

  For information on certificate requirements, see OPC UA client certificate requirements (page 7).

- **User authentication**: Strict user authentication makes sure that OPC UA client requests are only accepted from a recognized OPC UA client username/password. Relaxed user authentication automatically accepts anonymously generated requests from OPC UA clients.

The Vaisala OPC UA Server installation wizard provides the option to generate certificates for use with OPC UA clients.

Generate a Certificate	Install a Trusted Certificate
For companies with network access limited to a few PCs	For companies with remote network access needs
Created during Vaisala OPC UA Server installation	Certificate request generated internally and sent to a certificate signing authority for paid validation
Valid for up to 10 years	Valid for 2 years
Free	Cost varies/annual renewal fee
Use when relaxed security connections are allowed between Vaisala OPC UA Server and your OPC UA clients.	Use when strict security connections are required between Vaisala OPC UA Server and your OPC UA clients.

OPC UA client certificate requirements

OPC UA client certificates can be either self-signed certificates or CA-signed certificates. Both self-signed certificates and CA certificates must have the following minimum properties to be accepted.

1. **Key Usage**: the **`keyUsage`** property must have these options as a minimum:
   - **`digitalSignature`**
   - **`nonRepudiation`**
   - **`keyEncipherment`**
   - **`dataEncipherment`**
2. **Extended Key Usage**: the **`extendedkeyUsage`** property must have these properties:
   - **`serverAuth`**
   - **`clientAuth`**
3. **Subject Alternative**: the names list must have these entries as a minimum:
   - **URI.1** = Application URI
   - **DNS.1** = Fully qualified host name

Subject Alternative names list entry example:

- **URI.1** = **`urn:Vaisala:OpcUaServer`**
- **DNS.1** = **`myhost.vaisala.com`**

Allowing certificates to be trusted by the OPC UA Server

Both self-signed certificates and CA certificates must be made trusted in the OPC UA Server in order to be able to connect using them. For instructions on making the certificates trusted, see the following sections:

Allowing self-signed certificates to be trusted (page 7)

Allowing CA-signed certificates to be trusted (no certificate revocation list) (page 8)

Allowing CA-signed certificates to be trusted (with certificate revocation list) (page 8)

Allowing self-signed certificates to be trusted

If the OPC UA client has generated its own self-signed certificate, perform the following steps to allow the certificate to be trusted by the OPC UA server.

1. Allow the client to attempt a connection. Its certificate will be rejected, and the rejected certificate will be placed into the following folder:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Move (cut/paste) the certificate from the **rejected** folder to the following location:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Restart the OPC UA Server. The next connection attempt will be trusted.

Allowing CA-signed certificates to be trusted (no certificate revocation list)

If the OPC UA client certificate has been signed by a CA, perform the following steps to allow the certificate to be trusted by the OPC UA server.

These steps apply to CA certificates when a certificate revocation list is **not** associated with them. For instructions on allowing a CA certificate to be trusted when there is a certificate revocation list associated with it, see Allowing CA-signed certificates to be trusted (with certificate revocation list) (page 8).

1. Allow the client to attempt a connection. Its certificate will be rejected, and the rejected certificate will be placed into the following folder:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Move (cut/paste) the certificate from the **rejected** folder to the following location:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Copy the CA certificate to the following location:

   ```
   <data location>>\pki\DefaultApplicationGroup\issuer\certs
   ```

   The CA certificate must be in the **DER** format with a **`.der`** extension.

4. Make sure that **`VOPCUAServer.cfg`** has the following setting:
   `[opcua]`
   `suppress_revoke_status_unknown=1`
5. Restart the OPC UA Server. The next connection attempt will be trusted.

Allowing CA-signed certificates to be trusted (with certificate revocation list)

If the OPC UA client certificate has been signed by a CA, perform the following steps to allow the certificate to be trusted by the OPC UA server.

These steps apply to CA certificates when a certificate revocation list (CRL) is associated with them. For instructions on allowing a CA certificate to be trusted when there is **not** a CRL associated with it, see Allowing CA-signed certificates to be trusted (no certificate revocation list) (page 8).

1. Allow the client to attempt a connection. Its certificate will be rejected, and the rejected certificate will be placed into the following folder:

```
<data location>\pki\DefaultApplicationGroup\rejected\certs
```

2. Move (cut/paste) the certificate from the **rejected** folder to the following location:

```
<data location>\pki\DefaultApplicationGroup\trusted\certs
```

3. Copy the CA certificate to the following location:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

> The CA certificate must be in the **DER** format with a **`.der`** extension.

4. Copy the CRL to the following location:

```
<data location>\pki\DefaultApplicationGroup\issuer\crl
```

> The CRL must be in the **DER** format with a **`.crl`** extension.

5. Make sure that **`VOPCUAServer.cfg`** has the following setting:
   `[opcua]`
   `suppress_revoke_status_unknown=0`
6. Restart the OPC UA Server. The next connection attempt will be trusted.

Installing Vaisala OPC UA Server

Before you start the Vaisala OPC UA Server Installation Wizard, make sure you have completed the installation prerequisite tasks outlined in the setup checklist.

Vaisala OPC UA Server software is installed as a Windows service. This service will only run on the LOCALSYSTEM user account, the Windows default account with full control of the system. If your computer system is configured with custom security settings, the Vaisala OPC UA services may need additional configuration to run. See Troubleshooting (page 14).

Table 1 Setup checklist

VOPC UA Server installation prerequisite tasks	
☐	Vaisala OPC UA Server license key added to viewLinc. The same license key entered in viewLinc is entered during Vaisala OPC UA Server installation. Refer to the add license key instructions in the *viewLinc User Guide*.
☐	A dedicated group and user configured in viewLinc. The dedicated group must have View permission to access the required Zone and/or Location data. The user account is used only to transfer data to the Vaisala OPC UA Server so that activity between viewLinc and the Vaisala OPC UA Server can be traced clearly in the Events log. Refer to the add group and add user instructions in the *viewLinc User Guide*.
☐	viewLinc hostname identified, or IP address (a recognized certificate hostname is required if your network requires certificate authentication).[1)]
☐	viewLinc port number identified (default is 443).
☐	Vaisala OPC UA server port number identified (default is 55000).
☐	Your OPC UA client username and password identified (if your network requires a unique user to authenticate data requests).[2)]

1) *Your company security policy determines whether you are required to use strict or relaxed certificate authentication for connections between Vaisala OPC UA Server to viewLinc Enterprise Server*
2) *If strict user authentication is required to authorize data requests between Vaisala OPC UA Server and OPC UA clients, you must identify the username/password that will be used to initiate requests from the OPC UA client.*

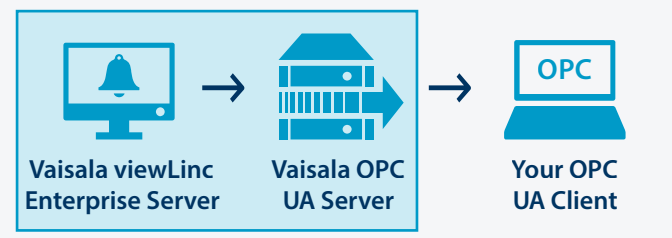
Install Vaisala OPC UA Server software

Check your Group Security Policy settings to make sure your user account has the necessary permission to run software on the installation server.

1. On a dedicated server, insert the Vaisala OPC UA Server USB and run *VOPCUAServerSetup.exe*.

> To install Vaisala OPC UA Server software on a remote server, copy the *VOPCUAServerSetup.exe* file from the USB to the destination server.

2. Select the installation language. This language setting is used in the wizard.
3. Make sure you have completed the setup prerequisites. Check each option to confirm, then click Next.
4. Enter your Vaisala OPC UA Server license key.
5. Accept the Vaisala General License Conditions.
6. Accept the default installation path for the software, or specify a new destination folder (location must have at least 2 GB of free disk space).
7. Accept the default installation path for data, or specify a new destination folder (location must have at least 1 GB of free disk space).
8. To configure the connection between viewLinc Enterprise Server and the Vaisala OPC UA Server, first choose the Certificate authentication settings:



Relaxed:
Data transfers permitted using a self-signed security certificate.

Strict:
Data transfers require that the viewLinc Enterprise Server provide a trusted certificate hostname. If this option is selected, the viewLinc hostname entered must match the trusted certificate, and the username and password must be configured in viewLinc.

9. Add the viewLinc connection details:

viewLinc IP address or hostname:
Type the viewLinc Enterprise Server hostname your network PCs use to connect with viewLinc through a browser, or the IP address. Note that a fully qualified domain name is required if you are setting up strict certificate authentication (for example, *viewLinc.mycompany.com*).

viewLinc Port number:
Accept the default port number, 443, or type a new port number.

viewLinc OPC UA username/password:
Type the dedicated username and password that was created in viewLinc. This user account is used by the Vaisala OPC UA Server to communicate with viewLinc.

10. Test the connection. When all viewLinc settings are valid, you can click Next to continue.

11. Choose to generate certificate files or upload trusted certificate and key files:

    Keep existing certificate and key

    For upgrade only. Choose this option to automatically use the certificate files currently installed on OPC UA clients.

    Upload a certificate and key (trusted)

    Choose this option if you already have trusted certificate and key files and they are available on your network.

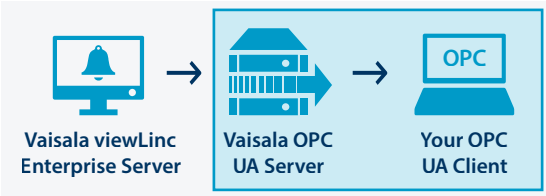
    Generate VOPC UA Server-signed certificate and key files

    Choose this option if your security policy permits a relaxed security connection with OPC UA clients, or you want to purchase a trusted certificate at a later time.

    You can use the generated **`.csr`** file to purchase a trusted certificate for installation on OPC UA clients. See Updating certificates (page 14).

12. To configure the connection between Vaisala OPC UA Server and your OPC UA client, choose the user authentication requirement:

    Relaxed:

    Ensures data transfers are accepted without requiring a dedicated username/password (anonymous data requests from an OPC UA client are permitted).

    Strict

    Data transfers are only recognized if the request is from a recognized user account. After selecting this option, enter the accepted username/password combination (see step 14).

13. Add the Vaisala OPC UA Server port number the OPC UA client will use to communicate with the Vaisala OPC UA Server (default is 55000).
14. If you selected strict user authentication, enter the designated OPC UA client username and password authorized to generate requests.
15. Click **Install**
16. Click **Finish** to complete the installation wizard.
17. To verify the installation was successful, open the Services window (open the Windows Start menu and type **`Services`**), and locate Vaisala OPC UA Server in the Name column. The status should read, **Running**. If the service is not running, see Troubleshooting (page 14).

viewLinc data parameters

After installation of the Vaisala OPC UA Server is complete, OPC UA clients can be configured to retrieve the following viewLinc parameters:

Parameter
Device name
Probe serial number
Device serial number
Device channel number
Calibration date
Location name
Location time stamp
Location value (measurement): realtime
Location value (measurement): historical
Location units

Maintenance activities

CAUTION! Changes to the VOPC UA Server configuration file should only be performed by system administrators.

Updating certificates

You can update an expired security certificate, or update the Vaisala OPC UA Server system to use a trusted certificate.

1. Stop the Vaisala OPC UA Server service.
2. Locate the certificate and key folders in the default data installation path, for example: *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\certs* *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\private*
3. Replace the existing *\certs* folder file, *application_rsa_sha256.der*, and *\private* folder file, *application_rsa_sha256_key.pem*.
4. Start Vaisala OPC UA Server service.

Changing security levels

Depending on your security policy, you may need to change security certificate or user authentication requirements. A full description of strict vs. relaxed authentication is covered in Security requirements (page 6).

1. Stop the Vaisala OPC UA Server service.
2. Start the installation wizard, *VOPCUAServerSetup.exe*.
3. To change the certificate authentication security level, go to **viewLinc Enterprise Server Connection** step and change the certificate authentication to **Strict** or **Relaxed**.
4. To change the user authentication security level, go to **Your OPC UA Client Connection** step and change the user authentication to **Strict** or **Relaxed**.
5. Complete the installation wizard steps as required.
6. Start the Vaisala OPC UA Server service.

Troubleshooting

Vaisala OPC UA Server Service not running

By default Vaisala OPC UA Server software installs as a Windows service which is permitted to run only on the LOCALSYSTEM user account; this is the Windows default account which has full control on the system. If your computer system is configured with custom security settings, the Vaisala OPC UA Server service may need additional configuration to run.

1. Open the Windows **Start** menu and open or type **Services**.

2. Locate the **Vaisala OPC UA Server Service** and open the **Properties** window.
3. On the **Log on** tab select **This account**, then enter an authorized username and password. The user must have read and execute permission on all installed program files sub folders, inheritable Full Control access on all sub folders, and network access rights to allow it to connect to other systems.

OPC UA Service fails to load

If the OPC UA Service fails to load, check the *Log\VOPCUAServerlog* file and the *log\VOPCUAServer_trace.log* file for the following messages:

- Vaisala OPC UA Server failed to load Configuration. [error code]
- Vaisala OPC UA Server failed to create add policy for level 1. [error code]
- Vaisala OPC UA Server failed to create add policy for level 2. [error code]
- Vaisala OPC UA Server initialize failed. [error code]
- Vaisala OPC UA Server failed to create certificate store. [error code]
- Vaisala OPC UA Server failed to create certificate. [error code]
- Vaisala OPC UA Server failed to create certificate request. [error code]

The [error code] shown at the end of the message is an internal error code for support purposes. Contact Vaisala Support to investigate why initialization is failing.

OPC UA client not connecting

If you generated security certificate files during installation, you may want to install the generated **.crt** file on connecting OPC UA client machines. This prevents possible connection errors when not using a trusted certificate.

1. On each OPC UA client, copy the generated certificate file (*VOPCUAServer-CA.crt)*) to any desktop location, then right-click on the file to select **Install Certificate**.
2. In the **Certificate Import Wizard Welcome** screen, select **Local Machine**.
3. On the **Certificate Store** screen select **Place all**, click **Browse**, and then select **Trusted Root Certification Authorities**. If you receive an unknown publisher warning, click **OK**.
4. Click **Finish**, then **Yes**.

Certificate rejected when attempting to connect

OPC UA client certificates can be either self-signed certificates or CA-signed certificates. Both self-signed certificates and CA certificates must have certain minimum properties in place, and they must be allowed to be trusted by the OPC UA server.

For information on correct certificate properties, see OPC UA client certificate requirements (page 7).

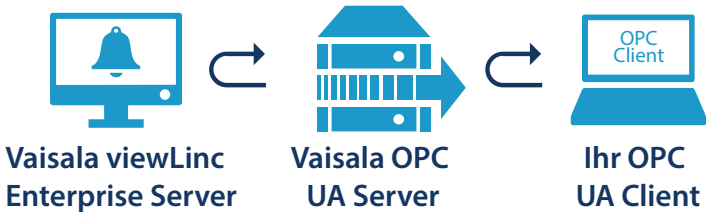
For instructions on allowing self-signed and CA-signed certificates to be trusted by OPC UA server, see the following sections:

- Allowing self-signed certificates to be trusted (page 7)
- Allowing CA-signed certificates to be trusted (no certificate revocation list) (page 8)
- Allowing CA-signed certificates to be trusted (with certificate revocation list) (page 8)

Vaisala OPC UA Server

Die Software Vaisala OPC UA Server unterstützt das Abrufen von Echtzeit- und historischen Daten aus Vaisala viewLinc Enterprise Server mit Drittanbieteranwendungen, die auf einem OPC UA Clientcomputer ausgeführt werden.

Wenn Vaisala OPC UA Server eine Datenanforderung von einem OPC UA Client empfängt, verwendet die Software Vaisala API-Aufrufe, um Daten aus viewLinc Enterprise Server abzurufen. Nachdem die Anforderung autorisiert wurde, sendet viewLinc Enterprise Server die Daten mittels sicherer Datenübertragung an Vaisala OPC UA Server. Diese Software überträgt die Daten wiederum an den anfordernden OPC UA Client.



Systemanforderungen

Verfügbarkeit	Dedizierter Server, der rund um die Uhr verfügbar ist
Servermanagement	Empfohlen: Verbunden mit einer unterbrechungsfreien Stromversorgung (USV)
	Empfohlen: Datensicherungslösung, die geöffnete Dateien sichern kann
Betriebssystem	Windows Server® 2019 (64 Bit) Windows Server® 2016 (64 Bit) Windows Server® 2012 R2 (64 Bit) Windows® 10 Enterprise (64 Bit)
Für die Anwendung erforderlicher Festplattenspeicher	2 GB
Sicherheitszertifikat für Weboberfläche	Autorisiertes TLS-Zertifikat mit Schlüssel
Lizenzschlüssel	OPC UA Server Lizenzschlüssel (auf USB-Laufwerk).

1) *Das Vaisala OPC UA Server signierte Zertifikat und der Schlüssel können im Rahmen der Installation generiert werden.*

Lizenzanforderungen

Die Software Vaisala OPC UA Server wird mit einem Lizenzschlüssel (auf dem USB-Datenträger mit den Installationsdateien) geliefert, damit die OPC Funktion in viewLinc Enterprise Server aktiviert werden kann. Der betreffende Lizenzschlüssel muss im Vaisala OPC UA Server Installationsassistenten eingegeben werden.

Die OPC UA Server Lizenz muss mindestens die gleiche Anzahl an Geräten unterstützen wie der viewLinc Enterprise Server Lizenzschlüssel.

Für ein Upgrade der Vaisala OPC UA Server Lizenz auf eine neue Größe muss nur der neue Lizenzschlüssel in viewLinc eingegeben werden.

Sicherheitsanforderungen

Vaisala OPC UA Server kann mit strikter oder lockerer Zertifikatauthentifizierung für viewLinc Enterprise Server und mit strikter oder lockerer Benutzerauthentifizierung zwischen Vaisala OPC UA Server und OPC UA Clients eingerichtet werden. Die Entscheidung für eine strikte oder lockere Authentifizierung hängt von der Sicherheitsrichtlinie des Unternehmens ab.

- **Certificate authentication**: Wenn die Sicherheitsrichtlinie die Verwendung vertrauenswürdiger Zertifikate voraussetzt, muss bei der Installation die **strikte** Zertifikatauthentifizierung gewählt werden. Zertifikatauthentifizierung bezeichnet ein Verfahren, mit dem die Sicherheitsstufe zwischen viewLinc und Vaisala OPC UA Server geprüft werden kann. Die **lockere** Zertifikatauthentifizierung erlaubt die Verwendung selbstsignierter Zertifikate.

  Weitere Informationen zu Zertifikatanforderungen siehe Anforderungen an OPC UA Clientzertifikate (Seite 19).

- **User authentication**: Die strikte Benutzerauthentifizierung stellt sicher, dass OPC UA Clientanforderungen nur akzeptiert werden, wenn sie mit einer bekannten Kombination aus OPC UA Clientbenutzername und -kennwort übermittelt werden. Bei lockerer Benutzerauthentifizierung werden anonym generierte Anforderungen von OPC UA Clients automatisch akzeptiert.

Der Vaisala OPC UA Server Installationsassistent ermöglicht das Generieren von Zertifikaten für die Verwendung mit OPC UA Clients.

Zertifikat generieren	Vertrauenswürdiges Zertifikat installieren
Für Unternehmen, in denen nur wenige PCs Netzwerkzugang haben	Für Unternehmen, die Remotenetzwerkzugriff benötigen
Während der Installation von Vaisala OPC UA Server erstellt	Zertifikatsanforderung wird intern generiert und zur kostenpflichtigen Validierung an eine Zertifizierungsstelle gesendet
Gültig für bis zu 10 Jahre	Gültig für 2 Jahre
Kostenlos	Kosten variieren/Jahresgebühr
Nutzen Sie diese Möglichkeit, wenn Verbindungen mit lockerer Sicherheit zwischen Vaisala OPC UA Server und den OPC UA Clients zulässig sind.	Nutzen Sie diese Möglichkeit, wenn Verbindungen mit strikter Sicherheit zwischen Vaisala OPC UA Server und den OPC UA Clients erforderlich sind.

Anforderungen an OPC UA Clientzertifikate

OPC UA Clientzertifikate können selbstsignierte oder CA-signierte Zertifikate sein. Sowohl selbstsignierte als auch CA-Zertifikate müssen mindestens die folgenden Eigenschaften aufweisen, damit sie akzeptiert werden.

1. **Schlüsselverwendung**: Die Eigenschaft **`keyUsage`** muss mindestens diese Optionen haben:
   - **`digitalSignature`**
   - **`nonRepudiation`**
   - **`keyEncipherment`**
   - **`dataEncipherment`**
2. **Erweiterte Schlüsselverwendung**: Die Eigenschaft **`extendedkeyUsage`** muss diese Eigenschaften haben:
   - **`serverAuth`**
   - **`clientAuth`**
3. **Subject Alternative**: Die Namensliste muss mindestens folgende Einträge enthalten:
   - **URI.1** = Anwendungs-URI
   - **DNS.1** = vollständig qualifizierter Hostname

Beispiel für Einträge in der Liste **Subject Alternative Names**:

- **URI.1** = **`urn:Vaisala:OpcUaServer`**
- **DNS.1** = **`myhost.vaisala.com`**

Zertifikate können vom OPC UA Server als vertrauenswürdig eingestuft werden

Selbstsignierte und CA-Zertifikate müssen im OPC UA Server als vertrauenswürdig eingestuft werden, damit eine Verbindung unter Verwendung dieser Zertifikate hergestellt werden kann. Anweisungen zum Einstufen von Zertifikaten als vertrauenswürdig finden Sie in den folgenden Abschnitten:

Selbstsignierte Zertifikate können als vertrauenswürdig eingestuft werden (Seite 20)

CA-signierte Zertifikate können als vertrauenswürdig eingestuft werden (keine Zertifikatsperrliste) (Seite 20)

CA-signierte Zertifikate können als vertrauenswürdig eingestuft werden (mit Zertifikatsperrliste) (Seite 21)

Selbstsignierte Zertifikate können als vertrauenswürdig eingestuft werden

Wenn der OPC UA Client ein selbstsigniertes Zertifikat generiert hat, führen Sie die folgenden Schritte aus, damit das Zertifikat vom OPC UA Server als vertrauenswürdig eingestuft werden kann.

1. Erlauben Sie dem Client, eine Verbindung herzustellen. Das Zertifikat wird abgelehnt und im folgenden Ordner gespeichert:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Verschieben Sie das Zertifikat (mittels Ausschneiden/Einfügen) aus dem Ordner **rejected** in folgenden Ordner:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Starten Sie OPC UA Server neu. Beim nächsten Verbindungsversuch wird das Zertifikat als vertrauenswürdig eingestuft.

CA-signierte Zertifikate können als vertrauenswürdig eingestuft werden (keine Zertifikatsperrliste)

Wenn das OPC UA Clientzertifikat von einer CA signiert wurde, führen Sie die folgenden Schritte aus, damit das Zertifikat vom OPC UA Server als vertrauenswürdig eingestuft werden kann.

Diese Schritte gelten für CA-Zertifikate, denen **keine** Zertifikatsperrliste zugeordnet ist. Anweisungen zur Einstufung eines CA-Zertifikats mit zugeordneter Zertifikatsperrliste als vertrauenswürdig siehe CA-signierte Zertifikate können als vertrauenswürdig eingestuft werden (mit Zertifikatsperrliste) (Seite 21).

1. Erlauben Sie dem Client, eine Verbindung herzustellen. Das Zertifikat wird abgelehnt und im folgenden Ordner gespeichert:

```
<data location>\pki\DefaultApplicationGroup\rejected\certs
```

2. Verschieben Sie das Zertifikat (mittels Ausschneiden/Einfügen) aus dem Ordner **rejected** in folgenden Ordner:

```
<data location>\pki\DefaultApplicationGroup\trusted\certs
```

3. Kopieren Sie das CA-Zertifikat in folgenden Ordner:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

> Das CA-Zertifikat muss im **DER**-Format mit der Dateinamenserweiterung **`.der`** vorliegen.

4. Stellen Sie sicher, dass für **`VOPCUAServer.cfg`** folgende Einstellung gilt:
   `[opcua]`
   `suppress_revoke_status_unknown=1`
5. Starten Sie OPC UA Server neu. Beim nächsten Verbindungsversuch wird das Zertifikat als vertrauenswürdig eingestuft.

CA-signierte Zertifikate können als vertrauenswürdig eingestuft werden (mit Zertifikatsperrliste)

Wenn das OPC UA Clientzertifikat von einer CA signiert wurde, führen Sie die folgenden Schritte aus, damit das Zertifikat vom OPC UA Server als vertrauenswürdig eingestuft werden kann.

> Diese Schritte gelten für CA-Zertifikate, denen keine Zertifikatsperrliste (CRL) zugeordnet ist. Anweisungen zur Einstufung eines CA-Zertifikats als vertrauenswürdig, dem **keine** CRL zugeordnet ist, siehe CA-signierte Zertifikate können als vertrauenswürdig eingestuft werden (keine Zertifikatsperrliste) (Seite 20).

1. Erlauben Sie dem Client, eine Verbindung herzustellen. Das Zertifikat wird abgelehnt und im folgenden Ordner gespeichert:

```
<data location>\pki\DefaultApplicationGroup\rejected\certs
```

2. Verschieben Sie das Zertifikat (mittels Ausschneiden/Einfügen) aus dem Ordner **rejected** in folgenden Ordner:

```
<data location>\pki\DefaultApplicationGroup\trusted\certs
```

3. Kopieren Sie das CA-Zertifikat in folgenden Ordner:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

Das CA-Zertifikat muss im **DER**-Format mit der Dateinamenserweiterung **`.der`** vorliegen.

4. Kopieren Sie die CRL in folgenden Ordner:

```
<data location>\pki\DefaultApplicationGroup\issuer\crl
```

Die CRL muss im **DER**-Format mit der Dateinamenserweiterung **`.crl`** vorliegen.

5. Stellen Sie sicher, dass für **`VOPCUAServer.cfg`** folgende Einstellung gilt:
   `[opcua]`
   `suppress_revoke_status_unknown=0`
6. Starten Sie OPC UA Server neu. Beim nächsten Verbindungsversuch wird das Zertifikat als vertrauenswürdig eingestuft.

Installieren von Vaisala OPC UA Server

Bevor Sie den Vaisala OPC UA Server Installationsassistenten starten, müssen die in der Setup-Checkliste angegebenen Installationsvorbereitungen getroffen worden sein.

Die Software Vaisala OPC UA Server wird als Windows-Dienst installiert. Dieser Dienst wird nur im Benutzerkonto LOCALSYSTEM ausgeführt, dem Windows-Standardkonto mit vollständiger Systemkontrolle. Wenn das Computersystem mit benutzerdefinierten Sicherheitseinstellungen konfiguriert ist, können für die Ausführung der Vaisala OPC UA Services zusätzliche Konfigurationsschritte erforderlich sein. Siehe Fehlerbehebung (Seite 29).

Tabelle 2 Setup-Checkliste

Vorbereitungen für die Installation von VOPC UA Server	
☐	Der Lizenzschlüssel von Vaisala OPC UA Server wurde viewLinc hinzugefügt. Der in viewLinc eingegebene Lizenzschlüssel wird auch während der Installation von Vaisala OPC UA Server eingegeben. Beachten Sie die Anleitung zum Hinzufügen von Lizenzschlüsseln im *viewLinc User Guide*.
☐	In viewLinc müssen eine dedizierte Gruppe und ein dedizierter Benutzer konfiguriert sein. Die dedizierte Gruppe benötigt das Anzeigerecht für die benötigten Gebiets- und/oder Standortdaten. Das Benutzerkonto wird nur verwendet, um Daten an Vaisala OPC UA Server zu übertragen, die Aktivität zwischen viewLinc und Vaisala OPC UA Server kann also problemlos anhand des Ereignisprotokolls verfolgt werden. Beachten Sie die Anleitungen zum Hinzufügen von Gruppen und Benutzern im *viewLinc User Guide*.
☐	viewLinc Hostname oder IP-Adresse (wenn das Netzwerk eine Zertifikatauthentifizierung voraussetzt, wird ein Zertifikathostname benötigt).[1)]
☐	viewLinc Anschlussnummer (Standardwert 443).
☐	Vaisala OPC UA Server Anschlussnummer (Standardwert 55000).
☐	Benutzername und Kennwort für den OPC UA Client (wenn das Netzwerk für die Authentifizierung von Datenanforderungen einen eindeutigen Benutzer voraussetzt).[2)]

1) *Die Sicherheitsrichtlinie des Unternehmens bestimmt, ob Sie die strikte oder die entspannte Zertifikatauthentifizierung für Verbindungen zwischen Vaisala OPC UA Server und viewLinc Enterprise Server voraussetzen.*
2) *Ist die strikte Benutzerauthentifizierung für die Autorisierung von Datenanforderungen zwischen Vaisala OPC UA Server und OPC UA Clients erforderlich, müssen Sie den Benutzernamen und das Kennwort für die Initiierung von Anforderungen seitens des OPC UA Clients angeben.*

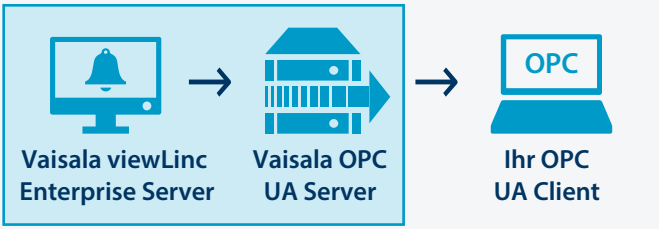
Installieren der Software Vaisala OPC UA Server

Überprüfen Sie die Einstellungen der Gruppensicherheitsrichtlinie, um sicherzustellen, dass das Benutzerkonto über die erforderliche Berechtigung zum Ausführen der Software auf dem Installationsserver verfügt.

1. Schließen Sie den USB-Datenträger mit Vaisala OPC UA Server an den dedizierten Server an und führen Sie *VOPCUAServerSetup.exe* aus.

   Um die Software Vaisala OPC UA Server auf einem Remoteserver zu installieren, kopieren Sie die Datei *VOPCUAServerSetup.exe* vom USB-Datenträger auf den Zielserver.

2. Wählen Sie die Installationssprache aus. Diese Spracheinstellung wird im Assistenten verwendet.
3. Stellen Sie sicher, dass die Setupvorbereitungen abgeschlossen wurden. Aktivieren Sie jede zu bestätigende Option und klicken Sie dann auf Weiter.
4. Geben Sie den Vaisala OPC UA Server Lizenzschlüssel ein.
5. Akzeptieren Sie die allgemeinen Lizenzbedingungen von Vaisala.
6. Übernehmen Sie den Standardinstallationspfad für die Software oder geben Sie einen neuen Zielordner an (benötigt werden mindestens 2 GB freier Festplattenspeicher).
7. Übernehmen Sie den Standardinstallationspfad für die Daten oder geben Sie einen neuen Zielordner an (benötigt wird mindestens 1 GB freier Festplattenspeicher).
8. Um die Verbindung zwischen viewLinc Enterprise Server und Vaisala OPC UA Server zu konfigurieren, wählen Sie zunächst die Einstellungen für die Zertifikatauthentifizierung:



Entspannt:
Datenübertragungen sind mit einem selbstsignierten Sicherheitszertifikat zulässig.

Strikt:
Datenübertragungen setzen voraus, dass viewLinc Enterprise Server den Hostnamen eines vertrauenswürdigen Zertifikats bereitstellt. Wenn diese Option ausgewählt ist, muss der eingegebene viewLinc Hostname dem vertrauenswürdigen Zertifikat entsprechen. Zudem müssen Benutzername und Kennwort in viewLinc konfiguriert sein.

9. Fügen Sie die viewLinc Verbindungsdetails hinzu:
   viewLinc IP-Adresse oder Hostname:
   Geben Sie den viewLinc Enterprise Server Hostnamen (oder die IP-Adresse) ein, den die PCs im Netzwerk verwenden sollen, um die Verbindung mit viewLinc über einen Browser herzustellen. Beachten Sie, dass ein vollständig qualifizierter Domänenname erforderlich ist, wenn Sie die strikte Zertifikatauthentifizierung einrichten (z. B. *viewLinc.mycompany.com*).

   viewLinc Anschlussnummer:
   Übernehmen Sie die Standardanschlussnummer 443 oder geben Sie eine neue Anschlussnummer ein.

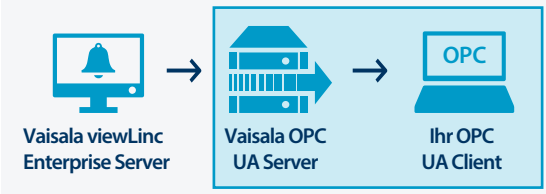
   viewLinc OPC UA Benutzername/Kennwort:
   Geben Sie den in viewLinc erstellten dedizierten Benutzernamen samt Kennwort ein. Das Benutzerkonto wird von Vaisala OPC UA Server für die Kommunikation mit viewLinc verwendet.
10. Testen Sie die Verbindung. Wenn alle viewLinc Einstellungen gültig sind, können Sie zum Fortfahren auf Weiter klicken.
11. Generieren Sie die Zertifikatdateien oder laden Sie vertrauenswürdige Zertifikat- und Schlüsseldateien hoch:
    Vorhandenes Zertifikat und vorhandenen Schlüssel beibehalten
    Nur für Upgrade. Wählen Sie diese Option, damit automatisch die Zertifikatdateien verwendet werden, die auf den OPC UA Clients installiert sind.

    Zertifikat und Schlüssel (vertrauenswürdig) hochladen
    Wählen Sie diese Option, wenn die Dateien für vertrauenswürdiges Zertifikat und Schlüssel bereits im Netzwerk verfügbar sind.

    OPC UA Server-signiertes Zertifikat und Schlüsseldateien generieren
    Wählen Sie diese Option, wenn Ihre Sicherheitsrichtlinie Verbindungen mit entspannter Sicherheit zu OPC UA Clients erlaubt oder Sie später ein vertrauenswürdiges Zertifikat erwerben möchten.

    Sie können die generierte **.csr**-Datei verwenden, um ein vertrauenswürdiges Zertifikat für die Installation auf OPC UA Clients zu erwerben. Siehe Aktualisieren von Zertifikaten (Seite 28).

12. Um die Verbindung zwischen Vaisala OPC UA Server und dem OPC UA Client zu konfigurieren, wählen Sie die Anforderung hinsichtlich der Benutzerauthentifizierung:



Entspannt:
Stellt sicher, dass Datenübertragungen ohne dedizierten Benutzernamen samt Kennwort akzeptiert werden (anonyme Datenanforderungen von einem OPC UA Client sind zulässig).

Strikt
Datenübertragungen werden nur erkannt, wenn die Anforderung von einem bekannten Benutzerkonto stammt. Nach Auswahl dieser Option geben Sie Benutzername und Kennwort ein (siehe Schritt 14).

13. Führen Sie die Vaisala OPC UA Server Anschlussnummer hinzu, die der OPC UA Client für die Kommunikation mit Vaisala OPC UA Server verwenden soll (Standardwert: 55000).
14. Wenn Sie die strikte Benutzerauthentifizierung gewählt haben, geben Sie den zum Generieren von Anforderungen autorisierten Benutzernamen für OPC UA Clients samt zugehörigem Kennwort ein.
15. Klicken Sie auf **Installieren**.
16. Klicken Sie auf **Beenden**, um den Installationsassistenten abzuschließen.
17. Um den Erfolg der Installation zu verifizieren, öffnen Sie das Dienste-Fenster (öffnen Sie das Windows-Startmenü und geben Sie `Services` ein). Suchen Sie dann in der Namensspalte nach Vaisala OPC UA Server. Der Status muss **Wird ausgeführt** lauten. Siehe Fehlerbehebung (Seite 29), wenn der Dienst nicht ausgeführt wird.

viewLinc Datenparameter

Nach der Installation von Vaisala OPC UA Server können OPC UA Clients dahingehend konfiguriert werden, die folgenden viewLinc Parameter abzurufen:

Messgröße
Gerätename
Sonden-Seriennummer
Geräte-Seriennummer
Gerätemesskanal-Nummer
Kalibrierdatum
Standortname
Standortzeitstempel
Standortwert (Messung): Echtzeit
Standortwert (Messung): Langzeitmesswerte

Messgröße
Standorteinheiten

Wartungsarbeiten

ACHTUNG Änderungen der Konfigurationsdatei von VOPC UA Server sollten nur von Systemadministratoren vorgenommen werden.

Aktualisieren von Zertifikaten

Sie können ein abgelaufenes Sicherheitszertifikat oder das Vaisala OPC UA Server System dahingehend aktualisieren, dass ein vertrauenswürdiges Zertifikat verwendet wird.

1. Stoppen Sie den Service Vaisala OPC UA Server.
2. Suchen Sie die Zertifikat- und Schlüsselordner im Standardinstallationspfad für Daten, z. B.: *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\certs* *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\private*
3. Ersetzen Sie die vorhandene Datei *application_rsa_sha256.der* im Ordner *\certs* sowie *application_rsa_sha256_key.pem* im Ordner *\private*.
4. Starten Sie den Service Vaisala OPC UA Server.

Ändern von Sicherheitsstufen

In Abhängigkeit von der geltenden Sicherheitsrichtlinie müssen Sie gegebenenfalls die Anforderungen an das Sicherheitszertifikat oder die Benutzerauthentifizierung ändern. Eine ausführliche Beschreibung der strikten im Vergleich zur entspannten Authentifizierung finden Sie unter Sicherheitsanforderungen (Seite 18).

1. Stoppen Sie den Service Vaisala OPC UA Server.
2. Starten Sie den Installationsassistenten *VOPCUAServerSetup.exe*.
3. Um die Sicherheitsstufe für die Zertifikatauthentifizierung zu ändern, navigieren Sie zum Schritt **viewLinc Enterprise Server Verbindung** und wählen für die Zertifikatauthentifizierung **Strikt** oder **Entspannt**.
4. Um die Sicherheitsstufe der Benutzerauthentifizierung zu ändern, navigieren Sie zum Schritt **Ihre OPC UA Client Verbindung** und wählen für die Benutzerauthentifizierung **Strikt** oder **Entspannt**.
5. Führen Sie die Schritte im Installationsassistenten nach Bedarf durch.
6. Starten Sie den Service Vaisala OPC UA Server.

Service Vaisala OPC UA Server wird nicht ausgeführt

Standardmäßig wird die Software Vaisala OPC UA Server als Windows-Dienst installiert, der nur im Benutzerkonto LOCALSYSTEM (Windows-Standardbenutzerkonto mit vollständiger Systemkontrolle) ausgeführt werden darf. Wenn das Computersystem mit benutzerdefinierten Sicherheitseinstellungen konfiguriert ist, können für die Ausführung des Services Vaisala OPC UA Server zusätzliche Konfigurationsschritte erforderlich sein.

1. Öffnen Sie das Windows-Menü **Start** und wählen Sie **`Services`** (oder geben Sie den Text ein).
2. Suchen Sie **Vaisala OPC UA Server Service** und öffnen Sie das Fenster **Properties**.
3. Wählen Sie auf der Registerkarte **Log on** die Option **This account**. Geben Sie dann einen autorisierten Benutzernamen und ein Kennwort ein. Der Benutzer benötigt Lese- und Ausführungsrechte für alle in Unterordnern installierten Programmdateien, vererbbaren Vollzugriff auf alle Unterordner sowie Netzwerkzugriffsrechte, damit Verbindungen zu anderen Systemen hergestellt werden können.

Der Service OPC UA kann nicht geladen werden

Wenn der Service OPC UA nicht geladen werden kann, überprüfen Sie die Dateien *`Log\VOPCUAServerlog`* und *`log\VOPCUAServer_trace.log`* auf die folgenden Meldungen:

- Der Vaisala OPC UA Server konnte die Konfiguration nicht laden. [Fehlercode]
- Der Vaisala OPC UA Server konnte keine Richtlinie zum Hinzufügen für Stufe 1 erstellen. [Fehlercode]
- Der Vaisala OPC UA Server konnte keine Richtlinie zum Hinzufügen für Stufe 2 erstellen. [Fehlercode]
- Die Initialisierung des Vaisala OPC UA Servers ist fehlgeschlagen. [Fehlercode]
- Der Vaisala OPC UA Server konnte keinen Zertifikatspeicher erstellen. [Fehlercode]
- Der Vaisala OPC UA Server konnte kein Zertifikat erstellen. [Fehlercode]
- Der Vaisala OPC UA Server konnte keine Zertifikatanforderung erstellen. [Fehlercode]

Der am Ende der Meldung angezeigte [Fehlercode] ist ein interner Fehlercode für Supportzwecke. Kontaktieren Sie den Kundendienst von Vaisala, um festzustellen, warum die Initialisierung fehlgeschlagen ist.

Der OPC UA Client stellt keine Verbindung her

Wenn Sie während der Installation Sicherheitszertifikatdateien generiert haben, können Sie die generierte **`.crt`**-Datei auf OPC UA Clientcomputern installieren, die eine Verbindung herstellen sollen. Das verhindert Verbindungsfehler, die auftreten können, wenn kein vertrauenswürdiges Zertifikat verwendet wird.

1. Kopieren Sie die generierte Zertifikatdatei (*`VOPCUAServer-CA.crt)`*) auf dem OPC UA Client an eine beliebige Position auf dem Desktop. Klicken Sie dann mit der rechten Maustaste auf die Datei und wählen Sie **Install Certificate**.
2. Wählen Sie im Bildschirm **Certificate Import Wizard Welcome** die Option **Local Machine**.
3. Wählen Sie im Bildschirm **Certificate Store** die Option **Place all**, klicken Sie auf **Browse** und wählen Sie dann **Trusted Root Certification Authorities**. Wenn eine Warnung wegen eines unbekannten Herausgebers angezeigt wird, klicken Sie auf **OK**.
4. Klicken Sie auf **Finish** und dann auf **Yes**.

Zertifikat bei Verbindungsherstellung abgewiesen

OPC UA Clientzertifikate können selbstsignierte oder CA-signierte Zertifikate sein. Selbstsignierte und CA-Zertifikate müssen bestimmte Mindesteigenschaften aufweisen und ihre Einstufung als vertrauenswürdig durch den OPC UA Server muss zugelassen werden.

Informationen zu den richtigen Zertifikateigenschaften siehe Anforderungen an OPC UA Clientzertifikate (Seite 19).

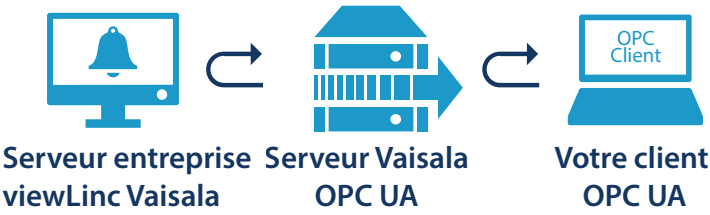
Anweisungen zum Zulassen der Einstufung selbstsignierter und CA-signierter Zertifikate als vertrauenswürdig durch den OPC UA Server enthalten folgende Abschnitte:

- Selbstsignierte Zertifikate können als vertrauenswürdig eingestuft werden (Seite 20)
- CA-signierte Zertifikate können als vertrauenswürdig eingestuft werden (keine Zertifikatsperrliste) (Seite 20)
- CA-signierte Zertifikate können als vertrauenswürdig eingestuft werden (mit Zertifikatsperrliste) (Seite 21)

À propos du serveur Vaisala OPC UA

Le logiciel du serveur Vaisala OPC UA prend en charge la récupération des données historiques et en temps réel à partir du serveur entreprise viewLinc Vaisala par des applications tierces tournant sur un client OPC UA.

Lorsque le serveur Vaisala OPC UA reçoit une demande de données d'un client OPC UA, il utilise des appels d'API Vaisala pour récupérer les données sur le serveur entreprise viewLinc. Une fois la demande autorisée, le serveur entreprise viewLinc envoie les données via un transfert sécurisé au serveur Vaisala OPC UA, qui les transfère vers le client OPC UA demandeur.



Configuration système requise

Disponibilité	Un serveur dédié, disponible 24h/24 et 7j/7
Gestion du serveur	Recommandé : connecté à un onduleur (UPS)
	Recommandé : Solution de sauvegarde prenant en charge la sauvegarde des fichiers ouverts
Système d'exploitation	Windows Server® 2019 (64 bits) Windows Server® 2016 (64 bits) Windows Server® 2012 R2 (64 bits) Windows® 10 Enterprise (64 bits)
Espace disque requis pour l'application	2 Go
Certificat de sécurité pour l'interface Web	Certification TLS et clé autorisés
Clé de licence	Clé de licence du serveur OPC UA (sur lecteur USB).

1) *Une clé et un certificat signés par le serveur Vaisala OPC UA peuvent être générés pendant l'installation.*

Conditions de licence

Le logiciel du serveur Vaisala OPC UA est fourni avec une clé de licence (sur la clé USB d'installation) pour activer la fonction OPC dans le serveur entreprise viewLinc. La clé de licence correspondante doit être saisie dans l'assistant d'installation du serveur Vaisala OPC UA.

La licence du serveur OPC UA doit prendre en charge un nombre égal ou supérieur de périphériques comme la clé de licence du serveur entreprise viewLinc.

Pour mettre à niveau la licence du logiciel du serveur Vaisala OPC UA, il vous suffit de saisir la nouvelle clé de licence dans viewLinc.

Exigences de sécurité

Le serveur Vaisala OPC UA peut être configuré avec des niveaux d'authentification de certificat stricts ou décontractés pour le serveur entreprise viewLinc et une authentification utilisateur stricte ou décontractée entre le serveur Vaisala OPC UA et les clients OPC UA. L'utilisation d'une sécurité stricte ou décontractée dépend de la politique de sécurité de votre entreprise.

- **Certificate authentication**: si votre politique de sécurité nécessite l'utilisation de certificats de confiance, l'authentification de certificat **stricte** doit être sélectionnée pendant l'installation. L'authentification par certificat fait référence à un processus de sécurité qui vérifie le niveau de sécurité entre viewLinc et le serveur Vaisala OPC UA. L'authentification de certificat **décontractée** permet l'utilisation de certificats auto-signés.

  Pour plus d'informations sur les exigences de certificat, consultez OPC UA client certificate requirements (page 33).

- **User authentication**: l'authentification utilisateur stricte veille à ce que les demandes de client OPC UA ne soient acceptées que si elles proviennent d'un nom d'utilisateur/mot de passe de client OPC UA reconnu. L'authentification utilisateur décontractée accepte automatiquement les demandes anonymes des clients OPC UA.

L'assistant d'installation du serveur Vaisala OPC UA propose en option de générer des certificats à utiliser avec des clients OPC UA.

Générer un certificat	Installer un certificat de confiance
Pour les entreprises disposant d'un accès réseau limité à quelques PC	Pour les entreprises nécessitant un accès réseau à distance
Créé pendant l'installation de du serveur Vaisala OPC UA	La demande de certificat est générée en interne et envoyée à une autorité de certification pour une validation payante
Valide pour une durée maximale de 10 ans	Valide pour 2 ans
Gratuit	Coût variable/frais de renouvellement annuels
À utiliser lorsque des connexions de sécurité décontractées sont permises entre le serveur Vaisala OPC UA et vos clients OPC UA.	À utiliser lorsque des connexions de sécurité strictes sont requises entre le serveur Vaisala OPC UA et vos clients OPC UA.

OPC UA client certificate requirements

Les certificats client OPC UA peuvent être des certificats auto-signés ou des certificats signés par une autorité de certification. Les certificats auto-signés et les certificats d'autorité de certification doivent avoir les propriétés minimales suivantes pour être acceptés.

1. **Utilisation de la clé** : la propriété **`keyUsage`** doit avoir au minimum ces options :
   - **`digitalSignature`**
   - **`nonRepudiation`**
   - **`keyEncipherment`**
   - **`dataEncipherment`**
2. **Utilisation étendue de la clé** : la propriété **`extendedkeyUsage`** doit avoir ces propriétés :
   - **`serverAuth`**
   - **`clientAuth`**
3. **Autre objet** : la liste des noms doit contenir au minimum ces entrées :
   - **URI.1** = URI d'application
   - **DNS.1** = Nom d'hôte complet

Exemple d'entrée de liste de noms **Autre objet** :

- **URI.1** = **`urn:Vaisala:OpcUaServer`**
- **DNS.1** = **`myhost.vaisala.com`**

Permettre aux certificats d'être approuvés par le serveur OPC UA

Les certificats auto-signés et les certificats d'autorité de certification doivent être approuvés dans le serveur OPC UA afin de pouvoir être utilisés pour la connexion. Pour obtenir des instructions sur l'approbation des certificats, consultez les sections suivantes :

Allowing self-signed certificates to be trusted (page 33)

Allowing CA-signed certificates to be trusted (no certificate revocation list) (page 34)

Allowing CA-signed certificates to be trusted (with certificate revocation list) (page 34)

Allowing self-signed certificates to be trusted

Si le client OPC UA a généré son propre certificat auto-signé, effectuez les étapes suivantes pour permettre au certificat d'être approuvé par le serveur OPC UA.

1. Autorisez le client à faire une tentative de connexion. Son certificat sera rejeté et placé dans le dossier suivant :

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Déplacez (couper/coller) le certificat du dossier **rejeté** vers l'emplacement suivant :

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Redémarrez le serveur OPC UA. La prochaine tentative de connexion sera approuvée.

Allowing CA-signed certificates to be trusted (no certificate revocation list)

Si le certificat du client OPC UA a été signé par une autorité de certification, effectuez les étapes suivantes pour permettre au certificat d'être approuvé par le serveur OPC UA.

Ces étapes s'appliquent aux certificats d'autorité de certification lorsqu'**aucune** liste de révocation de certificats n'est associée à ceux-ci. Pour obtenir des instructions afin de permettre à un certificat d'autorité de certification d'être approuvé lorsqu'une liste de révocation de certificats lui est associée, consultez Allowing CA-signed certificates to be trusted (with certificate revocation list) (page 34).

1. Allow the client to attempt a connection. Its certificate will be rejected, and the rejected certificate will be placed into the following folder:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Move (cut/paste) the certificate from the **rejected** folder to the following location:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Copiez le certificat d'autorité de certification à l'emplacement suivant :

   ```
   <data location>>\pki\DefaultApplicationGroup\issuer\certs
   ```

   Le certificat d'autorité de certification doit être au format **DER** avec une extension **`.der`**.

4. Assurez-vous que le réglage suivant s'applique à **`VOPCUAServer.cfg`** :
   `[opcua]`
   `suppress_revoke_status_unknown=1`
5. Restart the OPC UA Server. The next connection attempt will be trusted.

Allowing CA-signed certificates to be trusted (with certificate revocation list)

If the OPC UA client certificate has been signed by a CA, perform the following steps to allow the certificate to be trusted by the OPC UA server.

Ces étapes s'appliquent aux certificats d'autorité de certification auxquels une liste de révocation de certificats est associée. Pour obtenir des instructions afin de permettre à un certificat d'autorité de certification d'être approuvé lorsqu'**aucune** liste de révocation de certificats ne lui est associée, consultez Allowing CA-signed certificates to be trusted (no certificate revocation list) (page 34).

1. Allow the client to attempt a connection. Its certificate will be rejected, and the rejected certificate will be placed into the following folder:

```
<data location>\pki\DefaultApplicationGroup\rejected\certs
```

2. Move (cut/paste) the certificate from the **rejected** folder to the following location:

```
<data location>\pki\DefaultApplicationGroup\trusted\certs
```

3. Copy the CA certificate to the following location:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

> The CA certificate must be in the **DER** format with a **`.der`** extension.

4. Copiez la liste de révocation de certificats à l'emplacement suivant :

```
<data location>\pki\DefaultApplicationGroup\issuer\crl
```

> La liste de révocation de certificats doit être au format **DER** avec une extension **`.crl`**.

5. Make sure that **`VOPCUAServer.cfg`** has the following setting:
   `[opcua]`
   `suppress_revoke_status_unknown=0`
6. Restart the OPC UA Server. The next connection attempt will be trusted.

Installation du serveur Vaisala OPC UA

Avant de démarrer l'assistant d'installation du serveur Vaisala OPC UA Server, assurez-vous que vous avez réalisé toutes les tâches préalables à l'installation qui sont décrites dans la liste de contrôle d'installation.

Le logiciel serveur Vaisala OPC UA est installé sous forme de service Windows. Ce service ne fonctionne que sur le compte utilisateur LOCALSYSTEM, le compte Windows par défaut qui dispose du contrôle total sur le système. Si votre système informatique est configuré avec des paramètres de sécurité personnalisés, il se peut que les services Vaisala OPC UA nécessitent une configuration supplémentaire pour fonctionner. Voir dépannage (page 41).

Tableau 3 Liste de contrôle de la configuration

Tâches requises préalablement à l'installation du serveur VOPC UA	
☐	Ajout de la clé de licence du serveur Vaisala OPC UA à viewLinc. La même clé de licence que viewLinc est saisie pendant l'installation du serveur Vaisala OPC UA. Reportez-vous aux instructions d'ajout de clé de licence du *viewLinc User Guide*.
☐	Un groupe et un utilisateur dédiés sont configurés dans viewLinc. Le groupe dédié doit avoir l'autorisation d'affichage pour accéder à la zone et/ou aux données d'emplacement requises. Le compte utilisateur est utilisé uniquement pour transférer des données au serveur Vaisala OPC UA de façon à suivre clairement l'activité entre viewLinc et le serveur Vaisala OPC UA dans le journal des événements. Reportez-vous aux instructions d'ajout de groupe et d'ajout d'utilisateur du *viewLinc User Guide*.
☐	Nom d'hôte viewLinc reconnu, ou adresse IP (un nom d'hôte de certificat reconnu est requis si votre réseau nécessite l'authentification par certificat).[1)]
☐	Un numéro de port viewLinc est identifié (la valeur par défaut est 443).
☐	Un numéro de port du serveur Vaisala OPC UA est identifié (le port par défaut est 55000).
☐	Votre nom d'utilisateur et votre mot de passe de client OPC UA sont identifiés (si votre réseau nécessite un utilisateur unique pour authentifier les demandes de données).[2)]

1) *La politique de sécurité de votre entreprise détermine si vous devez utiliser l'authentification de certificat stricte ou décontractée pour les connexions entre le serveur Vaisala OPC UA et le serveur entreprise viewLinc*
2) *Si l'authentification utilisateur stricte est requise pour autoriser les demandes de données entre le serveur Vaisala OPC UA et les clients OPC UA, vous devez identifier le nom d'utilisateur/mot de passe qui seront utilisés pour envoyer des demandes à partir du client OPC UA.*

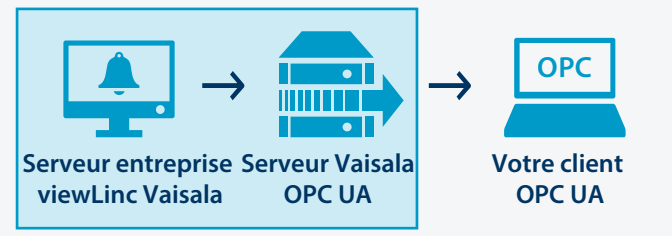
Installer le logiciel du serveur Vaisala OPC UA

Vérifiez vos paramètres de politique de sécurité de groupe pour être sûr que votre compte utilisateur a l'autorisation d'exécuter le logiciel sur le serveur d'installation.

1. Sur un serveur dédié, insérez la clé USB serveur Vaisala OPC UA et exécutez *VOPCUAServerSetup.exe*.

> Pour installer le logiciel serveur Vaisala OPC UA sur un serveur distant, copiez le fichier *VOPCUAServerSetup.exe* de la clé USB sur le serveur de destination.

2. Sélectionnez la langue d'installation. Ce paramètre de langue est utilisé dans l'assistant.
3. Confirmez que vous avez réuni les conditions préalablement requises avant l'installation. Confirmez chaque option, puis cliquez sur Suivant.
4. Saisissez votre clé de licence serveur Vaisala OPC UA.
5. Acceptez les conditions générales de licence Vaisala.
6. Acceptez le chemin d'installation par défaut du logiciel ou spécifiez un nouveau dossier de destination (l'emplacement de destination doit comporter au moins 2 Go d'espace disque disponible).
7. Acceptez le chemin d'installation par défaut des données ou spécifiez un nouveau dossier de destination (l'emplacement de destination doit comporter au moins 1 Go d'espace disque disponible).
8. Pour configurer la connexion entre le serveur entreprise viewLinc et le serveur Vaisala OPC UA, choisissez d'abord les paramètres d'authentification de certificat :



Décontractée :
Transferts de données autorisés à l'aide d'un certificat de sécurité auto-signé.

Stricte :
Les transferts de données exigent que le serveur entreprise viewLinc fournisse un nom d'hôte de certificat de confiance. Si cette option est sélectionnée, le nom d'hôte de viewLinc entré doit correspondre au certificat de confiance, et le nom d'utilisateur et le mot de passe doivent être configurés dans viewLinc.

9. Ajoutez les détails de connexion de viewLinc :

   Adresse IP ou nom d'hôte viewLinc :

   Saisissez le nom d'hôte du serveur entreprise viewLinc que les PC de votre réseau utilisent pour se connecter à viewLinc via un navigateur ou bien l'adresse IP. Veuillez noter qu'un nom de domaine complètement qualifié est requis si vous configurez l'authentification de certificat stricte (par exemple, ***`viewLinc.mycompany.com`***).

   Numéro de port viewLinc :

   Acceptez le numéro de port par défaut, 443, ou saisissez un nouveau numéro de port.

   Nom d'utilisateur/mot de passe viewLinc OPC UA :

   Saisissez le nom d'utilisateur et le mot de passe dédiés qui ont été créés dans viewLinc. Ce compte utilisateur est utilisé par le serveur Vaisala OPC UA pour communiquer avec viewLinc.

10. Testez la connexion. Lorsque tous les paramètres de viewLinc sont valides, vous pouvez cliquer sur Suivant.

11. Choisissez de générer des fichiers de certificat ou de télécharger un certificat de confiance et des fichiers de clé :

    Garder le certificat et la clé actuels

    Pour la mise à niveau uniquement. Choisissez cette option pour utiliser automatiquement les fichiers de certificat actuellement installés sur les clients OPC UA.

    Télécharger un certificat et une clé (de confiance)

    Choisissez cette option si vous possédez déjà un certificat de confiance et des fichiers de clé et que ceux-ci sont disponibles sur votre réseau.

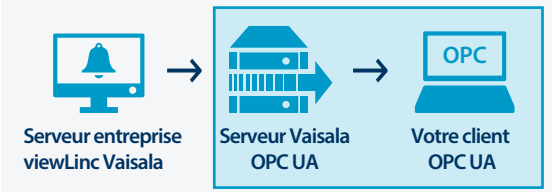
    Générer des fichiers de clé et de certificat signés VOPC UA Server

    Choisissez cette option si votre politique de sécurité permet une connexion de sécurité décontractée avec des clients OPC UA, ou si vous souhaitez acheter un certificat de confiance ultérieurement.

    Vous pouvez utiliser le fichier **`.csr`** généré pour acheter un certificat de confiance à installer sur les clients OPC UA. Voir Mise à jour des certificats (page 40).

12. Pour configurer la connexion entre le serveur Vaisala OPC UA et votre client OPC UA, sélectionnez la condition d'authentification de l'utilisateur :



Décontractée :
Garantit que les transferts de données sont acceptés sans exiger de nom d'utilisateur/mot de passe dédiés (les demandes de données anonymes d'un client OPC UA sont autorisées).

Stricte
Les transferts de données ne sont reconnus que si la demande provient d'un compte utilisateur identifié. Après avoir sélectionné cette option, saisissez la combinaison nom d'utilisateur/mot de passe acceptée (voir l'étape 14).

13. Ajoutez le numéro de port du serveur Vaisala OPC UA que le client OPC UA utilisera pour communiquer avec le serveur Vaisala OPC UA (le port par défaut est 55000).
14. Si vous avez sélectionné l'authentification utilisateur stricte, saisissez le nom d'utilisateur et le mot de passe autorisés du client OPC UA désigné pour générer les demandes.
15. Cliquez sur **Installer**
16. Cliquez sur **Terminer** pour terminer l'assistant d'installation.
17. Pour vérifier si l'installation a réussi, ouvrez la fenêtre Services (ouvrez le menu Démarrer de Windows et tapez `Services`), puis localisez Vaisala OPC UA Server dans la colonne Nom. L'état doit indiquer **En cours d'exécution**. Si le service ne fonctionne pas, voir dépannage (page 41).

Paramètres de données viewLinc

Une fois l'installation du serveur Vaisala OPC UA terminée, les clients OPC UA peuvent être configurés pour récupérer les paramètres viewLinc suivants :

Paramètre
Nom du périphérique
Numéro de série de la sonde
Numéro de série du périphérique
Numéro de canal du périphérique
Date de l'étalonnage
Nom de l'emplacement
Horodatage de l'emplacement
Valeur de l'emplacement (mesure) : temps réel
Valeur de l'emplacement (mesure) : historique
Unité de l'emplacement

Activités de maintenance

ATTENTION Le fichier de configuration de VOPC UA Server ne doit être modifié que par des administrateurs système.

Mise à jour des certificats

Vous pouvez mettre à jour un certificat de sécurité qui a expiré ou mettre à jour le système du serveur Vaisala OPC UA pour utiliser un certificat de confiance.

1. Arrêtez le service du serveur Vaisala OPC UA.
2. Localisez le certificat et les fichiers principaux dans le chemin d'installation par défaut des données, par exemple : *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\certs\ ...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\private*
3. Dans le dossier *\certs*, remplacez le fichier *application_rsa_sha256.der* existant et dans le dossier *\private*, le fichier *application_rsa_sha256_key.pem*.
4. Démarrez le service Vaisala OPC UA Server.

Modification des niveaux de sécurité

Selon votre politique de sécurité, vous devrez peut-être modifier les conditions de certificat de sécurité ou d'authentification utilisateur. Une description complète de l'authentification stricte par rapport à la version décontractée est décrite à la section Exigences de sécurité (page 32).

1. Arrêtez le service du serveur Vaisala OPC UA.
2. Lancez l'assistant d'installation, *VOPCUAServerSetup.exe*.
3. Pour modifier le niveau de sécurité d'authentification de certificat, accédez à l'étape **Connexion au serveur d'entreprise viewLinc** et changez l'authentification de certificat sur **Stricte** ou **Décontractée**.
4. Pour modifier le niveau de sécurité de l'authentification utilisateur, accédez à l'étape **Connexion de votre client OPC UA** et changez l'authentification utilisateur sur **Stricte** ou **Décontractée**.
5. Exécutez les étapes de l'assistant d'installation comme requis.
6. Démarrez le service du serveur Vaisala OPC UA.

Le service Vaisala OPC UA Server ne fonctionne pas

Par défaut, le logiciel Vaisala serveur OPC UA est installé en tant que service Windows qui ne peut être exécuté que sur le compte utilisateur LOCALSYSTEM ; c'est le compte Windows par défaut qui dispose du contrôle total sur le système. Si votre système informatique est configuré avec des paramètres de sécurité personnalisés, il se peut que le service Vaisala OPC UA Server nécessite une configuration supplémentaire pour fonctionner.

1. Ouvrez le menu **Start** de Windows, puis ouvrez ou tapez **`Services`**.
2. Localisez **Vaisala OPC UA Server Service** et ouvrez la fenêtre **Properties**.
3. Dans l'onglet **Log on**, sélectionnez **This account**, puis entrez un nom d'utilisateur et un mot de passe autorisés. L'utilisateur doit avoir des droits de lecture et d'exécution sur tous les sous-dossiers des fichiers programme installés, un accès Contrôle total héritable sur tous les sous-dossiers ainsi que des droits d'accès au réseau pour pouvoir se connecter à d'autres systèmes.

Le service OPC UA ne parvient pas à se charger

Si le service OPC UA ne parvient pas à se charger, recherchez dans le fichier *`Log\VOPCUAServerlog`* et le fichier *`log\VOPCUAServer_trace.log`* les messages suivants :

- Le serveur Vaisala OPC UA n'est pas parvenu à charger la configuration. [code d'erreur]
- Le serveur Vaisala OPC UA n'est pas parvenu à créer l'ajout de règle pour le niveau 1. [code d'erreur]
- Le serveur Vaisala OPC UA n'est pas parvenu à créer l'ajout de règle pour le niveau 2. [code d'erreur]
- L'initialisation du serveur Vaisala OPC UA a échoué. [code d'erreur]
- Le serveur Vaisala OPC UA n'est pas parvenu à créer le magasin de certificats. [code d'erreur]
- Le serveur Vaisala OPC UA n'est pas parvenu à créer le certificat. [code d'erreur]
- Le serveur Vaisala OPC UA n'est pas parvenu à créer la demande de certificat. [code d'erreur]

Le [code d'erreur] affiché à la fin du message est un code d'erreur interne à des fins d'assistance. Contactez l'assistance Vaisala pour savoir pourquoi l'initialisation échoue.

Absence de connexion du client OPC UA

Si vous avez généré des fichiers de certificat de sécurité pendant l'installation, vous souhaiterez peut-être installer le fichier **`.crt`** généré sur des ordinateurs client OPC UA qui se connectent. Cela empêche les erreurs de connexion possibles quand un certificat de confiance n'est pas utilisé.

1. Sur chaque client OPC UA, copiez le fichier de certificat généré (*`VOPCUAServer-CA.crt`*) n'importe où sur le bureau, puis cliquez avec le bouton droit sur le fichier pour sélectionner **Install Certificate**.
2. Dans l'écran **Certificate Import Wizard Welcome**, sélectionnez **Local Machine**.
3. Dans l'écran **Certificate Store**, sélectionnez **Place all**, cliquez sur **Browse**, puis sélectionnez **Trusted Root Certification Authorities**. Si un avertissement relatif à un éditeur inconnu s'affiche, cliquez sur **OK**.
4. Cliquez sur **Finish**, puis sur **Yes**.

Certificat rejeté lors de la tentative de connexion

OPC UA client certificates can be either self-signed certificates or CA-signed certificates. Les certificats auto-signés et les certificats d'autorité de certification doivent avoir certaines propriétés minimales et leur approbation par le serveur OPC UA doit être permise.

Pour plus d'informations sur les propriétés de certificat correctes, consultez OPC UA client certificate requirements (page 33).

Pour obtenir des instructions afin de permettre l'approbation par le serveur OPC UA de certificats auto-signés et de certificats signés par une autorité de certification, consultez les sections suivantes :

- Allowing self-signed certificates to be trusted (page 33)
- Allowing CA-signed certificates to be trusted (no certificate revocation list) (page 34)
- Allowing CA-signed certificates to be trusted (with certificate revocation list) (page 34)

Acerca del Servidor OPC UA de Vaisala

El software del Servidor OPC UA de Vaisala es compatible con la recuperación de datos históricos y en tiempo real del viewLinc Enterprise Server de Vaisala, por aplicaciones de terceros que se ejecutan en una máquina cliente OPC UA.

Cuando el servidor OPC UA de Vaisala recibe una solicitud de datos de un cliente OPC UA, utiliza las llamadas API de Vaisala para recuperar los datos del viewLinc Enterprise Server. Después de autorizar la solicitud, viewLinc Enterprise Server envía datos a través de una transferencia segura al servidor OPC UA de Vaisala, que luego transfiere los datos al cliente OPC UA solicitante.

Requisitos del sistema

Disponibilidad	El servidor dedicado está disponible las 24 horas, todos los días
Administración del servidor	Recomendado: Conectado a un sistema de alimentación ininterrumpida (SAI)
	Recomendado: Solución de respaldo con soporte para copias de respaldo de archivos abiertos
Sistema operativo	Windows Server® 2019 (64 bits) Windows Server® 2016 (64 bits) Windows Server® 2012 R2 (64 bits) Windows® 10 Enterprise (64 bits)
Se requiere espacio en disco de aplicación	2 GB
Certificado de seguridad para la interfaz web	Certificado y clave de TLS autorizados
Clave de licencia	Clave de licencia del Servidor OPC UA (en la unidad USB).

1) *Se puede generar el certificado firmado por el Servidor OPC UA de Vaisala y la clave durante la instalación.*

Requisitos de licencia

El software del Servidor OPC UA de Vaisala se entrega con una clave de licencia (se encuentra en el dispositivo USB de instalación) para habilitar la función OPC en viewLinc Enterprise Server. La clave de licencia correspondiente debe ingresarse en el Asistente de instalación del Servidor OPC UA de Vaisala.

La licencia del Servidor OPC UA debe admitir un número igual o mayor de dispositivos que la clave de licencia de viewLinc Enterprise Server.

Para actualizar el tamaño de la licencia del software del Servidor OPC UA de Vaisala, solo debe ingresar la nueva clave de licencia en viewLinc.

Requisitos de seguridad

El Servidor OPC UA de Vaisala se puede configurar con niveles estrictos o relajados de autenticación de certificado con viewLinc Enterprise Server y con autenticación estricta de usuario o aceptada entre el servidor OPC UA de Vaisala y los clientes OPC UA. La decisión de utilizar una seguridad estricta o relajada depende de la política de seguridad de su empresa.

- **Certificate authentication**: Si la política de seguridad requiere el uso de certificados de confianza, se debe seleccionar una autenticación de certificado **estricta** durante la instalación. La autenticación de certificado se refiere a un proceso de seguridad que verifica el nivel de seguridad entre viewLinc y el Servidor OPC UA de Vaisala. La autenticación de certificado **aceptada** permite el uso de certificados autofirmados.

  Para obtener información sobre los requisitos del certificado, consulte Requisitos del certificado de cliente OPC UA (página 45).

- **User authentication**: La autenticación de usuario estricta asegura que las solicitudes del cliente OPC UA solo se acepten desde un nombre de usuario y contraseña reconocidos del cliente OPC UA. La autenticación de usuario relajada reconoce de forma automática las solicitudes generadas anónimamente de los clientes OPC UA.

El asistente de instalación del servidor OPC UA de Vaisala ofrece la opción de generar certificados para utilizar con clientes OPC UA.

Generar un certificado	Instalar un certificado de confianza
Para empresas con acceso a la red limitado a algunos PCs	Para empresas con necesidades de acceso remoto a la red
Creado durante la instalación del servidor OPC UA de Vaisala	Solicitud de certificado generada internamente y enviada a una autoridad de firma de certificados para una validación pagada
Válido por hasta 10 años	Válido por 2 años
Gratuito	El costo varía/tarifa de renovación anual
Usar cuando se permitan conexiones de seguridad relajadas entre el Servidor OPC UA de Vaisala y sus clientes OPC UA.	Usar cuando se requieran conexiones de seguridad estrictas entre el Servidor OPC UA de Vaisala y sus clientes OPC UA.

Requisitos del certificado de cliente OPC UA

Los certificados del cliente OPC UA pueden ser certificados autofirmados o certificados CA autorizados. Para que ambos certificados (autofirmados y CA autorizados) sean aceptados deben tener las siguientes propiedades mínimas.

1. **Uso de claves**: la propiedad **`keyUsage`** debe tener estas opciones como mínimo:
   - **`digitalSignature`**
   - **`nonRepudiation`**
   - **`keyEncipherment`**
   - **`dataEncipherment`**
2. **Uso extendido de claves**: la propiedad **`extendedkeyUsage`** debe tener estas propiedades:
   - **`serverAuth`**
   - **`clientAuth`**
3. **Asunto alternativo**: la lista de nombres debe contar con estas entradas como mínimo:
   - **URI.1** = URI de aplicaciones
   - **DNS.1** = nombre de host completo

Asunto alternativo ejemplo de entrada de la lista de nombres:

- **URI.1** = **`urn:Vaisala:OpcUaServer`**
- **DNS.1** = **`myhost.vaisala.com`**

Permitir que el servidor OPC UA confíe en los certificados

Ambos certificados (autofirmados y los autorizados CA) deben ser confiables en el servidor OPC UA para poder conectarse con ellos. Para obtener instrucciones sobre cómo hacer que los certificados sean confiables, consulte las siguientes secciones:

Permitir que los certificados autofirmados sean de confianza

Si el cliente OPC UA ha generado su propio certificado autofirmado, realice los siguientes pasos para permitir que el servidor OPC UA confíe en el certificado.

1. Permita que el cliente intente una conexión. Su certificado será rechazado y el certificado rechazado se colocará en la siguiente carpeta:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Mueva (cortar y pegar) el certificado de la carpeta **rechazado** a la siguiente ubicación:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Reinicie el servidor OPC UA. Se confiará en el próximo intento de conexión.

Permitir que los certificados autorizados CA sean de confianza (sin lista de revocación de certificados)

Si el certificado de cliente OPC UA fue autorizado por una Autoridad de certificación (CA), realice los siguientes pasos para permitir que el servidor OPC UA confíe en el certificado.

Estos pasos se aplican a los certificados CA autorizados cuando se encuentra una lista de revocación de certificados **no** asociada a ellos. Para obtener instrucciones sobre cómo permitir un certificado CA autorizado de confianza cuando existe una lista de revocación de certificados asociada, consulte Permitir que los certificados autorizados CA sean de confianza (con lista de revocación de certificados) (página 47).

1. Permita que el cliente intente una conexión. Su certificado será rechazado y el certificado rechazado se colocará en la siguiente carpeta:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Mueva (cortar y pegar) el certificado de la carpeta **rechazado** a la siguiente ubicación:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Copie el certificado CA autorizado en la siguiente ubicación:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

> El certificado CA autorizado debe tener el formato **DER** con una extensión **.der**.

4. Asegúrate de que **VOPCUAServer.cfg** tiene la siguiente configuración:
   [opcua]
   suppress_revoke_status_unknown=1
5. Reinicie el servidor OPC UA. Se confiará en el próximo intento de conexión.

Permitir que los certificados autorizados CA sean de confianza (con lista de revocación de certificados)

Si el certificado de cliente OPC UA fue autorizado por una Autoridad de certificación (CA), realice los siguientes pasos para permitir que el servidor OPC UA confíe en el certificado.

> Estos pasos se aplican a los certificados CA autorizados cuando se encuentra una lista de revocación de certificados (CRL) asociada a ellos. Para obtener instrucciones sobre cómo permitir un certificado CA autorizado cuando **no** existe una CRL asociada, consulte Permitir que los certificados autorizados CA sean de confianza (sin lista de revocación de certificados) (página 46).

1. Permita que el cliente intente una conexión. Su certificado será rechazado y el certificado rechazado se colocará en la siguiente carpeta:

```
<data location>\pki\DefaultApplicationGroup\rejected\certs
```

2. Mueva (cortar y pegar) el certificado de la carpeta **rechazado** a la siguiente ubicación:

```
<data location>\pki\DefaultApplicationGroup\trusted\certs
```

3. Copie el certificado CA autorizado en la siguiente ubicación:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

> El certificado CA autorizado debe tener el formato **DER** con una extensión **.der**.

4. Copie la CRL en la siguiente ubicación:

```
<data location>\pki\DefaultApplicationGroup\issuer\crl
```

La CRL debe tener el formato **DER** con una extensión **`.crl`**.

5. Asegúrate de que **`VOPCUAServer.cfg`** tiene la siguiente configuración:
   `[opcua]`
   `suppress_revoke_status_unknown=0`
6. Reinicie el servidor OPC UA. Se confiará en el próximo intento de conexión.

Instalación del servidor OPC UA de Vaisala

Antes de iniciar el Asistente de instalación del servidor OPC UA de Vaisala, asegúrese de haber completado las tareas previas de instalación descritas en la lista de verificación de configuración.

El software de servidor OPC UA de Vaisala se instala como un servicio de Windows. Este servicio solo se ejecutará en la cuenta de usuario LOCALSYSTEM, la cuenta predeterminada de Windows con control total al sistema. Si el sistema del equipo está configurado con ajustes de seguridad personalizadas, los servicios OPC UA de Vaisala pueden requerir una configuración adicional para que se puedan ejecutar. Consulte Solución de problemas (página 54).

Tabla 4 Lista de verificación de configuración

Tareas previas de instalación del Servidor VOPC UA	
☐	Se agregó una clave de licencia del Servidor OPC UA de Vaisala a viewLinc. Se ingresa la misma clave de licencia en viewLinc durante la instalación del Servidor OPC UA de Vaisala. Consulte las instrucciones para agregar la clave de licencia en la *viewLinc User Guide*.
☐	Un grupo dedicado y un usuario configurado en viewLinc. El grupo dedicado debe tener permiso de Vista para acceder a los datos de Zona y/o ubicación requeridos. La cuenta de usuario solo se utiliza para transferir datos al servidor OPC UA de Vaisala para que la actividad entre viewLinc y este servidor se pueda rastrear claramente en el registro de eventos. Consulte las instrucciones para agregar grupo y agregar usuario en la *viewLinc User Guide*.
☐	Nombre de host de viewLinc identificado o dirección IP (se requiere un nombre de host con certificado reconocido si la red requiere autenticación de certificado).[1)]
☐	Número de puerto viewLinc identificado (el valor predeterminado es 443).
☐	Número de puerto del servidor OPC UA de Vaisala identificado (el valor predeterminado es 55000).
☐	El nombre de usuario y la contraseña del cliente OPC UA identificados (si la red requiere un usuario único para autenticar las solicitudes de datos).[2)]

1) *La política de seguridad de su empresa determina si debe utilizar una autenticación de certificado estricta o aceptada para las conexiones entre el servidor OPC UA de Vaisala y viewLinc Enterprise Server*
2) *Si se requiere una autenticación estricta del usuario para autorizar las solicitudes de datos entre el servidor OPC UA de Vaisala y los clientes OPC UA, debe identificar el nombre de usuario y la contraseña que se utilizarán para iniciar las solicitudes del cliente OPC UA.*

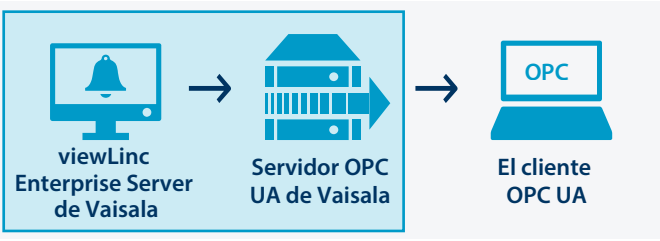
Instale el software del Servidor OPC UA de Vaisala

Verifique la configuración de su Política de seguridad del grupo para asegurarse de que la cuenta del usuario tenga los permisos necesarios para ejecutar el software en el servidor de instalación.

1. En un servidor dedicado, inserte el dispositivo USB del servidor OPC UA de Vaisala y ejecute *VOPCUAServerSetup.exe*.

   Para instalar el software del servidor OPC UA de Vaisala en un servidor remoto, copie el archivo *VOPCUAServerSetup.exe* del dispositivo USB al servidor de destino.

2. Seleccione el idioma de instalación. Esta configuración de idioma se utiliza en el asistente.
3. Asegúrese de haber completado los requisitos previos de configuración. Verifique cada opción para confirmar y luego haga clic en Siguiente.
4. Ingrese su clave de licencia del Servidor OPC UA de Vaisala.
5. Acepte las condiciones generales de licencia de Vaisala.
6. Acepte la ruta de instalación predeterminada para el software o especifique una nueva carpeta de destino (la ubicación debe tener al menos 2 GB de espacio libre en el disco).
7. Acepte la ruta de instalación predeterminada para los datos o especifique una nueva carpeta de destino (la ubicación debe tener al menos 1 GB de espacio libre en el disco).
8. Para configurar la conexión entre viewLinc Enterprise Server y el servidor OPC UA de Vaisala, primero elija la configuración de autenticación de Certificado:



Aceptado:
Se permiten las transferencias de datos mediante un certificado de seguridad autofirmado.

Estricto:
Las transferencias de datos requieren que viewLinc Enterprise Server proporcione un nombre de host de certificado de confianza. Si se selecciona esta opción, el nombre de host de viewLinc ingresado debe coincidir con el certificado de confianza y el nombre de usuario y la contraseña deben configurarse en viewLinc.

9. Agregue los detalles de la conexión viewLinc:
   Dirección IP o nombre de host de viewLinc:
   Escriba el nombre de host de viewLinc Enterprise Server que usan las computadoras de la red para conectarse con viewLinc, a través de un navegador o dirección IP. Tenga en cuenta que se requiere un nombre de dominio completo, si está configurando una autenticación de certificado estricta (por ejemplo, *`viewLinc.mycompany.com`*).

   Número de puerto viewLinc:
   Acepte el número de puerto predeterminado, 443, o escriba un nuevo número de puerto.

   Nombre de usuario y contraseña de viewLinc OPC UA:
   Escriba el nombre de usuario y la contraseña dedicados que se crearon en viewLinc. El servidor OPC UA de Vaisala utiliza esta cuenta de usuario para comunicarse con viewLinc.
10. Pruebe la conexión. Cuando todas las configuraciones de viewLinc son válidas, puede hacer clic en Siguiente para continuar.
11. Elija generar archivos de certificado o cargue un certificado de confianza y archivos de clave:
    Mantener el certificado y la clave existentes
    Solo para actualización. Elija esta opción para utilizar de forma automática los archivos de certificado actualmente instalados en los clientes OPC UA.

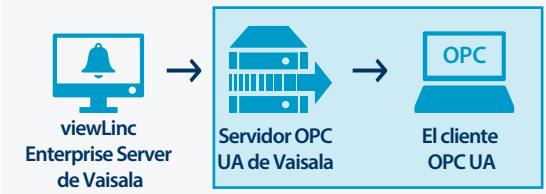
    Cargar un certificado y clave (de confianza)
    Elija esta opción si ya tiene un certificado de confianza y archivos de clave y están disponibles en la red.

    Genere certificados firmados por el servidor VOPC UA y archivos de clave
    Elija esta opción si su política de seguridad permite una conexión de seguridad aceptada con clientes OPC UA o si desea comprar un certificado de confianza más adelante.

    Puede usar el archivo **`.csr`** generado para comprar un certificado de confianza para la instalación en clientes OPC UA. Consulte Actualización de certificados (página 53).

12. Para configurar la conexión entre el Servidor OPC UA de Vaisala y el cliente que usa OPC UA, seleccione el requisito de autenticación del usuario:



Aceptado:
Garantiza que las transferencias de datos sean aceptadas sin requerir un nombre de usuario y contraseña dedicados (se permiten solicitudes de datos anónimos de un cliente que usa OPC UA).

Estricto
Las transferencias de datos solo se reconocen si la solicitud proviene de una cuenta de usuario reconocida. Después de seleccionar esta opción, ingrese la combinación de nombre de usuario y contraseña aceptados (consulte el paso 14).

13. Agregue el número de puerto del servidor OPC UA de Vaisala que el cliente que usa OPC UA utilizará para comunicarse con él (el valor predeterminado es 55000).
14. Si seleccionó la autenticación de usuario estricta, ingrese el nombre de usuario y la contraseña del cliente OPC UA designado autorizado para generar solicitudes.
15. Haga clic en **Instalar**
16. Haga clic en **Finalizar** para completar el asistente de instalación.
17. Para verificar que la instalación se realizó de forma correcta, abra la ventana Servicios (abra el menú Inicio de Windows y escriba `Services`) y busque el servidor OPC UA de Vaisala en la columna Nombre. El estado debería decir, **En ejecución**. Si el servicio no se está ejecutando, consulte Solución de problemas (página 54).

Parámetros de datos de viewLinc

Después de que se complete la instalación del Servidor OPC UA de Vaisala, se pueden configurar los clientes OPC UA para recuperar los siguientes parámetros de viewLinc:

Parámetro
Nombre del dispositivo
Número de serie de la sonda
Número de serie del dispositivo
Número de canal de dispositivo
Fecha de calibración
Nombre de ubicación
Marca de tiempo de la ubicación
Valor de la ubicación (medición): en tiempo real
Valor de la ubicación (medición): histórico
Unidades de ubicación

Actividades de mantenimiento

PRECAUCIÓN Solo los administradores del sistema deben realizar los cambios en el archivo de configuración del Servidor VOPC UA.

Actualización de certificados

Puede actualizar un certificado de seguridad expirado o actualizar el sistema del Servidor OPC UA de Vaisala para utilizar un certificado de confianza.

1. Detenga el servicio del servidor OPC UA de Vaisala.
2. Ubique el certificado y las carpetas de claves en la ruta de instalación de datos predeterminada, por ejemplo: *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\certs\ ...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\private*
3. Reemplace el archivo de la carpeta existente *\certs*, el archivo de carpeta *application_rsa_sha256.der* y *\private*, *application_rsa_sha256_key.pem*.
4. Inicie el servicio del Servidor OPC UA de Vaisala.

Cambio de niveles de seguridad

Dependiendo de la política de seguridad, es posible que deba cambiar el certificado de seguridad o los requisitos de autenticación del usuario. Una descripción completa de la autenticación estricta versus la aceptada, se incluye en Requisitos de seguridad (página 44).

1. Detenga el servicio del servidor OPC UA de Vaisala.
2. Inicie el asistente de instalación, *VOPCUAServerSetup.exe*.
3. Para cambiar el nivel de seguridad de autenticación del certificado, vaya al paso **Conexión de viewLinc Enterprise Server** y cambie la autenticación de certificado a **Estricto** o **Aceptado**.
4. Para cambiar el nivel de seguridad de autenticación de usuario, vaya al paso **Su conexión de cliente OPC UA** y cambie la autenticación de usuario a **Estricto** o **Aceptado**.
5. Complete los pasos del asistente de instalación según sea necesario.
6. Inicie el servicio del servidor OPC UA de Vaisala.

Solución de problemas

El servicio del Servidor OPC UA de Vaisala no se está ejecutando

De manera predeterminada, el software del Servidor OPC UA de Vaisala se instala como un servicio de Windows que solo se puede ejecutar en la cuenta de usuario LOCALSYSTEM. Esta es la cuenta predeterminada de Windows que tiene control total en el sistema. Si el sistema del equipo está configurado con ajustes de seguridad personalizados, el servicio del Servidor OPC UA de Vaisala puede requerir una configuración adicional para que se pueda ejecutar.

1. Abra el menú **Start** de Windows y luego abra o escriba **`Services`**.
2. Encuentre el **Vaisala OPC UA Server Service** y abra la ventana **Properties**.
3. En la pestaña **Log on**, seleccione **This account** y luego ingrese un nombre de usuario y contraseña autorizados. El usuario debe tener permiso de lectura y de ejecución en todas las subcarpetas de los archivos del programa instalado, acceso de Control total heredable en todas las subcarpetas y los derechos de acceso a la red para que pueda conectarse a otros sistemas.

Error al cargar el servicio OPC UA

Si hay un error al cargar el servicio OPC UA, verifique el archivo *`Log\VOPCUAServerlog`* y el archivo *`log\VOPCUAServer_trace.log`* para los siguientes mensajes:

- El Servidor OPC UA de Vaisala no pudo cargar la configuración. [código de error]
- El Servidor OPC UA de Vaisala no pudo crear una política de adición para el nivel 1. [código de error]
- El Servidor OPC UA de Vaisala no pudo crear una política de adición para el nivel 2. [código de error]
- Error al iniciar el Servidor OPC UA de Vaisala. [código de error]
- El Servidor OPC UA de Vaisala no pudo crear la tienda de certificados. [código de error]
- El Servidor OPC UA de Vaisala no pudo crear un certificado. [código de error]
- El Servidor OPC UA de Vaisala no pudo crear una solicitud de certificado. [código de error]

El [código de error] que se muestra al final del mensaje es un código de error interno con fines de asistencia. Póngase en contacto con el soporte de Vaisala para investigar por qué falla la inicialización.

El cliente OPC UA no se conecta

Si generó archivos de certificado de seguridad durante la instalación, es posible que desee instalar el archivo **`.crt`** generado en las máquinas conectadas del cliente OPC UA. Esto impide los posibles errores de conexión cuando no se utiliza un certificado de confianza.

1. En cada cliente OPC UA, copie el archivo del certificado generado (*`VOPCUAServer-CA.crt)`*) en cualquier ubicación del escritorio y luego haga clic derecho en el archivo para seleccionar **Install Certificate**.
2. En la pantalla **Certificate Import Wizard Welcome** , seleccione **Local Machine**.
3. En la pantalla **Certificate Store** seleccione **Place all**, haga clic en **Browse** y luego seleccione **Trusted Root Certification Authorities**. Si recibe una advertencia de un editor desconocido, haga clic en **OK**.
4. Haga clic en **Finish** y luego **Yes**.

Certificado rechazado al intentar conectarse

Los certificados del cliente OPC UA pueden ser certificados autofirmados o certificados CA autorizados. Ambos certificados (autofirmados y CA autorizados) deben tener determinadas propiedades mínimas y permitir que el servidor OPC UA confíe en los certificados.

Para obtener información sobre las propiedades correctas del certificado, consulte Requisitos del certificado de cliente OPC UA (página 45).

Para obtener instrucciones sobre cómo permitir que el servidor OPC UA confíe en certificados autofirmados y autorizados CA, consulte las siguientes secciones:

- Permitir que los certificados autofirmados sean de confianza (página 46)
- Permitir que los certificados autorizados CA sean de confianza (sin lista de revocación de certificados) (página 46)
- Permitir que los certificados autorizados CA sean de confianza (con lista de revocación de certificados) (página 47)

Sobre o Servidor OPC UA da Vaisala

O software do Servidor OPC UA da Vaisala oferece suporte à recuperação de dados históricos e em tempo real do Vaisala viewLinc Enterprise Server por aplicativos de terceiros em execução em uma máquina cliente OPC UA.

Quando o Servidor OPC UA da Vaisala recebe uma solicitação de dados de um cliente OPC UA, ele utiliza chamadas API da Vaisala para recuperar dados do viewLinc Enterprise Server. Após autorizar a solicitação, o viewLinc Enterprise Server envia dados por meio de uma transferência segura para o Servidor OPC UA da Vaisala, que transfere os dados para o cliente OPC UA solicitante.

Requisitos do sistema

Disponibilidade	Servidor dedicado, disponível 24 horas por dia, 7 dias por semana
Gerenciamento do servidor	Recomendado: Conectado a uma fonte de alimentação ininterrupta (UPS)
	Recomendado: Solução de backup com suporte a backup de arquivos abertos
Sistema operacional	Windows Server® 2019 (64 bits) Windows Server® 2016 (64 bits) Windows Server® 2012 R2 (64 bits) Windows® 10 Enterprise (64 bits)
Espaço em disco necessário para o aplicativo	2 GB
Certificado de segurança para a interface da Web	Certificado e chave TLS autorizados
Chave da licença	Chave de licença do servidor OPC UA (na unidade USB).

1) *A chave e o certificado assinados pelo Servidor OPC UA da Vaisala podem ser gerados durante a instalação.*

Requisitos de licença

O software do Servidor OPC UA da Vaisala é fornecido com uma chave de licença (encontrada no USB de instalação) para ativar o recurso OPC no viewLinc Enterprise Server. A chave de licença correspondente deve ser inserida no Assistente de instalação do servidor OPC UA da Vaisala.

A licença do servidor OPC UA deve oferecer suporte a um número igual ou superior de dispositivos como a chave de licença do viewLinc Enterprise Server.

Para atualizar o tamanho de licenciamento do software do Servidor OPC UA da Vaisala, você só precisa inserir a nova chave de licença no viewLinc.

Requisitos de segurança

O Servidor OPC UA da Vaisala pode ser configurado com níveis rígidos ou flexíveis de autenticação do certificado com o viewLinc Enterprise Server e autenticação rígida ou flexível do usuário entre o Servidor OPC UA da Vaisala e os clientes OPC UA. A decisão de usar segurança rígida ou flexível depende da política de segurança da sua empresa.

- **Certificate authentication**: Se a sua política de segurança exigir o uso de certificados confiáveis, a autenticação **rígida** do certificado deverá ser selecionada durante a instalação. A autenticação do certificado refere-se a um processo de segurança que verifica o nível de segurança entre o viewLinc e o servidor OPC UA da Vaisala. A autenticação **flexível** do certificado possibilita o uso de certificados autoassinados.

  Para obter informações sobre os requisitos de certificado, consulte Requisitos de certificado do cliente OPC UA (página 59).

- **User authentication**: A autenticação rígida do usuário garante que as solicitações do cliente OPC UA sejam aceitas apenas a partir de um nome de usuário/senha reconhecidos do cliente OPC UA. A autenticação flexível do usuário aceita automaticamente solicitações geradas anonimamente de clientes OPC UA.

O Assistente de instalação do servidor OPC UA da Vaisala oferece a opção de gerar certificados para uso com clientes OPC UA.

Gerar um certificado	Instalar um certificado confiável
Para empresas com acesso à rede limitado a alguns PCs	Para empresas com necessidades de acesso remoto à rede
Criado durante a instalação do Servidor OPC UA da Vaisala	Solicitação de certificado gerada internamente e enviada a uma autoridade de assinatura de certificado para validação paga
Válido por até 10 anos	Válido por 2 anos
Gratuito	Custo varia/taxa de renovação anual
Use quando forem permitidas conexões de segurança flexíveis entre o Servidor OPC UA da Vaisala e seus clientes OPC UA.	Use quando forem necessárias conexões de segurança rígidas entre o Servidor OPC UA da Vaisala e seus clientes OPC UA.

Requisitos de certificado do cliente OPC UA

Os certificados do cliente OPC UA podem ser autoassinados ou assinados pela CA. Certificados autoassinados e certificados de CA devem ter as seguintes propriedades mínimas para serem aceitos.

1. **Uso de chave**: a propriedade **`keyUsage`** deve ter estas opções (no mínimo):
   - **`digitalSignature`**
   - **`nonRepudiation`**
   - **`keyEncipherment`**
   - **`dataEncipherment`**
2. **Uso de chave estendido**: a propriedade **`extendedkeyUsage`** deve ter estas propriedades:
   - **`serverAuth`**
   - **`clientAuth`**
3. **Assunto alternativo**: a lista de nomes deve ter estas entradas (no mínimo):
   - **URI.1** = URI do aplicativo
   - **DNS.1** = Nome de host totalmente qualificado

Assunto alternativo exemplo de entrada da lista de nomes:

- **URI.1** = **`urn:Vaisala:OpcUaServer`**
- **DNS.1** = **`myhost.vaisala.com`**

Permitir que os certificados sejam confiáveis para o Servidor OPC UA

Certificados autoassinados e certificados de CA devem ser considerados confiáveis no Servidor OPC UA para que seja possível usá-los para se conectar. Para obter instruções sobre como tornar os certificados confiáveis, consulte as seguintes seções:

Permitir que certificados autoassinados sejam confiáveis

Se o cliente OPC UA gerou seu próprio certificado autoassinado, execute as etapas a seguir para permitir que o certificado seja confiável para o Servidor OPC UA.

1. Permita que o cliente tente uma conexão. Seu certificado será rejeitado e o certificado rejeitado será colocado na seguinte pasta:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Mova (corte/cole) o certificado da pasta **rejeitado** para o seguinte local:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Reinicie o Servidor OPC UA. A próxima tentativa de conexão será confiável.

Permitir que certificados assinados pela CA sejam confiáveis (sem lista de revogação de certificados)

Se o certificado de cliente OPC UA foi assinado por uma CA, execute as etapas a seguir para permitir que o certificado seja confiável para o Servidor OPC UA.

Essas etapas se aplicam a certificados de CA quando uma lista de revogação de certificado **não** está associada a eles. Para saber como permitir que um certificado de CA seja confiável quando há uma lista de revogação de certificados associada a ele, consulte Permitir que certificados assinados pela CA sejam confiáveis (com lista de revogação de certificados) (página 61).

1. Permita que o cliente tente uma conexão. Seu certificado será rejeitado e o certificado rejeitado será colocado na seguinte pasta:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Mova (corte/cole) o certificado da pasta **rejeitado** para o seguinte local:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Copie o certificado de CA no seguinte local:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

> O certificado de CA deve estar no formato **DER** com uma extensão **`.der`**.

4. Verifique se **`VOPCUAServer.cfg`** tem a seguinte configuração:
   `[opcua]`
   `suppress_revoke_status_unknown=1`
5. Reinicie o Servidor OPC UA. A próxima tentativa de conexão será confiável.

Permitir que certificados assinados pela CA sejam confiáveis (com lista de revogação de certificados)

Se o certificado de cliente OPC UA foi assinado por uma CA, execute as etapas a seguir para permitir que o certificado seja confiável para o Servidor OPC UA.

> Essas etapas se aplicam a certificados de CA quando uma lista de revogação de certificados (certificate revocation list, CRL) está associada a eles. Para saber como permitir que um certificado de CA seja confiável quando **não** há uma CRL associada a ele, consulte Permitir que certificados assinados pela CA sejam confiáveis (sem lista de revogação de certificados) (página 60).

1. Permita que o cliente tente uma conexão. Seu certificado será rejeitado e o certificado rejeitado será colocado na seguinte pasta:

```
<data location>\pki\DefaultApplicationGroup\rejected\certs
```

2. Mova (corte/cole) o certificado da pasta **rejeitado** para o seguinte local:

```
<data location>\pki\DefaultApplicationGroup\trusted\certs
```

3. Copie o certificado de CA no seguinte local:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

> O certificado de CA deve estar no formato **DER** com uma extensão **`.der`**.

4. Copie a CRL no seguinte local:

```
<data location>\pki\DefaultApplicationGroup\issuer\crl
```

> A CRL deve estar no formato **DER** com uma extensão **`.crl`**.

5. Verifique se **`VOPCUAServer.cfg`** tem a seguinte configuração:
   `[opcua]`
   `suppress_revoke_status_unknown=0`
6. Reinicie o Servidor OPC UA. A próxima tentativa de conexão será confiável.

Como instalar o Servidor OPC UA da Vaisala

Antes de iniciar o Assistente de instalação do servidor OPC UA da Vaisala, verifique se você concluiu as tarefas de pré-requisitos de instalação descritas na lista de verificação.

O software do Servidor OPC UA da Vaisala é instalado como um serviço do Windows. Esse serviço será executado apenas na conta do usuário LOCALSYSTEM, a conta padrão do Windows com controle total do sistema. Se o sistema do seu computador estiver configurado com definições de segurança personalizadas, os serviços do OPC UA da Vaisala poderão precisar de configuração adicional para serem executados. Consulte Resolução de problemas (página 68).

Tabela 5 Lista de verificação de configuração

Tarefas de pré-requisitos de instalação do Servidor VOPC UA	
☐	Chave de licença do servidor OPC UA da Vaisala adicionada ao viewLinc. A mesma chave de licença inserida no viewLinc é inserida durante a instalação do Servidor OPC UA da Vaisala. Para obter instruções sobre como adicionar a chave de licença, consulte o *viewLinc User Guide*.
☐	Um grupo dedicado e um usuário configurado no viewLinc. O grupo dedicado deve ter permissão Visualizar para acessar os Dados de local e/ou zona necessários. A conta do usuário é usada apenas para transferir dados para o Servidor OPC UA da Vaisala, para que a atividade entre o viewLinc e o Servidor OPC UA da Vaisala possa ser rastreada claramente no Registro de eventos. Para obter instruções sobre como adicionar grupo e adicionar usuário, consulte o *viewLinc User Guide*.
☐	Nome do host viewLinc identificado ou endereço IP (será necessário um nome de host certificado reconhecido se a sua rede exigir autenticação do certificado).[1)]
☐	Número da porta do viewLinc identificado (o padrão é 443).
☐	Número da porta do servidor OPC UA da Vaisala identificado (o padrão é 55000).
☐	Seu nome de usuário e senha do cliente OPC UA identificados (se a sua rede exigir um usuário único para autenticar solicitações de dados).[2)]

1) *A política de segurança da sua empresa determina se você precisa usar autenticação rígida ou flexível do certificado para conexões entre o Servidor OPC UA da Vaisala e o viewLinc Enterprise Server*
2) *Se for necessária uma autenticação rígida do usuário para autorizar solicitações de dados entre o Servidor OPC UA da Vaisala e os clientes OPC UA, você deverá identificar o nome de usuário/senha que serão usados para iniciar solicitações do cliente OPC UA.*

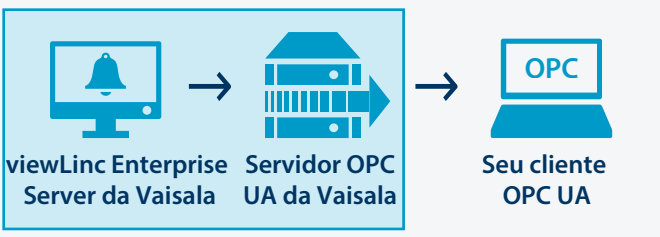
Instalar o software do Servidor OPC UA da Vaisala

Verifique as configurações da Política de segurança do grupo para garantir que sua conta de usuário tenha a permissão necessária para executar o software no servidor de instalação.

1. Em um servidor dedicado, insira o USB do Servidor OPC UA da Vaisala e execute *VOPCUAServerSetup.exe*.

> Para instalar o software do Servidor OPC UA da Vaisala em um servidor remoto, copie o arquivo *VOPCUAServerSetup.exe* do USB para o servidor de destino.

2. Selecione o idioma de instalação. Essa configuração de idioma é usada no assistente.
3. Verifique se você concluiu os pré-requisitos de configuração. Marque cada opção para confirmar e clique em Próximo.
4. Insira a sua chave de licença do servidor OPC UA da Vaisala.
5. Aceite as Condições gerais de licença da Vaisala.
6. Aceite o caminho de instalação padrão do software ou especifique uma nova pasta de destino (o local deve ter no mínimo 2 GB de espaço livre em disco).
7. Aceite o caminho de instalação padrão dos dados ou especifique uma nova pasta de destino (o local deve ter no mínimo 1 GB de espaço livre em disco).
8. Para configurar a conexão entre o viewLinc Enterprise Server e o Servidor OPC UA da Vaisala, primeiro escolha as configurações de Autenticação do certificado:



Flexível:
Transferências de dados permitidas mediante o uso de um certificado de segurança autoassinado.

Rígida:
As transferências de dados requerem que o viewLinc Enterprise Server forneça um nome de host de certificado confiável. Se esta opção for selecionada, o nome do host viewLinc digitado deverá corresponder ao certificado confiável, e o nome de usuário e a senha deverão ser configurados no viewLinc.

9. Adicione os detalhes de conexão do viewLinc:
   Nome de host ou endereço IP do viewLinc:
   Digite o nome do host do viewLinc Enterprise Server usado pelos seus computadores em rede para conectar-se ao viewLinc por meio de um navegador ou pelo endereço IP. Observe que um nome de domínio totalmente qualificado é necessário se você estiver configurando uma autenticação de certificado rígida (por exemplo, `viewLinc.mycompany.com`).

   Número da porta do viewLinc:
   Aceite o número da porta padrão, 443, ou digite um novo número de porta.

   Nome de usuário/Senha do OPC UA no viewLinc:
   Insira o nome de usuário e a senha dedicados que foram criados no viewLinc. Essa conta de usuário é usada pelo Servidor OPC UA da Vaisala para se comunicar com o viewLinc.

10. Teste a conexão. Quando todas as configurações do viewLinc forem validadas, clique em Próximo para continuar.

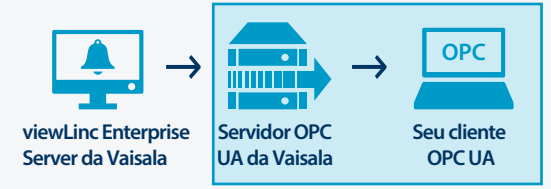
11. Escolha gerar arquivos de certificado ou carregar arquivos de certificado e chave confiáveis:
    Mantenha o certificado e a chave existentes
    Apenas para atualização. Escolha essa opção para usar automaticamente os arquivos de certificado instalados atualmente nos clientes OPC UA.

    Carregue um certificado e uma chave (confiável)
    Escolha esta opção se você já possui certificado confiável e arquivos de chave e se eles estão disponíveis na sua rede.

    Gere os arquivos de chave e o certificado assinado pelo Servidor VOPC UA
    Escolha esta opção se sua política de segurança permitir uma conexão segura flexível com clientes OPC UA ou se desejar adquirir um certificado confiável posteriormente.

    > Você pode usar o arquivo **`.csr`** gerado para adquirir um certificado confiável para instalação nos clientes OPC UA. Consulte Como atualizar certificados (página 67).

12. Para configurar a conexão entre o Servidor OPC UA da Vaisala e seu cliente OPC UA, escolha o requisito de autenticação do usuário:



    Flexível:
    Garante que as transferências de dados sejam aceitas sem a necessidade de um nome de usuário/senha dedicados (as solicitações de dados anônimas de um cliente OPC UA são permitidas).

    Rígida
    As transferências de dados são reconhecidas somente se a solicitação for de uma conta de usuário reconhecida. Após selecionar esta opção, digite a combinação de nome de usuário/senha aceitos (consulte a etapa 14).

13. Adicione o Número da porta do servidor OPC UA da Vaisala que o cliente OPC UA usará para se comunicar com o Servidor OPC UA da Vaisala (o padrão é 55000).
14. Se você selecionou a autenticação rígida do usuário, insira o nome de usuário e a senha designados do cliente OPC UA autorizados a gerar solicitações.
15. Clique em **Instalar**
16. Clique em **Concluir** para concluir o assistente de instalação.
17. Para verificar se a instalação foi bem-sucedida, abra a janela Serviços (abra o menu Iniciar do Windows e digite `Services`), e localize o Servidor OPC UA da Vaisala na coluna Nome. O status deve ser **Em execução**. Se o serviço não for executado, consulte Resolução de problemas (página 68).

Parâmetros de dados do viewLinc

Após a conclusão da instalação do servidor OPC UA da Vaisala, os clientes OPC UA podem ser configurados de modo a recuperar os seguintes parâmetros viewLinc:

Parâmetro
Nome do dispositivo
Número de série da sonda
Número de série do dispositivo
Número do canal de dispositivo
Data de calibração
Nome do local
Data e hora do local
Valor do local (medição): tempo real
Valor do local (medição): histórico
Unidades do local

Atividades de manutenção

CUIDADO Alterações no arquivo de configuração do Servidor VOPC UA devem ser realizadas somente por administradores de sistema.

Como atualizar certificados

Você pode atualizar um certificado de segurança expirado ou atualizar o sistema do Servidor OPC UA da Vaisala para usar um certificado confiável.

1. Pare o serviço do Servidor OPC UA da Vaisala.
2. Localize o certificado e as pastas chave no caminho de instalação de dados padrão, por exemplo: *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki \DefaultApplicationGroup\OWN\certs\ ...\Public Documents\Vaisala \Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\private*
3. Substitua o arquivo de pasta *\certs* existente, arquivo de pasta *application_rsa_sha256.der* e *\private*, *application_rsa_sha256_key.pem*.
4. Inicie o serviço do Servidor OPC UA da Vaisala

Como alterar os níveis de segurança

Dependendo da sua política de segurança, pode ser necessário alterar o certificado de segurança ou os requisitos de autenticação do usuário. Uma descrição completa da autenticação rígida versus flexível é abordada em Requisitos de segurança (página 58).

1. Pare o serviço do Servidor OPC UA da Vaisala.
2. Inicie o assistente de instalação, *VOPCUAServerSetup.exe*.
3. Para alterar o nível de segurança da autenticação do certificado, vá para a etapa **Conexão com o viewLinc Enterprise Server** e altere a autenticação do certificado para **Rígida** ou **Flexível**.
4. Para alterar o nível de segurança da autenticação do usuário, vá para a etapa **Sua conexão com o cliente OPC UA** e altere a autenticação do usuário para **Rígida** ou **Flexível**.
5. Conclua as etapas do assistente de instalação, conforme necessário.
6. Inicie o serviço do Servidor OPC UA da Vaisala.

Resolução de problemas

O Serviço do Servidor OPC UA da Vaisala não está em execução

Por padrão, o software do Servidor OPC UA da Vaisala é instalado como um serviço do Windows que tem permissão para ser executado apenas na conta do usuário LOCALSYSTEM; essa é a conta padrão do Windows que tem controle total sobre o sistema. Se o sistema do seu computador estiver configurado com definições de segurança personalizadas, o serviço do Servidor OPC UA da Vaisala poderá precisar de configuração adicional para ser executado.

1. Abra o menu **Start** do Windows e abra ou digite **`Services`**.
2. Localize o **Vaisala OPC UA Server Service** e abra a janela **Properties**.
3. Na guia **Log on**, selecione **This account** e insira um nome de usuário e senha autorizados. Para permitir a conexão com outros sistemas, o usuário deve ter permissão de leitura e execução de todas as subpastas dos arquivos de programas instalados, acesso herdável ao Controle Total em todas as subpastas e direitos de acesso à rede.

O Serviço OPC UA falha ao carregar

Se o serviço UA OPC falhar ao carregar, verifique o arquivo *`Log\VOPCUAServerlog`* e o arquivo *`log\VOPCUAServer_trace.log`* quanto às seguintes mensagens:

- Falha no Servidor OPC UA da Vaisala ao carregar a configuração. [código de erro]
- Falha no Servidor OPC UA da Vaisala ao criar política de adição para o nível 1. [código de erro]
- Falha no Servidor OPC UA da Vaisala ao criar política de adição para o nível 2. [código de erro]
- Falha na inicialização do Servidor OPC UA da Vaisala. [código de erro]
- O Servidor OPC UA da Vaisala falhou ao criar o armazenamento de certificados. [código de erro]
- O Servidor OPC UA da Vaisala falhou ao criar o certificado. [código de erro]
- O Servidor OPC UA da Vaisala falhou ao criar a solicitação de certificado. [código de erro]

O [código de erro] mostrado no final da mensagem é um código de erro interno para fins de suporte. Entre em contato com o suporte da Vaisala para investigar por que a inicialização está falhando.

Cliente OPC UA sem conexão

Se você gerou arquivos de certificado de segurança durante a instalação, talvez deseje instalar o arquivo **`.crt`** gerado na conexão de máquinas clientes OPC UA. Isso evitará possíveis erros de conexão quando não for usado um certificado confiável.

1. Em cada cliente OPC UA, copie o arquivo do certificado gerado (*`VOPCUAServer-CA.crt`*) em qualquer lugar da área de trabalho, clique com o botão direito no arquivo e selecione **Install Certificate**.
2. Na tela **Certificate Import Wizard Welcome** , selecione **Local Machine**.
3. Na tela **Certificate Store**, selecione **Place all**, clique em **Browse** e selecione **Trusted Root Certification Authorities**. Se você receber um alerta de emissor desconhecido, clique em **OK**.
4. Clique em **Finish** e depois em **Yes**.

Certificado rejeitado durante a tentativa de conexão

Os certificados do cliente OPC UA podem ser autoassinados ou assinados pela CA. Além de ter algumas propriedades mínimas, certificados autoassinados e certificados de CA devem ser confiáveis para o Servidor OPC UA.

Para obter informações sobre as propriedades corretas do certificado, consulte Requisitos de certificado do cliente OPC UA (página 59).

Para saber como permitir que certificados autoassinados e assinados pela CA sejam confiáveis para o Servidor OPC UA, consulte as seguintes seções:

- Permitir que certificados autoassinados sejam confiáveis (página 60)
- Permitir que certificados assinados pela CA sejam confiáveis (sem lista de revogação de certificados) (página 60)
- Permitir que certificados assinados pela CA sejam confiáveis (com lista de revogação de certificados) (página 61)

关于维萨拉 OPC UA 服务器

维萨拉 OPC UA 服务器软件支持通过在 OPC UA 客户端计算机上运行的第三方应用程序，从维萨拉 viewLinc 企业版服务器检索实时和历史数据。

当维萨拉 OPC UA 服务器从 OPC UA 客户端收到数据请求时，它利用维萨拉 API 调用从 viewLinc 企业版服务器检索数据。在对请求授权后，viewLinc 企业版服务器通过安全传输将数据发送到维萨拉 OPC UA 服务器，然后此服务器将数据传输到发出请求的 OPC UA 客户端。

系统要求

可用性	专用服务器每周 7 天、每天 24 小时可用
服务器管理	建议： 连接到不间断电源 (UPS)
	建议： 支持已打开文件备份的备份解决方案
操作系统	Windows Server® 2019（64 位） Windows Server® 2016（64 位） Windows Server® 2012 R2（64 位） Windows® 2010 企业版（64 位）
所需应用程序磁盘空间	2 GB
Web 接口的安全证书	已授权的 TLS 证书和密钥
许可证密钥	OPC UA 服务器许可证密钥（USB 驱动器中）。

1) 可以在安装过程中生成维萨拉 OPC UA 服务器签名的证书和密钥。

许可证要求

维萨拉 OPC UA 服务器软件附带许可证密钥（可在安装 USB 上找到），以在 viewLinc 企业版服务器中启用 OPC 功能。必须在维萨拉 OPC UA 服务器安装向导中输入匹配的许可证密钥。

OPC UA 服务器许可证支持的设备数必须不少于 viewLinc 企业版服务器许可证密钥。

要升级维萨拉 OPC UA 服务器软件许可规模，只需在 viewLinc 中输入新的许可证密钥。

安全要求

可以通过 viewLinc 企业版服务器为维萨拉 OPC UA 服务器设置严格或宽松的证书身份验证，并在维萨拉 OPC UA 服务器和 OPC UA 客户端之间设置严格或宽松的用户身份验证。 决定使用严格还是宽松的安全性身份验证决定取决于您公司的安全策略。

- **Certificate authentication**: 如果您的安全策略要求使用受信任的证书，则必须在安装期间选择**严格**的证书身份验证。 证书身份验证是指检查 viewLinc 和维萨拉 OPC UA 服务器之间的安全级别的安全流程。 **宽松**的证书身份验证允许使用自签名证书。

  有关证书要求的信息，请参见 OPC UA client certificate requirements (第 72 页)。

- **User authentication**: 严格的用户身份验证可确保仅从已识别的 OPC UA 客户端用户名/密码接受 OPC UA 客户端请求。 宽松的用户身份验证自动接受从 OPC UA 客户端匿名生成的请求。

维萨拉 OPC UA 服务器安装向导提供了生成用于 OPC UA 客户端的证书的选项。

Generate a Certificate（生成证书）	Install a Trusted Certificate（安装受信任的证书）
适合仅对几台 PC 进行网络访问的公司	适合具有远程网络访问需求的公司
在维萨拉 OPC UA 服务器安装期间创建	对于付费的验证，将内部生成的证书请求发送到证书签名机构
有效期长达 10 年	有效期为 2 年
免费	费用可能变化/每年支付续订费
在维萨拉 OPC UA 服务器与 OPC UA 客户端之间可接受宽松的安全连接时采用。	在维萨拉 OPC UA 服务器与 OPC UA 客户端之间需要严格的安全连接时采用。

OPC UA client certificate requirements

OPC UA 客户端证书可以是自签名证书或 CA 签名的证书。 自签名证书和 CA 证书必须至少具备以下属性才能被接受。

1. **密钥用法**： **`keyUsage`** 属性必须至少具备以下各项：
   - **`digitalSignature`**
   - **`nonRepudiation`**
   - **`keyEncipherment`**
   - **`dataEncipherment`**
2. **扩展密钥用法**： **`extendedkeyUsage`** 属性必须具备以下属性：
   - **`serverAuth`**
   - **`clientAuth`**

3. **主题替代**：名称列表必须至少包含这些条目：
   - **URI.1** = 应用程序 URI
   - **DNS.1** = 完全限定的主机名

主题替代名称列表条目示例：

- **URI.1** = `urn:Vaisala:OpcUaServer`
- **DNS.1** = `myhost.vaisala.com`

允许 OPC UA 服务器信任证书

自签名证书和 CA 证书均须在 OPC UA 服务器中受信任，以便他们能够用于连接。 有关使证书受信任的说明，请参见以下部分：

Allowing self-signed certificates to be trusted (第 73 页)

Allowing CA-signed certificates to be trusted (no certificate revocation list) (第 73 页)

Allowing CA-signed certificates to be trusted (with certificate revocation list) (第 74 页)

Allowing self-signed certificates to be trusted

如果 OPC UA 客户端已生成自己的自签名证书，请执行以下步骤来允许 OPC UA 服务器信任该证书。

1. 允许客户端尝试连接。 其证书将被拒绝，被拒绝的证书将放置在以下文件夹中：

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. 将此证书从**已拒绝**文件夹移动（剪切/粘贴）至以下位置：

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. 重新启动 OPC UA 服务器。 下一次连接尝试将被信任。

Allowing CA-signed certificates to be trusted (no certificate revocation list)

如果 OPC UA 客户端证书已由 CA 签名，请执行以下步骤来允许 OPC UA 服务器信任该证书。

当证书吊销列表**未**与 CA 证书相关联时，这些步骤适用于 CA 证书。 当证书吊销列表与 CA 证书相关联时，有关允许 CA 证书受信任的说明，请参见 Allowing CA-signed certificates to be trusted (with certificate revocation list) (第 74 页)。

1. Allow the client to attempt a connection. Its certificate will be rejected, and the rejected certificate will be placed into the following folder:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Move (cut/paste) the certificate from the **rejected** folder to the following location:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. 将 CA 证书复制到以下位置：

   ```
   <data location>>\pki\DefaultApplicationGroup\issuer\certs
   ```

   CA 证书必须为 **DER** 格式，扩展名为 **.der**。

4. 确保 **VOPCUAServer.cfg** 具有以下设置：
   [opcua]
   suppress_revoke_status_unknown=1
5. Restart the OPC UA Server. The next connection attempt will be trusted.

Allowing CA-signed certificates to be trusted (with certificate revocation list)

If the OPC UA client certificate has been signed by a CA, perform the following steps to allow the certificate to be trusted by the OPC UA server.

当证书吊销列表 (CRL) 与 CA 证书相关联时，这些步骤适用于此类证书。 当证书吊销列表**未**与 CA 证书相关联时，有关允许 CA 证书受信任的说明，请参见 Allowing CA-signed certificates to be trusted (no certificate revocation list) (第 73 页)。

1. Allow the client to attempt a connection. Its certificate will be rejected, and the rejected certificate will be placed into the following folder:

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. Move (cut/paste) the certificate from the **rejected** folder to the following location:

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. Copy the CA certificate to the following location:

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

> The CA certificate must be in the **DER** format with a **`.der`** extension.

4. 将 CRL 复制到以下位置：

```
<data location>\pki\DefaultApplicationGroup\issuer\crl
```

> CRL 必须为 **DER** 格式，扩展名为 **`.crl`**。

5. Make sure that **`VOPCUAServer.cfg`** has the following setting:
   `[opcua]`
   `suppress_revoke_status_unknown=0`
6. Restart the OPC UA Server. The next connection attempt will be trusted.

安装维萨拉 OPC UA 服务器

在启动维萨拉 OPC UA 服务器安装向导之前，确保您已完成设置清单中列出的安装先决条件任务。

维萨拉 OPC UA 服务器软件安装为一项 Windows 服务。此服务仅在 LOCALSYSTEM 用户帐户上运行，该帐户是对系统拥有完全控制权的 Windows 默认帐户。如果您的计算机系统配置了自定义安全设置，则运行维萨拉 OPC UA 服务可能需要其他配置。请参见故障排除 (第 80 页)。

表 6　设置检查列表

VOPC UA 服务器安装先决条件任务	
☐	维萨拉 OPC UA 服务器许可证密钥已添加到 viewLinc。在维萨拉 OPC UA 服务器安装期间，输入在 viewLinc 中输入的相同许可证密钥。请参阅 viewLinc User Guide 中的添加许可证密钥说明。
☐	在 viewLinc 中配置了专用组和用户。专用组必须具有“查看”权限才能访问所需的区域和/或位置数据。用户帐户仅用于将数据传输到维萨拉 OPC UA 服务器，以便可以在事件日志中清楚地跟踪 viewLinc 和维萨拉 OPC UA 服务器之间的活动。请参阅 viewLinc User Guide 中的添加组和添加用户说明。
☐	确定了 viewLinc 主机名或 IP 地址（如果您的网络需要证书身份验证，则需要使用识别的证书主机名）。[1)]
☐	确定了 viewLinc 端口号（默认为 443）。
☐	确定了维萨拉 OPC UA 服务器端口号（默认为 55000）。
☐	已确定您的 OPC UA 客户端用户名和密码（如果您的网络需要唯一用户来对数据请求进行身份验证）。[2)]

1) 您的公司安全策略确定您是否需要对维萨拉 OPC UA 服务器与 viewLinc 企业版服务器之间的连接使用严格或宽松的证书身份验证
2) 如果需要严格的用户身份验证来对维萨拉 OPC UA 服务器和 OPC UA 客户端之间的数据请求进行授权，则必须确定用于从 OPC UA 客户端启动请求的用户名/密码。

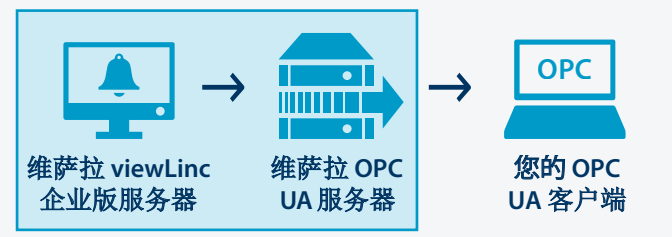
安装维萨拉 OPC UA 服务器软件

检查组安全策略设置，以确保您的用户帐户具有在安装服务器上运行软件所需要的权限。

1. 在专用服务器上，插入维萨拉 OPC UA 服务器 USB 并运行 *VOPCUAServerSetup.exe*。

要在远程服务器上安装维萨拉 OPC UA 服务器软件，请将 *VOPCUAServerSetup.exe* 文件从 USB 复制到目标服务器。

2. 选择安装语言。此语言设置用于向导中。
3. 确保您已完成设置先决条件。选中每个选项以确认，然后单击“下一步”。
4. 输入您的维萨拉 OPC UA 服务器许可证密钥。
5. 接受维萨拉一般许可条件。
6. 接受软件的默认安装路径，或指定新的目标文件夹（位置必须至少有 2 GB 的可用磁盘空间）。
7. 接受数据的默认安装路径，或指定新的目标文件夹（位置必须至少有 1 GB 的可用磁盘空间）。
8. 要配置 viewLinc 企业版服务器和维萨拉 OPC UA 服务器之间的连接，请首先选择证书身份验证设置：



Relaxed（宽松）：
允许使用自签名安全证书进行数据传输。

Strict（严格）：
数据传输要求 viewLinc 企业版服务器提供受信任的证书主机名。如果选择此选项，则输入的 viewLinc 主机名必须与受信任的证书匹配，并且必须在 viewLinc 中配置用户名和密码。

9. 添加 viewLinc 连接详细信息：
viewLinc IP address or hostname（viewLinc IP 地址或主机名）：
键入您的网络 PC 用于通过浏览器或 IP 地址与 viewLinc 连接的 viewLinc 企业版服务器主机名。请注意，如果要设置严格的证书身份验证，则需要完全限定的域名（例如，*viewLinc.mycompany.com*）。

viewLinc Port number（viewLinc 端口号）：
接受默认端口号 443 或键入新端口号。

viewLinc OPC UA username/password（viewLinc OPC UA 用户名/密码）：
键入在 viewLinc 中创建的专用用户名和密码。维萨拉 OPC UA 服务器使用此用户帐户与 viewLinc 进行通信。

10. 测试连接。当所有 viewLinc 设置都有效时，您可以单击“下一步”继续。

11. 选择生成证书文件或上传受信任的证书和密钥文件：

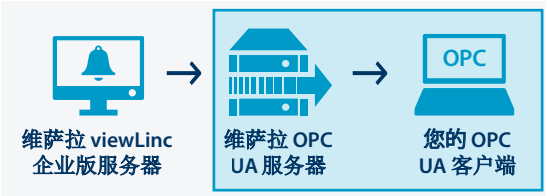
Keep existing certificate and key（保留现有证书和密钥）
仅用于升级。选择此选项可自动使用 OPC UA 客户端上当前安装的证书文件。

Upload a certificate and key (trusted)（上传证书和密钥（受信任））
如果您已经具有受信任的证书和密钥文件，而且可以在您的网络中提供这些文件，则选择此选项。

Generate VOPC UA Server-signed certificate and key files (生成 VOPC UA 服务器签名的证书和密钥文件)
如果您的安全策略允许对 OPC UA 客户端应用宽松的安全连接，或者您希望以后再购买受信任的证书，请选择此选项。

> 您可以使用生成的 **.csr** 文件购买受信任的证书，以便在 OPC UA 客户端上安装。请参见更新证书 (第 80 页)。

12. 要配置维萨拉 OPC UA 服务器与 OPC UA 客户端之间的连接，请选择用户身份验证要求：



Relaxed（宽松）：
确保接受数据传输而无需专用的用户名/密码（允许来自 OPC UA 客户端的匿名数据请求）。

Strict（严格）
仅当请求来自已识别的用户帐户时，才会识别数据传输。选择此选项后，输入接受的用户名/密码组合（请参阅步骤 14）。

13. 添加 OPC UA 客户端将用于与维萨拉 OPC UA 服务器通信的维萨拉 OPC UA 服务器端口号（默认为 55000）。
14. 如果您选择严格的用户身份验证，请输入获授权可生成请求的指定的 OPC UA 客户端用户名和密码。
15. 单击 **Install**（安装）
16. 单击 **Finish**（完成）以完成安装向导。
17. 要验证安装是否成功，请打开“服务”窗口（打开 Windows 的“开始”菜单并键入 `Services`），然后在“名称”列中找到维萨拉 OPC UA 服务器。状态应显示 **Running**（正在运行）。如果服务未在运行，请参阅故障排除 (第 80 页)。

viewLinc 数据参数

在完成维萨拉 OPC UA 服务器的安装后，您可将 OPC UA 客户端配置为检索以下 viewLinc 参数：

参数
设备名称

参数
探头序列号
设备序列号
设备信道号
校准日期
位置名称
位置时间戳
位置值（测量值）：实时
位置值（测量值）：历史
位置单位

维护活动

警告 只能由系统管理员对 VOPC UA 服务器配置文件进行更改。

更新证书

您可以更新过期的安全证书，或更新维萨拉 OPC UA 服务器系统以使用受信任的证书。

1. 停止维萨拉 OPC UA 服务器服务。
2. 在默认数据安装路径中找到证书和密钥文件夹，例如：*...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\certs\ ...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\private*
3. 替换现有的 *\certs* 文件夹文件 *application_rsa_sha256.der* 和 *\private* 文件夹文件 *application_rsa_sha256_key.pem*。
4. 启动维萨拉 OPC UA 服务器服务。

更改安全级别

根据您的安全策略，您可能需要更改安全证书或用户身份验证要求。有关严格与宽松的身份验证的完整说明，请参阅安全要求 (第 72 页)。

1. 停止维萨拉 OPC UA 服务器服务。
2. 启动安装向导 *VOPCUAServerSetup.exe*。
3. 要更改证书身份验证安全级别，请转至 **viewLinc Enterprise Server Connection**（viewLinc 企业版服务器连接）步骤，然后将证书身份验证更改为 **Strict**（严格）或 **Relaxed**（宽松）。
4. 要更改用户身份验证安全级别，请转至 **Your OPC UA Client Connection**（您的 OPC UA 客户端连接）步骤，然后将用户身份验证更改为 **Strict**（严格）或 **Relaxed**（宽松）。
5. 根据需要完成安装向导步骤。
6. 启动维萨拉 OPC UA 服务器服务。

故障排除

维萨拉 OPC UA 服务器服务未在运行

默认情况下，维萨拉 OPC UA 服务器软件安装为 Windows 服务，只允许在 LOCALSYSTEM 用户帐户上运行；该帐户是对系统拥有完全控制权的 Windows 默认帐户。 如果您的计算机系统配置了自定义安全设置，则维萨拉 OPC UA 服务器服务可能需要运行其他配置。

1. 打开 Windows **Start**（开始）菜单并打开或键入 **Services**。

2. 找到 **Vaisala OPC UA Server Service**（维萨拉 OPC UA 服务器服务）然后打开 **Properties**（属性）窗口。
3. 在 **Log on**（登录）选项卡上选择 **This account**（此帐户），然后输入授权的用户名和密码。 用户必须对所有已安装的程序文件子文件夹具有读取和执行权限，对所有子文件夹的可继承的完全控制访问权限，以及允许其连接到其他系统的网络访问权限。

OPC UA 服务加载失败

如果 OPC UA 服务加载失败，请查阅 *Log\VOPCUAServerlog* 文件和 *log\VOPCUAServer_trace.log* 文件查找以下信息：

- 维萨拉 OPC UA 服务器加载配置失败。 [错误代码]
- 维萨拉 OPC UA 服务器无法为级别 1 创建添加策略。[错误代码]
- 维萨拉 OPC UA 服务器无法为级别 2 创建添加策略。[错误代码]
- 维萨拉 OPC UA 服务器初始化失败。 [错误代码]
- 维萨拉 OPC UA 服务器创建证书存储失败。 [错误代码]
- 维萨拉 OPC UA 服务器创建证书失败。 [错误代码]
- 维萨拉 OPC UA 服务器创建证书请求失败。 [错误代码]

消息末尾显示的 [错误代码] 是用于支持用途的内部错误代码。 请联系维萨拉支持人员调查初始化失败的原因。

OPC UA 客户端未连接

如果在安装期间生成了安全证书文件，则可能需要在连接的 OPC UA 客户端计算机上安装生成的 **.crt** 文件。 这可以防止在不使用受信任的证书时出现可能的连接错误。

1. 在每个 OPC UA 客户端上，将生成的证书文件 (*VOPCUAServer-CA.crt*) 复制到任意桌面位置，然后右键单击该文件以选择 **Install Certificate**（安装证书）。
2. 在 **Certificate Import Wizard Welcome**（证书导入向导欢迎）选项卡上，选择 **Local Machine**（本地机器）。
3. 在 **Certificate Store**（证书存储）屏幕上选择 **Place all**（放置全部），点击 **Browse**（浏览），然后选择 **Trusted Root Certification Authorities**（受信任的根认证机构）。 如果您收到未知发布者警告，请单击 **OK**（确定）。
4. 请单击 **Finish**（完成），然后单击 **Yes**（是）。

尝试连接时证书被拒绝

OPC UA client certificates can be either self-signed certificates or CA-signed certificates. 自签名证书和 CA 证书必须至少具备某些属性，且必须被允许受 OPC UA 服务器信任。

有关相关证书属性的信息，请参见 OPC UA client certificate requirements (第 72 页)。

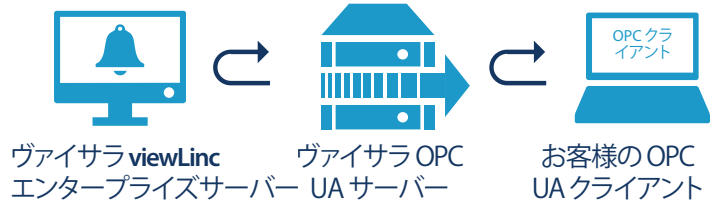
有关允许 OPC UA 服务器信任自签名和 CA 签名证书的说明，请参见以下部分：

- Allowing self-signed certificates to be trusted (第 73 页)
- Allowing CA-signed certificates to be trusted (no certificate revocation list) (第 73 页)
- Allowing CA-signed certificates to be trusted (with certificate revocation list) (第 74 页)

ヴァイサラ OPC UA サーバーについて

ヴァイサラ OPC UA サーバーソフトウェアは、OPC UA クライアントコンピューター上で実行されているサードパーティのアプリケーションを通じて、ヴァイサラ viewLinc エンタープライズサーバーからリアルタイムデータや履歴データを取得するのをサポートします。

ヴァイサラ OPC UA サーバーは、OPC UA クライアントからデータ要求を受け取ると、ヴァイサラ API コールを使用して viewLinc エンタープライズサーバーからデータを取得します。viewLinc エンタープライズサーバーは、要求を認証してから、安全な転送によりヴァイサラ OPC UA サーバーにデータを送信します。その後、ヴァイサラ OPC UA サーバーは、データを要求元の OPC UA クライアントに転送します。



システム要件

可用性	専用サーバーは 24 時間年中無休で稼働可能
サーバー管理	推奨：無停電電源（UPS）に接続
	推奨：オープンファイルのバックアップに対応したバックアップソリューション
オペレーティングシステム	Windows Server® 2019（64 ビット） Windows Server® 2016（64 ビット） Windows Server® 2012 R2（64 ビット） Windows® 10 Enterprise（64 ビット）
必要なアプリケーションディスク容量	2GB
Web インターフェース用のセキュリティ証明書	認証済みの TLS 証明書とキー
ライセンスキー	OPC UA サーバーのライセンスキー（USB ドライブ上）。

1) ヴァイサラ OPC UA サーバー署名証明書とキーはインストール中に生成できます。

ライセンス要件

ヴァイサラ OPC UA サーバーソフトウェアにはライセンスキーが同梱されています（インストール USB に保存されています）。そのライセンスキーを使用すると、viewLinc エンタープライズサーバーの OPC 機能を有効にできます。一致するライセンスキーを、ヴァイサラ OPC UA サーバーのインストールウィザードに入力する必要があります。

OPC UA サーバーライセンスは、viewLinc エンタープライズサーバーライセンスキーと同等またはそれ以上の数のデバイスをサポートする必要があります。

ヴァイサラ OPC UA サーバーソフトウェアのライセンスは、viewLinc に新しいライセンスキーを入力するだけでアップグレードできます。

セキュリティ要件

ヴァイサラ OPC UA サーバーでは、viewLinc エンタープライズサーバーとの間で厳格または寛容なレベルの証明書の認証を、OPC UA クライアントとの間で厳格または寛容なユーザー認証を設定できます。厳格なセキュリティを使用するか、寛容なセキュリティを使用するかについては、会社のセキュリティポリシーに応じて決定してください。

- **Certificate authentication**:セキュリティポリシーによって信頼できる証明書の使用が求められている場合、インストール時に**厳格な**証明書の認証を選択する必要があります。証明書の認証とは、viewLinc とヴァイサラ OPC UA サーバーとの間でセキュリティレベルのチェックを行うセキュリティプロセスです。**寛容な**証明書の認証では、自己署名証明書を使用できます。

  証明書の要件については、OPC UA クライアント証明書の要件 (ページ 85)を参照してください。

- **User authentication**:厳格なユーザー認証を選択した場合、OPC UA クライアントの要求は、承認済み OPC UA クライアントのユーザー名/パスワードからの要求のみ受理されます。寛容なユーザー認証では、OPC UA クライアントから生成された匿名の要求が自動的に受理されます。

ヴァイサラ OPC UA サーバーインストールウィザードには、OPC UA クライアントで使用する証明書を生成するオプションが用意されています。

証明書を生成する	信頼できる証明書をインストールする
ネットワークアクセスが少数の PC に制限されている会社の場合	リモートネットワークアクセスが必要な会社の場合
ヴァイサラ OPC UA サーバーのインストール時に作成	有償で検証してもらうために手元で生成した証明書リクエストを証明書署名機関に送信
最大 10 年間有効	2 年間有効
無償	費用はそれぞれ異なり、年間更新手数料がかかる場合がある
ヴァイサラ OPC UA サーバーと OPC UA クライアント間で寛容なセキュリティ接続が認められている場合に使用	ヴァイサラ OPC UA サーバーと OPC UA クライアント間で厳格なセキュリティ接続が求められている場合に使用

OPC UA クライアント証明書の要件

OPC UA クライアント証明書は、自己署名証明書または CA 署名証明書のいずれかです。受け入れられるためには、自己署名証明書と CA 証明書の両方で少なくとも次のプロパティが必要です。

1. **鍵用途**：**keyUsage** プロパティには少なくとも次のオプションが必要です。
   - **digitalSignature**
   - **nonRepudiation**
   - **keyEncipherment**
   - **dataEncipherment**
2. **拡張キー用途**：**extendedkeyUsage** プロパティには次のプロパティが必要です。
   - **serverAuth**
   - **clientAuth**
3. **サブジェクトの別名**：この名前リストには、少なくとも次のエントリが必要です。
   - **URI.1** = アプリケーション URI
   - **DNS.1** = 完全修飾ホスト名

サブジェクトの別名名前リストのエントリの例：

- **URI.1** = **urn:Vaisala:OpcUaServer**
- **DNS.1** = **myhost.vaisala.com**

OPC UA サーバーが証明書を信頼できるようにする

自己署名証明書と CA 証明書の両方について、それらを使用して接続するには、それらが OPC UA サーバーで信頼されている必要があります。証明書を信頼できるようにする手順については、次のセクションを参照してください。

自己署名証明書を信頼できるようにする (ページ 85)

CA 署名付き証明書を信頼できるようにする（証明書失効リストなし） (ページ 86)

CA 署名付き証明書を信頼できるようにする（証明書失効リストあり） (ページ 86)

自己署名証明書を信頼できるようにする

OPC UA クライアントが独自の自己署名証明書を生成した場合は、次の手順を実施して、OPC UA サーバーが証明書を信頼できるようにします。

1. クライアントが接続を試行できるようにします。その証明書は拒否され、拒否された証明書は次のフォルダーに配置されます。

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. 証明書を **rejected** フォルダーから次の場所に移動（切り取り/貼り付け）します。

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. OPC UA サーバーを再起動します。次の接続試行は信頼されます。

CA 署名付き証明書を信頼できるようにする（証明書失効リストなし）

OPC UA クライアント証明書が CA によって署名された場合は、次の手順を実施して、OPC UA サーバーが証明書を信頼できるようにします。

これらの手順は、証明書失効リストが CA 証明書に関連付けられて**いない**場合に CA 証明書に適用されます。証明書失効リストが関連付けられている場合に CA 証明書を信頼できるようにする手順については、CA 署名付き証明書を信頼できるようにする（証明書失効リストあり） (ページ 86)を参照してください。

1. クライアントが接続を試行できるようにします。その証明書は拒否され、拒否された証明書は次のフォルダーに配置されます。

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. 証明書を **rejected** フォルダーから次の場所に移動（切り取り/貼り付け）します。

   ```
   <data location>\pki\DefaultApplicationGroup\trusted\certs
   ```

3. CA 証明書を次の場所にコピーします。

   ```
   <data location>>\pki\DefaultApplicationGroup\issuer\certs
   ```

   CA 証明書は **.der** 拡張子を持つ **DER** 形式である必要があります。

4. **VOPCUAServer.cfg** で次の設定がされていることを確認してください。
   [opcua]
   suppress_revoke_status_unknown=1
5. OPC UA サーバーを再起動します。次の接続試行は信頼されます。

CA 署名付き証明書を信頼できるようにする（証明書失効リストあり）

OPC UA クライアント証明書が CA によって署名された場合は、次の手順を実施して、OPC UA サーバーが証明書を信頼できるようにします。

これらの手順は、証明書失効リスト（CRL）が CA 証明書に関連付けられている場合に CA 証明書に適用されます。CRL が関連付けられて**いない**場合に CA 証明書を信頼できるようにする手順については、CA 署名付き証明書を信頼できるようにする（証明書失効リストなし） (ページ 86)を参照してください。

1. クライアントが接続を試行できるようにします。その証明書は拒否され、拒否された証明書は次のフォルダーに配置されます。

   ```
   <data location>\pki\DefaultApplicationGroup\rejected\certs
   ```

2. 証明書を **rejected** フォルダーから次の場所に移動（切り取り/貼り付け）します。

```
<data location>\pki\DefaultApplicationGroup\trusted\certs
```

3. CA 証明書を次の場所にコピーします。

```
<data location>>\pki\DefaultApplicationGroup\issuer\certs
```

CA 証明書は **.der** 拡張子を持つ **DER** 形式である必要があります。

4. CRL を次の場所にコピーします。

```
<data location>\pki\DefaultApplicationGroup\issuer\crl
```

CRL は **.crl** 拡張子を持つ **DER** 形式である必要があります。

5. **VOPCUAServer.cfg** で次の設定がされていることを確認してください。
   [opcua]
   suppress_revoke_status_unknown=0
6. OPC UA サーバーを再起動します。次の接続試行は信頼されます。

ヴァイサラ OPC UA サーバーのインストール

ヴァイサラ OPC UA サーバーインストールウィザードを起動する前に、設定チェックリストに記載されているインストール前提条件タスクを完了していることを確認します。

ヴァイサラ OPC UA サーバーソフトウェアは Windows サービスとしてインストールされます。このサービスは、LOCALSYSTEM ユーザーアカウント（システムのフルコントロール権限を持つ Windows の既定アカウント）でのみ実行されます。コンピューターシステムがカスタムセキュリティ設定で構成されている場合、ヴァイサラ OPC UA サービスの実行にあたり、追加の構成が必要になる場合があります。「トラブルシューティング (ページ 93)」を参照してください。

表 7　設定チェックリスト

VOPC UA サーバーのインストール前提条件タスク	
☐	ヴァイサラ OPC UA サーバーライセンスキーが viewLinc に追加されている。ヴァイサラ OPC UA サーバーのインストール時に、viewLinc に入力されているものと同じライセンスキーを入力している。『viewLinc User Guide』のライセンスキーの追加手順を参照してください。
☐	viewLinc に専用のグループおよびユーザーが構成されている。必要なゾーンやロケーションデータにアクセスするには、専用のグループに表示アクセス許可が必要です。ユーザーアカウントは、ヴァイサラ OPC UA サーバーへのデータ転送にのみ使用されます。そのため、viewLinc とヴァイサラ OPC UA サーバー間のアクティビティをイベントログで明確にトレースできます。『viewLinc User Guide』のグループの追加手順とユーザーの追加手順を参照してください。
☐	viewLinc ホスト名または IP アドレスが識別されている（ネットワークで証明書の認証が必要な場合は、承認済みの証明書ホスト名が必要です）。[1]
☐	viewLinc ポート番号が識別されている（既定値は 443）。
☐	ヴァイサラ OPC UA サーバーポート番号が識別されている（既定値は 55000）。
☐	OPC UA クライアントのユーザー名とパスワードが識別されている（ネットワークで一意のユーザーがデータ要求を認証する必要がある場合）。[2]

1) 会社のセキュリティポリシーを参照して、ヴァイサラ OPC UA サーバーと viewLinc エンタープライズサーバー間の接続に、厳格または寛容な証明書の認証を使用する必要があるか判断してください。
2) ヴァイサラ OPC UA サーバーと OPC UA クライアント間のデータ要求を認証するうえで厳格なユーザー認証が必要となる場合、OPC UA クライアントからの要求を開始するために使用するユーザー名/パスワードが識別されている必要があります。

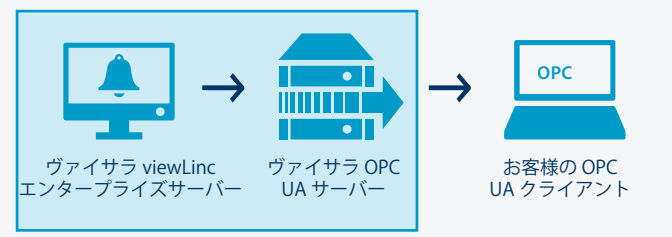
ヴァイサラ OPC UA サーバーソフトウェアのインストール

グループセキュリティポリシー設定を確認し、自分のユーザーアカウントに、インストールサーバーでのソフトウェアの実行に必要なアクセス許可があることを確認してください。

1. 専用サーバー上で、ヴァイサラ OPC UA サーバー USB を挿入し、*VOPCUAServerSetup.exe* を実行します。

> リモートサーバー上でヴァイサラ OPC UA サーバーをインストールするには、USB から *VOPCUAServerSetup.exe* ファイルを保存先サーバーにコピーします。

2. インストール言語を選択します。この言語設定がウィザードで使用されます。
3. 設定の前提条件を完了していることを確認します。各オプションを確認し、確定したら、[次へ] をクリックします。
4. ヴァイサラ OPC UA サーバーのライセンスキーを入力します。
5. ヴァイサラの一般ライセンス条件に同意します。
6. ソフトウェアの既定のインストールパスを承諾するか、別の保存先フォルダー（ディスクの空き領域に最低 2 GB が必要）を指定します。
7. データの既定のインストールパスを承諾するか、別の保存先フォルダー（ディスクの空き領域に最低 1 GB が必要）を指定します。
8. viewLinc エンタープライズサーバーとヴァイサラ OPC UA サーバー間の接続を構成するには、まず証明書の認証設定を選択します。



Relaxed：
自己署名セキュリティ証明書を使用して、データの転送を許可します。

Strict：
データの転送には、viewLinc エンタープライズサーバーが提供する信頼できる証明書ホスト名が必要です。このオプションを選択した場合、入力した viewLinc ホスト名が信頼できる証明書と一致している必要があります。また、ユーザー名とパスワードは viewLinc で構成する必要があります。

9. viewLinc 接続の詳細を追加します。

viewLinc IP アドレスまたはホスト名：
ブラウザーから viewLinc に接続するために、ネットワーク PC で使用されている viewLinc エンタープライズサーバーのホスト名、または IP アドレスを入力します。厳格な証明書の認証を設定している場合、完全修飾ドメイン名が必要であることに注意してください（例：*viewLinc.mycompany.com*）。

viewLinc ポート番号
既定のポート番号 443 を承諾するか、別のポート番号を入力します。

viewLinc OPC UA ユーザー名/パスワード：
viewLinc で作成した専用のユーザー名とパスワードを入力します。このユーザーアカウントは、viewLinc と通信するためにヴァイサラ OPC UA サーバーによって使用されます。

10. 接続をテストします。viewLinc 設定がすべて有効である場合、[次へ] をクリックして続行します。
11. 証明書ファイルを生成するか、信頼できる証明書とキーファイルをアップロードするかを選択します。

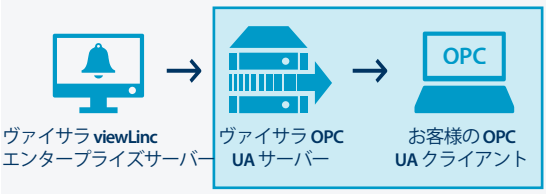
    既存証明書とキーを保持
    アップグレード専用。このオプションを選択すると、OPC UA クライアントに現在インストールされている証明書ファイルが自動的に使用されます。

    証明書とキー（信頼済み）のアップロード
    信頼できる証明書とキーファイルをすでにお持ちで、お使いのネットワーク上で使用可能な状態の場合は、このオプションを選択します。

    VOPC UA サーバー署名証明書とキーファイルの生成
    セキュリティポリシーによって OPC UA クライアントでの寛容なセキュリティ接続が認められている場合、または信頼できる証明書を後で購入する場合は、このオプションを選択します。

    > OPC UA クライアントにインストールする信頼できる証明書を購入するために、生成済みの **.csr** ファイルを使用できます。証明書の更新 (ページ 92)を参照してください。

12. ヴァイサラ OPC UA サーバーと OPC UA クライアント間の接続を構成するには、ユーザー認証要件を選択します。

    Relaxed：
    専用のユーザー名/パスワードがなくても、データ転送が受け入れられます（OPC UA クライアントからの匿名データ要求が許可されます）。

    厳格
    承認済みのユーザーアカウントからの要求である場合のみ、データの転送が承認されます。このオプションを選択した場合、承諾済みのユーザー名/パスワードの組み合わせを入力します（手順 14 を参照）。
13. OPC UA クライアントがヴァイサラ OPC UA サーバーと通信するために使用するヴァイサラ OPC UA サーバーのポート番号（既定値は 55000）を追加します。
14. 厳格なユーザー認証を選択した場合、要求の生成が許可されている指定の OPC UA クライアントのユーザー名とパスワードを入力します。
15. [**インストール**] をクリックします。
16. [**終了**] をクリックして、インストールウィザードを完了します。
17. インストールの検証が成功したら、[サービス] ウィンドウを開き（Windows の [スタート] メニューを開き、`Services` と入力してください）、[名前] 列から [Vaisala OPC UA Server Service] を見つけます。状態が [**実行中**] と表示されているはずです。サービスが実行中でない場合は、「トラブルシューティング (ページ 93)」を参照してください。

viewLinc データパラメーター

ヴァイサラ OPC UA サーバーのインストールが完了したら、次の viewLinc パラメーターを取得するように OPC UA クライアントを設定できます。

パラメーター
デバイス名
プローブシリアル番号
デバイスシリアル番号
デバイスチャネル番号
校正日
ロケーション名
ロケーションタイムスタンプ
ロケーション値（測定）：リアルタイム
ロケーション値（測定）：履歴
ロケーション単位

保守活動

注意 VOPC UA サーバー構成ファイルの変更は、システム管理者のみが行う必要があります。

証明書の更新

信頼できる証明書を使用するために、有効期限切れのセキュリティ証明書の更新やヴァイサラ OPC UA サーバーシステムの更新を行うことができます。

1. ヴァイサラ OPC UA サーバーサービスを停止します。
2. 既定のデータインストールパス（以下の例を参照）から証明書とキーフォルダーを見つけます。 *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\certs* *...\Public Documents\Vaisala\Vaisala OPC UA Server\pki\DefaultApplicationGroup\OWN\private*
3. 既存の *\certs* フォルダーのファイル（*application_rsa_sha256.der*）と *\private* フォルダーのファイル（*application_rsa_sha256_key.pem*）を置き換えます。
4. ヴァイサラ OPC UA サーバーサービスを開始します。

セキュリティレベルの変更

セキュリティポリシーによっては、セキュリティ証明書の認証要件またはユーザー認証要件の変更が必要になる場合があります。厳格な認証と寛容な認証の違いに関する詳細な説明については、「セキュリティ要件 (ページ 84)」を参照してください。

1. ヴァイサラ OPC UA サーバーサービスを停止します。
2. インストールウィザード *VOPCUAServerSetup.exe* を起動します。
3. 証明書の認証に関するセキュリティレベルを変更するには、[**viewLinc Enterprise Server の接続**] の手順に進み、証明書の認証を [**Strict**] または [**Relaxed**] に変更します。
4. ユーザー認証に関するセキュリティレベルを変更するには、[**OPC UA クライアントの接続**] の手順に進み、ユーザー認証を [**Strict**] または [**Relaxed**] に変更します。
5. 必要に応じて、インストールウィザードの各手順を完了します。
6. ヴァイサラ OPC UA サーバーサービスを開始します。

トラブルシューティング

ヴァイサラ OPC UA サーバーサービスが実行されない

ヴァイサラ OPC UA サーバーソフトウェアは、既定では、LOCALSYSTEM ユーザーアカウントでのみ実行が許可される Windows サービスとしてインストールされます。このユーザーアカウントは、システムのフルコントロール権限を持つ Windows の既定のアカウントです。コンピューターシステムがカスタムセキュリティ設定で構成されている場合、ヴァイサラ OPC UA サーバーサービスの実行にあたり、追加の構成が必要になる場合があります。

1. Windows の [**Start**] メニューを開き、[**`Services`**] を開くか、入力します。
2. [**Vaisala OPC UA Server Service**] を見つけて、[**Properties**] ウィンドウを開きます。
3. [**Log on**] タブで、[**This account**] を選択し、承認済みのユーザー名とパスワードを入力します。ユーザーには、インストールされているすべてのプログラムファイルサブフォルダーの読み取りおよび実行アクセス許可、すべてのサブフォルダーに対する継承可能なフルコントロールアクセス権、他のシステムとの接続を許可するネットワークアクセス権が必要です。

OPC UA サービスが読み込みに失敗する

OPC UA サービスが読み込みに失敗した場合は、*`Log\VOPCUAServerlog`* ファイルおよび *`log\VOPCUAServer_trace.log`* ファイルに次のメッセージがないか確認します。

- ヴァイサラ OPC UA サーバーが設定の読み込みに失敗しました。[エラーコード]
- ヴァイサラ OPC UA サーバーがレベル 1 の追加ポリシーの作成に失敗しました。[エラーコード]
- ヴァイサラ OPC UA サーバーがレベル 2 の追加ポリシーの作成に失敗しました。[エラーコード]
- ヴァイサラ OPC UA サーバーの初期化に失敗しました。[エラーコード]
- ヴァイサラ OPC UA サーバーが証明書ストアの作成に失敗しました。[エラーコード]
- ヴァイサラ OPC UA サーバーが証明書の作成に失敗しました。[エラーコード]
- ヴァイサラ OPC UA サーバーが証明書リクエストの作成に失敗しました。[エラーコード]

メッセージの最後に表示される [エラーコード] は、サポートのための内部エラーコードです。初期化が失敗する理由を調査するには、ヴァイサラサポートにお問い合わせください。

OPC UA クライアントが接続できない

インストール時にセキュリティ証明書ファイルを生成した場合、接続する OPC UA クライアントコンピューターに、生成した **`.crt`** ファイルをインストールできます。これにより、信頼できる証明書を使用しない場合でも、想定される接続エラーを回避できます。

1. 各 OPC UA クライアントで、生成した証明書ファイル（*`VOPCUAServer-CA.crt`*）をデスクトップにコピーし、そのファイルを右クリックして、[**Install Certificate**] を選択します。
2. [**Certificate Import Wizard Welcome**] 画面で、[**Local Machine**] を選択します。
3. [**Certificate Store**] 画面で [**Place all**] を選択し、[**Browse**] をクリックしてから、[**Trusted Root Certification Authorities**] を選択します。不明な発行元の警告が表示されたら、[**OK**] をクリックします。
4. [**Finish**] をクリックし、[**Yes**] をクリックします。

接続を試みた際に証明書が拒否されました

OPC UA クライアント証明書は、自己署名証明書または CA 署名証明書のいずれかです。自己署名証明書と CA 証明書はどちらも、最低限のプロパティを備えている必要があり、OPC UA サーバーにより信頼できる必要があります。

証明書の適切なプロパティについては、OPC UA クライアント証明書の要件 (ページ 85)を参照してください。

自己署名証明書と CA 署名証明書を OPC UA サーバーが信頼できるようにする手順については、次のセクションを参照してください。

- 自己署名証明書を信頼できるようにする (ページ 85)
- CA 署名付き証明書を信頼できるようにする（証明書失効リストなし） (ページ 86)
- CA 署名付き証明書を信頼できるようにする（証明書失効リストあり） (ページ 86)

VAISALA

www.vaisala.com