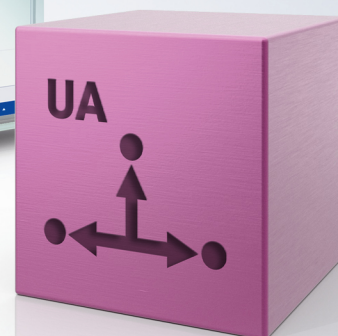
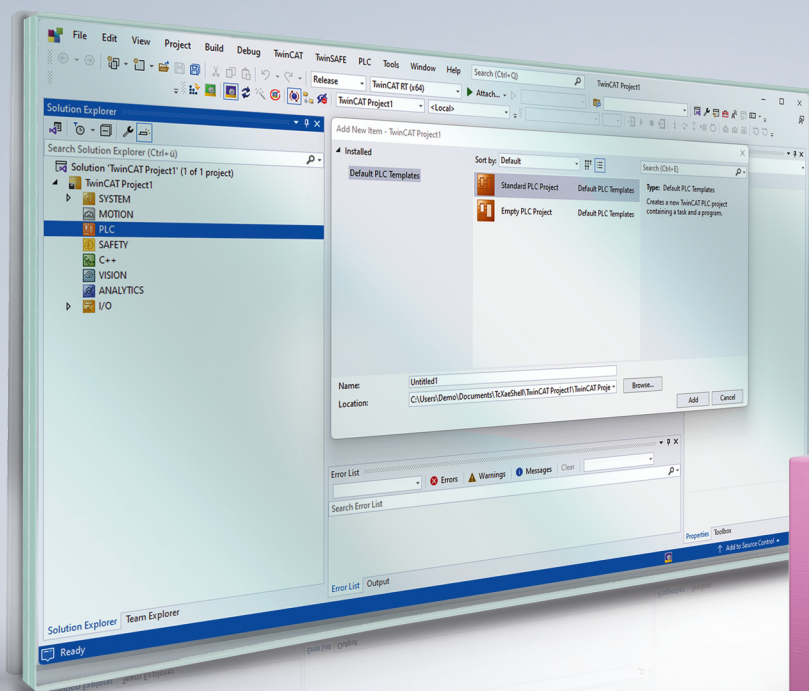


手册 | ZH

TF6100

TwinCAT 3 | OPC UA Gateway



1 前言	5
1.1 文档说明	5
1.2 安全信息	6
1.3 信息安全说明	6
1.4 文档发行状态	7
2 概述	8
3 安装	9
3.1 系统要求	9
3.2 安装	9
3.3 安装型号	11
4 技术简介	15
4.1 快速入门	15
4.2 建议的步骤	17
4.3 支持的功能	19
4.4 配置器	19
4.5 应用程序目录	20
4.6 通用设置	21
4.7 附加服务器的配置	23
4.8 端点的配置	24
4.9 TF6120 的迁移	25
4.10 安全	27
4.10.1 概述	27
4.10.2 端点	27
4.10.3 证书交换	28
4.10.4 身份验证	29
4.11 日志记录	30
5 教程	31
6 附录	32
6.1 错误诊断	32
6.2 ADS 返回代码	32
6.3 技术支持和服务	35

1 前言

1.1 文档说明

本说明仅适用于熟悉国家标准且经过培训的控制和自动化工程专家。

在安装和调试组件时，必须遵循文档和以下说明及解释。

操作人员应具备相关资质，并始终使用最新的生效文档。

相关负责人员必须确保所述产品的应用或使用符合所有安全要求，包括所有相关法律、法规、准则和标准。

免责声明

本文档经过精心准备。然而，所述产品正在不断开发中。

我们保留随时修改和更改本文档的权利，恕不另行通知。

不得依据本文档中的数据、图表和说明对已供货产品的修改提出赔偿。

商标

Beckhoff®、ATRO®、EtherCAT®、EtherCAT G®、EtherCAT G10®、EtherCAT P®、MX-System®、Safety over EtherCAT®、TC/BSD®、TwinCAT®、TwinCAT/BSD®、TwinSAFE®、XFC®、XPlanar® 和 XTS® 是 Beckhoff Automation GmbH

的注册商标并由其授权使用。本出版物中所使用的其它名称可能是商标名称，任何第三方出于其自身目的使用它们可能会侵犯商标所有者的权利。



EtherCAT® 是注册商标和专利技术，由 Beckhoff Automation GmbH 授权使用。

版权所有

© Beckhoff Automation GmbH。

未经明确授权，不得复制、分发、使用和传播本文档内容。

违者将被追究赔偿责任。Beckhoff Automation GmbH 保留所有发明、实用新型和外观设计专利权。

第三方商标

本文档可能使用了第三方商标。有关商标信息，可以访问：<https://www.beckhoff.com/trademarks>。

1.2 安全信息

安全规范

为了确保您的使用安全，请务必仔细阅读并遵守本文中每个产品的安全使用说明。

责任免除

所有组件在供货时都配有适合应用的特定硬件和软件配置。严禁未按文档所述修改硬件或软件配置，否则，德国倍福自动化有限公司对由此产生的后果不承担责任。

人员资格

本说明仅供熟悉适用国家标准的控制、自动化和驱动工程专家使用。

警示性词语

文档中使用的警示信号词分类如下。为避免人身伤害和财产损失，请阅读并遵守安全和警告注意事项。

人身伤害警告

⚠ 危险

存在死亡或重伤的高度风险。

⚠ 警告

存在死亡或重伤的中度风险。

⚠ 谨慎

存在可能导致中度或轻度伤害的低度风险。

财产或环境损害警告

注意

可能会损坏环境、设备或数据。

操作产品的信息



这些信息包括：
有关产品的操作、帮助或进一步信息的建议。

1.3 信息安全说明

Beckhoff Automation GmbH & Co.KG (简称 Beckhoff) 的产品，只要可以在线访问，都配备了安全功能，支持工厂、系统、机器和网络的安全运行。尽管配备了安全功能，但为了保护相应的工厂、系统、机器和网络免受网络威胁，必须建立、实施和不断更新整个操作安全概念。Beckhoff 所销售的产品只是整个安全概念的一部分。客户有责任防止第三方未经授权访问其设备、系统、机器和网络。它们只有在采取了适当的保护措施的情况下，方可与公司网络或互联网连接。

此外，还应遵守 Beckhoff 关于采取适当保护措施的建议。关于信息安全和工业安全的更多信息，请访问本公司网站 <https://www.beckhoff.com/secguide>。

Beckhoff 的产品和解决方案持续进行改进。这也适用于安全功能。鉴于持续进行改进，Beckhoff 明确建议始终保持产品的最新状态，并在产品更新可用后马上进行安装。使用过时的或不支持的产品版本可能会增加网络威胁的风险。

如需了解 Beckhoff 产品信息安全的信息，请订阅 <https://www.beckhoff.com/secinfo> 上的 RSS 源。

1.4 文档发行状态

版本	修改
1.1.x	自产品版本 1.7.0 起，目录结构发生变更。 新增： 安装 [► 9]：TwinCAT 2 安装程序 支持的功能 [► 19] 教程 [► 31]

2 概述

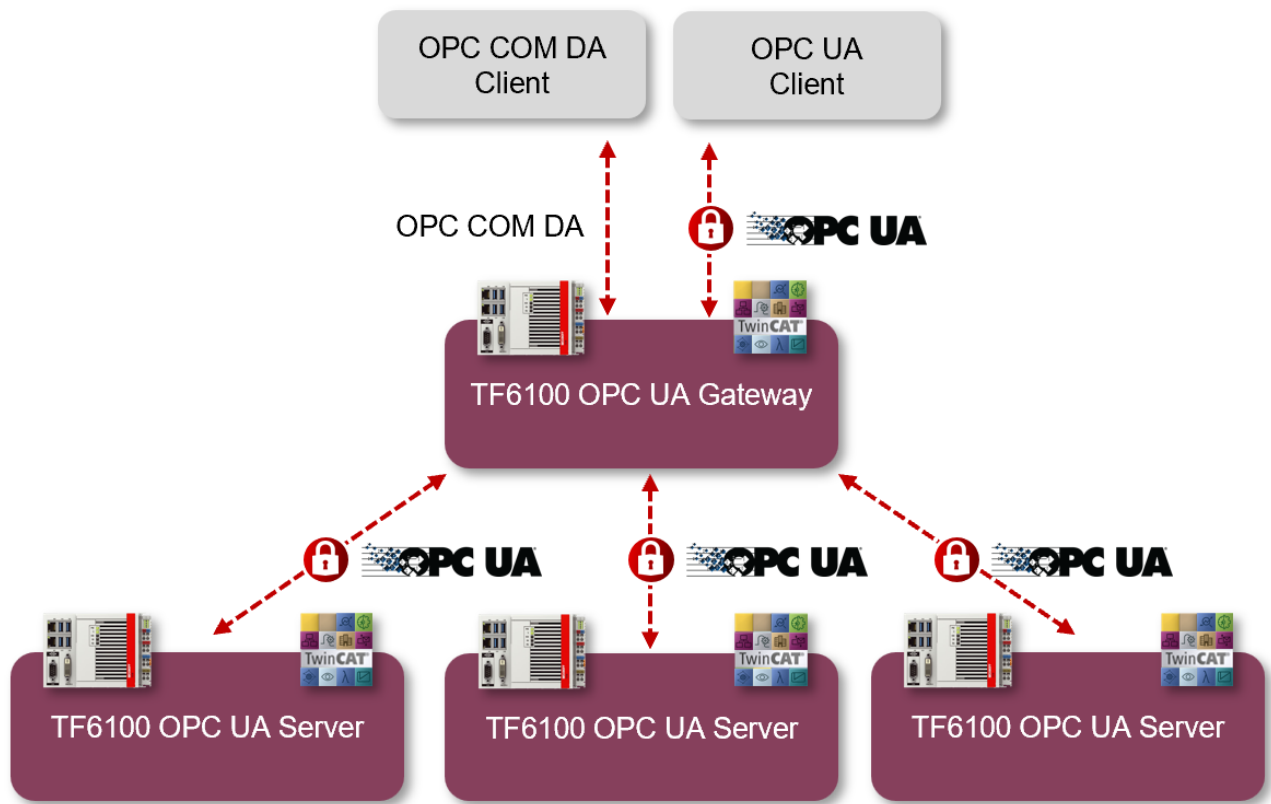
OPC 统一架构 (OPC UA) 是熟知的 OPC 标准的下一代产品。此为全球标准化通信协议，无论制造商和平台如何，都可以通过它交换机器数据。OPC UA 已经在协议中直接集成了通用安全标准。与 OPC 常规标准相比，OPC UA 的另一大优势是独立于 COM/DCOM 系统。

i 有关 OPC UA 的详细信息，请访问 [OPC 基金会网页](#)。

TwinCAT 3 功能 TF6100 OPC UA 由多个软件组件组成，可根据 OPC UA 与 TwinCAT 进行数据交换。下表概述了各个产品组件。

软件组件	描述
TwinCAT OPC UA 服务器	提供 OPC UA 服务器接口，以便 UA 客户端访问 TwinCAT 运行时。
TwinCAT OPC UA 客户端	根据 PLCopen 标准化功能块和易于配置的 I/O 设备，提供 OPC UA 客户端功能，实现与其他 OPC UA 服务器的通信。
TwinCAT OPC UA 配置器	用于配置 TwinCAT OPC UA 服务器的图形用户界面。
TwinCAT OPC UA 示例客户端	OPC UA 客户端的图形示例实现，用于与 TwinCAT OPC UA 服务器进行首次连接测试。
TwinCAT OPC UA 网关	可提供 OPC COM DA 服务器接口和 OPC UA 服务器聚合功能的封装技术。

本文档介绍了 TwinCAT OPC UA Gateway，该软件组件提供 OPC COM DA 接口，并支持 OPC UA 服务器聚合功能。



如需快速了解该产品，我们推荐我们的 [安装 \[▶ 9\]](#) 和 [快速入门 \[▶ 15\]](#) 章节。请注意该产品的 [系统要求 \[▶ 9\]](#)。

3 安装

3.1 系统要求

以下系统要求适用于本产品的安装和操作。

技术数据	描述
操作系统	Windows 10 Windows 11 Windows Server
目标平台	PC 架构 (x86、x64、Arm®)
.NET Framework	---
最低 TwinCAT 版本	运行本软件无需安装 TwinCAT。
所需 TwinCAT 授权	运行本软件无需 TwinCAT 授权。
支持的服务器	TwinCAT OPC UA Gateway 仅与需要 TF6100 授权的 TwinCAT OPC UA Server 进行通信。如果您想要将第三方设备连接至该网关，则需要使用 Unified Automation 提供的“UA Gateway”软件。
COM/DCOM	本软件支持本地 OPC COM DA 通信。不支持基于 DCOM 的通信。



安装型号

另请注意 TwinCAT OPC UA Gateway 所支持的不同安装版本 [► 11]。

防火墙端口

若要通过 OPC UA 与 TwinCAT OPC UA Gateway 进行通信，必须在该设备的防火墙中打开以下网络端口：

48050/tcp (incoming)

例如，如果在倍福工业 PC 上安装了 TwinCAT OPC UA Gateway，必须在操作系统的防火墙中将该端口打开，作为传入通信端口。

3.2 安装

根据所使用的 TwinCAT 版本和操作系统，该 TwinCAT 3 功能可以采用不同的安装方式，下面将详细介绍。

注意

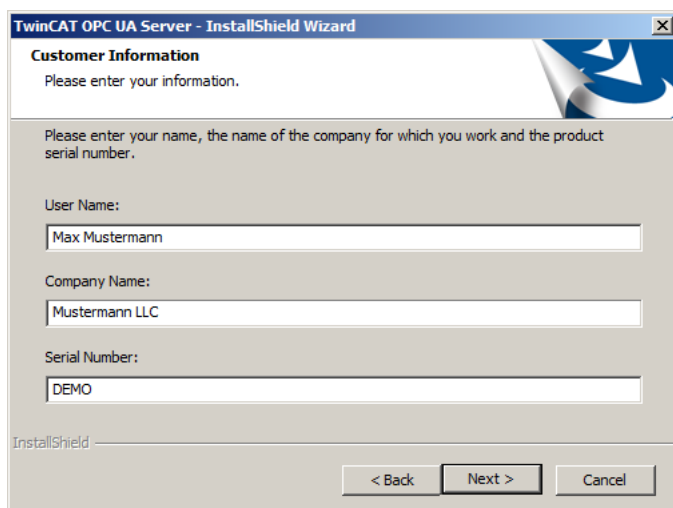
更新安装

更新安装总是会卸载之前安装的版本。请确保事先已备份配置文件。

TwinCAT 2 设置

如果您使用的是 TwinCAT 2，则可以通过安装包安装该插件，安装包可从倍福网站 <https://www.beckhoff.com/download> 下载。

安装可以在工程设计或运行时端进行，具体取决于您需要补充的系统。请注意，在 TwinCAT 2 下，安装过程中该插件会直接获得授权。另一个对话框会提示您输入授权密钥。如果您想安装 30 天试用版的插件，请输入 DEMO 作为授权密钥。



Windows CE 上的 TwinCAT 2 有单独的设置下载，名称为 TS6100-0030 OPC UA。该设置会安装 CAB 文件，然后您可以将其传输到 Windows CE 设备并进行安装。

TwinCAT 3 Package Manager

如果在 Microsoft Windows 操作系统上使用 TwinCAT 3.1 Build 4026（及更高版本），则可以通过 TwinCAT Package Manager 安装此功能，请参见 [安装文档](#)。

通常情况下，可通过相应的工作量安装此功能；然而，您也可以单独安装工作量中包含的软件包。本文档简要介绍了通过工作量进行安装的过程。

注意

未做好准备的 TwinCAT 重启会导致数据丢失

安装该功能可能会导致 TwinCAT 重启。

确保系统上没有运行重要的 TwinCAT 应用程序，或者先有序关闭这些应用程序。

命令行程序 TcPkg

您可以使用 TcPkg Command Line Interface（命令行界面，CLI）来显示系统上的可用工作量，并安装特定的工作量。

```
tcpkg list -t workload
tcpkg install TF6100.OpcUaGateway.XAR
```

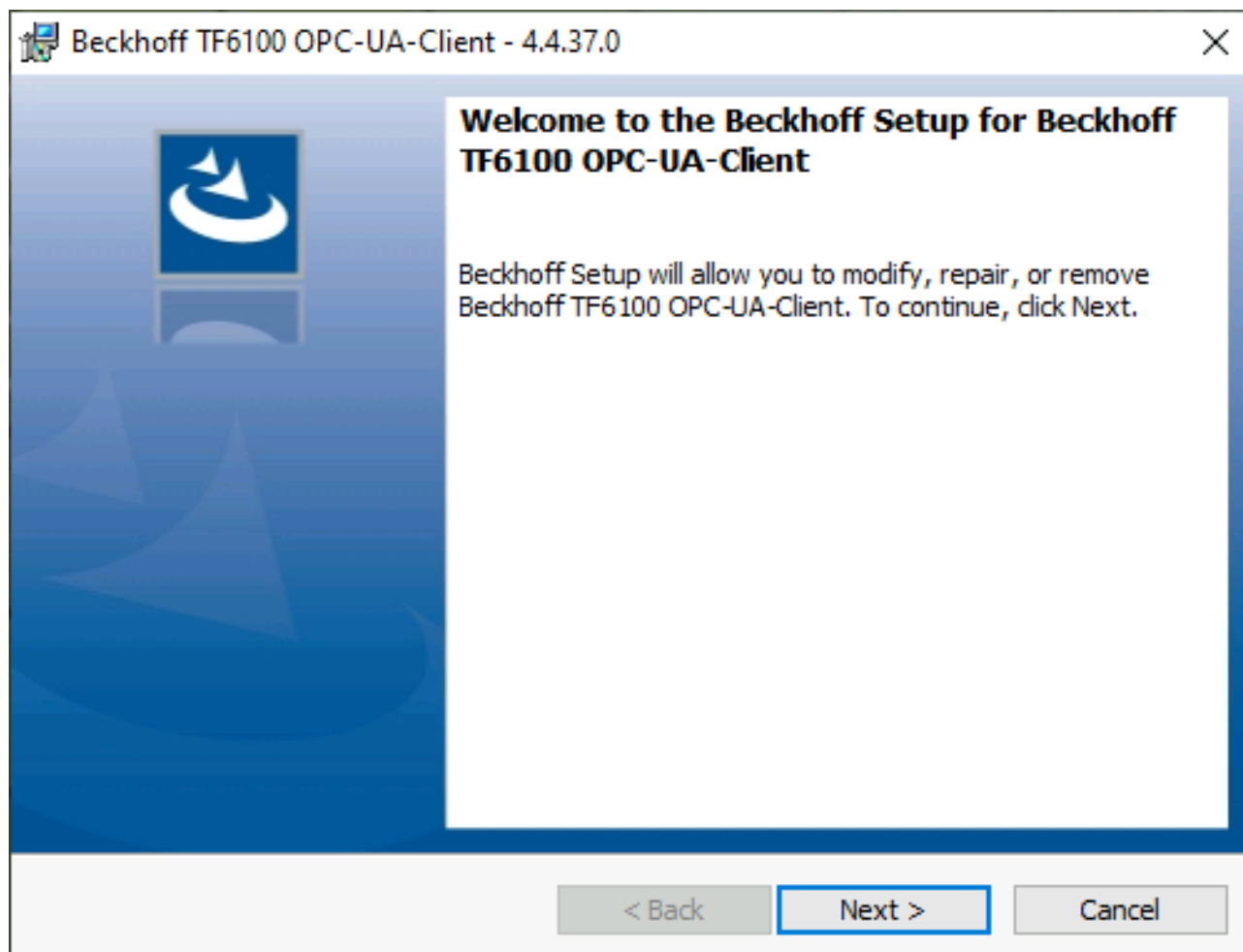
TwinCAT Package Manager UI

您可以使用 User Interface（用户界面，UI）显示所有可用的工作量，并根据需要进行安装。为此，请按照界面中的相应说明操作。

TwinCAT 3 设置

如果您在 Microsoft Windows 操作系统上使用的是 TwinCAT 3.1 Build 4024，您可以通过一个安装包来安装该功能，该安装包可以从倍福网站 <https://www.beckhoff.com/download> 上下载。

根据需要使用该功能的系统，可以在工程设计或运行时端进行安装。下方截图显示的是使用 TF6100 TwinCAT OPC UA 客户端设置的设置界面示例。



要完成安装过程，请按照设置“对话框”中的说明进行操作。

注意

未做好准备的 TwinCAT 重启会导致数据丢失

安装该功能可能会导致 TwinCAT 重启。

确保系统上没有运行重要的 TwinCAT 应用程序，或者先有序关闭这些应用程序。

3.3 安装型号

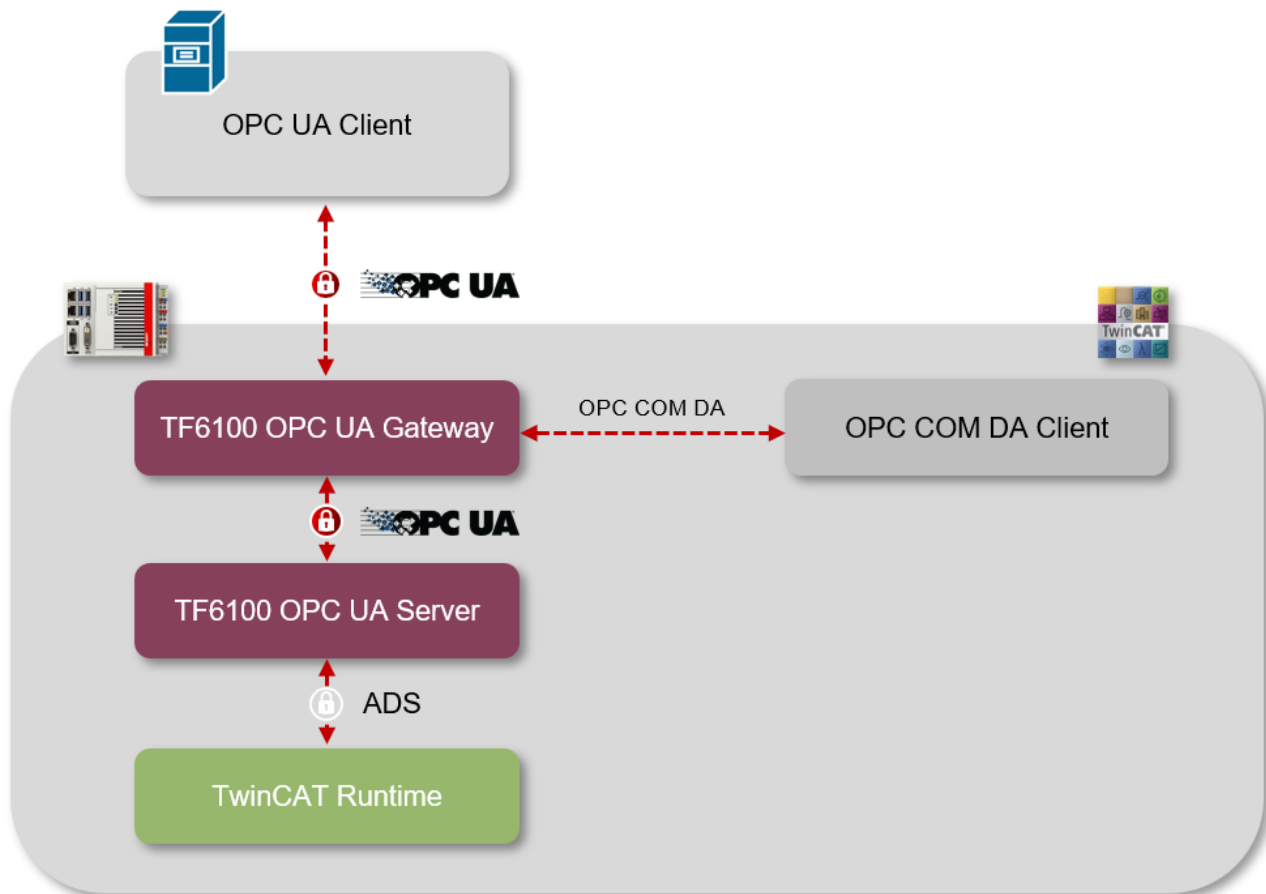
本章介绍了 TwinCAT OPC UA Gateway 所支持的不同安装版本。请注意，这些版本的复杂程度几乎可以任意扩展。此处所给出的示例仅代表常见的安装版本。

网关与服务器位于同一台设备上

在此场景下，TwinCAT OPC UA Gateway 与 TwinCAT OPC UA Server 安装在同一台设备上。网关采用默认设置进行配置，以便与本地 TwinCAT OPC UA Server 建立连接，其服务器 URL 为：opc.tcp://localhost:4840。

从客户端的角度来看，此情况下支持两种场景：

- OPC UA 客户端通过网关访问下层服务器，以获取 TwinCAT Runtime 中的符号。客户端可以位于同一台设备上，也可以位于网络中的另一台设备上。客户端与网关之间的通信连接为 OPC UA。
- OPC COM DA 客户端通过网关访问下层服务器，以获取 TwinCAT Runtime 中的符号。客户端必须位于同一台设备上。客户端与网关之间的通信连接为 OPC COM DA。

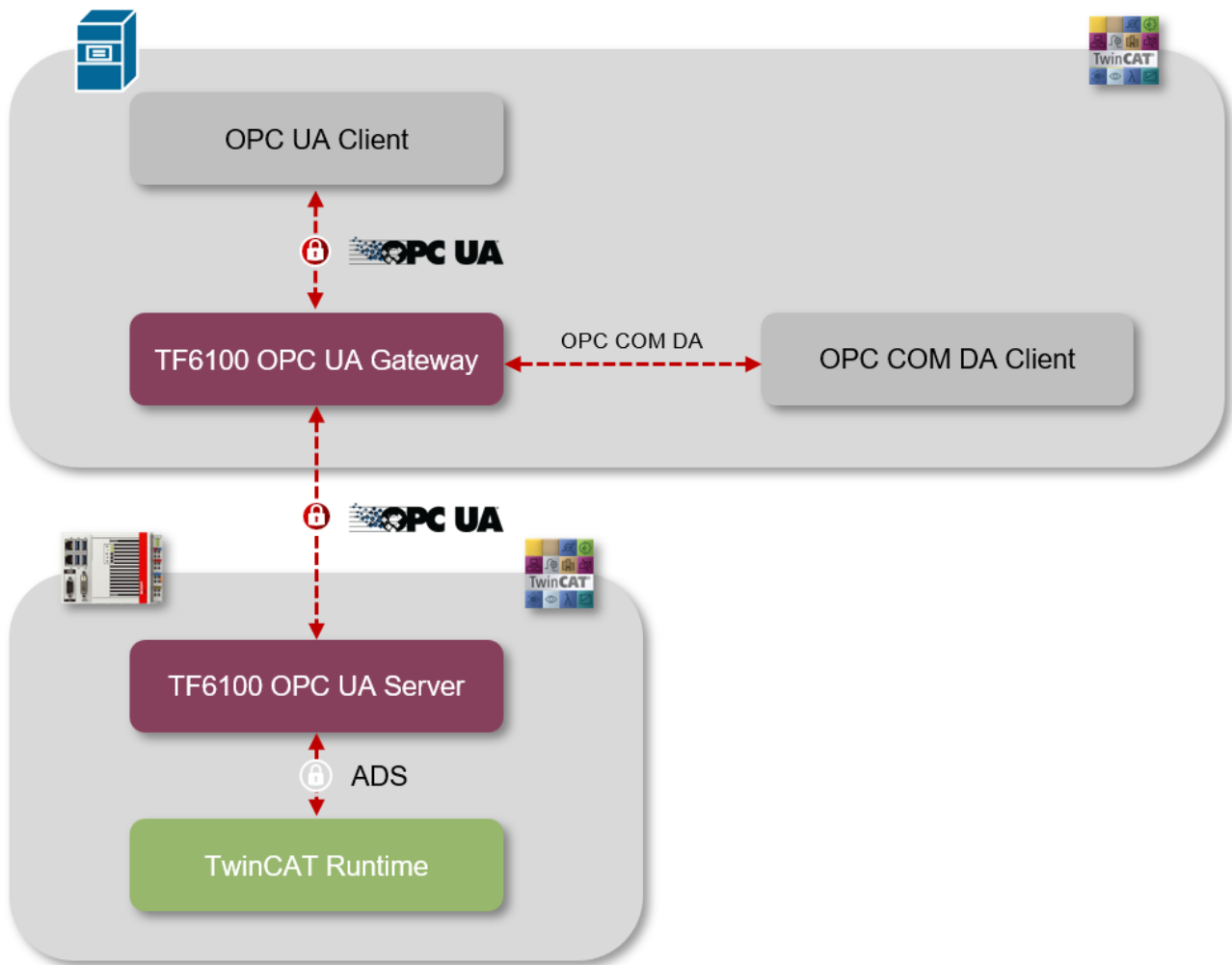


网关与服务器位于不同设备上

在此场景下，TwinCAT OPC UA Gateway 与 TwinCAT OPC UA Server 安装在不同设备上。对网关进行配置，通过在其中存储远程 TwinCAT OPC UA Server 的服务器 URL（例如 `opc.tcp://192.168.1.1:4840`），以建立与该服务器的连接。

从客户端的角度来看，此情况下支持两种场景：

- OPC UA 客户端通过网关访问下层服务器，以获取 TwinCAT Runtime 中的符号。客户端可以位于同一台设备上，也可以位于网络中的另一台设备上。客户端与网关之间的通信连接为 OPC UA。
- OPC COM DA 客户端通过网关访问下层服务器，以获取 TwinCAT Runtime 中的符号。客户端必须位于同一台设备上。客户端与网关之间的通信连接为 OPC COM DA。

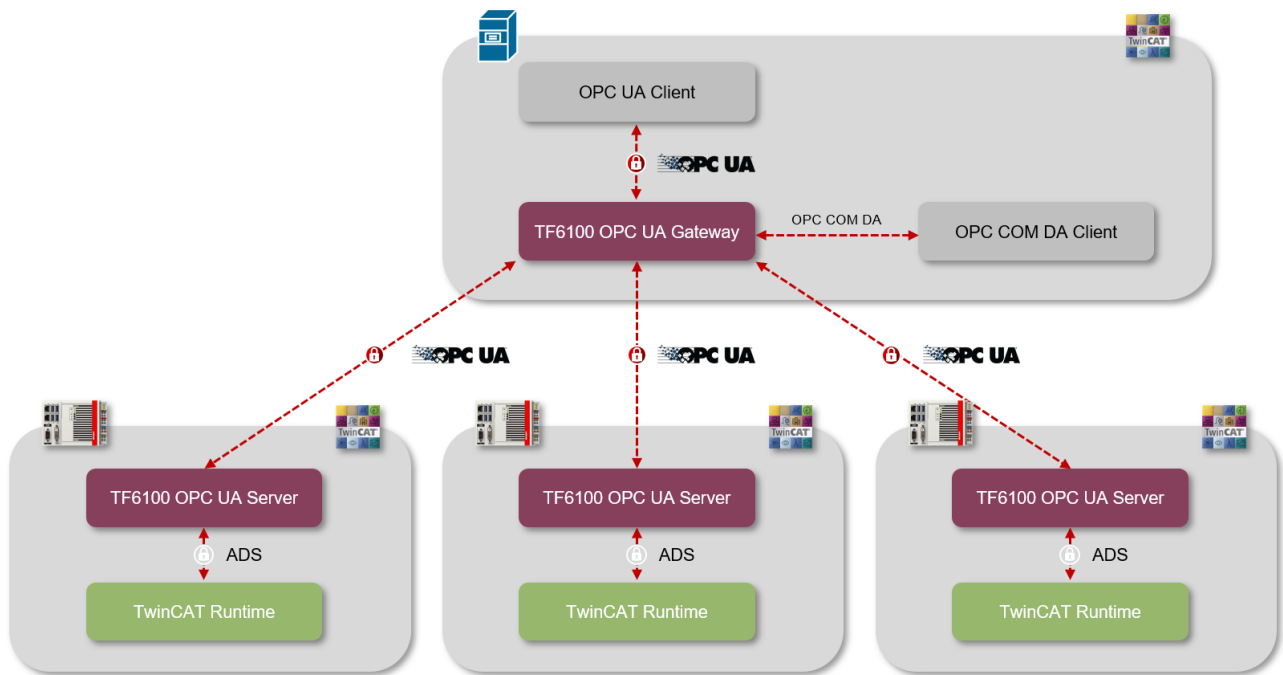


将网关连接至多台服务器

您还可以将 TwinCAT OPC UA Gateway 连接至多台下层的 TwinCAT OPC UA Server。这些服务器可以安装在同一台设备上，也可以安装在网络中的其他设备上。当然，此场景可根据需要任意扩展。下图展示了一种场景，其中三台 TwinCAT OPC UA Server 通过网络连接至该网关。

从客户端的角度来看，此情况下支持两种场景：

- OPC UA 客户端通过网关访问下层服务器，以获取各个 TwinCAT Runtime 中的符号。客户端可以位于同一台设备上，也可以位于网络中的另一台设备上。客户端与网关之间的通信连接为 OPC UA。
- OPC COM DA 客户端通过网关访问下层服务器，以获取各个 TwinCAT Runtime 中的符号。客户端必须位于同一台设备上。客户端与网关之间的通信连接为 OPC COM DA。



4 技术简介

4.1 快速入门

TwinCAT OPC UA Gateway 可作为独立安装包下载。该安装包会自动配置对运行于网关所在同一计算机上的 TwinCAT OPC UA Server 的访问。

如果向网关中添加多台 OPC UA 服务器，或者服务器在另一台计算机上运行，则需要对标准配置进行修改。请使用配置器来配置这些设置。

● TwinCAT OPC UA Server 的配置



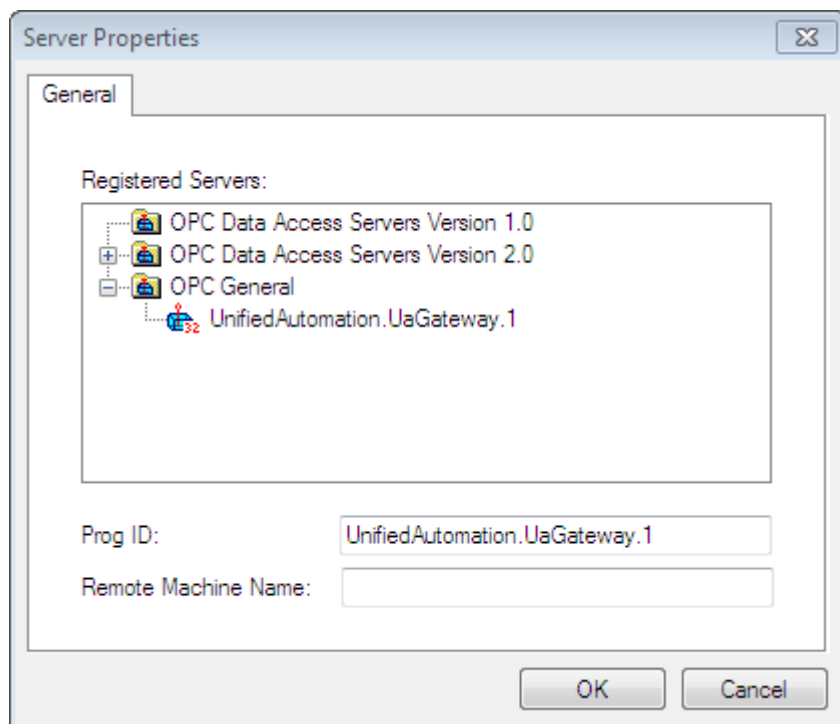
在继续操作之前，请检查 OPC UA 服务器的配置，并确保其运行符合预期。

有关 OPC UA Server 配置的更多信息，请参阅“OPC UA Server”一章中的。

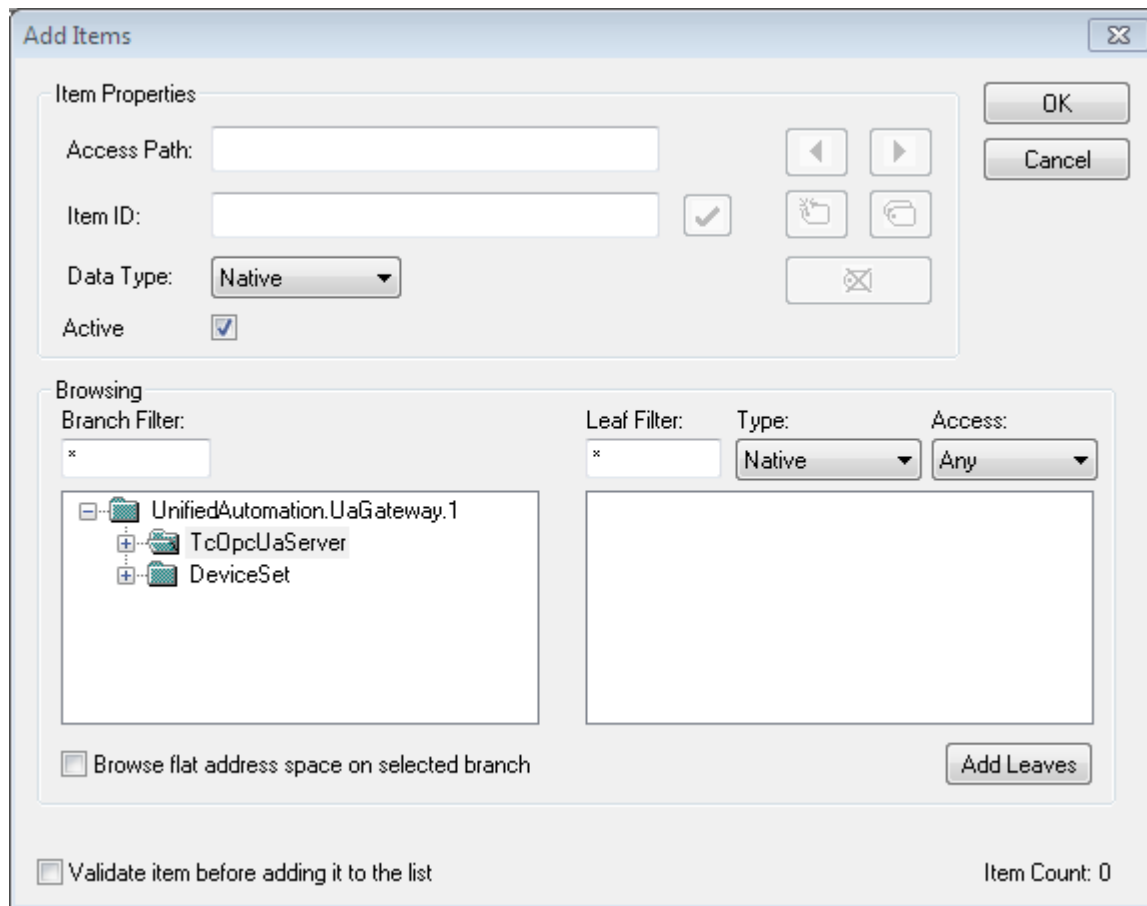
快速入门 – OPC COM DA

要将 OPC COM DA Client 连接到网关，请启动客户端并建立与以下 ProgID 的连接：

UnifiedAutomation.UaGateway.1



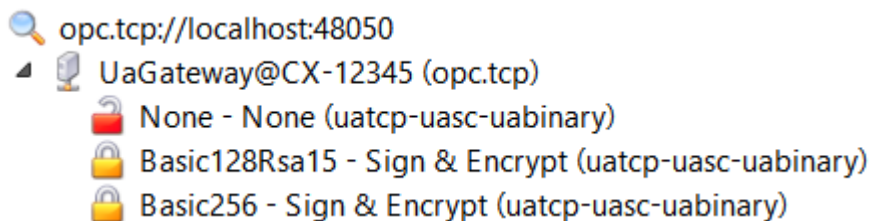
浏览网关时，在网关的命名空间中将会看到一台或多台 OPC UA Server。



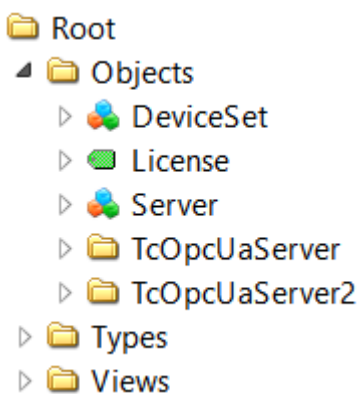
快速入门 – OPC UA

该网关不仅提供 OPC COM DA 接口，还支持聚合一台或多台 OPC UA Server。为此，网关还会开放一个 OPC UA 接口。通过以下 OPC UA Server URL 可以访问该网关：

```
opc.tcp://[HostnameOrIpAddressOrLocalhost]:48050
```



此时，网关的命名空间中包含所有下层的 TwinCAT OPC UA Server。

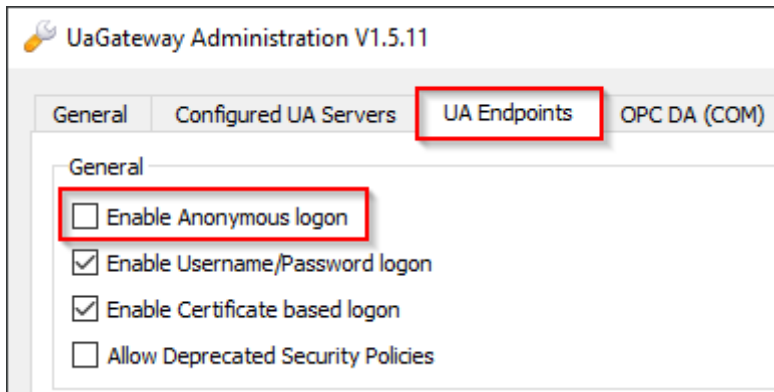


4.2 建议的步骤

初次调试完成后，我们建议您注意以下几点，以便进一步配置网关并确保运行环境稳定、安全。

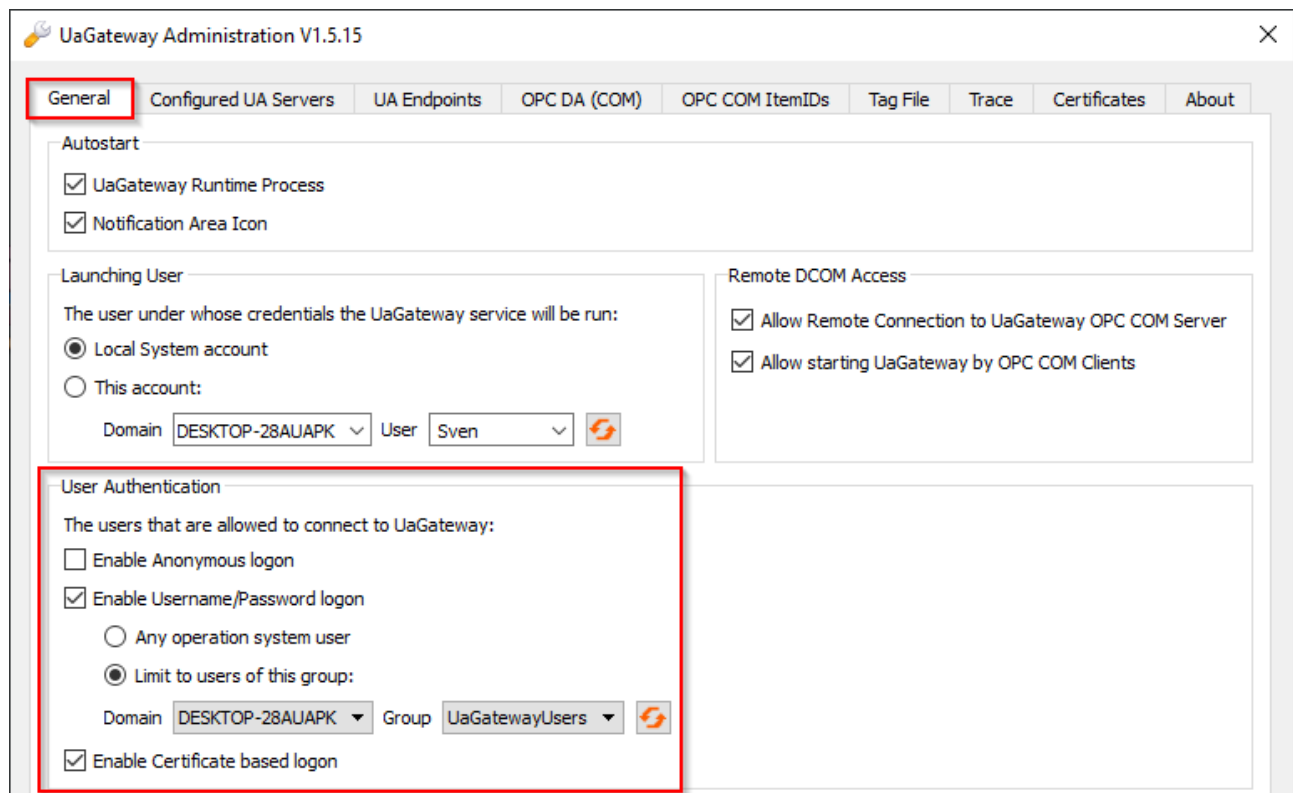
只使用安全的身份令牌

网关在交付状态下配置了已激活的身份令牌“匿名”。我们建议禁用此身份令牌，以便只有经过身份验证的用户才能连接到网关的 OPC UA 服务器接口。您可以在 TwinCAT OPC UA Gateway 配置器的端点配置 [► 24] 中禁用此设置。



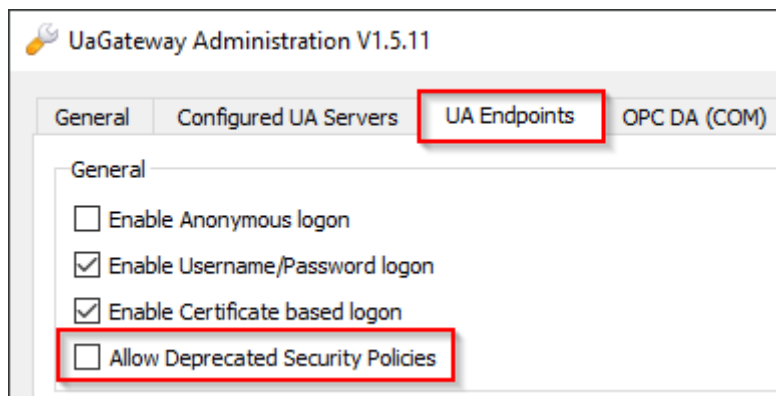
配置具有访问权限的用户组

您应使用 TwinCAT OPC UA Gateway 配置器来定义具有网关访问权限的用户组。然后，在将 OPC UA 客户端连接到网关时，可以将该用户组中的用户指定为身份令牌。

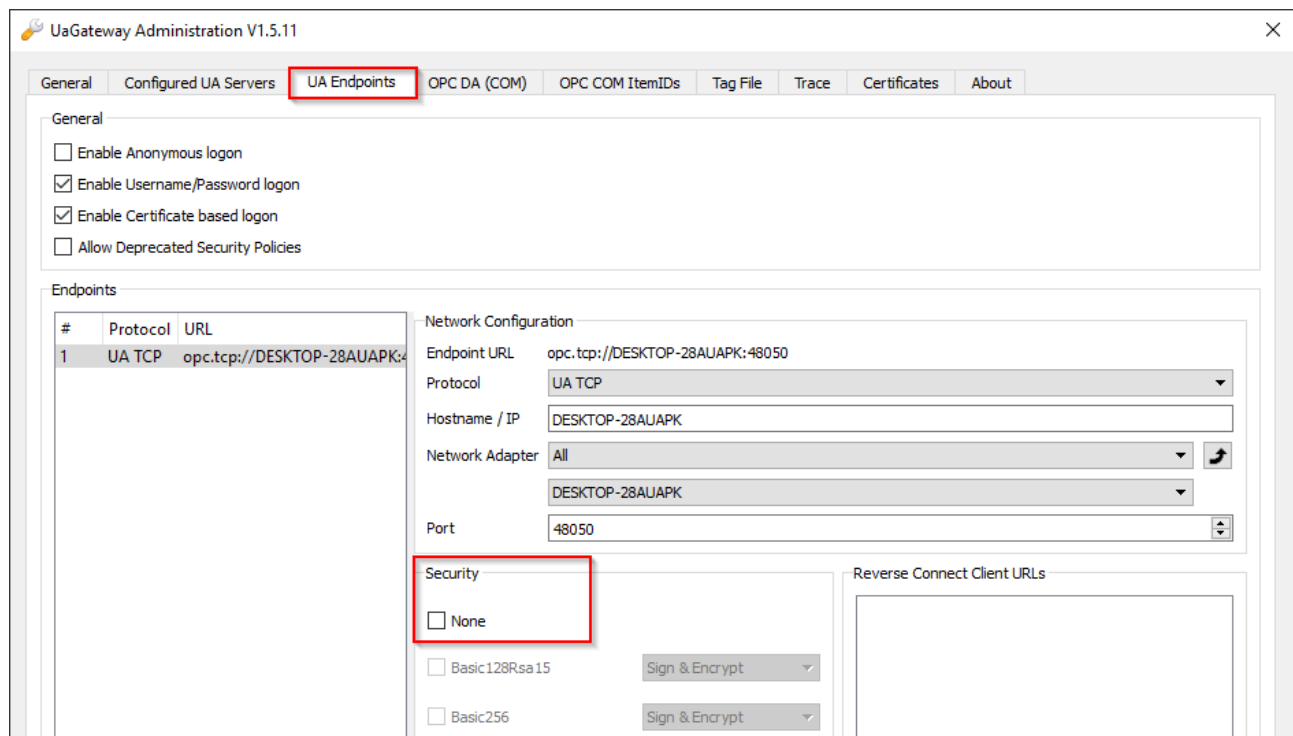


将不安全端点保持禁用状态

TwinCAT OPC UA Gateway 默认不提供被列为不安全的端点。在配置端点 [► 24] 时，可通过配置参数将这些端点设置在网关中启用——然而，我们强烈建议不要这样做，并仅推荐使用当前被视为安全的端点。

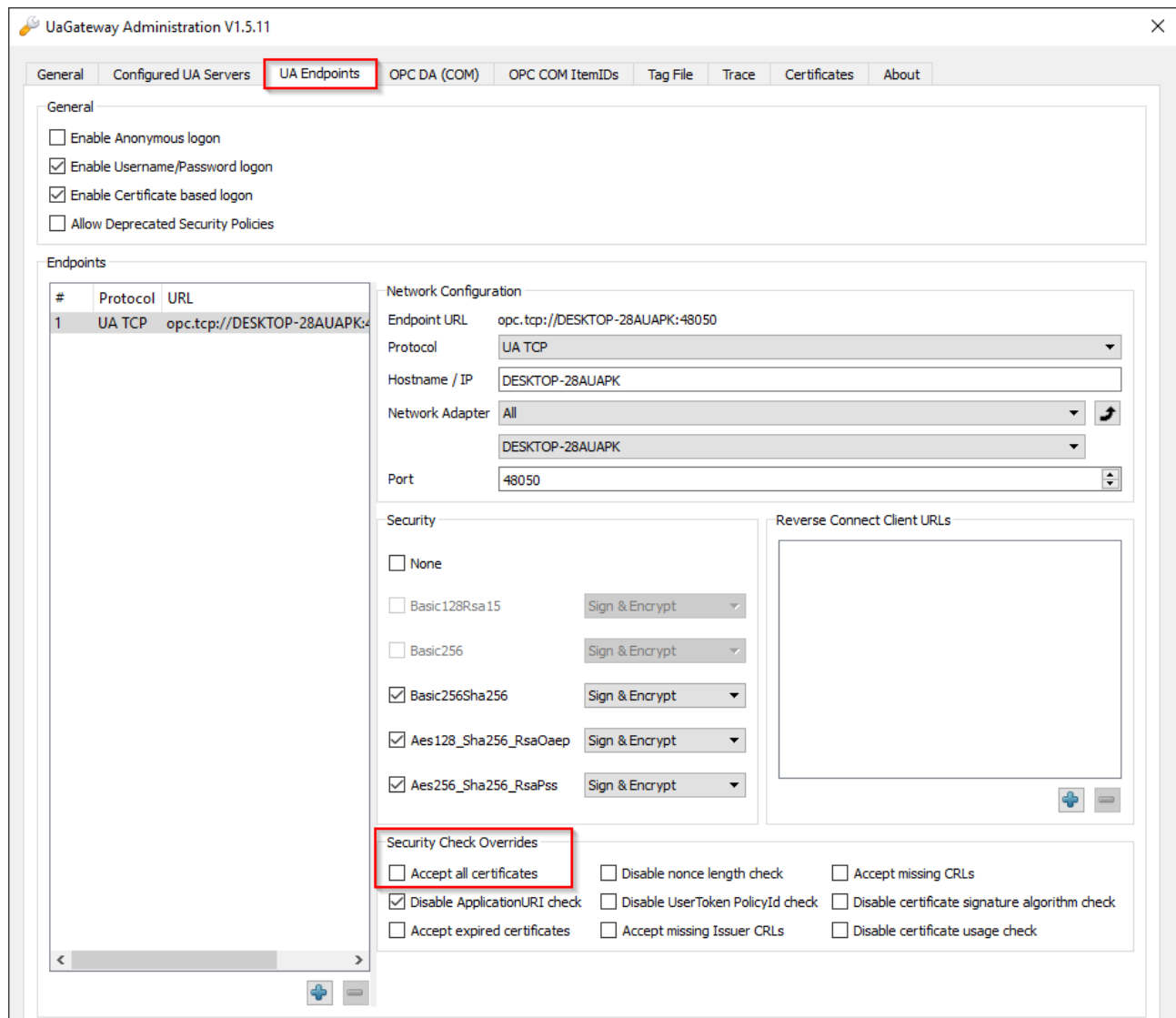


此外，网关在交付状态下已禁用未加密的端点（“None/None”），我们建议保持其禁用状态。如果出于兼容性原因需要激活此设置，也可通过配置器中的配置参数来实现。



禁用“接受所有证书”

默认情况下，网关是为方便调试而配置的，因此它会自动信任所有客户端证书，无需在网关端手动交换证书。出于安全考虑，我们建议禁用此设置。配置端点 [► 24] 时，可通过 TwinCAT OPC UA Gateway 配置器禁用此设置。

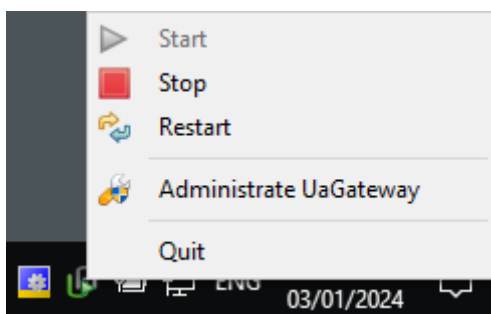


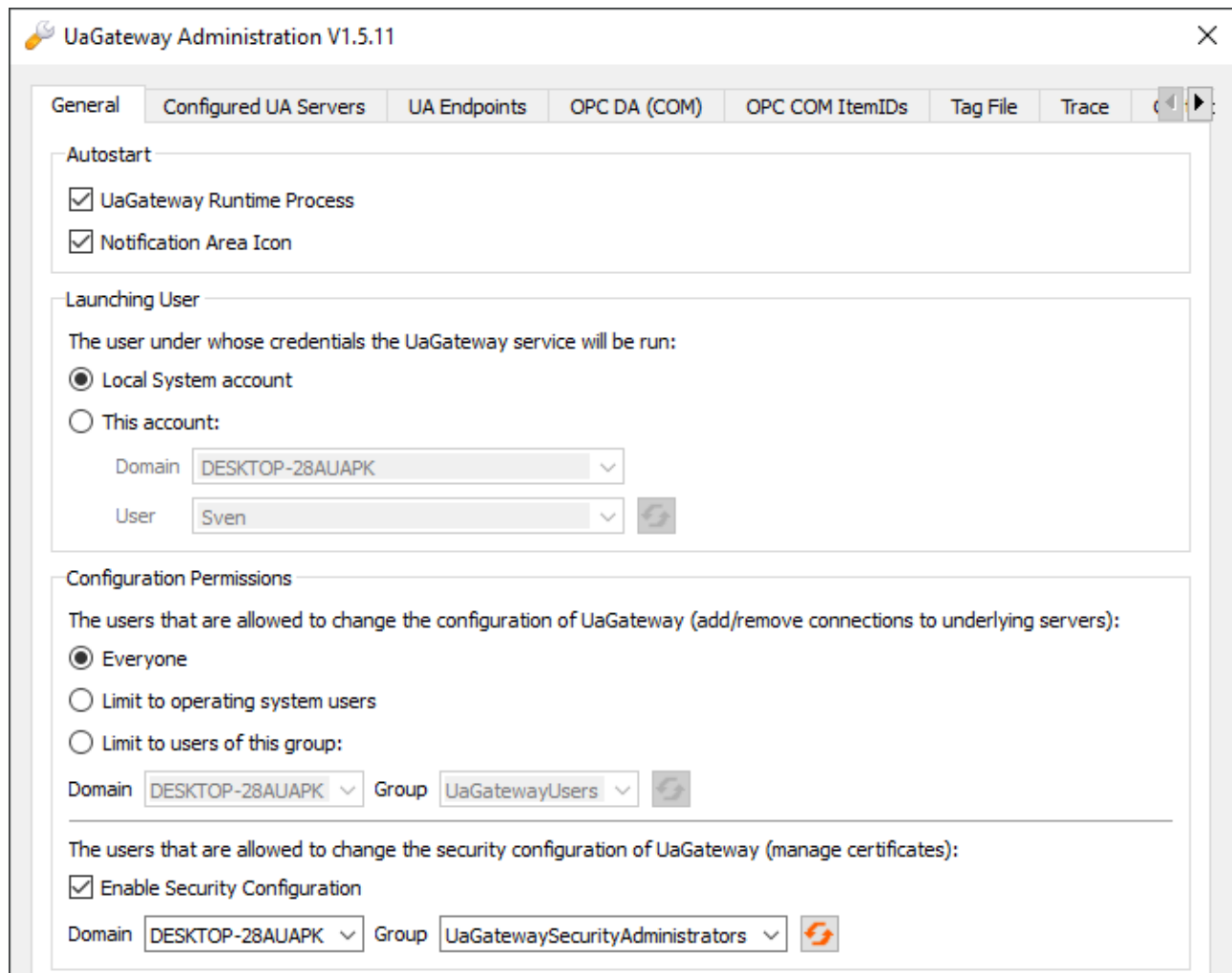
4.3 支持的功能

TwinCAT OPC UA Gateway 仅连接至 TwinCAT OPC UA Server。此外，仅提供数据访问功能。如需连接第三方服务器或使用其他 OPC UA 功能，请考虑购买 Unified Automation 的 [UA Gateway](#) 软件。

4.4 配置器

TwinCAT OPC UA Gateway 包含一个用于配置该软件的图形用户界面。您可以通过 Windows 系统托盘中网关图标的上下文菜单中的 **Administrate UaGateway**（管理 UaGateway）条目打开此配置器。





4.5 应用程序目录

该应用程序使用各种目录来存储相关信息，例如配置或证书文件。

安装目录

在所有操作系统上，应用程序的基本安装目录均始终与 TwinCAT 安装目录相关。

```
%TcInstallDir%\Functions\TF6100-OPC-UA
```

然后，应用程序即安装在该目录下的以下目录中。

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway
```

PKI 基础设施的基本目录 (服务器)

用于与网关的 OPC UA 服务器建立安全通信连接的证书文件，存储在以下目录中：

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver
```

自产品版本 1.7.0 起，该目录在 ProgramData 下创建：

```
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\pki\pkiserver
```

受信任证书目录 (服务器)

声明称，该目录中的客户端证书为“受信任”证书。

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\trusted\certs
```

自产品版本 1.7.0 起，该目录在 ProgramData 下创建：

```
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\pki\pkiserver\trusted\certs
```

被拒绝证书目录 (服务器)

声明称，该目录中的客户端证书为“被拒绝”证书。

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\rejected
```

自产品版本 1.7.0 起，该目录在 ProgramData 下创建：

```
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\pki\pkiserver\rejected
```

PKI 基础设施的基本目录 (客户端)

网关作为 OPC UA 客户端，用于与下层 TwinCAT OPC UA Server 建立安全通信连接时所使用的证书文件，存储在以下目录中：

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient
```

自产品版本 1.7.0 起，该目录在 ProgramData 下创建：

```
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\pki\pkiclient
```

受信任证书目录 (客户端)

声明称，该目录中的客户端证书为“受信任”证书。

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient\trusted\certs
```

自产品版本 1.7.0 起，该目录在 ProgramData 下创建：

```
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\pki\pkiclient\trusted\certs
```

被拒绝证书目录 (客户端)

声明称，该目录中的服务器证书为“被拒绝”证书。

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient\rejected
```

自产品版本 1.7.0 起，该目录在 ProgramData 下创建：

```
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\pki\pkiclient\rejected
```

服务器和客户端证书目录

网关的 OPC UA 服务器和客户端证书目录的定义如下，其中，公钥目录（“certs”）与私钥目录（“private”）之间存在区别。服务器和客户端使用相同的证书。

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\own\certs
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\own\private
```

自产品版本 1.7.0 起，这些目录在 ProgramData 下创建：

```
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\pki\pkiserver\own\certs
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\pki\pkiserver\own\private
```

日志文件

日志文件存储在以下目录中。

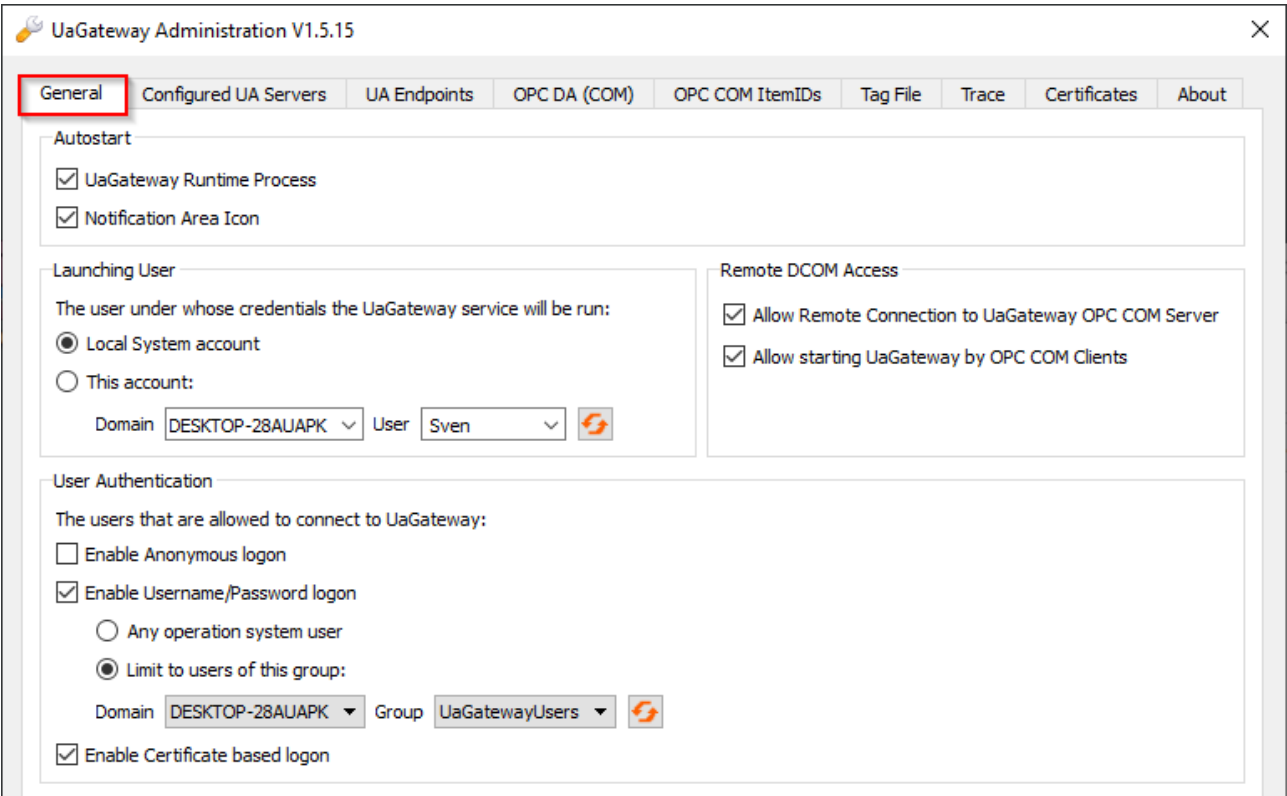
```
%ProgramData%\UnifiedAutomation\TwinCAT OPC UA Gateway\Trace
```

自产品版本 1.7.0 起，该目录按如下方式创建：

```
c:\ProgramData\Beckhoff\TF6100-OPC-UA\TcOpcUaGateway\trace\
```

4.6 通用设置

TwinCAT OPC UA Gateway [配置器 \[► 19\]](#)中的 **General**（常规）选项卡可用于对网关进行常规设置。



这些设置在下文有详细说明。

AutoStart (自动启动)

在此区域中，您可以配置 TwinCAT OPC UA Gateway 的自动启动行为。启用 **UaGateway Runtime Process**（UaGateway 运行时进程）选项，可在计算机开机时自动启动网关的 Windows 服务。启用 **Notification Area Icon**（通知区域图标）选项，可在用户登录时启动网关的 Windows 系统托盘图标。

启动用户

TwinCAT OPC UA Gateway 默认注册为 Windows 服务，并在系统启动时自动启动。该 Windows 服务被分配了特定的用户上下文。您在此处选择的用户将被分配给该 Windows 服务。此外，该用户将被授予“LogOnAsService”权限，并添加到本地用户组“UaGatewayUsers”中。

用户身份验证

在此区域中，您可以定义当 OPC UA 客户端连接到网关时可用的身份令牌类型。您还可以定义应具有网关访问权限的用户组。然后，OPC UA 客户端在建立连接时，可以使用该用户组中的用户。

配置权限

可以仅允许特定用户更改网关的配置，即添加或移除与下层服务器的连接。您可以从以下设置中进行选择：

所有人	任何能够与网关建立连接的用户（包括通过 OPC UA 匿名登录的用户）均可更改配置。
仅限于操作系统用户	仅限本地用户和同一域中的用户可以更改配置。
仅限于此组中的用户	仅限特定组中的用户才被允许更改配置。

UA Discovery 注册

如果要将网关注册到本地发现服务器（LDS），请启用 **Register at Local Discovery Server**（在本地发现服务器上注册）选项。

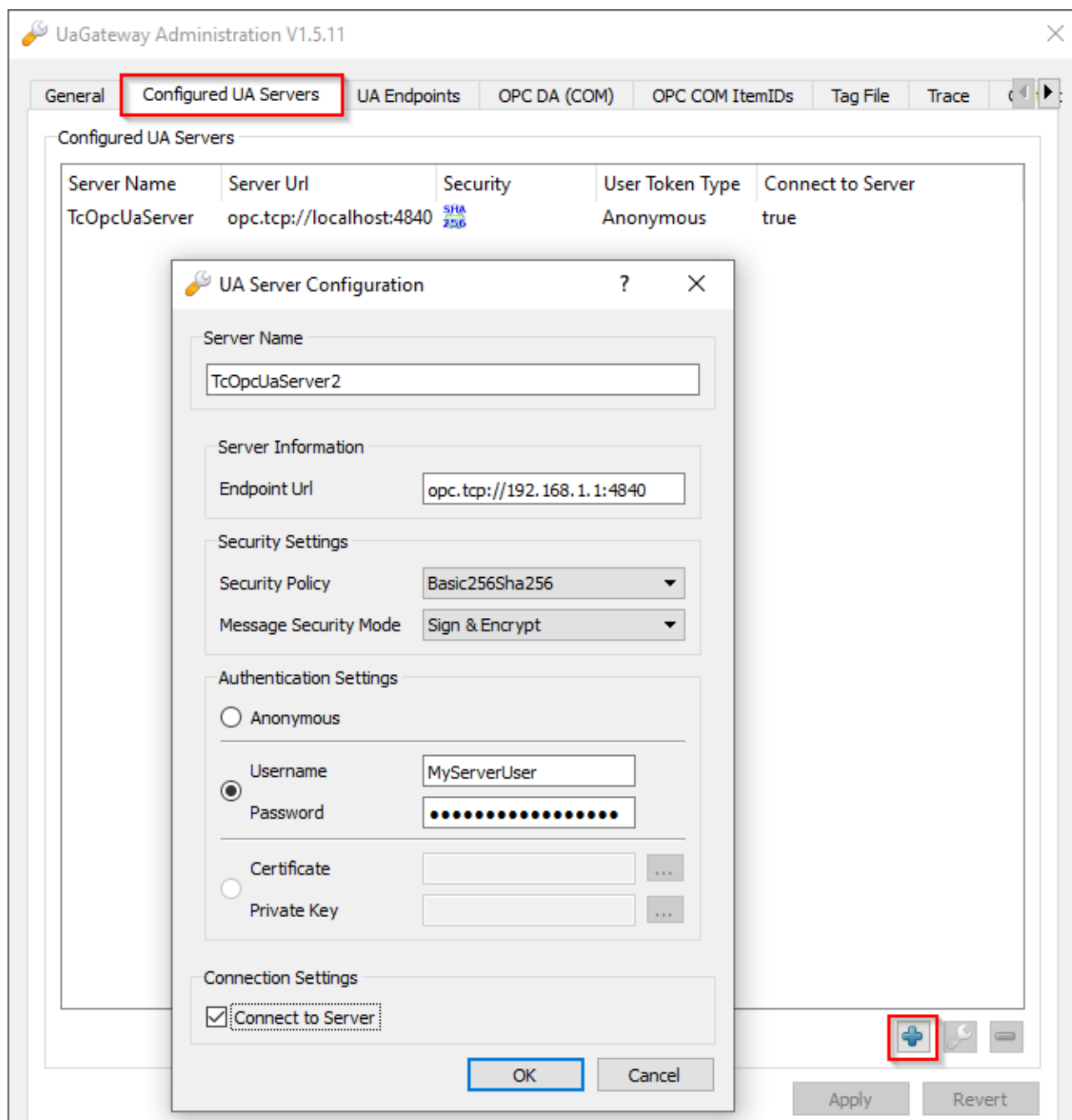


远程 DCOM 访问

根据所使用的 TwinCAT OPC UA Gateway 版本的不同，可能还会显示配置选项 **Remote DCOM Access**（远程 DCOM 访问）。网关不支持这些配置参数，可以忽略。另请参见 [系统要求 \[► 9\]](#)。

4.7 附加服务器的配置

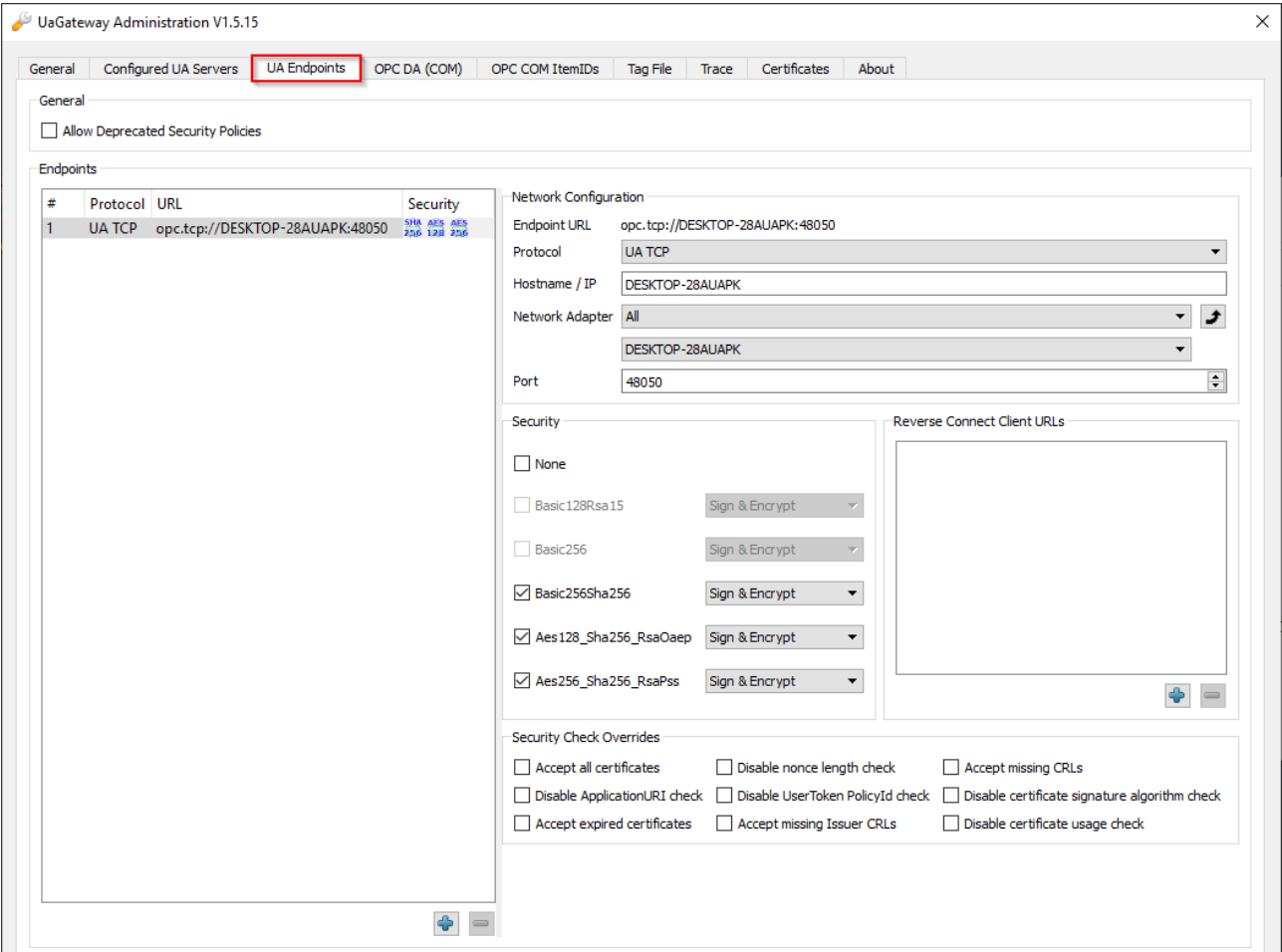
通过 TwinCAT OPC UA Gateway 配置器 [► 19] 中的 **Configured UA Servers**（已配置的 UA 服务器）选项卡，您可以为网关添加更多的下层 TwinCAT OPC UA Server。交付时，网关已建立与安装在同一系统上的 TwinCAT OPC UA Server 的连接。



如要配置其他 TwinCAT OPC UA Server 或将其从配置中移除，请点击加号或减号按钮，然后点击 **Apply**（应用）以保存更改。

4.8 端点的配置

通过 TwinCAT OPC UA Gateway 配置器 [► 19] 中的 **UA Endpoints**（UA 端点）选项卡，您可以为 OPC UA 端点配置进行相关设置。OPC UA 端点是 OPC UA 客户端连接至网关所需的连接信息。



下文将详细介绍此选项卡中可用的配置选项。

一般信息

在此区域中，您可以启用配置开关 **Allow deprecated security policies**（允许已弃用的安全策略），以在网关中激活已弃用且可能不安全的安全策略。不过，我们建议保持此选项禁用状态，仅在与旧版 OPC UA 客户端存在兼容性问题时才启用它。然而，在这种情况下，正确的做法应当是联系客户端供应商，以获取更新。

端点

您在此处可以定义不同 OPC UA 端点所需的所有设置，创建新端点或移除现有端点。交付时已预定义一个端点，该端点通常情况下应足以满足所有应用需求。该端点定义了可用的安全策略，以及网络配置、端口、反向连接客户端 URL 和任何安全检查覆盖项的设置。

以下章节将更详细地介绍这些配置元素。

网络配置

在此区域中，您可以定义要配置端点时所针对的网络接口。网关在交付状态下定义的端点将自动为所有网络接口进行配置。这意味着可以通过在操作系统中安装并配置的任何网络接口来访问该网关。在此处可定义以下配置参数：

配置参数	描述
端点 URL	调用 GetEndpoint 时，网关在 OPC UA 客户端中显示的端点 URL。

配置参数	描述
协议	要使用的协议。仅支持“UA TCP”协议。
主机名/IP	安装网关的设备的主机名或 IP 地址。
网络适配器	选择 OPC UA 客户端可通过哪个网络适配器访问该网关。
端口	OPC UA 客户端可通过哪个网络端口（TCP）访问该网关。

安全

在此区域中，您可以配置该端点所支持的安全策略。勾选相应安全策略前方的复选框，即可将其配置到该端点中。安全策略旁边有一个用于选择该端点所适用的消息安全模式的选项。

反向连接客户端 URL

在此区域中，您可以输入要用于反向连接功能的客户端的端点 URL。

安全检查覆盖项

在此区域中，您可以配置用于验证各种安全选项的例外规则。

4.9 TF6120 的迁移

UA Gateway 的主要用途之一是提供可持续的连接能力，以取代 Tx6120 OPC DA 附件/功能。如果您希望将 Tx6120 OPC DA 迁移至 UA Gateway，请注意以下事项。

标准配置

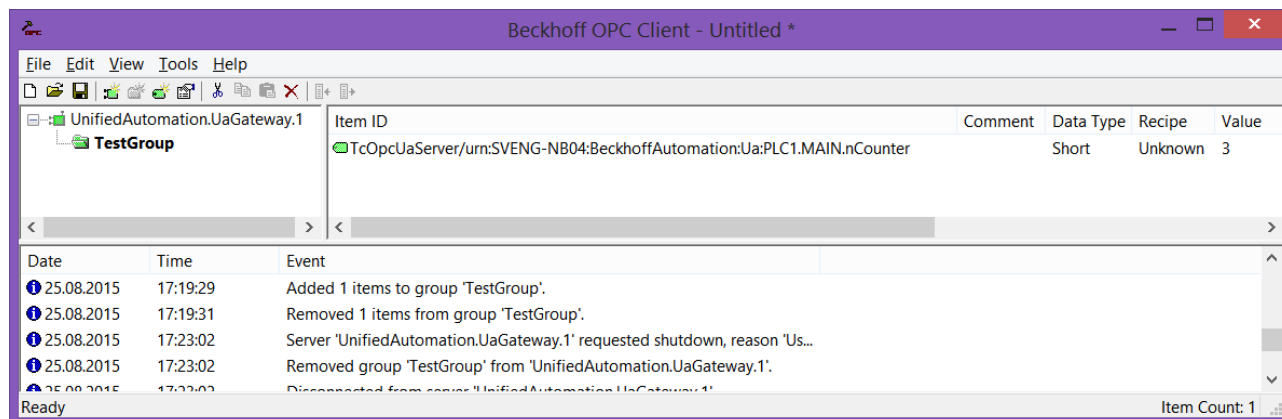
UA Gateway 的标准配置会自动与本地 OPC UA Server 建立连接，并为 OPC DA 客户端提供 OPC DA 接口。对于基于此标准配置的连接，OPC DA 客户端必须注意以下事项：

- UA Gateway 的默认 ProgID 为“UnifiedAutomation.Gateway.1”。TwinCAT OPC DA Server 使用不同的 ProgID（“Beckhoff.TwinCATOpcServerDA”）。
- UA Gateway 始终使用一个 ProgID，而非多个克隆副本。
- OPC 符号的 ItemIdentifier 在 UA Gateway 中生成的方式与在 TwinCAT OPC DA Server 中不同。此行为可以调整为与 OPC DA 服务器的行为更加相似。

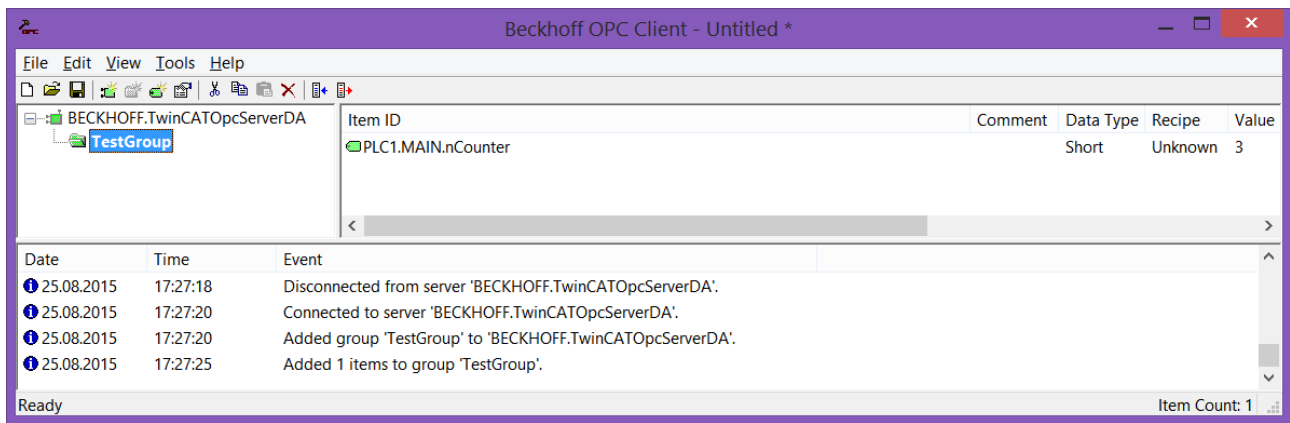
更改 ItemIdentifier 的语法

可以更改 UA Gateway 用于 ItemIdentifier 的语法，使其更接近于 TwinCAT OPC DA Server 的类型。默认情况下，UA Gateway 在创建标识符时使用的语法与 TwinCAT OPC DA Server 不同。

UA Gateway 示例：



TwinCAT OPC DA Server 示例：



UA Gateway 使用前缀，以便能够明确标识该变量所源自的下层 OPC UA Client。

要将 UA Gateway 配置为以与 TwinCAT OPC DA Server 大致相同的方式生成其标识符，需要执行以下步骤。该功能旨在简化迁移过程。

1. 打开 UA Gateway 配置文件
C:\Program Files (x86)\UnifiedAutomation\UaGateway\bin\uagateway.config.xml
2. 在 XML 文件中查找以下 XML 标签：

```
<OpcServerConfig>
  <ComDaServerConfig>
    <ComDaNamespaceUseAlias>false</ComDaNamespaceUseAlias>
  </ComDaServerConfig>
</OpcServerConfig>
```

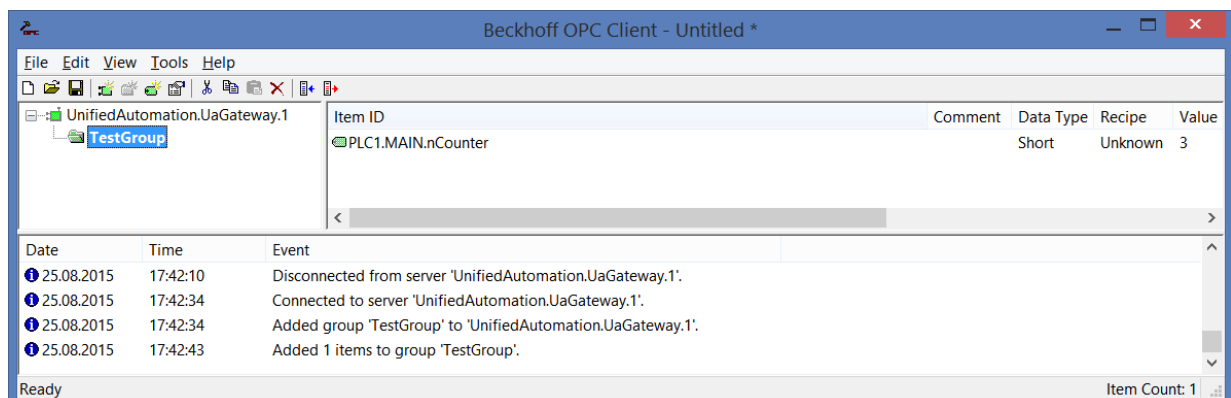
3. 如果将 XML 标签 ComDaNamespaceUseAlias 设置为“true”，则可以指定用户定义的前缀。为此，请在同一个 XML 文件中查找以下 XML 标签：

```
<OpcServerConfig>
  <UaServerConfig>
    <ConfiguredNamespaces>
      ...
    </ConfiguredNamespaces>
  </UaServerConfig>
</OpcServerConfig>
```

4. 在此 XML 结构中，识别 TwinCAT OPC UA Server 的命名空间。默认情况下，其内容应如下所示：

```
<OpcServerConfig>
  <UaServerConfig>
    <ConfiguredNamespaces>
      ...
      <Namespace>
        <Index>...</Index>
        <Uri>TcOpcUaServer/urn:Hostname:BeckhoffAutomation:Ua:PLC1</Uri>
        <AllowRenameUri>false</AllowRenameUri>
        <UniqueId>TcOpcUaServer#TcOpcUaServer/urn:Hostname:BeckhoffAutomation:Ua:PLC1</UniqueId>
        <ComAlias>...</ComAlias>
      </Namespace>
      ...
    </ConfiguredNamespaces>
  </UaServerConfig>
</OpcServerConfig>
```

5. 在您的计算机上，占位符“...”可能显示不同。将 <ComAlias> 设置为您首选的前缀，例如“PLC1”。然后，这些标识符将以前缀“PLC1”创建。



4.10 安全

4.10.1 概述

OPC UA 作为一种通信技术如此成功的原因之一是其集成式安全机制。基于 OPC UA 的数据通信可以在 2 个层面上确保安全：传输层和应用层。在与服务器连接时，客户端首先要选择一个端点，该端点指定了将使用的安全功能。

端点

服务器会向客户端提供一个不同端点 [▶ 27] 的列表，客户端可以与之连接。端点描述的是通过该端点进行的通信连接应实现的安全功能（如“消息安全”模式、“安全策略”和可用“身份令牌”）。例如，端点可能需要对数据包进行签名和加密（传输层），以及根据用户名/密码对客户端进行额外的身份验证（应用层）。

传输层

基于 OPC UA 的通信连接可以在传输层得到保护。这是通过使用客户端/服务器证书以及客户端和服务器应用程序之间的相互信任关系来实现的。在这里，客户端必须信任服务器证书，反之亦然，这样才能建立通信连接。这需要相互交换证书 [▶ 28]。

应用层

除了传输层，还可以在应用层确保通信连接的安全性。为此，可以使用服务器端点提供的各种身份验证机制 [▶ 29]。

4.10.2 端点

TwinCAT OPC UA Gateway 通过标准端口 48050/tcp 为 OPC UA 客户端提供各种端点。端点定义了客户端与服务器的连接类型，以及是否应确保其连接的安全性。



信任关系

请注意，若要使用安全端点，必须在服务器与客户端之间建立信任关系，而这种关系通常是通过两者的证书来实现的。此处 [▶ 28] 介绍了如何在网关端配置这种信任关系。



已弃用的端点

请注意，随着时间的推移，端点中当前可用的安全配置文件可能会被归类为潜在不安全文件，并由新版文件所取代。在这种情况下，建议更新 TwinCAT OPC UA Gateway。可以使用配置开关来重新激活已弃用且被列为不安全文件的安全策略。然而，出于安全考虑，我们建议保持此配置开关处于禁用状态。

端点列表

以下列表对 TwinCAT OPC UA Gateway 的端点进行了汇总。其中包括已经停止使用的端点。默认情况下，TwinCAT OPC UA Gateway 仅提供目前公认安全的端点。

安全配置文件	安全模式	简介
None	None	该端点不对消息进行加密或签名。相反，可以进行身份验证 [▶ 29]。
Basic128Rsa15（已弃用）	签名/签名和加密	从安全角度来看，该端点已被列为弃用端点，并且默认处于禁用状态。如有必要，可以再次启用该端点。
Basic256（已弃用）	签名/签名和加密	从安全角度来看，该端点已被列为弃用端点，并且默认处于禁用状态。如有必要，可以再次启用该端点。

安全配置文件	安全模式	简介
Basic256Sha256	签名/签名和加密	服务器中当前存在的端点，用于进行安全签名和加密。可以进行额外的身份验证 [▶ 29]。
Aes256_Sha256_RsaPss	签名/签名和加密	服务器中当前存在的端点，用于进行安全签名和加密。可以进行额外的身份验证 [▶ 29]。
Aes256_Sha256_RsaOaep	签名/签名和加密	服务器中当前存在的端点，用于进行安全签名和加密。可以进行额外的身份验证 [▶ 29]。

可以通过网关配置启用或禁用列表中的所有端点。下图中的所有端点均已启用。

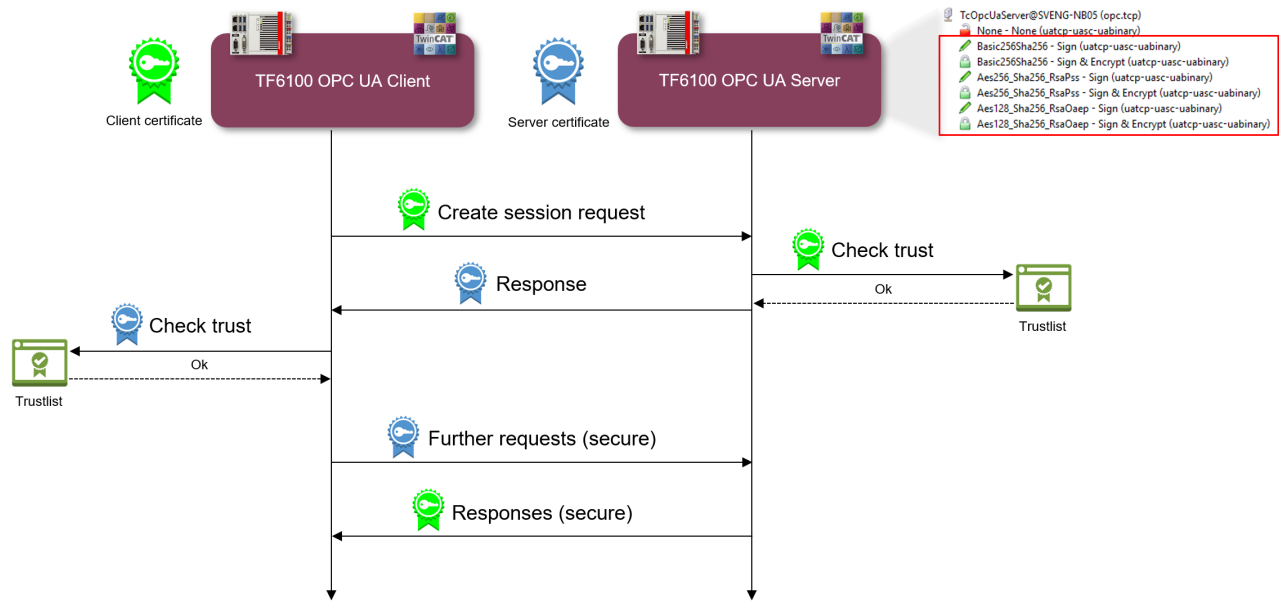
- None - None (uatcp-uasc-uabinary)
- Basic128Rsa15 - Sign (uatcp-uasc-uabinary)
- Basic128Rsa15 - Sign & Encrypt (uatcp-uasc-uabinary)
- Basic256 - Sign (uatcp-uasc-uabinary)
- Basic256 - Sign & Encrypt (uatcp-uasc-uabinary)
- Basic256Sha256 - Sign (uatcp-uasc-uabinary)
- Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)
- Aes256_Sha256_RsaPss - Sign (uatcp-uasc-uabinary)
- Aes256_Sha256_RsaPss - Sign & Encrypt (uatcp-uasc-uabinary)
- Aes128_Sha256_RsaOaep - Sign (uatcp-uasc-uabinary)
- Aes128_Sha256_RsaOaep - Sign & Encrypt (uatcp-uasc-uabinary)

4.10.3 证书交换

要通过安全端点 [▶ 27] 确保传输层通信连接的安全，就必须在客户端和服务端之间建立连接。默认情况下，TwinCAT OPC UA Gateway 在首次启动时会生成一个机器特定的自签名密钥对，该密钥对由一个公钥和一个私钥组成。然而，您也可以使用任意证书颁发机构或技术，例如 Active Directory 或 OpenSSL，将其集成到您的 IT 基础设施中。为了实现简单管理和安全访问证书，设置全局发现服务器是很有意义的。

若要在任何 OPC UA 客户端与 TwinCAT OPC UA Gateway 之间建立信任关系，需要使用客户端证书的公钥。网关必须相应地信任此服务器。网关在应用程序目录的一个子目录中管理客户端证书的信任设置。

下图以 TwinCAT OPC UA Client 和 TwinCAT OPC UA Server 为例，说明了建立安全通信连接时客户端和服务端证书之间的关系。然而，对于后者，这一点也可以 1:1 地应用到网关上。



客户端随 CreateSession 请求一起传输其公钥。然后，服务器可选择检查信任关系。如果服务器信任客户端，便会在响应中传输自己的公钥。因此，客户端还可以选择检查与服务器之间的信任关系。

如果确保互信，则启动通信连接。然后，服务器的公钥用于加密客户端向服务器发出的请求。然后，服务器对客户端的响应将使用客户端的公钥进行加密。然后，通信双方都可以选择用自己的私钥对收到的消息进行解密。

信息是反向签名的：信息是用发件人的私钥签名的。由于收件人能识别发件人的公钥，因此可以验证签名。

通过文件系统配置信任关系

通过在信任/拒绝目录之间移动客户端证书，可以相应地调整信任设置。客户端证书的公钥会在客户端首次尝试与安全端点连接时自动存储在拒绝证书的目录中。通过随后将公钥移至受信任证书的目录，客户端在下次尝试连接时就会受到信任，可以进行连接。

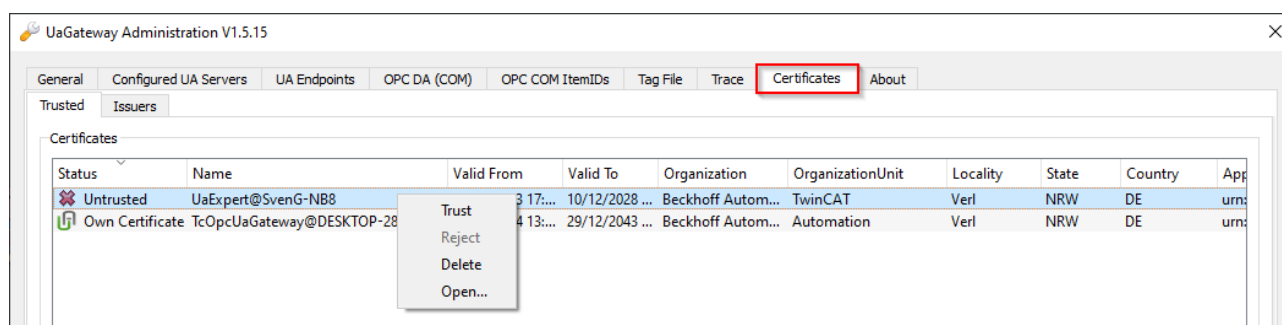
● 接受所有证书



如果在网关的端点配置 [► 24] 中启用了此选项，则网关将自动信任所有客户端证书。在这种情况下，服务器不会将这些证书列在上述任何目录中。

使用配置器配置信任关系

您还可以通过 配置器 进行信任设置。配置器包括一个用于配置信任设置的图形用户界面。您可以通过上下文菜单来信任或拒绝证书。



4.10.4 身份验证

OPC UA 客户端可以使用多种登录方法向 TwinCAT OPC UA Gateway 进行身份验证。支持使用以下“身份令牌”：

- Anonymous (匿名)
- User name/Password (用户名/密码)
- User certificate (用户证书)

● 交付状态



网关交付时，身份令牌“匿名”已启用。我们建议在初次调试后，配置用于访问服务器的用户或用户组。有关更多信息，请参见 建议的步骤 [► 17]。

Anonymous (匿名)

此类身份验证允许任何 OPC UA 客户端与网关建立连接。不需要指定用户身份。我们建议在调试网关后禁用此身份验证方法。可以通过配置器来完成此操作。

User name/Password (用户名/密码)

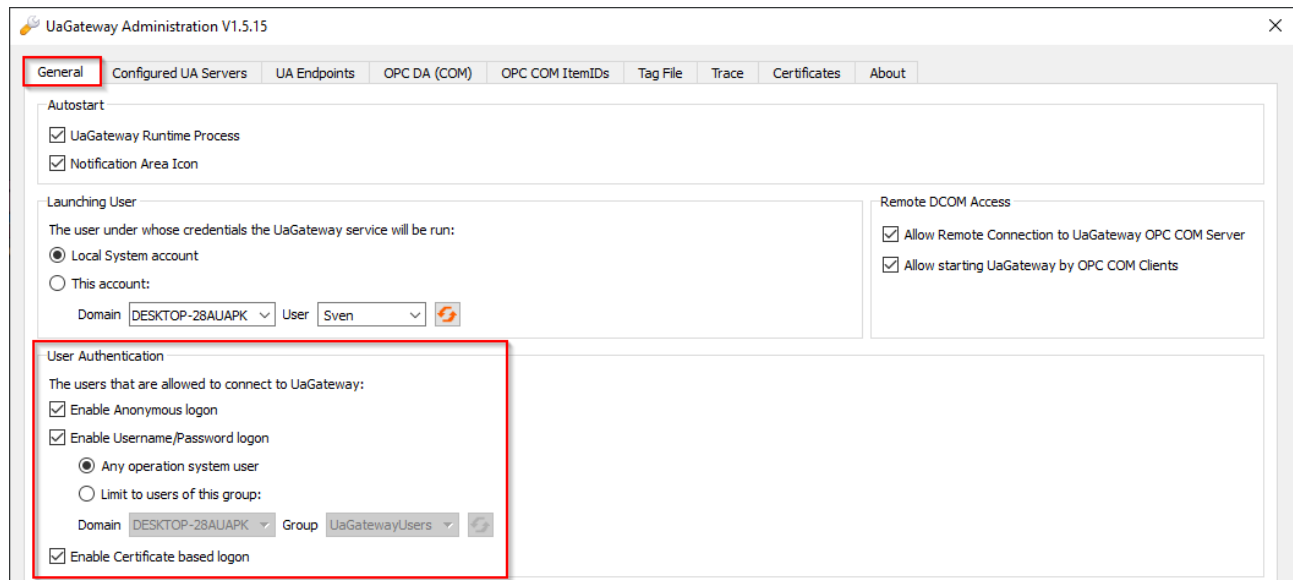
此身份验证方法使用用户名/密码组合，在网关的 OPC UA 服务器上对客户端进行身份验证。用户或用户组在操作系统中进行创建和管理。

User certificate (用户证书)

此类身份验证使用证书对网关的 OPC UA 服务器进行身份验证。网关端对用户证书的处理与传输层对证书的使用完全相同，即网关必须信任（用户）证书，客户端才能成功地通过证书向网关进行身份验证。为此，可在网关上创建一个用于管理用户证书的独立应用程序目录 [► 20]（“pkuser”）。

配置

通常通过配置器来启用/禁用各种身份验证方法。



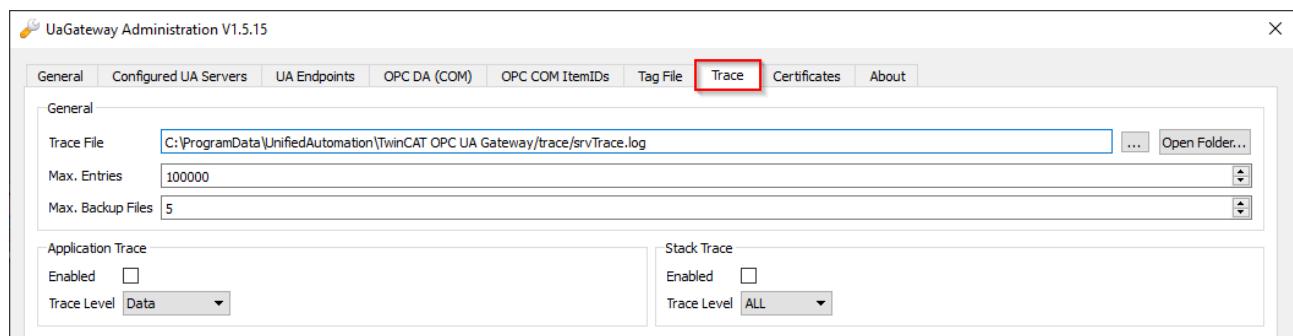
4.11 日志记录

您可以启用网关中的日志文件，以便进行扩展诊断，然后根据不同的日志等级记录各种信息。

● 日志记录对运行特性的影响

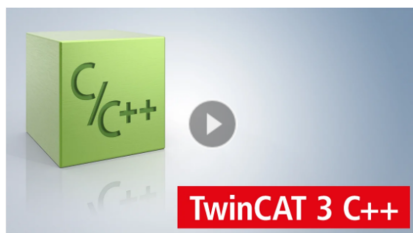
i 请注意，激活日志文件可能会对 TwinCAT OPC UA Gateway 的速度和运行特性产生负面影响。

所创建的日志文件的默认路径在应用程序目录 [► 20]一章中有更详细的说明，也可以在 TwinCAT OPC UA Gateway 配置器中进行查看。



5 教程

可在我们的网站 <https://www.beckhoff.com/tutorials> 上查看本产品的视频教程。视频教程提供了对产品和产品各个方面的快速入门。



14.03.2024 | Multimedia

Tutorial: TwinCAT 3 C++ overview

Get an overview of the C++ integration into TwinCAT.

[Learn more →](#)



12.02.2024 | Multimedia

Tutorial: Chart synchronization in TwinCAT Scope

Learn how to dock and synchronize charts in TwinCAT Scope.

[Learn more →](#)



12.02.2024 | Multimedia

Tutorial: Getting started with TF6100 TwinCAT 3 OPC UA Server

Learn how to configure the TwinCAT OPC UA Server.

[Learn more →](#)

6 附录

6.1 错误诊断

行为	注意
网关无法连接到服务器。	可能的原因之一是使用了旧的配置。例如，如果存在新的服务器证书，则只有当已配置的端点被删除并以不同名称重新添加时，网关才会注意到该变更。如果使用相同的端点或名称相同的新端点，网关将使用缓存中的连接信息，从而导致无法再连接到服务器。

6.2 ADS 返回代码

错误代码分组：

全局错误代码：0x0000 [► 32]... (0x9811_0000 ...)

路由器错误代码：0x0500 [► 33]... (0x9811_0500 ...)

一般 ADS 错误：0x0700 [► 33]... (0x9811_0700 ...)

RTime 错误代码：0x1000 [► 34]... (0x9811_1000 ...)

全局错误代码

Hex	Dec	HRESULT	名称	描述
0x0	0	0x98110000	ERR_NOERROR	无错误。
0x1	1	0x98110001	ERR_INTERNAL	内部错误。
0x2	2	0x98110002	ERR_NORTIME	不具有实时性。
0x3	3	0x98110003	ERR_ALLOCCLOCKEDMEM	分配已锁定 - 内存错误。
0x4	4	0x98110004	ERR_INSERTMAILBOX	邮箱已满 - 无法发送 ADS 消息。减少每个周期的 ADS 消息数量将有所帮助。
0x5	5	0x98110005	ERR_WRONGRECEIVEHMSG	HMSG 错误。
0x6	6	0x98110006	ERR_TARGETPORTNOTFOUND	未找到目标端口 - ADS 服务器未启动或无法访问。
0x7	7	0x98110007	ERR_TARGETMACHINENOTFOUND	未找到目标计算机 - 未找到 AMS 路由。
0x8	8	0x98110008	ERR_UNKNOWNCMDID	未知命令 ID。
0x9	9	0x98110009	ERR_BADTASKID	任务 ID 无效。
0xA	10	0x9811000A	ERR_NOIO	No IO。
0xB	11	0x9811000B	ERR_UNKNOWNAMSCMD	未知 AMS 命令。
0xC	12	0x9811000C	ERR_WIN32ERROR	Win32 错误。
0xD	13	0x9811000D	ERR_PORTNOTCONNECTED	端口未连接。
0xE	14	0x9811000E	ERR_INVALIDAMSLENGTH	AMS 长度无效。
0xF	15	0x9811000F	ERR_INVALIDAMSNETID	AMS Net ID 无效。
0x10	16	0x98110010	ERR_LOWINSTLEVEL	安装级别 - TwinCAT 2 授权错误。
0x11	17	0x98110011	ERR_NODEBUGINTAVAILABLE	无调试可用。
0x12	18	0x98110012	ERR_PORTDISABLED	端口已禁用 - TwinCAT 系统服务未启动。
0x13	19	0x98110013	ERR_PORTALREADYCONNECTED	端口已连接。
0x14	20	0x98110014	ERR_AMSSYNC_W32ERROR	AMS Sync Win32 错误。
0x15	21	0x98110015	ERR_AMSSYNC_TIMEOUT	AMS Sync 超时。
0x16	22	0x98110016	ERR_AMSSYNC_AMSERROR	AMS Sync 错误。
0x17	23	0x98110017	ERR_AMSSYNC_NOINDEXINMAP	不存在适用于 AMS Sync 的索引映射。
0x18	24	0x98110018	ERR_INVALIDAMSPORT	AMS 端口无效。
0x19	25	0x98110019	ERR_NOMEMORY	无内存。
0x1A	26	0x9811001A	ERR_TCPSEND	TCP 发送错误。
0x1B	27	0x9811001B	ERR_HOSTUNREACHABLE	主机无法访问。
0x1C	28	0x9811001C	ERR_INVALIDAMSFRAGMENT	AMS 片段无效。
0x1D	29	0x9811001D	ERR_TLSEND	TLS 发送错误 - ADS 安全连接失败。
0x1E	30	0x9811001E	ERR_ACCESSDENIED	拒绝访问 - 拒绝 ADS 安全访问。

路由器错误代码

Hex	Dec	HRESULT	名称	描述
0x500	1280	0x98110500	ROUTERERR_NOLOCKEDMEMORY	无法分配锁定的内存。
0x501	1281	0x98110501	ROUTERERR_RESIZEMEMORY	路由器内存大小无法更改。
0x502	1282	0x98110502	ROUTERERR_MAILBOXFULL	邮箱已达到最大消息数。
0x503	1283	0x98110503	ROUTERERR_DEBUGBOXFULL	调试邮箱已达到最大消息数。
0x504	1284	0x98110504	ROUTERERR_UNKNOWNPORTTYPE	端口类型未知。
0x505	1285	0x98110505	ROUTERERR_NOTINITIALIZED	路由器未初始化。
0x506	1286	0x98110506	ROUTERERR_PORTALREADYINUSE	端口号已分配。
0x507	1287	0x98110507	ROUTERERR_NOTREGISTERED	端口未注册。
0x508	1288	0x98110508	ROUTERERR_NOMOREQUEUES	已达到最大端口数。
0x509	1289	0x98110509	ROUTERERR_INVALIDPORT	端口无效。
0x50A	1290	0x9811050A	ROUTERERR_NOTACTIVATED	路由未激活。
0x50B	1291	0x9811050B	ROUTERERR_FRAGMENTBOXFULL	邮箱已达到最大片段消息数。
0x50C	1292	0x9811050C	ROUTERERR_FRAGMENTTIMEOUT	发生片段超时。
0x50D	1293	0x9811050D	ROUTERERR_TOBEREMOVED	端口已移除。

一般性 ADS 错误代码

Hex	Dec	HRESULT	名称	描述
0x700	1792	0x98110700	ADSERR_DEVICE_ERROR	一般性设备错误。
0x701	1793	0x98110701	ADSERR_DEVICE_SRVNOTSUPP	服务器不支持该服务。
0x702	1794	0x98110702	ADSERR_DEVICE_INVALIDGRP	索引组无效。
0x703	1795	0x98110703	ADSERR_DEVICE_INVALIDOFFSET	索引偏移量无效。
0x704	1796	0x98110704	ADSERR_DEVICE_INVALIDACCESS	不允许读取或写入。 可能有几种原因。例如，创建路由时输入了错误的密码。
0x705	1797	0x98110705	ADSERR_DEVICE_INVALIDSIZE	参数大小不正确。
0x706	1798	0x98110706	ADSERR_DEVICE_INVALIDDATA	无效数据值。
0x707	1799	0x98110707	ADSERR_DEVICE_NOTREADY	设备尚未准备好运行。
0x708	1800	0x98110708	ADSERR_DEVICE_BUSY	设备正忙。
0x709	1801	0x98110709	ADSERR_DEVICE_INVALIDCONTEXT	操作系统上下文无效。这可能是由于在不同的任务中使用 ADS 函数块造成的。可以通过在 PLC 中进行多任务同步解决这个问题。
0x70A	1802	0x9811070A	ADSERR_DEVICE_NOMEMORY	内存不足。
0x70B	1803	0x9811070B	ADSERR_DEVICE_INVALIDPARM	参数值无效。
0x70C	1804	0x9811070C	ADSERR_DEVICE_NOTFOUND	未找到（文件…）。
0x70D	1805	0x9811070D	ADSERR_DEVICE_SYNTAX	文件或命令中存在语法错误。
0x70E	1806	0x9811070E	ADSERR_DEVICE_INCOMPATIBLE	对象不匹配。
0x70F	1807	0x9811070F	ADSERR_DEVICE_EXISTS	对象已存在。
0x710	1808	0x98110710	ADSERR_DEVICE_SYMBOLNOTFOUND	符号未找到。
0x711	1809	0x98110711	ADSERR_DEVICE_SYMBOLVERSIONINVALID	符号版本无效。这可能是由于联机更改造成的。创建新句柄。
0x712	1810	0x98110712	ADSERR_DEVICE_INVALIDSTATE	设备（服务器）处于无效状态。
0x713	1811	0x98110713	ADSERR_DEVICE_TRANSMODENOTSUPP	不支持 AdsTransMode。
0x714	1812	0x98110714	ADSERR_DEVICE_NOTIFYHNDINVALID	通知句柄无效。
0x715	1813	0x98110715	ADSERR_DEVICE_CLIENTUNKNOWN	通知客户端未注册。
0x716	1814	0x98110716	ADSERR_DEVICE_NOMOREHDLs	没有更多的句柄可用。
0x717	1815	0x98110717	ADSERR_DEVICE_INVALIDWATCHSIZE	通知大小过大。
0x718	1816	0x98110718	ADSERR_DEVICE_NOTINIT	设备未初始化。
0x719	1817	0x98110719	ADSERR_DEVICE_TIMEOUT	设备超时。
0x71A	1818	0x9811071A	ADSERR_DEVICE_NOINTERFACE	接口查询失败。
0x71B	1819	0x9811071B	ADSERR_DEVICE_INVALIDINTERFACE	请求的接口错误。

Hex	Dec	HRESULT	名称	描述
0x71C	1820	0x9811071C	ADSERR_DEVICE_INVALIDCLSID	Class ID 无效。
0x71D	1821	0x9811071D	ADSERR_DEVICE_INVALIDOBJID	Object ID 无效。
0x71E	1822	0x9811071E	ADSERR_DEVICE_PENDING	请求待定。
0x71F	1823	0x9811071F	ADSERR_DEVICE_ABORTED	请求已中止。
0x720	1824	0x98110720	ADSERR_DEVICE_WARNING	警告信号。
0x721	1825	0x98110721	ADSERR_DEVICE_INVALIDARRAYIDX	数组索引无效。
0x722	1826	0x98110722	ADSERR_DEVICE_SYMBOLNOTACTIVE	符号未激活。
0x723	1827	0x98110723	ADSERR_DEVICE_ACCESSDENIED	拒绝访问。 有几种可能的原因。例如，单向 ADS 路由用于相反方向。
0x724	1828	0x98110724	ADSERR_DEVICE_LICENSENOTFOUND	缺少授权。
0x725	1829	0x98110725	ADSERR_DEVICE_LICENSEEXPIRED	授权已过期。
0x726	1830	0x98110726	ADSERR_DEVICE_LICENSEEXCEEDED	超出授权。
0x727	1831	0x98110727	ADSERR_DEVICE_LICENSEINVALID	授权无效。
0x728	1832	0x98110728	ADSERR_DEVICE_LICENSESYSTEMID	授权问题：系统 ID 无效。
0x729	1833	0x98110729	ADSERR_DEVICE_LICENSENOTIMELIMIT	授权不受时间限制。
0x72A	1834	0x9811072A	ADSERR_DEVICE_LICENSEFUTUREISSUE	授权问题：未来的时间。
0x72B	1835	0x9811072B	ADSERR_DEVICE_LICENSETIMETOLONG	授权期限太长。
0x72C	1836	0x9811072C	ADSERR_DEVICE_EXCEPTION	系统启动异常。
0x72D	1837	0x9811072D	ADSERR_DEVICE_LICENSEDUPLICATED	授权文件读取了两次。
0x72E	1838	0x9811072E	ADSERR_DEVICE_SIGNATUREINVALID	签名无效。
0x72F	1839	0x9811072F	ADSERR_DEVICE_CERTIFICATEINVALID	证书无效。
0x730	1840	0x98110730	ADSERR_DEVICE_LICENSEOEMNOTFOUND	OEM未知公钥。
0x731	1841	0x98110731	ADSERR_DEVICE_LICENSERESTRICTED	此系统 ID 授权无效。
0x732	1842	0x98110732	ADSERR_DEVICE_LICENSEDEMODENIED	演示授权已禁止。
0x733	1843	0x98110733	ADSERR_DEVICE_INVALIDFNCD	无效函数 ID。
0x734	1844	0x98110734	ADSERR_DEVICE_OUTOFRANGE	超出有效范围。
0x735	1845	0x98110735	ADSERR_DEVICE_INVALIDALIGNMENT	无效对齐。
0x736	1846	0x98110736	ADSERR_DEVICE_LICENSEPLATFORM	无效平台级别。
0x737	1847	0x98110737	ADSERR_DEVICE_FORWARD_PL	上下文 - 转到被动级别。
0x738	1848	0x98110738	ADSERR_DEVICE_FORWARD_DL	上下文 - 转到调度级别。
0x739	1849	0x98110739	ADSERR_DEVICE_FORWARD_RT	上下文 - 转到实时。
0x740	1856	0x98110740	ADSERR_CLIENT_ERROR	客户端错误。
0x741	1857	0x98110741	ADSERR_CLIENT_INVALIDPARM	服务包含无效参数。
0x742	1858	0x98110742	ADSERR_CLIENT_LISTEMPTY	轮询列表为空。
0x743	1859	0x98110743	ADSERR_CLIENT_VARUSED	Var 连接已在使用中。
0x744	1860	0x98110744	ADSERR_CLIENT_DUPLINVOKEID	调用的 ID 已在使用中。
0x745	1861	0x98110745	ADSERR_CLIENT_SYNCTIMEOUT	已发生超时 - 远程终端在指定的 ADS 超时中未响应。远程终端的路由设置可能配置不正确。
0x746	1862	0x98110746	ADSERR_CLIENT_W32ERROR	Win32 子系统中发生错误。
0x747	1863	0x98110747	ADSERR_CLIENT_TIMEOUTINVALID	客户端超时值无效。
0x748	1864	0x98110748	ADSERR_CLIENT_PORTNOTOPEN	端口未打开。
0x749	1865	0x98110749	ADSERR_CLIENT_NOAMSADDR	无 AMS 地址。
0x750	1872	0x98110750	ADSERR_CLIENT_SYNCINTERNAL	Ads sync 中发生内部错误。
0x751	1873	0x98110751	ADSERR_CLIENT_ADDHASH	哈希表溢出。
0x752	1874	0x98110752	ADSERR_CLIENT_REMOVEHASH	未在表格中找到密钥。
0x753	1875	0x98110753	ADSERR_CLIENT_NOMORESVM	缓存中没有符号。
0x754	1876	0x98110754	ADSERR_CLIENT_SYNCRESINVALID	收到无效响应。
0x755	1877	0x98110755	ADSERR_CLIENT_SYNCPORTLOCKED	同步端口已锁定。
0x756	1878	0x98110756	ADSERR_CLIENT_REQUESTCANCELLED	请求被取消。

RTime 错误代码

Hex	Dec	HRESULT	名称	描述
0x1000	4096	0x98111000	RTERR_INTERNAL	实时系统中发生内部错误。
0x1001	4097	0x98111001	RTERR_BADTIMERPERIODS	计时器值无效。

Hex	Dec	HRESULT	名称	描述
0x1002	4098	0x98111002	RTERR_INVALIDTASKPTR	任务指针提供了无效值 0（零）。
0x1003	4099	0x98111003	RTERR_INVALIDSTACKPTR	堆栈指针提供了无效值 0（零）。
0x1004	4100	0x98111004	RTERR_PRIOEXISTS	请求任务优先级已分配。
0x1005	4101	0x98111005	RTERR_NOMORETCB	没有可用的空闲 TCB（任务控制块）。TCB 的最大数量为 64。
0x1006	4102	0x98111006	RTERR_NOMORESEMAS	没有可用的空闲信号。信号的最大数量为 64。
0x1007	4103	0x98111007	RTERR_NOMOREQUEUES	队列中没有可用的空闲空间。队列中的最大位置数为 64。
0x100D	4109	0x9811100D	RTERR_EXTIRQALREADYDEF	已应用外部同步中断。
0x100E	4110	0x9811100E	RTERR_EXTIRQNOTDEF	未应用外部同步中断。
0x100F	4111	0x9811100F	RTERR_EXTIRQINSTALLFAILED	外部同步中断应用失败。
0x1010	4112	0x98111010	RTERR_IRQNOTLESSOREQUAL	在错误的上下文中调用服务函数
0x1017	4119	0x98111017	RTERR_VMXNOTSUPPORTED	不支持 Intel® VT-x 扩展。
0x1018	4120	0x98111018	RTERR_VMXDISABLED	BIOS 中未启用 Intel® VT-x 扩展。
0x1019	4121	0x98111019	RTERR_VMXCONTROLSMISSING	Intel® VT-x 扩展中缺少函数。
0x101A	4122	0x9811101A	RTERR_VMXENABLEFAILS	Intel® VT-x 激活失败。

具体的正向 HRESULT 返回代码：

HRESULT	名称	描述
0x0000_0000	S_OK	无错误。
0x0000_0001	S_FALSE	无错误。 示例：处理成功，但有一个负面或不完整的结果。
0x0000_0203	S_PENDING	无错误。 示例：处理成功，但还没有结果。
0x0000_0256	S_WATCHDOG_TIMEOUT	无错误。 示例：处理成功，但发生了超时。

TCP Winsock 错误代码

Hex	Dec	名称	描述
0x274C	10060	WSAETIMEDOUT	发生连接超时 - 在创建连接时发生错误，因为远程终端在特定时间后未正确响应，或者所建立连接因所连接主机未响应而无法维持。
0x274D	10061	WSAECONNREFUSED	连接遭到拒绝 - 无法建立连接，因为目标计算机明确拒绝了该连接。此错误通常由尝试连接到外部主机上处于非活动状态的服务（即没有运行服务器应用程序的服务）导致。
0x2751	10065	WSAHOSTUNREACH	不存在至主机的路由 - 套接字操作引用了不可用的主机。
更多 Winsock 错误代码： Win32 错误代码			

6.3 技术支持和服务

倍福公司及其合作伙伴在世界各地提供全面的技术支持和服务，对与倍福产品和系统解决方案相关的所有问题提供快速有效的帮助。

下载搜索器

我们的下载搜索器包含我们供您下载的所有文件。您可以通过它搜索我们的应用案例、技术文档、技术图纸、配置文件等等。

可供下载的文件格式多种多样。

倍福分公司和代表处

若需要倍福产品的本地支持和服务，请联系倍福分公司或代表处！

倍福遍布世界各地的分公司和代表处地址可在倍福官网上找到：<http://www.beckhoff.com.cn>

该网页还提供更多倍福产品组件的文档。

倍福技术支持

技术支持部门为您提供全面的技术援助，不仅帮助您应用各种倍福产品，还提供其他广泛的服务：

- 技术支持
- 复杂自动化系统的设计、编程和调试
- 以及倍福系统组件的各种培训课程

热线电话：+49 5246 963-157

电子邮箱：support@beckhoff.com

倍福售后服务

倍福服务中心提供所有售后服务：

- 现场服务
- 维修服务
- 备件服务
- 热线服务

热线电话：+49 5246 963-460

电子邮箱：service@beckhoff.com

倍福公司总部

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20

33415 Verl

Germany

电话：+49 5246 963-0

电子邮箱：info@beckhoff.com

网址：www.beckhoff.com

Trademark statements

Beckhoff®, ATRO®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, MX-System®, Safety over EtherCAT®, TC/BSD®, TwinCAT®, TwinCAT/BSD®, TwinSAFE®, XFC®, XPlanar® and XTS® are registered and licensed trademarks of Beckhoff Automation GmbH.

Third-party trademark statements

Arm, Arm9 and Cortex are trademarks or registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere.

DALI, DALI-2, D4i, DALI+, and DiiA are trademarks in various countries in the exclusive use of the Digital Illumination Interface Alliance.

Excel, IntelliSense, Microsoft, Microsoft Azure, Microsoft Edge, PowerShell, Visual Studio, Windows and Xbox are trademarks of the Microsoft group of companies.

MAX®, Stratix®, Cyclone®, Altera®, Agilex™, Arria®, Intel, the Intel logo, Intel Core, Xeon, Intel Atom, Celeron and Pentium are trademarks of Intel Corporation or its subsidiaries.

OPC UA is a registered trademark of the OPC Foundation.

更多信息:
www.beckhoff.com/TF6100

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Germany
电话号码: +49 5246 9630
info@beckhoff.com
www.beckhoff.com

