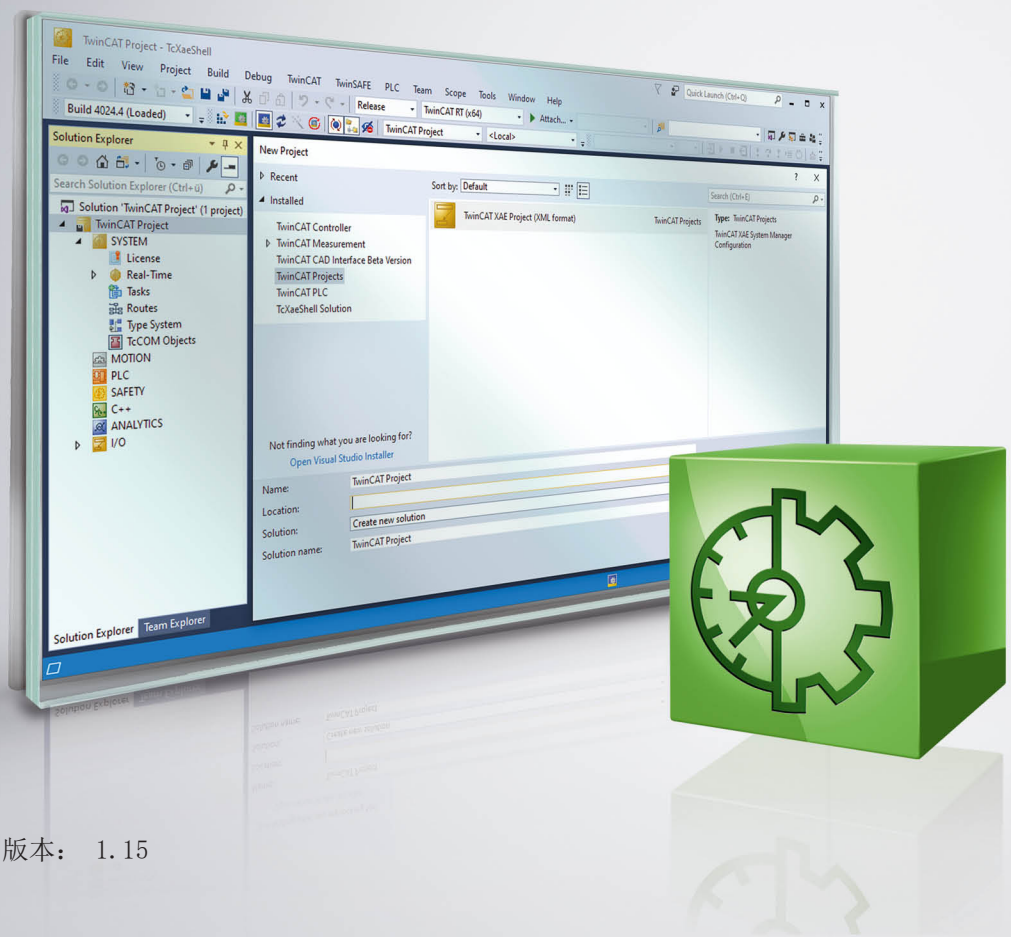
BECKHOFF New Automation Technology

手册 | ZH

TE1000

TwinCAT 3 | Software Protection



2022-003-21 | 版本： 1.15

目录

1 前言

1.1 文档说明

本说明仅供熟悉适用国家标准的控制和自动化工程专家使用。
在安装和调试元器件时，必须遵循本文档及以下注意事项和说明。
技术人员应负责在每次安装和调试时使用已发布的文档。

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®、TwinCAT®、TwinCAT/BSD®、TC/BSD®、EtherCAT®、EtherCAT G®、EtherCAT G10®、EtherCAT P®、Safety over EtherCAT®、TwinSAFE®、XFC®、XTS® 和 XPlanar® 均为倍福自动化有限公司的注册商标并由公司授权使用。
本出版物中使用的其他名称可能是商标，第三方出于自身目的使用它们可能侵犯商标所有者的权利。

正在申请的专利

涵盖 EtherCAT 技术，包括但不限于以下专利申请和专利：：
EP1590927、EP1789857、EP1456722、EP2137893、DE102015105702
包括在其他各国家的相应专利申请或注册。

EtherCAT® 是注册商标和专利技术，由德国倍福自动化有限公司授权使用

版权所有

1.2 安全说明

安全规范

请注意以下安全说明和阐述！
可在以下页面或安装、接线、调试等区域找到产品相关的安全说明。

责任免除

所有元器件在供货时都配有适合应用的特定硬件和软件配置。禁止未按文档所述修改硬件或软件配置，德国倍福自动化有限公司不对此承担责任。

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。

符号说明

在本文档中，下列符号随安全指示或说明一起使用。必须仔细阅读并严格遵守安全说明！

⚠ 危险

严重受伤的风险！

未遵守带有此符号的安全说明将直接危及人员生命和健康。

⚠ 警告

受伤的风险！

未遵守带有此符号的安全说明将危及人员生命和健康。

⚠ 谨慎

人身伤害！

未遵守带有此符号的安全说明可能导致人员受伤。

注意

危害环境或损坏设备

未遵守带有此符号的安全说明可能危害环境或损坏设备。

提示或指示

此符号表示该信息有助于更好地理解。

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。

2 介绍

TwinCAT 3 Engineering 配备不同的应用软件保护功能：

- 通过定义用户组和分配访问级别（“对象保护级别”）对源代码进行可配置的访问限制
- 通过加密源代码和根文件的专有技术保护
- 使用 TwinCAT 3 授权技术对 OEM 应用软件进行克隆保护（需要倍福 IPC/EPC 或 TwinCAT 3 加密狗）

通过使用 TwinCAT 3 授权技术，OEM 还可以为其应用软件的功能扩展自行生成授权并在市场上出售（需要倍福 IPC/EPC 或 TwinCAT 3 加密狗）。

为了能够使用应用软件保护功能，需要有倍福签署的 OEM 证书。访问保护的中心交换点为用户数据库。

内容

2.1 操作系统以及软件版本需求

操作系统：

- 要使用软件保护的功能，需要安装Windows 7 或更高版本的系统（或对应的嵌入式版本）。Windows XP 和 Windows CE（Windows Embedded Compact）不支持启动文件的加密或 OEM 授权。

只有使用最新版本的 TwinCAT 3，才会获得可靠的保护。

为确保获得可靠的保护（例如安全加密），请始终使用最新版本的TwinCAT 3。这可以提供最高的安全性。

至少应使用 TwinCAT 3.1 Build 4024.x。
鉴于安全因素，请勿使用旧版本！

2.2 软件访问保护的三大支柱

软件访问保护的三大支柱：

- 加密（*=不再可读*）
- 签名（*=不再可交换*）
- 访问权的分配（->“对象保护级别 [▶ 64]”）。

因此，有以下措施可以保护项目免受未经授权的访问：

- 为项目组件加密和签名
- 定义项目组件的访问权限
- **重要提示：对相关项目文件进行加密和签名**

未设置正确访问级别的加密可以在操作系统层面上保护相应的文件，但仍然可以通过 TwinCAT 3 开发环境来访问项目。

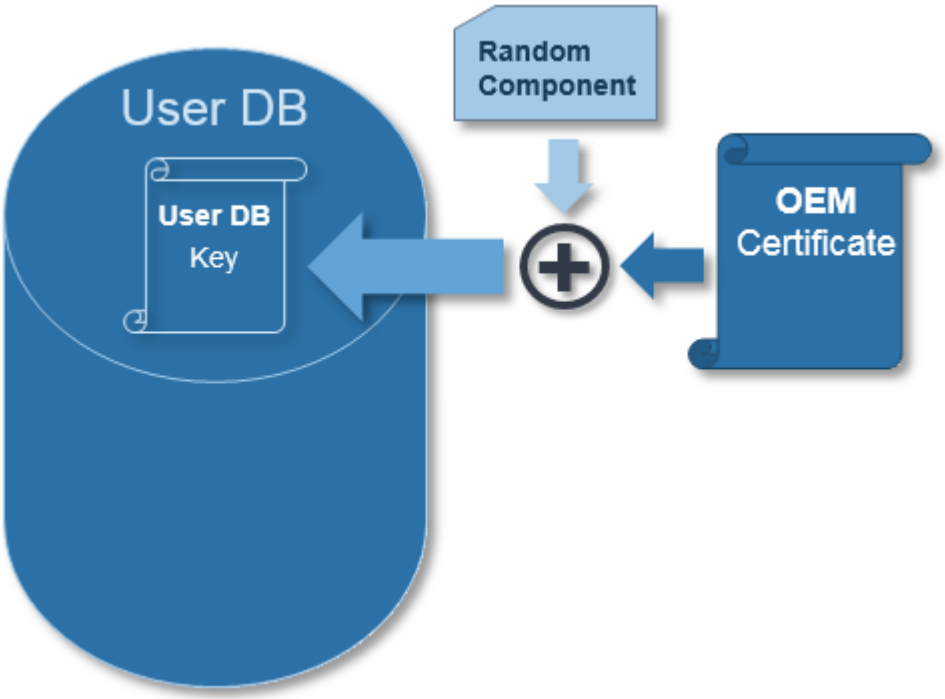
反之，正确设置访问级别会定义 TwinCAT 3 Engineering 内部的访问，且仍可以通过操作系统级别访问源代码。

如果没有签名，一个项目文件或一个项目组件可能被交换成另一个同名的文件。

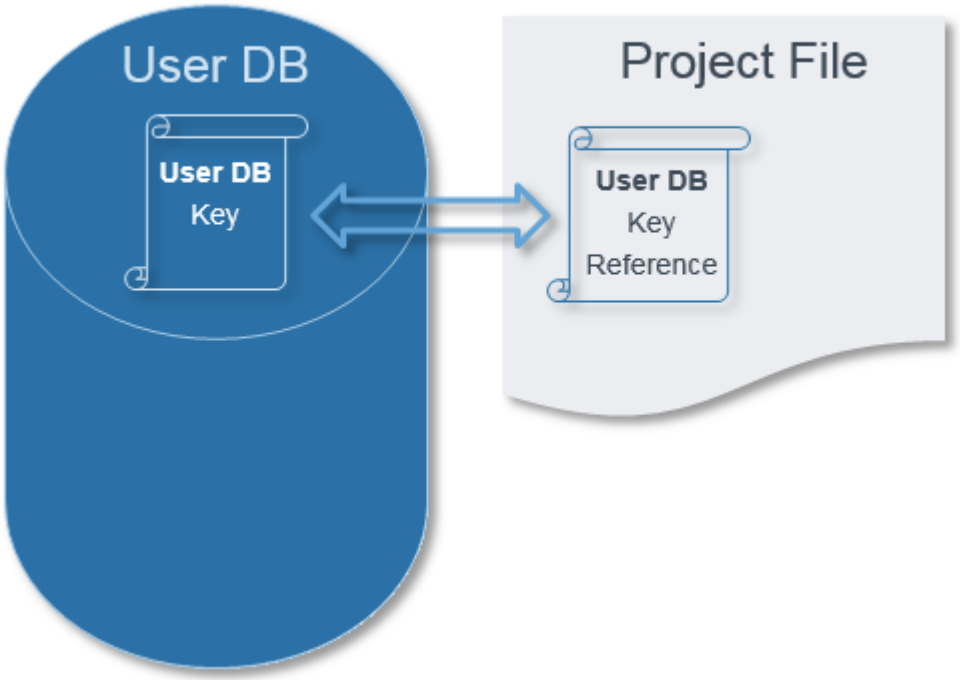
2.3 用户数据库作为中间节点

通过用户数据库（User DB） [▶ 31]来控制项目组件的访问。

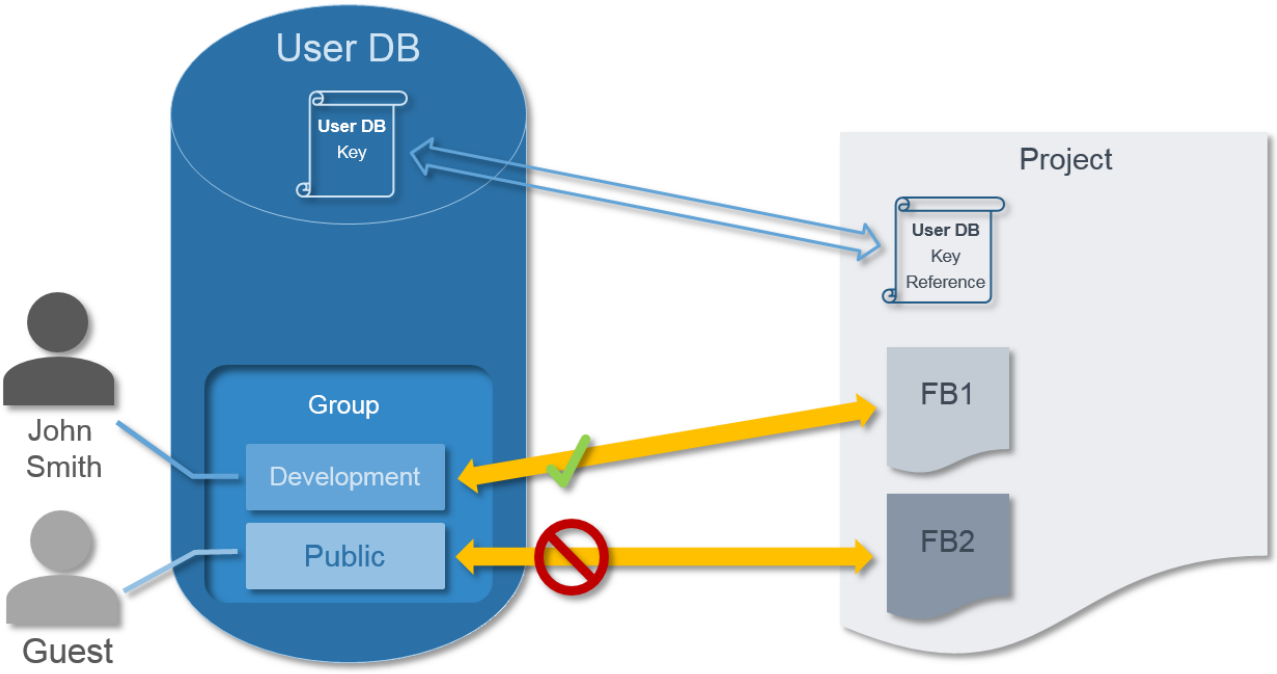
数据库的内容通过管理员的签名得到保护，以防止未经授权的更改。为确保能够明确地识别数据库，提供一个“用户数据库密钥”——这是由 OEM 证书的组件和一个随机组件组成的独特标识。随机组件确保每个创建的用户数据库都会有一个唯一的用户数据库密钥。



如果一个项目被授权用户与一个特定用户数据库联系起来，其用户数据库密钥则会存储在项目中。此后，这个项目只能与此用户数据库一起打开。



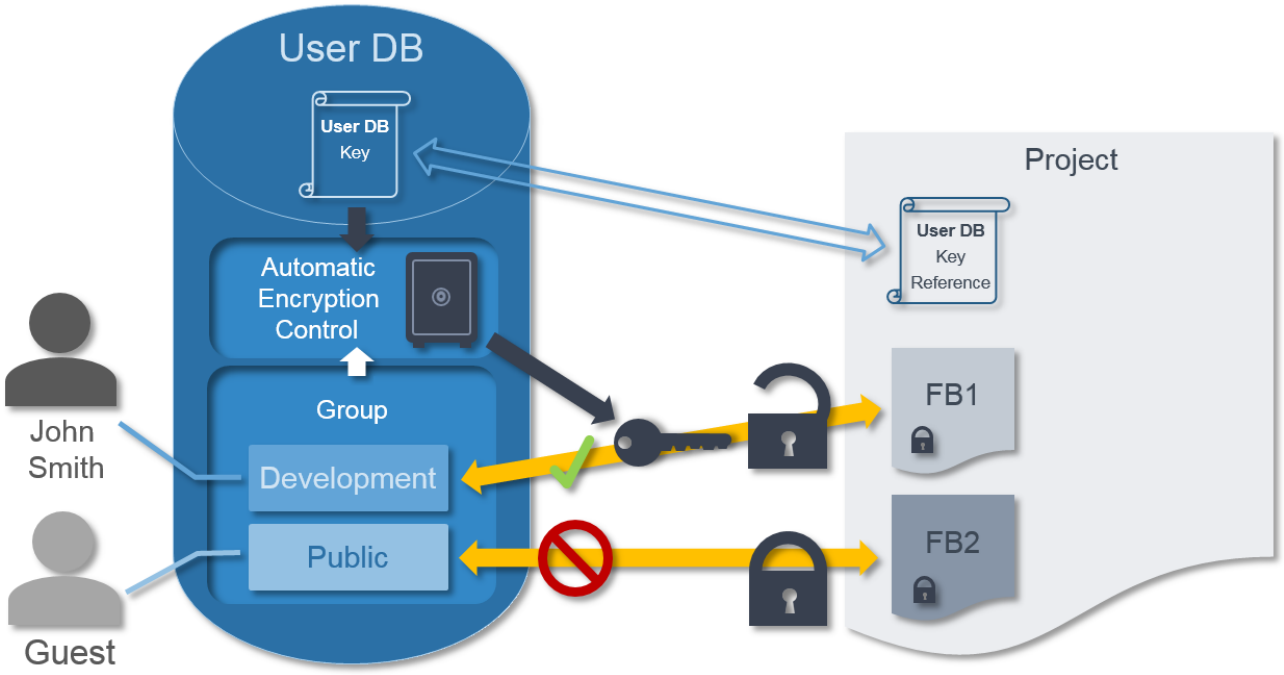
用户的介绍 [▶ 53] 在用户数据库内通过分组来调节。



也就是说，从一开始便在 TwinCAT 3 Engineering 中指定了访问权限。然而，仍可以通过操作系统层面访问源代码的或交换项目文件。因此，除了对访问权限的规定外，TwinCAT 3 Engineering 中还有另外两项保护措施：项目文件的签名和加密。

项目文件的签名确保了项目文件在操作系统层面不会被交换成另一个同名的文件。文件的签名数据保存在上级项目节点中。该项目必须与用户数据库链接。

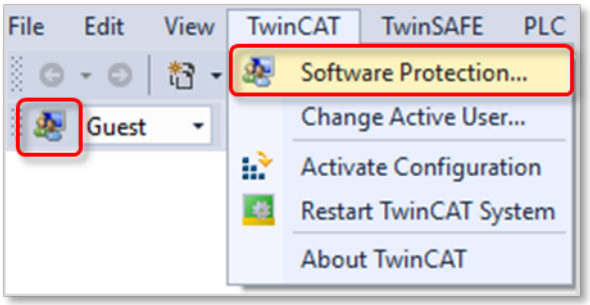
用于加密项目文件的密钥则保存在用户数据库中。因此，相应的用户数据库必须始终存在于**工程计算机**上（路径：*c:\Twincat\3.1\CustomConfig\userDBs*）。



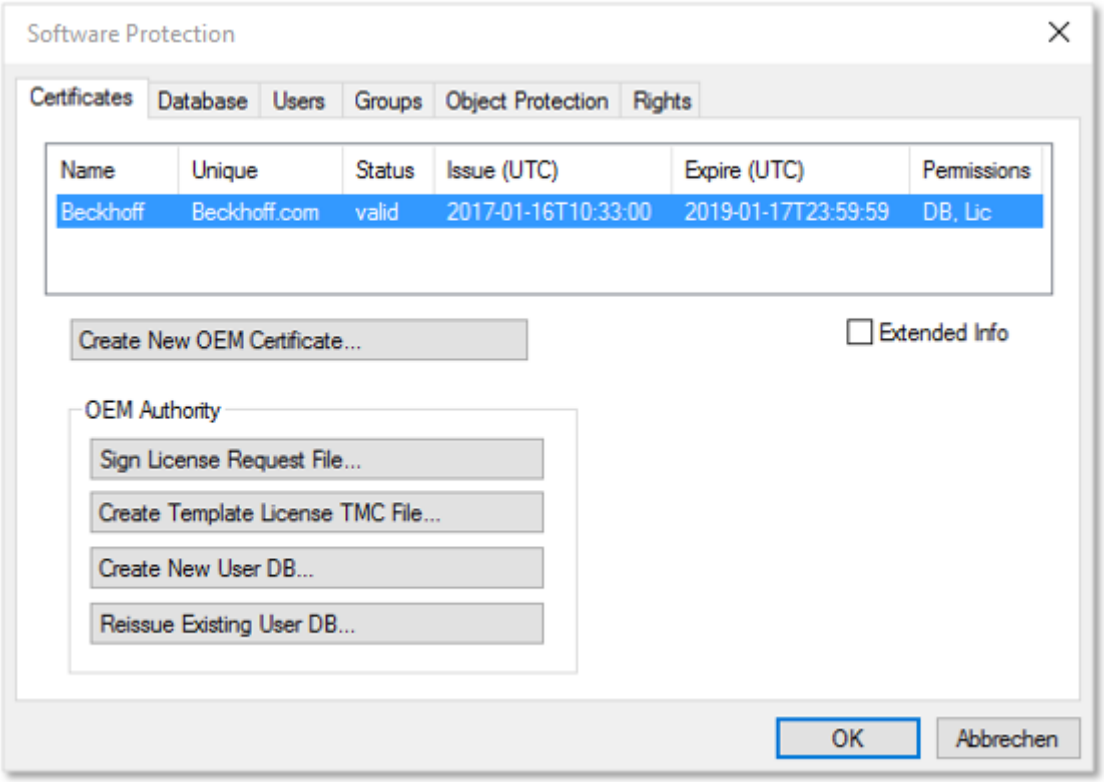
2.4 软件保护配置器

您可以使用软件保护配置器对一般的软件保护功能进行配置。

如需启动**软件保护**配置器，请选择 TwinCAT 菜单下的 Software Protection (**软件保护**)命令，或点击 TwinCAT XAE Software Protection (TwinCAT XAE **软件保护**)工具栏中的相关按钮。如需将工具栏添加到用户界面，可在 View (**查看**) > Toolbars (**工具栏**) 菜单中激活。



配置器随即打开，可在此对应用软件保护进行配置。



下列章节中包含有关配置的提示信息：

- TwinCAT OEM 证书 [▶ 17]
- 用户数据库 [▶ 31]
- 设置 OEM 应用软件的基本保护 [▶ 70]

3 快速入门

3.1 源代码访问控制

从 Build 4024 版本开始，TwinCAT 3 提供了对 PLC 源代码进行加密的选项，并通过权限管理来控制对源代码的访问。核心要素是一个用户数据库（User DB），创建时包含了 OEM 证书（作为验证基础）。

注意：仅在创建用户数据库时需要 OEM 证书，而在使用或修改时则不需要。

系统要求

- TwinCAT 3 OEM 证书 TC0007（加密版本 1 或 2）。
- 操作系统：至少为 Windows 7（也可以是嵌入式版本）。
- TwinCAT 版本：至少为 TwinCAT 3.1 Build 4024

只有使用最新版本的 TwinCAT 3，才会获得可靠的保护。

为确保获得可靠的保护（例如安全加密），请始终使用最新版本的TwinCAT 3。这可以提供最高的安全性。

至少应使用 TwinCAT 3.1 Build 4024.x。
鉴于安全因素，请勿使用旧版本！

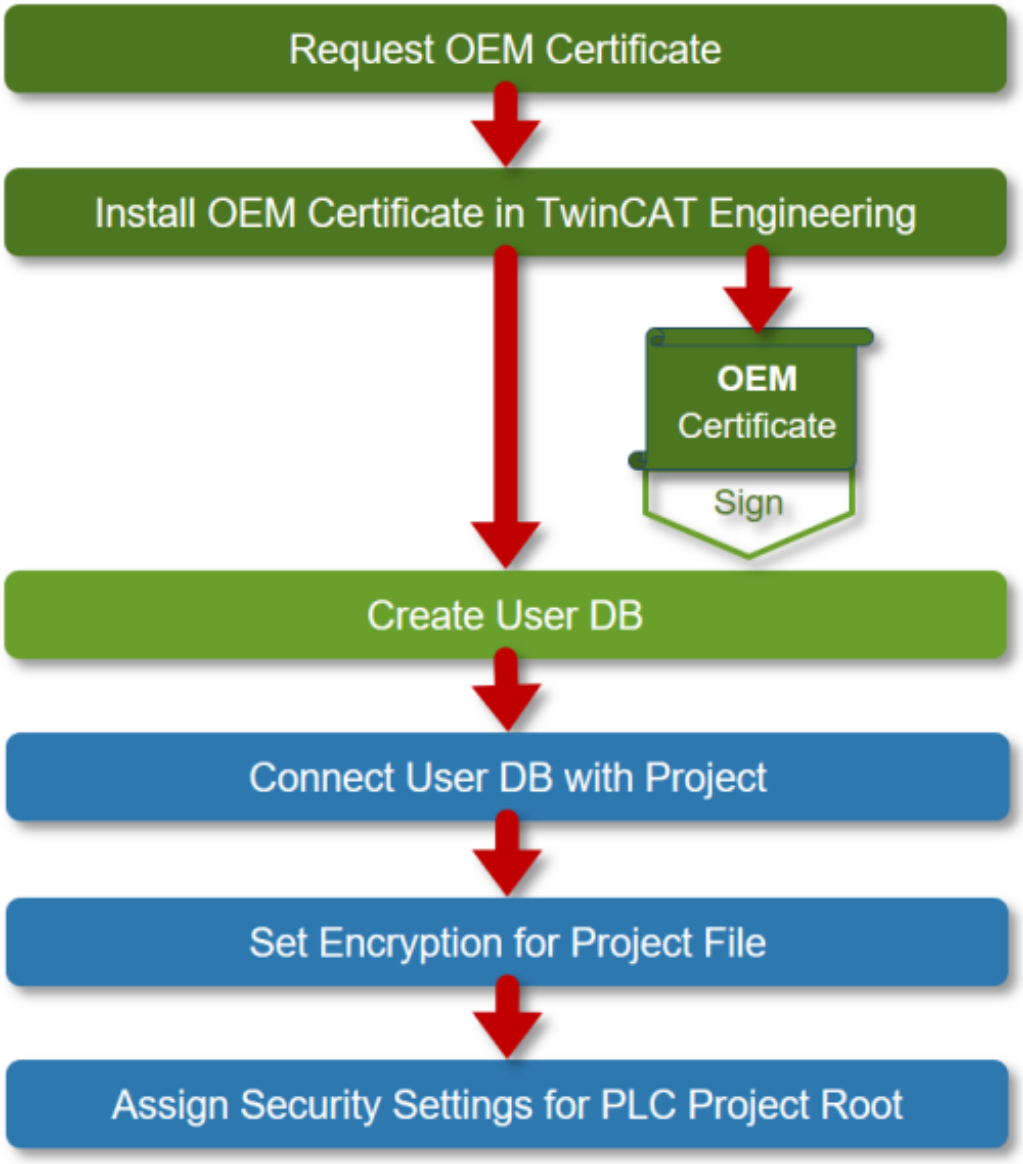
一般注意事项

- 请遵守有关 OEM 证书的一般信息。
- 只有在创建用户数据库时需要使用一次 OEM 证书。
- 修改用户数据库时，只需要用户数据库管理员的签名（不使用 OEM 证书）。
- 对于用户数据库管理员来说，拥有一个高强度密码至关重要。否则，用户数据库很容易被攻击。
- 用户数据库的有效性与 OEM 证书的有效期无关。因此，即使在 OEM 证书有效期结束后，用户数据库仍然有效，并且也可以在此后进行修改。
- 关于以后的证书延期（2 年后）说明，可以在这此查阅：OEM 证书延期 [▶ 29]。
- **重要提示：**请将 OEM 证书和用户数据库管理员的密码妥善存放在安全之处。如果密码丢失，倍福则无法恢复密码！
- 在目标系统上不需要 OEM 证书，因此出于安全原因，不应存储在目标系统上。

程序

以下程序说明了最简单的示例：

- 有一个用户（“管理员”）对项目有完整的访问权限
- 所有其他人（“访客”）都不允许查看或修改该项目。
- 管理员通过安全密码来验证自己的身份。



文档链接

1. 申请（订购）OEM 证书 [▶ 26]
2. 安装 OEM 证书 [▶ 27]
3. 创建用户数据库 [▶ 31]
   对于最简单的标准示例，只需要定义管理员的名字及其密码，在用户数据库中不需要进一步的设置（例如：不创建其他用户）。
4. 将用户数据库链接到一个项目 [▶ 63]
5. 设置项目文件的加密方式 [▶ 71]
6. 设置 PLC 项目根的访问权限 [▶ 64]

3.2 OEM 授权：防止未授权使用软件功能的保护措施

使用 TwinCAT 3 授权技术，可通过绑定硬件（倍福 IPC 或 TwinCAT 加密狗）来保护 PLC 应用不被未经授权使用/克隆。通过同样的授权技术，也可为终端客户激活应用程序的其他功能。

系统要求

- TwinCAT 3 OEM 证书
  （仅适用于**创建**授权类型和**签名**授权文件，不适用于**使用** OEM 授权。）

- 操作系统：至少为 Windows 7（也可以是嵌入式版本）
  （不支持 Windows CE / Windows Embedded Compact！）。
- 倍福 IPC 或 TwinCAT 3 授权加密狗
- TwinCAT 版本：至少为 TwinCAT 3.1 Build 4022
- TC3 PLC Lib Tc2_Utilities v3.3.24（或更高）。

注意：使用 OEM 授权时，不需要用户数据库。

只有使用倍福 IPC 或 TwinCAT 授权加密狗，才能获得可靠的保护

为了获得安全保护，请务必使用倍福 IPC 或 TwinCAT 3 授权加密狗。在没有 TwinCAT 3 授权加密狗的非倍福计算机上使用 OEM 授权是不安全的，且不被支持！

只有使用最新版本的 TwinCAT 3，才会获得可靠的保护。

为确保获得可靠的保护（例如安全加密），请始终使用最新版本的TwinCAT 3。这可以提供最高的安全性。

至少应使用 TwinCAT 3.1 Build 4024.x。
鉴于安全因素，请勿使用旧版本！

一般注意事项

使用 OEM 授权时，请确保启动项目已加密！

请记住，通过二进制代码的 FB_CheckLicense [▶ 85] 查询的授权码 [▶ 79]很容易被找到，并可通过十六进制编辑器轻松地进行控制。因此，请确保加密启动项目 [▶ 72]（最安全），或尽可能地在源代码中隐藏查询到的授权码。

- 应用程序授权无需用户数据库。
- 授权由 TwinCAT 3 runtime (XAR) 进行验证。因此，必须在 IPC 上安装 TwinCAT 3 runtime。
- 应用程序授权的有效期与 OEM 证书的有效期无关。因此，即使 OEM 证书已失效，应用程序授权仍然有效。
- 如需使用 OEM 应用程序授权，必需使用 TwinCAT 3 加密狗或倍福 IPC。
- 出于安全考虑，对平台级别 >= 90 的 IPC (非倍福 IPC)，必须使用 TwinCAT-3 加密狗作为“授权设备”！

典型应用

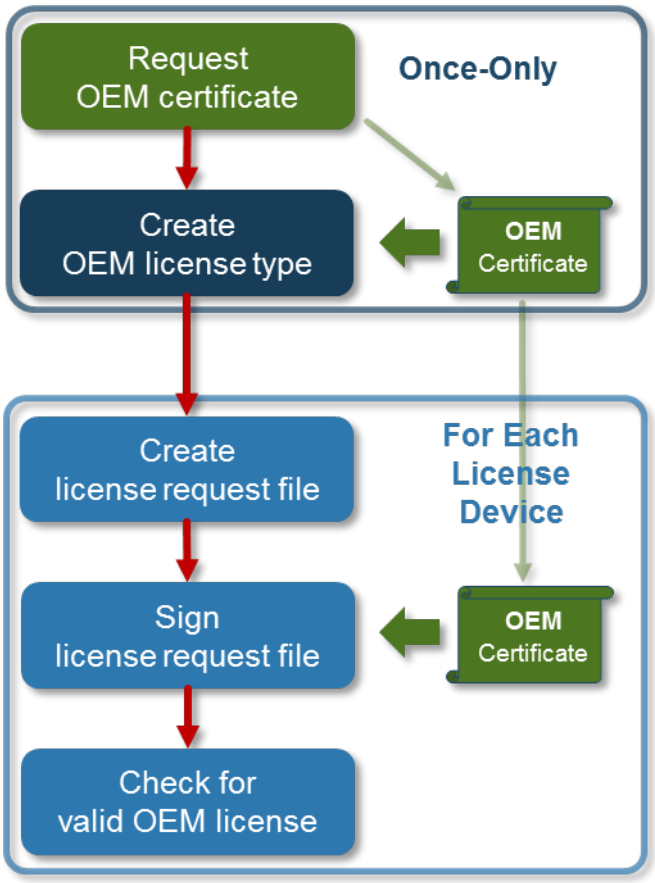
- 通过绑定硬件 (TwinCAT 3 加密狗或倍福 IPC)，防止应用程序被克隆。
- 应用程序的其他附加功能将由关联授权激活。

步骤

为了生成应用程序授权，首先必须对 TwinCAT 3 进行配置。为此需要一个小工具，该工具不在标准供货范围内。

有关 TwinCAT 3生成应用程序授权的准备工作，详见 TwinCAT 3的准备工作 [▶ 79]。

授权过程原理见下图：



申请 OEM 证书

授权的基础是由倍福签名的 OEM 证书，凭此证书发放授权（通过签名授权申请文件）。

如何申请和安装该证书，详见 创建“OEM 证书申请文件” [▶ 20] 章节。

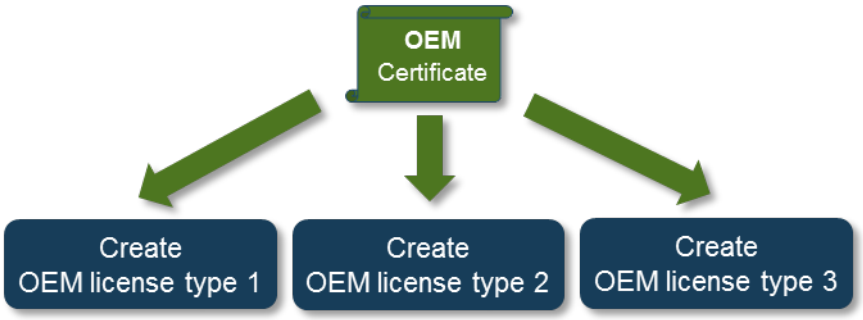
请确保为您的 OEM 证书使用高强度的密码！

创建 OEM 授权类型

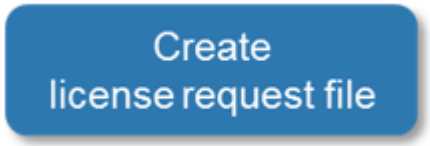
借助 OEM 证书的数据 (OEM GUID)，可生成授权类型的说明文件。该授权说明文件是创建“授权申请文件”的基础（见下一步）。

有关生成授权说明文件的过程，详见 创建 OEM 应用授权说明文件 [▶ 79]。

一个 OEM 证书，可生成任意数量的授权说明文件：



创建授权申请文件



现在可以生成指定“授权设备”的“授权申请文件”了 (TwinCAT 3 加密狗或倍福 IPC)。

有关生成授权申请文件的过程，详见 创建 OEM 应用授权申请文件 [▶ 82]。

出于安全考虑，对平台级别 >= 90 的非倍福 IPC，其应用程序授权必须使用 TwinCAT3 加密狗！

签署授权申请文件

生成的“授权申请文件”必须用 OEM 证书签名，从而成为“授权响应文件”。该文件为实际的授权文件，与创建“授权申请文件”时指定的设备绑定。

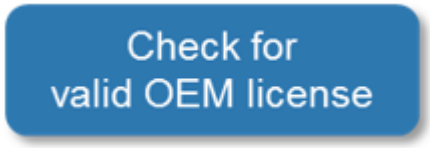
使用 OEM 证书签署“授权申请文件”的步骤，可参见通过 TwinCAT 编程环境手动创建 [▶ 83]。

随后，生成的授权只有在“授权设备” (TwinCAT 3 加密狗或倍福 IPC) 上才可用 (参见导入OEM 应用授权响应文件 [▶ 84])。

TwinCAT 3 Build 4022.16 及以上版本包含 TC3 PLC Lib Tc2_Utilities 3.3.24，提供各种授权处理功能块。其中一些功能块可将授权文件直接存储在 TwinCAT 3 加密狗的 PLC 应用中，或从后者下载。(参见 TC3 PLC Lib Tc2 Utilities 的手册)

您可以下载所需的 TC3 PLC Lib Tc2_Utilities：https://infosys.beckhoff.com/content/1033/tc3_security_management/Resources/zip/5299845387.zip

检查有效的 OEM 授权



在启动 (及运行) 时，TwinCAT 3 runtime 将会检查应用程序授权是否有效。您可以使用 PLC 功能块 FB_CheckLicense 查询检查结果 (参见查询 PLC 应用的 OEM 应用授权 [▶ 85])。

您可以在 PLC 应用中，按要求对授权验证检查结果作出反馈，从而对应用授权存在与否的反馈进行控制。

4 TwinCAT OEM 证书

如果要使用应用软件保护功能，必须有倍福签名的 TwinCAT OEM 证书。

在 TwinCAT Build 4024 中，TwinCAT OEM 证书 TC0008 版本还可用于签名以 TwinCAT 3 在 C++ 中创建的 TwinCAT *.tmx 文件。

与 Build 4022 相比，TwinCAT 3.1 Build 4024 的推出，引入了几项与 TwinCAT OEM 证书相关的新功能：

- 为内部证书数据更新到一个更新的加密版本
- 引入了扩展的证书版本 TC0008，在 TwinCAT 3 中创建的 C++ TwinCAT 驱动程序软件也可以用其进行签名
- 由于是在 Windows 环境下使用，因此该证书版本需要对申请人数据进行安全验证。
- 为此，申请 TwinCAT OEM 证书的过程已被修改。**所有的 OEM 证书，必须**正规**订购**，目的是为了验证地址和联系信息。（但发放 TwinCAT OEM 证书仍然免费）。
- TwinCAT OEM 证书扩展验证（TC0008）只发放给现有倍福客户。

TwinCAT OEM 证书订单号

TC0007：TwinCAT OEM 证书标准（TwinCAT 软件保护）。

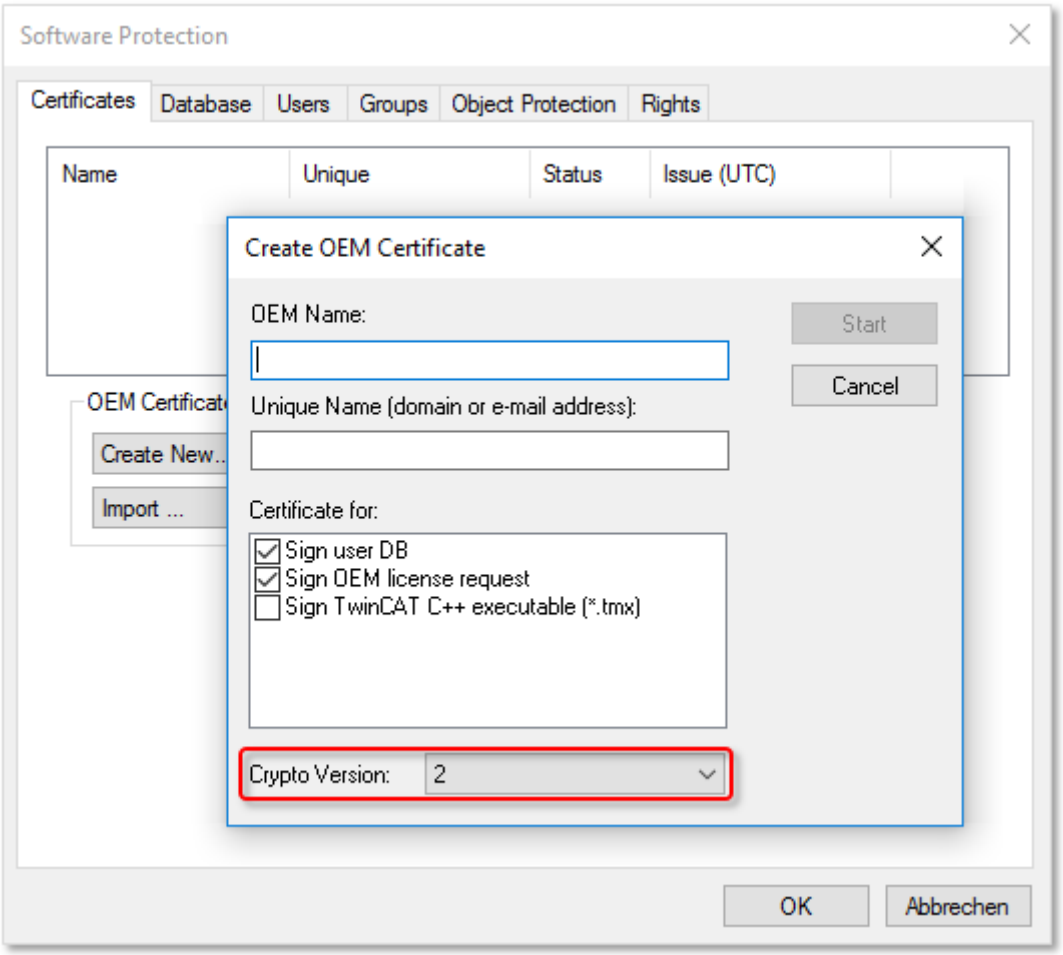
TC0008：TwinCAT OEM 证书扩展验证（与 TC0007 一样，还可以为 TwinCAT 3 以 C++ 创建的可执行文件进行签名。）

仅对 TwinCAT 3.1 Build 4024.0 有效：创建一个用户数据库需要加密版本 1

在 TwinCAT Build**4024.0** 版本中，用于 TwinCAT 软件保护的用户数据库 [▶ 31]只能用带有加密版本 1 的 OEM 证书来创建！

请注意：

- **TC0008** 包括 TC0007 的所有功能。
- 标准证书版本 **TC0007** 可以选择与 TwinCAT 3.1 Build 4022 或 4024 的加密版本一起发放。
- 具有扩展验证功能的证书版本 **TC0008** 只能在 TwinCAT 3.1 Build**4024** 的更新加密版本中发放。
- 证书的加密版本是由用户在创建“OEM 证书请求文件”时 [▶ 20]定义的（而不是在下订单时！）。



OEM 证书的兼容性：Build 4022 <-> Build 4024：

- Build 4022 的加密版本（=1）（例如，使用 Build 4022 创建的现有 OEM 证书或用其创建的用户数据库或 OEM 应用授权）也可用于 4024（反之，其只适用于加密版本 1！）。
- 带有 Build **4024** 加密版本的 TwinCAT OEM 证书（仅限标准）**1**（或用其生成的用户数据库或 OEM 应用授权）可用于 TwinCAT 3.1 Build**4022**。（->Build 4022 可以解密加密版本 1 的证书数据）
- 具有 Build **4024** 加密版本的 TwinCAT OEM 证书 **2**（或用其生成的用户数据库或 OEM 应用授权）**不能**用于 TwinCAT 3.1 Build **4022**！（->Build 4022 不能解密加密版本 2 的证书数据！）
- 不同加密版本的 TwinCAT OEM 证书可以在 TwinCAT 3.1 Build **4024** 中并行使用：一个具有 TwinCAT 3.1 Build 4022 加密版本的 OEM 证书用于保护用户软件，另一个具有 TwinCAT 3.1 Build 4024 加密版本的 OEM 证书用于签名 TwinCAT 驱动程序软件。

应用区的存储说明：保护 OEM 的应用软件

所有证书版本中包含的 OEM 密钥有助于使用保护 TwinCAT 3 应用软件的功能。

- 创建一个用户数据库（user DB），用于控制用户访问
- 创建 OEM 应用授权描述文件
  （分发 OEM 应用授权的基础）。
- 发放（签名）OEM 应用授权

OEM 标准证书（TC0007）只需要用于这三个目的。

OEM 证书 TC0007 应存储在哪一台计算机上？

OEM 证书只应置于执行上述三项活动的计算机上。

不需要 OEM 证书 TC0007：

- 使用用户数据库时

- 程序顺序
- 发放（签署）OEM 应用授权

出于安全考虑，该证书不应交付给控制计算机或随机安装在装有 TwinCAT Engineering 的计算机上。

使用 OEM 授权时，只需要使用 OEM 证书一次来**发放**授权（因为该证书用来签名授权文件）。

应用区的存储说明：签名 TwinCAT 驱动程序软件

包含在证书版本 TC0008（TwinCAT OEM 证书扩展验证）中的 OEM 密钥可另外用于签名使用 TwinCAT 3 在 C++ 中创建的 TwinCAT 驱动程序软件。

如果仅将 TC0008 用于此目的，则以下情况适用：

OEM 证书 TC0008 应存储在哪一台计算机上？

OEM 证书仅应置于以 TwinCAT 3 在 C++ 中创建 TwinCAT 驱动程序软件所签名的计算机上。

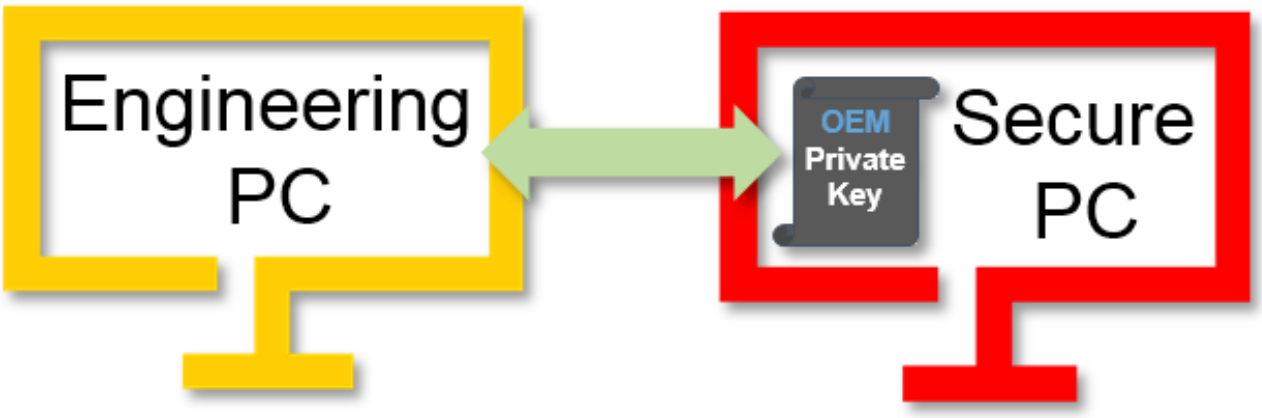
如果也使用 TC0008 进行 TwinCAT 软件保护，那么对于可能/应该存储该证书的计算机的相关说明也适用。

运行用该证书签名的 TwinCAT 驱动程序软件时，不需要 OEM 证书 TC0008。

该证书不应交付给控制计算机或随机安装在装有 TwinCAT Engineering 的计算机上。

使用安全的个人计算机

在需要处理 OEM 证书私钥密码的活动时，请使用安全的个人计算机，防止密码被嗅探。



TwinCAT OEM 证书的有效性

出于安全考虑，OEM 证书的有效期限定为两年。

OEM 可以在两年期满之前（或之后）申请证书延期，以便能够不间断继续工作。（请参阅 OEM 证书延期 [▶ 29]）

如果证书期满会发生什么事？

如果 OEM 证书无效（期满），以下功能**无法**继续使用：

- 创建用户数据库
- 创建 OEM 应用授权描述文件
- 发放（签名）OEM 应用授权
- 用 OEM 证书签名 C++ 可执行文件（Build 4024）。

所有其他功能继续有效：

- 仍可执行程序。
- 已颁发的 OEM 授权仍然有效。
- 用 TC0008 签名的 C++ 可执行文件继续运行（Build 4024）。

- 用户数据库仍然有效，而且管理员可以继续修改/调整数据库。（但已经不能新建用户数据库）。

4.1 创建“OEM 证书申请文件”

TwinCAT OEM 证书只发放给现有的倍福客户。
请与您的倍福销售联系专员联系，以获得更多信息。

系统要求
- 至少为 TwinCAT 3.1 Build 4024
- 至少为 Windows 10 或 TwinCAT/BSD®（在目标系统上）

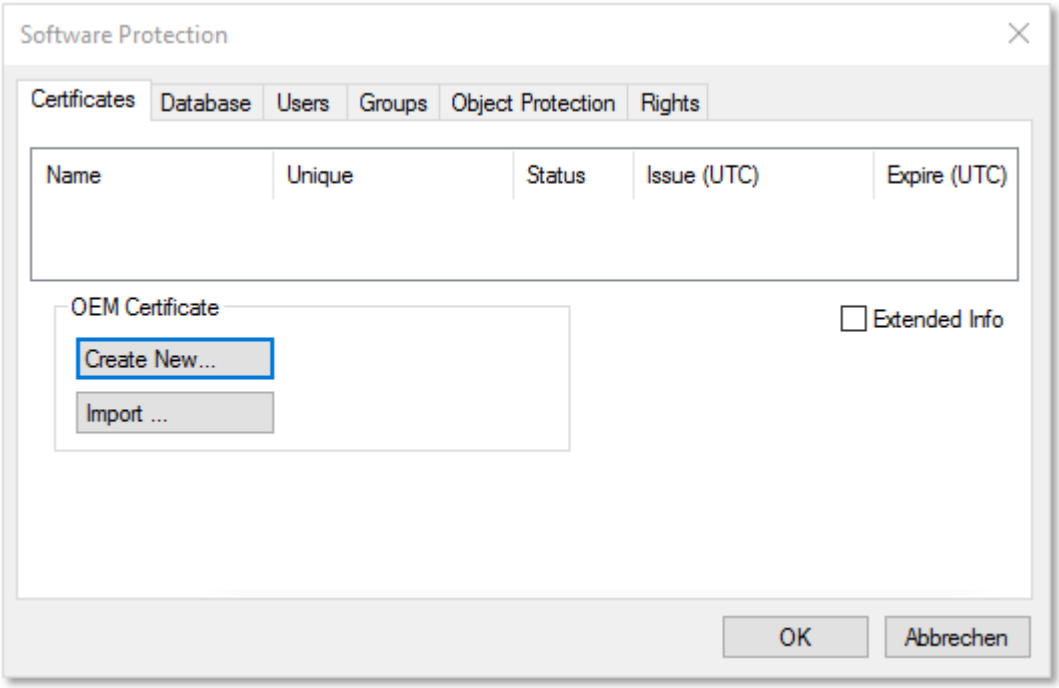
TwinCAT OEM 证书订单号

TC0007：TwinCAT OEM 证书标准（TwinCAT 软件保护）。

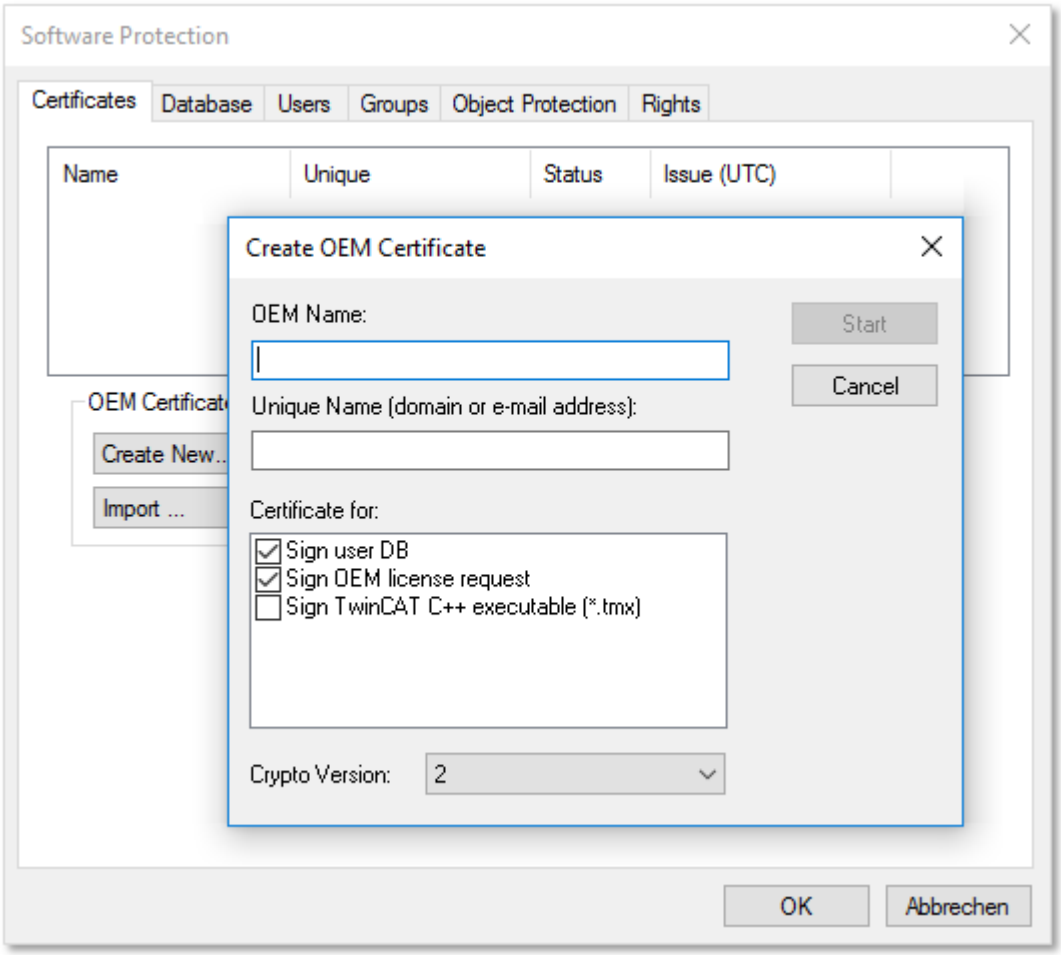
TC0008：TwinCAT OEM 证书扩展验证（与 TC0007 一样，还可以为 TwinCAT 3 以 C++ 创建的可执行文件进行签名。）

✓ 软件保护配置器 [▶ 10] 已被打开。

1. 选择**Certificates**（证书）选项卡。
2. 点击**Create New...**（新建...）。

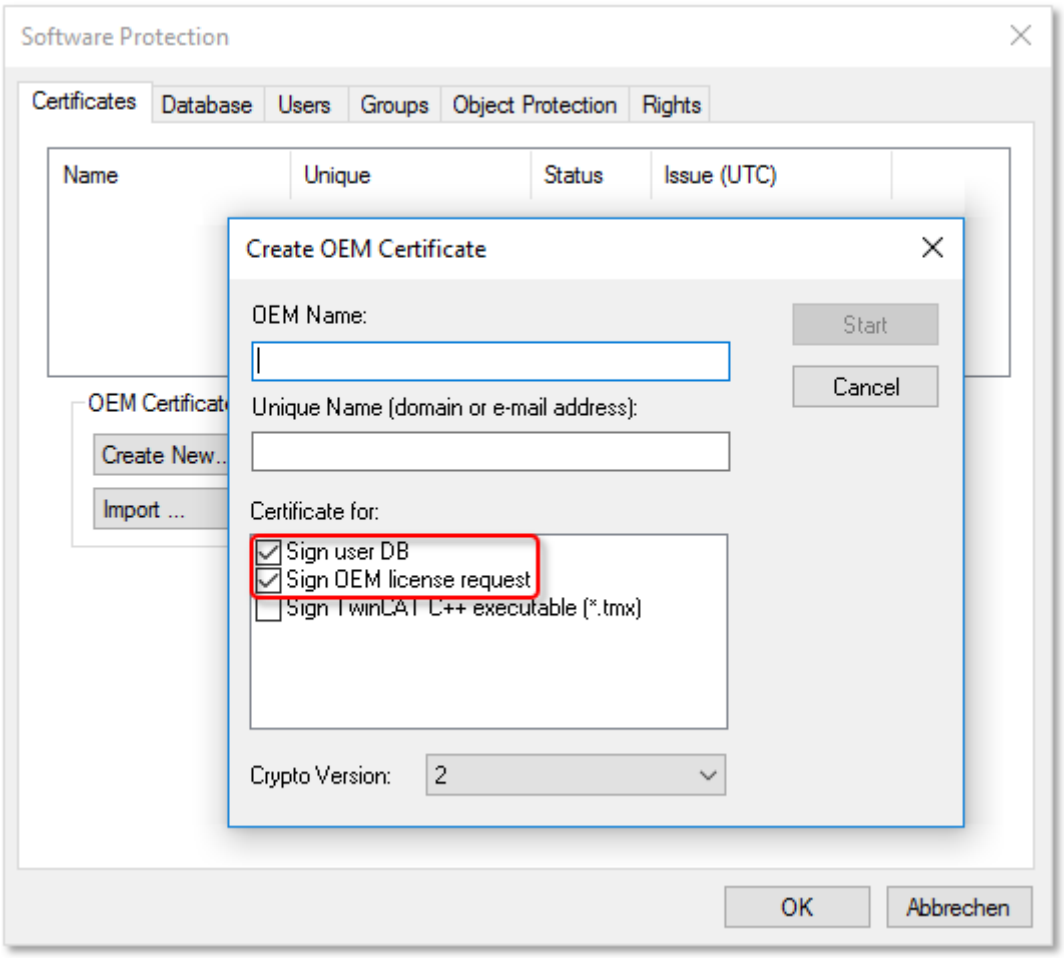


⇨ 出现**Create OEM Cerfificate**（创建 OEM 证书）输入窗口。

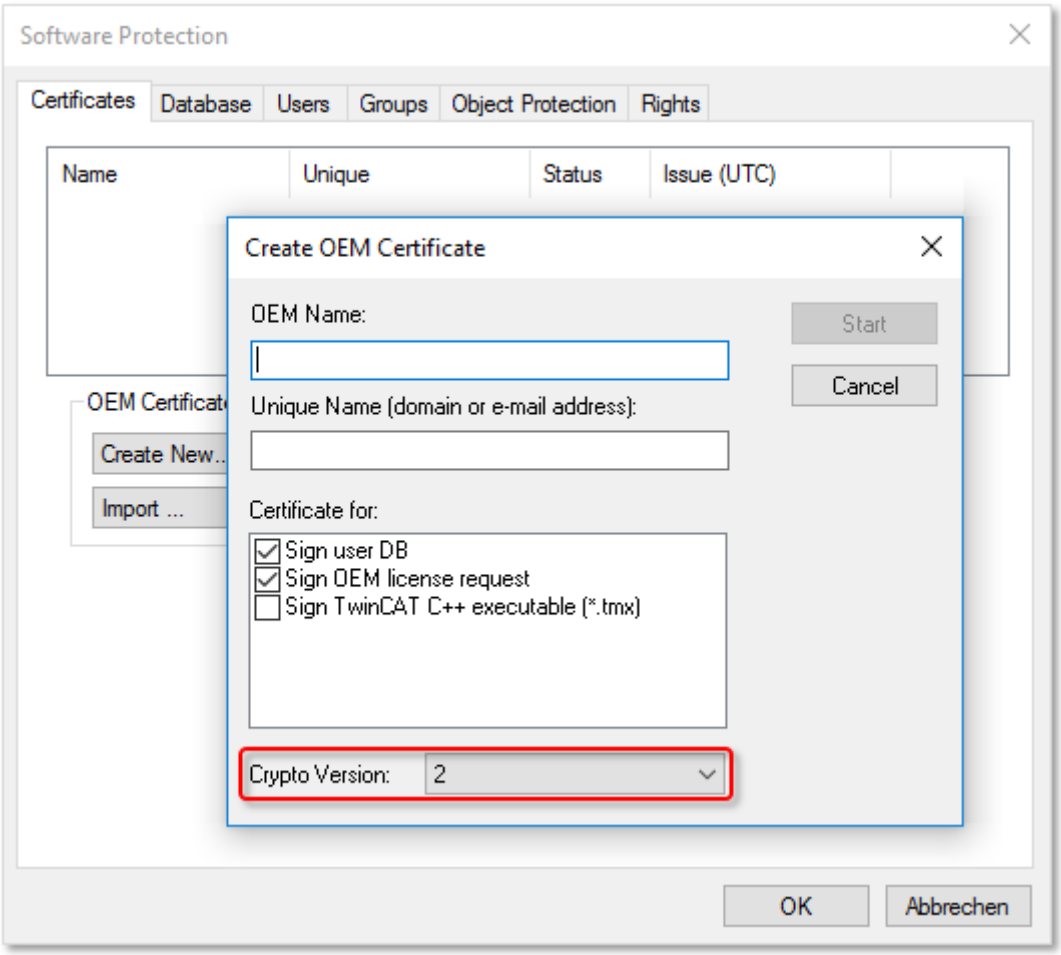


3. 输入“OEM 证书申请文件”所需数据：
   - 在 **OEM Name**（OEM 名称）文本框中输入贵公司名称。该名称必须明确提及贵公司或您的业务单位。
   - 输入一个**Unique Name**（唯一名称）。“OEM 唯一名称”必须是一个能够独一识别全世界的证书所有者的唯一名称，最好是贵公司网站的 URL 或您的电子邮件地址。电子邮件地址必须是公司的电子邮件地址，也就是说，必须能够明确将其分配给一家公司。

- 对于**标准证书**（TC0007），请确保在证书应用领域至多选中这两个复选框：



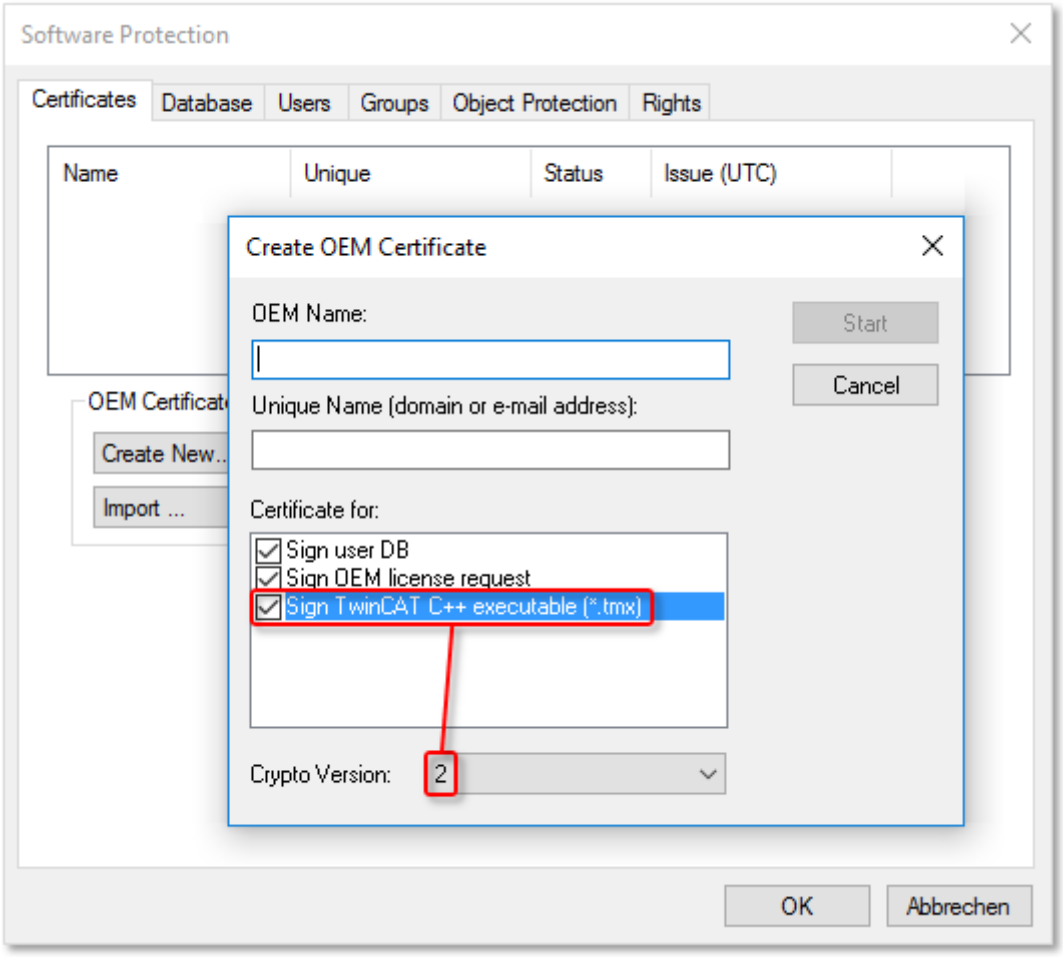
- 目前的加密版本（用于证书的加密内容）是“2”。如果希望在 TwinCAT 3.1 Build 4022.x 中使用该证书，则应仅选择较早的加密版本“1”。注意：加密版本“1”只能被选择用于标准证书（TC0007）。



仅对 TwinCAT 3.1 Build 4024.0 有效：创建一个用户数据库需要加密版本 1

在 TwinCAT Build4024.0 版本中，用于 TwinCAT 软件保护的用户数据库 [▶ 31]只能用带有加密版本 1 的 OEM 证书来创建！

- 复选框“**Sign TwinCAT C++ executables**（*.tmx）”只能用于申请具有“**Extended Validation**”（TC0008）的证书，该证书可用于签名以 TwinCAT 3（包括 Matlab/Simulink）生成的 C++ 可 执行文件。该证书版本需要在证书订购期间对您的联系资料进行**更复杂的验证**（因此需要更多时间），因此只有在您确实需要这一选项时，才应选择：



- 具有“扩展验证”（TC0008）的证书始终需要加密版本“2”。（请注意：该证书版本不能用于 TwinCAT 3 Build 4022.x！）

4. 输入数据之后，点击**Start**（开始），并选择一个目录来保存文件。**重要提示：**建议使用默认目录 “c:\twincat\3.1\customconfig\certificates”。新创建的文件保存在该目录下，以便能够在后续步骤中读取该文件的文件指纹。

   ⇨ 出现一个用来为 OEM 私钥选择密码的对话框。

5. 设置一个 OEM 私钥的密码。

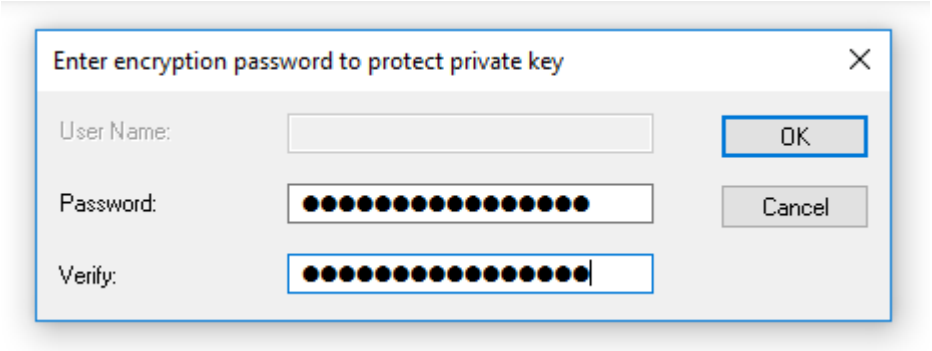
重要提示：请注意密码安全！

请务必为您的 OEM 证书设置强密码！
采用适当措施保护密码，以免被恶意盗用！

密码丢失后无法恢复

倍福无法恢复或重置您的密码。如果忘记或丢失了 OEM 证书的密码，则无法再使用证书，必须申请一个新的 OEM 证书。

6. 再次输入密码确认，然后点击 **OK**，关闭对话框。



⇨ 文件被保存。

以这种方式生成的“OEM 证书请求文件“现在必须由倍福证书部门签名，才能生效。该程序的说明详见“申请 OEM 证书 [▶ 26]” 一章。

4.2 确定 OEM 证书文件的文件指纹

需要这项功能来申请 **TwinCAT OEM 证书扩展验证**（TC0008）。

系统要求

这项功能需要 TwinCAT 3.1 build 4024 以上版本。

“OEM 证书申请文件”说明

“OEM 证书申请文件”经过 Beckhof f签名之后，即成为 TwinCAT OEM 证书。除此签名之外，这些文件没有任何区别。因此，在以下章节中，“TwinCAT OEM 证书文件”这一术语用于两个文件版本。

通过 TwinCAT 3 Engineering 读取 OEM 证书文件的“文件指纹”。

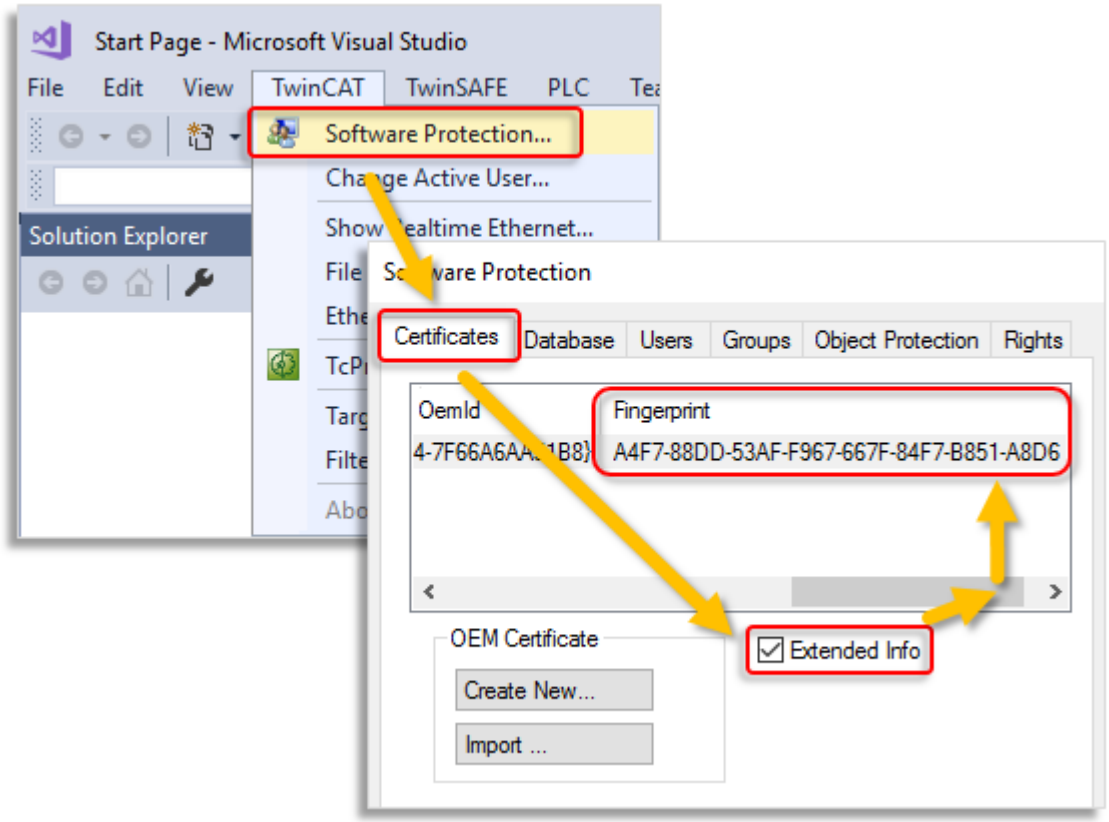
为了能使用这个功能，OEM 证书文件必须存放在以下文件夹中：“c:\twincat\3.1\customconfig\certificates”。

注意事项：

- 如果您已经有证书并想更新证书，那么证书需要被保存在这个目录下。
- 如果在创建“OEM 证书请求文件“时没有改变建议的文件夹，该文件则已在该文件夹中。

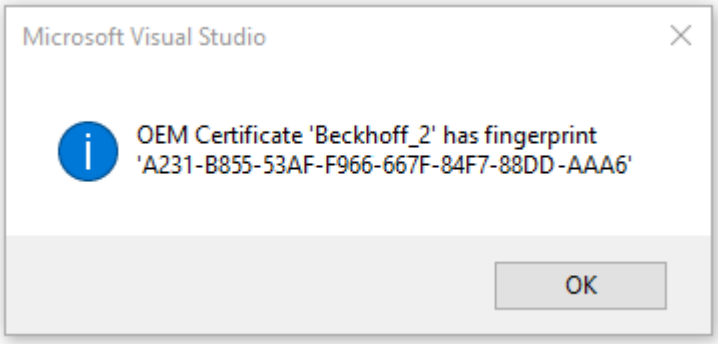
程序：

1. 调用 TwinCAT 3 软件保护配置器



2. 选择“证书“选项卡
3. 勾选“扩展信息“框
4. 在窗口中向右滚动，直至看到指纹列

注意：作为第 3+4 项的替代方法，只要双击证书行即可。然后，文件指纹会显示在一个弹出窗口中：



注意：可使用快捷键 Ctrl + C，将指纹数据从信息窗口复制到 Windows 剪贴板。

4.3 申请 OEM 证书

请参考前几章的信息，如果适用，请参考关于 OEM 证书延期的信息：

TwinCAT OEM 证书 [▶ 17]

创建“OEM 证书申请文件” [▶ 20]

OEM 证书延期 [▶ 29]

TwinCAT OEM 证书订购流程

申请 TwinCAT OEM 证书时，需要正式的订单。请与您的倍福销售联系专员联系。

注意事项：

- TwinCAT OEM 证书的发放和延期均为免费。
- TwinCAT OEM 证书只发放给现有倍福客户。
- 对于新的 OEM 证书，在 TwinCAT Engineering 中创建 创建“OEM 证书申请文件” [▶ 20]。
- 如果证书已延期，只需重新签名现有 OEM 证书文件，并在接下来 2 年内有效。（在这种情况下，无需创建“OEM 证书请求文件”）。
- 倍福一旦签名，“OEM 证书申请文件“即成为 TwinCAT OEM 证书。除此签名之外，这些文件没有任何区别。
- 在下文中，为方便起见，“OEM 证书文件”一词代表这两个文件版本。
- 由于 TwinCAT OEM 证书是数字身份证，因此有必要验证查询者的联系资料。
- 这两个 OEM 证书版本代表着不同的安全级别，所以验证过程有一定的差异。
- 只有在您确实需要时，才应该订购 TC0008（TwinCAT OEM 证书扩展验证）（对 TwinCAT 3 C++ 可执行文件进行签名）。

TwinCAT OEM 证书订单号

TC0007：TwinCAT OEM 证书标准（TwinCAT 软件保护）。

TC0008：TwinCAT OEM 证书扩展验证（与 TC0007 一样，还可以为 TwinCAT 3 以 C++ 创建的可执行文件进行签名。）

订购和验证流程概述

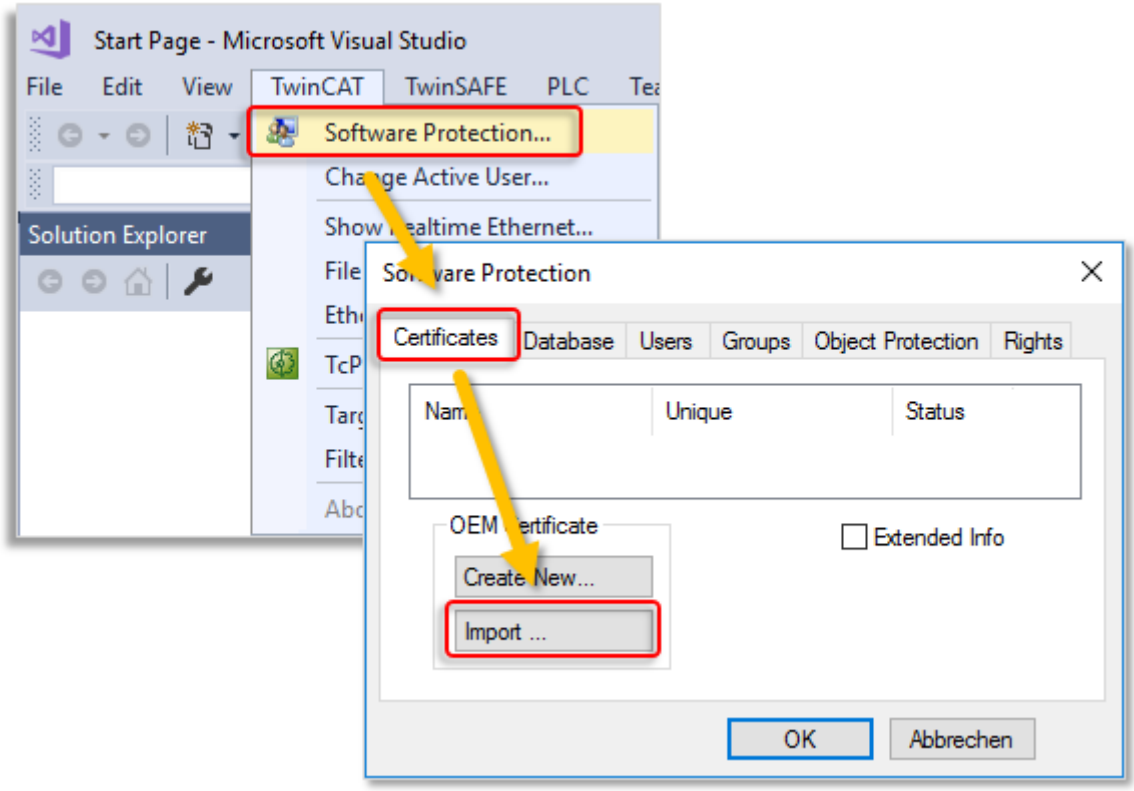
您的电子邮件地址必须是公司电子邮件账户（不允许使用 GMail 或类似的免费电子邮件），并符合询问者的公司名称。

1. 请联系您的倍福销售联系专员，并指明申请 TwinCAT 3 OEM 证书。订购“TC0007“或“TC0008”。
2. 重要提示：作为询问者，请提供您的详细联系方式作为交付地址（=联系人姓名和电子邮件地址）和证书使用区域（公司名称、地址）。
3. 订单中提供的详细联系信息将会予以核实，倍福销售部会与您（交付地址中指定的询问者）联系。
4. 申请新 OEM 证书时，请在 TwinCAT 3 Engineering 中创建一个创建“OEM 证书申请文件” [▶ 20]。
5. 仅限 TC0008：使用 TwinCAT Engineering 确定 OEM 证书文件的“文件指纹”（请参阅 确定 OEM 证书文件的文件指纹 [▶ 25]）。请将此文件指纹告知倍福销售联系专员，作为您联系资料验证的一部分。传输文件指纹时，必须通过与发送 OEM 证书请求文件不同的通信渠道。
6. 现在将“OEM 证书文件“发送给倍福销售联系专员。
7. 在倍福总部签名证书文件后，您会通过电子邮件从您联系人那里收到该文件。

请注意，可能需要数天时间来验证您的联系信息并签发证书。

4.4 安装 OEM 证书

收到签名的证书后，请通过软件保护控制中心导入：



注意：仅 TwinCAT 3.1 build 4024 及以上版本提供该重要功能。

您也可以手动将文件保存在编程电脑的指定 *c:\twincat\\3.1\customconfig\certificates* 目录下。

重启 TwinCAT 3，证书将显示在软件保护配置器的 **Certificates（证书）** 选项卡中。

检查证书是否显示为“valid（有效）”。

应用区的存储说明：保护 OEM 的应用软件

所有证书版本中包含的 OEM 密钥有助于使用保护 TwinCAT 3 应用软件的功能。

- 创建一个用户数据库（user DB），用于控制用户访问
- 创建 OEM 应用授权描述文件
  （分发 OEM 应用授权的基础）。
- 发放（签名）OEM 应用授权

OEM 标准证书（TC0007）只需要用于这三个目的。

OEM 证书 TC0007 应存储在哪一台计算机上？

OEM 证书只应置于执行上述三项活动的计算机上。

不需要 OEM 证书 TC0007：

- 使用用户数据库时
- 程序顺序
- 发放（签署）OEM 应用授权

出于安全考虑，该证书不应交付给控制计算机或随机安装在装有 TwinCAT Engineering 的计算机上。

使用 OEM 授权时，只需要使用 OEM 证书一次来**发放**授权（因为该证书用来签名授权文件）。

应用区的存储说明：签名 TwinCAT 驱动程序软件

包含在证书版本 TC0008（TwinCAT OEM 证书扩展验证）中的 OEM 密钥可另外用于签名使用 TwinCAT 3 在 C++ 中创建的 TwinCAT 驱动程序软件。

如果仅将 TC0008 用于此目的，则以下情况适用：

OEM 证书 TC0008 应存储在哪一台计算机上？

OEM 证书仅应置于以 TwinCAT 3 在 C++ 中创建 TwinCAT 驱动程序软件所签名的计算机上。

如果也使用 TC0008 进行 TwinCAT 软件保护，那么对于可能/应该存储该证书的计算机的相关说明也适用。

运行用该证书签名的 TwinCAT 驱动程序软件时，不需要 OEM 证书 TC0008。

该证书不应交付给控制计算机或随机安装在装有 TwinCAT Engineering 的计算机上。

4.5 OEM 证书延期

延长 OEM 证书的过程与申请新证书相同。在这种情况下，也必须订购证书（证书延期的订单号与新证书申请的订单号相同）。

与新证书不同的是，您不需要生成一个新的 "OEM 证书申请文件"，而是将您现有的证书发送给 Beckhoff 证书部门进行更新。请在电子邮件中告知我们，您想要为证书办理延期，而不是申请新的证书。否则，会以申请新证书的标准来处理电子邮件内容。

将重新签发现有的证书，并在两年内有效。

由于该证书只获得一个新的签名，因此与原始版本完全兼容。

4.6 更新现有 OEM 证书？

很抱歉，现有 OEM 证书不能更新（新加密版本或不同应用领域）。在这种情况下，始终需要签发一个新 OEM 证书。但可以通过重新签名来延长 OEM 证书有效期。

对于使用现有或新 TwinCAT UserDBs [▶ 31]、OEM 授权描述文件 [▶ 79]或 OEM 应用授权 [▶ 83]的应用，新 OEM 证书会有什么影响？

TwinCAT 用户数据库

- 用例：要重新使用现有用户数据库，同时要使用一个新 OEM 证书。没问题：仍然可以使用和修改现有用户数据库，因为两种情况都不需要 OEM 证书。这也适用于从 Build 4022 到 B Builduild 4024 的转换（以及 4022的用户数据库）。
- 用例：现有用户数据库（用旧的 OEM 证书 1 创建）被新用户数据库（用新的 OEM 证书 2 创建）取代。只要考虑到下面所述对加密版本的要求，就不会有问题。然而，一旦使用新用户数据库 [▶ 63]，则必须与该项目进行链接。在文件层面的简单交换是不可能的，也就是说，被替换的用户数据库必须始终重新分配给项目，因为新用户数据库有不同的用户数据库密钥。

  注意：项目的所有安全设置均会丢失！
- 基于加密版本 2 的证书所创建的用户数据库不能在 Build 4022 下使用。（在用户数据库中加密的信息不能被 Build 4022 解密）。

TwinCAT OEM 应用授权

OEM 授权描述文件：一般来说，OEM 授权描述文件必须是用与签名 OEM 应用授权的同一证书来创建。（否则，授权描述文件中的 OEM 密钥将与应用程序授权中的 OEM 密钥不一致）。

这与 TwinCAT 版本或加密版本无关。

注释：

- 用加密版本 2 证书创建的 OEM 授权描述文件和 OEM 应用程序授权不能在 Build 4022 中使用。

- 但是，用加密版本 1 证书创建的 OEM 授权描述文件和 OEM 应用授权可以在 Build 4024 中使用。

5 用户数据库

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

项目打开时，无法切换用户

切换用户时，不能打开任何项目。

TwinCAT 3 Build 4024.8 新增功能：用户数据库扩展文件

从该版本开始，可使用“扩展文件”对用户数据库进行扩展。您可以在此处 [▶ 38]了解详细信息。

5.1 创建用户数据库

仅对 TwinCAT 3.1 Build 4024.0 有效：创建一个用户数据库需要加密版本 1

在 TwinCAT Build4024.0 版本中，用于 TwinCAT 软件保护的用户数据库 [▶ 31]只能用带有加密版本 1 的 OEM 证书来创建！

用户数据库保存目录

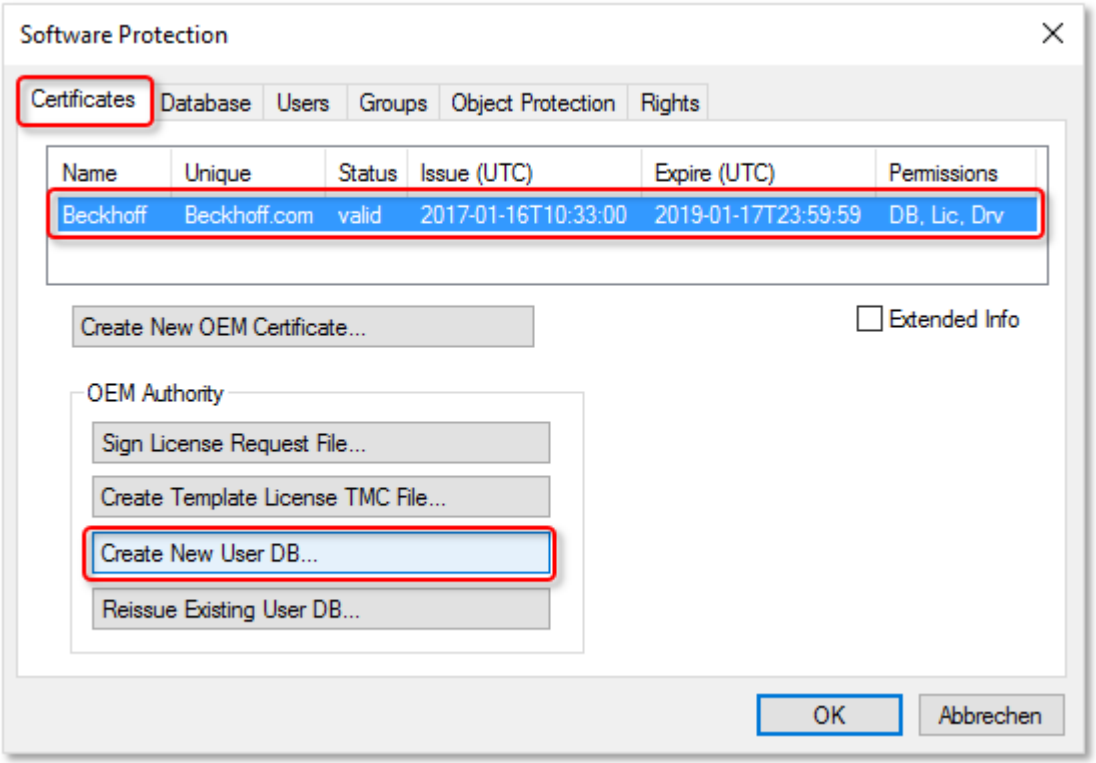
为了在 TwinCAT 3中使用，用户数据库必须保存在以下目录：C:\TwinCAT\3.1\CustomConfig\UserDBs

根据 TwinCAT 版本，有两种方法可创建用户数据库。

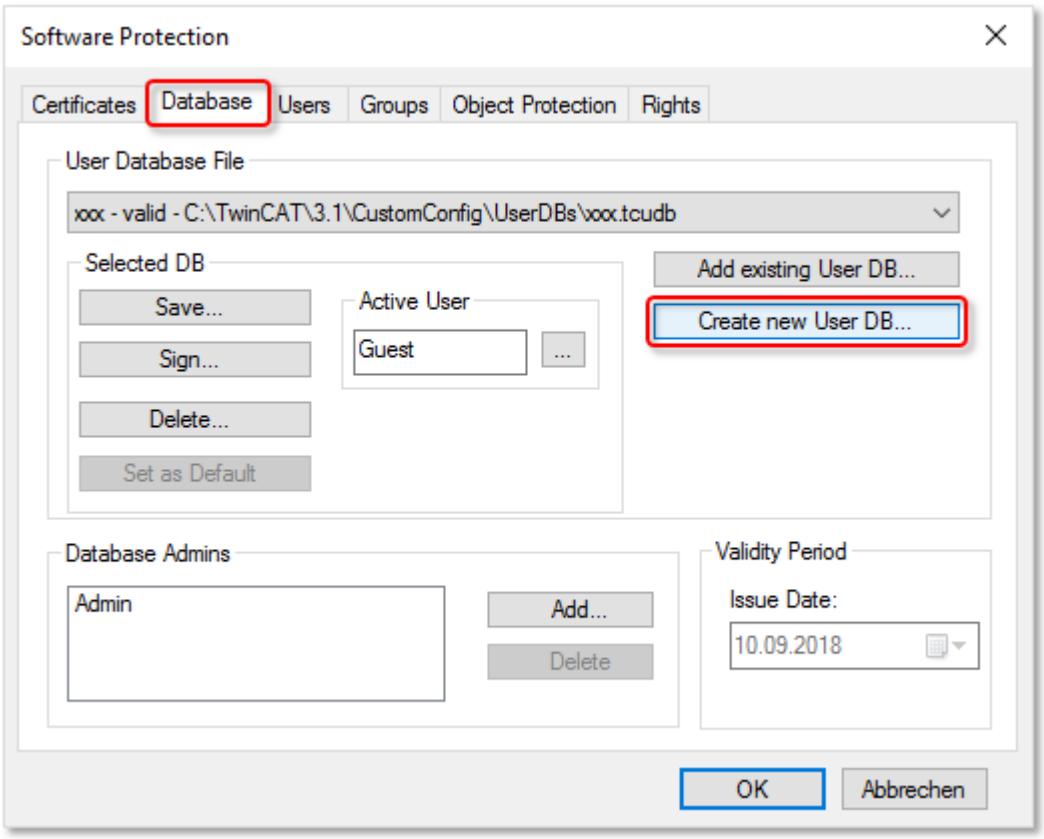
✓ 只有在没有项目打开时，才能创建或编辑用户数据库。关闭所有打开的项目。

✓ 打开软件保护配置器 [▶ 10]。

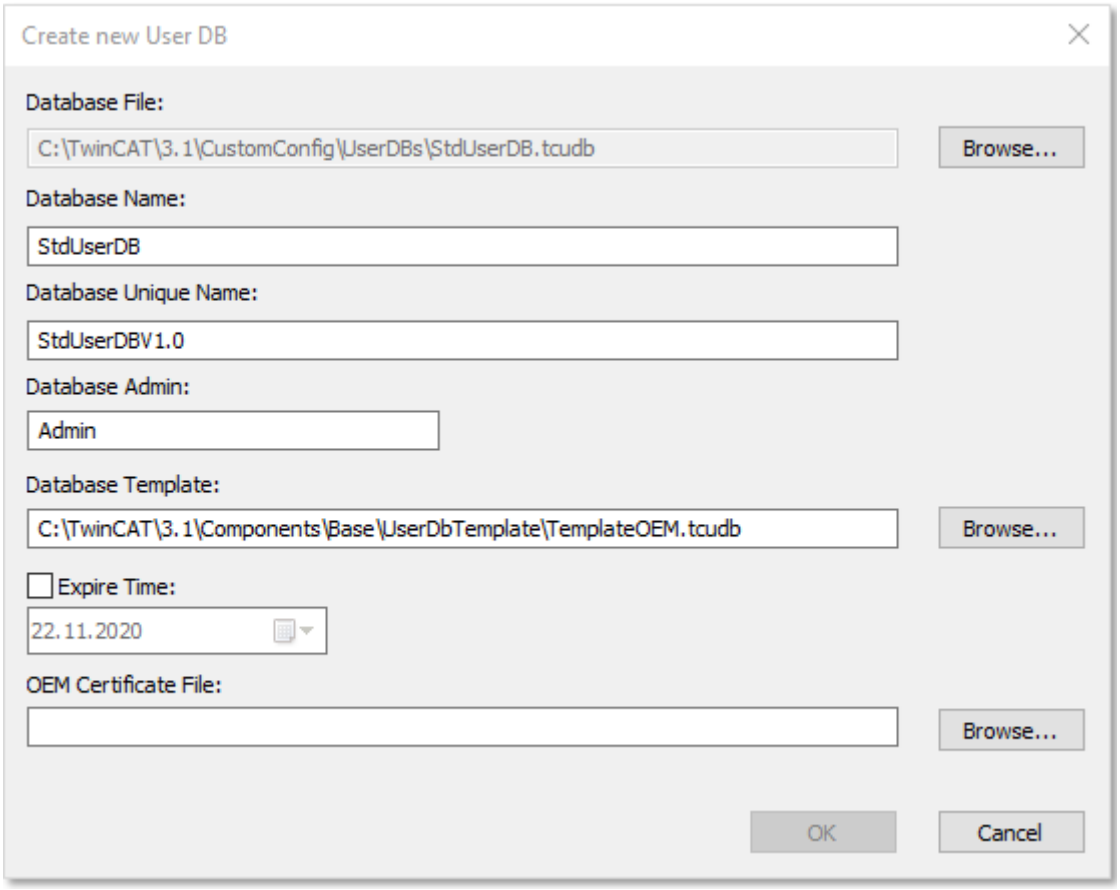
1. 如果 TwinCAT 低于 build 4022.25 版本，请打开 **Certificates（证书）** 选项卡，选择 OEM 证书，并点击 **Create New User DB...（创建新用户数据库...）**



2. 如果 TwinCAT 为 build 4022.25 及以上版本，**Create New User DB... (创建新用户数据库...)**按钮也出现在 **Database (数据库)** 选项卡上。直接在输入掩码中选择 OEM 证书。点击 **Create New User DB… (创建新用户数据库...)**



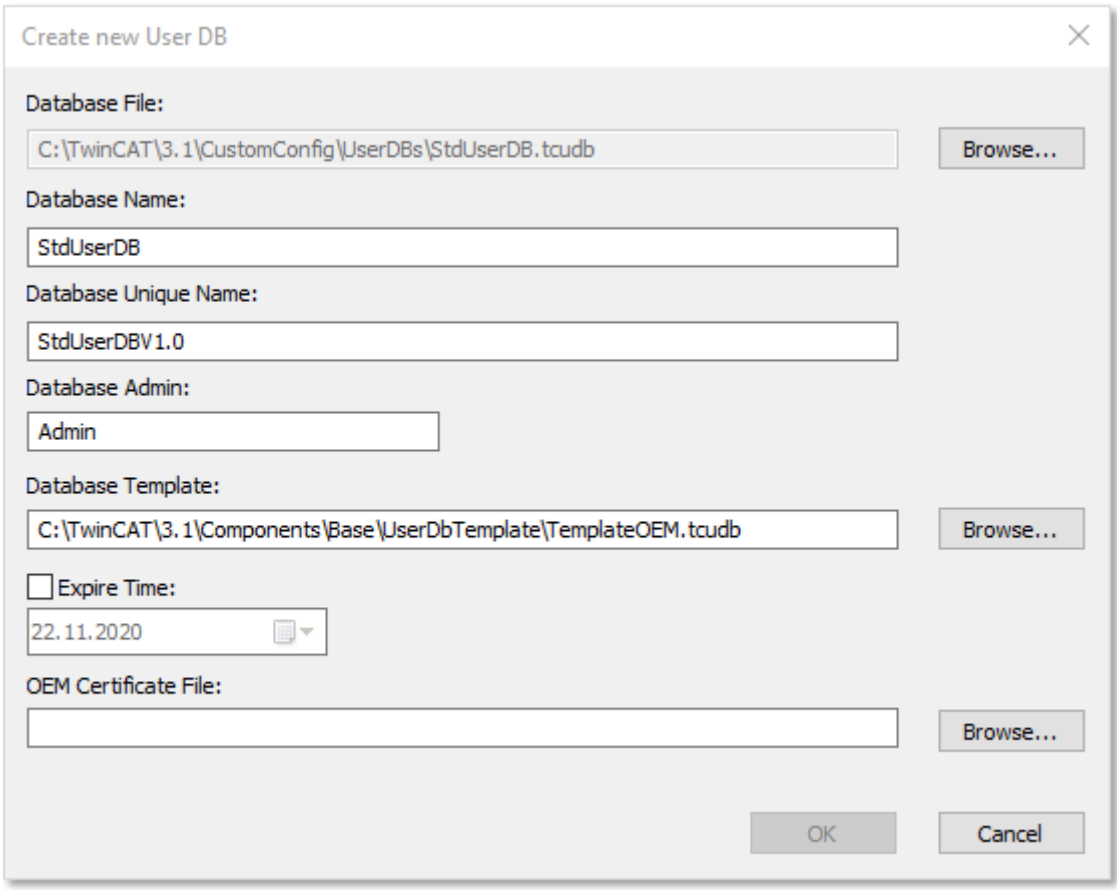
⇨ **Create new User DB (创建新用户数据库)** 对话框打开。



3. 输入数据库名称（**Database Name（数据库名称）**）。该名称用于在程序中显示选定的数据库。
4. 指定 **Database Unique Name（数据库唯一名称）**（例如，加上版本号），用于在组织内部准确识别数据库（版本）。
5. 输入数据库管理员名称。此处创建的 **Database Admin（数据库管理员）** 仅用于签署数据库，不能用于登录或对数据库进行修改。为了对数据库进行更改，至少必须有一个数据库用户是管理员组成员。
6. 定义新数据库的模板。
   为简便起见，你可以在 *TemplateOEM.tcudb* 模板的基础上进行。如果 TwinCAT 版本不包含该模板，可在此下载：https://infosys.beckhoff.com/content/1033/tc3_security_management/Resources/zip/5943612299.zip.

   如需选择其他模板，点击 **Database Template（数据库模板）** 框旁的 **Browse...（浏览）**，从资源管理器窗口中选择想要的文件。

   ⇨ 模板在 **Database Template（数据库模板）** 框中显示。



注意 **此外，还可以创建自己的数据库模板，例如基于原有的数据库创建模板。**

7. 创建的数据库必须先用有效的 OEM 证书签署。OEM 证书数据也用于生成用户数据库密钥，用于准确识别数据库。

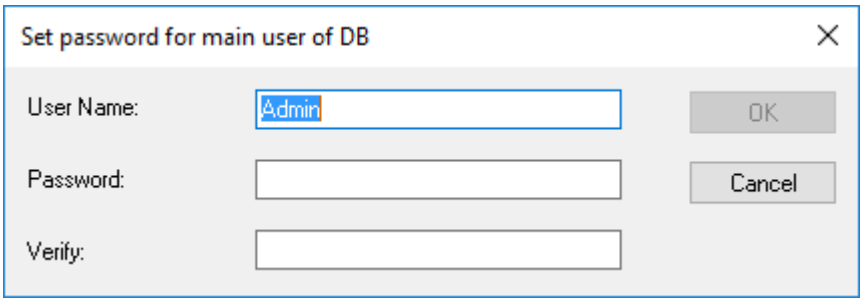
   如所需证书不在 **OEM Certificate File（OEM 证书文件）** 框中，可点击 **Browse...**

   （浏览） 选择 OEM 证书OEM 证书的默认目录为：*c:\twincat\3.1\customconfig\certificates*.

   ⇨ 证书在 **OEM Certificate File（OEM 证书文件）** 框中显示。
8. 点击 **OK（确认）**。

⇨ 此时将出现对话框，提示您设置数据库（签名）管理员密码。

9. 输入密码，并再次输入，以确认密码。请务必使用强密码，否则数据库容易被攻击！
10. 点击 **OK（确认）**。
11. 仅限 Build 4024：此时会提示您创建数据库的第二个（内容管理）管理员：

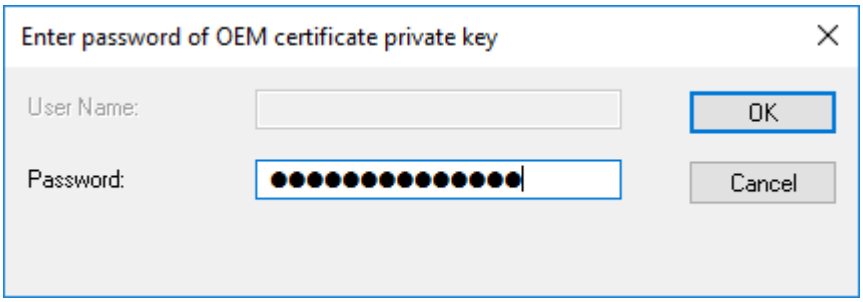


可以使用与签名管理员相同的用户名和密码。这样更便于对数据库进行管理。因此，建议将之前创建的签名管理员的用户名作为默认值。

当然，也可以将内容管理（内容管理员）和发布修改（签名管理员）的功能分开。

注意 **也可以在数据库创建后，再创建其他管理员或进行修改。**
注意 **如果只需要单一用户完成所有功能，不必再创建其他用户。例如，只是想对的项目进行加密，而不对访问权限进行其他区分这种情况。**

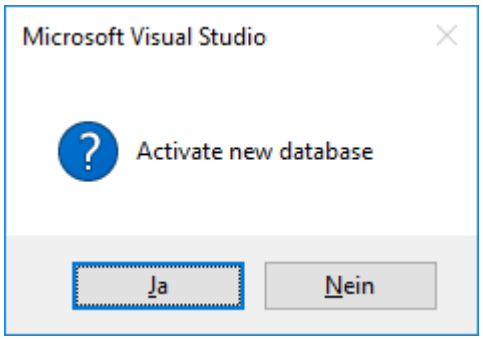
12. 点击 **OK（确认）**。
    ⇨ 数据库已保存。此时将出现对话框，提示您输入 OEM 专用密钥的密码，使用数据库时必须用它来签名。
13. 输入 OEM 证书密码并点击 **OK** 确认。



注意：从现在开始，使用数据库时（例如修改内容）无需再使用 OEM 证书。

⇨ 此时会出现另一个对话框，询问是否将该数据库设置为 Visual Studio 中的当前数据库（“激活”）。

14. 如果确认无误，点击 **OK** 。



⇨ 此时，新的数据库被设置为 Visual Studio 的**当前**数据库。

当前设置的数据库被用于建立项目与数据库的（新）关联。

分配给项目的数据库被保存在项目中（文件名和用户数据库密钥）。

该数据库位于：C:\TwinCAT\3.1\CustomConfig\UserDBs。

如果想把这个数据库（或其他数据库）定义为默认数据库，即 Visual Studio 启动时默认使用的数据库，可在配置窗口的 **Database（数据库）** 选项卡中设置。具体过程见下节。

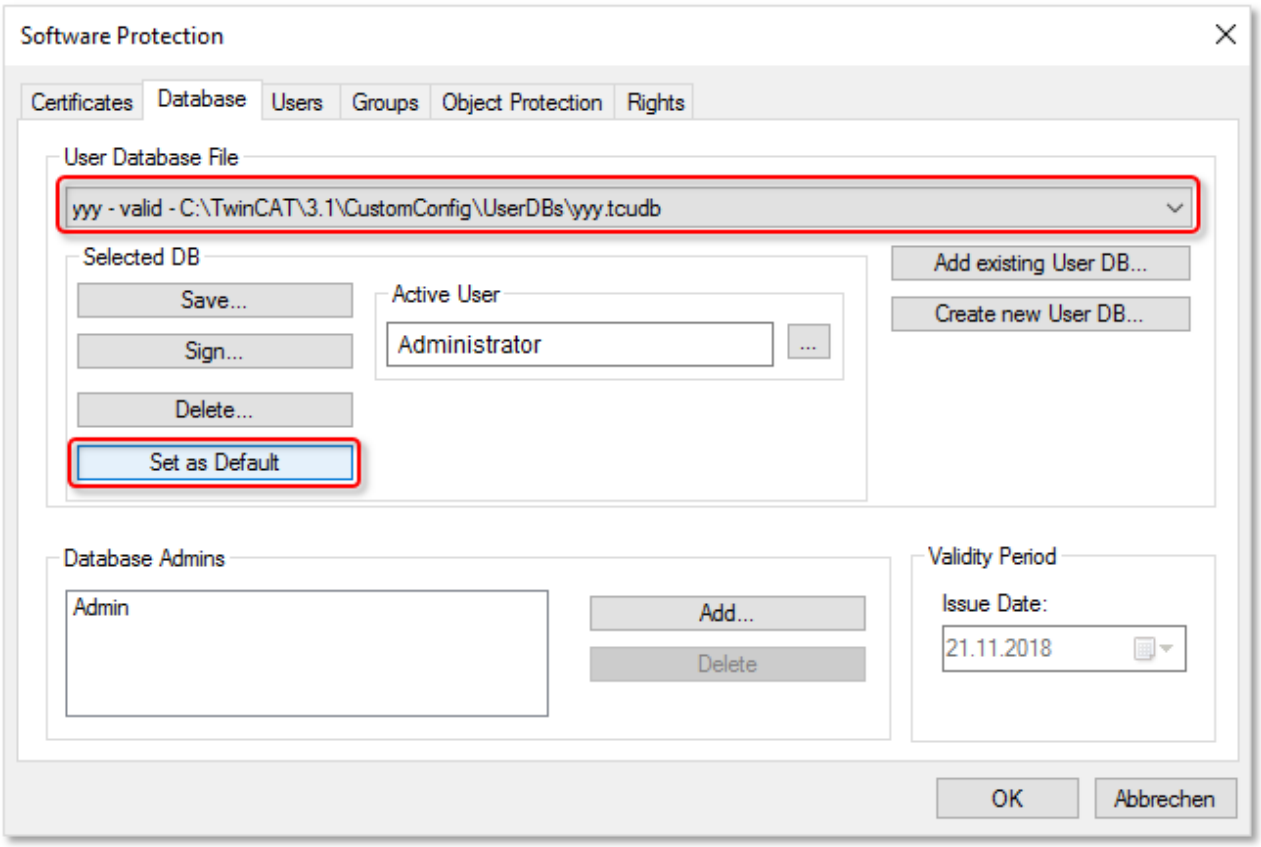
5.2 在 Visual Studio 中设置用户数据库默认值

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

指定 Visual Studio 启动时的默认设置

如果要把数据库设置为默认数据库（Visual Studio 启动时默认使用），可在软件保护配置窗口的 **Database（数据库）** 选项卡中选中所需的数据库，并点击 **Set as Default（设置为默认值）**。

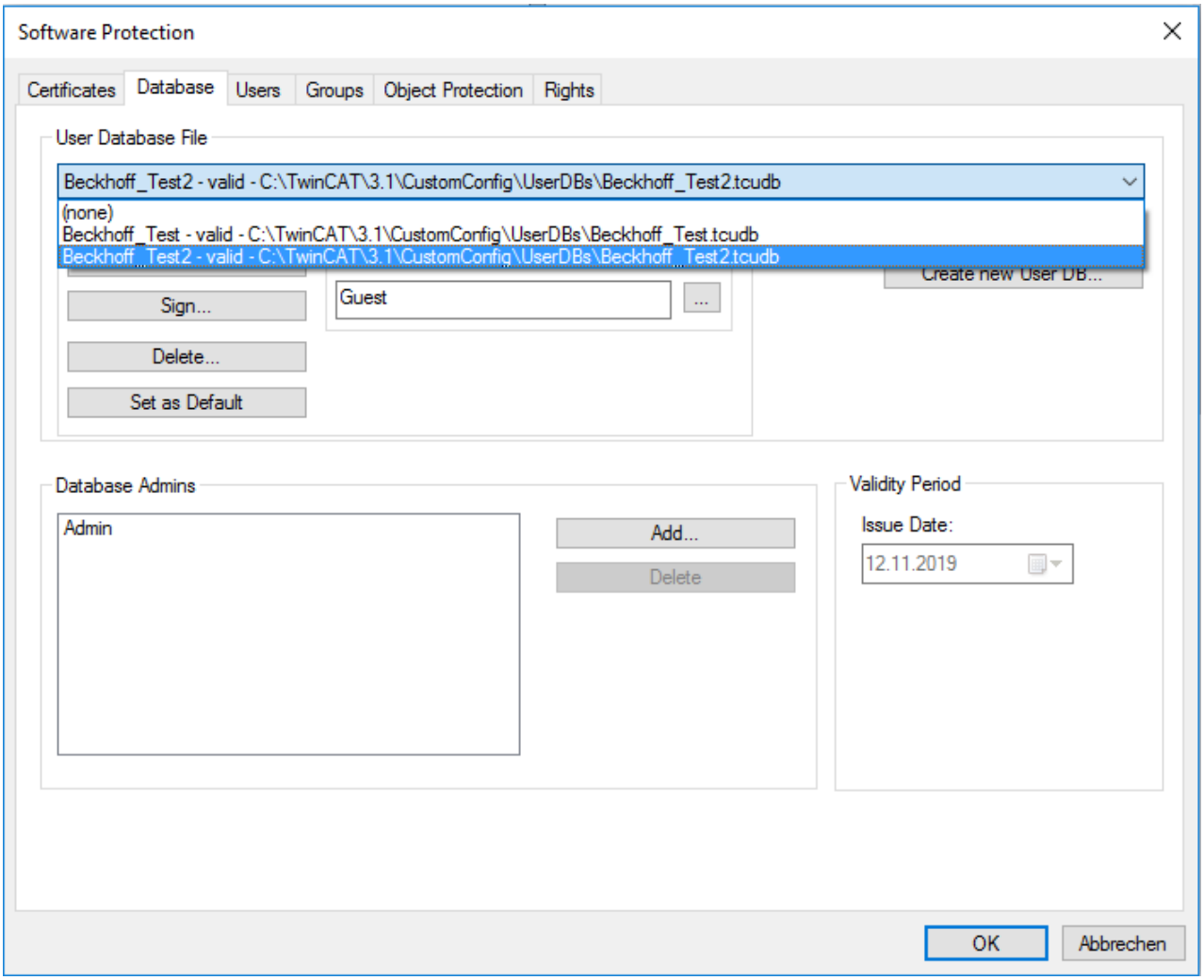


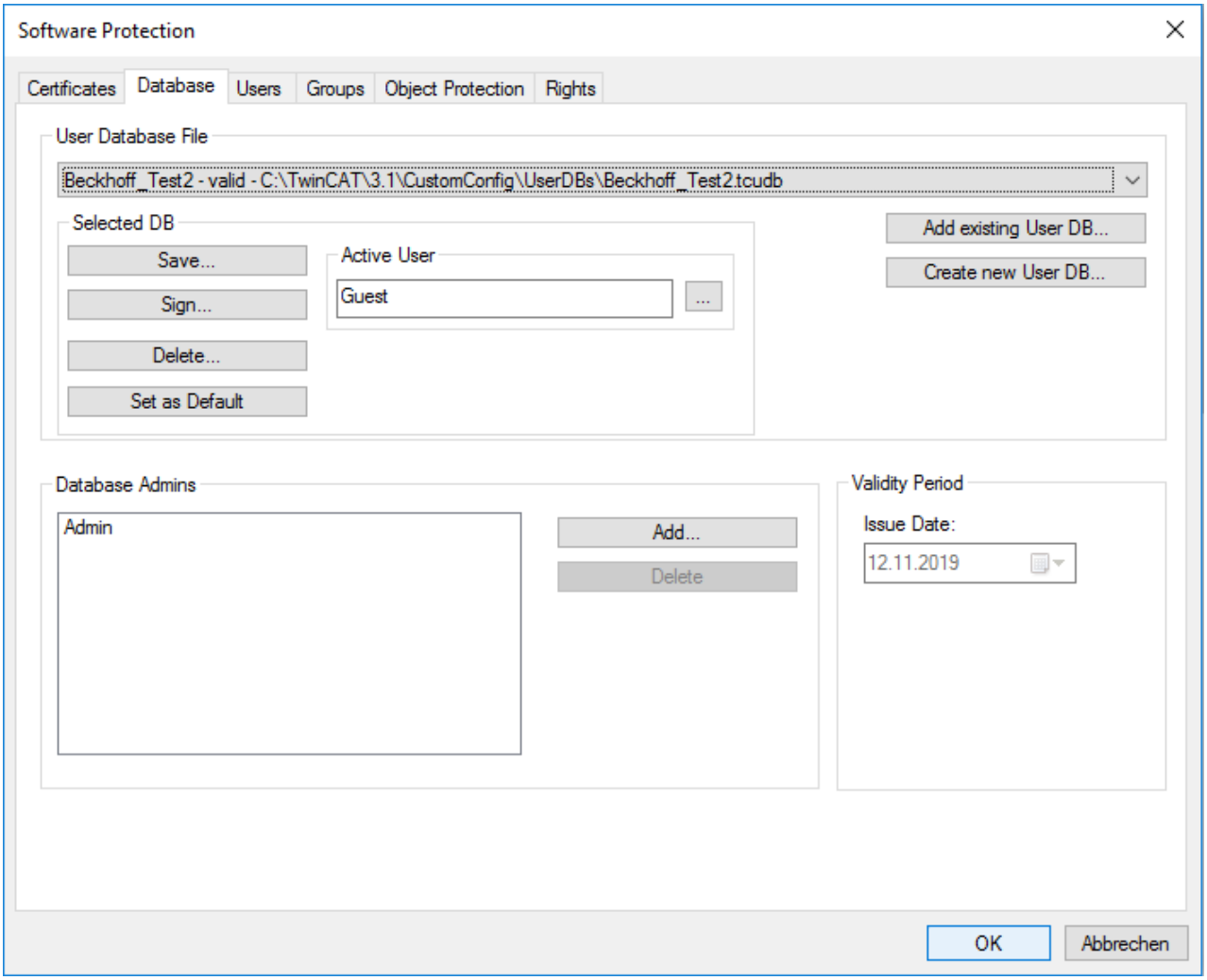
此外，可在 Visual Studio 启动后指定自动激活的用户。可在 **Active User（当前用户）** 文本框中指定。

5.3 在 Visual Studio 中选择当前用户数据库

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。


Software Protection
Certificates
Database
Users
Groups
Object Protection
Rights
User Database File
Beckhoff_Test2 - valid - C:\TwinCAT\3.1\CustomConfig\UserDBs\Beckhoff_Test2.tcudb
(none)
Beckhoff_Test - valid - C:\TwinCAT\3.1\CustomConfig\UserDBs\Beckhoff_Test.tcudb
Beckhoff_Test2 - valid - C:\TwinCAT\3.1\CustomConfig\UserDBs\Beckhoff_Test2.tcudb
Create new User DB...
Sign...
Guest
...
Delete...
Set as Default
Database Admins
Admin
Add...
Delete
Validity Period
Issue Date:
12.11.2019
OK
Abbrechen



5.4 用户数据库的默认用户

使用 TemplateOEM 模板创建的用户数据库包含两个默认用户：

- 访客（不能进行任何操作）
- 管理员*（可以进行任何操作）
  * 管理员名称在创建用户数据库 [▶ 31]时设置。

最简单的使用情况是：一个可以进行任何操作的用户（管理员）和一个不能进行任何操作的用户（访客），无需创建更多用户，且无需进行任何配置，即可使用新创建的用户数据库。在这种情况下，点击这里继续：将用户数据库与项目关联 [▶ 63]

如果需要在更加复杂的场景下使用，工程师可根据需要扩充用户数据库。参见扩充用户数据库 [▶ 46]一节。

5.5 用户数据库扩展文件

要求：TwinCAT 3 Build 4024.8 及以上版本

以下功能要求 TwinCAT 3 Build 4024.8 及以上版本。

用户数据库保存目录

为了在 TwinCAT 3中使用，用户数据库必须保存在以下目录：C:\TwinCAT\3.1\CustomConfig\UserDBs

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

介绍

从 Build 4024.8 版本开始，TwinCAT 软件保护支持用户数据库的扩展文件，即“用户数据库扩展文件”。

- 用户数据库可使用“扩展文件”进行扩展。
- 扩展文件是一个附加的 XML 文件，其结构与主用户数据库相同，但只能与主用户数据库同时使用。也就是说，扩展文件不能脱离主用户数据库单独使用。
- 扩展文件可以只包含用户定义，但不包含组或对象保护级别的定义。
- 扩展文件没有自己的管理员。主用户数据库的签名管理员也是相关扩展文件的签名管理员。
- 在文件层面上，现有的扩展文件可以方便地进行添加和删除。并不需要在相关的主用户数据库中进行配置，即无需管理员权限。
- 扩展文件保存在与主用户数据库名称相同的子目录中（包含主用户数据库目录的下级目录）：C:\TwinCAT\3.1\CustomConfig\UserDBs\<UserDB name>。
- 扩展文件通常有时间限制。
- 用户数据库可以有任意数目的扩展文件。

注意 **安全的时间限制需要一个防篡改的时间基准。**

应用：

- 主用户数据库存储静态信息，如组或对象保护级别的定义。
- 扩展文件存储有时间限制的信息（如用户信息），例如用于服务目的。

可以方便地用另一个名称和用户数据库密钥相同的数据库文件替换当前用户数据库。为了使用户数据库的修改不被篡改（防止被旧版本的数据库文件替换），必须创建一个全新的用户数据库（有不同的用户数据库密钥）并再次链接到项目。然而，这在实践中往往是不可行的。使用用户数据库扩展文件可轻松解决这个问题：

- 主用户数据库（存储静态信息，如组或对象保护级别的定义）被永久关联到项目。
- 扩展文件（有时间限制）则存储所有可能随时间变化的信息(如用户信息)。

注意 **在简单的使用场景中（用户很少），也可以不用扩展文件，而用有时间限制的用户数据库来实现。但对于更复杂的场景，这个解决方案并不实用。**

对于有不同用户组/对象保护级别的场景，用扩展文件来实现更简单。例如，内部开发人员可以在自己的扩展文件中进行总结，但交付时绝不会复制到目标控制器。这就可以根据需要添加或删除数据库区（或个别用户），而不必改变整个用户数据库。

这也大大简化了用户数据库的版本管理。

服务领域应用示例

- 主用户数据库只包含最必要的信息（签名和编辑管理员，对象保护级别和组的定义）。
- 扩展文件专为服务任务而创建，用户只有服务人员。扩展文件的时间限制在服务任务期间。
- 该服务人员将扩展文件保存在服务笔记本（或U盘）上携带。

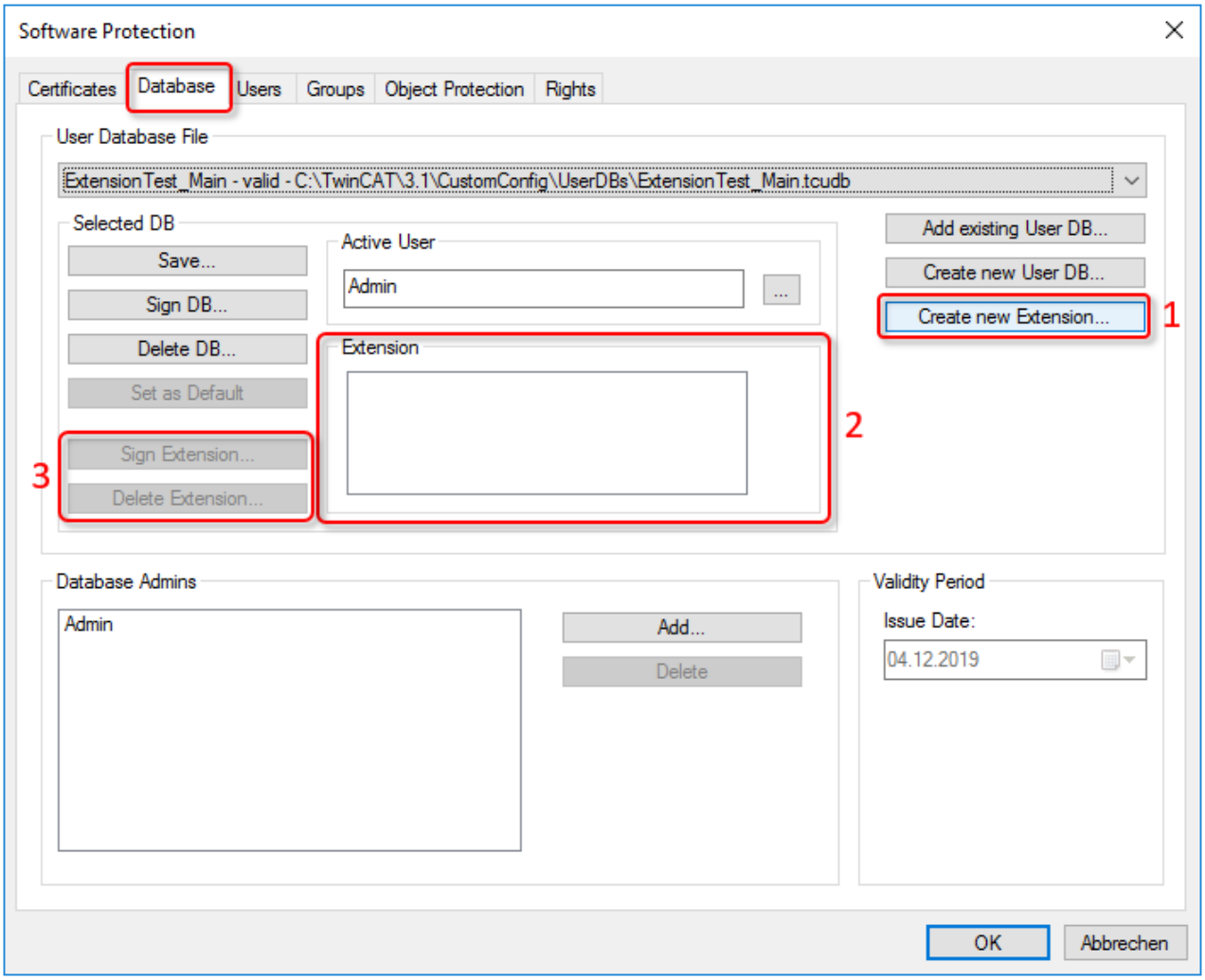
用户数据库/扩展文件的时间限制

防篡改的时间限制需要一个防篡改的时间基准！

5.5.1 软件保护配置控制台的相关元素

为了对扩展文件及其中定义的用户进行管理，在软件保护配置控制台的用户界面上包含以下元素。

数据库选项卡：

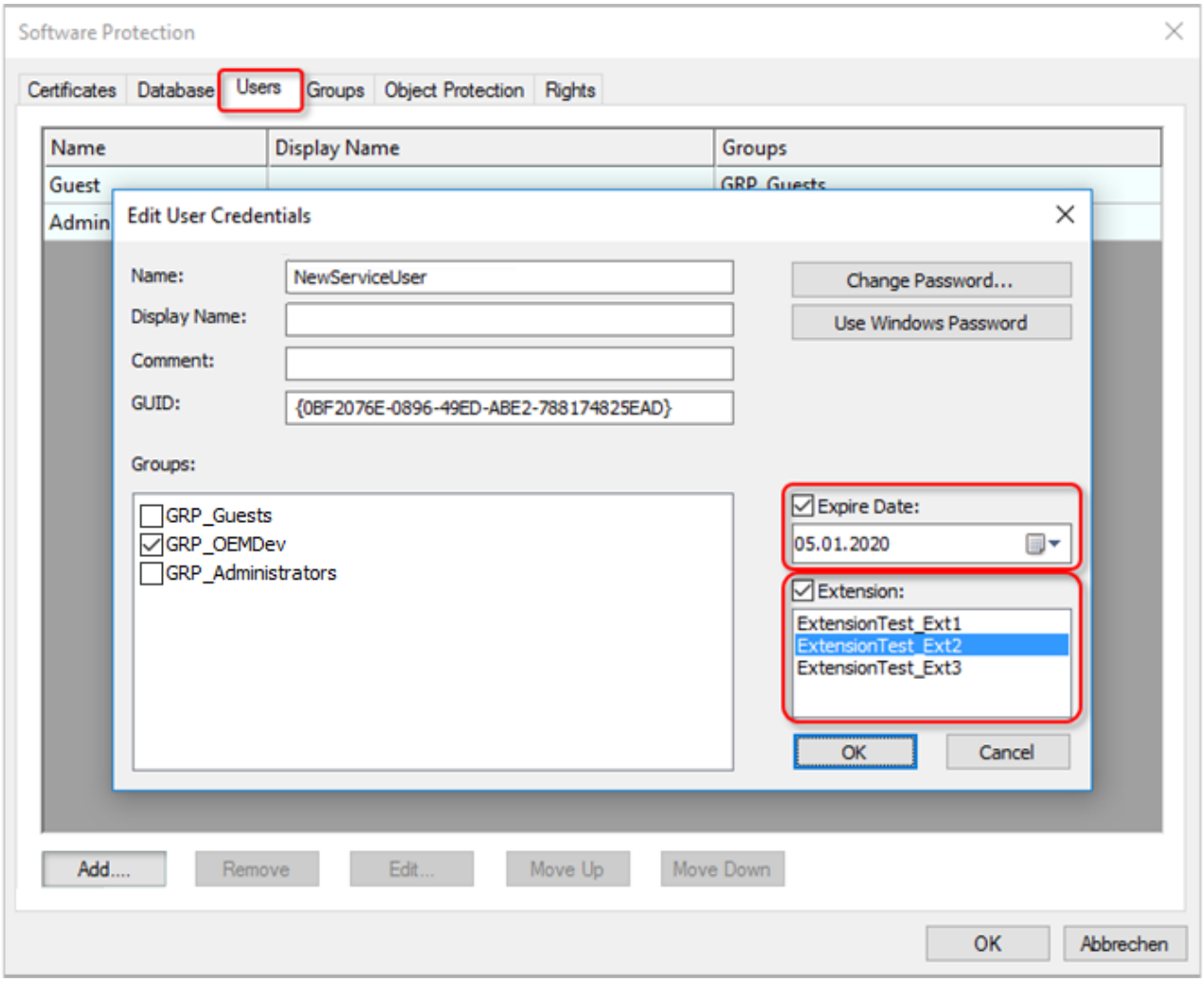


1：为当前选定的用户数据库创建新的扩展文件

2：现有扩展文件列表

3：签署或删除在步骤（2）中选中的扩展文件

用户选项卡：



可为现有的扩展文件分配一个用户账号，并设置该账号的有效期。

5.5.2 TwinCAT 3中的手动配置的步骤

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

5.5.2.1 创建扩展文件

项目打开时，无法修改用户数据库设置

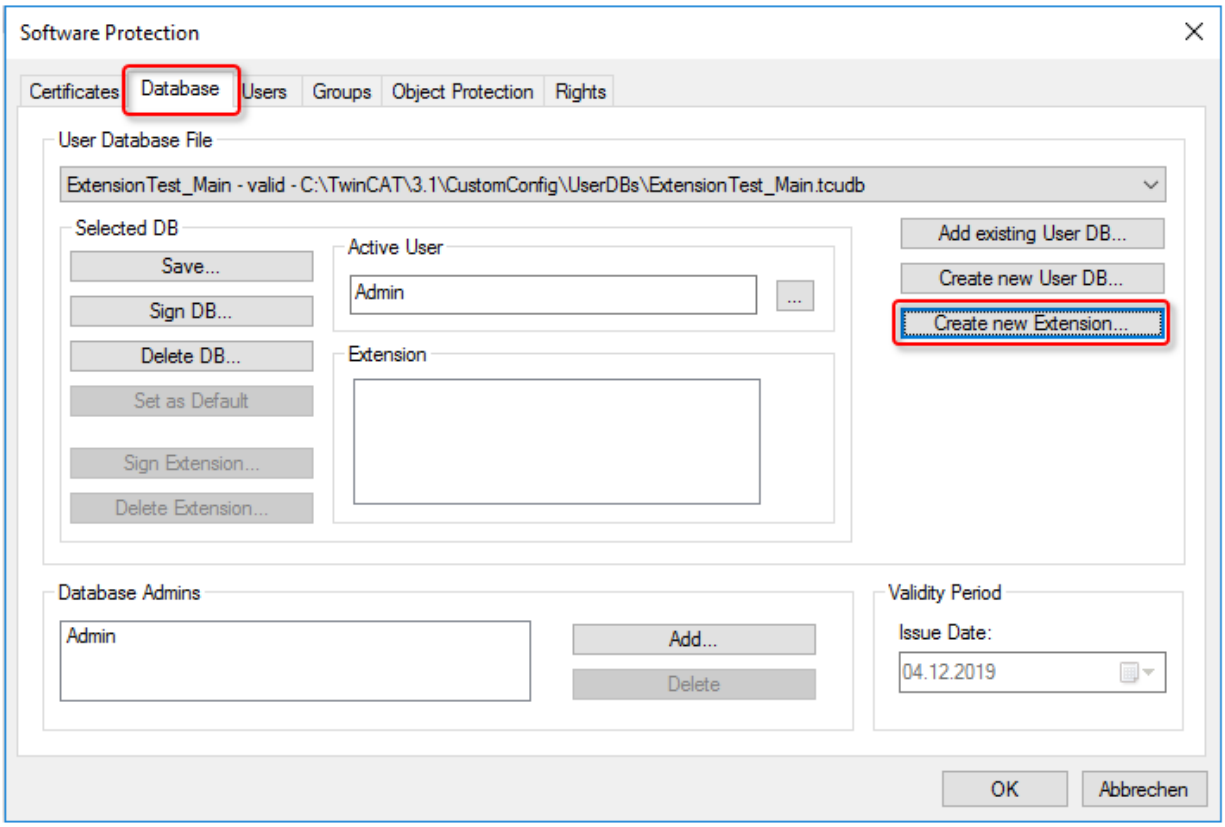
修改用户数据库设置时，不能打开任何项目。

扩展文件的修改必须被签名

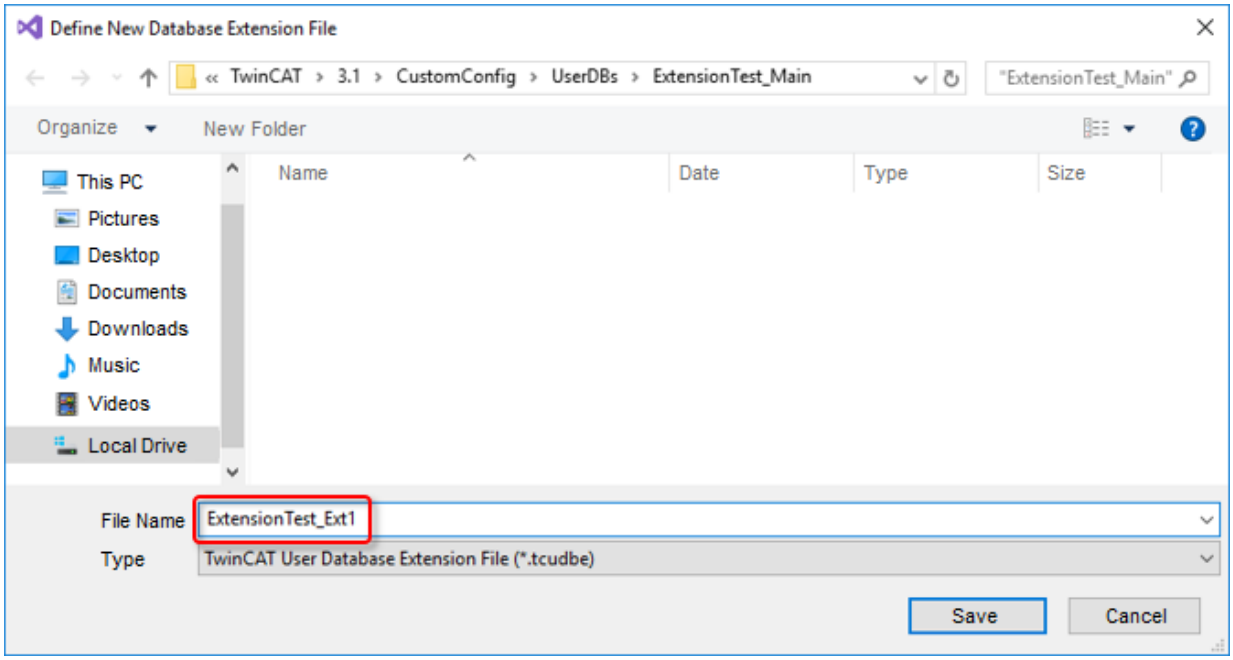
扩展文件修改（包括扩展文件的初始创建）必须由签名管理员签名，否则扩展文件无效。

创建新的扩展文件

✓ 当前用户必须有（编辑）管理员权限！

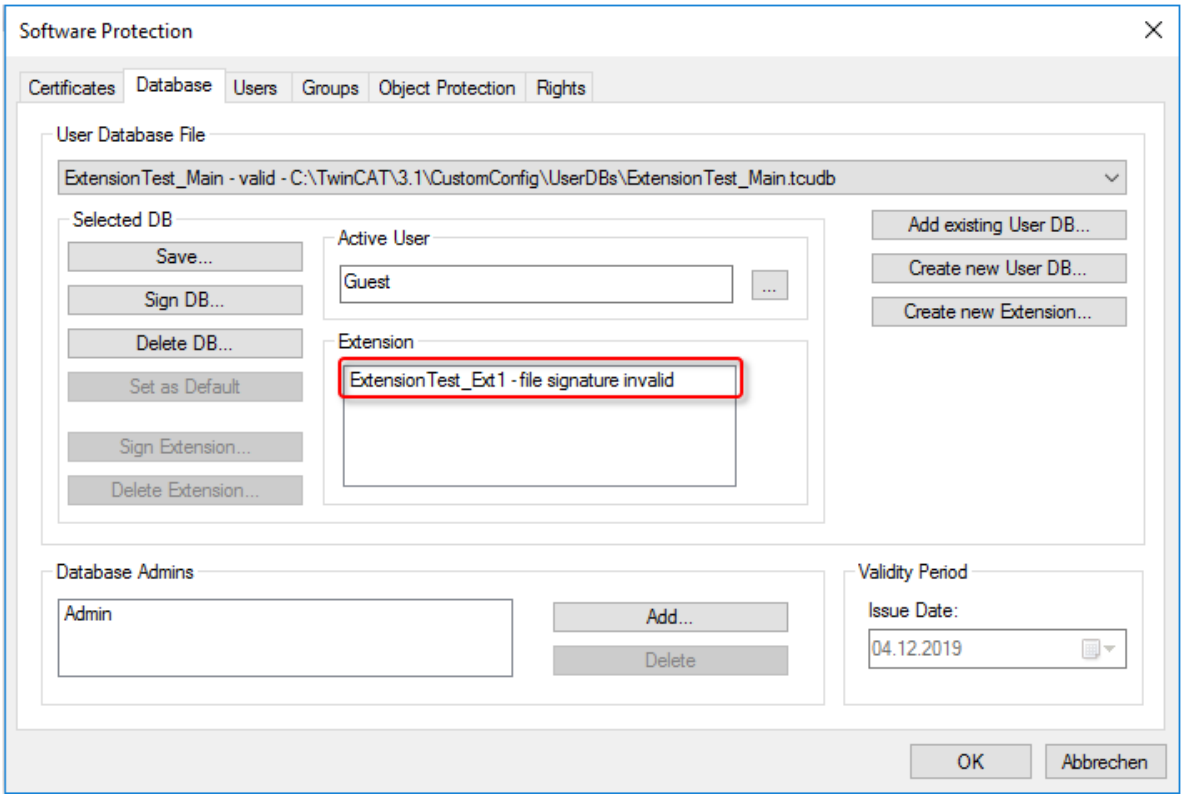


1. 点击 **Create new Extension（创建新的扩展文件）**，打开创建新扩展文件的对话框：

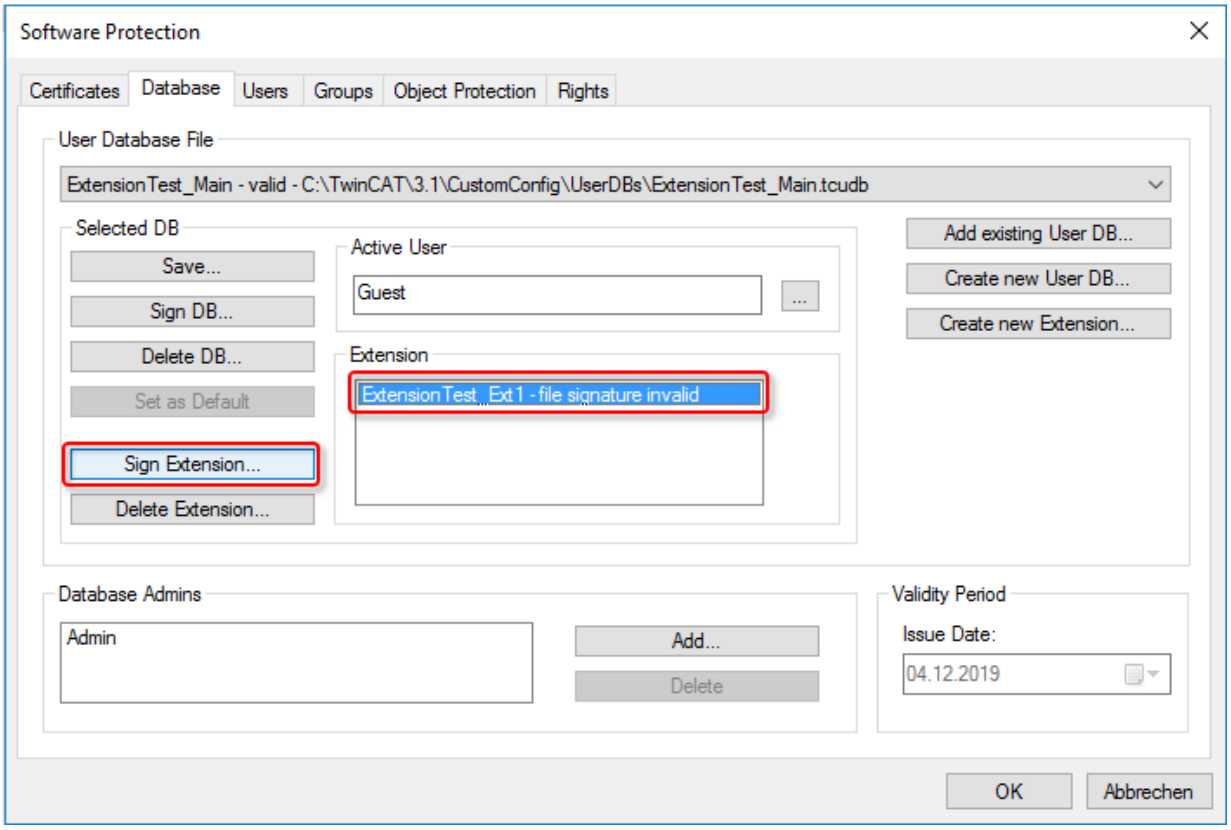


注意 **不得更改指定目录！**

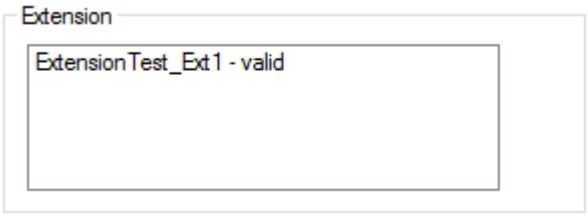
⇨ 新的扩展文件已创建，但并未签名，因此初始状态为“无效”：



2. 首先，在 **Database（数据库）**选项卡的扩展文件列表中，点击选中的扩展文件，即可由签名管理员（主用户数据库）进行签名…



3. ... 签名后其状态变成“有效”：



已创建的扩展文件为空文件，必须填充内容（用户）。

5.5.2.2 在扩展文件中创建用户

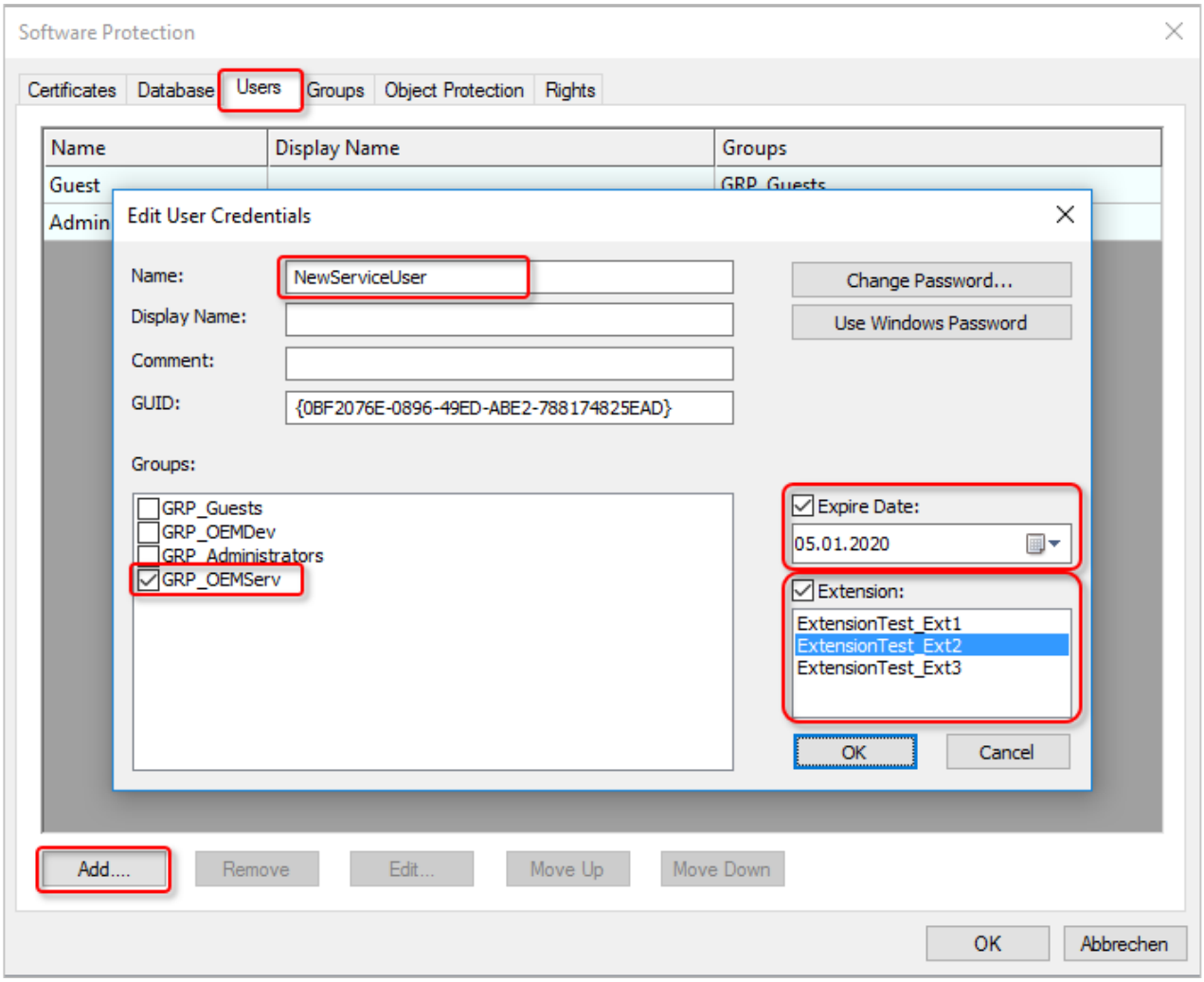
项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

扩展文件的修改必须被签名

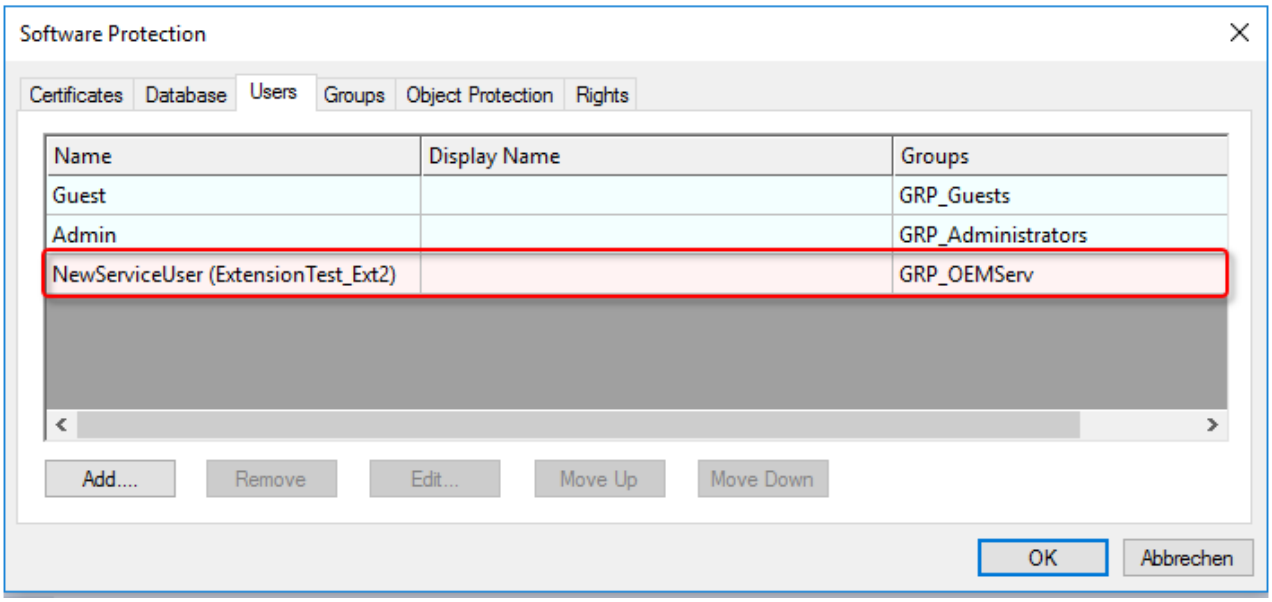
扩展文件修改（包括扩展文件的初始创建）必须由签名管理员签名，否则扩展文件无效。

例如：在 **Users（用户）** 选项卡中，创建新用户 NewServiceUser，将其分配给 GRP_OEMServ 组以及扩展文件，并设置所需的时间限制：



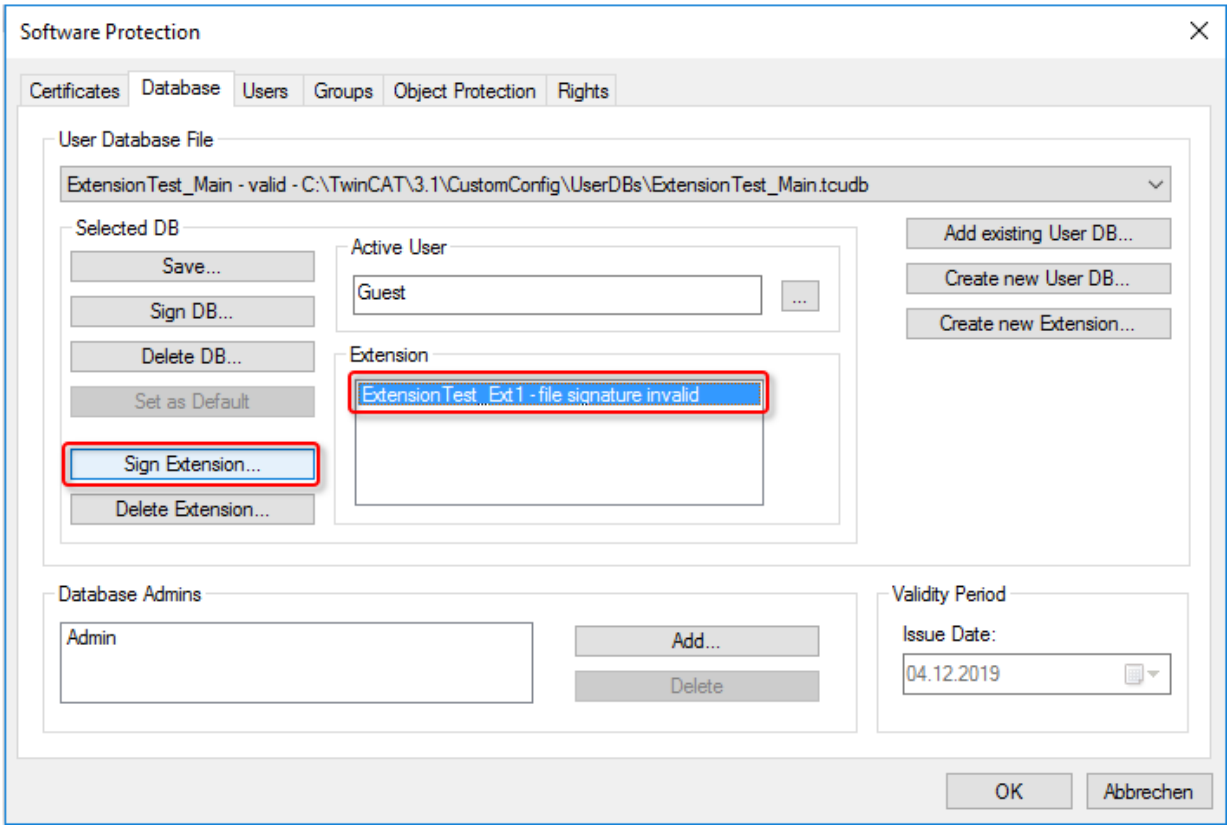
这样就在选定的扩展文件中完成了新用户创建。

在现有用户账号列表中，用户与扩展文件的隶属关系以不同颜色表示，扩展文件名称标注在用户名后的括号内：

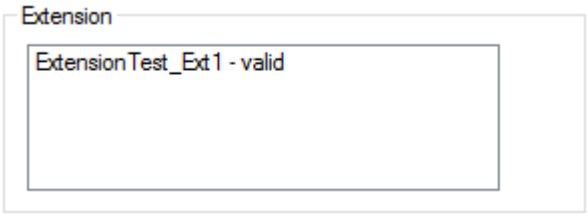


扩展文件修改仍需签名才能生效。

1. 首先，在 **Database（数据库）** 选项卡的扩展文件列表中，点击选中的扩展文件，即可由签名管理员（主用户数据库）进行签名…



2. ... 签名后其状态变成“有效”：



5.5.3 自动步骤

命令行工具用于自动创建扩展文件和其中的用户，并将其整合到基础结构中。

5.6 扩充用户数据库

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

保存数据库修改时必须签名

数据库的修改操作必须由管理员签名，否则该操作无效。保存过程中会自动询问是否签名。

数据库模板 TemplateOEM

数据库模板 *TemplateOEM* 的设计覆盖了最常见的（简单）应用场合，无需自定义组权限。包括：

- 两个用户：一个可以进行任何操作，另一个不能进行任何操作 [▶ 38]。
- 添加/修改数据库管理员 [▶ 46]
- 区分数据库管理员和开发人员的功能 [▶ 50]
- 添加更多具有“开发人员”组任务的用户 [▶ 51]

必须为其他应用场合定义单独的组权限 [▶ 52]。

下载链接：组权限和对象保护级别规划表

关于组权限和访问权限群组（对象保护级别）的简单规划，点击https://infosys.beckhoff.com/content/1033/tc3_security_management/Resources/zip/9007208137629963.zip下载 Excel 表格。

5.6.1 添加/修改数据库管理员

项目打开时，无法修改用户数据库设置

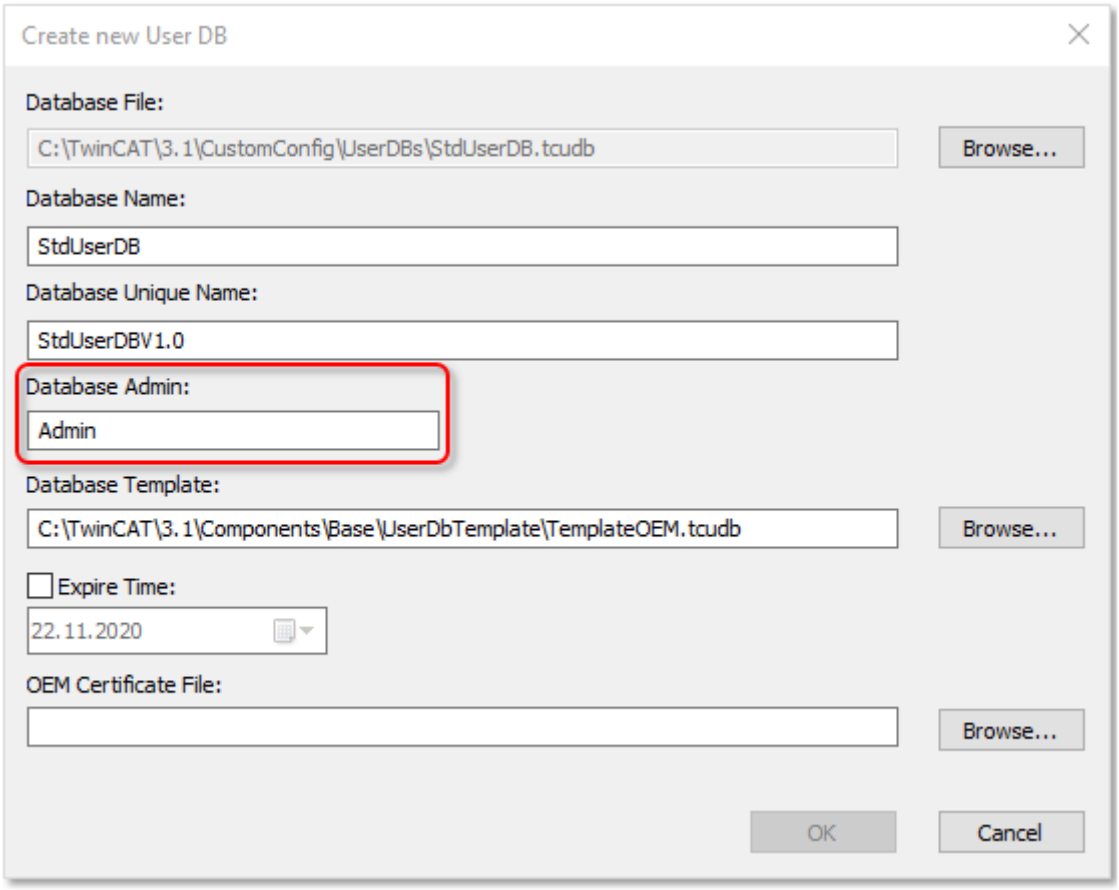
修改用户数据库设置时，不能打开任何项目。

本说明适用于 Build 4024。

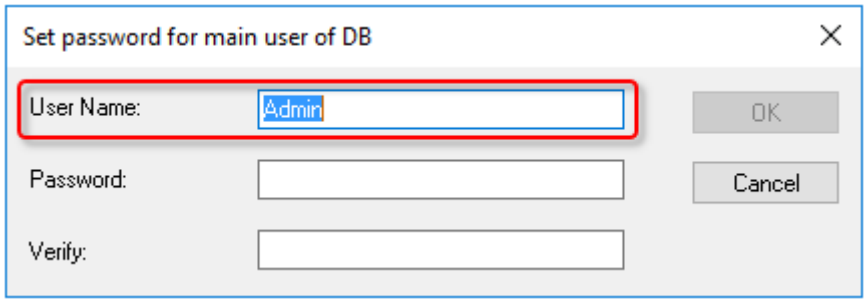
用户数据库包含两个管理员，分管不同的任务：

1. 签署（发布）对数据库的修改
2. 修改数据库内容

创建用户数据库时，直接创建第一（签名）管理员：



在第一管理员创建后，TwinCAT 3 创建第二（编辑）管理员作为数据库用户（“主用户”），并建议将第一（签名）管理员名称作为用户名。这使得两种管理员的功能可以很轻松地结合起来，在需要的时候使用相同的用户名和密码即可方便的使用。



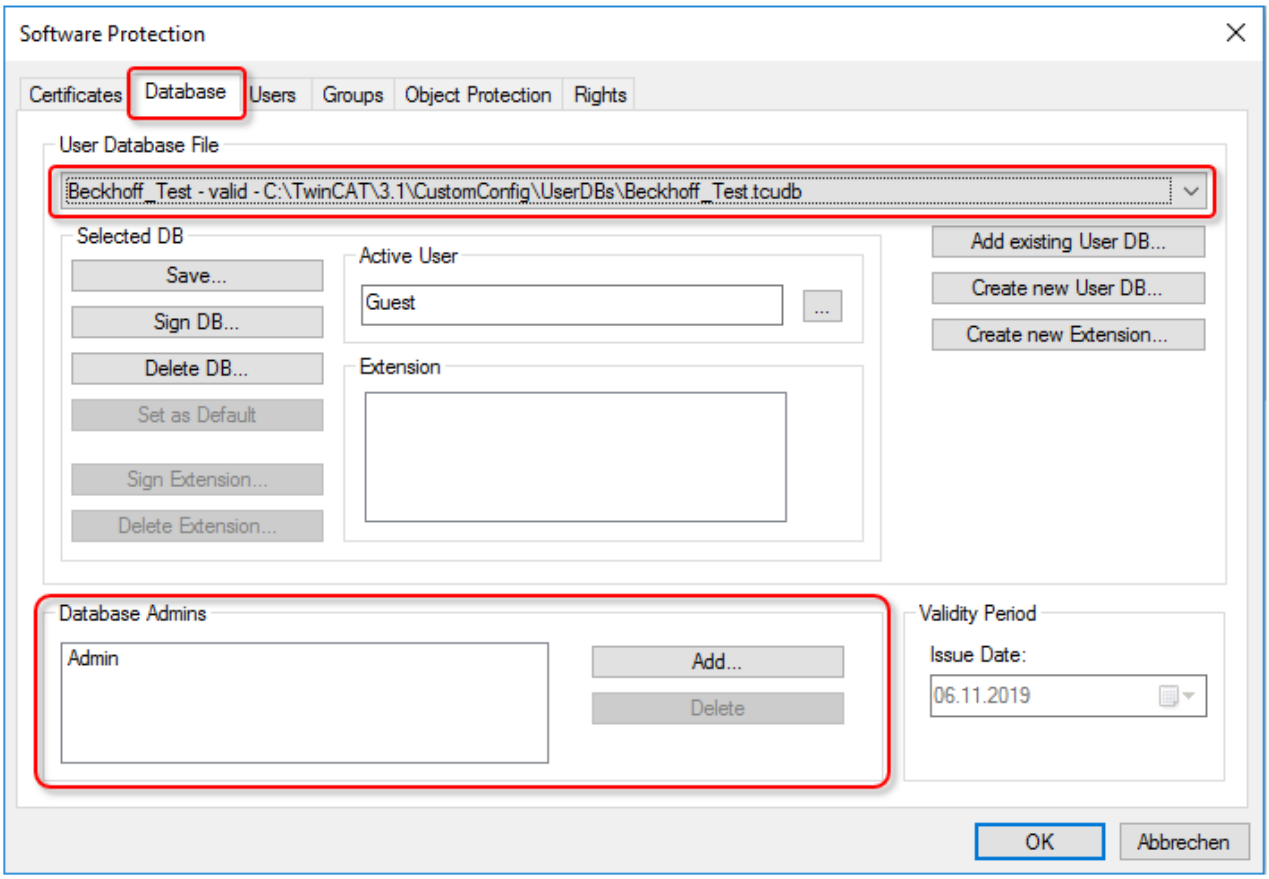
Build 4022 版本：

该版本没有相应的输入窗口。因此，在创建用户数据库后，必须手动创建编辑管理员为数据库用户，并分配到 GRP_Administrators 组。

创建新的数据库签名管理员

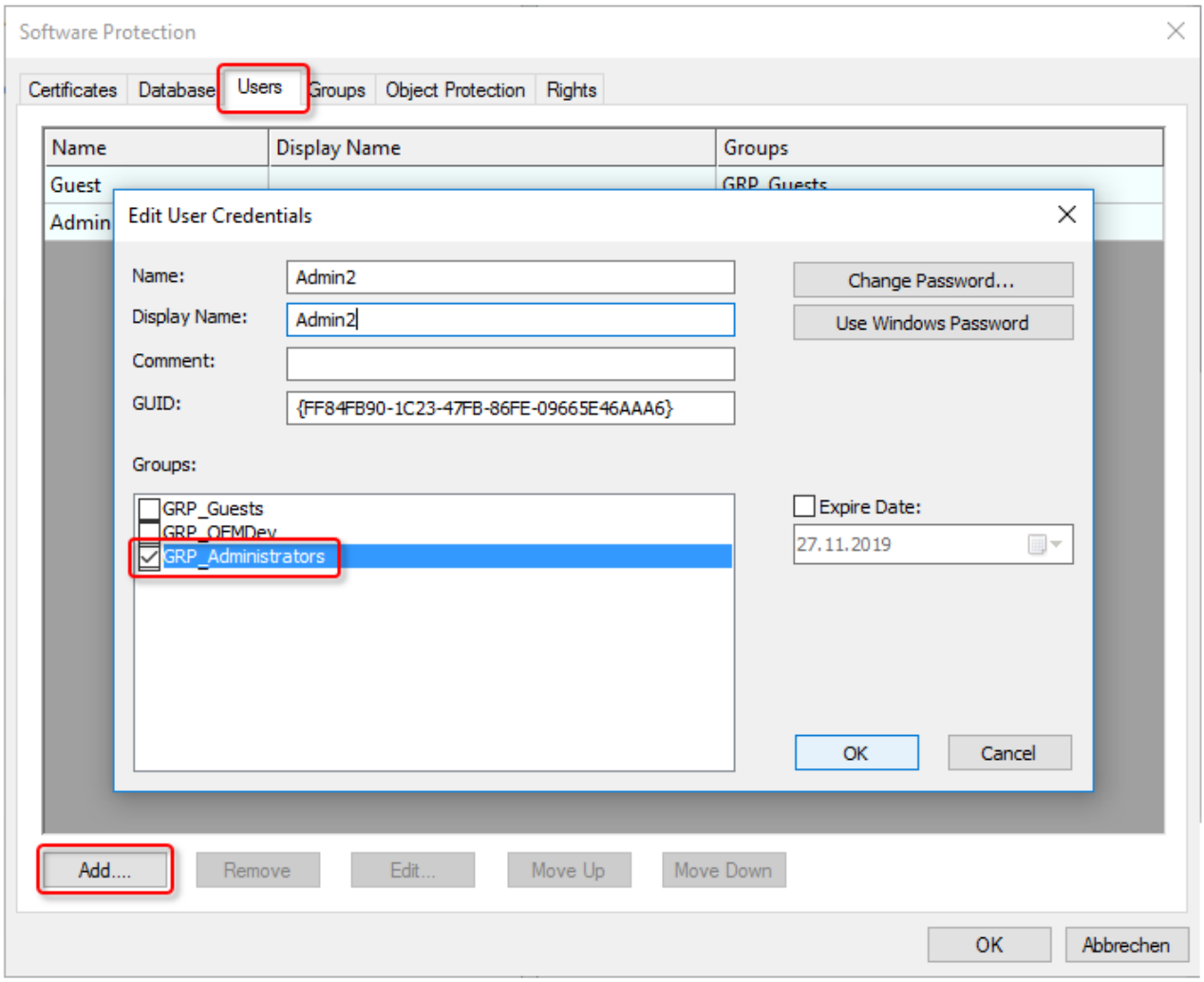
在软件保护配置控制台的 **Database（数据库）**选项卡中，可创建新的签名管理员。

选中所需的数据库；在 **Database Admin（数据库管理员）**窗口可创建或删除管理员：



创建新的数据库编辑管理员

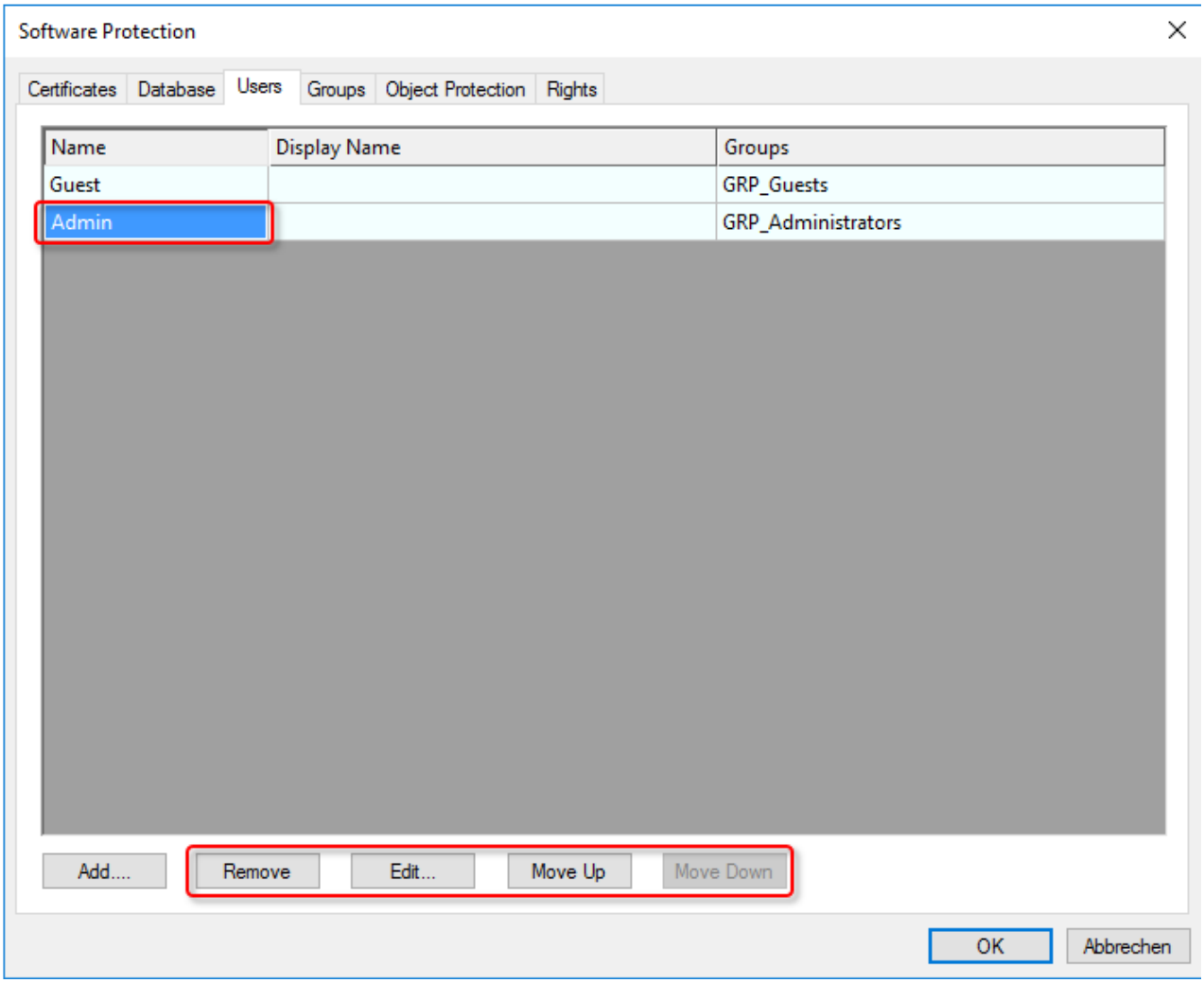
在软件保护配置控制台的 Users（用户）选项卡中，可创建新的编辑管理员：



新用户必须分配到 GRP_Administrators 组。

用户也可以是 Windows 账号（域用户）；在这种情况下，相关的 Windows 密码可用于自动登录。

选择用户后，还可在列表中进行删除、修改或上下移动：



必须有一个用户拥有管理员权限！

如果用户数据库中没有用户具有管理员权限，将无法对数据库进行任何修改，包括添加新的管理员！因此，至少必须有一个用户拥有（编辑）管理员权限！(有签名管理员还不够，因为他不能修改数据库)。

5.6.2 区分数据库管理员和开发人员的功能

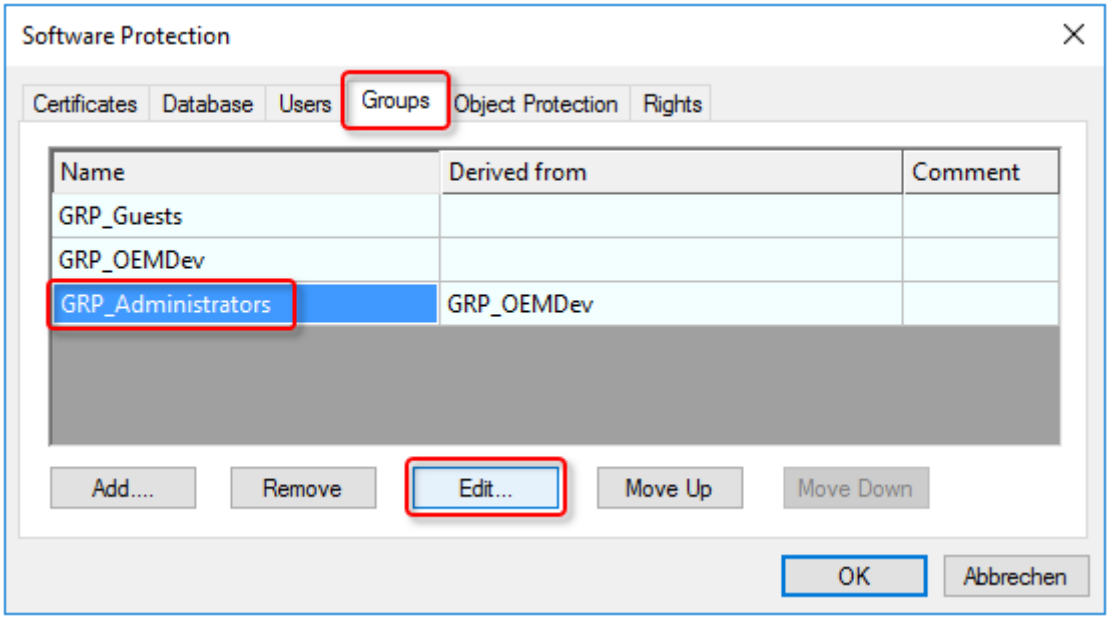
项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

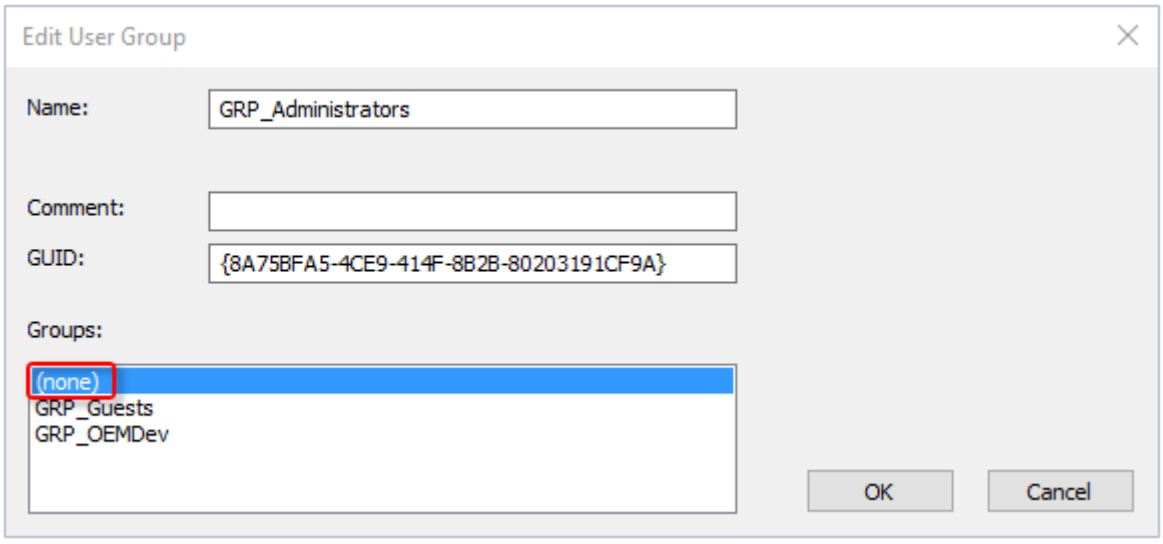
在默认情况下，GRP_Administrators 组也继承了 GRP_OEMDev（开发人员）组的权限。

如果用户数据库的（编辑）管理员没有修改 TwinCAT Solution 的权限，只需修改 GRP_Administrators 组中 GRP_OEMDev 组的成员资格即可。

在软件保护配置控制台的 **Groups（组）** 选项卡上选择 GRP_Administrators 组，并点击 **Edit（编辑）** 按钮：



选择所需的组成员（或 “None（无）”）：



现在（编辑）管理员可以修改用户数据库，但不再有 GRP_OEMDev 组（开发人员）的权限。

5.6.3 将用户添加至用户组

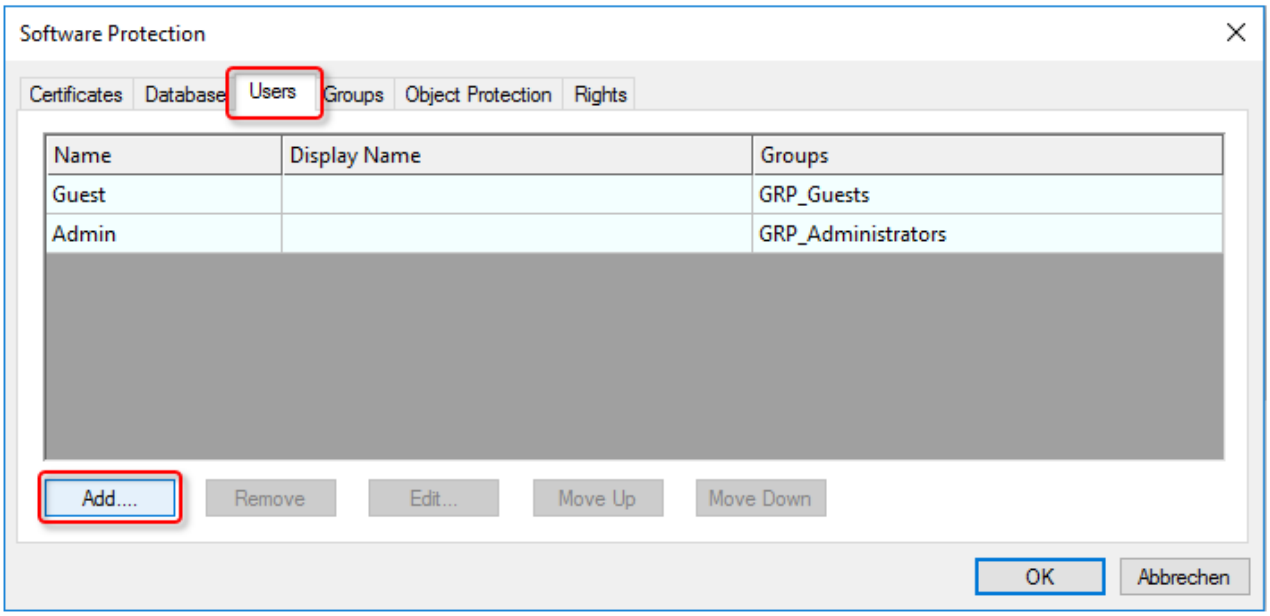
项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

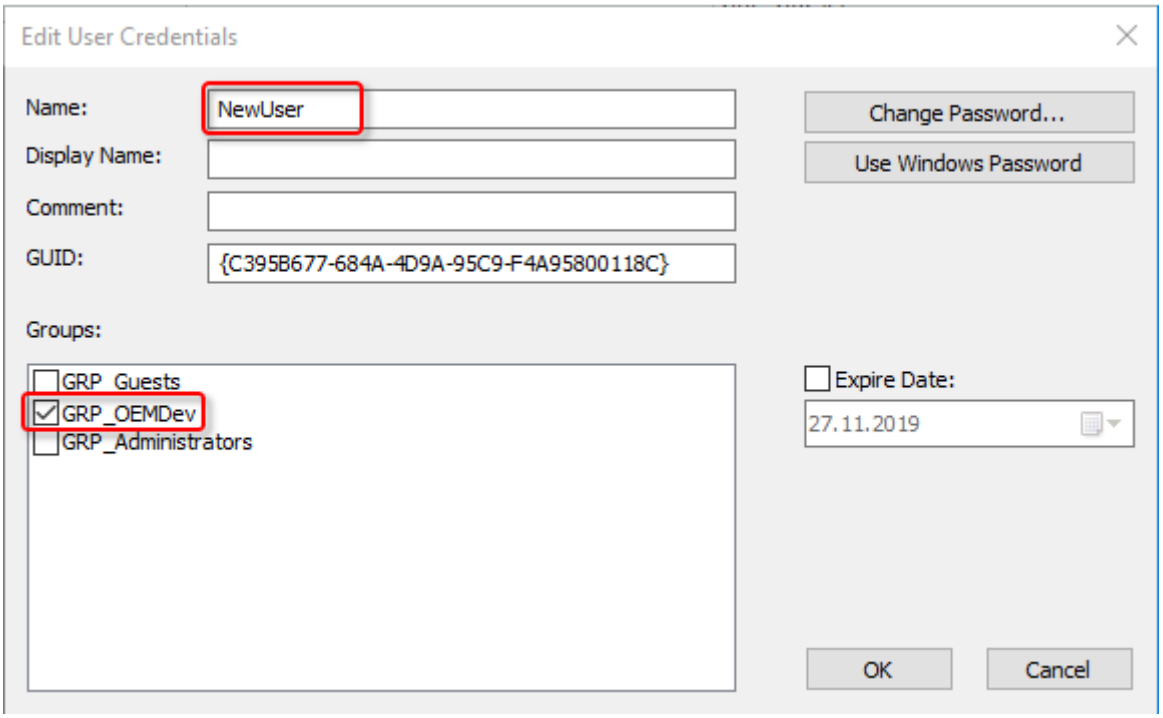
以下为将用户添加到 GRP_OEMDev 组的例子。该步骤也同样适用于其他组。

用户可以是多个组的成员。

点击配置控制台 **Users（用户）** 选项卡中的 **Add...（添加）** 按钮：



现在可以创建新用户，并可以根据需求设置为目标组的成员：



用户也可以是 Windows 账号（域用户）；在这种情况下，相关的 Windows 密码可用于自动登录。

从 Build 4024.8 版本开始

也可以在“扩展文件 [▶ 44]”中创建用户。详见此处 [▶ 38]。

有关如何创建新的用户组和修改现有用户组，参见“创建和编辑用户组” [▶ 57]。

5.6.4 自定义组访问权限

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

下载链接：组权限和对象保护级别规划表

关于组权限和访问权限群组（对象保护级别）的简单规划，点击https://infosys.beckhoff.com/content/1033/tc3_security_management/Resources/zip/9007208137629963.zip下载 Excel 表格。

5.6.4.1 介绍

系统要求

操作系统：

- Windows 7 及以上版本（或对应的嵌入式版本），以便能够使用所有应用软件保护功能。Windows XP 和 Windows CE（Windows Embedded Compact）不支持启动文件的加密或 OEM 授权。

TwinCAT 版本：

- 所述功能要求 TwinCAT 3.1 build 4022 及以上版本。

只有使用最新版本的 TwinCAT 3，才会获得可靠的保护。

为确保获得可靠的保护（例如安全加密），请始终使用最新版本的TwinCAT 3。这可以提供最高的安全性。

至少应使用 TwinCAT 3.1 Build 4024.x。
鉴于安全因素，请勿使用旧版本！

下载链接：组权限和对象保护级别规划表

关于组权限和访问权限群组（对象保护级别）的简单规划，点击https://infosys.beckhoff.com/content/1033/tc3_security_management/Resources/zip/9007208137629963.zip下载 Excel 表格。

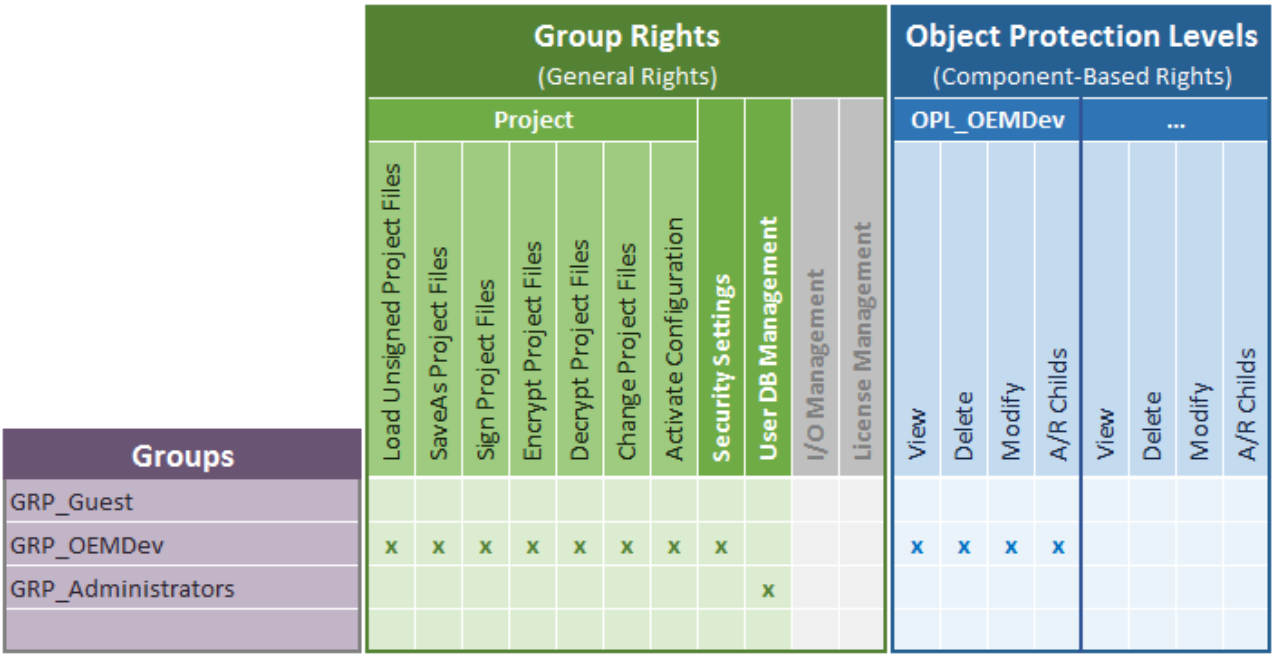
TwinCAT 用户访问权限

- 在 TwinCAT 3 中给各个组分配访问权限。
- 用户可以分配到几个组别。
- 分组可以是**另一**组的成员。

注意：为了便于管理，建议不要将一个组分配为另一个组的成员，而是给每一个用户组独立设置权限。

权限在 TwinCAT 3 Engineering 中主要分为两类：

1. 项目中的一般权限（例如签名文件的权限）。这些权限都是单独分配给用户组的，因为权限始终适用于整个项目。
2. 特定组件专用的权限（“查看”、“删除”、“修改”和“添加/删除子权限”）。
   因为这些权限可能会根据分组成员的不同而在项目的不同部分有所不同，所以被组织成一个“权限集”，将所有分组的个人权限汇总到一项分配指定下。



上图中灰色权限是在当前版本中提供的“供将来使用”，尚未实施。

这样的权限集被称为“对象保护级别”，代表一个对象的现有组及其权限矩阵。有了对象保护级别，个别项目组件可以很方便地一次性为每个组提供预制的权限集，而且这些权限不必分组指定给每个项目组件。

如果一个项目的对象在访问权限设置上没有区别（最简单的用例），那么定义和使用一个单一的对象保护级别就已足够。然后，这将被分配给项目中的所有对象。

在上面示例中，除了对数据库进行修改之外，开发人员组被允许做任何事情，管理员组只允许对数据库进行修改，而访客组不允许做任何事情（甚至不允许加载项目）。

请牢记其他分组中的分组成员！

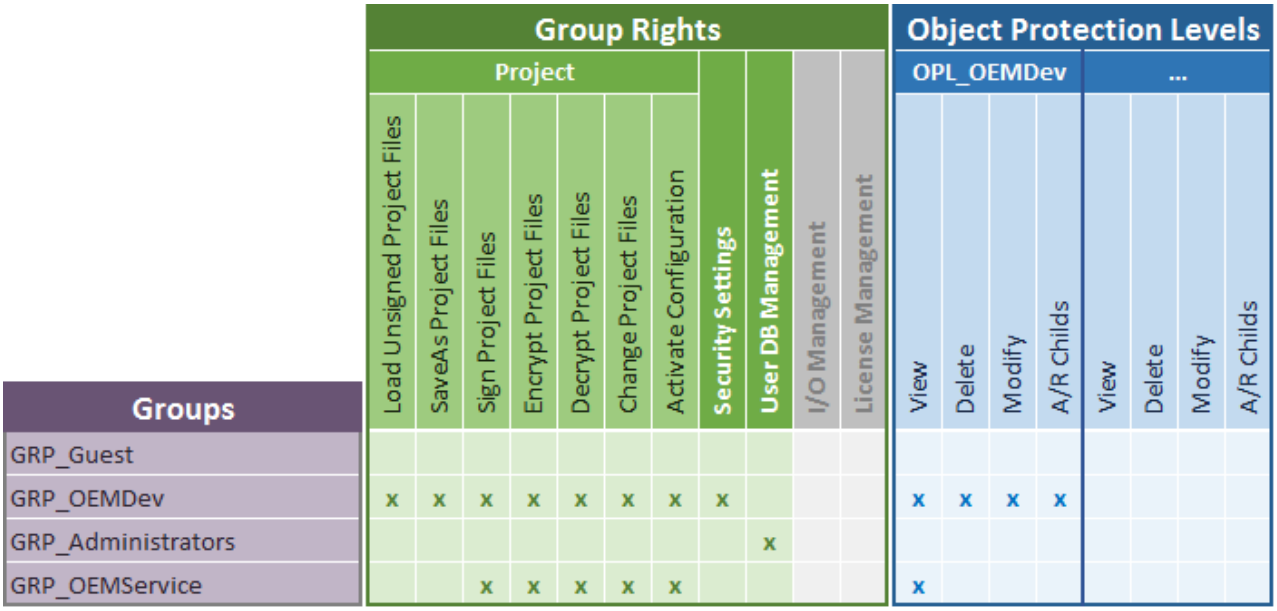
示例 1

在下面的示例中，将添加一个名为 GRP_OEMService 的新组。

(关于如何创建新组和分配权限，参见此处 [▶ 57])。

新组可以查看所有信息，但不能进行任何修改，还可以激活项目。

为了查看项目，该组必须有“解密项目文件”的权限（否则 Visual Studio 将无法加载项目的加密部分）。



Groups	Group Rights: Project: Load Unsigned Project Files	SaveAs Project Files	Sign Project Files	Encrypt Project Files	Decrypt Project Files	Change Project Files	Activate Configuration	Security Settings	User DB Management	I/O Management	License Management	Object Protection Levels: OPL_OEMDev: View	Delete	Modify	A/R Childs	...: View	Delete	Modify	A/R Childs
GRP_Guest																			
GRP_OEMDev	x	x	x	x	x	x	x	x				x	x	x	x				
GRP_Administrators									x										
GRP_OEMService			x	x	x	x	x					x							

为了激活项目，除了“激活配置”权限外，还必须能修改项目文件（因为激活时会保存特定的信息），并以加密形式保存修改。因此，还需要“修改项目文件”和“加密项目文件”的权限。

对于组件特定权限，只赋予必要的“查看”权限。

无需创建新的对象保护级别，因为这个权限集合应当总是适用于整个项目。

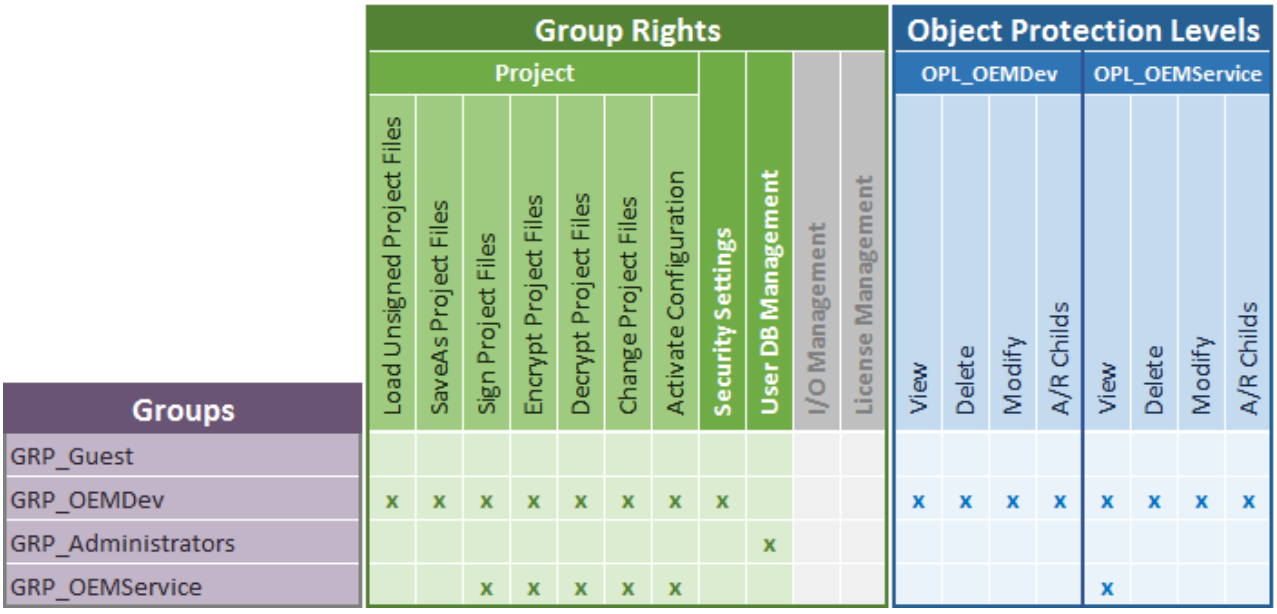
示例 2

在下述示例中，GRP_OEMService 组只能查看项目的定义组件。

因此需要创建一个新的组权限集合，即新的对象保护级别 (OPL)，以便区分特定项目组件的权限分配。我们将新的对象保护级别称为 OPL_OEMService。

(关于如何创建新的对象保护级别，参见此处 [▶ 61])。

GRP_OEMService 组的查看权限从 OPL_OEMDev 中删除，并添加到新的 OPL_OEMService 中：



Groups	Group Rights: Project: Load Unsigned Project Files	SaveAs Project Files	Sign Project Files	Encrypt Project Files	Decrypt Project Files	Change Project Files	Activate Configuration	Security Settings	User DB Management	I/O Management	License Management	Object Protection Levels: OPL_OEMDev: View	Delete	Modify	A/R Childs	OPL_OEMService: View	Delete	Modify	A/R Childs
GRP_Guest																			
GRP_OEMDev	x	x	x	x	x	x	x	x				x	x	x	x	x	x	x	x
GRP_Administrators									x										
GRP_OEMService			x	x	x	x	x									x			

由于 GRP_OEMDev 组在新的 OPL_OEMService 中可进行任何操作，这个组也被分配了所有权限（浏览、修改…）。

示例 3

在下述示例中，GRP_OEMService 组可修改特定的项目组件。(但仍然无法删除或添加项目组件)。

因此，需创建新的对象保护级别 (OPL)。我们称之为 OPL_OEMServiceEdit：

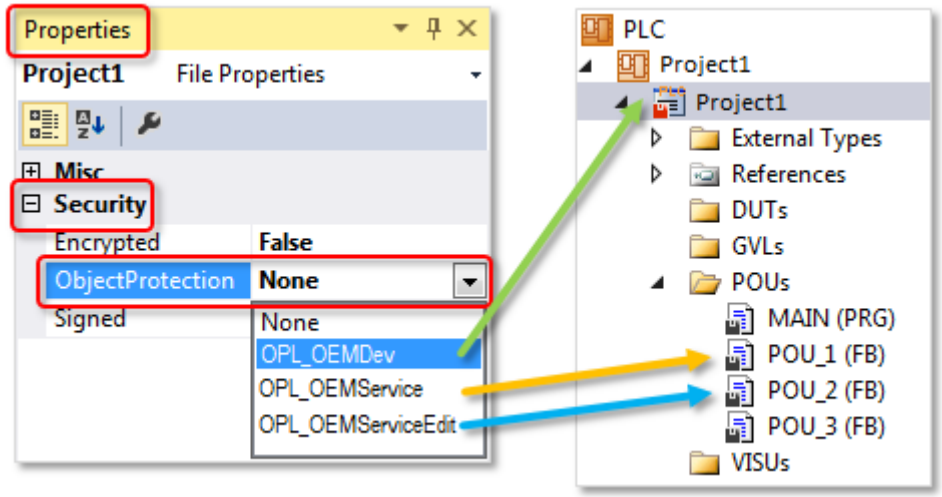
Groups	Group Rights: Project: Load Unsigned Project Files	SaveAs Project Files	Sign Project Files	Encrypt Project Files	Decrypt Project Files	Change Project Files	Activate Configuration	Security Settings	User DB Management	I/O Management	License Management	Object Protection Levels: OPL_OEMDev: View	Delete	Modify	A/R Childs	OPL_OEMService: View	Delete	Modify	A/R Childs	OPL_OEMServiceEdit: View	Delete	Modify	A/R Childs
GRP_Guest																							
GRP_OEMDev	x	x	x	x	x	x	x	x				x	x	x	x	x	x	x	x	x	x	x	x
GRP_Administrators									x														
GRP_OEMService			x	x	x	x	x									x				x		x	

相比 OPL_OEMService，仅增加了“修改”权限，其余权限相同。

现在，分配给 OPL_OEMServiceEdit 的项目组件，也可以由 GRP_OEMService 组的用户进行修改。

项目中对象保护级别的指定

现在我们只需要将在前面示例中创建的 OPL 分配给项目组件。（如何具体在 TwinCAT Engineering 中分配 OPL，请参阅此处 [▶ 64]）。



OPL 被继承

分配给 PLC 项目根的 OPL 被继承到底层节点中。只有和 PLC 项目根节点的设置需求不同的其他节点，才需单独设置所需的对象保护级别。

示例 4

下述示例中，服务人员可激活项目，但无法查看。

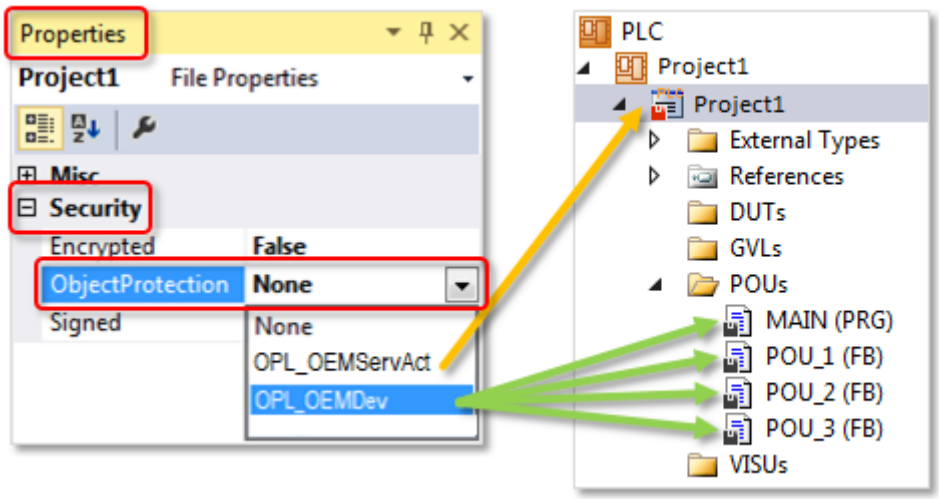
这里只需要对 PLC 项目的根用户进行特殊的权限配置，因此需要自定义对象保护级别。我们称之为 OPL_OEMServAct：

Groups	Group Rights: Project: Load Unsigned Project Files	SaveAs Project Files	Sign Project Files	Encrypt Project Files	Decrypt Project Files	Change Project Files	Activate Configuration	Security Settings	User DB Management	I/O Management	License Management	Object Protection Levels: OPL_OEMDev: View	Delete	Modify	A/R Childs	OPL_OEMService: View	Delete	Modify	A/R Childs	OPL_OEMServiceEdit: View	Delete	Modify	A/R Childs
GRP_Guest																							
GRP_OEMDev	x	x	x	x	x	x	x	x				x	x	x	x	x	x	x	x	x	x	x	x
GRP_Administrators									x														
GRP_OEMService			x	x	x	x	x									x				x		x	

不同于示例 2，GRP_OEMService 组只有修改权限，而没有查看权限。“查看”不包含在“修改”权限中。

Visual Studio 要求对项目文件的“修改”权限，因为激活时会进行修改。

PLC 项目根被赋予 OPL_OEMServAct 对象保护级别。



然而，由于这个属性会传递给根下面的项目组件（除非进行了明确的单独设置），可能必须将根以下的项目组件逐个手动切换到另一对象保护级别。在这种情况下，就不能使用便利的 PLC 根属性继承功能了。

有关此的文档

RightsOverview_TcSoftwareProtection.zip (Resources/zip/9007208137629963.zip)

5.6.4.2 创建和编辑用户

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

至少一个用户拥有管理员权限

为了对数据库进行更改，至少必须有一个数据库用户是管理员组成员。因此，必须创建至少一个拥有管理员权限的用户。

创建用户数据库时定义的“数据库管理员”，专门用于签署数据库。这个账号不能用于登录或修改数据库。

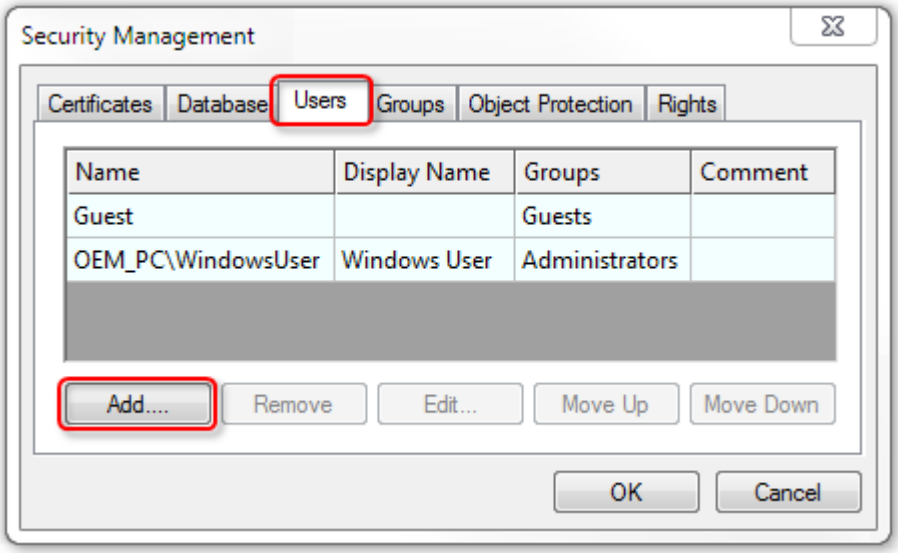
创建和编辑用户

在软件保护配置器的 **Users（用户）** 选项卡中，可修改现有用户设置或创建新用户。

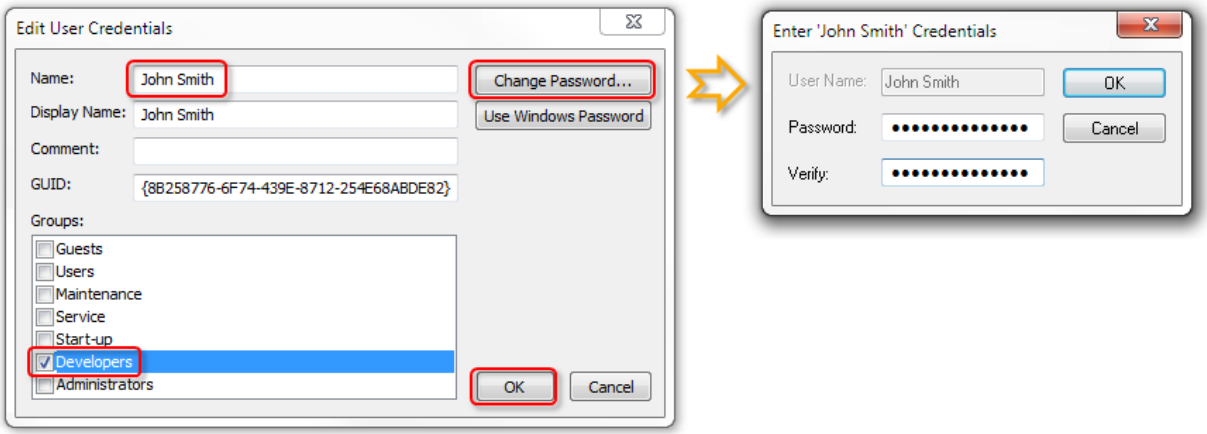
✓ 只有在没有项目打开时，才能创建或编辑用户数据库。关闭所有打开的项目。

✓ 打开软件保护配置器 [▶ 10]。

1. 选择 **Users（用户）** 选项卡。



2. 点击 **Add（添加）** 添加新用户。
   ⇨ 打开**Edit User Credentials（编辑用户凭证）** 对话框。
3. 指定用户 **name（名称）**，并勾选相应（**Groups（组）**）复选框，将用户分配到用户组。
4. Windows 账号的身份验证可通过 Windows 自动完成。对于其他用户需指定特定的用户密码。首先，点击 **Change Password（更改密码）**。
   ⇨ 密码设置对话框打开。
5. 设置用户密码后，重新输入并确认。
6. 选择 **OK（确认）** 关闭对话框。



   ⇨ 新用户出现在列表中。
7. 在列表中选择用户，并点击 **Edit（编辑）**，可进行编辑。
8. 点击 **OK**，关闭 **Edit User Credentials（编辑用户凭证）** 对话框。

⇨ 这样就在系统中完成了用户创建。

从 Build 4024.8 版本开始：

也可以在“扩展文件 [▶ 44]”中创建用户。详见此处 [▶ 38]。

在保存并签署用户数据库后，修改才能最终被确认并生效。

5.6.4.3 创建和编辑用户组

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

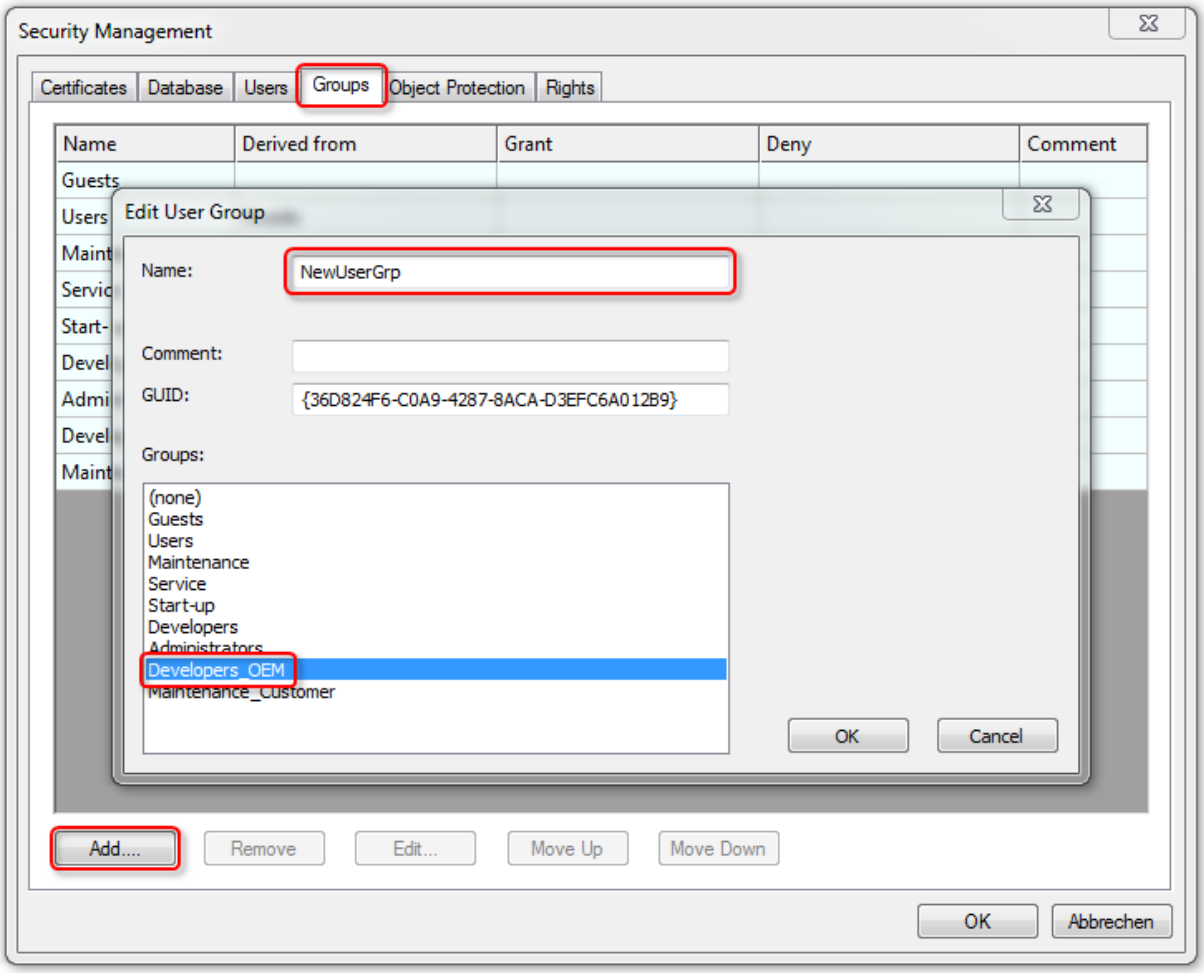
创建和编辑用户组

在软件保护配置器的 **Groups（组）** 选项卡中，可修改现有用户组的基本设置或创建新的用户组。

注意：分配给用户组的权限在“Rights（权限）”选项卡中修改。具体过程见下节 [▶ 60]。

✓ 打开软件保护配置器 [▶ 10]。

1. 选择 **Groups（组）** 选项卡。



2. 点击 **Add（添加）** 创建新的用户组。
   ⇨ **Edit User Group（编辑用户组）** 对话框打开。
3. 输入组名（**Name（名称）**）。
4. 如果该组要继承另一个组的权限，在 **Groups（组）** 中选择相应的组。
5. 选择 **OK（确认）** 关闭对话框。
   ⇨ 新的用户组出现在列表中。
6. 在列表中选择用户组，并点击 **Edit（编辑）**，可进行编辑。
7. 点击 **OK**，关闭 **Edit User Credentials（编辑用户组）** 对话框。

⇨ 这样就在系统中创建好了用户组。

在保存并签署用户数据库后，修改才能最终被确认并生效。

在 **Rights（权限）** 选项卡中，可以为用户组分配权限。详情请参见定制用户组权限 [▶ 60]部分。

5.6.4.4 修改用户组的访问权限

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

在软件保护配置器的 **Rights（权限）** 选项卡中，可对用户组权限进行管理。

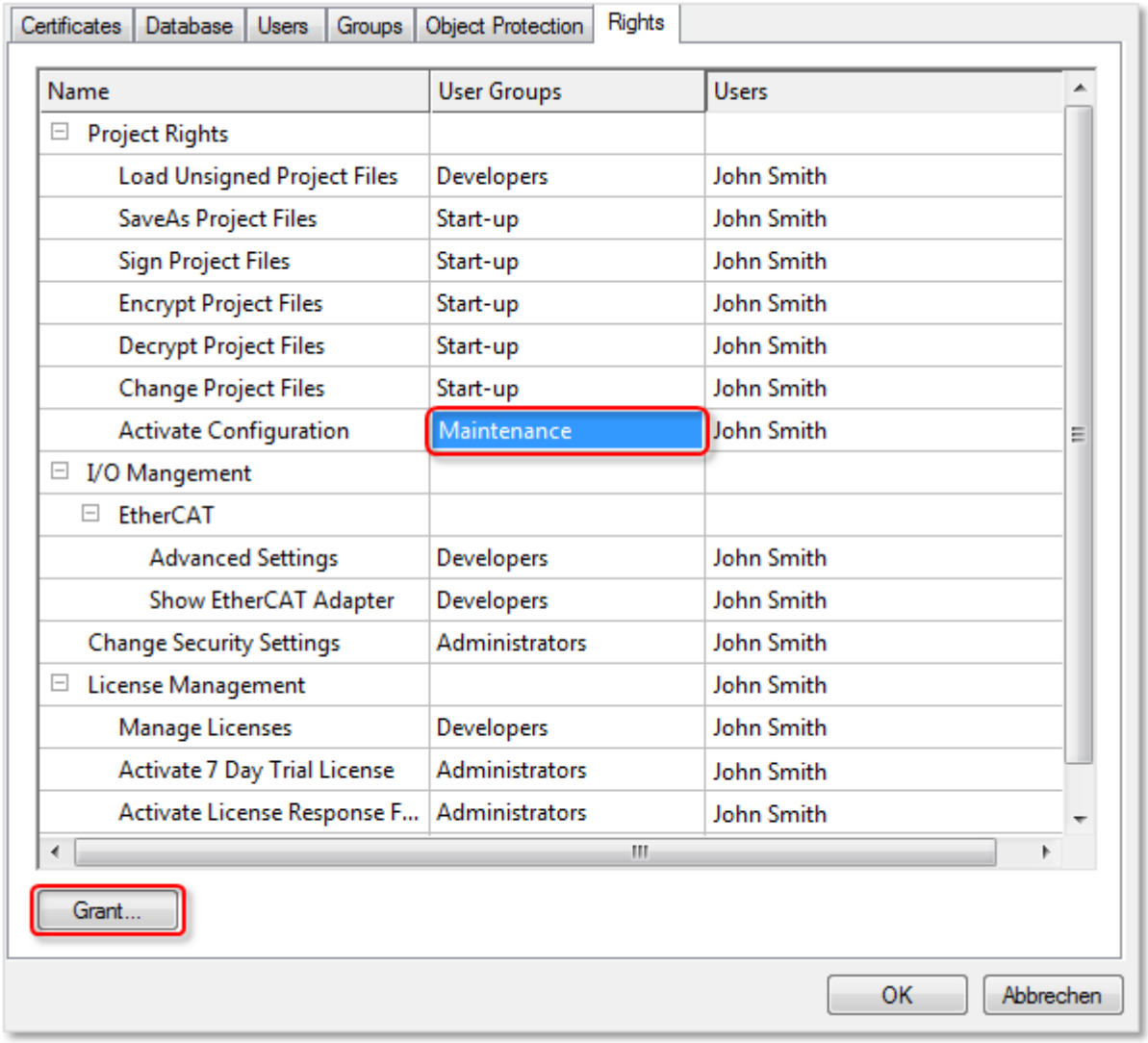
下载链接：组权限和对象保护级别规划表

关于组权限和访问权限群组（对象保护级别）的简单规划，点击https://infosys.beckhoff.com/content/1033/tc3_security_management/Resources/zip/9007208137629963.zip下载 Excel 表格。

✓ 只有在没有项目打开时，才能创建或编辑用户数据库。关闭所有打开的项目。

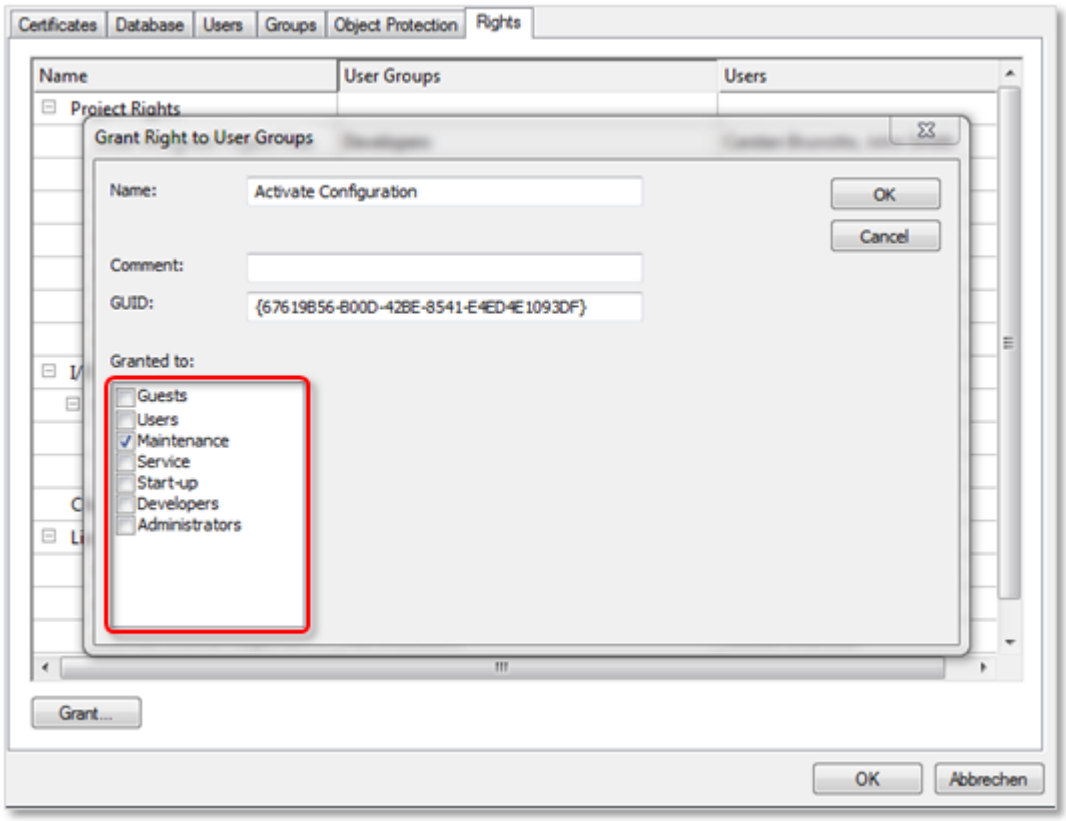
✓ 打开软件保护配置器 [▶ 10]。

1. 选择 **Rights（权限）** 选项卡。
2. 在 **UserGroups（用户组）** 列中，标记所需的权限行，然后点击 **Grant（授权）** 按钮。



⇨ **Grant Right to User Groups（用户组授权）** 对话框打开。

3. 使用复选框选择应当分配该权限的用户组。



4. 点击 **OK（确认）**。

⇨ 修改已应用（暂时地）。

在保存并签署用户数据库后，修改才能最终被确认并生效。

5.6.4.5 创建和编辑访问权限群组（对象保护级别）

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

下载链接：组权限和对象保护级别规划表

关于组权限和访问权限群组（对象保护级别）的简单规划，点击https://infosys.beckhoff.com/content/1033/tc3_security_management/Resources/zip/9007208137629963.zip下载 Excel 表格。

✓ 只有在没有项目打开时，才能创建或编辑用户数据库。关闭所有打开的项目。

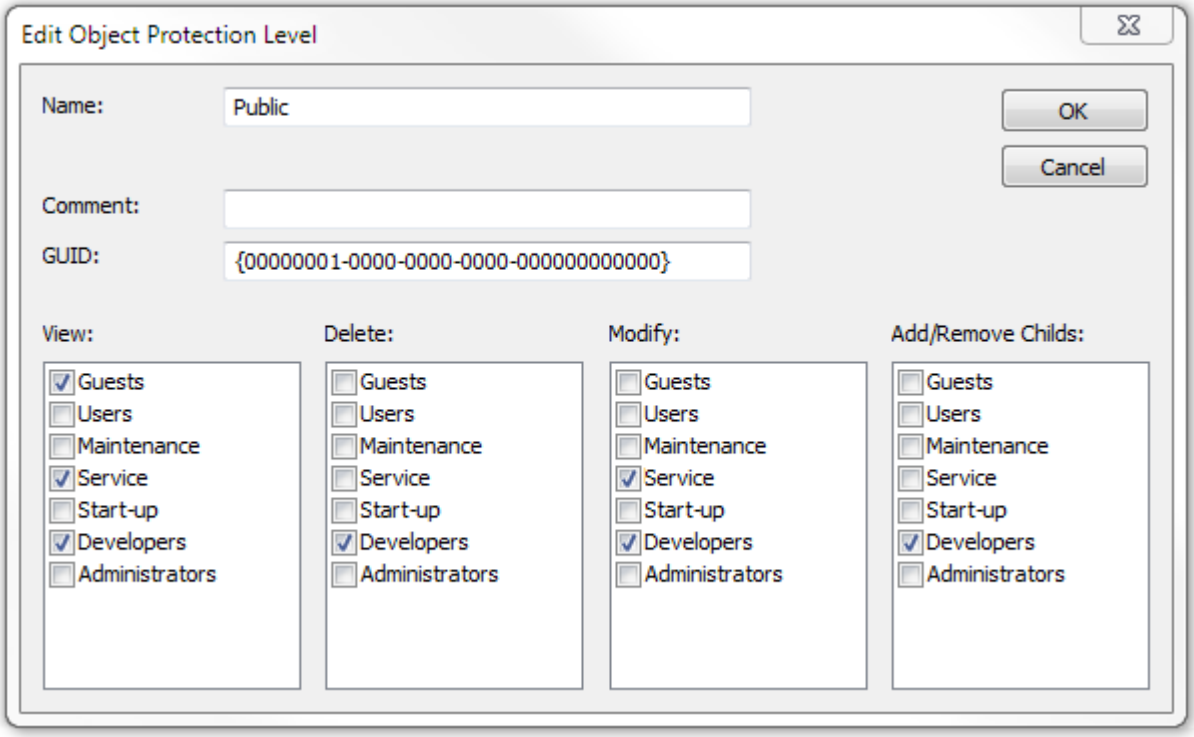
✓ 打开软件保护配置器 [▶ 10]。

1. 选择 **Object Protection（对象保护）** 选项卡。
2. 点击 **Add（添加）**。

⇨ **Edit Object Protection Level（对象保护级别）** 对话框打开。

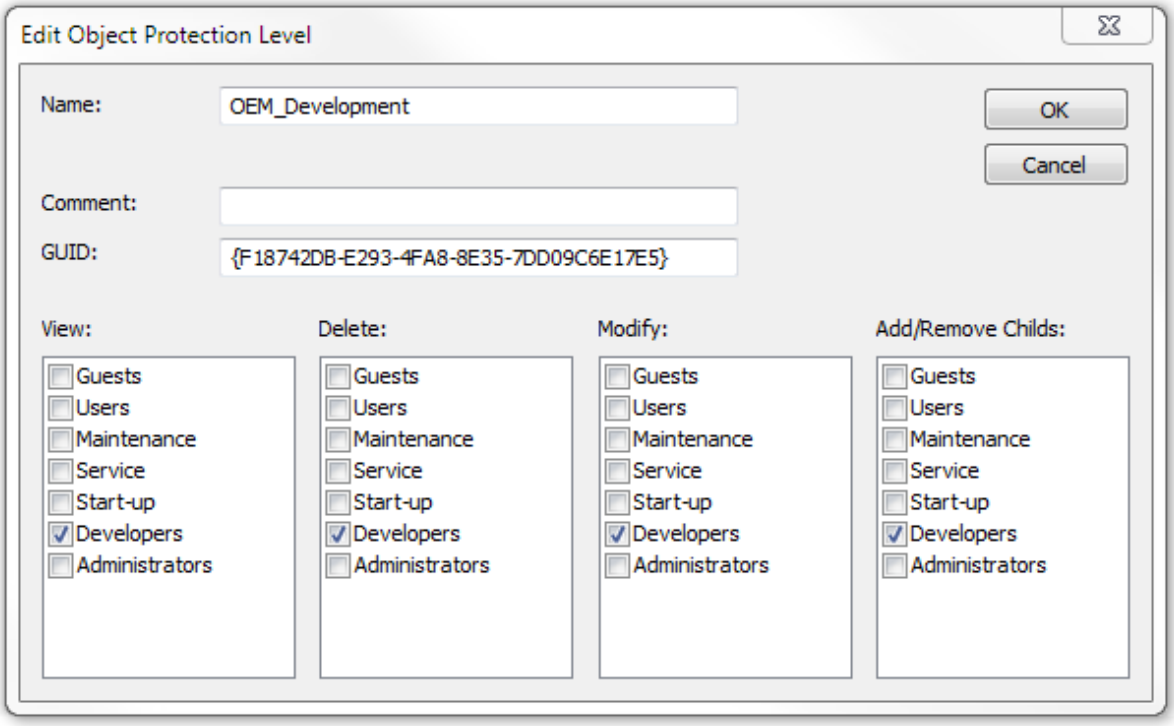
3. 勾选相应的复选框，为该对象保护级别下定义的所有组分配个人用户权限。

   以下示例为“公共”对象保护级别的定义：



- “访客”用户组可读取该对象保护级别的 TwinCAT 对象，但不能进行修改。
- “服务”用户组可读取和修改该对象保护级别的 TwinCAT 对象，但不能删除。
- “开发人员”用户组有完全访问权限。

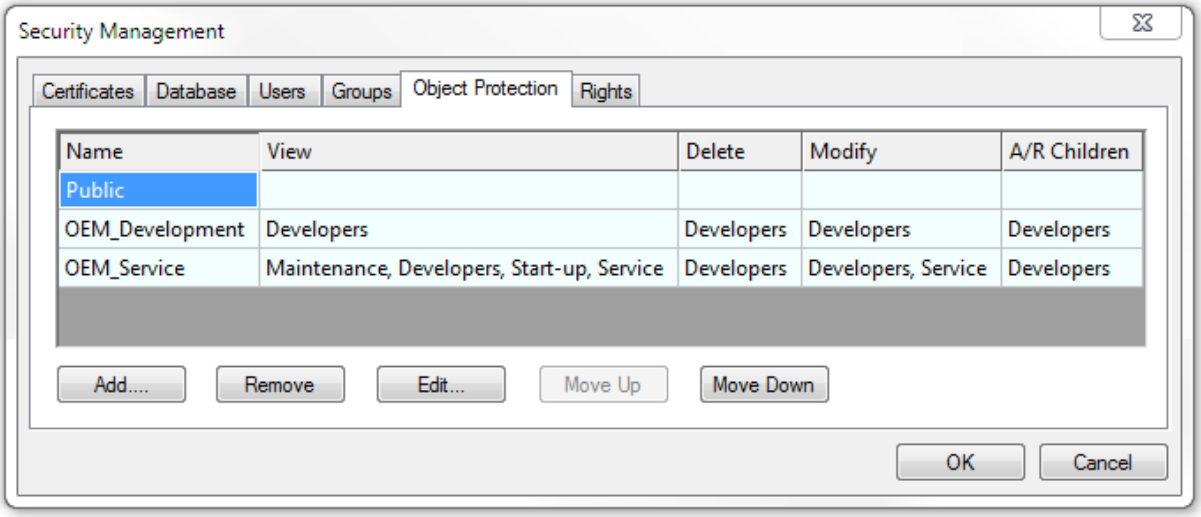
在下述示例中，只有“开发人员”用户组能访问 TwinCAT 对象。其他用户组没有任何权限。



4. 选择 **OK（确认）** 确认对话框。

⇨ 在系统中创建的带用户权限的对象保护级别，在软件保护配置器 **Object Protection（对象保护）** 选项卡概览中显示。

5. 为对象保护级别中的其他用户组分配相应的权限。
6. 如需编辑对象保护级别，选中相应的列并点击 **Edit（编辑）**。



7. 如需删除对象保护级别，点击 **Remove（删除）**。
8. 如需改变概览中所选对象保护级别的位置，点击 **Move up（上移）** or **Move down（下移）**。

在保存并签署用户数据库后，修改才能最终被确认并生效。

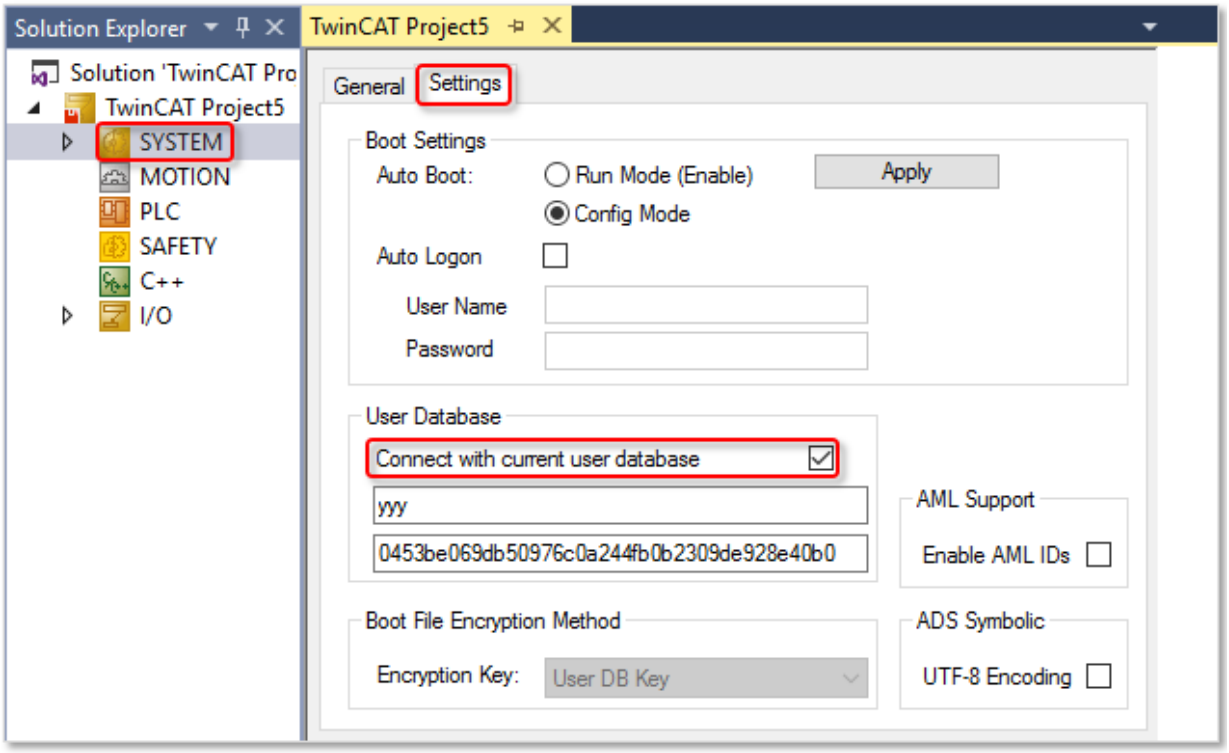
5.7 将用户数据库与项目关联

开始时，项目必须手动关联到用户数据库。与数据库的关联信息将被存储在项目中。

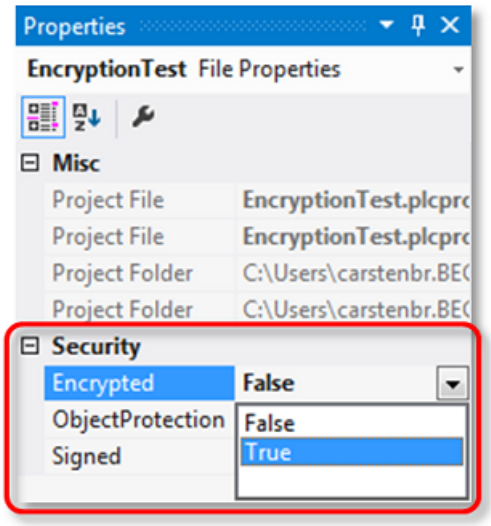
✓ 在关联数据库之前，请务必进行项目备份。
✓ 用户数据库已创建并激活。打开TwinCAT 项目。

1. 在 TwinCAT 项目中，双击 SYSTEM 节点，打开系统设置。
2. **Settings（设置）** 选项卡打开。

3. 在 **User Database（用户数据库）** 区，选中 **Connect with current user database（关联当前的用户数据库）** 复选框。



⇨ 项目已与用户数据库关联。在项目组件 **Properties（属性）** 中，**Security（安全）** 区变成可见。



5.8 分配项目用户访问权限

下载链接：组权限和对象保护级别规划表

关于组权限和访问权限群组（对象保护级别）的简单规划，点击https://infosys.beckhoff.com/content/1033/tc3_security_management/Resources/zip/9007208137629963.zip下载 Excel 表格。

可以将创建的对象保护级别 [▶ 61]分配给 TwinCAT 对象，例如 PLC 项目。

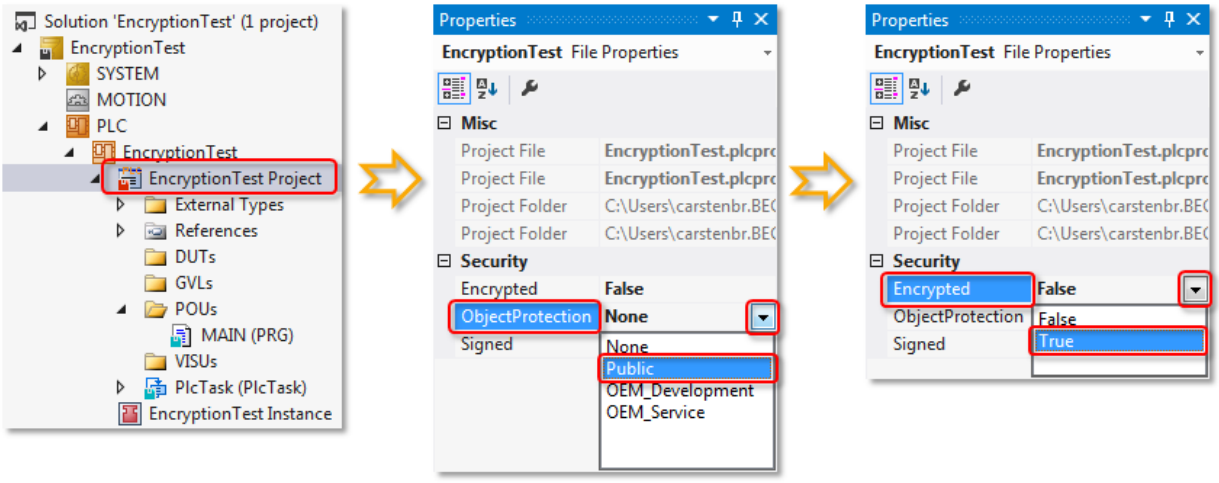
✓ 访问授权组已定义。

✓ 项目已经与用户数据库关联。

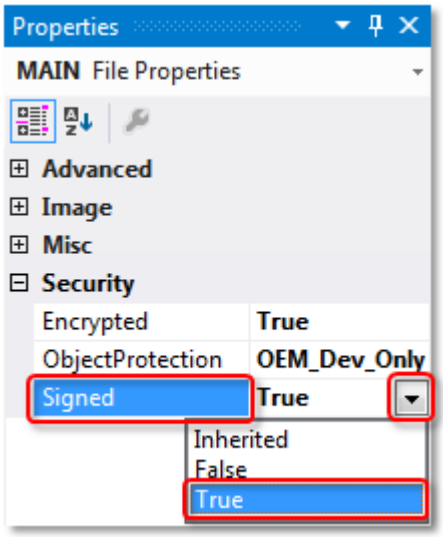
1. 在解决方案资源管理器的 PLC 项目树中，选择 PLC 对象。

⇨ Properties（属性）视图已更新。（如果 Properties（属性）视图未打开，可在 View（视图）菜单下选择 Properties Window（属性窗口）命令打开视图）。

2. 在 Security（安全）类别中的 Object Protection（对象保护）属性下拉列表中，选择所需的对象保护级别。

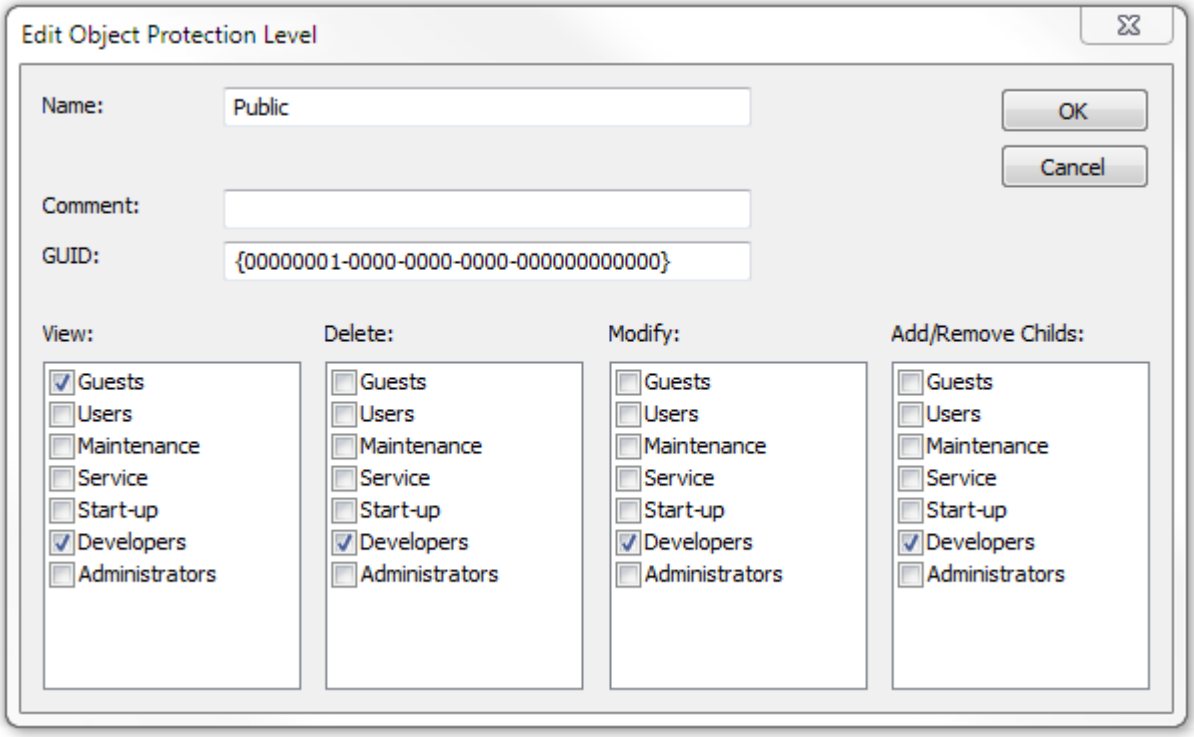


3. 然后在下拉列表中，将 Encrypted（加密）属性设为 TRUE（真）。这是个重要设置，用于防止访问源代码，这是一种系统层面的保护。
4. 然后在下拉列表中，将 Signed（签名）属性设为 TRUE（真）。这是个重要设置，用于防止未经授权时，不通过TwinCAT软件，而是在系统层面直接将对象文件替换为其它同名文件。



⇨ 现在，对象保护级别中指定的用户组就可以访问 PLC 项目了。保存 PLC 项目以使设置生效。

示例中“公共”对象保护级别：

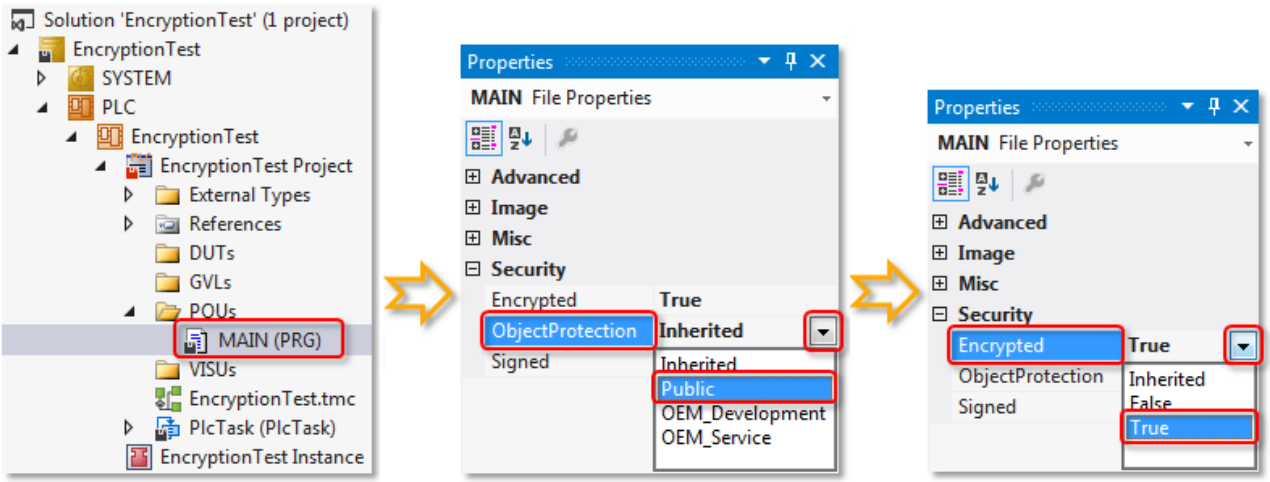


- “访客”用户组对 PLC 项目有只读权限。
- “开发人员”用户组有完全访问权限。

（示例项目中未使用其他用户组，因此未定义其访问权限。）

如果 SPS 对象的子元素有 **Object Protection Level（对象保护级别）** 和 **Encryption（加密）** 属性，PLC 项目树中的根对象的访问权限会自动传递给它们。

另外，还可为每个子元素单独分配对象保护级别和加密属性。这些可在子元素属性中设置。



此处也必须在下拉列表中将 **Encrypted（加密）** 和 **Signed（签名）** 属性设为 TRUE（真）。这样做的目的首先是为了防止通过系统层面的方式（如使用记事本直接打开程序文件）来访问源代码；其次是为了防止在未经授权的情况下将对象文件替换为同名文件。

5.9 用户数据库的分发与交换

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

使用用户数据库时，请注意以下几点：

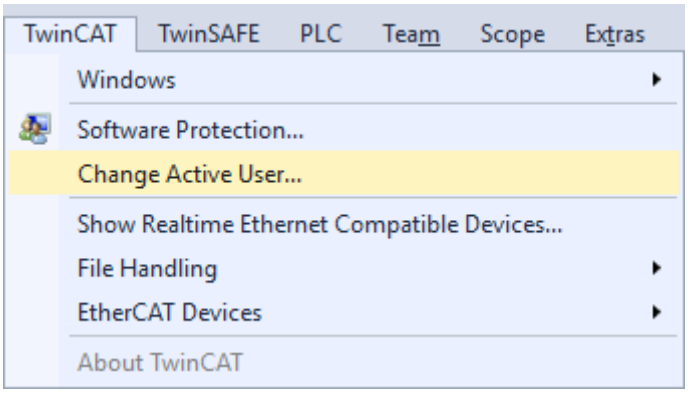
- 在当前的 TwinCAT 3 版本中，用户数据库必须保存在 *c:\TwinCAT\3.1\CustomConfig\UserDBs* 目录中。
- 用户数据库文件可以直接复制和粘贴。
- 在创建用户数据库时，会同时生成一对一的用户数据库密钥，用于准确识别数据库。
- 与用户数据库关联的项目，只能用名称和密钥都相同的用户数据库才能打开。
- 对用户数据库内容进行修改不会影响密钥（密钥只在创建用户数据库时生成一次）。因此，原则上你可以使用几个不同版本的用户数据库。例如：不同于目标控制器上的最终用户版本，用户数据库的“内部”版本可包含其他用户账号。最终客户只能看到指定的可用账号。相比“内部”开发环境，您可以对交付计算机上的可用访问选项进行严格限制。
- 创建用户数据库后，使用用户数据库时无需 OEM 证书。
- 用户数据库的修改必须由用户数据库的（签名）管理员签名。修改用户数据库后，在退出软件保护配置器时，会自动跳出相应的询问。

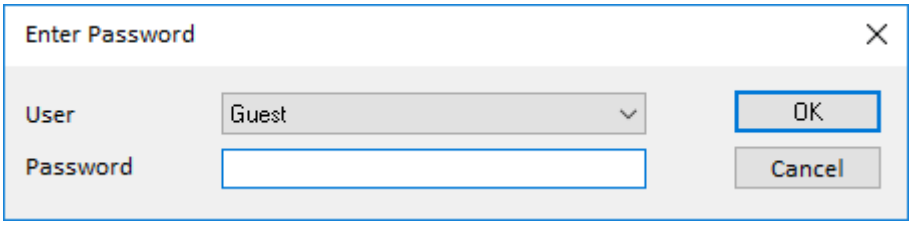
6 登录并选择用户账号

项目打开时，无法修改用户数据库设置

修改用户数据库设置时，不能打开任何项目。

可过工具栏或主菜单选项 **TwinCAT -> Change Active User（切换当前用户）** 切换用户帐号：





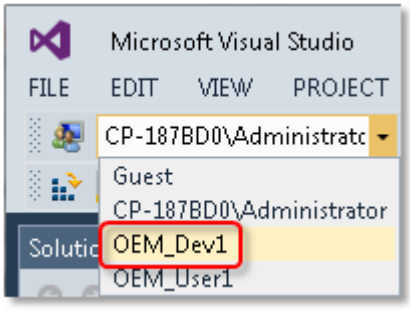
只有在没有项目打开时，才可以切换用户。

6.1 TwinCAT 3 4022 版本

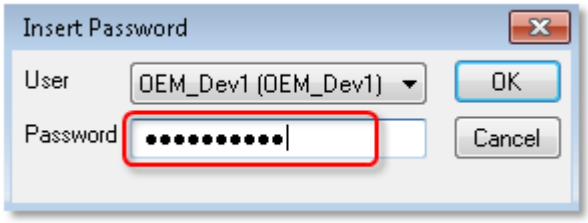
您可以直接在安全管理工具栏中的选择框中，选择用户账号。

✓ 打开 Security Management toolbar（安全管理工具栏）[▶ 10]。

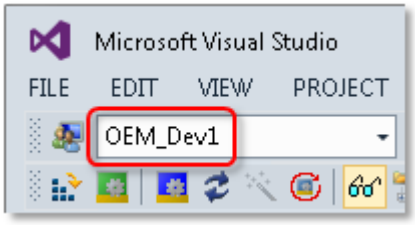
1. 从下拉列表中选择用户账号。



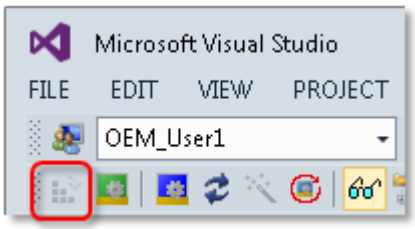
2. 如果用户登录需要密码，会出现一个对话框以供输入密码。按照提示输入密码。如果通过 Windows 用户账号进行身份验证，则不要求输入密码，因为在 Windows 系统登录时已经验证过了。



⇨ 安全管理工具栏显示选中的用户账号。



根据用户账号权限的不同，TwinCAT 的某些菜单选项可能变灰，即被禁用。



7 设置 OEM 应用软件的基本保护

7.1 加密

加密前先进行未加密的备份！

在加密项目之前：一定要对未加密状态的项目进行备份！

TwinCAT 3 使用 256 位 AES 加密，并对 OEM 证书采用私钥和公钥程序。

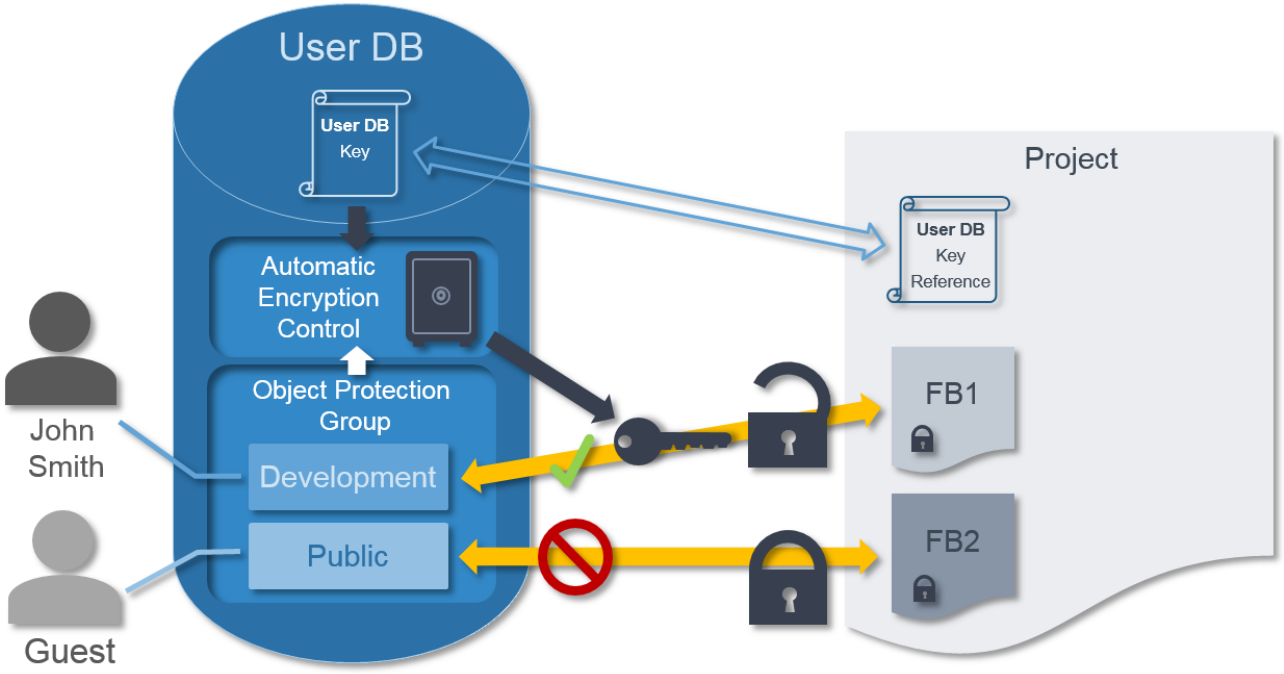
以下对象可以在 TwinCAT 中进行加密：

- 源代码
- 项目文件
- 根项目

仅对项目文件进行加密的安全保护

在任何情况下，使用加密时始终必须对项目文件进行加密，因为其中包含关于项目属性的重要信息。如果这一信息受到操纵篡改，会导致无法对源代码安全加密。

用于加密的密钥保存在用户数据库中。因此，相应的用户数据库必须一直保存在用于编程配置的计算机上。(目录：*C:\Twincat\3.1\CustomConfig\userDBs*)



解密根项目（= 二进制文件）不需要用户数据库。

系统要求

操作系统：

- Windows 7 及以上版本（或对应的嵌入式版本），以便能够使用所有应用软件保护功能。Windows XP 和 Windows CE（Windows Embedded Compact）不支持启动文件的加密或 OEM 授权。

TwinCAT 版本：

- 所述功能要求 TwinCAT 3.1 build 4022 及以上版本。

只有使用最新版本的 TwinCAT 3，才会获得可靠的保护。

为确保获得可靠的保护（例如安全加密），请始终使用最新版本的TwinCAT 3。这可以提供最高的安全性。

至少应使用 TwinCAT 3.1 Build 4024.x。
鉴于安全因素，请勿使用旧版本！

7.1.1 源代码加密

加密前先进行未加密的备份！

在加密项目之前：一定要对未加密状态的项目进行备份！

访问加密对象受到对象保护级别的控制。因此，除了加密之外，还必须为 TwinCAT 3 对象设置必要的对象保护级别。对象保护级别和加密可以在相应的 TwinCAT 对象（例如 PLC 项目）属性中轻松分配。该项目必须与用户数据库链接。加密和对象保护级别的规范详见 分配项目用户访问权限 [▶ 64] 章节。保存项目，以便应用这些设置。

7.1.2 项目文件加密

仅对项目文件进行加密的安全保护

在任何情况下，使用加密时始终必须对项目文件进行加密，因为其中包含关于项目属性的重要信息。如果这一信息受到操纵篡改，会导致无法对源代码安全加密。

加密前先进行未加密的备份！

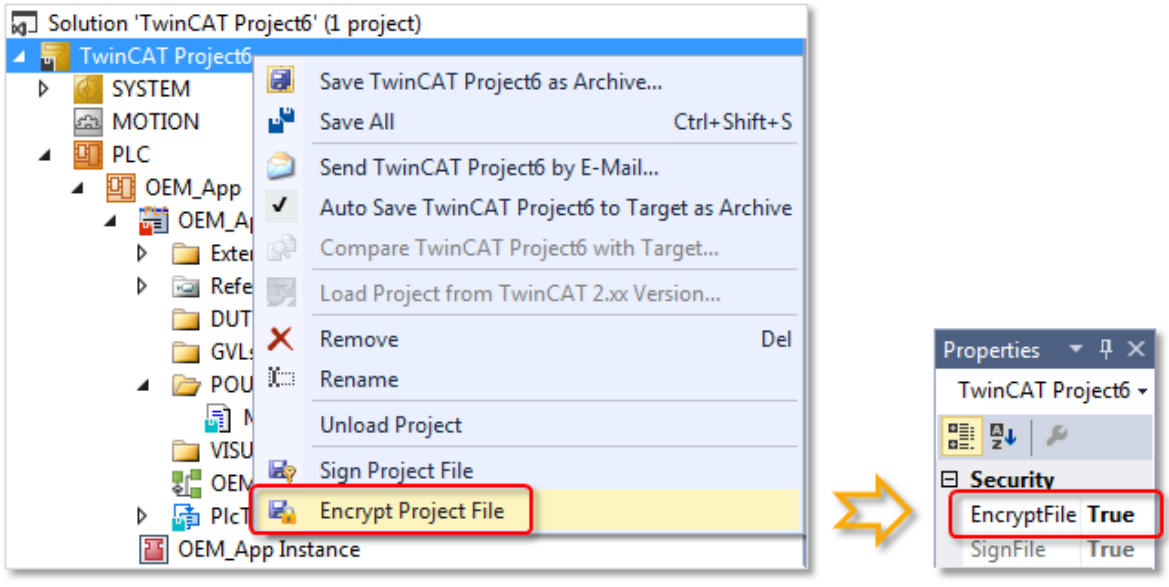
在加密项目之前：一定要对未加密状态的项目进行备份！

项目文件的加密通过 TwinCAT 项目节点进行设置。

✓ 该项目与一个用户数据库链接。

1. 在解决方案资源管理器的项目树中选择 TwinCAT 项目节点。
2. 在上下文菜单中选择**加密项目文件**命令。

   ⇨ 在Properties（属性）视图中，Security（安全）类别中的EncryptFile（加密文件）属性的值设置为TRUE。



⇨ 项目文件已加密。其中包含关于解决方案组成部分的信息。在设置加密时，项目文件本身现在也已被加密。加密不会继承给项目中包含的组件。必须为项目的所有（主要）组件单独设置加密。

仅对 TwinCAT 3.1 Build 4024.0 有效：创建一个用户数据库需要加密版本 1

在 TwinCAT Build4024.0 版本中，用于 TwinCAT 软件保护的用户数据库 [▶ 31]只能用带有加密版本 1 的 OEM 证书来创建！

7.1.3 启动项目的加密

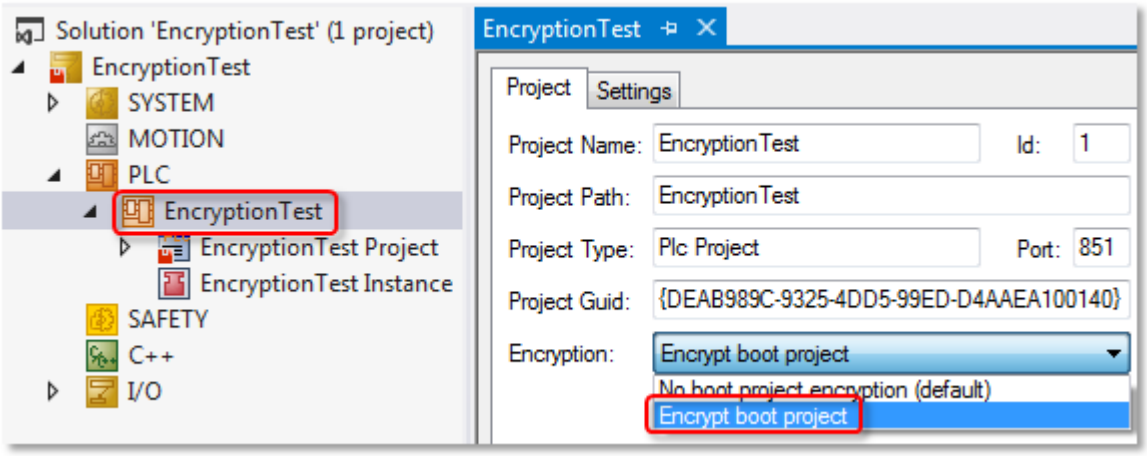
要求：目标系统上有最新版本的 Windows 或 TC/BSD®

旧操作系统不支持加密，例如 Windows NT、Windows CE / Windows Embedded Compact。

根项目的加密在（目标系统上）PLC 项目的根节点中设置。

✓ **TwinCAT Engineering 中选定了一个**用户数据库 [▶ 36]**（并且有效）**。
原因：来自用户数据库的信息被用于加密。
（但该项目不一定要与用户数据库链接。）

1. 双击解决方案资源管理器中 PLC 项目树中的 PLC 项目对象。
   ⇨ PLC 项目设置在编辑器中打开。
2. 在**项目**选项卡上，在**加密**设置的下拉列表中选择**加密根项目**条目。



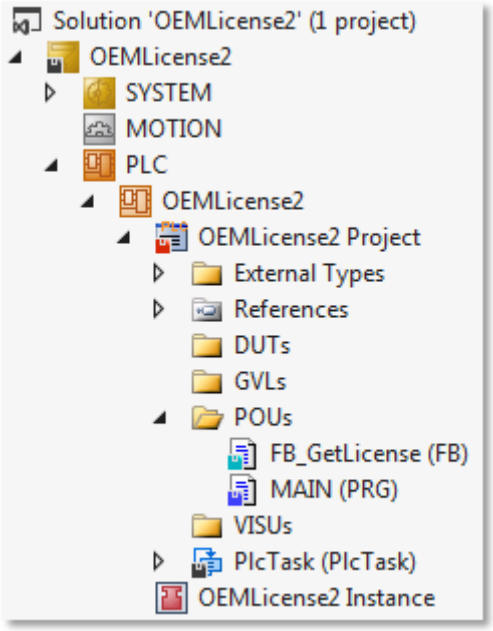
⇨ 当根项目为目标系统激活时，则被加密存储在目标系统上。

解密目标系统上的根项目时，不需要用户数据库或 OEM 证书。

加密的根项目不能以文件级别复制到任何目标系统，因为无法在那里被解密。在选定目标系统的项目激活过程中，目标系统被配置用于解密根项目。

7.1.4 显示对象保护状态

在项目树中，TwinCAT 对象状态由对象图标中的磁盘符号表示。



用于显示TwinCAT 对象状态的功能经扩展后可以用于显示 TwinCAT 对象的保护状态。下表显示了这些符号及其含义。

TwinCAT 对象状态符号

符号	含义
	无更改
	更改未保存
	已签名
	已加密

规则：

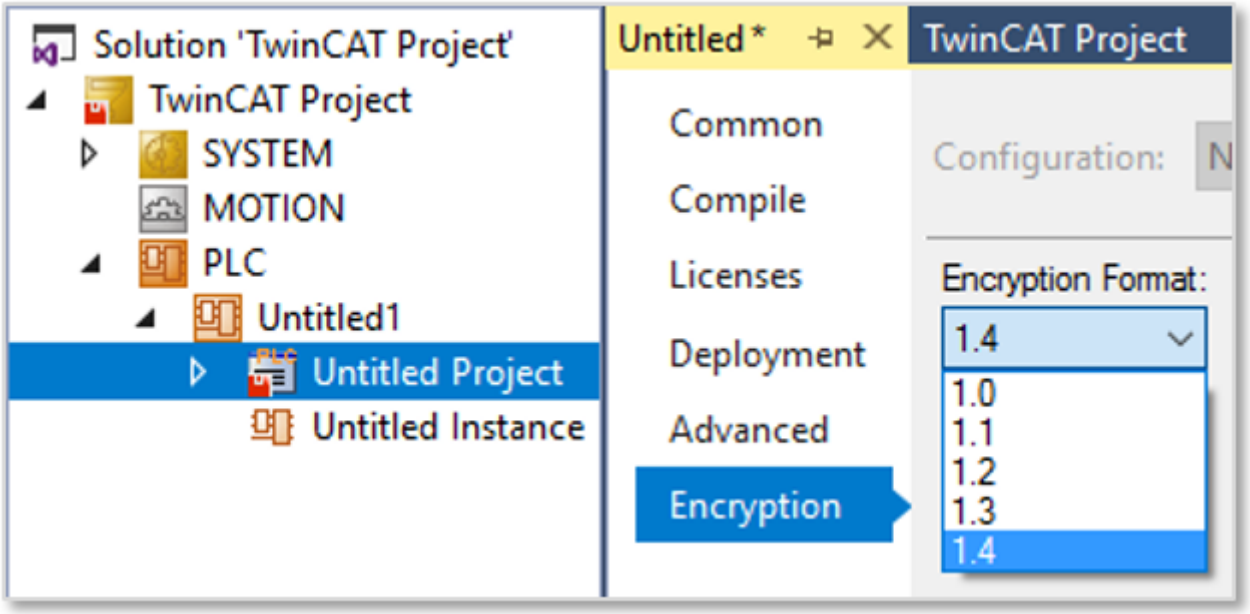
1. 蓝绿色优先于蓝色
2. 红色优先于其他颜色

7.1.5 显示当前加密版本

当前 TwinCAT 版本使用当前加密版本。在本文件创建时，TwinCAT build 4022.x 为 1.4 版本。

之前使用版本为 1.0-1.3 (build 4020.x)。强烈建议不要使用旧的加密版本。请使用最新版本。

当前使用的加密版本可在项目属性中查看：



如果是用 build 4020.x 创建的旧项目，在这里可以设置新的加密版本。

当前的加密版本只在当前的 TwinCAT 3 版本中可用。例如，TwinCAT 3 build 4020.x 版本不支持加密版本 1.4。

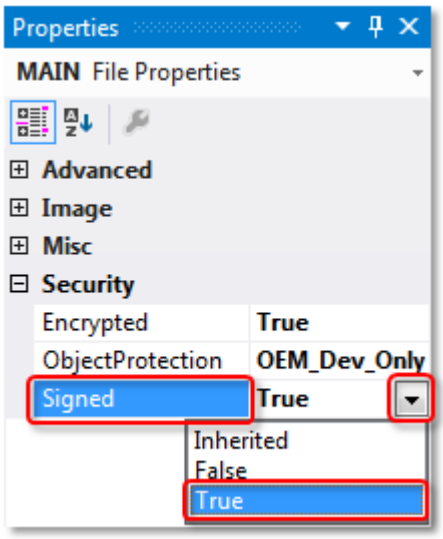
安全加密的前提是使用支持当前加密版本的 TwinCAT!

7.2 签署文件（防止未经授权的更改）

签署项目组件（文件）后，可防止项目组件在未经授权的情况下被替换。

此外，还应签署项目文件，因为它存储了项目组件的签名信息。

如果项目与用户数据库关联，可以在各项目组件的属性中设置签名。在解决方案资源管理器中标记项目组件，并在 **Properties（属性）** 视图中，将 **Signed（签名）** 的属性设为 TRUE（真）。



系统要求

操作系统：

- Windows 7 及以上版本（或对应的嵌入式版本），以便能够使用所有应用软件保护功能。Windows XP 和 Windows CE（Windows Embedded Compact）不支持启动文件的加密或 OEM 授权。

TwinCAT 版本：

- 所述功能要求 TwinCAT 3.1 build 4022 及以上版本。

只有使用最新版本的 TwinCAT 3，才会获得可靠的保护。

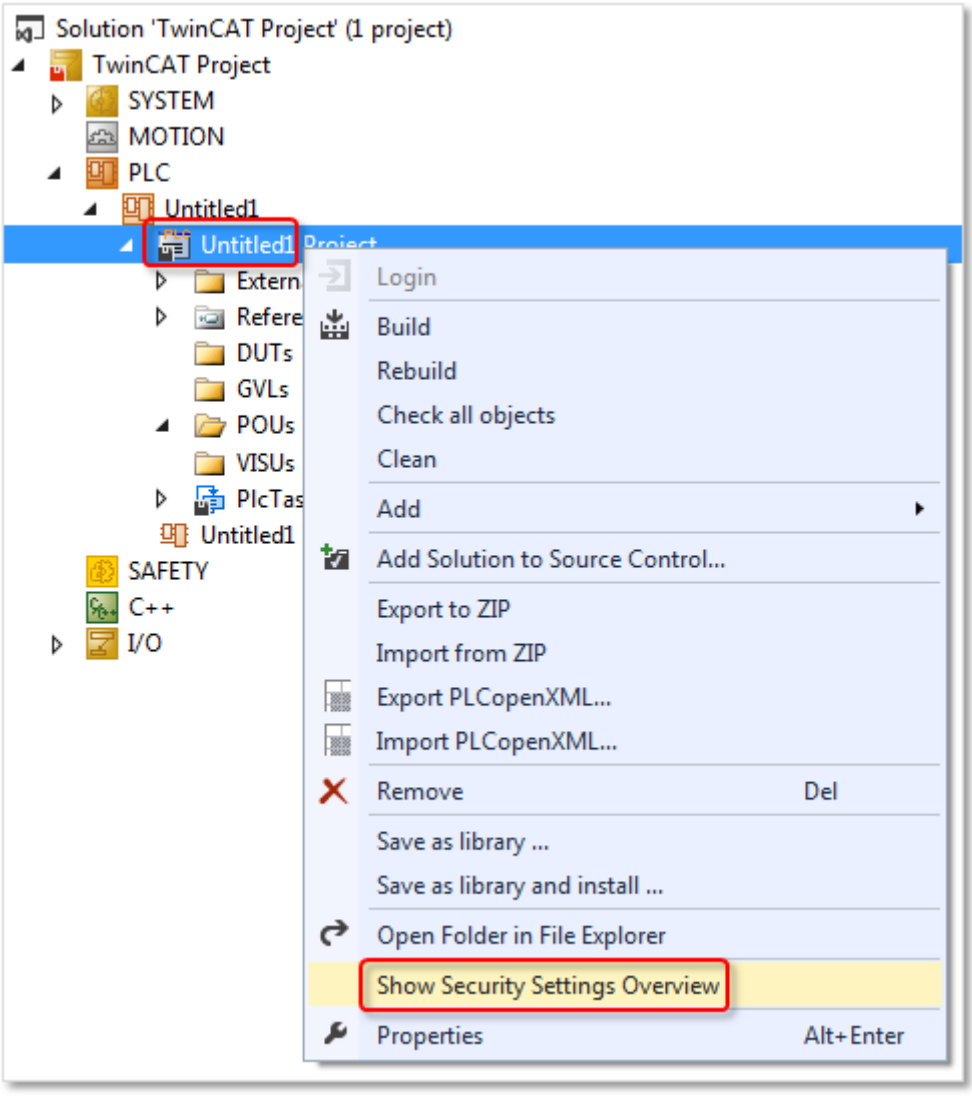
为确保获得可靠的保护（例如安全加密），请始终使用最新版本的TwinCAT 3。这可以提供最高的安全性。

至少应使用 TwinCAT 3.1 Build 4024.x。
鉴于安全因素，请勿使用旧版本！

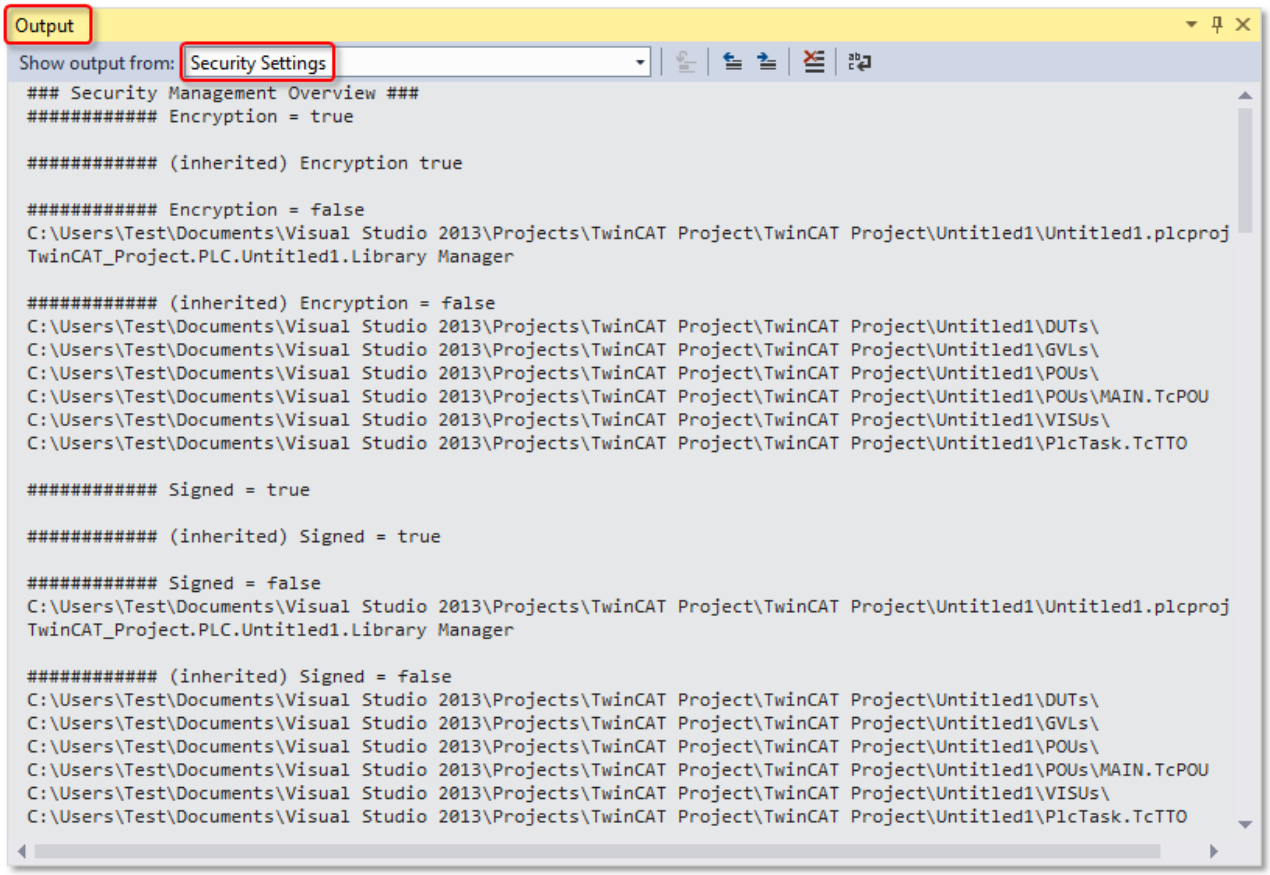
7.3 显示项目软件保护设置概览

可以在TwinCAT3开发环境的窗口中找到应用软件的保护设置。

在解决方案资源管理器中标记 PLC 项目根节点，并在右键弹出的下拉菜单中选择 **Show Security Settings Overview（显示安全设置概览）**命令。



在窗口中显示当前项目的安全设置概览。


Output
Show output from: Security Settings
Security Management Overview
############ Encryption = true
############ (inherited) Encryption true
############ Encryption = false
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\Untitled1.plcproj
TwinCAT_Project.PLC.Untitled1.Library Manager
############ (inherited) Encryption = false
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\DUTs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\GVLs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\POUs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\POUs\MAIN.TcPOU
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\VISUs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\PlcTask.TcTTO
############ Signed = true
############ (inherited) Signed = true
############ Signed = false
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\Untitled1.plcproj
TwinCAT_Project.PLC.Untitled1.Library Manager
############ (inherited) Signed = false
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\DUTs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\GVLs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\POUs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\POUs\MAIN.TcPOU
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\VISUs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\PlcTask.TcTTO

8 发放和使用您自己的 OEM 授权

采用 TwinCAT 3 授权技术，可通过绑定硬件（倍福 IPC 或 TwinCAT 加密狗）来保护 PLC 应用不被克隆。此外，应用程序的附加功能可通过创建“功能授权”来授权给最终用户。

在此您可以获得快速开始使用 [▶ 13]。

系统要求

操作系统：

- 至少需要 Windows 7（或其嵌入式版本），才能使用保护应用软件的所有功能。Windows XP 和 Windows CE（Windows Embedded Compact）不支持启动文件的加密或 OEM 授权。

TC3 PLC Lib Tc2_Utiltities：

- 至少需要使用 TC3 PLC Lib Tc2_Utilities 的 3/3/24 版本，新版本的库提供了各种功能，可以方便处理 TwinCAT 3 授权。对于使用 TwinCAT 3 加密狗的 OEM 应用授权来说，这是必须的。TC3 PLC Lib 包括在 TwinCAT 3.1 Build 4022.16 中。

TwinCAT 版本：

- 上述功能需要 TwinCAT 3.1 build 4024 或更高版本。

只有使用最新版本的 TwinCAT 3，才会获得可靠的保护。

为确保获得可靠的保护（例如安全加密），请始终使用最新版本的TwinCAT 3。这可以提供最高的安全性。

至少应使用 TwinCAT 3.1 Build 4024.x。
鉴于安全因素，请勿使用旧版本！

一般注意事项

使用 OEM 授权时，请确保启动项目已加密！

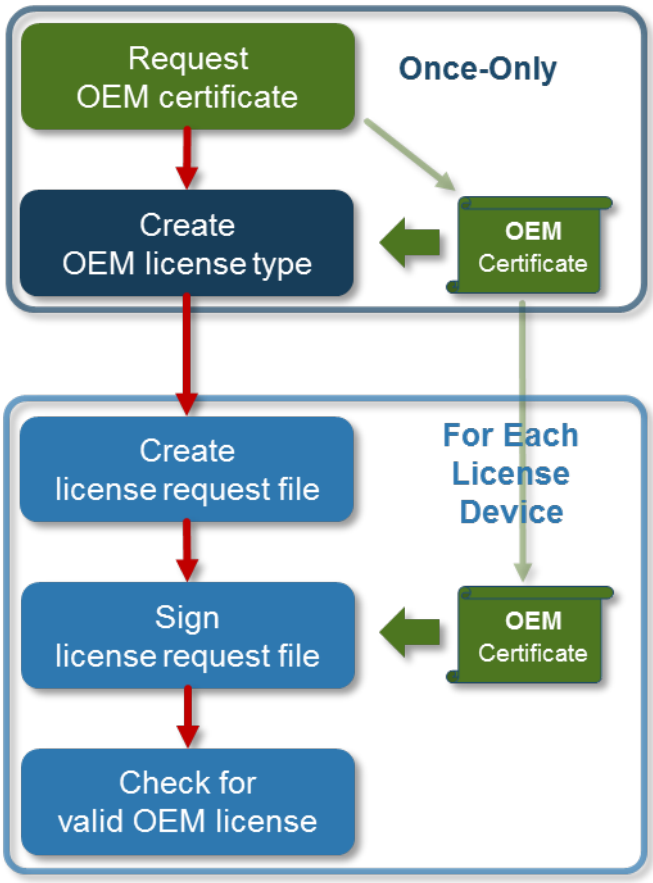
请记住，通过二进制代码的 FB_CheckLicense [▶ 85] 查询的授权码 [▶ 79]很容易被找到，并可通过十六进制编辑器轻松地进行控制。因此，请确保加密启动项目 [▶ 72]（最安全），或尽可能地在源代码中隐藏查询到的授权码。

- 应用程序授权无需用户数据库。
- 授权由 TwinCAT 3 runtime (XAR) 进行验证。因此，必须在 IPC 上安装 TwinCAT 3 runtime。
- 应用程序授权的有效期与 OEM 证书的有效期无关。因此，即使 OEM 证书已失效，应用程序授权仍然有效。
- 如需使用 OEM 应用程序授权，必需使用 TwinCAT 3 加密狗或倍福 IPC。
- 出于安全考虑，对平台级别 >= 90 的 IPC (非倍福 IPC)，必须使用 TwinCAT-3 加密狗作为“授权设备”！

授权过程

授权过程分为以下步骤：

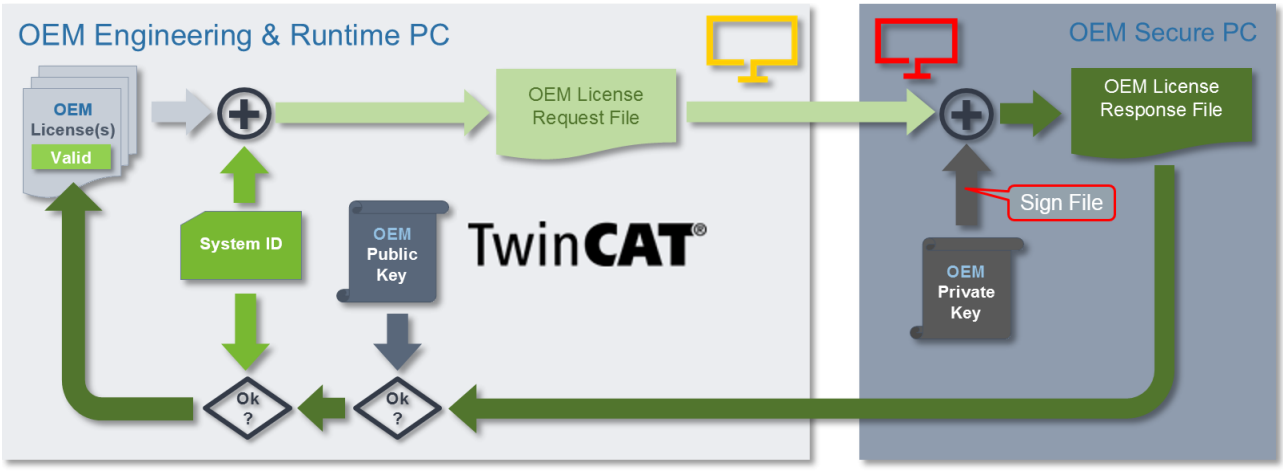
1. 创建通用的授权说明文件。
   授权说明文件用于在授权过程中描述并选择特定的授权类型。它还包含唯一的授权码，用于准确识别授权类型。
2. 为所需的目标系统创建授权申请文件。
3. 用 OEM 证书签署授权申请文件，由此为指定的目标系统创建授权响应文件。分别在目标系统上激活相应的 OEM 应用授权。



授权过程详见以下章节。

8.1 创建 OEM 应用授权

下图为授权过程总览：



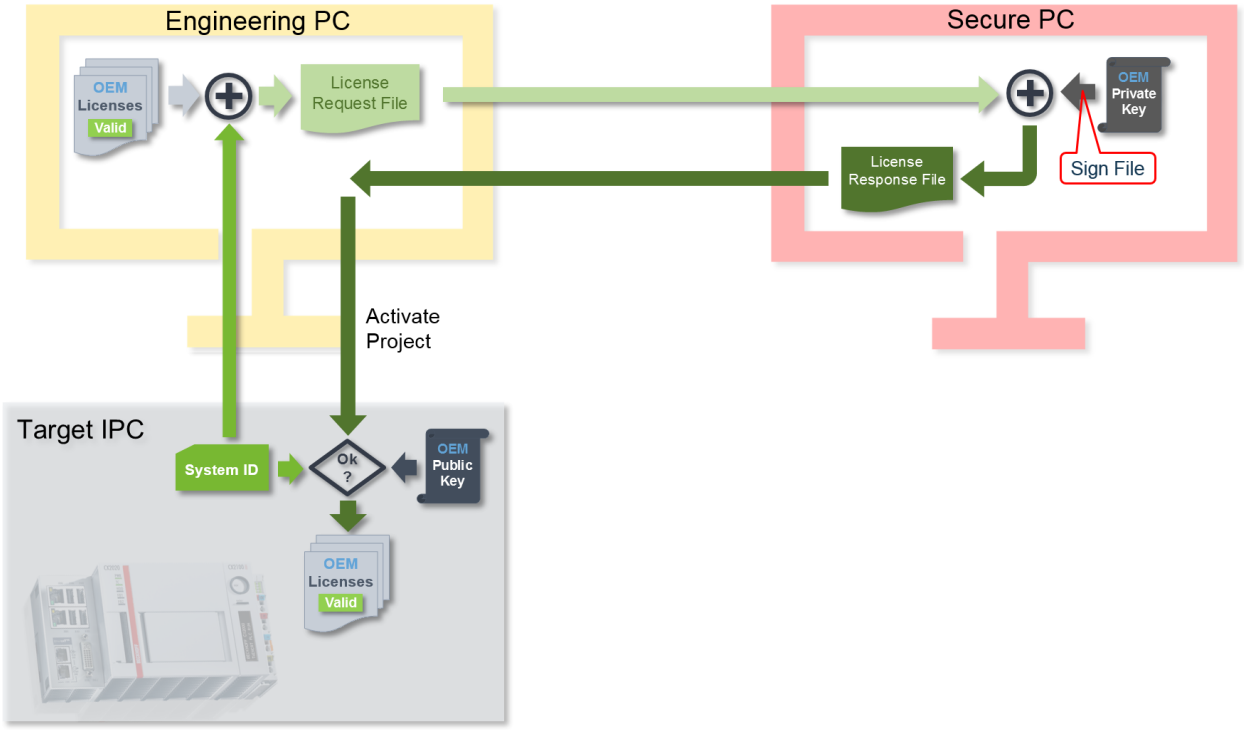
图中左侧的浅灰色框显示创建 TwinCAT 3 授权申请文件，并在 TwinCAT 3 Runtime 中进行验证的过程。

图中右侧的深灰色框显示由倍福授权服务器处理的授权过程。
OEM 通过使用 OEM 专用密钥进行签名，从而完成 OEM 应用授权的发放。换言之，倍福授权服务器并未整合在 OEM 应用授权生成过程中。

OEM 证书只能在安全环境下使用

由于生成 OEM 应用授权需要处理 OEM 证书及其密码，为防止 OEM 专用密钥的密码被恶意软件窃取，该过程必须在安全环境中进行（受保护的计算机）。

如果控制计算机和编程配置用的计算机是互相独立的，授权过程如下所示：



8.1.1 准备 TwinCAT 3 编程环境

默认情况下，TwinCAT 编程环境中没有为生成 OEM 授权进行预配置。

1. 创建以下目录：
   - *c:\TwinCAT\3.1\CustomConfig\Licenses*
   - *c:\TwinCAT\3.1\Components\Base\License*
2. 将“CreateLicense.exe*”工具复制到 *c:\TwinCAT\3.1\Components\Base\License* 目录。如需申请该工具，请发送电子邮件到 tccertificate@beckhoff.com。

8.1.2 创建 OEM 应用授权说明文件

TwinCAT 3 授权的类型参数在 XML 格式的授权说明文件中指定，文件扩展名为 .tmc。

授权说明文件包含：

- 一对一“授权码”，以便可靠识别授权类型
- 一对一 OEM 身份识别码（来自 OEM 证书）
- OEM 名称
- 授权类型
- 订单号
- 接收授权申请文件的另一个电子邮箱

```
<Vendor>
    <Name>SampleOEM Inc</Name>
</Vendor>
<Licenses>
    <License>
        <LicenseId>{CF1A625C-F2EC-477F-9008-65C305079F03}</LicenseId>
        <OemId OemName="SampleOEM Inc" OrderAddress="license@SampleOEM.com">{DB77E273-19F3-C4B6-2A2D-007613D67AA4}</OemId>
        <OrderNo>4711-0815</OrderNo>
        <DisplayName>Sample_License A1</DisplayName>
    </License>
</Licenses>
```

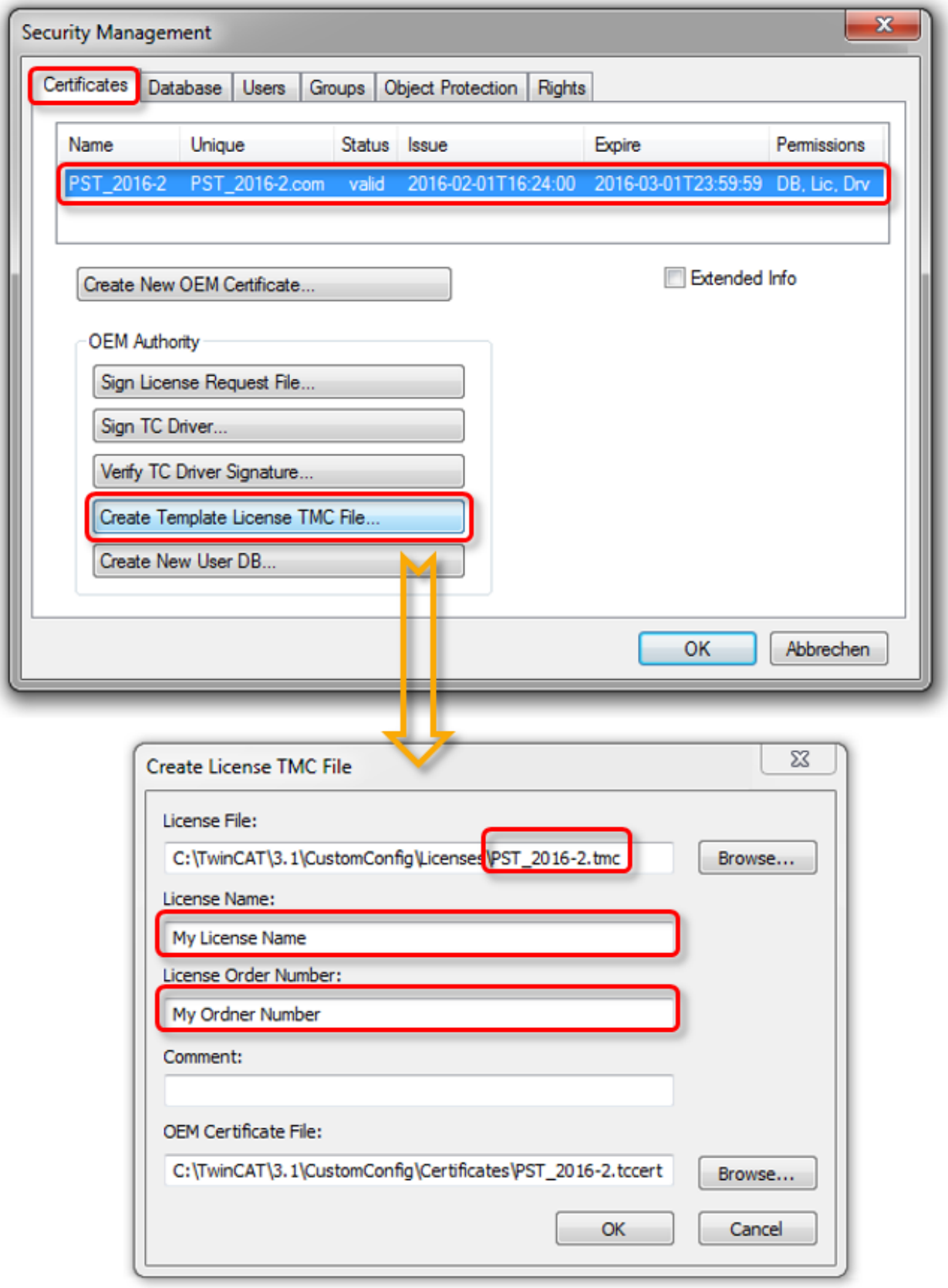
OEM 身份识别码可用于将授权分配给指定的 OEM。只有 OEM 证书上的身份识别码对应的 OEM，才能用该 OEM 证书签署授权并使之生效。

合适的编辑器可打开并修改 OEM 授权说明文件。确保 XML 文件结构未损坏。

创建新的 OEM 授权说明文件

✓ 打开软件保护配置器 [▶ 10]。

1. 在 **Certificates（证书）** 选项卡中，选择相应的 OEM 证书，以创建 OEM 授权说明文件。
2. 点击 **Create Template License TMC File（创建授权说明文件模板）**。
   ⇨ 打开 **Create Licenses TMC File（创建授权说明文件）** 对话框。
3. 输入 OEM 授权说明文件参数：
   - 将授权说明文件保存到 *C:\TwinCAT\3.1\CustomConfig\Licenses* 文件夹，并重启 TwinCAT 3 编程环境。重启后 TwinCAT 3 才能识别授权说明文件。
   - 输入授权名称和订单号。



4. 重启 TwinCAT 3，以便检测新的授权类型。

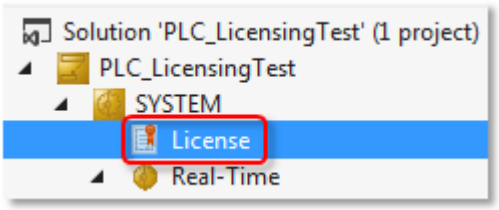
⇨ 授权说明文件已创建。

8.1.3 创建 OEM 应用授权申请文件

用于非倍福 IPC 的 TwinCAT 3 授权

如果使用一个来自非倍福公司的制造商的 IPC (TwinCAT 3 平台级别 >= 90)，则始终需要使用 TwinCAT 3 授权加密狗来授权 TwinCAT 3。

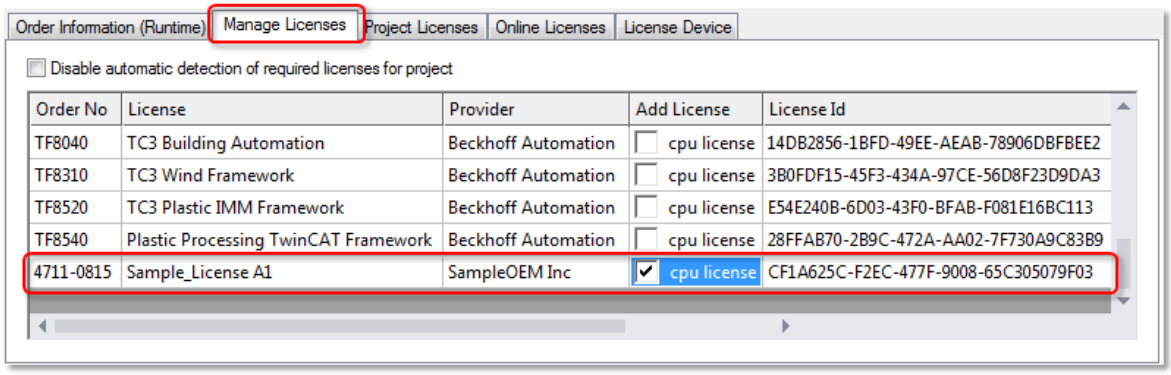
1. 在 TwinCAT 项目树的 SYSTEM 子节点中，双击 **License (授权)**，打开 TwinCAT 3 授权管理器。



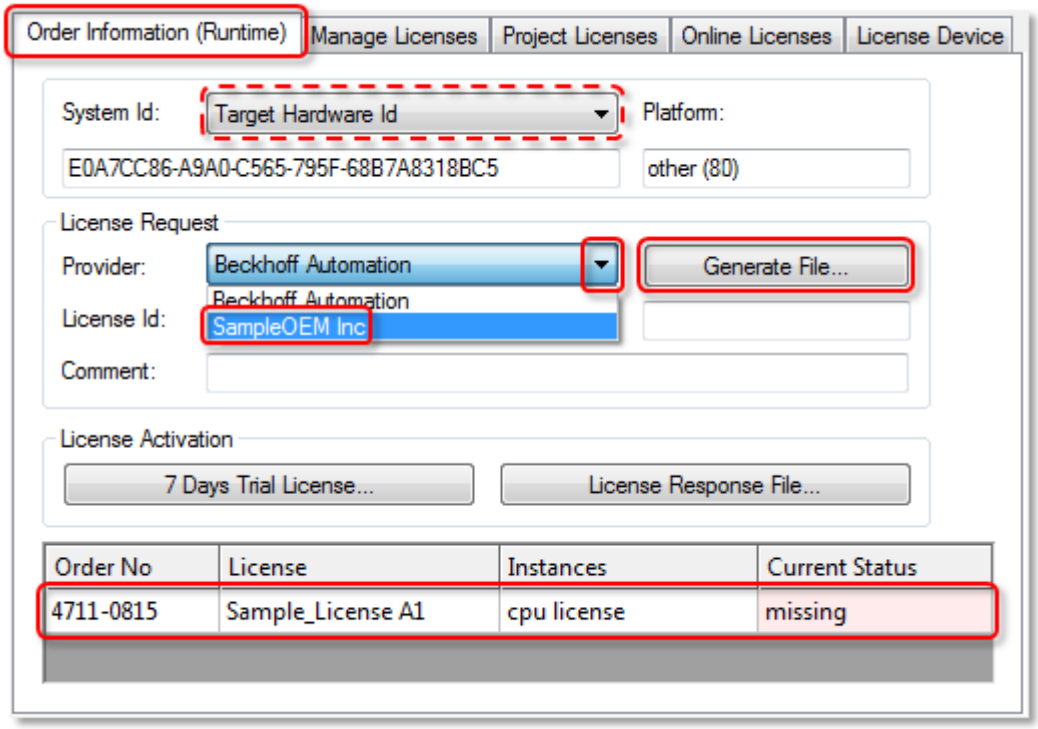
⇨ 在编辑器中打开授权设置。

2. 打开 **Manage Licenses (管理授权)** 选项卡并向下滚动。

⇨ 在列表的最后，可以找到新生成的 OEM 授权。



3. 在复选框中勾选该授权。
4. 打开 **Order Information (订单信息)** 选项卡。



5. 您也可以在 **System ID (系统 ID)** (虚线框) 中，选择 TwinCAT 3 加密狗作为授权硬件。

6. 选择相应的 OEM 作为 **Provider（提供者）**。您不能选择“Beckhoff（倍福）”选项——该选项仅适用于倍福的 TwinCAT 3 授权。
   ⇨ 在窗口底部的列表中，所选的 OEM 授权必须显示为激活状态，而非显示灰色。如果授权显示灰色，说明选择了错误的 Provider（提供者）。只有显示为”激活“的授权才会发送到授权申请文件。
7. 点击 **Generate File（生成文件）**，生成扩展名为 *.tclrq 的授权申请文件。
   ⇨ 用于保存文件的标准对话框打开。
8. 选择保存位置并确认。

⇨ OEM 应用授权申请文件已创建。

8.1.4 创建 OEM 应用授权响应文件

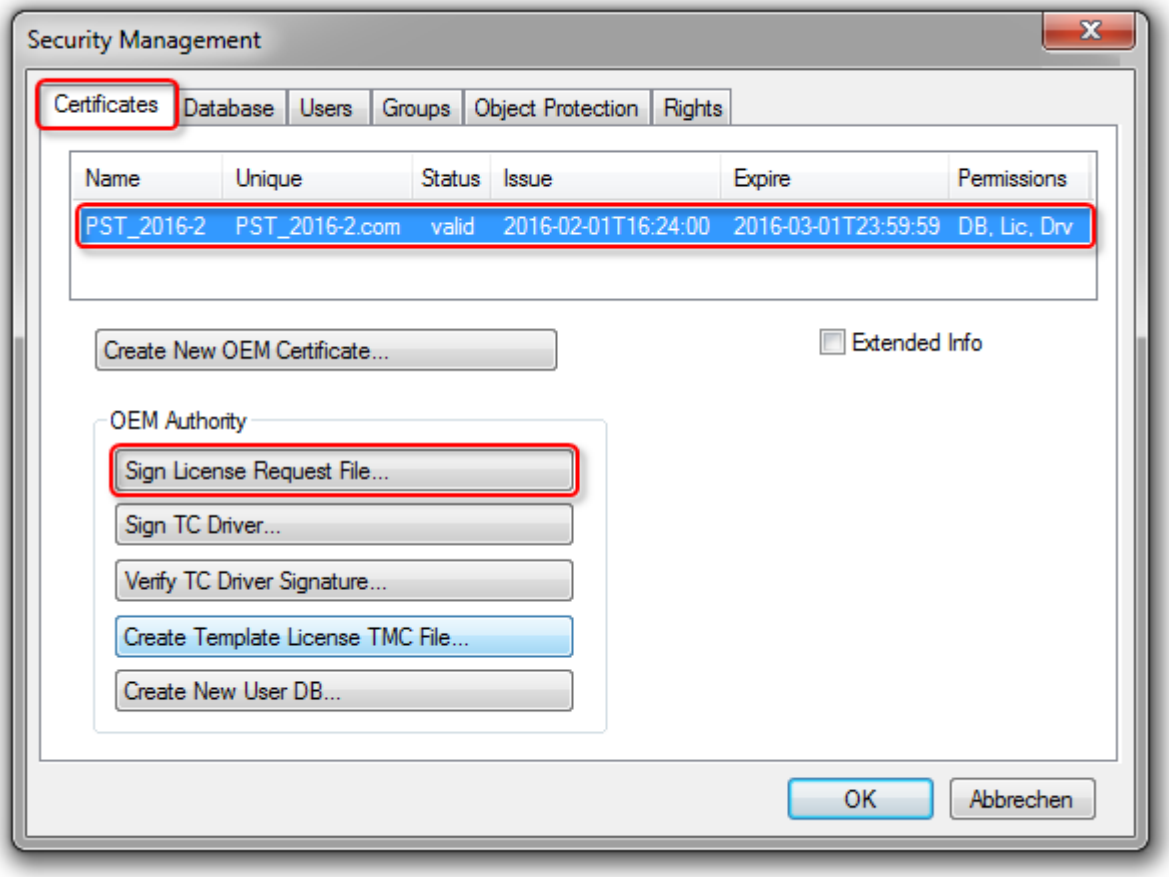
8.1.4.1 通过 TwinCAT 编程环境手动创建

OEM 证书只能在安全环境下使用

由于生成 OEM 应用授权需要处理 OEM 证书及其密码，为防止 OEM 专用密钥的密码被恶意软件窃取，该过程必须在安全环境中进行（受保护的计算机）。

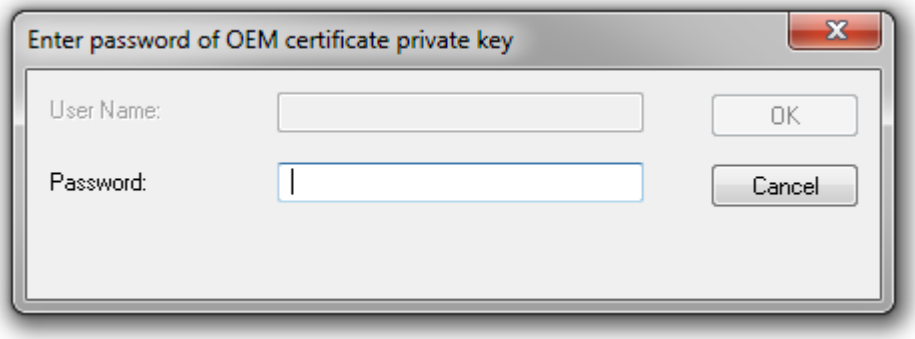
在TwinCAT 3的软件保护配置器 [▶ 10]，手动签署授权申请文件，并创建授权响应文件。

1. 在 **Certificates（证书）** 选项卡中选择 OEM 证书。



2. 点击 **Sign License Request File（签署授权申请文件）**。
   ⇨ 打开浏览器窗口。
3. 选择要签署的授权申请文件（扩展名为 *.tclrq）。

⇨ 弹出提示框要求输入密码。



4. 输入密码并点击 **OK**。

⇨ 授权申请文件已签署，结果保存为授权响应文件（扩展名为 *.tclrs）。此时需将授权响应文件发回到编程计算机或目标控制器。

8.1.4.2 通过命令行工具自动创建

OEM 证书只能在安全环境下使用

由于生成 OEM 应用授权需要处理 OEM 证书及其密码，为防止 OEM 专用密钥的密码被恶意软件窃取，该过程必须在安全环境中进行（受保护的计算机）。

TwinCAT 3编程环境中使用命令行工具（TcSignTool.exe）发放（签署）OEM 授权。该工具也可从用户程序中调用，用于自动发放 OEM 授权。

TcSignTool.exe 位于 TwinCAT 3 安装目录中，即：C:\TwinCAT\3.1\sdk\Bin。

调用参数

tcsigntool licsign /f certificatefile [/p password] [/i issueTime] [/d validDays] [/q] licfile1 [licfile2]

- certificatefile：OEM 证书文件
- password：OEM 证书密码
- issueTime：发放时间，格式为：年-月-日-时-分-秒（默认值 = 当前时间）
- validDays：有效期，默认值 = 无限期
- licfile<n>：授权申请文件（扩展名为 *.tclrq）或授权响应文件(扩展名为 *.tclrs)。扩展名为 *.tclrq 的授权申请文件将被重命名为 *.tclrs。
- /q：安静模式
- 返回值，0 = 成功，1 = 失败

8.1.5 导入OEM 应用授权响应文件

用于非倍福 IPC 的 TwinCAT 3 授权

如果使用一个来自非倍福公司的制造商的 IPC（TwinCAT 3 平台级别 >= 90），则始终需要使用 TwinCAT 3 授权加密狗来授权 TwinCAT 3。

OEM 应用申请的激活方式与 TwinCAT 3 标准授权相同。在 TwinCAT 3 中激活 TwinCAT 3 授权响应文件最简单的方法是通过 TwinCAT 3 授权管理器导入该文件。详情请参见“授权”文件中的导入和激活授权响应文件部分。

授权文件也可直接存储在目标系统目录：*C:\twincat\3.1\target\license*。

将授权文件保存到 TwinCAT 3 加密狗的步骤，请参见“授权”文件中的在加密狗上手动保存授权文件部分。

8.2 将 OEM 应用授权保存到加密狗

将 OEM 应用授权保存到加密狗有两种方法，参见 TwinCAT 3 授权部分：

- 在加密狗上手动保存授权文件
- PLC 功能块与授权加密狗的存储功能关联

8.3 查询 PLC 应用的 OEM 应用授权

使用 OEM 授权时，请确保启动项目已加密！

请记住，通过二进制代码的 FB_CheckLicense [▶ 85] 查询的授权码 [▶ 79]很容易被找到，并可通过十六进制编辑器轻松地进行控制。因此，请确保加密启动项目 [▶ 72]（最安全），或尽可能地在源代码中隐藏查询到的授权码。

TwinCAT Runtime 启动过程中，授权检查分两个步骤进行：

1. TwinCAT 3 首先读取存储在系统中（硬盘上）的授权文件，检查其内容，并将所找到的授权创建成一个内部列表。
2. 授权的最终检查在 EtherCAT 总线调试后进行，因为只有在这时才能获得所有必要的信息。（在此之前，例如 EL6070 授权终端的存在无法被验证）

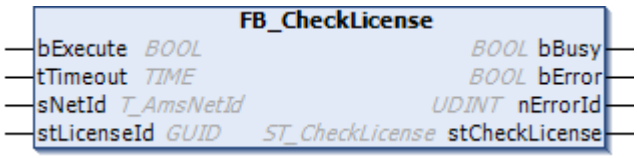
可以在启动完成后，使用 FB_CheckLicense 功能块检索到结果。

在运行期间（在启动和最终授权检查之后），TwinCAT Runtime 会大约**每两分钟**重新检查授权的状态。在 PLC 程序中应相应考虑到这一点（例如，每 10 秒才调用 FB_CheckLicense）。

注意事项：

- FB_CheckLicense 只读取当前存储在内部表格中的授权状态，但不触发新的授权检查。因此，在系统运行时移除加密狗，可能需要两分钟时间才能看到相关授权的状态。
- 提示：如果需要，可以使用功能块 FB_GetLicenseDongles 来确定当前连接到系统的加密狗。
- 授权检查是 TwinCAT Runtime 启动过程的一部分。即：没有运行的运行时间 = 没有当前的授权信息！

FB_CheckLicense



该功能块根据给定的授权码确定 TwinCAT 3 授权的状态。

VAR_INPUT

```
VAR_INPUT
    bExecute    : BOOL;
    tTimeout    : TIME;
    sNetId      : T_AmsNetId;
    stLicenseId : GUID;
END_VAR
```

bExecute：功能块由该输入引脚的上升沿触发。

tTimeout：执行命令时的时间限制，超过该限制将会报超时错误。

sNetId：需读取授权状态的 TwinCAT 控制器的 AmsNetId（AMS 网络标识符）（类型：T_AmsNetId）。如果读取的是本地（localhost）的授权状态，该引脚可以留空不填。

stLicenseId：授权码（类型GUID）

VAR_OUTPUT

```
VAR_OUTPUT
    bBusy          : BOOL;
    bError         : BOOL;
    nErrorId       : UDINT;
    stCheckLicense : ST_CheckLicense
END_VAR
```

bBusy：TRUE（真）表示功能块处于运行中。

bError：TRUE（真）表示命令执行过程中出错。

nErrorId：功能块报错时输出相应的报错代码。

stCheckLicense：包含授权信息的结构体(类型：ST_CheckLicense [▶ 86])

STRUCT ST_CheckLicense

```
TYPE ST_CheckLicense :
STRUCT
    stLicenseId     : GUID;
    tExpirationTime : TIMESTRUCT;
    sExpirationTime : STRING(80);
    eResult         : E_LicenseHResult;
    nCount          : UDINT;
END_STRUCT
END_TYPE
```

变量名称	说明
stLicenseId	授权ID
tExpirationTime	有效日期
sExpirationTime	有效日期
eResult	授权状态（参见 E_LicenseHResult [▶ 86]）
nCount	该授权的实例数量（0 = 无限）

ENUM E_LicenseHResult

```
TYPE E_LicenseHResult :
(
    //success
    E_LHR_LicenseOK                : DINT := 0,
    E_LHR_LicenseOK_Pending        : DINT := 16#203,
    E_LHR_LicenseOK_Demo           : DINT := 16#254,
    E_LHR_LicenseOK_OEM            : DINT := 16#255,
    //error
    E_LHR_LicenseNoFound           : DINT := DWORD_TO_DINT(16#98110700+16#24),
    E_LHR_LicenseExpired           : DINT := DWORD_TO_DINT(16#98110700+16#25),
    E_LHR_LicenseExceeded          : DINT := DWORD_TO_DINT(16#98110700+16#26),
    E_LHR_LicenseInvalid           : DINT := DWORD_TO_DINT(16#98110700+16#27),
    E_LHR_LicenseSystemIdInvalid   : DINT := DWORD_TO_DINT(16#98110700+16#28),
    E_LHR_LicenseNoTimeLimit       : DINT := DWORD_TO_DINT(16#98110700+16#29),
    E_LHR_LicenseTimeInFuture      : DINT := DWORD_TO_DINT(16#98110700+16#2A),
    E_LHR_LicenseTimePeriodToLong  : DINT := DWORD_TO_DINT(16#98110700+16#2B),
    E_LHR_DeviceException          : DINT := DWORD_TO_DINT(16#98110700+16#2C),
    E_LHR_LicenseDuplicated        : DINT := DWORD_TO_DINT(16#98110700+16#2D),
    E_LHR_SignatureInvalid         : DINT := DWORD_TO_DINT(16#98110700+16#2E),
    E_LHR_CertificateInvalid       : DINT := DWORD_TO_DINT(16#98110700+16#2F),
    E_LHR_LicenseOemNotFound       : DINT := DWORD_TO_DINT(16#98110700+16#30),
    E_LHR_LicenseRestricted        : DINT := DWORD_TO_DINT(16#98110700+16#31),
    E_LHR_LicenseDemoDenied        : DINT := DWORD_TO_DINT(16#98110700+16#32),
    E_LHR_LicensePlatformLevelInv  : DINT := DWORD_TO_DINT(16#98110700+16#33)
)DINT;
END_TYPE
```

变量值	含义
E_LHR_LicenseOK	授权有效
E_LHR_LicenseOK_Pending	需进行授权设备验证（例如：授权密钥终端）
E_LHR_LicenseOK_Demo	试用授权有效
E_LHR_LicenseOK_OEM	OEM 授权有效
E_LHR_LicenseNoFound	缺少授权
E_LHR_LicenseExpired	授权已过期
E_LHR_LicenseExceeded	授权的实例太少
E_LHR_LicenseInvalid	授权无效
E_LHR_LicenseSystemIdInvalid	授权的系统 ID 错误
E_LHR_LicenseNoTimeLimit	授权不受时间限制
E_LHR_LicenseTimeInFuture	授权问题：签发时间为未来（多为windows系统时钟设置错误）
E_LHR_LicenseTimePeriodToLong	授权期限太长
E_LHR_DeviceException	系统启动异常
E_LHR_LicenseDuplicated	多次读取授权数据
E_LHR_SignatureInvalid	签名无效
E_LHR_CertificateInvalid	证书无效
E_LHR_LicenseOemNotFound	未知 OEM 的授权
E_LHR_LicenseRestricted	授权对该系统无效
E_LHR_LicenseDemoDenied	不允许试用授权
E_LHR_LicensePlatformLevelInv	授权的平台级别无效

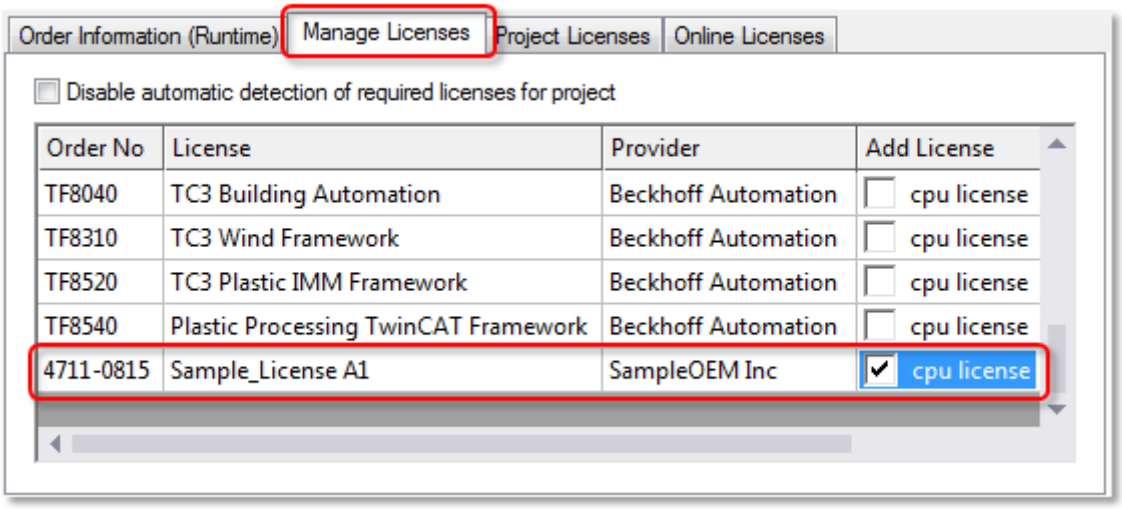
确定 OEM 授权码

OEM 授权码可从相应的授权说明文件或授权管理器中获得。

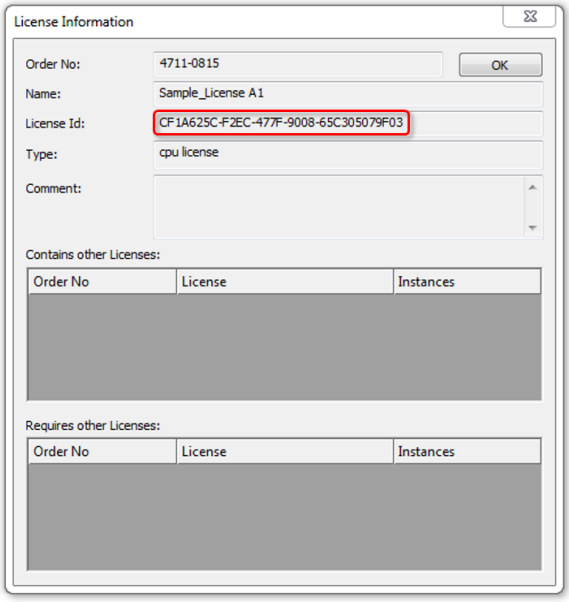
授权说明文件：

```
<Licenses>
    <License>
        <LicenseId>{CF1A625C-F2EC-477F-9008-65C305079F03}</LicenseId>
        <OemId OemName="SampleOEM Inc" OrderAddress="license@SampleOEM
        <OrderNo>4711-0815</OrderNo>
        <DisplayName>Sample_License A1</DisplayName>
    </License>
</Licenses>
```

授权管理器“管理授权”选项卡：



双击授权所在的行，打开显示授权码等授权属性的窗口：



OEM 可以在 PLC 应用中，指定系统对 OEM 应用授权存在与否作出反馈，包括终止程序或激活附加功能。

系统要求

操作系统：

- 至少需要 Windows 7（或其嵌入式版本），才能使用保护应用软件的所有功能。Windows XP 和 Windows CE（Windows Embedded Compact）不支持启动文件的加密或 OEM 授权。

TC3 PLC Lib Tc2_Utiltities：

- 至少需要使用 TC3 PLC Lib Tc2_Utilities 的 3/3/24 版本，新版本的库提供了各种功能，可以方便处理 TwinCAT 3 授权。对于使用 TwinCAT 3 加密狗的 OEM 应用授权来说，这是必须的。TC3 PLC Lib 包括在 TwinCAT 3.1 Build 4022.16 中。

TwinCAT 版本：

- 上述功能需要 TwinCAT 3.1 build 4024 或更高版本。

只有使用最新版本的 TwinCAT 3，才会获得可靠的保护。

为确保获得可靠的保护（例如安全加密），请始终使用最新版本的TwinCAT 3。这可以提供最高的安全性。

至少应使用 TwinCAT 3.1 Build 4024.x。
鉴于安全因素，请勿使用旧版本！

另请参阅：PLC 库 Tc2_Utilities 的文档，授权功能章节

8.4 为 OEM PLC 库提供授权保护

始终使用 FB_CheckLicense 查询 OEM 授权！

以下说明的方法可以作为 FB_CheckLicense 查询的补充（而不是作为替代方法）。

必须始终使用 FB_CheckLicense [▶ 85] 来查询授权状态，因为这是确定当前授权安全状态的唯一方法。

使用 FB_CheckLicense 进行授权检查完全足够；没有必要（因此也不建议）在自创库的属性中额外输入授权 GUID。

如果在自建数据库的属性中另外输入授权 GUID，TwinCAT 3 Runtime 将知道该项目需要该授权，并在运行开始时对该授权进行**第一次**检查。

第一次检查发生在 TwinCAT Runtime 启动阶段的早期。例如，EtherCAT 总线在启动过程后期才会启动；因此，只有在之后才能验证 EL6070 授权密钥终端的存在。

因此，当整个系统已经启动**之后**（从而使 EtherCAT 总线处于运行状态），在任何情况下，使用 FB_CheckLicense 进行授权检查非常重要。

在运行过程中，TwinCAT Runtime（启动后）会大约**每两分钟**检查所有授权的状态。在 PLC 程序中应相应考虑到这一点（例如，在每个 PLC 周期中不调用 FB_CheckLicense）。

9 防止应用被克隆

参见发放和使用您自己的 OEM 授权 [▶ 77]

10 支持和服务

倍福及其合作伙伴在世界各地提供全面的支持与服务，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。

倍福分公司和代表处

有关倍福产品当地支持和服务方面的信息，请联系倍福分公司或代表处！

可以在以下网址找到世界各地的倍福分公司和代表处的地址：https://www.beckhoff.com

您还可以在该网页找到更多倍福组件的文档。

倍福支持部门

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：

- 支持
- 设计、编程和调试复杂的自动化系统
- 以及倍福系统组件广泛的培训计划

热线电话：	+49 5246 963 157
传真：	+49 5246 963 9157
电子邮箱：	support@beckhoff.com

倍福服务部门

倍福服务中心为您提供所有售后服务：

- 现场服务
- 维修服务
- 备件服务
- 热线服务

热线电话：	+49 5246 963 460
传真：	+49 5246 963 479
电子邮箱：	service@beckhoff.com

倍福公司总部

德国倍福自动化有限公司

Huelshorstweg 20
33415 Verl
Germany

电话：	+49 5246 963 0
传真：	+49 5246 963 198
电子邮箱：	info@beckhoff.com
网址：	https://www.beckhoff.com

更多信息:
www.beckhoff.com/te1000

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