指南

安全的 KEPServerEX® 部署

2018 年 6
月参考号 1.000

目录

1. 序言

KEPServerEX 为工业自动化和工业物联网提供通信支持。它常用于以下行业的生产系统：离散、工艺和批量制造；石油和天然气生产与分销；楼宇自动化：能源生产和分销；等等。安全和正常运行时间是这些系统的关键组成部分，但网络安全威胁的频率和复杂性都在增加。因此，在生产环境中使用软件时，KEPServerEX 用户必须尽可能安全地部署应用程序。本文档全程指引用户以最大的安全性部署 KEPServerEX。建议管理员在生产环境中部署 KEPServerEX 时尽可能紧密遵循本指南。

Kepware/PTC 建议新用户尽可能使用本指南来指引新的 KEPServerEX 生产安装。Kepware/PTC 还建议现有软件用户将现有配置与本指南中的推荐配置进行比较，并按照最佳做法进行调整。

2. 网络环境和系统配置

网络安全与工业控制系统 (ICS) 网络安全是一个非常复杂的议题。最佳做法层出不穷，包括：网络划分、使用 DMZ、流量评估、维护最新的物理和逻辑库存、反常和入侵检测的高级算法，以及从安全性角度不间断重新审视网络安全。但是，最佳做法并非一成不变，而具体实施则取决于特定的用例 (例如：运营网络、卫星或移动网络、计算机上的本地网络)。这些最佳做法的确定和实施不在本文讨论之列。用户可以培养和维持内部专业人员以确保 ICS 网络的安全，或者与具有相应专业人士的系统集成商进行合作。在为 ICS 网络制定安全策略时，咨询或参考下列组织和资源对于用户可能有所帮助。

KEPServerEX 可用于连接成千上万个不同的工业自动化设备和系统。因此，安全的设备和系统配置不在本文讨论之列。在部署和连接任何设备时，请遵循最佳做法。这包括但不限于在需要时对连接进行适当的身份验证。与 ICS 网络安全一样，我们建议用户在该领域培养内部专业人员，或者与熟悉环境中特定设备的合格系统集成商进行合作。

2.1 ICS 网络安全资源

- 美国国土安全局工业控制系统网络应急工作组 (ICS CERT) (https://ics-cert.us-cert.gov)
- 美国国家标准与技术协会 (https://www.nist.gov/)
  - 美国国家标准和技术协会工业控制系统安全指南 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf)
- North American Electric Reliability Corp.《关键基础设施保护标准》(https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx)

2.2 系统集成商

- Kepware® 系统集成商计划关联的系统集成商 (https://www.kepware.com/en-us/partners/system-integrators/)

3. 主机操作系统

KEPServerEX 应当始终部署在尽可能安全的环境中。确保主机操作系统 (OS) 从一开始就是安全的，并采取一切可行措施来保持 OS 在系统生命周期内的安全。KEPServerEX 应部署在采用“纵深防御”原则的环境中，而不是采用“面向外围”的安全理念。安全的操作系统涉及范围包括但不限于系统安全性、用户管理、防火墙设置和文件管理。

3.1 系统

- 落实适当的访问控制措施，使得只有适合用户才能实际接触目标硬件。
- 始终在主动支持的 Windows 版本上部署 KEPServerEX，并按照 ICS 安全最佳做法安装 Windows 安全修补程序。正如 ICS-CERT 概述：“各个组织应针对 ICS 制定系统化的补丁和漏洞管理方法，并确保在维护 ICS 正常运作的同时减少系统漏洞风险。”。

- 加密主机的硬盘驱动器，时刻保护所有数据。
- 使用具有最新签名文件的知名杀毒软件，定期扫描主机系统。
- 关闭主机上所有未使用的服务。
- 为了减少攻击面，避免使 KEPServerEX 和任何其他应用程序在同一台主机上运行。

3.2 用户管理

- 创建一个与管理员帐户分开的 Windows 用户，用于配置和管理 KEPServerEX。
- 根据 Windows 最佳做法管理管理员帐户。
- 用户密码必须遵循与特定域对应的正式密码策略。
- 不要在多个用户之间共享登录名或密码。
- 安全存储密码。.
- 定期检查访问控制模型，以确保按照“最低权限”原则设置访问权限 (即，仅对需要执行所需功能的用户授予权限，并且在不再需要时撤销权限)。

3.3 外围

- 利用防火墙来最小化外部访问，并定期检查防火墙设置。
- 利用入侵检测系统 (IDS)。
- 监视对主机操作系统的远程访问并记录活动。

3.4 非生产文件

- 定期从生产系统中删除备份文件。
- 定期从生产系统中删除示例、测试文件或脚本。

4. 安装

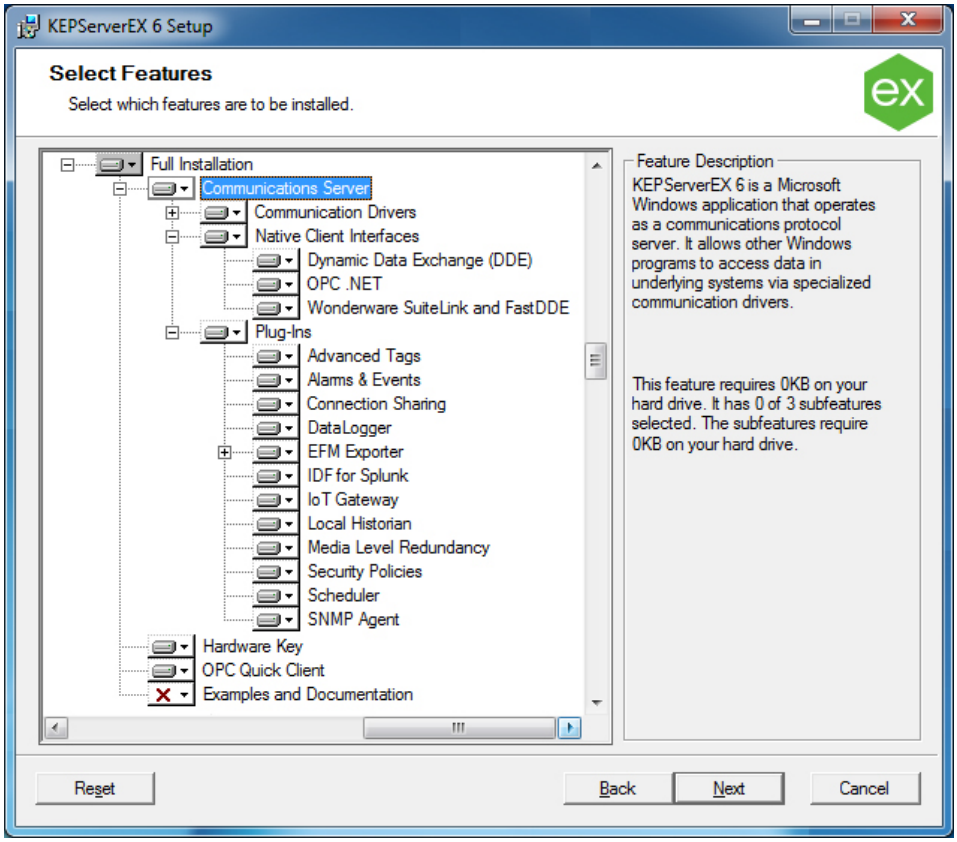
用户应当验证 KEPServerEX 安装，并且仅安装特定应用程序所需的功能。在安装过程中设置强管理员密码。

4.1 验证

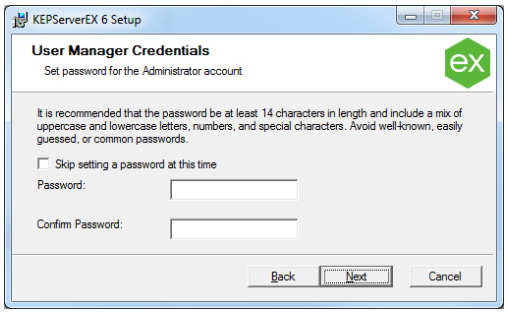
4.1.1 对于正式发布的软件，Kepware 为其保留唯一的识别码。客户应根据这些代码进行验证，以确保仅安装经过认证的可执行文件。
按照以下说明验证软件：https://www.kepware.com/digitalsignature.

4.2 安装

4.2.1 在安装过程中使用”选择功能“对话框时，仅安装生产环境所需的功能。



4.2.2 在安装过程中使用“用户管理器登录凭据”对话框时，设置强管理员密码。建议密码至少为 14 个字符，并包括大写和小写字母、数字和特殊字符的组合。避免众所周知、容易猜到的或常见的密码。安全存储密码。.



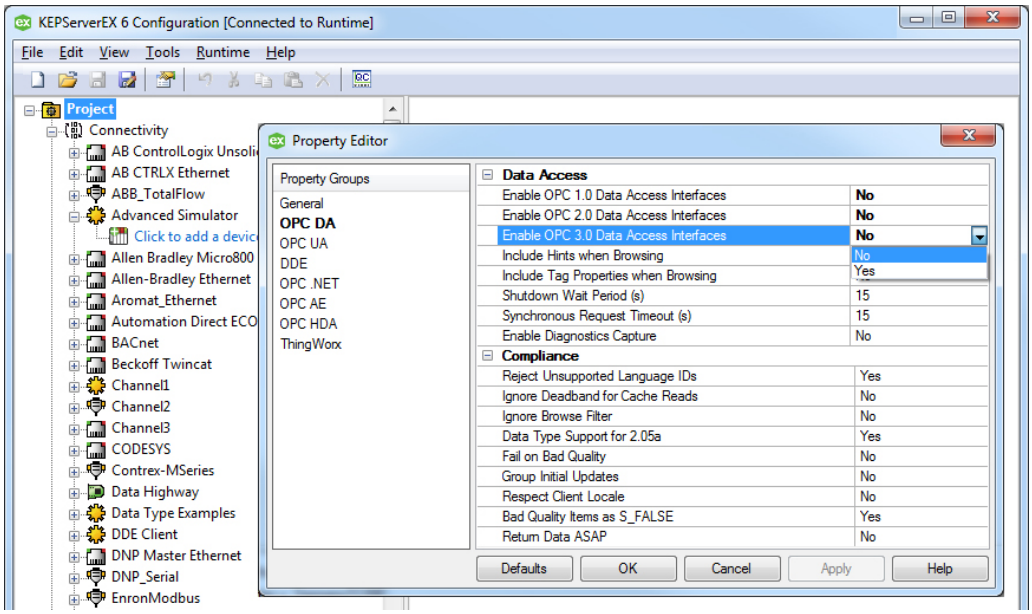
5. 安装后

安装产品后，KEPServerEX 管理员应执行多项操作以保持最高级别的安全性。这包括禁用应用程序中未被用户使用的任何不安全接口，以及以“最低权限”原则配置用户组和用户。

5.1 不安全的接口

5.1.1 如果应用程序不需要 OPC DA 接口，则禁用该接口。OPC DA 是旧式协议，难以部署为足够的安全级别。用户应尽量使用本文列举的安全协议之一。

1. 运行 KEPServerEX 配置。
2. 右键单击项目，并选择**项目属性**。



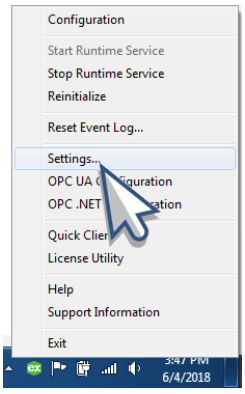
3. 选择 **OPC DA** 项目属性。
4. 通过禁用前三个属性，禁用 OPC 1.0、2.0 和 3.0 数据访问接口。

5.1.2 每次创建不需要 OPC DA 连接的新项目时，都要重复这些步骤。

- 禁用 OPC DA 接口将拒绝访问用于测试连接性的内置 Quick Client 工具。请利用第三方工具（例如 UA Expert）来测试连接性。

5.2 服务器用户

5.2.1 为 Server Users 用户组中的用户 Default User 创建强用户密码。



1. 右键单击系统托盘中的 KEPServerEX 图标并选择“设置”，以打开“管理设置”。
2. 选择**用户管理器**选项卡。

- 此实例中，访问**设置**菜单所需的具有适当权限级别的用户名和密码是管理员用户名和密码。

3. 双击 Server Users 组下的 **Default User**。

4. 设置强密码。建议密码至少为 14 个字符，并包括大写和小写字母、数字和特殊字符的组合。避免众所周知的、容易猜到的或

   常见的密码。安全存储密码。.

5.2.2 按照“最低权限”原则调整 Default User 的权限 (即，只对需要执行所需功能的用户授予权限，并且在不再需要时撤销权限)。

1. 打开 KEPServerEX“设置”中的**安全策略**选项卡。

2. 展开分配给 Server Users 的权限，按照“最低权限”原则调整权限。

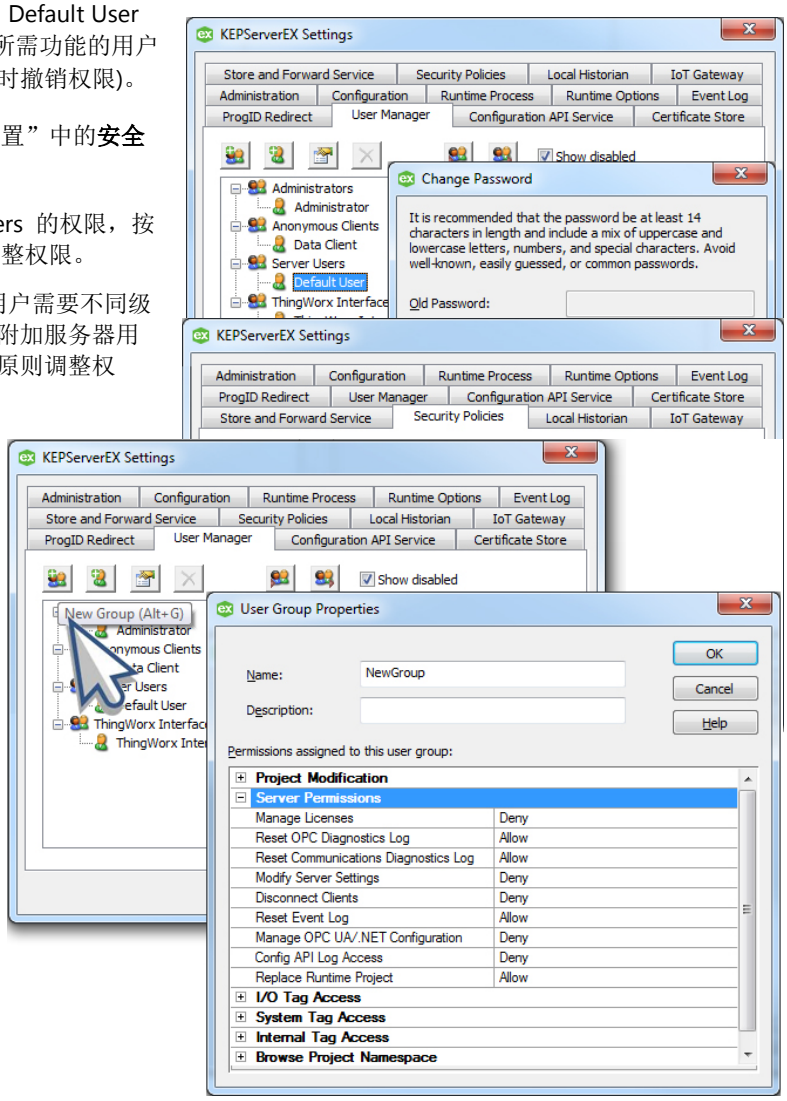
5.2.3 如果 KEPServerEX 的配置用户需要不同级别的权限，则根据需要创建附加服务器用户组，并按照“最低权限”原则调整权限。

1. 打开 KEPServerEX“设置”中的**用户管理器**选项卡。

2. 单击**新建组**。

3. 按照“最低权限”原则为新创建的组分配权限。

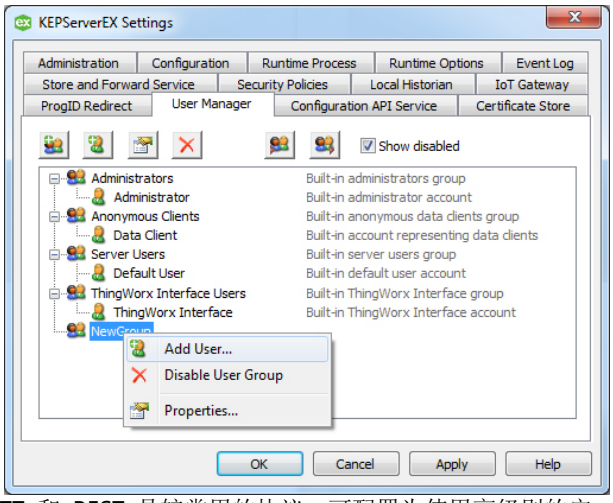
4. 右键单击新组。



5. 单击**添加用户**。

6. 设置强密码。建议密码至少为 14 个字符，并包括大写和小写字母、数字和特殊字符的组合。

- 避免众所周知、容易猜到的或常见的密码。安全存储密码。.
- 不要在多个用户之间共享用户名或密码！当用户需要不同级别的权限时，请创建新用户和/或新组。



6. 安全接口

KEPServerEX 基于工业自动化和工业物联网 (IIOT) 的常用协议进行通信。其中一些协议更安全，并且有更多安全选项。OPC UA、MQTT 和 REST 是较常用的协议，可配置为使用高级别的安全性。还有其他协议可以安全地配置 (SNMP、ThingWorx 本机接口以及其他)。

- *有关其他安全协议的详细信息，请参阅 KEPServerEX 手册。*

6.1 OPC UA

6.1.1 为使用 OPC UA 接口的特定用途创建服务器用户组，并按照“最低权限”原则调整该组的权限。

1. 打开 KEPServerEX“设置”中的“用户管理器”。

2. 单击**新建组**。

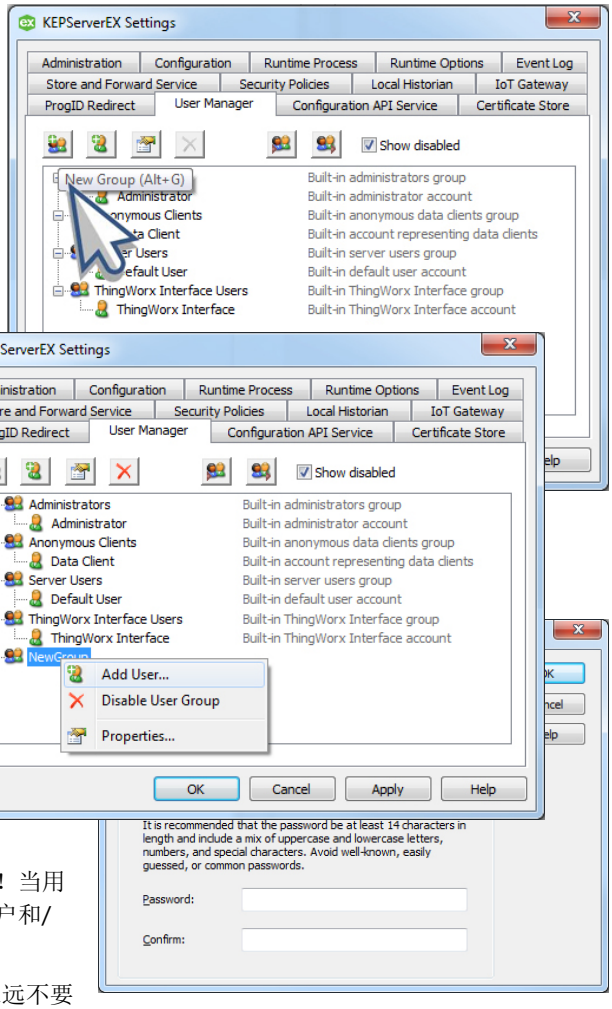
3. 按照“最低权限”原则为新组分配权限。

4. 右键单击新组。

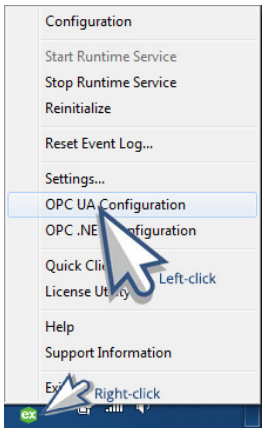
5. 单击**添加用户**。

6. 设置强密码。建议密码至少为 14 个字符，并包括大写和小写字母、数字和特殊字符的组合。

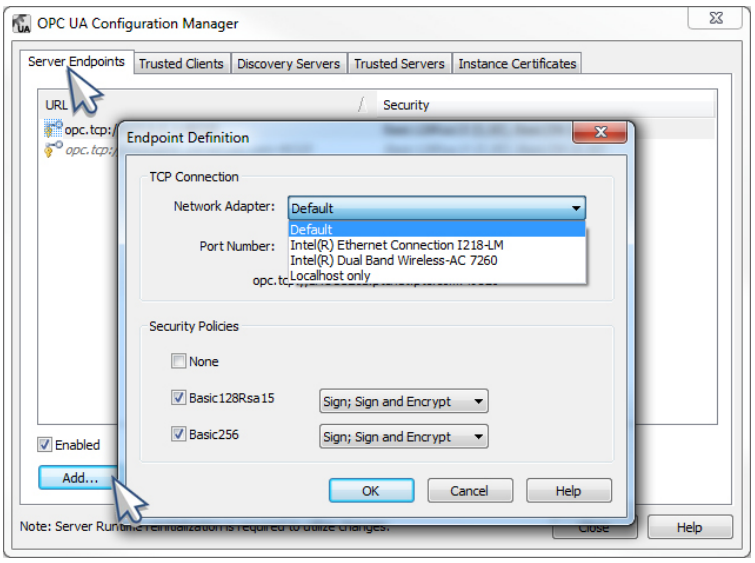
- 避免众所周知、容易猜到的或常见的密码。安全存储密码。.
- 不要在多个用户之间共享用户名或密码！当用户需要不同级别的权限时，请创建新用户和/或新组。
- 默认情况下禁用 UA 匿名登录。建议永远不要允许匿名 UA 客户端访问。



6.1.2 在构建 OPC UA 服务器端点时，利用当前可用的最强安全设置。

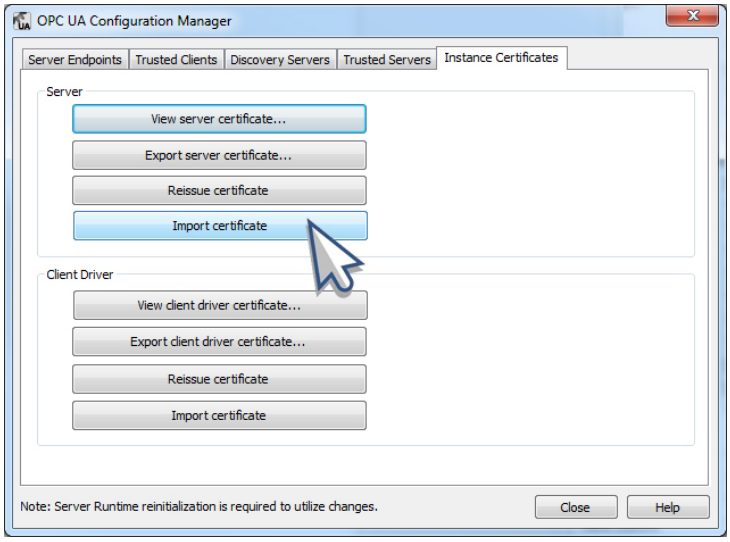


1. 通过右键单击系统托盘中的 KEPServerEX 图标并选择 **OPC UA 配置**，打开 OPC UA Configuration Manager。
2. 单击**服务器端点**选项卡。
3. 单击**添加...**按钮以定义新端点。
4. 确保选中最新的安全策略选项。
5. 单击**确定**。



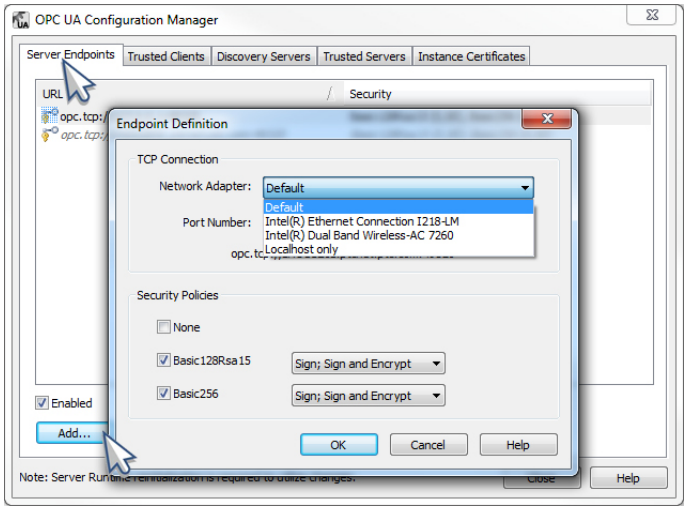
6.1.3 尽可能使用证书颁发机构 (CA) 签名的证书。

在 OPC UA Configuration Manager 的“实例证书”选项卡中，单击**导入证书**并导入由 CA 签名的证书。



- 在构建 OPC 服务器端点时，所用的网络适配器必须只能连接通过运行 OPC UA 客户端来访问 KEPServerEX 的网络 (即，如果网络适配器可访问互联网或其他不需要连接的网络，则不能使用该适配器)。

1. 打开 OPC UA Configuration Manager。
2. 添加新端点。



3. 确保所用的网络适配器只能连接运行 OPC UA 客户端的网络。

6.2 MQTT

6.2.1 当配置 KEPServerEX 将连接的 MQTT 代理时，尽可能设置强用户名和密码，使用强大且新型的加密方式，使用证书颁发机构 (CA) 签名的证书。

- 配置这些项目将取决于所使用的特定代理。

6.3 REST 客户端

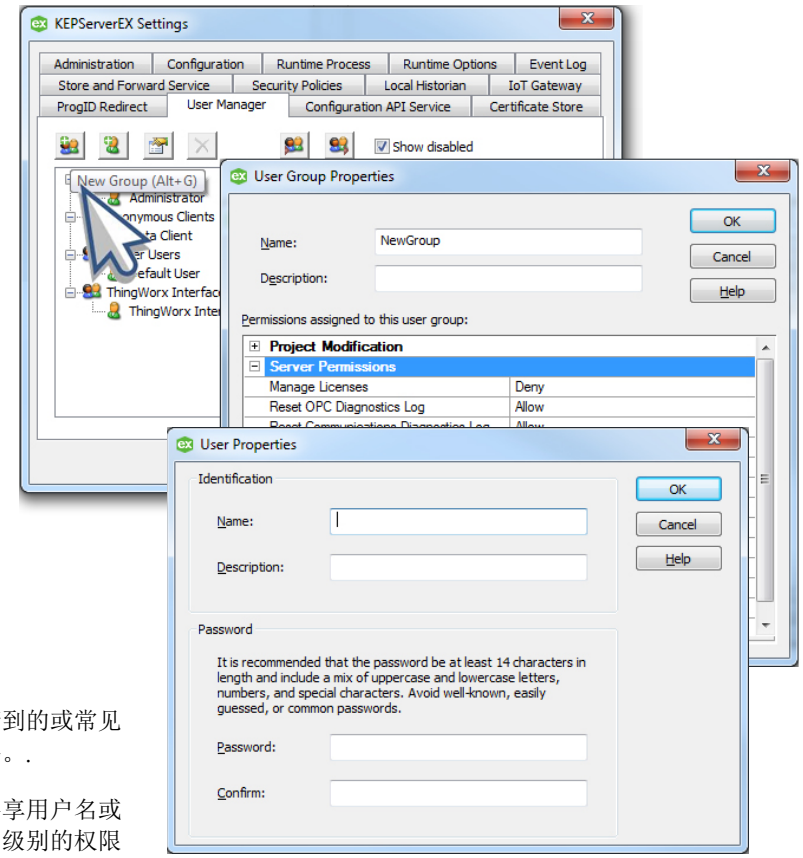
6.3.1 当配置 KEPServerEX 将连接的 REST 服务器时，尽可能设置强用户名和密码，使用强大且新型的加密方式，使用证书颁发机构 (CA) 签名的证书。

- 配置这些项将取决于所使用的特定服务器。
- 使用适当的证书进行身份验证可能需要在运行 KEPServerEX 的系统 OS 中安装证书 (有关信息，请参阅 *IoT Gateway Manual*)。

6.4 REST 服务器

6.4.1 为使用 REST 服务器代理的特定用途创建服务器用户组，并按照“最低权限”原则调整该组的权限。

1. 打开 KEPServerEX “设置”中的“用户管理器”(通过右键单击系统托盘中的 KEPServerEX 图标进行访问)。
2. 单击**添加组**。
3. 按照“最低权限”原则为新创建的组分配权限。
4. 右键单击新组，然后选择**添加用户...**。
5. 设置强密码。



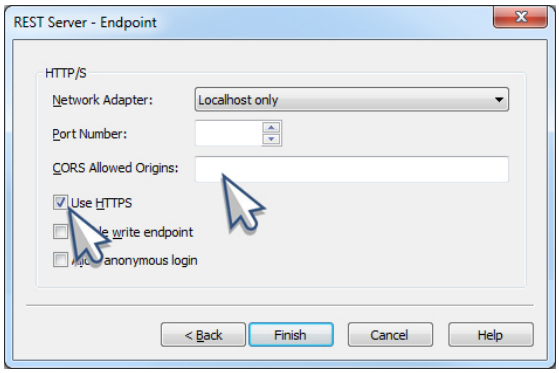
- 建议密码至少为 14 个字符，并包括大写和小写字母、数字和特殊字符的组合。
- 避免众所周知、容易猜到的或常见的密码。安全存储密码。.
- 不要在多个用户之间共享用户名或密码。当用户需要不同级别的权限时，创建新用户和新组。

6.4.2 在 KEPServerEX 中配置 REST 服务器时，使用强加密 (HTTPS)。

- 配置 REST 服务器端点时，确保启用“使用 HTTPS”属性。

6.4.3 建议使用特定的白名单域填充 CORS (Cross Origin Domain Sharing，交叉源域共享) 设置；请勿使用星号选项来全部接受。

- 配置 REST 服务器端点时，将白名单域输入 **CORS Allowed Origins** 属性。



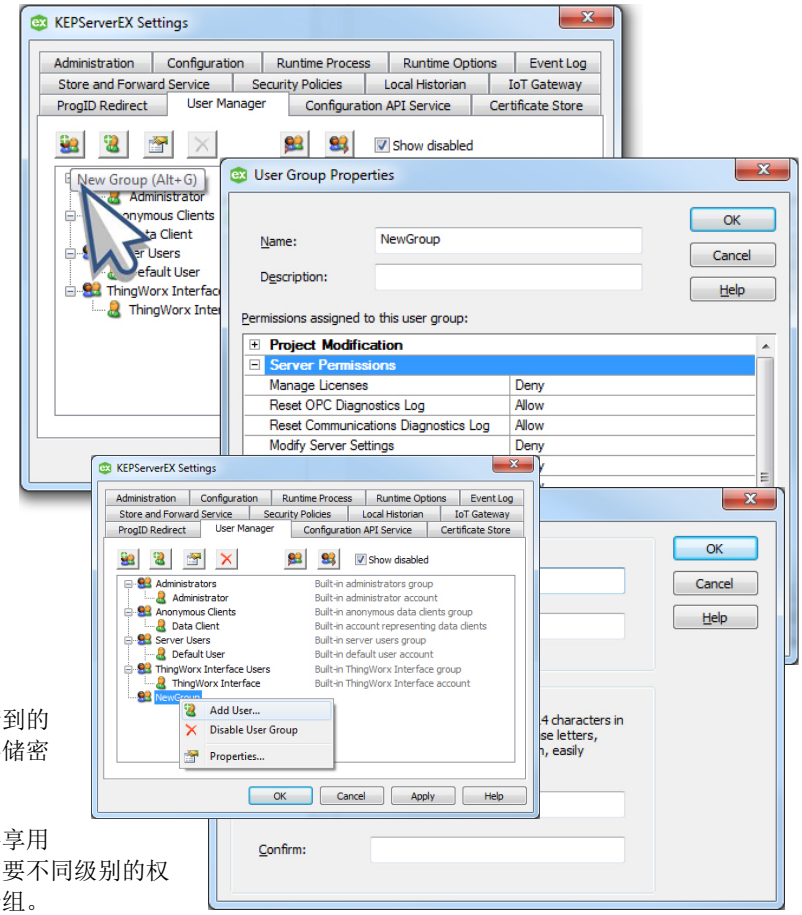
7. 配置 API

用户可以利用配置 API 以编程方式配置 KEPServerEX 驱动程序和插件。这样，面对众多 KEPServerEX 实例或不断更改的产品，用户可以无间隙地更新其配置。值得注意的是，利用此功能需要确保最高级别的安全。

7.1 配置 API

7.1.1 为使用配置 API 的特定用途创建服务器用户组，并按照“最低权限”原则调整该组的权限。

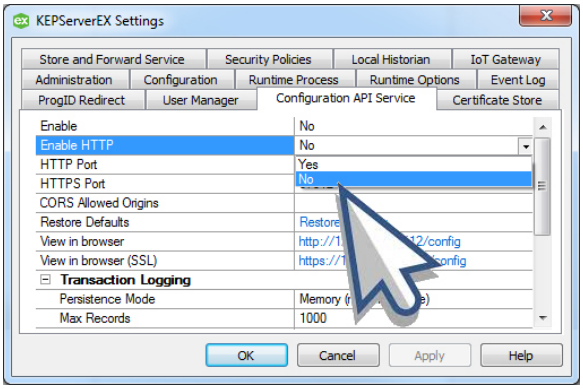
1. 打开 KEPServerEX “设置”中的“用户管理器”(通过右键单击系统托盘中的 KEPServerEX 图标进行访问)。
2. 单击**添加组**。
3. 按照“最低权限”原则为新创建的组分配权限。
4. 右键单击新组，选择**添加用户...。**
5. 设置强密码。



- 建议密码至少为 14 个字符，并包括大写和小写字母、数字和特殊字符的组合。
- 避免众所周知、容易猜到的或常见的密码。安全存储密码。.
- 不要在多个用户之间共享用户名或密码。当用户需要不同级别的权限时，创建新用户和新组。

7.1.2 建议只使用 HTTPS；不要对生产用途启用 HTTP。

1. 打开 KEPServerEX “设置”中的“配置 API 服务”设置 (通过右键单击系统托盘中的 KEPServerEX 图标进行访问)。
2. 禁用 HTTP。

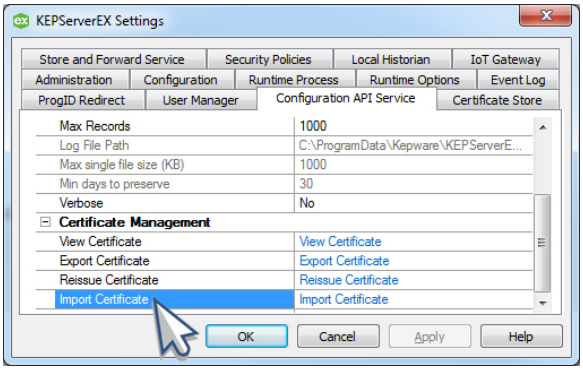


7.1.3 尽可能使用证书颁发机构 (CA) 签名的证书。

在“配置 API 服务”设置中，单击**导入证书...**并导入由 CA 签名的证书。

在“配置 API 服务”设置中，将白名单域输入 **CORS allowed origins** 设置。

- 建议使用白名单域填充 CORS (Cross Origin Domain Sharing，交叉源域共享) 设置。
- 请勿使用星号选项来全部接受。
- 在使用配置 API 时，始终监控事务日志和服务器事件日志。



事件日志的端点为 /config/v1/event_log，可通过向该端点发出 "get" 来检索。

8. 持续进行的维护

在生产环境中部署时，必须不断地评估和维护系统和 KEPServerEX 的安全性。这包括 (但不限于) 尽快将 KEPServerEX 升级到最新版本，监控外部依赖项，并在系统的整个生命周期和环境中遵循安全性最佳做法。

8.1 KEPServerEX 升级

8.1.1 用户，尤其是在安全性至关重要的环境中部署 KEPServerEX 的用户，应尽快升级到最新版本以利用安全增强功能。

8.1.2 在生产环境中部署之前，能够快速验证软件的较新版本非常重要。

- 用户应该有一个计划来快速验证和实施新版本，而不会对操作产生任何影响。ICS CERT 建议：“系统管理员应在包含相同模型和 ICS 类型的测试环境中离线测试所有修补程序，以确定修补程序是否会造成意外后果”。
- 自动化这些测试可以加快此过程。

8.2 诊断

8.2.1 仅在必要时使用产品的各种诊断功能，并在不使用时关闭诊断模式。

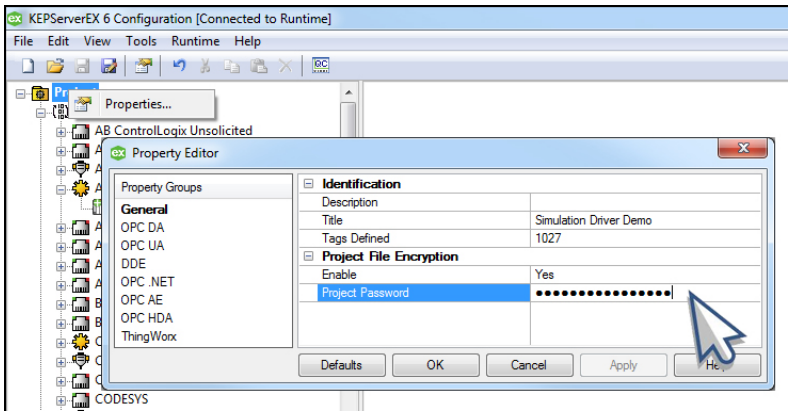
8.3 外部依存关系

8.3.1 监控所有外部依赖项，并尽快升级到最新版本。

8.4 项目文件安全性

8.4.1 在保存项目时，使用所有可用的安全机制。

1. 打开 KEPServerEX 配置。
2. 打开**项目属性**。
3. 打开**常规**属性组。
4. 设置强密码以保护 .opf 项目文件。建议密码至少为 14 个字符，并包括大写和小写字母、数字和特殊字符的组合。避免众所周知、容易猜到的或常见的密码。安全存储密码。.保存为 JSON 的项目文件对于用户可读且可编辑。最终用户在使用此格式时应仔细处理。



8.5 文档记录

8.5.1 建议记录对 KEPServerEX 的所有配置、管理或运行时更改，以及与 KEPServerEX 交互的所有系统。

这样可以支持回滚到以前的系统状态，以及在必要时能够复制任何配置。

8.5.2 定期比对本指南来检查系统配置，并验证两者间的差异是谨慎选择的结果，且不危及安全性。

9. 后续步骤

1. 访问 KEPServerEX 版本 6 产品手册中的其他信息。
2. 访问 Kepware 指南，获取有关 KEPServerEX 功能入门的信息。
3. 给 sales@kepware.com 发送电子邮件，安排一次深度演示，并了解如何在特定的环境中使用 KEPServerEX。