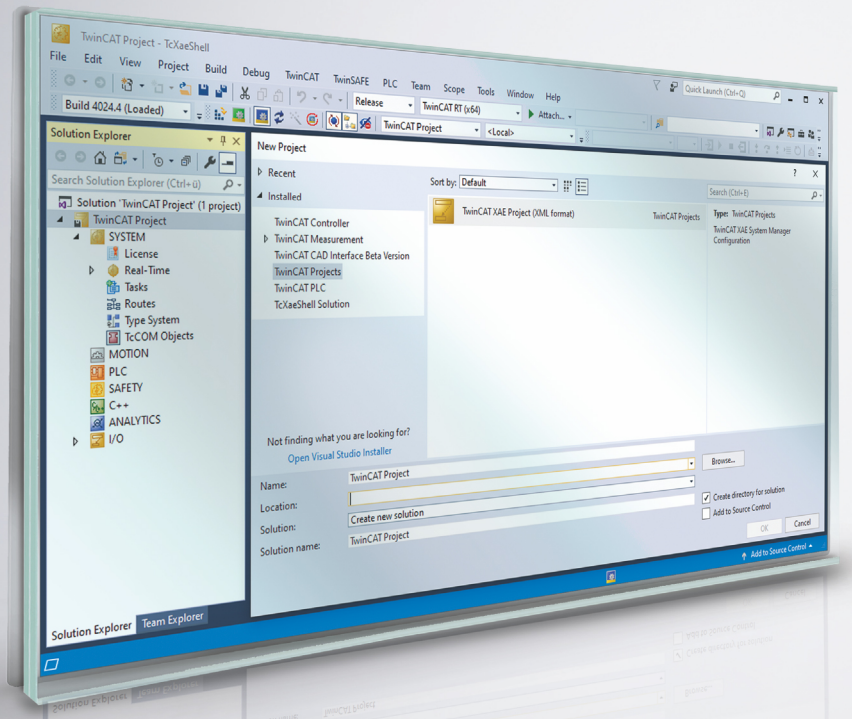
BECKHOFF New Automation Technology

手册 | ZH

IPC Security Guideline

for Windows 10



2026-03-17 | 版本： 1.8

1 □□□□

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。

□□□□

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。

□□

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。

□□□□

□□□□□

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。

1.1 □□□□

我们恳请安全分析师在公布安全漏洞之前，给我们足够的时间来制定解决方案。协调披露可确保客户获得有关安全漏洞被修复的最新信息，并确保他们在更新过程中不会受到不必要的威胁。在客户得到保护的情况下，关于安全漏洞的公开讨论将有助于整个行业改进其产品和解决方案。

如果倍福有疑似存在安全漏洞的产品，那么安全漏洞的发现方和协调方应联系 product-securityincident@beckhoff.com，并提供漏洞报告，最好是英语或德语报告。务必保密。发送加密消息的方法见 。

请发现者在漏洞报告中提供所有必要的联系信息，以便查询。不过，匿名漏洞报告也在考虑范围内。请提供尽可能详细的信息，以便复现案例。如果发现者想要发布这一发现，倍福会尝试在 30 天内协调出一个合适的初步发布日期。在发布日期之前，发现者会被告知可用的解决方案，并收到倍福发布的相关公告。倍福会收到发现者的发表计划（包括所要求的 CVE（如适用））。然后商定最终发布日期。在这一天，会同时发布发现者的发表内容和倍福的相关公告。如果发现者有意愿并遵守上述流程，则会在咨询报告中添加感谢信，提及发现者的发表内容，如果有帮助，还会提供有关发表内容的信息。

1.2 联系倍福事件响应团队

地址

Beckhoff Automation GmbH & Co. KG
产品管理部（安保）
Hülshorstweg 20
33415 Verl
Germany

电子邮件

<product-securityincident@beckhoff.com>

发送至本地址的电子邮件会发送给倍福事件响应团队的负责成员。

公共密钥

倍福事件响应团队有两个密钥可供建立联系：

- 带有 ID `B4 F4 15 9A` 和指纹 `C9 6F 56 5C 39 49 43 58 AE B5 07 93 80 95 E1 2D B4 F4 15 9A` 的 PGP 密钥
- 带有 ID `0a 0e 85 68 56 18 0f 5c 8a 5c 4e 83` 和指纹 `4c b4 d0 99 d4 a0 6c f0 af 69 ee 7a 8f 81 a1 c3 42 eb 17 da` 的 S/MIME 证书

密钥下载：https://download.beckhoff.com/download/document/product-security/Keys

工作时间

事件响应团队在北莱茵-威斯特法伦州的工作时间通常为上午 9 时至下午 5 时，公共假日除外。时区：中欧标准时间（欧洲/柏林）。

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 安全设计目标

还请参阅有关此

重要 TCP/UDP 端口 [▶ 51]

2 □□□□□□□

本节介绍了自动化系统的危害和风险评估。描述了不同的攻击者和攻击类型以及典型的威胁场景和保护原则。

2.1 □□□

□□□□□□□□□

根据攻击者对系统的访问，可以将其分为四类：

等级	描述
内部攻击者	意图在自动化系统上执行某些操作的攻击者。其目的是执行未获授权的破坏性行为。此外，这些攻击者可以访问需要执行授权操作的私人信息，例如密码。
本地攻击者	可以直接访问自动化系统组件的攻击者。此类攻击者还包括可以通过硬件接口直接访问某些组件或者在其他地方更改网络拓扑的本地攻击者。
内部网络中的攻击者	控制内部网络设备的攻击者。这些攻击者通常无法更改网络拓扑，只能使用网络中的现有服务。
来自外部网络的攻击者	例如，攻击者只能通过连接到互联网的接口来执行操作。这些攻击者在成功攻击内部组件后，可以升级为内部网络攻击者。

□□

对于所有攻击者，必须假设：

- 他们可以接收公共信息，例如来自互联网或通过服务调用接收的文件；
- 他们能够获取公开市场上的任何产品，并通过分析这些产品来准备有针对性的攻击；
- 他们拥有强大支配计算的能力，例如通过向云提供商租用计算算力。

根据攻击者动机偶然发起的分类通常是不可取的，因为它涉及许多假设和推测。

这种分类有助于进行安全分析，但应注意的是，真正的攻击者在多个类别中拥有各种能力。

2.2 □□□□

可以根据攻击的执行方式进行分类。攻击所涉及的结果起着关键作用：

类别	描述
广泛的病毒攻击	这些攻击利用普遍存在的漏洞，并蔓延到可抵达的相邻设备。这种“无目标攻击”旨在尽可能多地攻击受影响系统，以使攻击者获益。攻击者可以得到的好处来自勒索加密数据（“勒索软件”）或使用被攻击方的资源（“僵尸网络”），诸如此类。这些攻击通常利用未修补的漏洞或常见的组织缺陷，比如弱密码。
针对供应商和集成商的攻击	这些攻击利用某些产品的漏洞，这些漏洞可能不太常见。这些攻击可以自动传播，但它们针对的是作为漏洞的特殊产品或配置（例如，倍福或集成商配置/扩展（如适用））。攻击目标也可能针对特定行业，比如窃取专有技术等。
针对特定用户的攻击	此类攻击针对单一的系统部署，因此被称为针对性攻击。它们很难被发现，由攻击者精心实施。以针对性的系统配置来实现攻击目的。攻击目标多种多样，通常很难预测。

这些安全指南所提供的措施只用于防范广泛的病毒和针对供应商的攻击。针对用户的攻击需要用户进行分析并采取应对措施。

2.3 典型的威胁场景

本节描述各种典型的威胁。但无法详尽无遗地列举。

操纵的启动介质

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	不包括	不包括	不包括
针对供应商和集成商的攻击	包括	包括	不包括	不包括

将一个准备好的数据存储设备连接到一个组件上，组件通过该设备启动。如果 UEFI/BIOS 中的启动顺序设置为从外部磁盘启动，或者攻击者能够更改启动顺序，则上述情况是可能的。

通过该攻击，攻击者可以对组件上的所有数据进行读写访问，特别是配置和专有技术。发生此类访问后，整个组件被认为是不安全的。

防御措施：

- BIOS 密码 (BIOS 设置 [▶ 14])
- 设置引导介质 (BIOS 设置 [▶ 14])
- 锁定控制柜 [▶ 12]

未授权的 **PXE** 启动服务器

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	不包括	包括	不包括
针对供应商和集成商的攻击	不包括	不包括	包括	不包括

从内部网络中未授权的 PXE 启动服务器启动。攻击包括执行由攻击者控制的代码。

通过该攻击，攻击者可以对组件上的所有数据进行读写访问，特别是配置和专有技术。发生此类访问后，整个组件被认为是不安全的。

防御措施：

- 禁用 PXE 启动 (BIOS 设置 [▶ 14])

操纵的 **USB** 设备

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	包括	不包括	不包括
针对供应商和集成商的攻击	包括	包括	不包括	不包括

如果连接了被操纵的 USB 设备，攻击者就可以在受影响的设备上执行恶意代码。此外，受影响的 USB 设备也可以用来窃取专有技术。例如，任何代码都可以通过适当配置的自动启动来执行。经过适当准备的输入设备，可执行未经授权的输入或记录。

此攻击使攻击者能够对大量与操作系统相关的数据进行读写访问，特别是配置和专有技术。发生此类访问后，整个组件被认为是不安全的。

防御措施：

- 禁用自动启动 (AutoStart（自动启动） [▶ 36])
- 白名单 USB 设备 (USB 过滤器 [▶ 45])
- 锁定控制柜 [▶ 12]
- 在BIOS 中禁用接口 (BIOS 设置 [▶ 14])
- 程序白名单 [▶ 31]

通过本地接口猜测弱密码

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	不包括	不包括	不包括
针对供应商和集成商的攻击	包括	包括	不包括	不包括

弱密码（比如默认密码或容易猜到的密码）可能会被本地攻击者利用。攻击者可以像获得授权的本地用户一样使用未修改的默认密码登录。

此攻击使攻击者能够对大量与操作系统相关的数据进行读写访问，特别是配置和专有技术。发生此类访问后，整个组件被认为是不安全的。

防御措施：

- 安全密码 [▶ 19]
- 设置个人用户，无集体账户
- 为用户提供最低权限（“最低权限”），尤其是在没有必要的情况下不提供管理员权限

数据载体被盗

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	不包括	不包括	不包括
针对供应商和集成商的攻击	包括	包括	不包括	不包括

攻击者可以通过未经授权移除的数据载体，获取系统中服务的相关信息和访问信息。

通过这样的攻击，攻击者可以读取大量与操作系统相关的数据，尤其是访问数据、配置、知识和其他敏感的私人数据。

攻击者还可能会在存储介质被弃置后，通过窃取存储介质来获取敏感数据。

防御措施：

- 文件加密 [▶ 18]
- 锁定控制柜 [▶ 12]
- 安全销毁数据 [▶ 12]

从废弃材料中提取敏感数据

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	不包括	不包括	不包括
针对供应商和集成商的攻击	包括	包括	不包括	不包括

攻击者可以访问存储介质上包含敏感数据的废弃材料。

通过这样的攻击，攻击者可以读取大量与操作系统相关的数据，尤其是访问数据、配置、知识和其他敏感的私人数据。

防御措施：

- 文件加密 [▶ 18]
- 安全销毁数据 [▶ 12]

处理不受信任的电子邮件

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	不包括	包括	包括
针对供应商和集成商的攻击	不包括	不包括	包括	包括

不受信任的电子邮件是传播恶意软件的典型方式。特别是，此攻击会利用过时的浏览器和电子邮件附件来打开超链接。有时，电子邮件的表达方式看起来值得信赖。

一个成功的攻击可以执行未经授权的操作，而这些操作是需要通过交互用户的特权执行的。

防御措施：

- 不要使用控制电脑处理电子邮件
- 定期或自动更新软件 (更新 [▶ 15])
- 程序白名单 [▶ 31]

□□□□□□□□□□□□□

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	包括	包括	包括	包括
针对供应商和集成商的攻击	包括	包括	包括	包括

制造商发布软件更新用以修补已知的漏洞。如果不更新所使用的软件，则大量的病毒攻击可能成功地入侵。

一个成功的攻击可以执行未经授权的操作，这些操作会在相关软件环境中产生影响。

防御措施：

- Windows 更新 (更新 [▶ 15])
- 定期或自动更新软件 (更新 [▶ 15])
- 基于网络的检测机制 (IDS/IPS)
- 禁用不需要的服务
- 删除不再需要的组件 [▶ 35]

□□□□□

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	不包括	不包括	包括
针对供应商和集成商的攻击	不包括	不包括	不包括	包括

用户被骗去访问一个不受信任的网站。浏览器中的漏洞被用于执行任意恶意代码，或者网站的设计方式使得用户泄露机密信息，如登录数据。

一个成功的攻击可以执行未经授权的操作，而这些操作是需要通过交互用户的特权执行的。

防御措施：

- 定期或自动更新软件 (更新 [▶ 15])
- 有组织措施的上网行为。

□□□□□

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	包括	不包括	不包括	不包括
针对供应商和集成商的攻击	包括	包括	包括	包括

当使用不安全的网络协议时，攻击者可以假装是网络中受信任的远程站。这使得通过该协议发送的信息被操纵或拦截。

一个成功的攻击可以导致自动化系统中出现意外的服务操作。

防御措施：

- 网络分割
- 使用安全网络协议

未经授权使用网络服务

攻击类型/攻击者	内部	本地	内部网络	远程
广泛的病毒攻击	不包括	不包括	包括	包括
针对供应商和集成商的攻击	不包括	不包括	包括	包括

如果存在攻击者能够访问的网络服务，则可能导致未经授权的操作。

一个成功的攻击可以导致自动化系统中出现意外的服务操作。

防御措施：

- 网络分割
- 使用身份验证网络服务
- 禁用不需要的服务
- 删除不再需要的组件 [▶ 35]

3 □□□□

3.1 □□□□

训练有素的人员是系统的重要保障。接触设备的员工应该知道如何操作该系统。其中包括妥善的管理密码和 USB 盘类数据载体等一般措施。每位员工都应了解干预系统可能产生的影响。

3.2 □□□□

最简单、最安全的安全措施之一就是物理保护。确保只有管理员和技术人员才能访问设备。通过这种方式可以减少通过 USB 闪存盘和其他数据载体等物理访问导致的攻击，这些攻击是最大的风险之一。设备的物理保护可通过锁定的控制柜等方式实现。

□□□□□

工业控制器的标准环境应该为控制柜上锁。通过只允许个别接口从控制柜外部进行连接，攻击面将大大减少。引出的接口应得到额外保护（可上锁）。只有需执行任务的人员才能使用控制柜。也可以使用电子锁定系统，例如智能卡。与所有的密钥管理系统一样，当不再需要时，应取消对控制柜的访问。

□□□□

视频监控适合于轮班工作，在多人需要访问控制器或设施在地理上分布较为分散的环境中。但是，视频监控只能检测攻击，而不能阻止攻击。因此，这一措施只能与其他措施结合使用。

3.3 □□□□□□

对于报废或停用的组件，必须可靠地销毁数据。多次覆盖数据载体是一种合适而可靠的方法。

完整硬盘上的数据可以通过使用特殊软件进行覆盖从而被完全地、不可恢复地删除。数据会被指定字符或随机数字覆盖一次或多次，这在大多数情况下就足够了。

Windows 现在会在“慢速”格式化过程中用零覆盖整个分区。如果是旧硬盘（< 80 GB），那么应覆盖数据 7 次。现代硬盘允许使用 ATA-“增强安全擦除”命令。此类情况下，硬盘中会启动一个针对供应商的例行程序，该例行程序应清除整个硬盘，包括有缺陷的内存区域。建议在 SSD 或 SSHD 上使用这种擦除方法。该命令应与上述覆盖流程相结合。数据载体覆盖后仍可正常使用。

市售免费软件和商业产品都可以执行上述覆盖方法。这些工具大多会提供不同的覆盖方法。我们建议使用可从可启动介质（如 CD、USB 闪存盘）启动的程序来覆盖硬盘，并覆盖整个硬盘的方式。

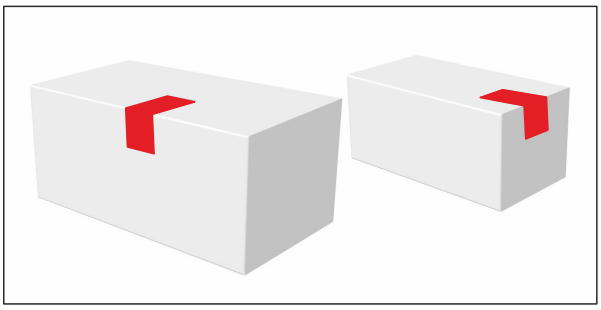
□□□□

如果不想覆盖硬盘或因硬盘缺陷而无法覆盖，则应物理损坏或销毁硬盘。

3.4 □□□□□□□□□□

从 2021 年底起，某些用于工业电脑和嵌入式电脑的产品包装将会在出厂时被贴上具有安全特征的封条：

封条的位置和特征决定了，从包装中取出商品时将会导致包装和封条上出现不可逆转的可见变化。 由此可以在打开前通过目视检查确定产品是否完好无损。



封条有助于提高检查包装产品时的工作效率。 因为没有绝对的安全，所以封条的使用仅限于以下应用： 允许有根据地猜测包装中商品的完好无损性、完整性和真实性，而不必打开包装。 如果封条或包装被损坏，那么收货人就应当在收货时或使用商品前确认其正确状态。 如果商品旨在用于对 IT 安全性具有重大意义的应用，那么例如在封条或包装的状态显示发货期间商品可能被擅动时，收货人就可以决定，在使用前检查其是否被擅动。

收货人负责在收货时以及在使用 Beckhoff 产品前设计和决定合理的流程和规则。

封条被打开

Beckhoff 产品通常通过一个多级分配链到达收货人处。 封条可能在产品加工时被打开。 不能因封条被打开而提出保修索赔。

4 BIOS □□

建议您为 BIOS 设置一个密码，以确保关键设置（如启动顺序、CPU 时钟或重要设置）无法在未经授权的情况下更改。设置启动顺序和禁止外部磁盘启动也可能有用。BIOS 中的设置只能由精通人士执行。改变未知参数对系统功能存在不利影响。

5 □□□□

5.1 □□□□□

应为每台设备制定备份和还原策略，并防止出现以下情况：

- 安全事件，
- 由存储介质缺陷导致数据丢失，
- 或因关机不当导致数据损坏。

可以在最短时间内还原上次创建的备份，从而避免出现严重的生产停机。除了创建备份，确定还原过程也很重要。

备份和还原不完全是安全问题，但有助于在发生安全事件时最大限度地减少停机时间。

应确定创建安全副本的流程以及还原安全副本的流程。这样做时，还应考虑到安全问题。

如果使用完全自动化的备份解决方案，备份系统本身大多可以在网络中访问，因此也容易受到攻击；这里最好使用手动（“离线”）备份。异地备份，即在本地单独存储的备份，其优势是即使发生本地改动事件，即机器本身不受影响的情况下，也可以还原备份。

因此，可以有多种多样的实施方案可供选择和想象。

由于 TwinCAT 启动项目和所有必要信息都以文件形式存储在相应操作系统的文件系统中，因此基于文件的安全性就足够了。

倍福会以“倍福服务工具 (BST)”的形式提供备份和还原解决方案。有关 BST 的更多信息，请参见：Infosys 关于 BST 的条目。

如果您的工业 PC 在出厂时为系统分区启用了 BitLocker 加密，那么在无人值守启动过程中解密分区的密钥会受到设备主板上可信平台模块 (TPM) 的保护。只有在早期启动过程的评估结果表明，已启动的具有已知配置且先前受信任软件，并且该软件、配置和下一个要启动的软件（即内核）均未被篡改的情况下，TPM 模块才会向 Windows 内核提供用于解密的密钥。

完整备份必须包括启动分区和系统分区。如果将整个启动盘作为原始设备备份，备份中就会包含加密系统分区。除备份外，还必须导出还原密钥。要在其他硬件上还原和使用备份，尤其需要还原密钥。请将该还原密钥妥善保管。此外，还强烈建议始终随身携带还原密钥，以防在早期启动过程中涉及对软件和配置进行合法的改动。例如，被授权人员对固件 (BIOS) 的启动顺序进行更改的这种场景。

如果启用 BitLocker 加密，则除了对分区（包括加密系统分区）进行完整备份之外，还有另一种方法：您可以暂时禁用系统分区的加密，然后像往常一样创建离线备份。之后请不要忘记重新启用加密。

5.2 □□

有多种方法可以让您的操作系统和程序保持最新版本：

- 更新整个镜像
- 更新单个程序
- 集成操作系统更新

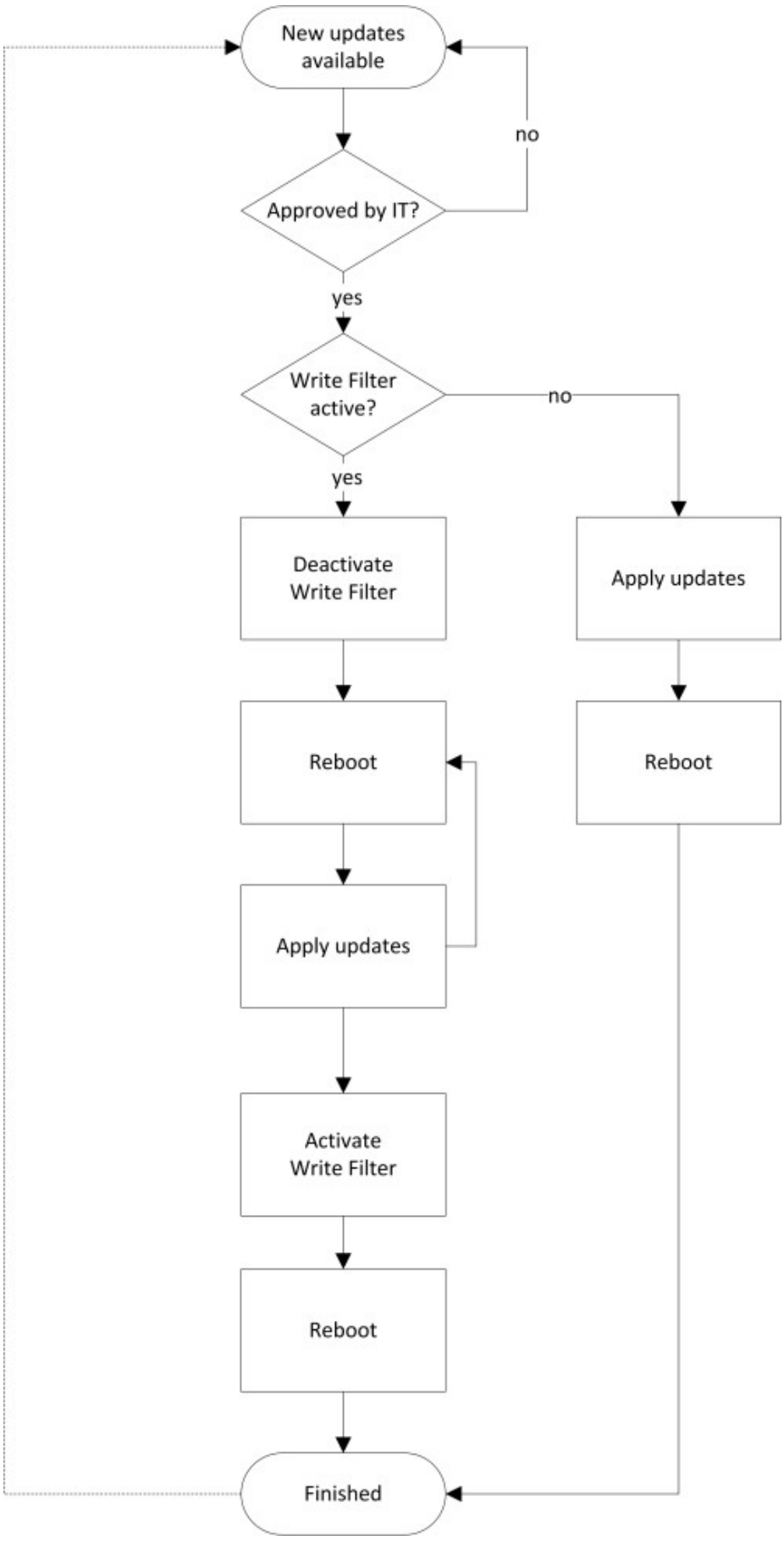
注意

避免数据丢失

进行更新前，请先备份数据。首先，借助 BST（倍福服务工具，https://www.beckhoff.de/default.asp?industrial_pc/bst.htm）创建 PC 的备份镜像。

Windows 7/10/11 操作系统有自己的更新机制，即 Windows 更新服务。为防止无意中更改系统，倍福提供的镜像中禁用了 Windows 更新服务。Windows 更新仍可从 Microsoft 下载并手动安装。如果启用了 Windows 更新服务，则会使用标准设置从 Microsoft Windows 更新服务器获取更新。与服务器的通信是通过加密的签名连接进行的。所购买的更新都有 Microsoft 官方证书的签名，以便检查其真实性。

工程计算机应通过更新保持最新版。这对工业环境中的计算机来说可能更加困难。例如，如果使用了写保护过滤器，则在重新启动时会丢弃未采取进一步措施而安装的更新。为了避免这种情况，建议采用以下步骤：



在此步骤之后，需要操作员进行密集的测试，以确保系统正常运行。倍福设备每半年提供一次经过更新和测试的镜像，其中包含兼容的 Windows 更新。

这些镜像可通过倍福服务获取，适用于 Windows 7/10/11。为此需要提供设备的序列号。

另请参见：

- https://www.beckhoff.de/default.asp?industrial_pc/bst.htm

5.3 □□□□

注意

故障

不要加密整个系统分区、Windows 系统文件或 TwinCAT 文件夹。这可能引发故障。

一般来说，已建立的访问控制足以保护敏感文件和目录免遭未经授权的访问。但是，如果数据载体丢失，这些数据的保护就不再有保障，因此有必要对单个文件和目录进行加密，以提供额外的保护。

通过 EFS（加密文件系统），Windows 提供了加密功能，可对单个文件或整个目录进行加密。因此，可以提供额外的安全级别和加密保护。

加密后的一个重要方面是管理密钥和澄清以下问题：

- 谁应该获得访问权？
- 有哪些身份验证选项？（USB 身份锁、PIN、密码、用户名加密码等）
- 如何管理密钥？

无论如何，数据在解密和使用时都是不受保护的。

相比之下，BitLocker 支持对整个数据载体进行加密。此外，BitLocker 与 TPM（可信平台模块）一起使用时可提供最大程度的保护，详见 TPM 文档。

□□ EFS

1. 右键单击一个文件夹或文件，然后从打开的上下文菜单中选择**属性**。
2. 打开**常规**选项卡并点击**高级**。
3. 要加密文件夹或文件，可选择**加密内容以便保护数据**复选框。

⇨ 如果这是第一个以这种方式加密的数据，那么 Windows 将自动在本地证书存储区中创建 EFS 证书。务必保存证书，否则无法恢复数据（请参见保存证书 [▶ 18]）。

□□□□

1. 启动 **certmgr.msc**。
2. 点击**添加**，选择**我的用户账户**，然后点击**结束**。
3. 展开“个人”文件夹并点击**证书**

   ⇨ 您应该看到一个以“加密文件系统”作为“预期目的”的证书。
4. 要保存证书，右键单击证书并选择**所有任务 > 导出**。
5. 选择**导出私钥**。
6. 选择**个人信息交换、包括所有证书…...**以及**启用强保护**。
7. 指定用于保护证书的密码。此证书稍后将被要求导入。
8. 指定保存证书的路径。将证书保存在另一个安全位置。

5.4 用户和权限管理

5.4.1 安全密码

安全密码是保证系统安全的重要前提。倍福会为镜像提供操作系统的标准用户名和标准密码。用户必须修改用户名和密码。否则，您的设备很容易受到网络攻击和未经授权人员的访问。

控制器交付时不带 UEFI/BIOS 密码。同样建议为此分配一个密码。

系统中集成了安全向导。这是在本地访问期间启动设备后直接启动的。该向导要求用户更改密码。然而，也可以使用操作系统工具在本地更改密码。

以下规则适用：

- 每个用户和服务的密码应该是唯一的。
- 密码复杂度：密码应包含大写字母、小写字母、数字、标点符号和特殊字符。
- 密码长度：密码至少为 10 个字符。
- 与之前的一些建议相反，在此建议不再定期更改密码，而只在密码被未经授权的人知道之后才更改。另请参见 https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/
- 在登录尝试失败之后设置强制等待时间会生效。

生成安全密码

有多种方式创建安全密码。下表描述了生成密码的一种方法。这个过程还有助于记忆复杂密码：

程序	示例
1. 从一个或两个句子开始。	复杂密码更安全
2. 删除空格。	Complexpasswordsaremoresecure
3. 缩写单词或添加拼写错误。	Complxpasswordsarmorescure
4. 插入数字和特殊字符以扩展密码。	Complxpasswordsarmorescure#529954#

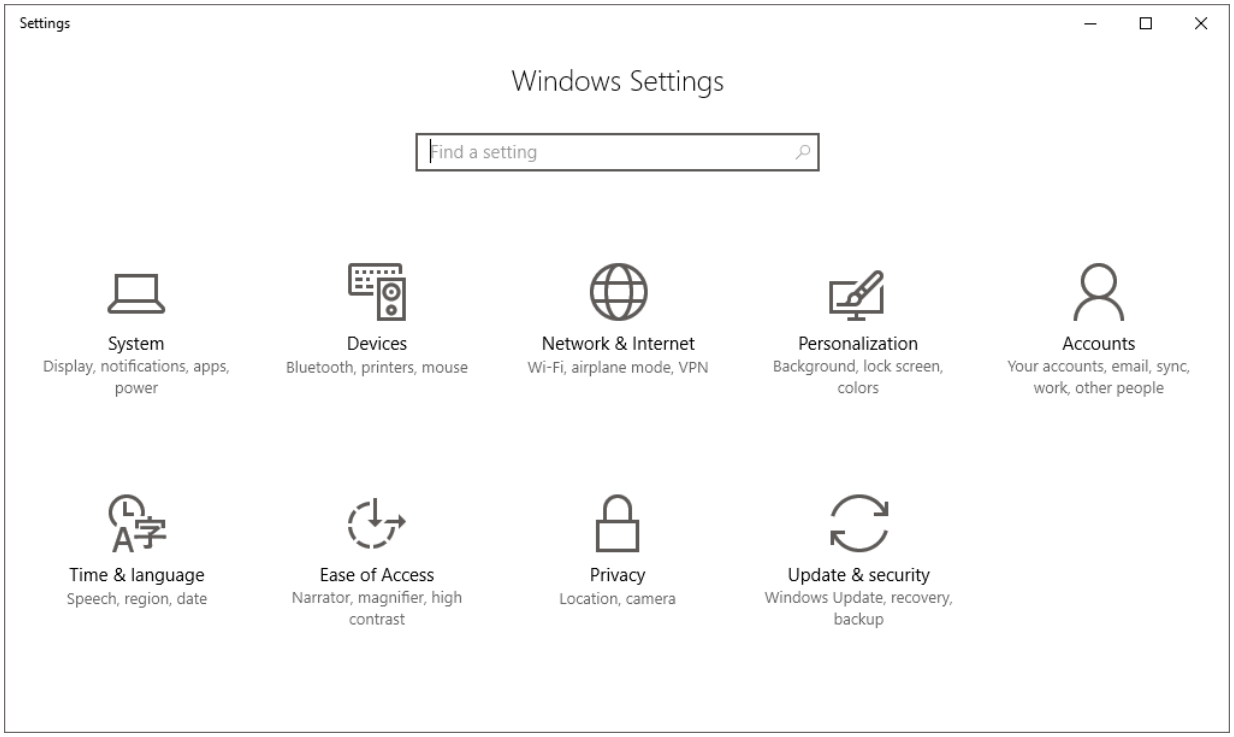
有问题的密码

网络犯罪分子使用复杂的工具能够对密码进行高效的攻击。因此，最好避免：

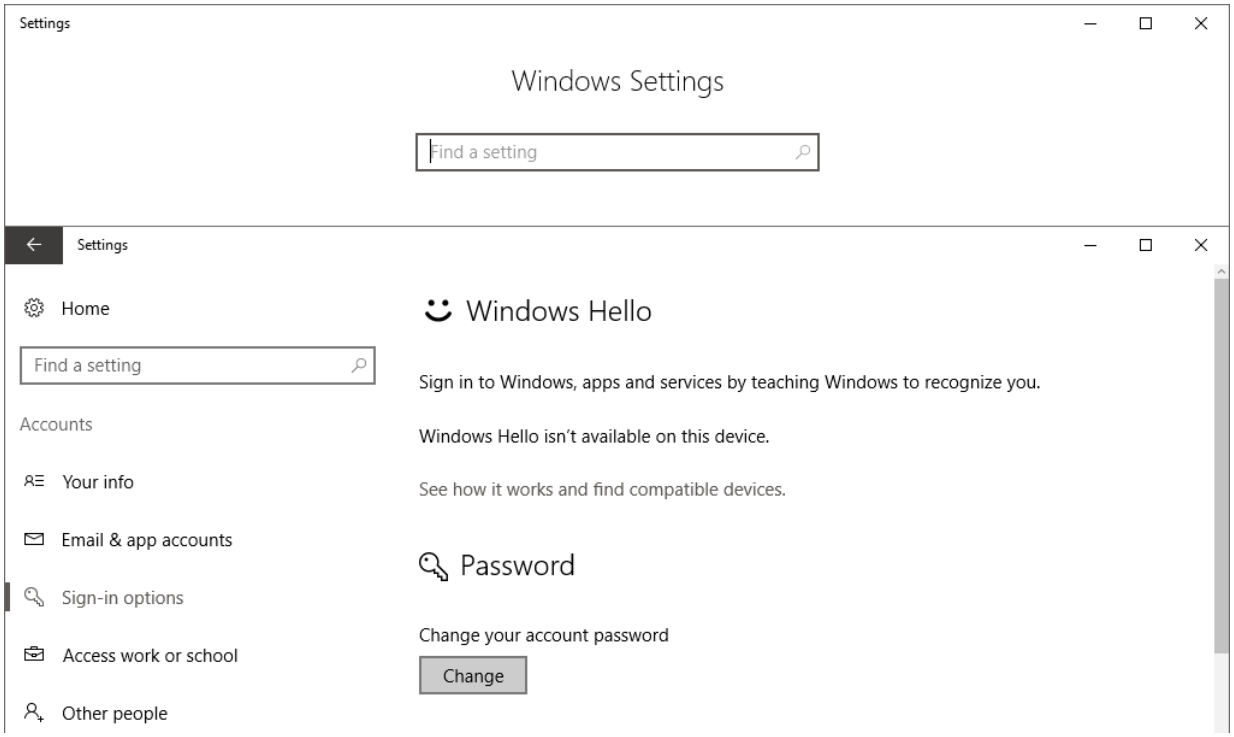
- 字典中的单词
- 反向书写单词、常见拼写错误和缩写
- 重复序列，如 12345678 或 abcdefgh
- 个人信息，如生日、身份证号码、电话号码

5.4.1.1 □□□□

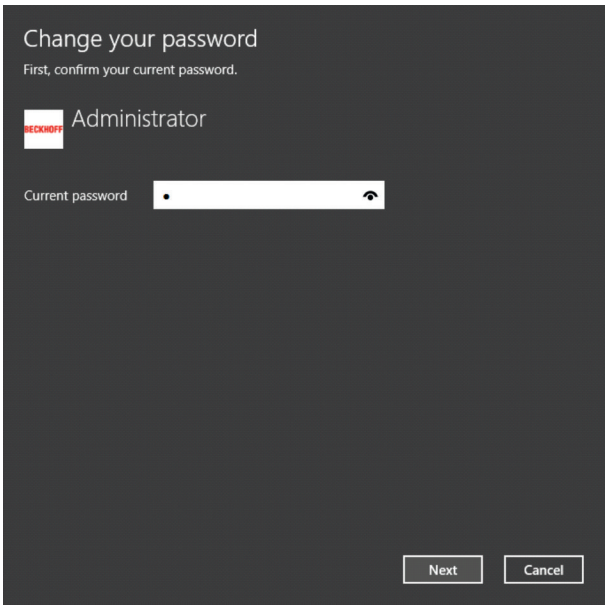
1. 打开设置，点击**账户**。



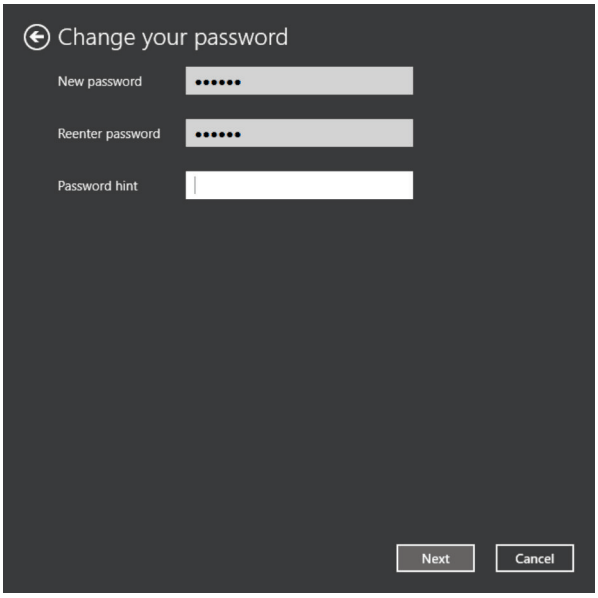
2. 选择**登录选项**，点击密码区域中的**更改**。



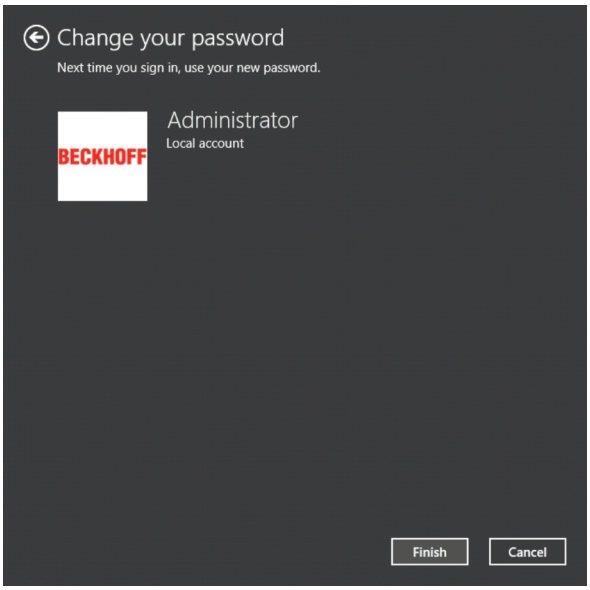
3. 输入当前密码，点击**下一步**。



4. 输入新密码，点击**下一步**。



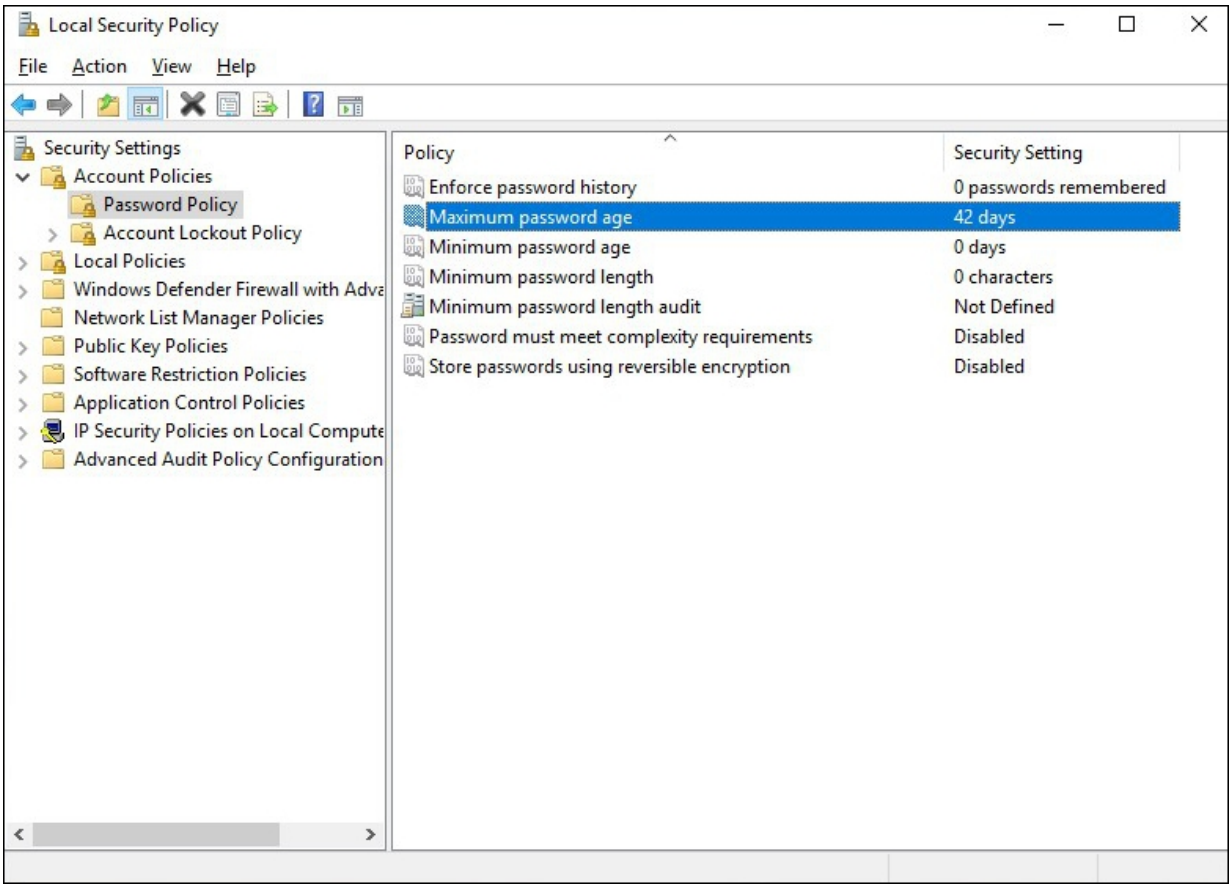
⇨ 密码现已重置。



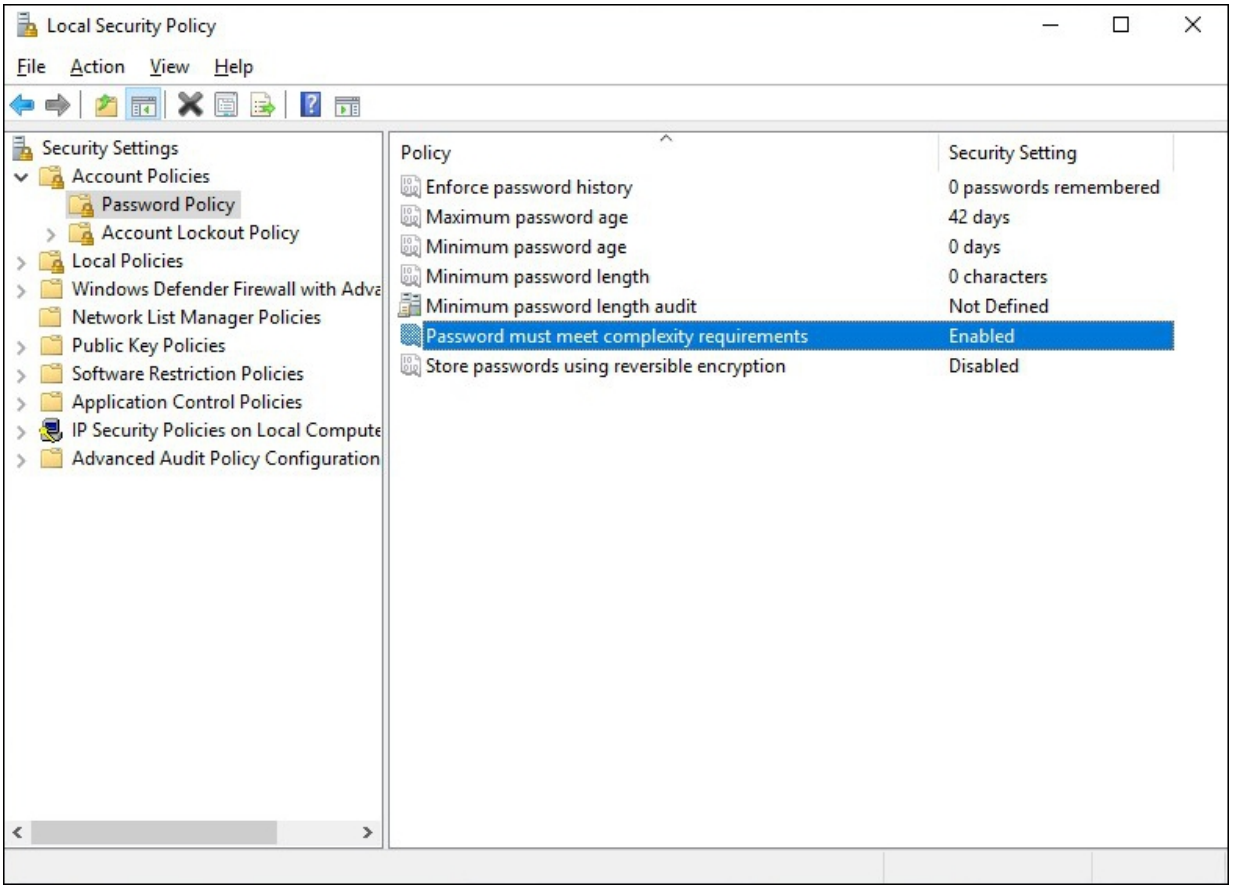
5.4.1.2 □□□□

使用密码策略可以限制用户账户的密码选择，迫使用户选择安全密码。单独的密码策略可防止系统使用弱密码。设置使用用户密码的长度和复杂程度。

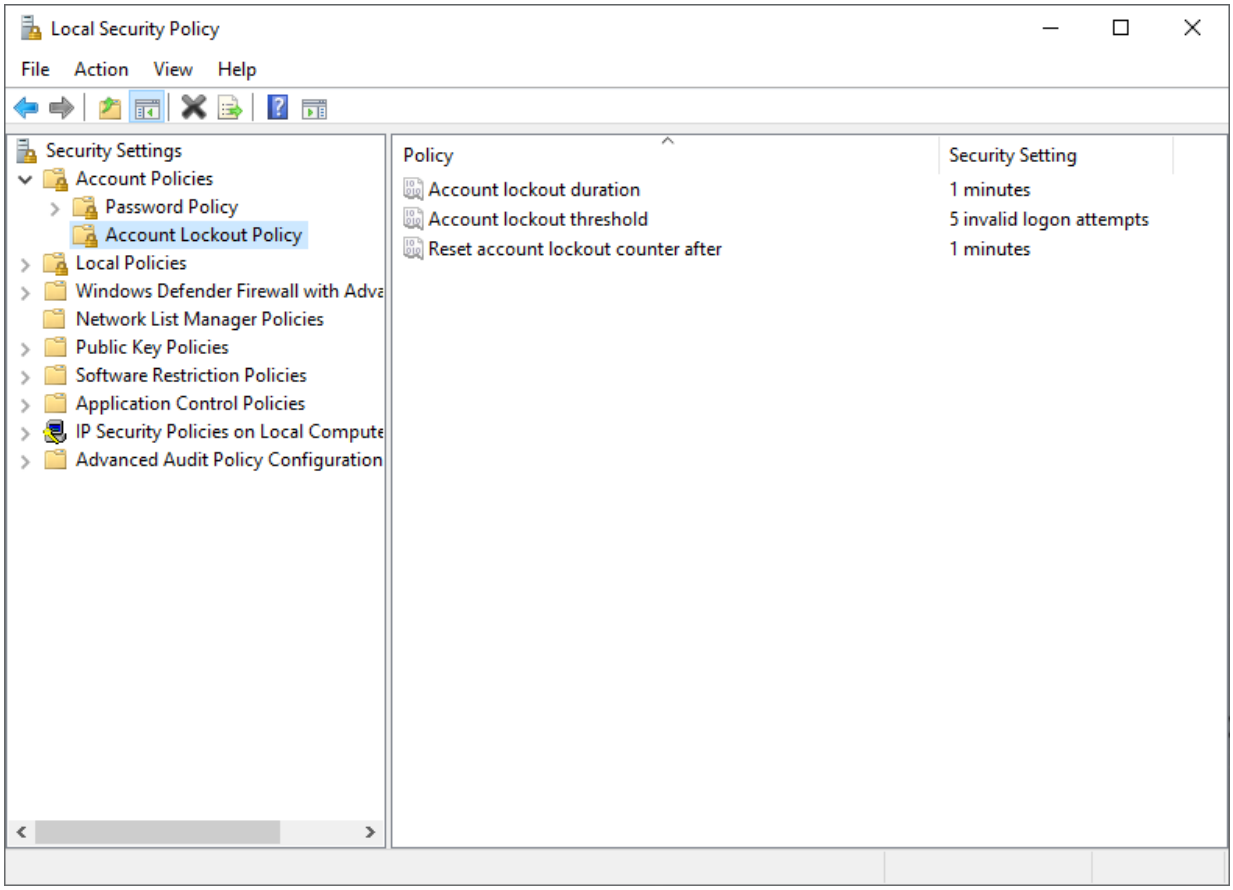
1. 打开**控制面板**并选择**管理工具 > 本地安全策略**。
2. 在打开的窗口中选择**账户策略 > 密码策略**
3. 指定密码策略设置。
4. 设置密码有效期，可为策略**密码有效期**确定一个时间段（以天为单位），然后系统会提示用户更改密码。



5. 为了要求密码的复杂性，可以设置**密码必须满足复杂性要求**策略。启用该策略后，设置的密码都必须至少包含大写字母、小写字母、数字和特殊字符。



6. 为防止猜测用户身份验证数据的攻击，可在**账户锁定策略**中进行设置。设置锁定用户账户的登录失败次数。您可以利用**账户锁定时长**策略来设置锁定账户在自动解锁前保持锁定的时长（以分钟为单位）。



⇨ 密码策略的定义

5.4.1.3 IPC □□□□

可通过 IPC 诊断网页设置用户密码。可通过端口 443 以 https 方式访问。

在出厂状态下，当用户通过 https 连接或在设备上进行本地作业时，IPC 安全向导就会启动。

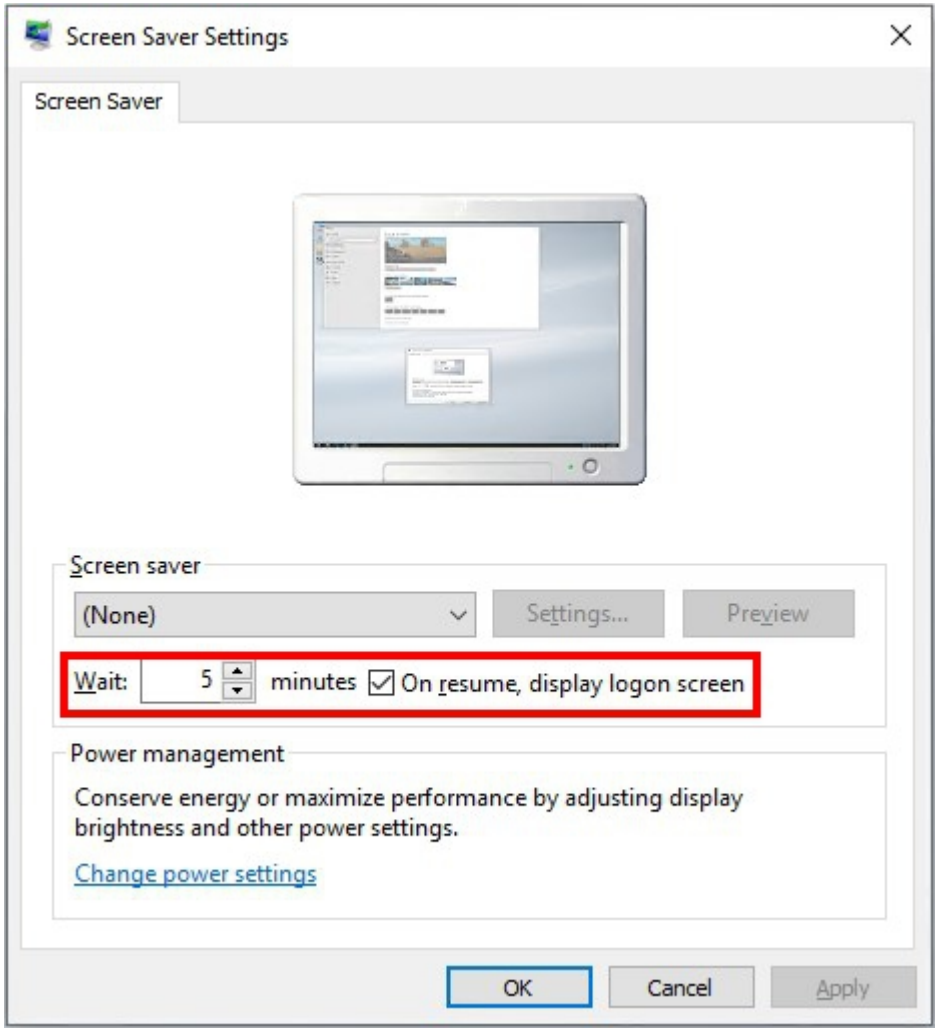
IPC 安全向导会提示用户更改默认密码。

另请参见：

- 信息系统中有关 IPC 诊断的文档

5.4.2 □□□□

为了防止已经登录的用户在一段时间未使用系统时误用系统，可以设置用户自动退出。为此，可以在“屏幕保护程序”设置中确定一个时间。时间一到，未使用的系统就会锁定，用户需要再次进行身份验证。



5.4.3 □□□□

作为将设备集成到网络中的安全方案的一部分，应规定哪一级安全审计适合检测潜在的攻击。安全审计指的是，一旦发生与设备的交互，工业 PC 就会立即创建事件审计日志。例如，用户每次访问选定的文件或文件夹时，都可以对文件和文件夹的访问进行记录。

这些日志可用于审查，偏离正常的使用情况以发现潜在的攻击，或用于取证，以重建有关攻击的细节。可以随时进行检查，也可以通过自动化机制或人工定期进行。至于哪些异常是相关的，这取决于环境和应用。因此，通常使用审计策略来配置哪些操作需要被记录。

然而，配置过多规则会导致盲区的形成。日志可能会被无关条目充斥，相关条目很容易被人为忽略，或者不能被自动监控机制快速处理。有时，将日志转发到中央位置进行自动审查和/或存档等操作，是避免耗尽有限日志容量的良好做法。

Microsoft 发布了一份 Windows 安全审计指南，其中包含相关设置和最佳实践。基本审计策略包括以下类别，这些类别可以启用，默认为禁用：

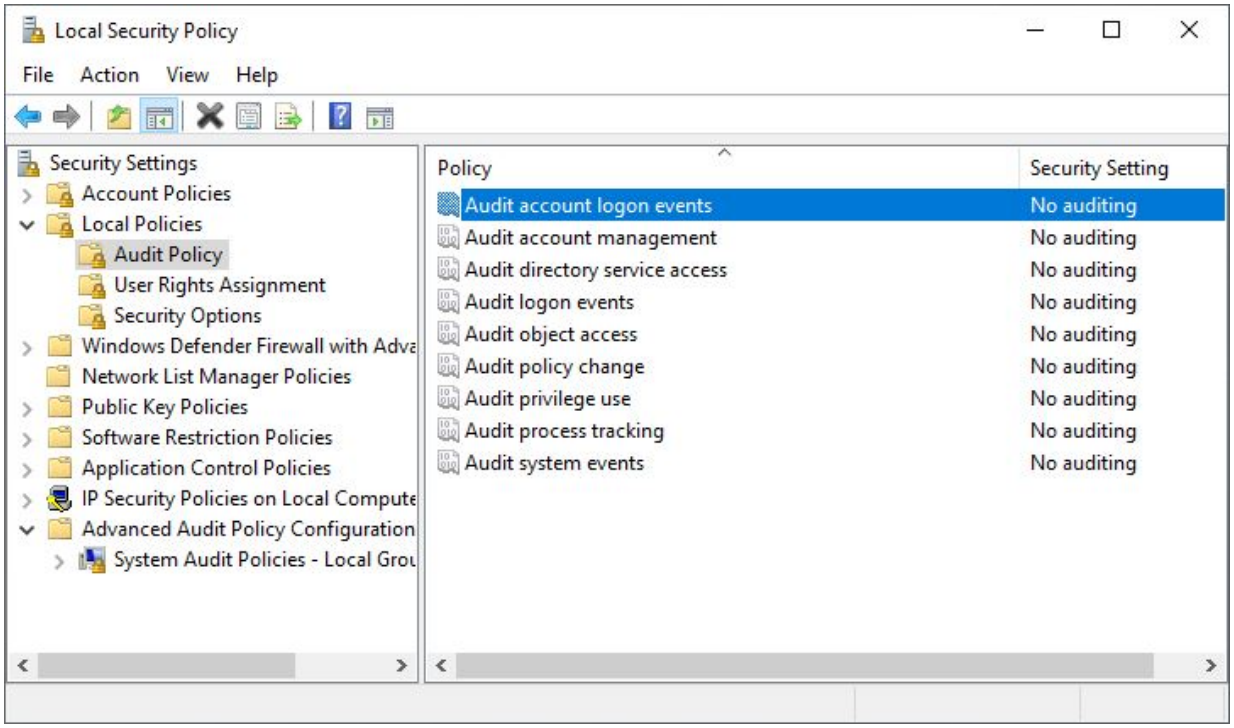
- 审计账户登录事件 [▶ 26]
- 审计目录服务访问 [▶ 27]
- 审计登录事件
- 审计对象访问
- 审计策略变更
- 审计权限使用情况
- 审计流程跟踪
- 审计系统事件

5.4.3.1 □□□□□□□□

在倍福设备管理器中审计登录事件，如果要确定谁从哪个 IP 地址登录了网络界面等，则会启用相应的策略。

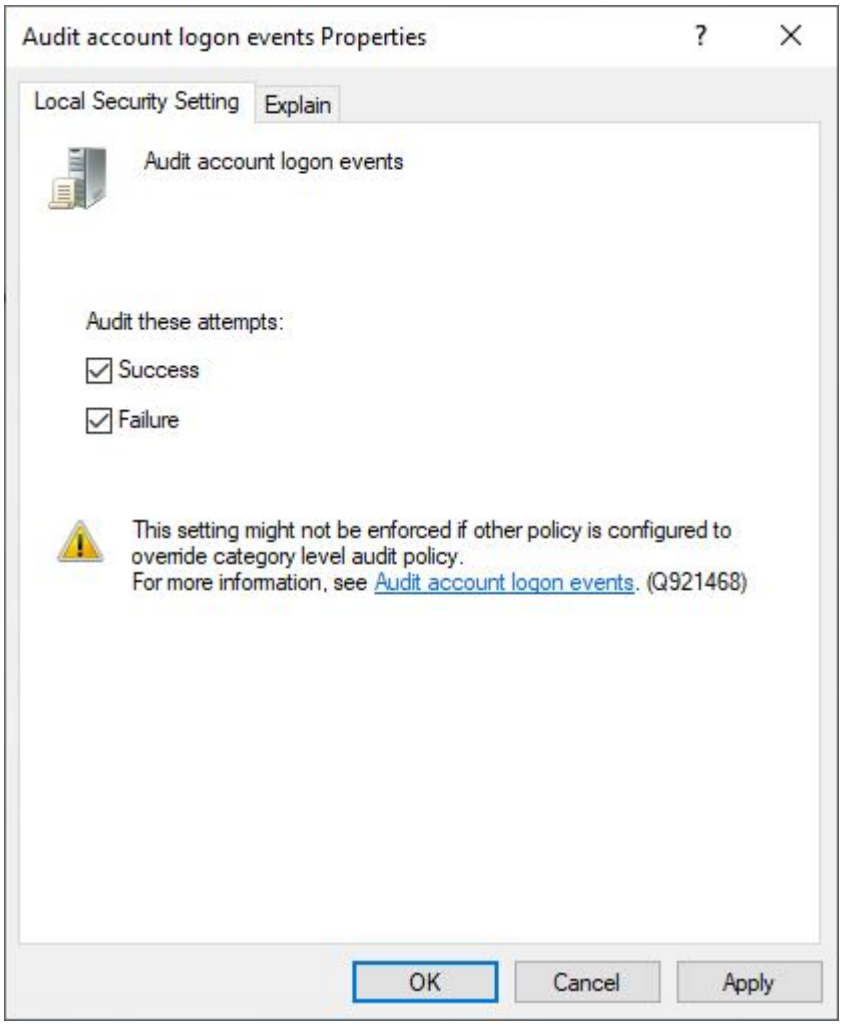
操作步骤如下：

1. 通过快捷键 **[Windows 键] + [R]** 调出“运行”对话框，输入 **secpol.msc**。
   出现**本地安全策略**窗口。



2. 点击左侧结构树中的**本地策略 > 审计策略**，然后选择策略**审计账户登录事件**。

3. 如果只想记录未成功的尝试，请选择**失败**复选框。如果还想记录成功尝试，请选择**成功**复选框。



⇨ 现在可以在**事件查看器**中查看记录的条目，通过 **[Windows 键] + [R]** 和条目 **eventvwr** 即可调用。然后可以在 **Windows 日志 > 安全**下查看这些条目。

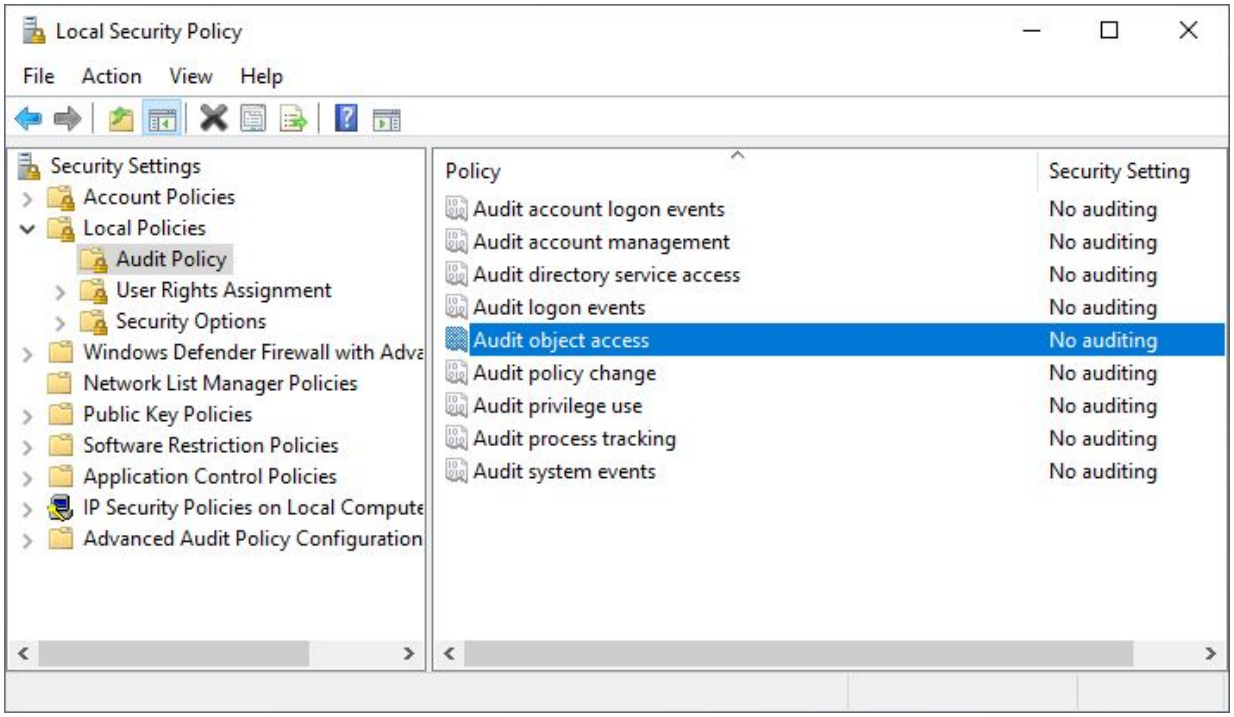
5.4.3.2 □□□□□□□□

Windows 日志的大小随着每条日志条目的添加而增大。注意可用的硬盘空间。

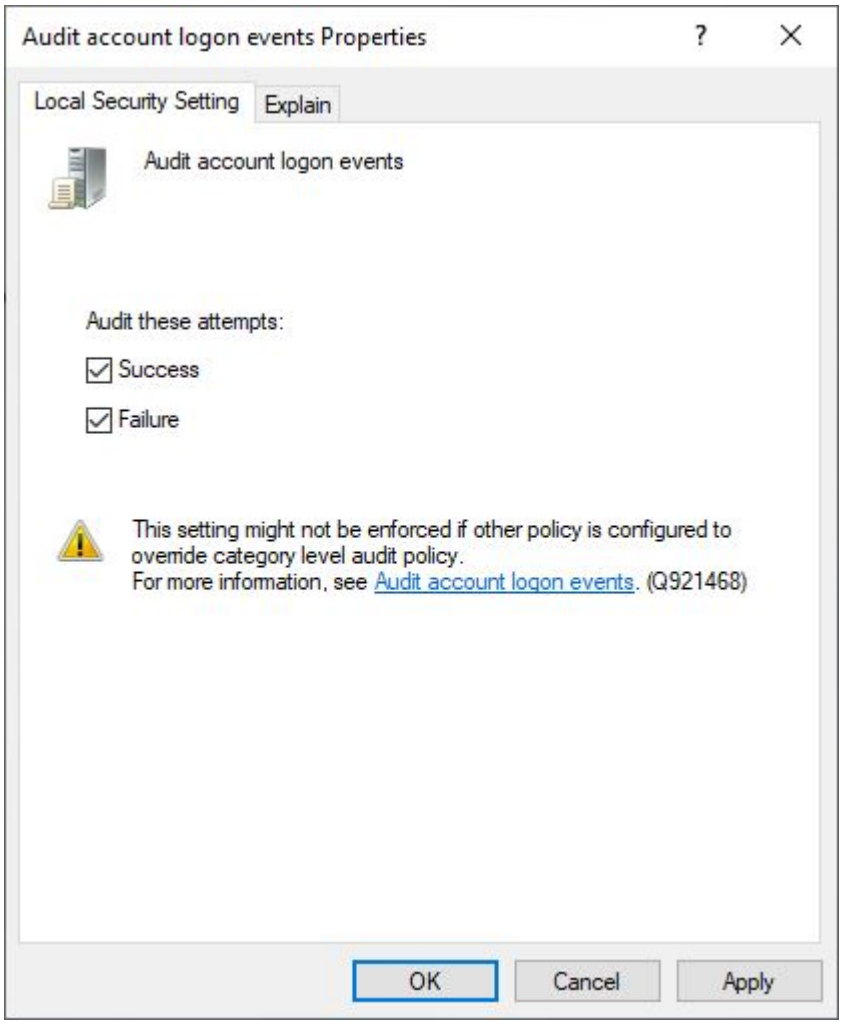
文件和文件夹访问操作可以在 Windows 中进行记录。每当用户访问选定的文件或文件夹时，Windows 日志中就会记录所谓的审核事件。

创建文件和文件夹访问审计策略：

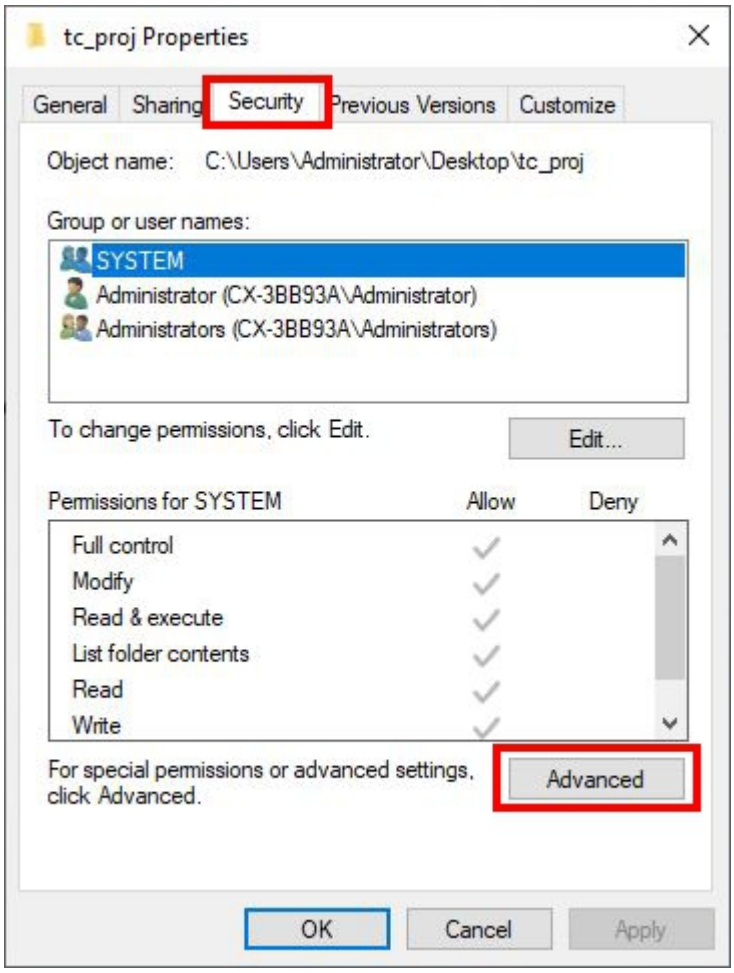
1. 通过快捷键 **[Windows 键] + [R]** 调出“运行”对话框，输入 **secpol.msc**。
   出现**本地安全策略**窗口。



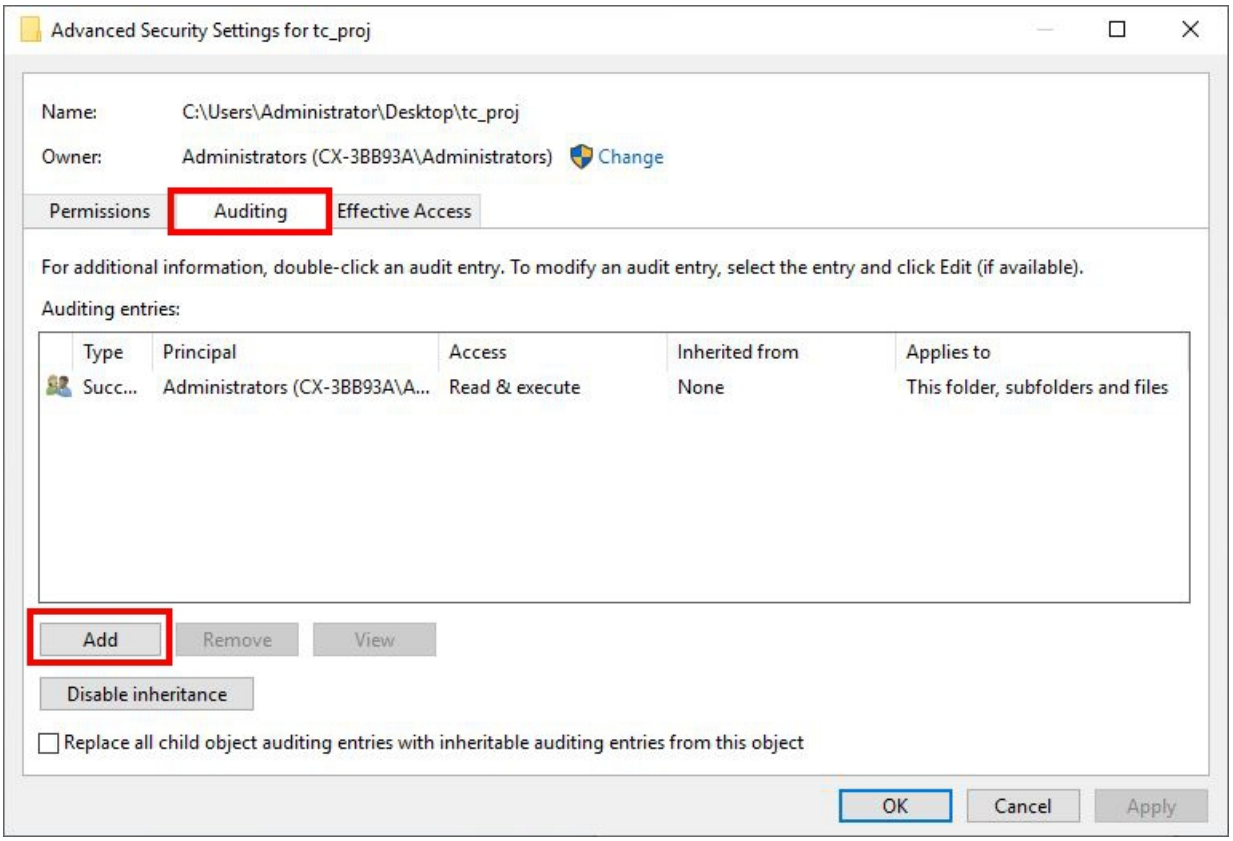
2. 单击左侧结构树中的**本地策略 > 审计策略**，然后选择**审核对象访问**策略。
3. 如果只想记录未成功的访问，请选择**失败**复选框。如果还想记录成功访问，请选择**成功**复选框。



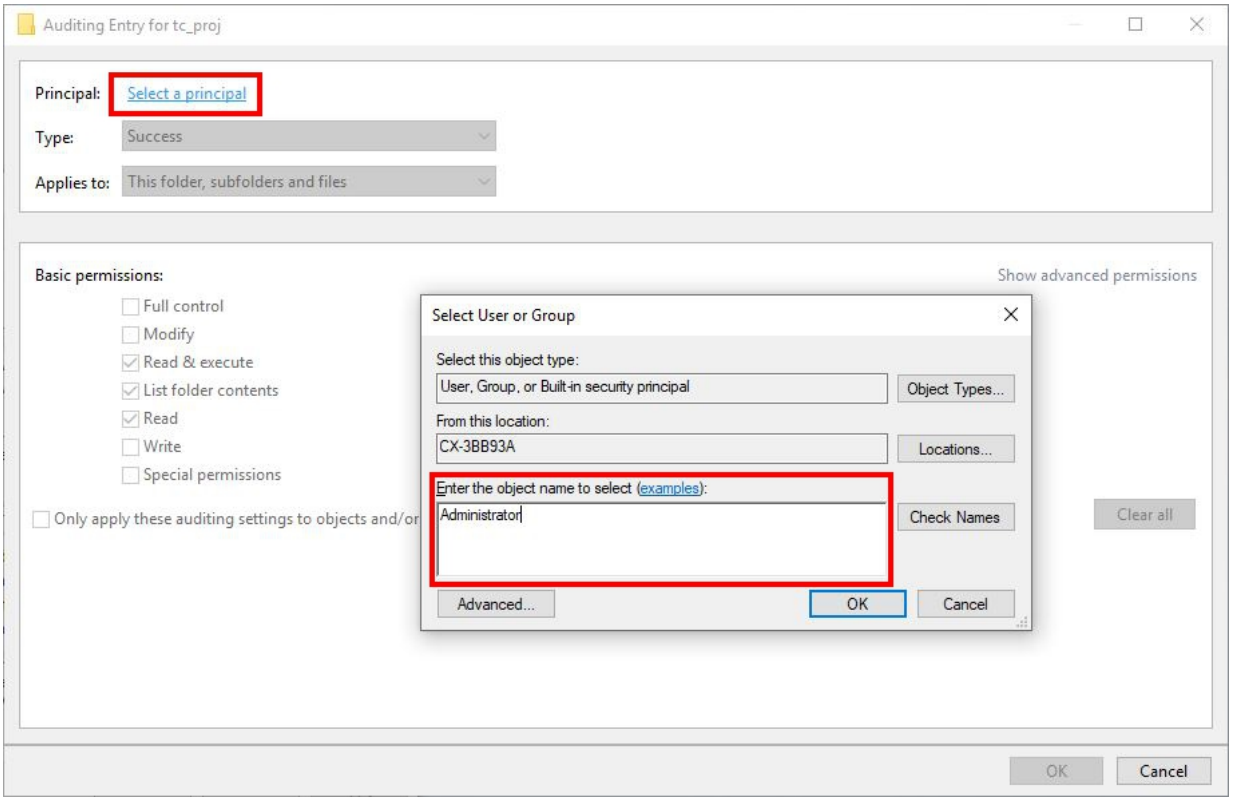
4. 右键单击相关文件或文件夹，然后点击**属性**。
5. 选择**安全**选项卡，然后点击**高级**。



6. 选择**审计**选项卡，点击**添加**，创建新的审计条目。



7. 要为用户或组设置审计，请输入所需用户或组的名称，然后选择**确定**。



8. 现在可以在**事件查看器**中查看记录的条目，通过 **[Windows 键] + [R]** 和条目 **eventvwr** 即可调用。然后可以在 **Windows 日志 > 安全**下查看这些条目。

5.5 □□

5.5.1 □□□□□

应用程序白名单可防止执行所有未经系统批准的程序。通过白名单，管理员可创建一个允许系统执行的经批准的应用程序列表。与杀毒软件不同的是，无需持续更新即可修复当前的安全漏洞。只有在添加新的应用程序时，才需要扩大列表。在工业实践中，该列表往往比杀毒软件更容易维护。Windows 内置功能名为 AppLocker。

通过白名单措施，您可以明确指定哪些程序可以在系统上执行。这些措施可防范不受信任的代码。

Windows 提供两种白名单制定方式：

- 软件限制策略 (SRP)
- AppLocker

软件限制策略提供一个范围，明确指定哪些程序可以在系统上执行。所有其他程序都不再能执行。这些策略可通过“本地安全策略”获得。

Windows 7 提供 AppLocker，具有扩展的功能范围。AppLocker 和 SRP 的差别参见此处。

5.5.1.1 □□□□□□ (SRP)

可以将安全级别设置为默认值。可以为默认级别定义例外情况。

安全级别	描述
不允许	程序无法执行。
默认用户	程序可以使用默认用户的权限运行。
无限制	每个用户都可以不受限制地运行程序。

可以为某些程序定义下列例外规则。这些规则被称为附加规则：

类型	描述
哈希规则	对于特定版本中的未修改程序文件，忽略文件名。 **注意 如需更新，必须更新这些哈希规则。**
证书规则	用于正确签署的已设置其发行者证书的程序文件。
路径规则	用于特定路径中的程序文件。路径还可以包含占位符和环境变量 (如 %PROGRAMFILES%)。
联网区规则	由 Internet Explorer 定义的网络区域中的程序。

以下步骤可以帮助您设置 Windows 的 kiosk 模式，在该模式下可以运行多个应用程序：

https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/applocker-overview

Microsoft 的一般部署指南可在此处找到：

https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-policies-deployment-guide

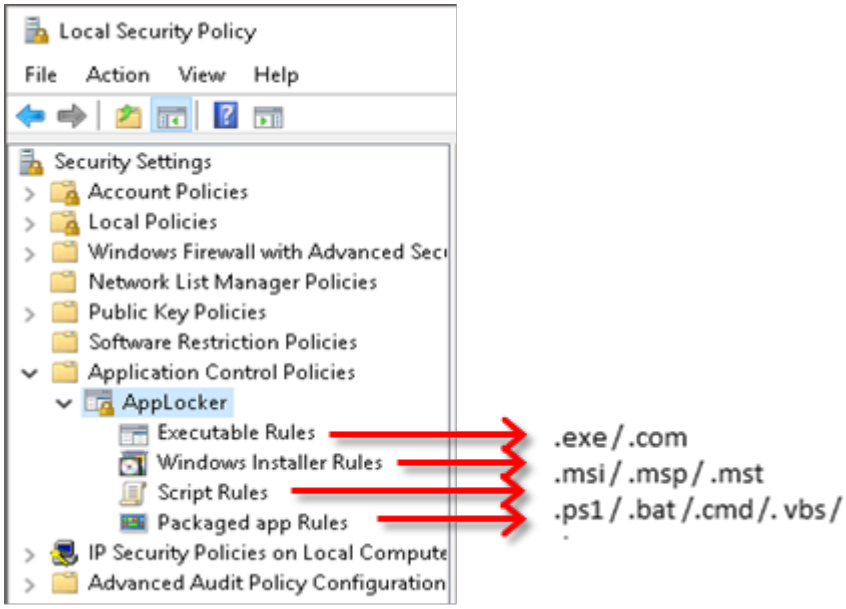
另请参见：

- AppLocker [▶ 31]

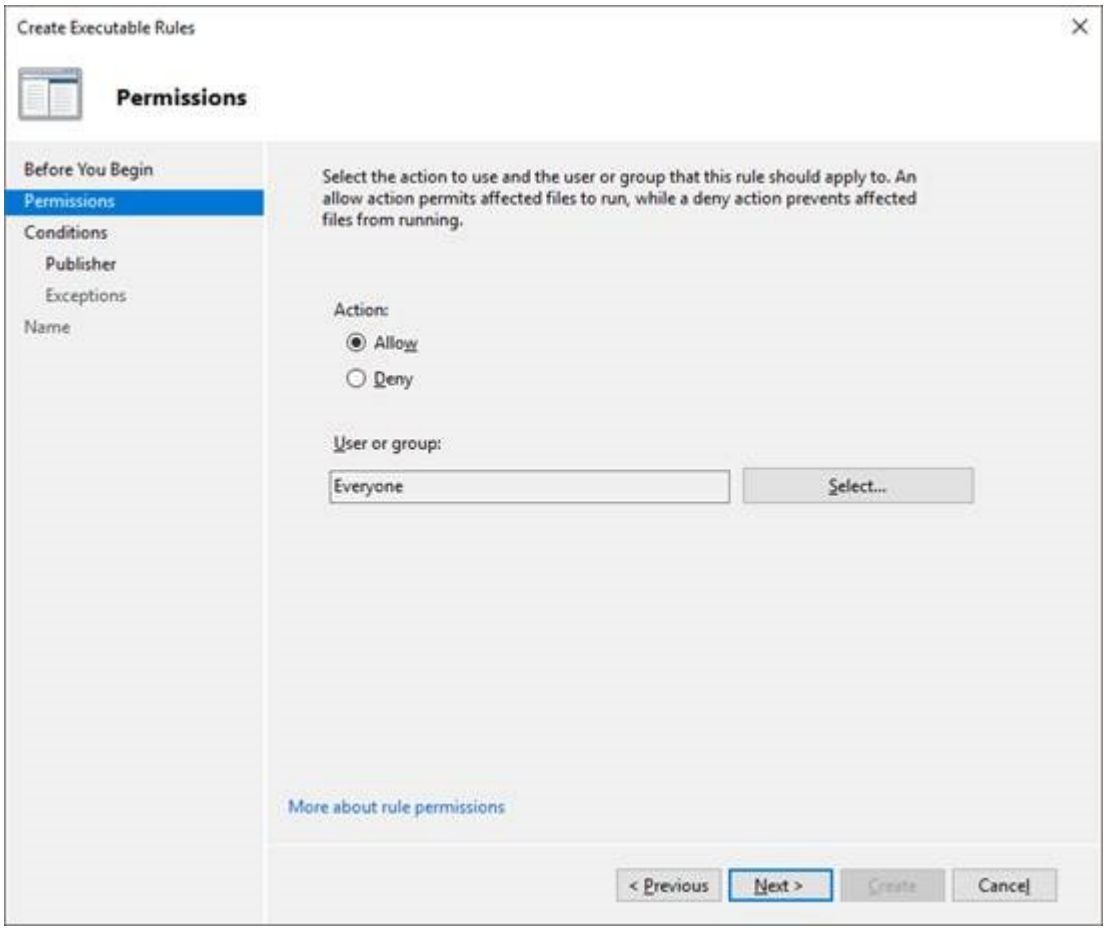
5.5.1.2 AppLocker

AppLocker 可以限制程序的运行。

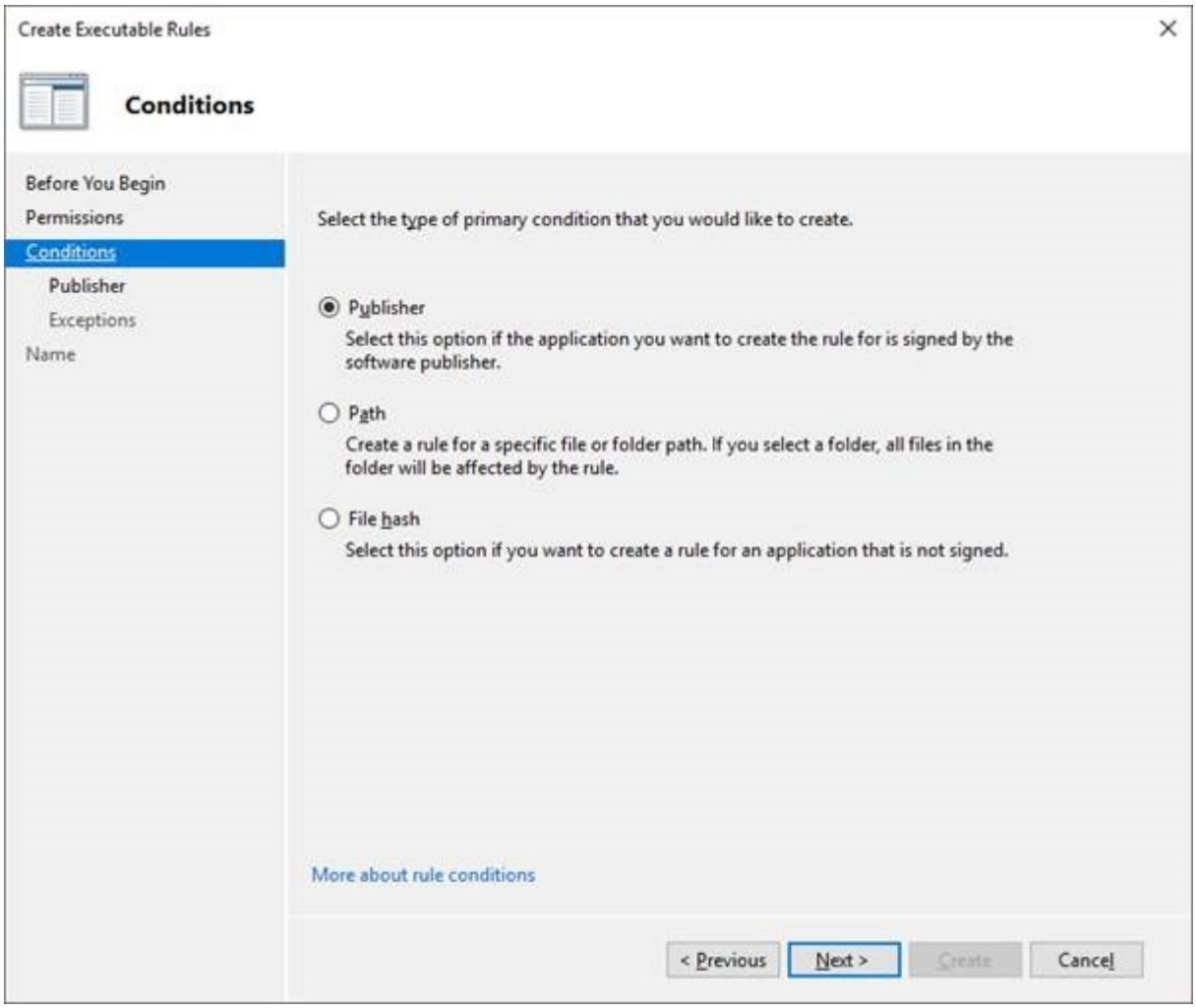
1. 运行 **secpol.msc** 打开安全策略。选择**应用程序控制策略**，在其下方选择 **AppLocker**。规则可涵盖各种数据类型：



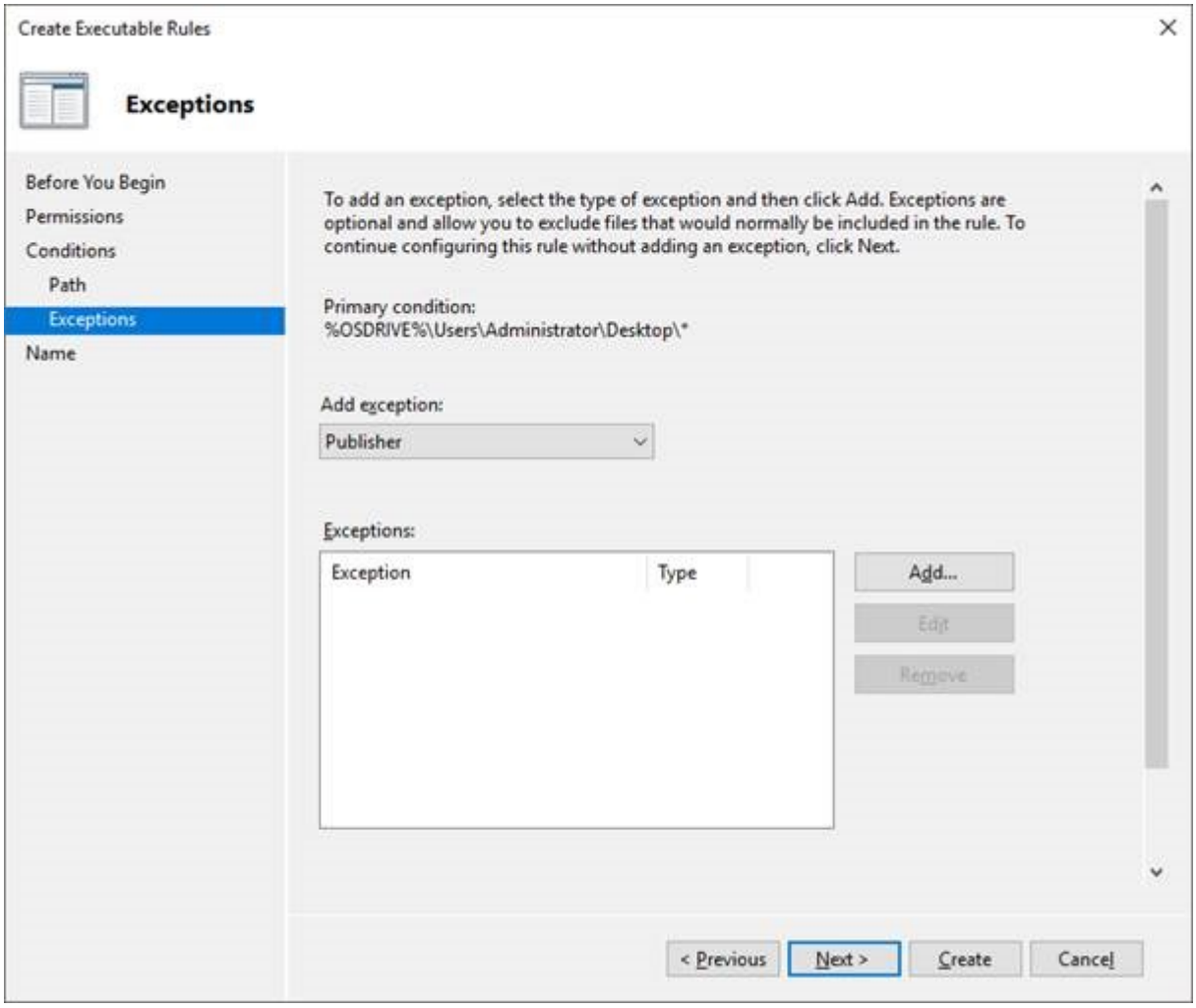
2. 您可以右键单击其中一条规则，选择**创建新规则**。
3. 选择**允许**或**拒绝**，以及规则应适用的**用户**或**组**：



4. 为新规则选择主要条件类型：



5. 您可以通过指定**“发布者”**、**“路径”**或**“文件”哈希值**更精确地指定规则。此外，“发布者”、“路径”和“文件”哈希值都可以从规则中排除：



⇨ 至此，配置工作就完成了。

注意事项：

- AppLocker 默认作为“允许列表”运行。
  - AppLocker 最初会检查是否有任何拒绝操作的规则。
  - 拒绝操作的规则比允许操作的规则优先级更高。
- 应允许使用所有 Windows 系统文件。
- 可以创建所谓的“标准规则”（Windows 系统文件规则）。
- 您可以通过 AppLocker 将自己锁定在自己的系统之外。

补充说明：

- 可以将规则从一台机器导入/导出到另一台机器。
- 规则保存在 HLKM\Software\Policies\Microsoft\Windows\SrpV2 中。
- 必须启动应用程序身份识别服务 (Appidsvc) 才能识别文件。

更多信息请参见 Microsoft 文档：

- https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/using-software-restriction-policies-and-applocker-policies

5.5.2 □□□□

为了禁止使用某些只提供给有限用户组的特性，应通过操作系统的功能阻断或隐藏这些特性。

也可以通过白名单措施限制程序及其执行。

另请参见：

程序白名单 [▶ 31]

在 Windows 下，可以通过更改注册表隐藏以下功能：

□□□

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
```

名为“DisableRegistryTool”且值为 1 的条目可以防止用户启动注册表编辑器。

□□□□□

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
```

名为“DisableCMD”的条目根据其值有不同的作用：

- 0：允许命令行访问，可以执行批处理文件。
- 1：不允许命令行访问，不可以执行批处理文件。
- 2：不允许命令行访问，但可以执行批处理文件。

□□□□

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEum\
```

名为“{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}”且值为 1 的 DWORD 条目将隐藏网络环境。

□□□□□□□□

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
```

名为“NoViewOnDrive”和“NoDrives”的 REG_DWORD 条目可以用来配置应该被限制的驱动器字母。“NoViewOnDrives”限制访问驱动器。“NoDrives”仅隐藏驱动器字母。访问仍可进行。要输入的值是下表中对应字母的条目总和：

A：1	**G**：64	**M**：4096	**S**：262144	**Y**：16777216
B：2	**H**：128	**N**：8192	**T**：524288	**Z**：33554432
C：4	**I**：256	**O**：16384	**U**：1048576	**All**：67108863
D：8	**J**：512	**P**：32768	**V**：2097152	
E：16	**K**：1024	**Q**：65536	**W**：4194304	
F：32	**L**：2048	**R**：131072	**X**：8388608	

例如，若要限制对驱动器 A、B、D 和 P 的访问，输入数值 1 + 2 + 8 + 32768 = 32779。设置值之后，操作系统必须重新启动，以使设置生效。

更多设置选项汇总于此处。

5.5.3 □□□□□□□□□

为了减小攻击面，应删除不需要的程序和操作系统组件。

只能由精通人士卸载系统组件。否则可能会出现异常导致程序无法再正确运行。

在**程序和功能**下的**控制面板**中，您可以卸载不需要的程序和 Windows 组件。

运行“control appwiz.cpl”可直接访问该功能。

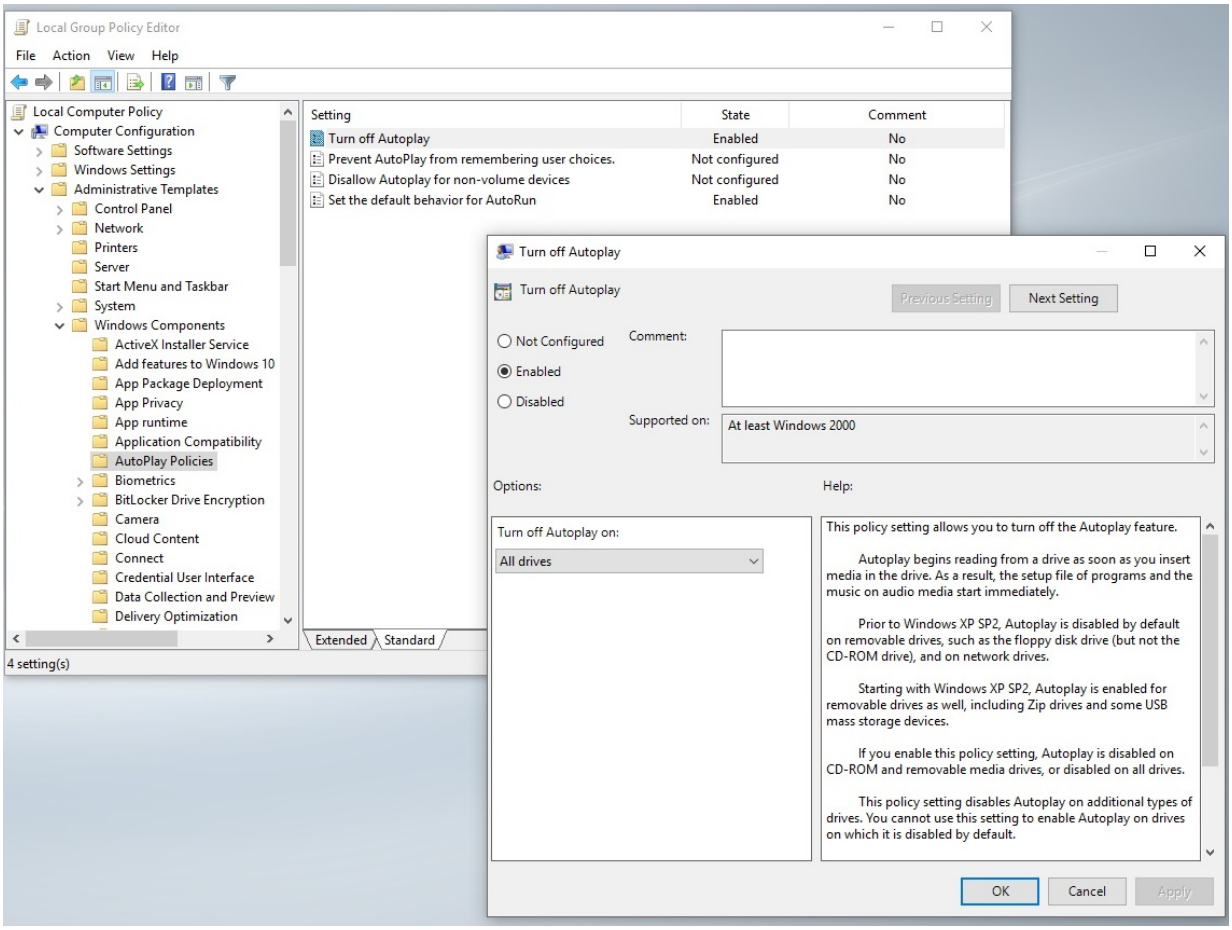
5.5.4 AutoStart□□□□□□

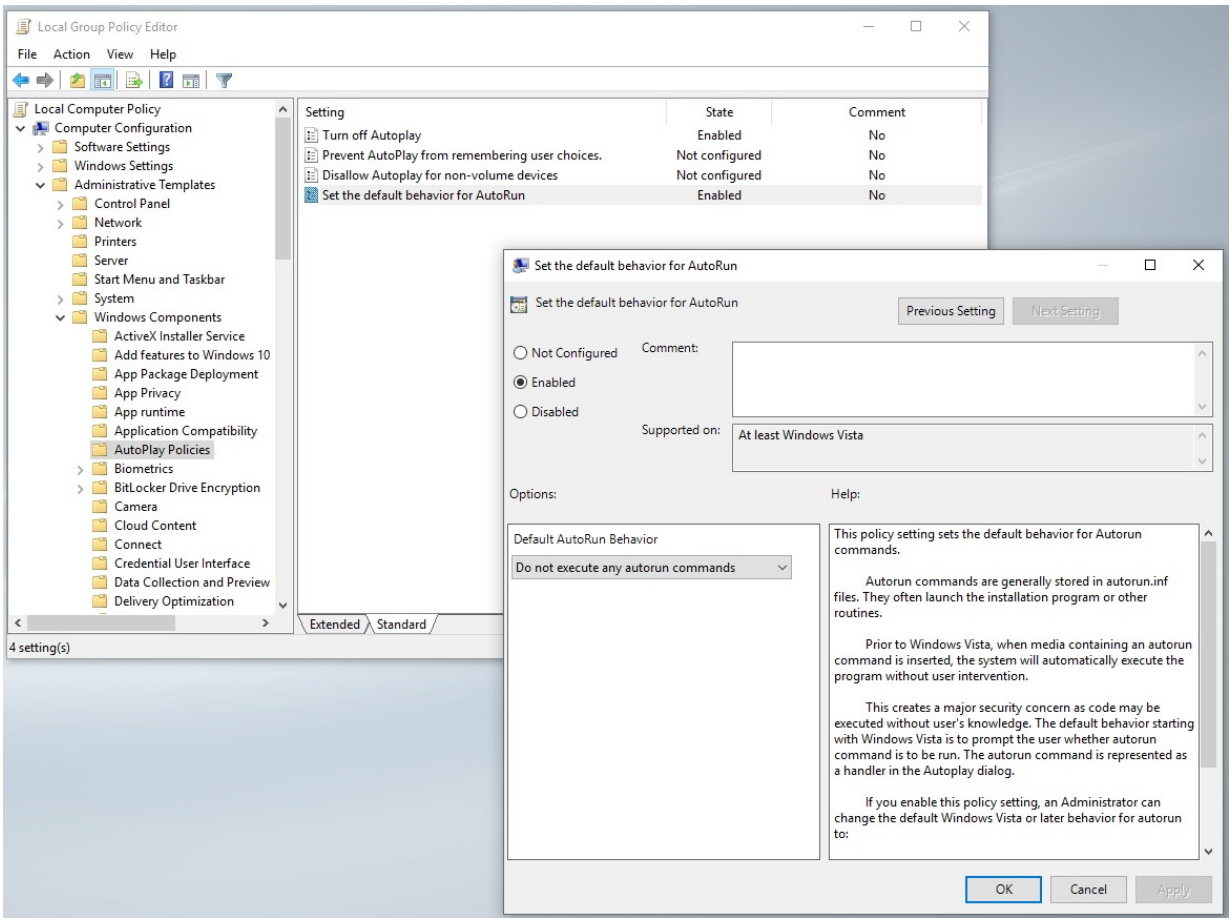
当连接外部设备时 (例如 USB 存储介质或键盘)，控制器很容易通过这些连接被感染。尤其是当插入 USB 介质后操作系统就立即执行自启动操作。

如果不需要这些机制，应该将其停用。这里对 AutoPlay（自动播放）（播放已安装软件的媒体）和 AutoRun（自动运行）（启动程序）进行了区分。

为了要通过组策略完全停用自动运行和自动播放功能，应采取以下步骤。

1. 打开组策略（运行“gpedit.msc”）并导航至计算机配置 > 管理模板 > Windows 组件 >**自动播放策略**。在这里，配置策略**关闭自动播放**和**设置自动运行的默认行为**，如下所示





⇨ 重新启动后，设置完成。

5.5.5 □□□□

杀毒软件可保护系统，防止恶意软件通过数据载体或网络侵入系统。它代表的是已知恶意软件的黑名单。杀毒软件必须始终保持最新状态，以便识别恶意软件。这样做也有弊端。

反病毒程序会识别已知的恶意软件（“黑名单”），并试图阻止执行恶意软件代码。

然而，需要不断的对该黑名单（“恶意软件模式”）进行更新，这反而可能增加杀毒程序对系统的危害。

如果在一台机器上总是运行同一个程序，则应使用前面介绍的白名单方法。在任何情况下，都必须进行权衡：像杀毒程序那样采用黑名单方法从总体上看是否有利。总之，应把白名单方法较高的配置工作量，与需要不断更新杀毒程序的工作量进行权衡。

过去的实践证明，Windows Defender 是可靠的，并且与 TwinCAT 兼容。然而，它必须始终更新到最新版本，以修复当前的安全漏洞。

特别是与 TwinCAT 结合使用时，必须对杀毒程序的使用进行谨慎的评估，因为这些程序会在操作系统中进行深度设置，从而影响 TwinCAT 的实时集成能力。

TwinCAT 对自身与杀毒程序的兼容性有自己的描述：

杀毒程序的兼容性

更多信息请参阅 Microsoft 文档：https://support.microsoft.com/en-us/windows/stay-protected-with-the-windows-security-app-2ae0363d-0ada-c064-8b56-6a39afb6a963

5.6 □□□□□

Windows 写入过滤器是 Microsoft Windows 专门开发的工具，用于保护分区免受写入访问。写入访问会重定向到 RAM，因此分区在预配置状态下会得到保护。在重新启动后，系统会自动重置为最初定义的状态。

可根据使用情况配置写入保护过滤器。这样，系统便不会受到意外写入访问的影响。排除项定义了仍允许写入访问的文件夹。

□□□□□□□□□□

从操作员的角度来看，如果在重新启动后，恶意软件所作的更改被撤销，并且可以恢复操作，这是合理的。但这样做的结果是，很少能收集到关于感染或攻击的信息，攻击随后可能再次发生。

而且，打开和关闭写过滤器并无安全保证。在攻击已经发生的情况下，如果用户改变写入过滤器设置，那么攻击者也有权限这样做。

注意

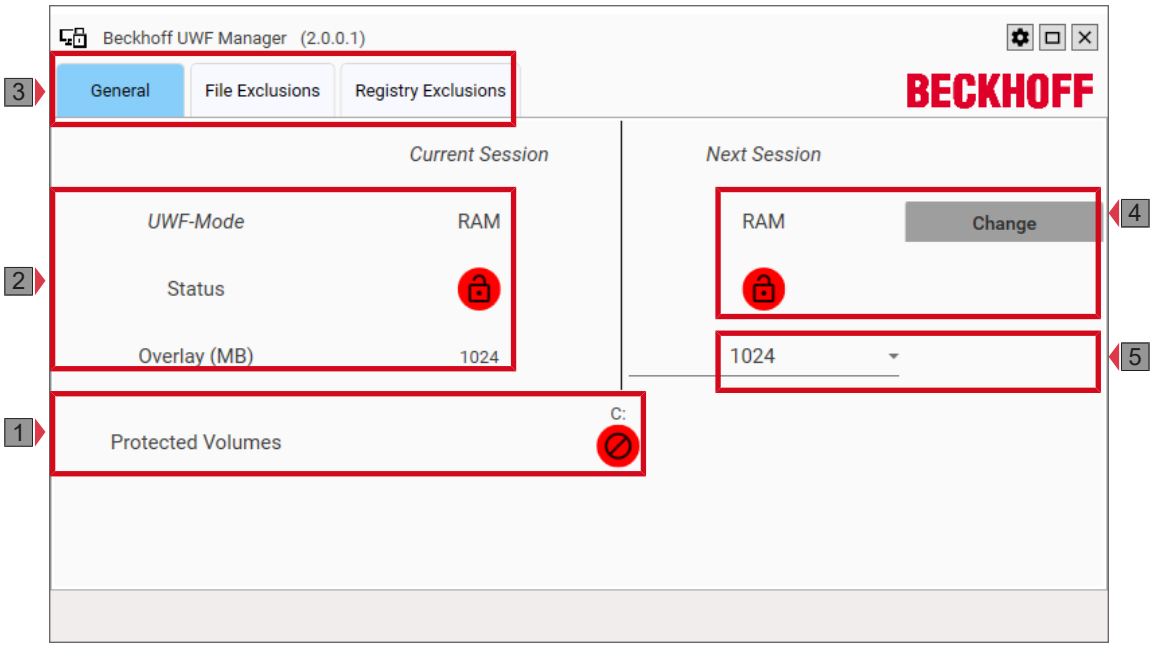
过满的 RAM 覆盖和磁盘覆盖

在没有持续监控容量使用和默认容量设置的情况下，UWF 不适合连续运行（全天候）。由于写入访问（即使在排除区域），RAM 覆盖或磁盘覆盖会分别持续增长到最大预设值，直到写入访问失败。这样，操作系统便无法再运行。

UWF（统一写入过滤器）是从 Windows 10 以上版本安装的写入过滤器。用户可以通过图形用户界面使用“倍福统一写入过滤器管理器”控制 UWF。该软件提供了一个简单的配置选项。全部功能可在 Windows 命令行中使用，Microsoft 文档中有详细介绍：
https://docs.microsoft.com/de-de/windows-hardware/customize/enterprise/unified-write-filter

UWF □□□□□

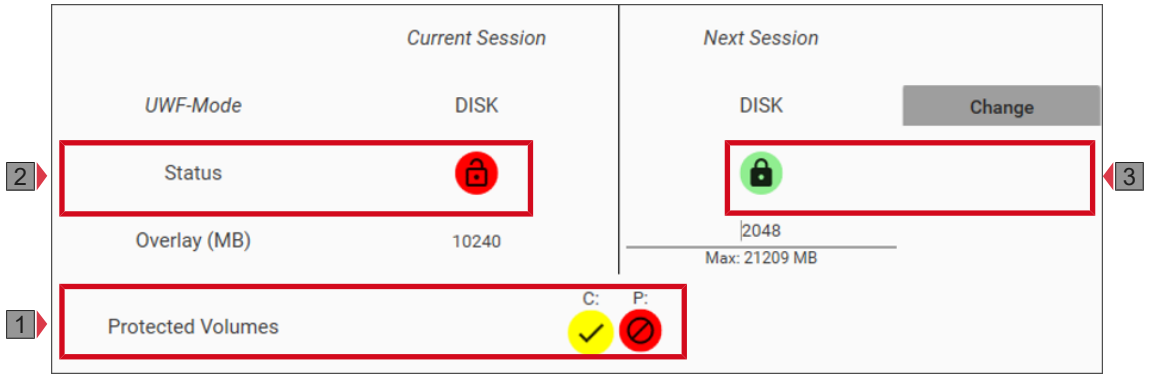
可以在**常规**选项卡上设置 UWF 模式、状态和覆盖大小。在此启用或禁用写入过滤器。



附图 1: UWF 管理器处于 RAM 模式，分区 C：未受保护。

表 1: *UWF* □□□□□□

编号	描述
1	通过该按钮可以保护各个分区。
2	此处显示当前的 UWF 模式、状态和覆盖大小。
3	可在这些选项卡上定义文件和注册表排除项。
4	如果发生变化，此处会显示 UWF 的未来状态。使用**更改**按钮在 RAM 和磁盘模式之间切换。
5	可通过此框设置覆盖大小。



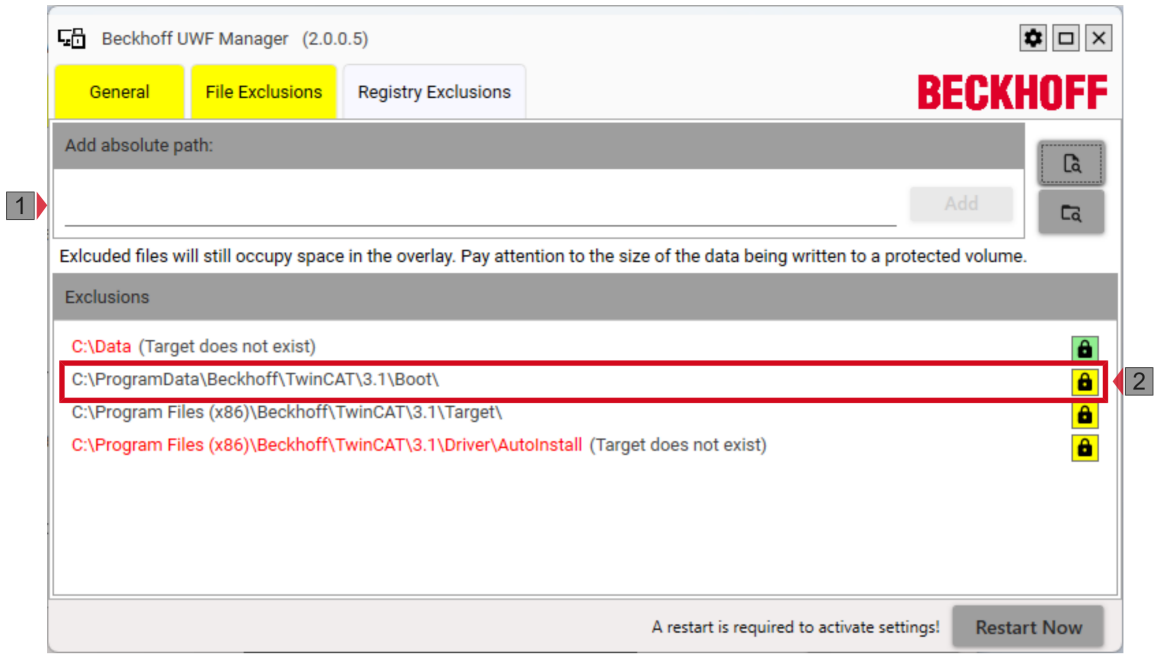
附图 2: UWF 管理器处于磁盘模式，下一次重启时保护分区 C：。

表 2: *UWF* □□□□□□□□□

编号	描述
1	红色 = 关闭，无保护
2	绿色 = 开启，受保护
3	黄色 = 开启，下次重启后受保护。

□□□□□

在“文件排除项”选项卡上，可以确定例外情况，并允许对单个文件或文件夹进行写入访问。



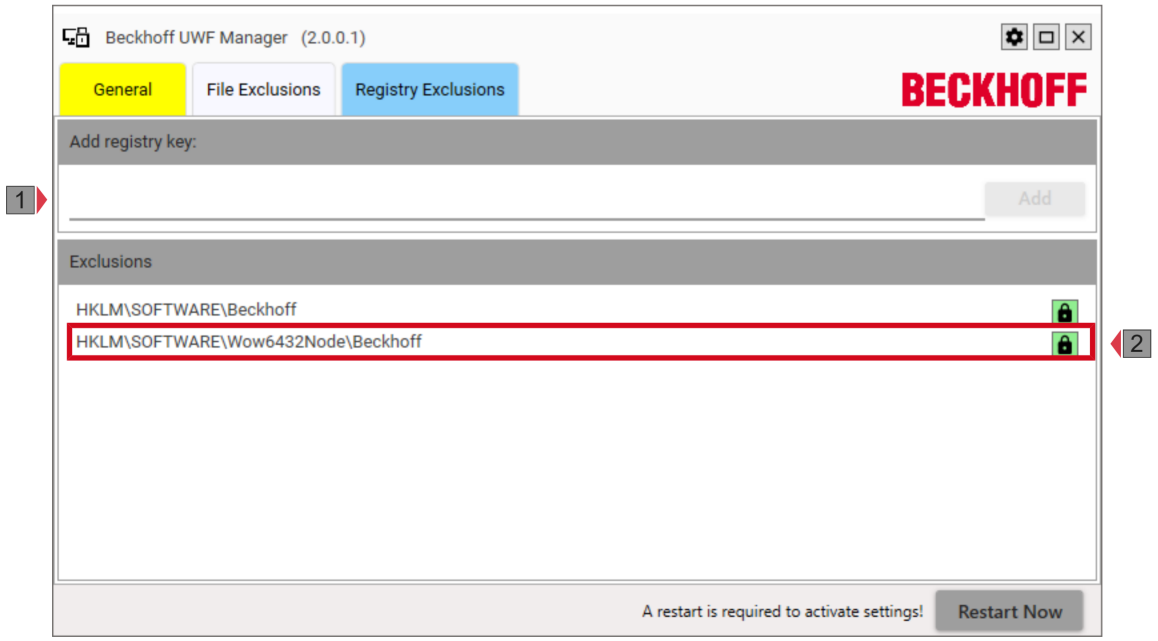
附图 3: UWF 管理器的文件排除项。

表 3: *UWF* 管理器图例（文件排除项）。

编号	描述
1	可通过此框在排除项中添加新文件夹。
2	可通过此按钮打开或关闭现有排除项。

注册表排除项

可以在“注册表排除项”选项卡上确定例外情况，并允许对单个注册表键值进行写入访问。



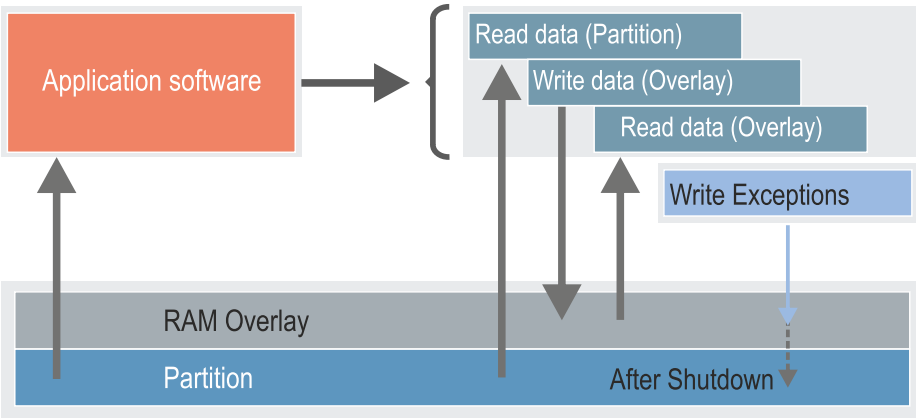
附图 4: UWF 管理器的注册表排除项。

表 4: *UWF* 管理器图例（注册表排除项）。

编号	描述
1	可通过此框将新注册表键值添加到排除项中。

编号	描述
2	可通过此按钮打开或关闭现有排除项。

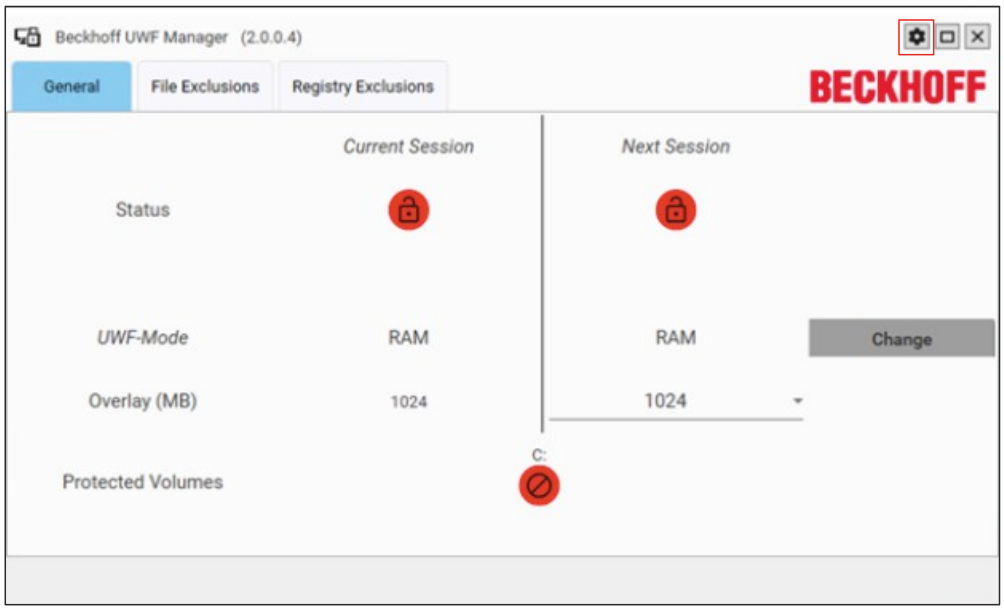
在 UWF 处于活动状态的情况下，对主存（RAM 覆盖）或磁盘覆盖的所有写入访问会分别被分流，分区仅用于读取。重启后，Windows 将重新以先前定义的状态启动。



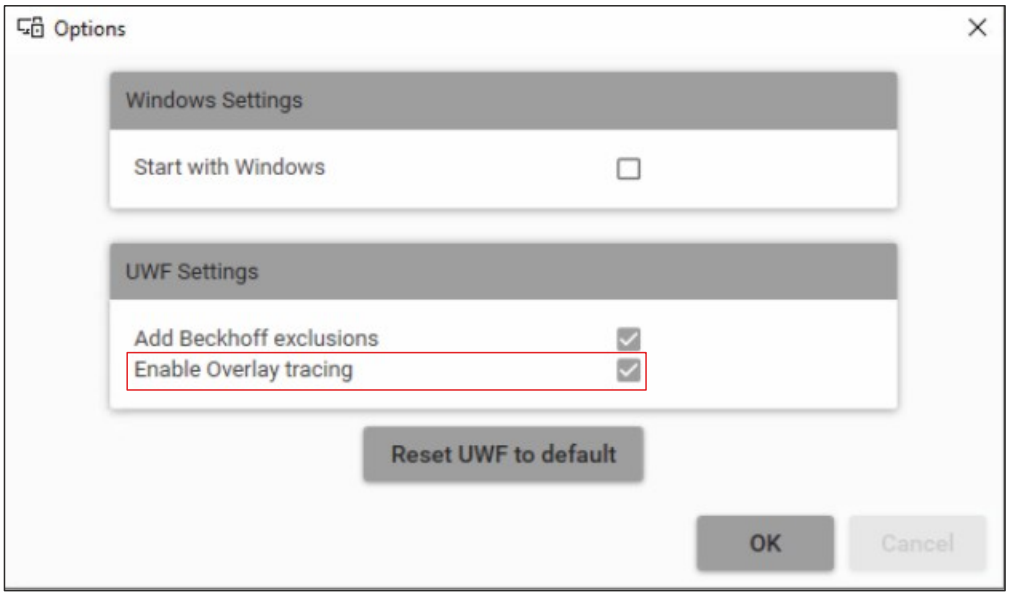
附图 5: Windows 写入过滤器，应用软件在 RAM 模式下的运行模式。

此外，还可以使用 UWF 确定例外情况，从而允许对单个文件、文件夹或注册表键值进行写入访问。请注意，例外情况只会在重启后写入分区，在此之前将在 RAM 覆盖或磁盘覆盖中缓冲。

如果系统向覆盖层写入大量数据，则应在 UWF 中将这些数据定义为例外情况。可以使用倍福 UWF 管理器分析覆盖内存及其包含的文件，以识别其内存占用。为此，必须在倍福 UWF 管理器的设置中设置“启用覆盖跟踪”复选框。

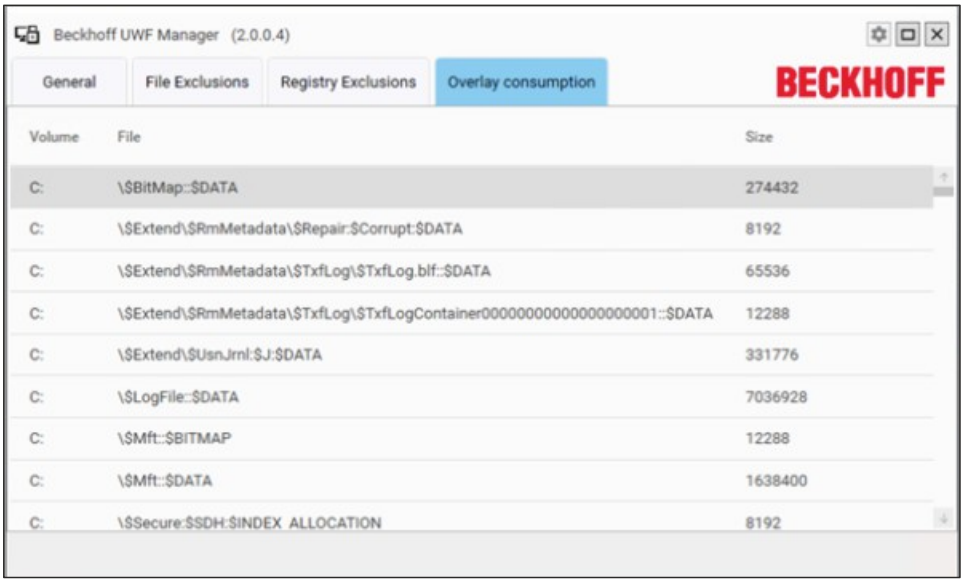


附图 6: UWF 管理器设置



附图 7: UWF 管理器“启用覆盖跟踪”复选框

启用 UWF 后重启 Windows，倍福 UWF 管理器中会出现一个附加选项卡，其中列出了覆盖层中的文件和相关文件大小。



附图 8: UWF 管理器覆盖消耗

在默认设置下，UWF 不适合连续运行

在默认设置下，UWF 不适合连续运行（全天候）。由于写入访问（即使在排除区域），RAM 覆盖或磁盘覆盖会分别持续增长到最大预设值，直到写入访问失败。只有在重启后才会再次启用覆盖功能。

无论 RAM 覆盖或磁盘覆盖的设置有多大，最终都可能在不重启的情况下填满。RAM 覆盖尤其岌岌可危，因为它最多可占主存总量的 50 %。如果 RAM 或磁盘覆盖已满，进一步的写入尝试会失败。在这种状态下，您的设备可能不再有反应，并可能变得迟缓。磁盘覆盖可能是一种解决方案，因为有足够的空闲内存就能生成相应的大覆盖。

请参见 Microsoft 文档：
https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/uwfoverlay

使用率高的警告

覆盖层负荷无法精确预测。新的 UWF 管理器优化了操作系统，以供使用 UWF，但无法确保全天候无故障运行，无一例外。在覆盖利用率为 50 % 和 70 % 时，为用户显示消息。请务必注意这些警告。

使用 UWF 进行备份和还原

在创建系统备份之前，必须先关闭 UWF。否则，还原系统中的 UWF 会被错误配置。恢复备份后，可再次为新创建的磁盘启用 UWF。

一般建议

1. 请勿在连续运行（全天候运行）中使用带有 RAM 覆盖的 UWF。
2. 在系统中连续开启 UWF 之前，应对其行为进行谨慎的分析。

针对不同应用场景的建议

- 数据少、RAM 充足、磁盘可用空间小 → RAM 模式
- 磁盘上有足够的可用空间，数据量可能较大 → 磁盘模式
- 数据量大 → 为数据创建第二卷，仅使用 UWF 保护 C:

5.7 □□□□□

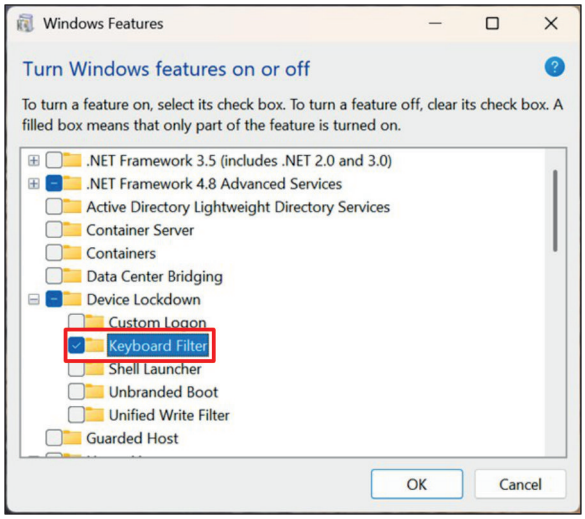
键盘过滤器是一种保护系统免受不良访问的可能性。例如，可以阻止导致应用程序退出的快捷键。仅启用应用程序操作所需的键盘输入。此外，还可以指定禁用键盘过滤器的快捷键。管理员不启用过滤器的选项也很常用。

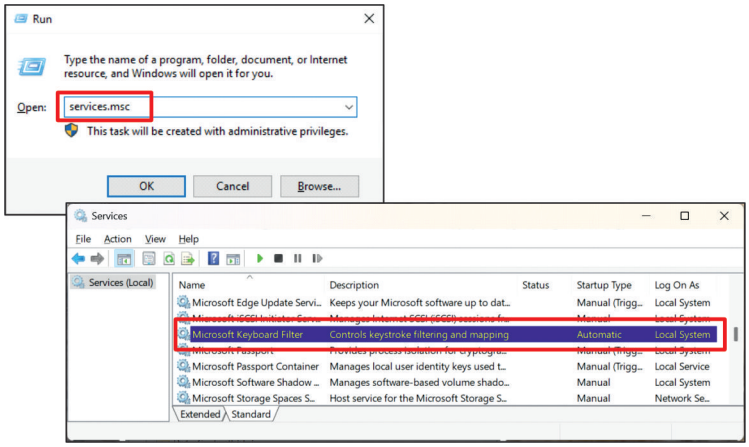
键盘过滤器提供了另一种方案，可以限制用户处理操作系统，从而将攻击的可能性降到最低。

通常情况下，会配置“kiosk 模式”，例如，成功登录的用户只能启动 HMI 应用程序。用户无法启动其他程序，也无法向 IPC 发送关闭等命令。

Windows 10 为此提供了一项服务。在此，我们将介绍如何激活以及如何进行配置。

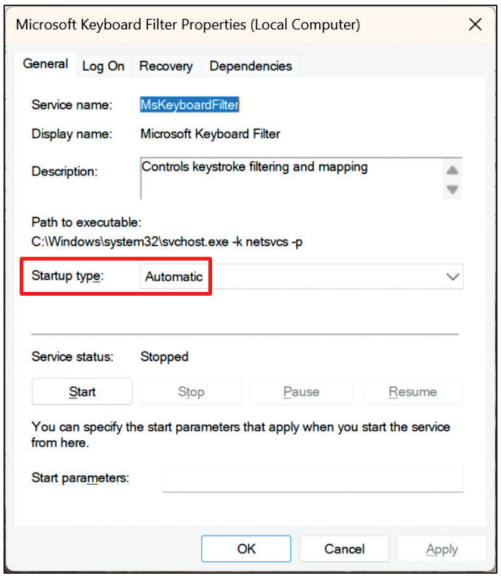
首先打开内置 Windows 10 功能，即可使用该服务。为此，请打开对话框**打开或关闭 Windows 功能**，并选择菜单项**设备锁定**下的**键盘过滤器**功能。然后重启 PC。



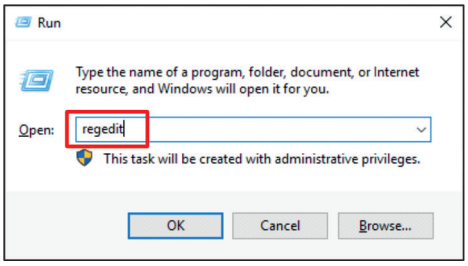


1. 启动 **Microsoft 键盘过滤器**服务。

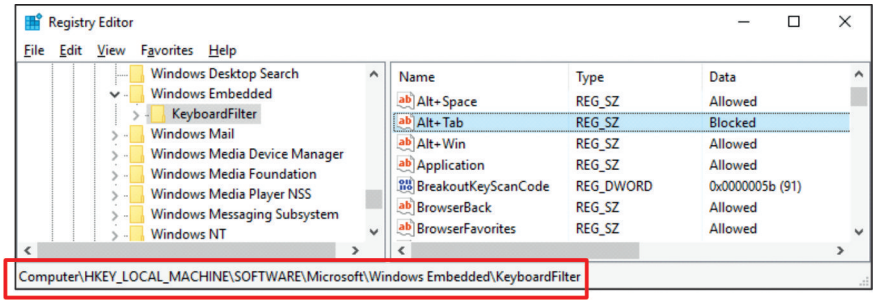
2. 将启动类型设置为**自动**：



3. 打开**注册表编辑器**



4. 导航至 **KeyboardFilter：HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows Embedded**



5. 数值和常用快捷方式都列在下表中。

⇨ 键盘过滤器现已激活。

以下数值代表各个快捷方式：

值	描述
“允许”	允许快捷方式
“封锁”	封锁快捷方式
DisableKeyboardFilterForAdministrator 至“1”	管理员不启用键盘过滤器
BreakoutKeyScanCode 至“01”	作为退出键的 ESC 扫描码

下列快捷方式通常会被屏蔽：

值	描述
CTRL-SHIFT-ESC	打开任务管理器
CTRL-ALT-DEL	使用以下选项打开菜单： 锁定系统 打开任务管理器 更改密码 关闭系统 切换用户

更多信息请参阅 Microsoft 文档：https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/keyboardfilter

5.8 USB □□□

与应用程序白名单类似，USB 设备也可以被列为受信任设备。操作系统将不接受不在批准列表中的 USB 设备。因此，为了维护设备，可以定义统一的 USB 服务闪存盘，其中只包含经批准的应用程序，并定期检查。因此，非特定应用程序（如私人）USB 闪存盘不会造成任何危害。USB 过滤器服务可作用于所有通过 USB 连接的设备。例如，还包括鼠标/键盘等 HID 设备，以及 USB 闪存盘、硬盘和读卡器等所有大容量存储设备。

然而，操作系统中的 USB 过滤器是指 USB 中的供应商和产品 ID（供应商 ID [VID]/产品 ID [PID]），这些 ID 没有加密安全性，可以伪造。

为了阻断 USB 等外部接口，可以对其进行物理保护，例如通过控制柜。但是，即使设备安装在控制柜里，也会出现已经使用或必须使用 USB 接口的情况。为了减小攻击面，在操作系统中对接口的使用应该是适当的和限制的。

然而，USB 过滤器匹配过的设备的 ID 并没有加密保护，这意味着使用经过专门伪造的 USB 设备进行恶意攻击可以绕过 USB 过滤器。

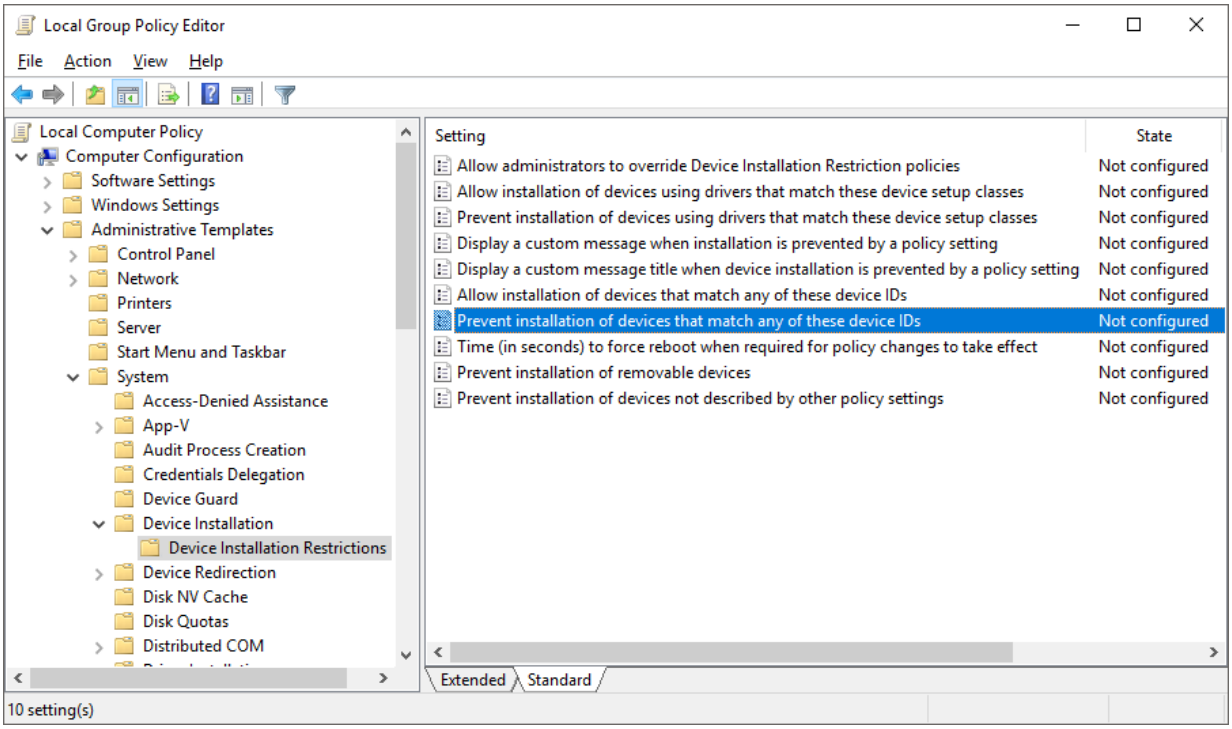
有多种在操作系统级别上限制 USB 设备的方法。

- 如果设备尚未安装，可通过拒绝当前用户和系统用户访问以下文件来防止安装：
  - %SystemRoot%\Inf\Usbstor.pnf
  - %SystemRoot%\Inf\Usbstor.inf
  - %SystemRoot%\System32\DriverStore\Usbstor.inf*
- 为了防止 USB 大容量存储设备的普遍使用，可在 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSer\services\USBSTOR` 下的注册表中将条目“ImagePath”设置为无效路径。
- 此处描述了如何通过策略设置 (分组策略) 更精确地限制 USB 设备的使用。
- 也可以在 BIOS 中关闭 USB 接口。注意，使用这种方式时，键盘和鼠标等输入设备将不能通过关闭的接口工作。

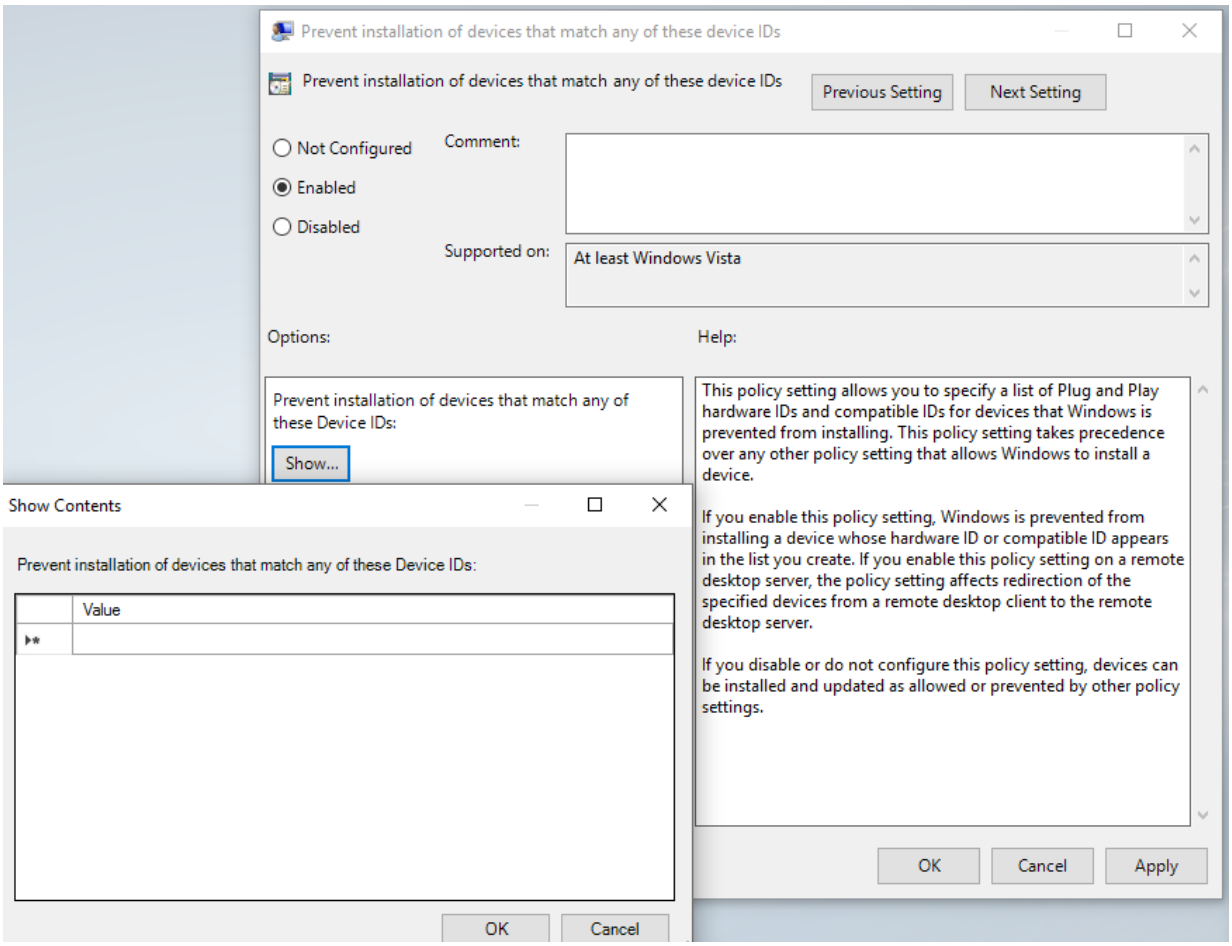
请注意，通过注册表设置的值不会自动与组策略中设置的值同步。建议完全通过组策略进行设置。

自 Windows 10 起，可配置用于处理 USB 设备的选项。

1. 在“运行”窗口中输入 **gpedit.msc**，打开组策略编辑器。根据应用程序，选择**防止/允许安装与这些设备 ID 中任何一个匹配的设备**



2. 激活组策略并输入允许或应阻止的设备：



⇨ USB 过滤器现已配置完毕。

有关更多信息，请参见 Microsoft 文档：http://msdn.microsoft.com/en-us/library/bb530324.aspx

6 □□□□

在此，我们将概述一些与通信有关的措施。不涉及实际 IPC 以外的主题，如网络分段。

TwinCAT 产品使用的端口列表可见此处：重要 TCP/UDP 端口 [▶ 51]。

6.1 □□□□

远程维护在工业设施中起着重要的作用。它使服务技术人员和程序员能够在发生故障时进行远程维护。

出于便于维修的目的，远程维护通道通常是长期可用的，且为了能够在发生故障时快速反应，安全措施常常被忽略，因此这些通道经常成为被攻击的目标。

在这方面采取措施是绝对必要，以防止可能破坏系统运行的攻击。

另请参见：

- VPN [▶ 51]
- RDP [▶ 51]

6.2 □□□

防火墙设置是保护系统免受网络攻击的一种手段。应阻止不需要的传入端口。然而，比这更好的办法是不要启动任何打开这些端口的服务。要进行必要的设置，就必须对所使用的端口进行概述，并与每个相关人员进行协调。

防火墙可以用来过滤传输的网络数据包。防火墙技术可以基于地址、端口、通信关系状态、数据包内容等制定过滤规则。因此，防火墙是减少攻击面的工具。

防火墙可以是额外安装的软件，也可以是操作系统的一部分或自带设备。每种形式各有利弊。例如，与外部防火墙不同，作为操作系统组成部分的防火墙对可配置的程序进行管理，但它也更容易被恶意软件修改、激活或停用。

带深度数据包检测的防火墙也可以评估数据包中的用户数据，但无法看到加密连接的内容。为了能够处理内容（例如网站应用），在防火墙中的加密通常会被终止，数据会在客户端重新进行加密。因此，防火墙可以看到内容，同时端到端加密被中断。

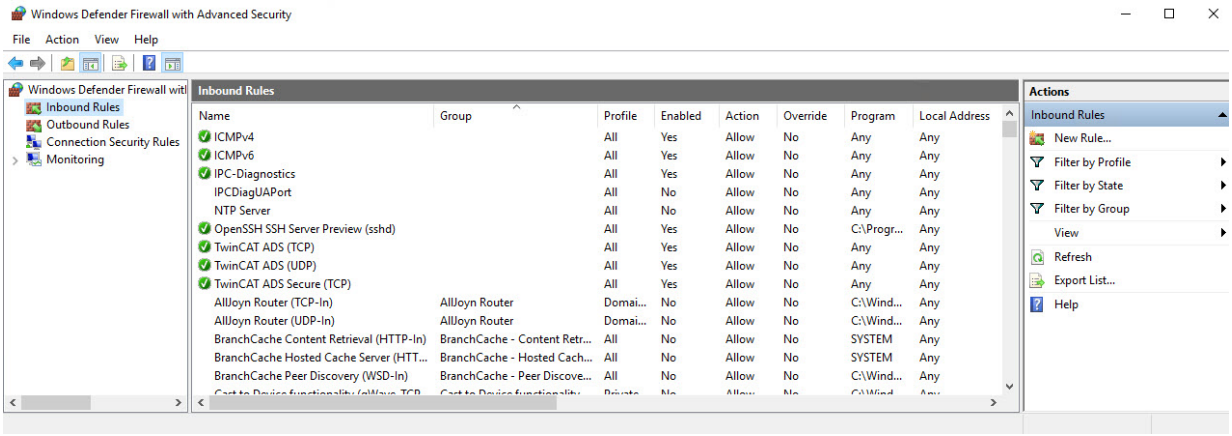
对防火墙通信采取明确的设置是一项重要的措施，从而只在必要范围内允许网络访问。

重要 TCP/UDP 端口 [▶ 51] 包含配置防火墙时通常需要考虑的 TCP/UDP 端口列表。

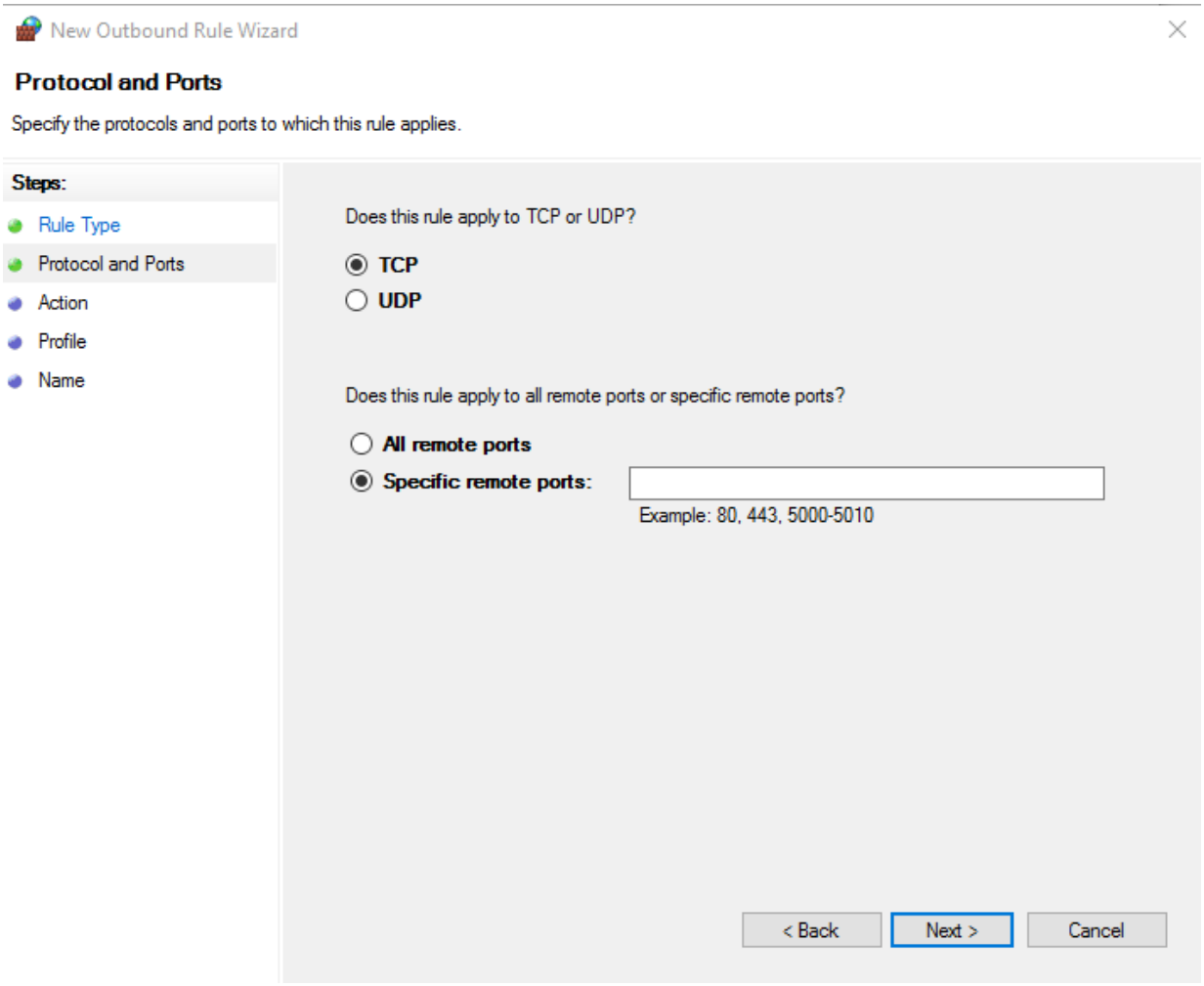
要配置防火墙，可以从命令行通过命令 **wf.msc** 打开 MMC 插件**具有高级安全性的 Windows 防火墙**。可使用**新规则**按钮添加规则。

选定的端口或服务开放规则也可以再次关闭。通过右键单击规则，可以用**禁用规则**或**删除**规则来禁用该规则。

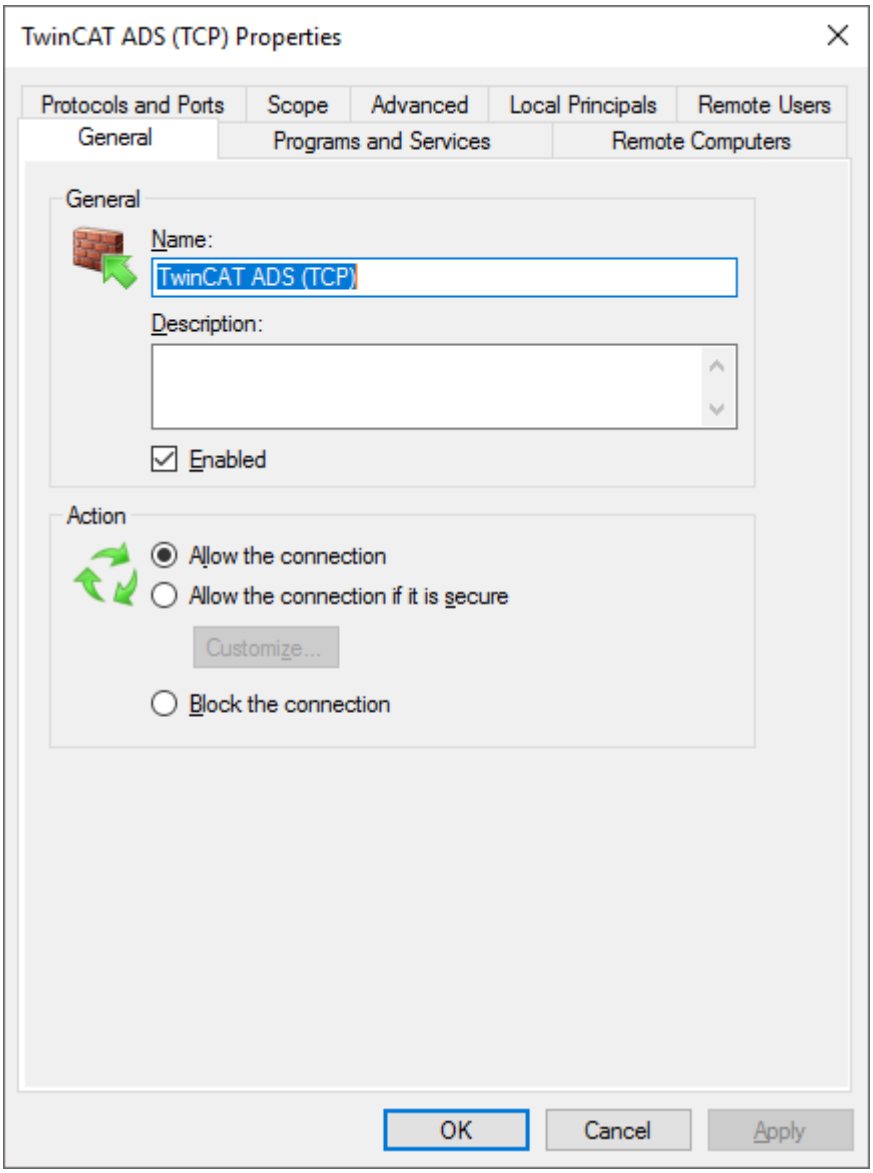
1. 打开防火墙设置



2. 双击现有规则，即可更改该规则，即允许或阻断连接。使用**新建规则**创建新规则。
这将启动向导，引导您完成各种选项：



3. 这些规则的选项也可以事后更改：



⇨ 您已为防火墙创建一条新规则。

更多信息请参见 Microsoft 文档：

https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-integration-and-best-practices

6.3 □□□□

本节会描述一些协议的安全相关特性。

6.3.1 Modbus

Modbus 协议最初于 1970 年代后期作为串行通信协议被开发。其主要目标是为工业应用提供一种通信协议，这种通信协议易于建立和维护，并且可以在无需开发信息模型的情况下传输数据。由于这一简单性，它已经流行了 30 年。但是，这种简单性使得 Modbus 在现代工业工厂中难以使用，这些工厂对通信协议有更复杂的要求，比如安全性和信息模型。最初的 Modbus 协议不包括加密或身份验证等安全措施。

尽管倍福为 Modbus RTU 和 Modbus TCP 提供两种 TwinCAT 功能，我们仍然建议使用更先进的协议，如本身带有安全机制的 OPC UA。

6.3.2 ADS

自动化设备规范 (ADS) 是倍福开发的专有通信协议。其设计是为了满足不同传输协议下的高通信量和可移植性（如 TCP 或串行）。ADS 在设计时未考虑安全性，也不包括加密操作，因为它们对性能和通信量有负面影响。

建议仅在安全环境中使用 ADS 或使用适当的安全传输通道。

ADS 目前有两个 TCP 传输通道支持加密：

- ADS-over-MQTT
- 安全 ADS

6.3.3 OPC UA

OPC 统一架构 (IEC 62541) 是 OPC 基金会的新一代技术，其目的是安全、可靠并与制造商无关的方式传输原始数据和预处理信息，使其从制造阶段进入生产规划或 ERP 系统。通过 OPC UA，所有授权的应用和授权人员可在任何时间、任何地点获得所有所需信息。

有关更多信息，请参见 TF6100 TC3 OPC UA 文档

6.3.4 VPN

虚拟专用网络 (VPN) 可以通过公共网络在不同设备之间建立虚拟局域网。在大多数情况下，通过公共网络传输的通信数据是加密的。例如，可以使用 VPN 解决方案来临时开通不安全协议，直到安全的替代方案开始运作。

6.3.5 RDP

远程桌面协议 (RDP) 是一种专用于图形远程访问的 Microsoft 专有协议。

6.3.6 CerHost

CerHost 是 Microsoft 专有的非加密协议，用于图形远程访问基于 Windows CE 的操作系统。

建议仅在安全环境中使用 CerHost（例如通过安全传输通道）。

6.4 □□□□

保护系统不受网络影响的另一种方案是使用安全网关。该硬件解决方案可安装在 IPC 前方的网络中。这样，某些网络段或每一台 PC 都能得到保护。

除了网络保护功能外，设备还会提供运行杀毒软件等选项，从而监控通过本地剪贴板实现的文件传输，而不会限制实际控制电脑的实时能力。

6.5 □□ TCP/UDP □□

根据不同的应用情况，必须禁用不安全的协议，或通过较低层次的协议（如物理安全网络或 VPN）来确保安全。

在使用安全协议的情况下，必须根据产品文档进行安全调试。

□□□□

下表概述了在交付镜像中，正常情况下开放的传入端口

服务	端口（传入）
IPC 诊断	https: 443 / tcp
远程桌面 – RDP（仅限 Windows 7/10）	3389 / tcp
TwinCAT ADS	发现：48899 / udp（也可传出） 不安全：48898 / tcp（也可传出）。 TwinCAT/BSD® 下端口是关闭的 安全 ADS：8016 / tcp（也可传出）

□□□□

下表概述了可额外打开的常用服务

服务	端口（传入）
SMB	137-139 / tcp 445 / tcp OPC-UA: 4852 / tcp
Cerhost (Windows CE)	987 / tcp
FTP	21 / tcp

TwinCAT □□

下表概述了 TwinCAT 产品通常使用的端口：

服务	端口（默认设置）
TF1810 TwinCAT PLC HMI Web	80 / tcp（传入） 另请参见：TF1810 上的文档
TF2000 TwinCAT HMI	1010（版本 ≤ 1.12）、2010（版本 ≥ 1.14） / tcp（本地） 1020（版本 ≤ 1.12）、2020（版本 ≥ 1.14） / tcp（传入） 另请参见：TF2000 上的文档
TF6100 OPC UA	4840 / tcp（UA 服务器，传入），可更改 48050 / tcp（UA 网关，传入），可更改 另请参见：TF6100 上的文档
TF6100 OPC DA	1024 与 65535 之间的动态端口（取决于 DCOM）（传入） 另请参见：TF6120 上的文档
TF6250 Modbus TCP	502 / tcp（传入），可更改 另请参见：TF6250 上的文档
TF6310 TCP-IP	可更改 / tcp（传入、传出） 另请参见：TF6310 上的文档
TF6311 TCP/UDP Realtime	可更改 / tcp（传入、传出） 通信不会受到操作系统防火墙的影响。 另请参见：TF6311 上的文档
TF6300 FTP	20 / tcp（传出） 21 / tcp（传出） 另请参见：TF6300 上的文档
TF6420 数据库服务器	可根据数据库 / tcp（传出）进行更改 另请参见：TF6420 上的文档

服务	端口（默认设置）
TF67xx IoT TF35xx 分析	可根据代理 / tcp（传出）进行更改 另请参见：TF670x 和 TF35xx 上的文档
TwinCAT EAP	34980 / udp（传入），前提是通过 UDP 使用 EAP。 通信不会受到操作系统防火墙的影响。 另请参见：EAP 的文档
TwinCAT ADS-over-MQTT	可根据代理 / tcp（传出）进行更改 另请参见：ADS-over-MQTT 上的文档

6.6 IIS

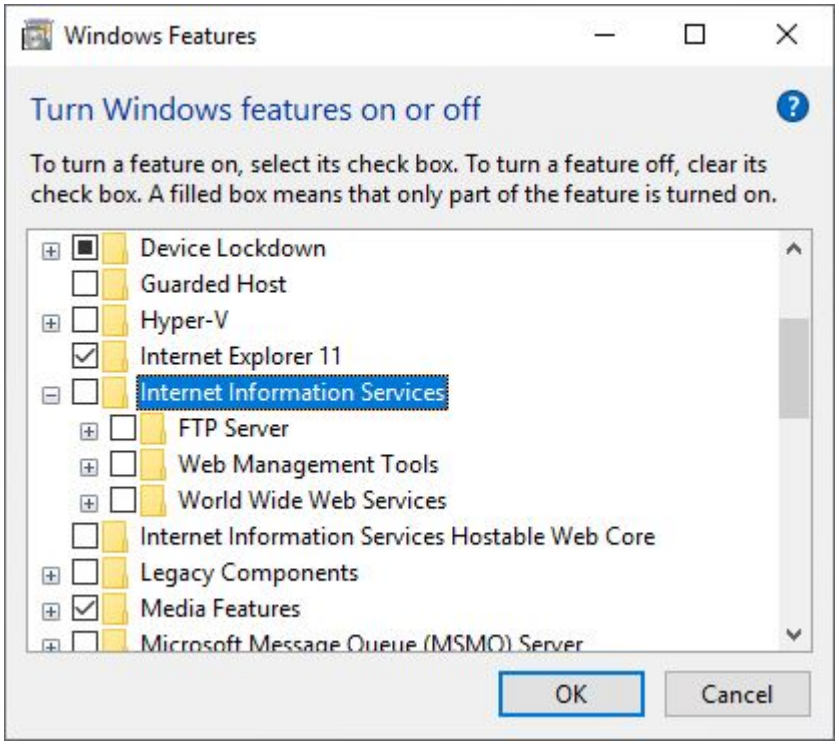
默认情况下，IIS 网络服务器会在 Windows 下处于活动状态，例如用于倍福设备管理器和 PLC HMI。为了进一步确保系统安全并限制通过网络服务器进行访问，您可以：

- 禁用 IIS 网络服务器
- 或限制从外部访问。

至于这两种方案中哪一种适合您，取决于您的使用条件。请注意，在完全禁用的情况下，所有访问 IIS 网络服务器的应用程序都会受到影响，无法继续运行。限制性的访问时，只有倍福设备管理器不能再可访问。倍福设备管理器的本地访问仍可使用，所有其他应用程序也不受禁用的影响。

禁用 IIS 网络服务器：

1. 使用快捷键 **[Windows 键] + [R]** 调用执行对话框，然后输入 **optionalfeatures**。
   打开Windows 功能窗口。
2. 禁用 **Internet 信息服务**下的选项。

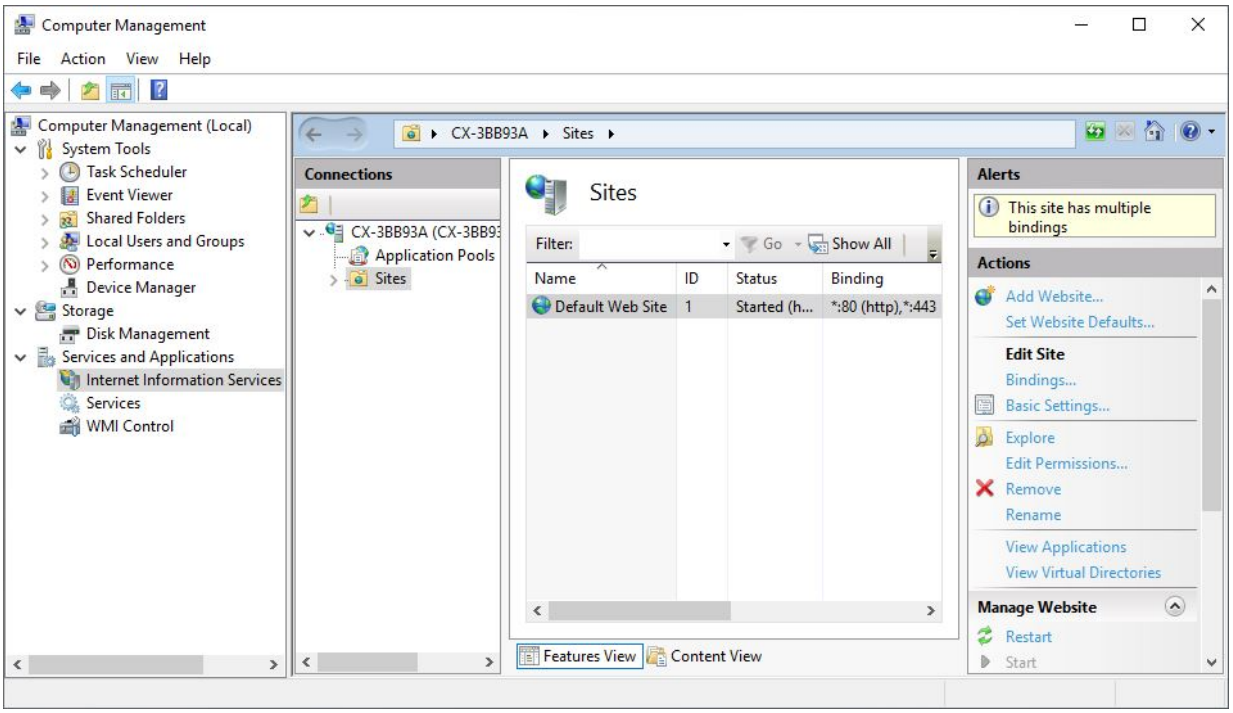


3. 从而禁用 IIS 网络服务器。访问 IIS 网络服务器的所有应用程序都会受到这一变更的影响。

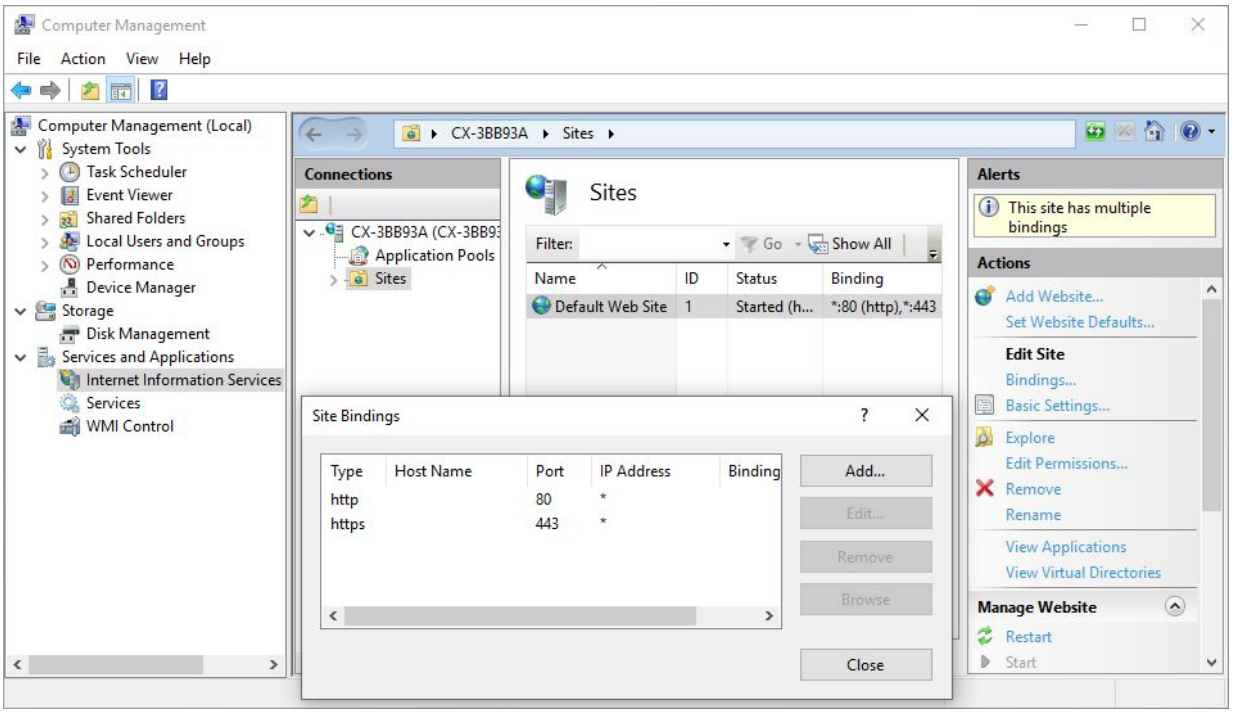
限制从外部访问：

1. 要禁止从外部访问，请使用快捷键 **[Windows 键] + [R]** 调用执行对话框，然后输入 **compmgmt.msc**。

2. 在左侧结构树中选择**互联网信息服务**条目，并在**连接**项下选择**站点**文件夹。

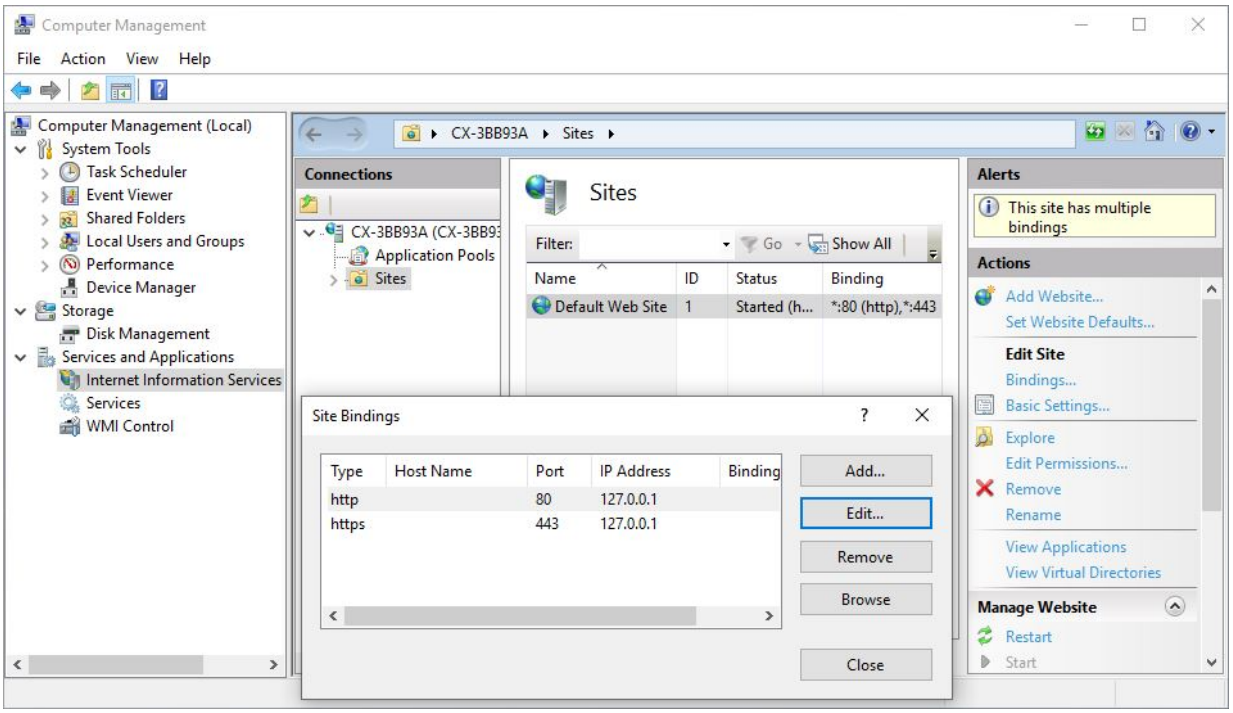


3. 在右侧“操作”项下点击**绑定**。在**站点绑定**窗口中，http 和 https 的**IP 地址**栏中会显示星号 (*)。



从而允许所有来自外部的访问。

4. 编辑 http 或 https 条目，并使用 **127.0.0.1** 条目只允许本地访问。



⇨ 从此，外部访问倍福设备管理器受限制。仍可通过 **127.0.0.1/config** 进行本地访问，并且所有其他应用程序不受完全禁用的影响。

6.7 HTTPS □□

如果倍福为网络界面（设备管理器）默认提供的证书不适合您的应用程序，那么本章会介绍如何创建和导入您自己的 HTTPS 证书。

证书在信息技术中用于安全身份证明。这样便可以对消息或文件进行加密，只有目标接收者才能再次解密内容。此外，每个网络浏览器在通过 HTTPS 协议检索页面时都会使用这项技术。

网络订阅者会在建立通信连接时请求获取其他订阅者的证书。检查证书以及另一方是否使用相关密钥进行身份验证。身份得到证明后，通过连接进行的消息交换便可以得到保护，既可以防止未经授权的操纵，还可以防止未经授权的查看。

要使用专门生成的 HTTPS 证书：

- 必须禁用为工业 PC 自动生成证书的功能，
- 必须向证书颁发机构 (CA) 申请证书
- 然后必须导入 HTTPS 证书。

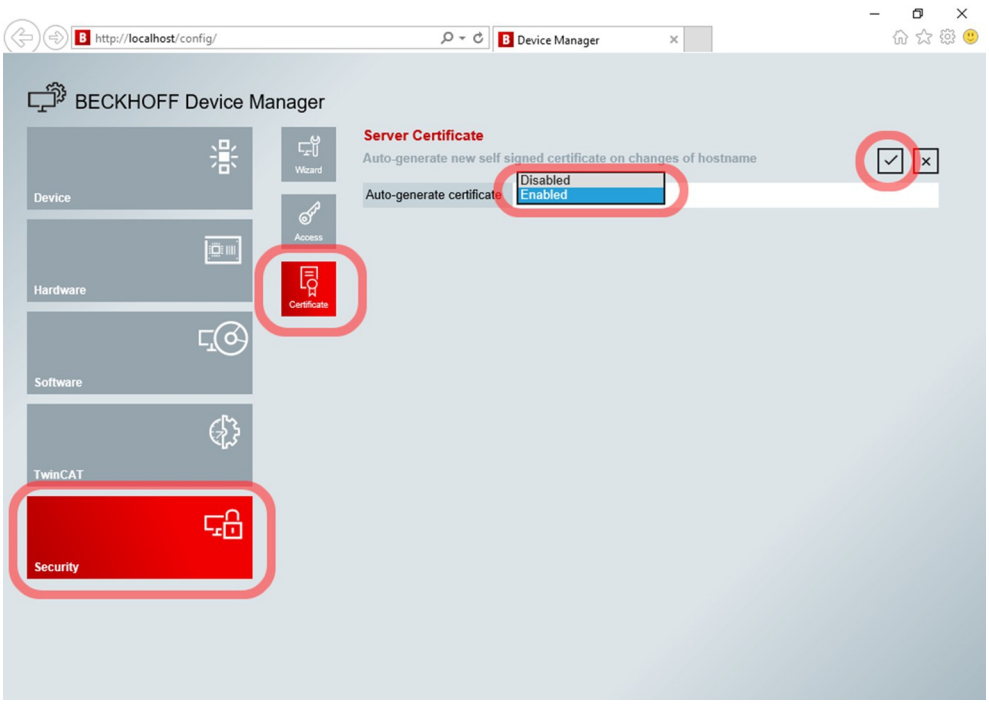
本章将介绍具体程序和必要步骤。

6.7.1 □□□□□□□□

首先必须禁用自动创建证书功能，以便安装自有证书。可借助倍福设备管理器进行设置，该管理器可在工业 PC 本地或远程调用。

操作步骤如下：

1. 如果在工业 PC 上进行本地运行，可在浏览器的搜索框中输入 URL `http://localhost/config`，启动倍福设备管理器。如果希望使用远程连接，请输入 `https://<IP-Adresse>/config`。
2. 点击左侧**安全**磁贴，然后点击**证书**。



3. 在**自动生成证书**处，选择**禁用**。
4. 点击右上角的复选标记，应用更改。

⇨ 自动生成证书功能禁用完成。下一步，可向证书颁发机构 (CA) 申请证书（见：申请 HTTPS 证书 [▶ 57]）。

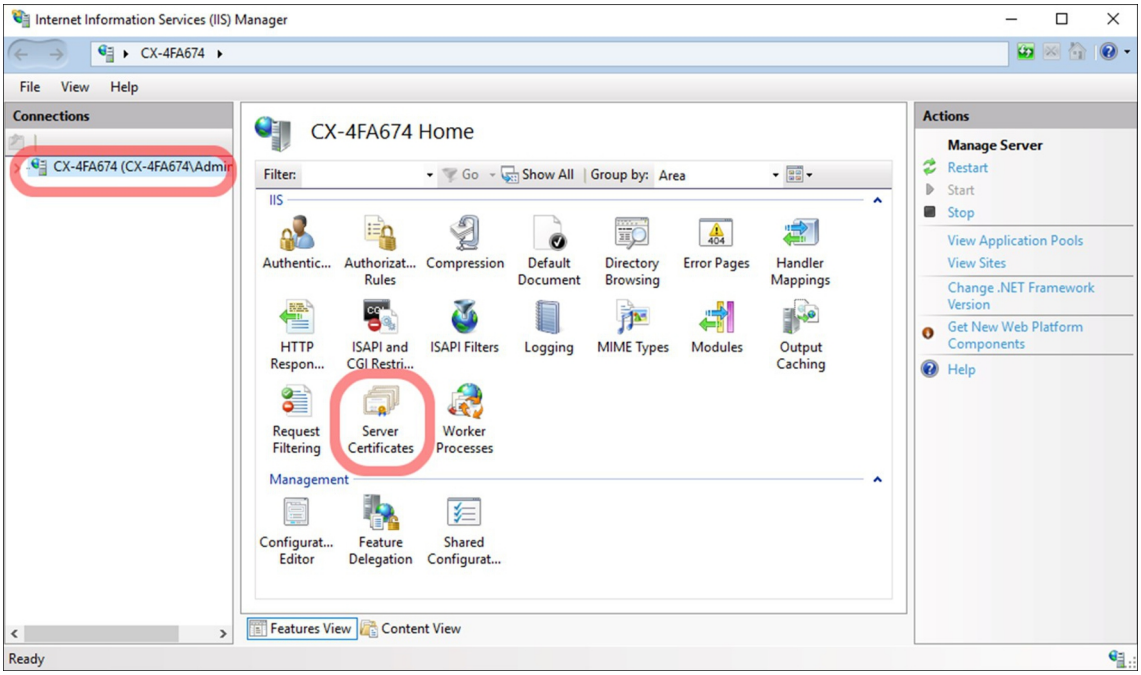
6.7.2 □□ HTTPS □□

倍福工业 PC 所使用的 HTTPS 服务器是 Windows 提供的互联网信息服务 (IIS) 服务器。通常情况下，对于 IIS 服务器，证书颁发机构 (CA) 会提供有关如何安装其颁发的证书的安装说明。证书颁发机构甚至会提供有关如何申请证书的说明。请主要遵循证书颁发机构的说明。如果您在自己的 Windows 域内使用软件实例进行认证，尤其如此。另外，后面会有分步说明。

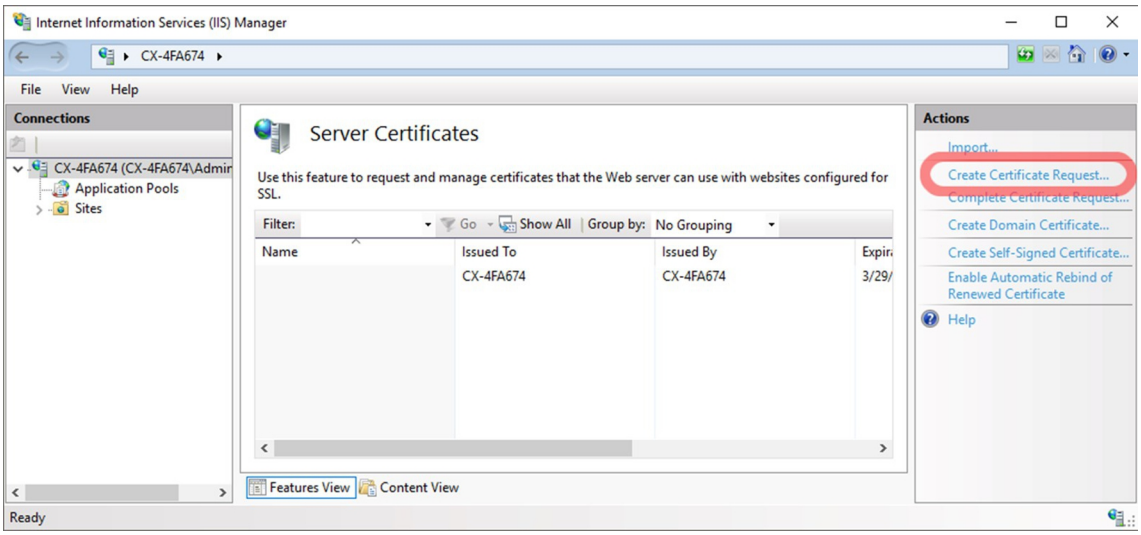
首先，您必须使用工业 PC 上的 IIS 管理器创建证书签名请求 (CSR)，并按照证书颁发机构的说明将证书请求转发给证书颁发机构。然后，证书颁发机构将向您提供服务器证书和中间证书，以创建证书签名请求

操作步骤如下：

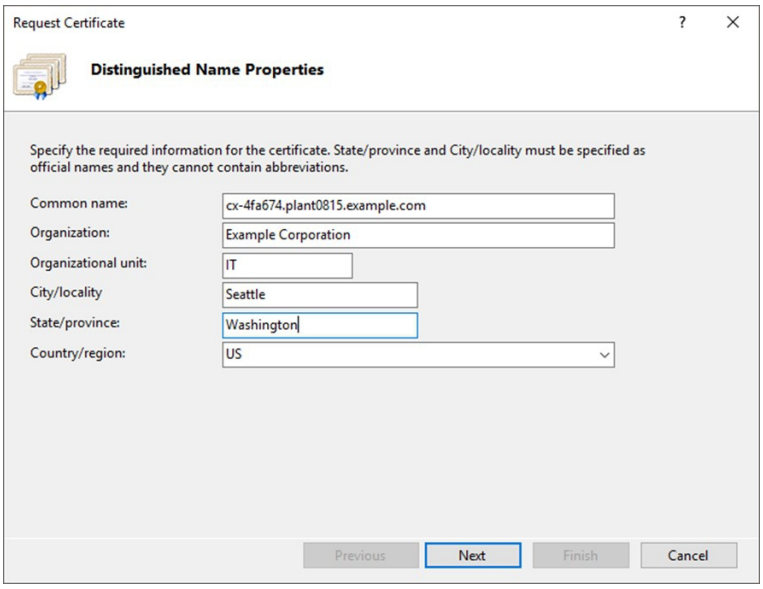
1. 以管理员身份打开工业 PC 上的互联网信息服务 (IIS) 管理器。
2. 从左侧**连接**菜单中选择网络服务器，然后双击**服务器证书**。



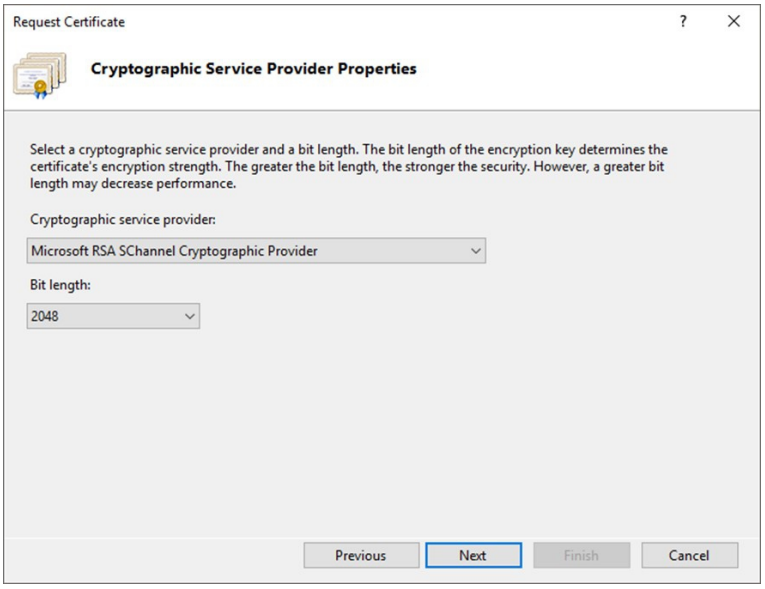
3. 在**操作**部分，选择**创建证书请求**，然后根据要求填写表格。



4. 出于兼容性考虑，必须在**通用名称**字段中输入客户端可以访问工业 PC 的完全合格 DNS 名称。如果没有 DNS 名称，也可以使用 IP 地址。一般来说，它必须是客户在 URL 中提出请求时在其应用程序中使用的名称或 IP 地址。如果需要指定备用 IP 地址或 DNS 名称，请要求证书颁发机构将其作为颁发证书的扩展名（主题备用名称）输入。在这种情况下，此类扩展请求的提出方式与 CSR 不同。



5. 您应该考虑根据自己的需求创建一个强密钥。1024 位的 RSA 不再被认为是强的。



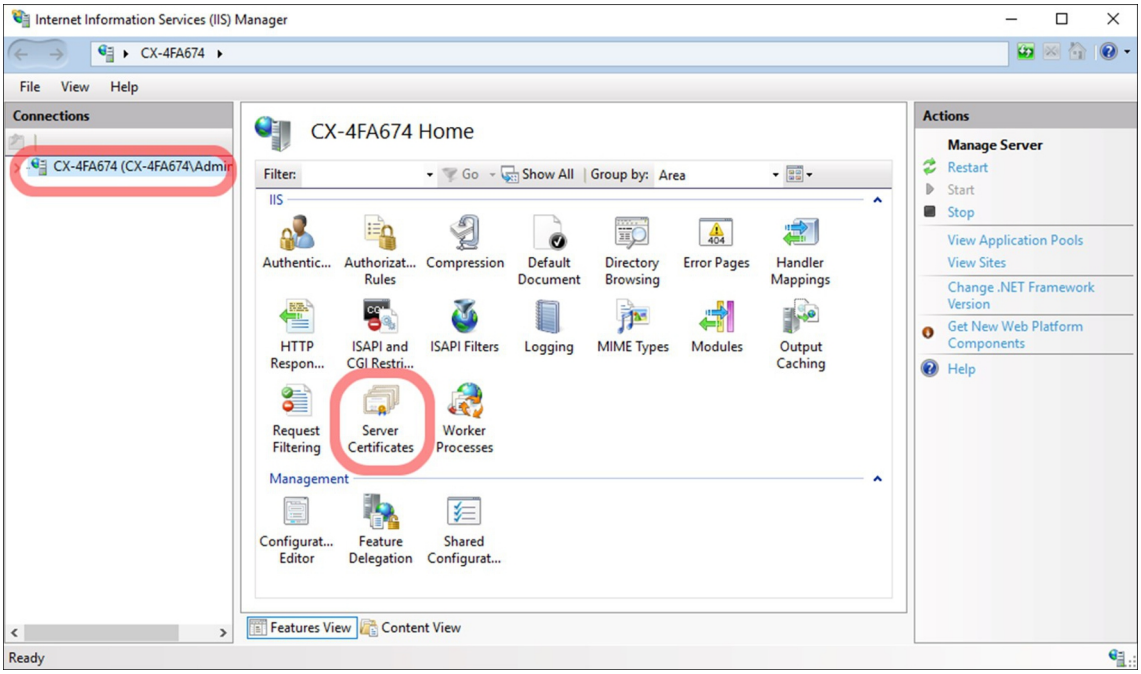
⇨ 保存 CSR 文件并将其发送给证书颁发机构。收到证书颁发机构的回复后，下一步就是导入证书（见：导入证书 [▶ 59]）。

6.7.3 □□□□

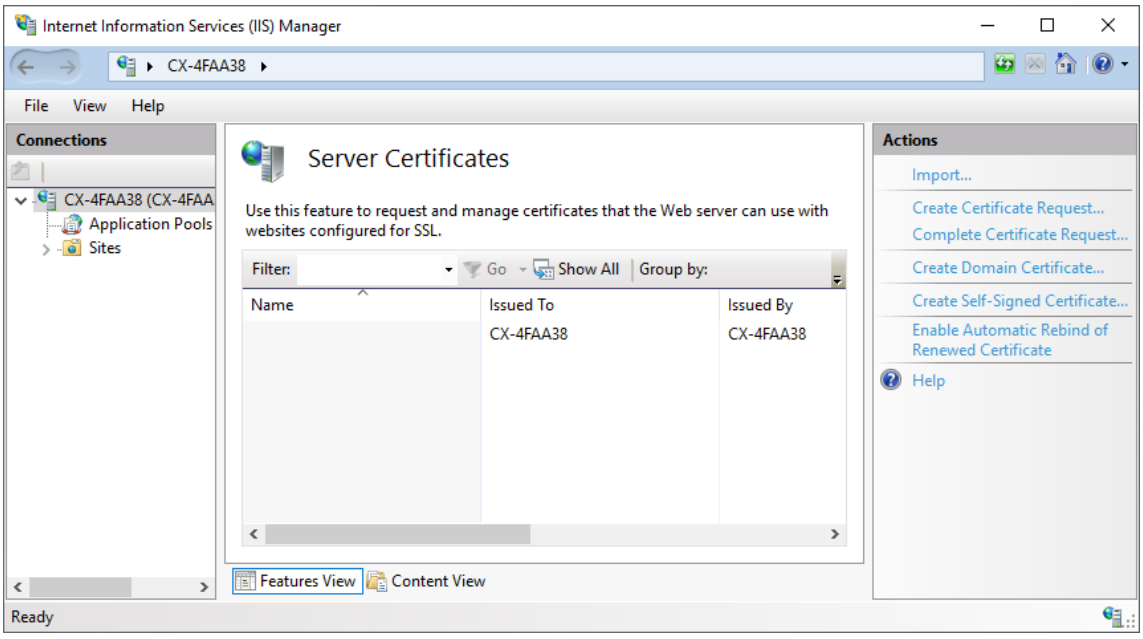
向证书颁发机构 (CA) 发送证书签名请求 (CSR) 后，您应该会收到一个回复文件。将应答文件复制到工业 PC，然后按以下步骤操作。如果您收到了多个文件，理想情况下，您需要一个扩展名为 *.p7b 的文件，该文件包含完整的证书链。

操作步骤如下：

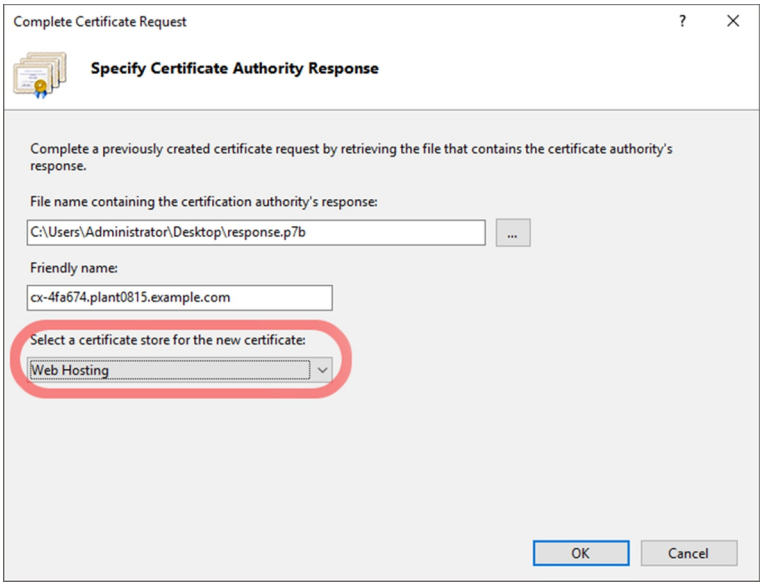
1. 以管理员身份打开工业 PC 上的互联网信息服务 (IIS) 管理器。
2. 从左侧**连接**菜单中选择网络服务器，然后双击**服务器证书**。



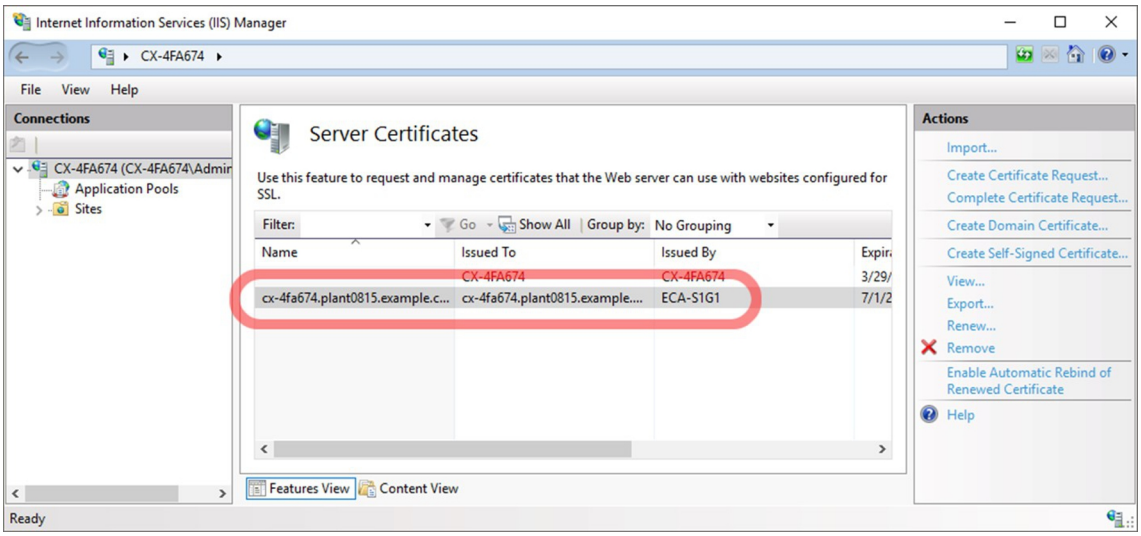
3. 在**操作**部分，点击**完成证书申请**选项并加载要导入的证书，其扩展名为 *.p7b。



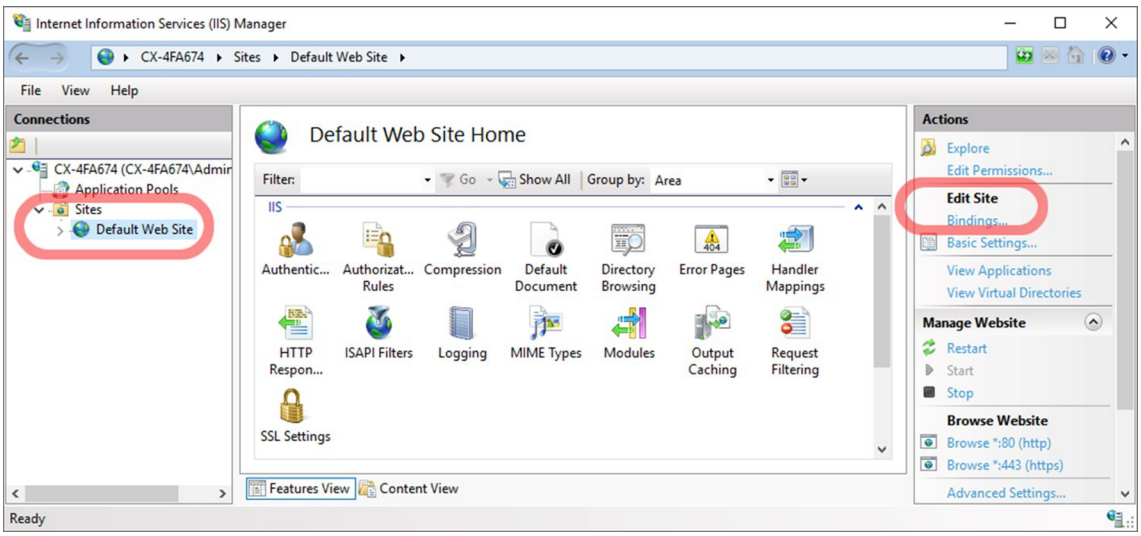
4. 出现**指定证书颁发机构回复**窗口。为证书命名，以便将其存储到证书存储区。最好选择与您在证书签名请求 (CSR) 过程中在**通用名称**字段中选择的相同值。不要忘记为证书存储选择**网络托管**选项。



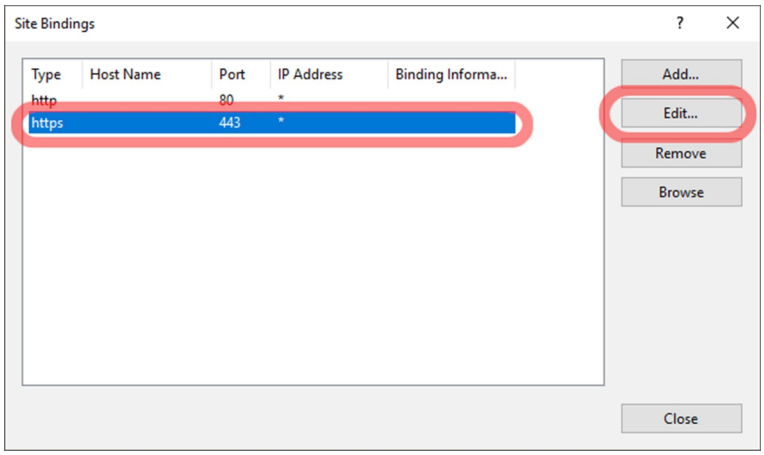
5. 导入后，证书将出现在可用服务器证书列表中。



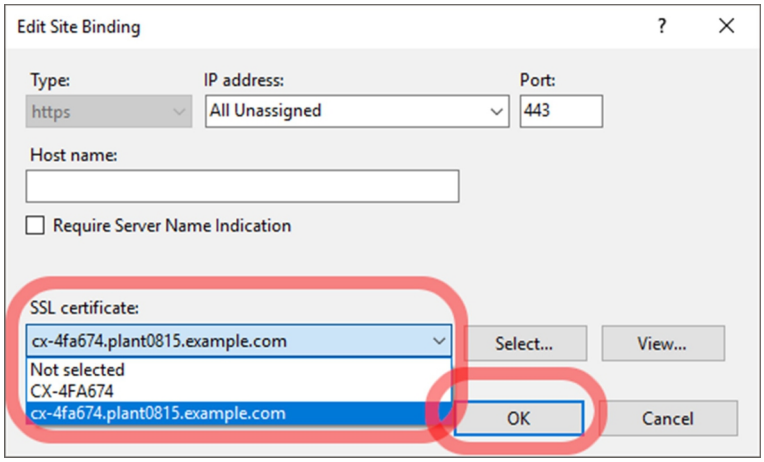
6. 点击左侧的**默认网站**，然后点击**编辑站点**菜单中的**绑定**。



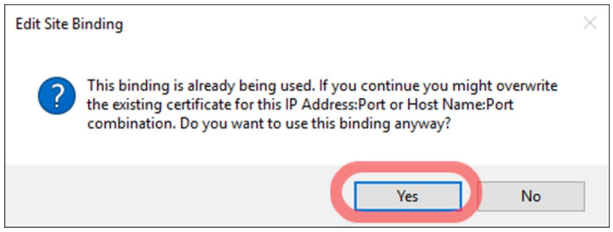
7. 点击 **https**，然后点击**编辑**。



8. 在 **SSL 证书**中选择导入的证书，并点击**确定**接受选择。



9. 确认设置以替换先前的证书并使用新创建的证书。



⇨ 设置完成后，工业 PC 会立即使用新证书。您可以使用客户端（如网络浏览器）进行检查。请注意，您可能需要重启网络浏览器或清除缓存才能连接。

7 TwinCAT

对于 eXtended Automation Engineering (XAE) 和 eXtended Automation Runtime (XAR) 来说，什么才是威胁，必须从工厂的安全理念出发。IEC 62433 标准对必要的威胁分析等进行了解释，为创建安全理念提供了帮助。此外，还可参考 VDMA 指南，以帮助提高操作流程的安全性和产品抵御网络攻击的能力：https://www.vdma.org/viewer/-/v2article/render/16110956

本章列举了一些与 XAE 和 XAR 相关的威胁示例，但并不完整。

7.1 eXtended Automation Engineering (XAE)

表 5: 未经授权篡改源代码。

对策	描述
技术性	• 定义授权并通过软件保护加以实施 • 使用版本控制系统，使更改具有可追溯性 • 对版本控制系统使用单独的访问控制
组织性	• 使用 IT 安全管理系统（如符合 ISO 27001 标准） • 使用版本控制系统（见：源代码控制）： • 使用“分级”： ◦ 首先在开发源代码控制库中签入 ◦ 使用单独的（预）发布构建仓库，从那里构建 alpha、beta、RC 和发布版本 ◦ 仅在审查后，例如通过项目比较工具，才会将开发库转移至发布（预）构建仓库（见：项目比较工具）

表 6: 未经授权访问源代码。

对策	描述
技术性	• 使用软件保护存储加密源代码（见：软件保护）
组织性	• 使用 IT 安全管理系统（如符合 ISO 27001 标准）。 • 安全访问存储位置。 • 使用加密存储。

7.2 eXtended Automation Runtime (XAR)

表 7: 通过 *ADS* 或安全 *ADS* 进行未经授权的访问。

对策	描述
技术性	使用安全 ADS（见：安全 ADS）： • 仅对已定义的远程站开放 • 防火墙限制 • 静态路径 • 保护远程站免受操纵
组织性	• 将通过安全 ADS 的访问替换为通过 OPC UA 的访问。

表 8: 通过 *ADS* / 安全 *ADS* 影响实时的情况。

对策	描述
技术性	使用安全 ADS（见：安全 ADS）：

对策	描述
	• 仅对已定义的远程站开放 • 防火墙限制 • 静态路径 • 保护远程站免受操纵
组织性	• 将通过安全 ADS 的访问替换为通过 OPC UA 的访问。

7.3 □□□□□□

本章以链接集的形式汇总了有关 TwinCAT 安全性的更多主题。提供了详细描述相关主题的倍福文档的链接。选择是一种引导。旨在作为查找资料的第一站，并不详尽。

TwinCAT 综述	更多信息
TwinCAT 3 软件保护	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_security_management/index.html&id=355557539833111233
ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_intro/index.html&id=7262890787652929099
禁用 ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/6917981195.html&id=5745105416081707706
安全 ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/index.html&id=2501949194726739202
ADS over MQTT	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_over_mqtt/index.html&id=120186874503837909

OPC UA	更多信息
服务器安全	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1448394251.html&id=2325029100913163478
IO 客户端安全	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=
PLCLib 客户端安全	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=7305736008379229744
网关安全	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=954414165455750259

8 □□

8.1 □□□□

IEC 62443 是关于自动化系统安全性的一系列国际标准。个别章节仍在制定中。已经发表的部分描述了系统和组件的组织和技术概念和措施。URL: https://webstore.iec.ch/publication/7029

NIST SP800-82《工业控制系统安全指南》具体描述了对工业设施安全威胁的分析和措施。URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

BSI IT 基本保护纲要针对风险分析和措施应用提供了结构化的功能模块。纲要还包含与工业 IT 有关的功能块 URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

8.2 □□

我们的安全公告旨在帮助客户保护其倍福工业 PC 和嵌入式 PC 免受某些影响。下表概述了有关安全薄弱环节的现有公告，并提供了用于下载文件的链接。

这些安全公告还会以 RSS 源的形式提供。此外，作为 CERT@VDE 的一部分，倍福与其他制造商一起发布了这些公告：https://cert.vde.com/de/advisories/vendor/beckhoff/。

如果您怀疑我们的产品之一存在安全薄弱环节，请通过 中所述流程告知我们。

编号	标题	版本	语言	下载	外部 CNA
2024-005	通过 TwinCAT Package Manager 注入本地命令	1.0	ZH	PDF	HTML,CSAF
2024-004	TwinCAT/BSD 软件包“MDP”中的本地拒绝服务问题	1.0	ZH	PDF	HTML,CSAF
2024-003	TwinCAT/BSD 软件包“IPC-Diagnostics”中的本地拒绝服务问题	1.0	ZH	PDF	HTML,CSAF
2024-002	TwinCAT/BSD 软件包“IPC-Diagnostics-www”中输入的中和不当	1.0	ZH	PDF	HTML,CSAF
2024-001	TwinCAT/BSD 软件包“IPC-Diagnostics”中的本地验证绕过漏洞	1.0	ZH	PDF	HTML,CSAF
2023-001	在 TwinCAT/BSD 软件包“authelia-bhf”中打开重定向	1.0	ZH	PDF	HTML
2022-001	采用 OPC UA 技术的产品中的空指针取消引用漏洞	1.0	ZH	PDF	HTML
2021-003	通过 TwinCAT OPC UA 服务器的相对路径遍历漏洞	1.0	ZH	PDF	HTML
2021-002	各种 OPC UA 产品中的堆栈溢出和 XXE 漏洞	1.0	ZH	PDF	HTML
2021-001	TwinCAT OPC UA 服务器和 IPC 诊断 UA 服务器的 DoS 漏洞	1.2	ZH	PDF	HTML
2020-003	通过 TwinCAT 系统托盘 (TcSysUI.exe) 进行权限升级	1.1	ZH	PDF	HTML
2020-002	TwinCAT RT 网络驱动程序中的以太网数据泄漏问题	1.1	ZH	PDF	HTML
2020-01	BK9000 耦合器 – 拒绝服务抑制功能	1.0	ZH	PDF	HTML
2019-07	使用 Profinet 协议的 TwinCAT 上的拒绝服务问题	1.1	ZH	PDF	HTML

编号	标题	版本	语言	下载	外部 CNA
2019-06	CE 远程显示屏在使用错误凭证时行为不正确	1.2	ZH	PDF	
2019-05	远程桌面服务中的远程代码执行（“Dejablue”）	1.0	ZH	PDF	
2019-04	ADS 发现	1.1	ZH	PDF	
2019-03	远程桌面服务中的远程代码执行	1.4	ZH	PDF	
2019-02	微架构数据取样 (MDS) 漏洞	1.2	ZH	PDF	
2019-01	Spectre-V2 及其对应用程序性能和 TwinCAT 兼容性的影响	1.4	ZH	PDF	
2018-02	OPC-UA 组件更新（若干漏洞）	1.0	ZH	PDF	
2018-01	TwinCAT 2 和 3.1 内核驱动程序权限升级	1.1	ZH	PDF	
2017-02	使用基于固定密钥的“加密密码”添加路由	1.3	ZH	PDF	
2017-01	ADS 仅基于于保护环境的设计	1.4	ZH	PDF	
2015-001	可能误用 IPC 诊断程序版本 < 1.8 的后端程序	1.1	ZH	PDF	
2014-003	更改默认密码的建议	1.1	ZH	PDF	
2014-002	ADS 通信端口允许暴力破解密码	1.1	ZH	PDF	
2014-001	若干管理服务可能被滥用	1.1	ZH	PDF	

8.3 □□□□□□□

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。

□□□□□

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。

□□□□□□□□□

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。

□□□□□□

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

□□□□□□

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

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

Modbus is a registered trademark of Schneider Electric USA, Inc.

更多信息:
www.beckhoff.com

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