



Handbuch

Sichere Bereitstellung von KEPServerEX®

Juni 2018
Ref. 1.000

Inhalt

1.	Einführung.....	1
2.	Netzwerkumgebung und Systemkonfiguration.....	1
2.1	Ressourcen für ICS-Netzwerksicherheit.....	1
2.2	Systemintegratoren	2
3.	Host-Betriebssystem	2
3.1	System	2
3.2	Benutzerverwaltung.....	2
3.3	Umkreis.....	3
3.4	Nicht-Produktions-Dateien	3
4.	Installation	3
4.1	Validierung.....	3
4.2	Installation.....	3
5.	Nach der Installation.....	4
5.1	Unsichere Benutzeroberflächen	4
5.2	Server Users.....	5
6.	Sichere Benutzeroberflächen.....	7
6.1	OPC UA.....	7
6.2	MQTT	10
6.3	REST-Client	10
6.4	REST-Server	10
7.	Konfigurations-API.....	12
7.1	Konfigurations-API	12
8.	Laufende Wartung.....	14
8.1	KEPServerEX Upgrades	14
8.2	Diagnose	14
8.3	Externe Abhängigkeiten.....	14
8.4	Projektdatei-Sicherheit.....	14
8.5	Dokumentation	15
9.	Nächste Schritte.....	15

1. Einführung

KEPServerEX ermöglicht Kommunikation für die industrielle Automation und das Industrial IoT. KEPServerEX kommt häufig in Produktionssystemen in der diskreten Fertigung, Prozessfertigung und Batch-Fertigung zum Einsatz sowie bei der Herstellung und Vertrieb von Öl und Gas, Gebäudeautomation, Energieerzeugung und -verteilung, etc. Sicherheit und Betriebszeit sind wichtige Komponenten in diesen Systemen, doch die Komplexität und Häufigkeit von Sicherheitsbedrohungen wächst ständig. Es ist daher dringend erforderlich, dass KEPServerEX bei Verwendung der Software in einer Produktionsumgebung so sicher wie möglich bereitgestellt wird. Dieses Dokument führt Benutzer durch den Bereitstellungsprozess für KEPServerEX mit maximaler Sicherheit. Wir empfehlen, dass sich Administratoren bei der Bereitstellung von KEPServerEX in einer Produktionsumgebung soweit wie möglich an dieses Handbuch halten.

Kepware und PTC empfehlen, dass neue Benutzer dieses Handbuch für neue Installationen von KEPServerEX in einer Produktionsumgebung verwenden, wenn dies praktisch durchführbar ist. Außerdem empfehlen wir vorhandenen Benutzern der Software, vorhandene Konfigurationen mit den Empfehlungen in diesem Handbuch zu vergleichen und den optimalen Vorgehensweisen entsprechend anzupassen.

2. Netzwerkkumgebung und Systemkonfiguration

Netzwerksicherheit und Industrial Control System (ICS)-Netzwerksicherheit sind ein hochkomplexes Thema. Es haben sich eine Reihe von optimalen Vorgehensweisen ergeben, wozu Netzwerksegmentierung, Verwendung von demilitarisierten Zonen (DMZ), Verkehrsauswertung, die Überwachung der aktuellen physischen und logischen Bestände, erweiterte Algorithmen zur Erkennung von Anomalien und Angriffen sowie die ständige erneute Überprüfung des Netzwerks in puncto Sicherheit gehören. Optimale Vorgehensweisen ändern sich jedoch ständig und die Implementierung variiert abhängig vom konkreten Anwendungsfall (z.B. operatives Netzwerk, Satellitennetzwerk oder zelluläres Netzwerk oder ein lokales Netzwerk auf einem Rechner). Die Identifikation und Implementierung dieser optimalen Vorgehensweisen würden den Rahmen dieses Dokuments sprengen. Benutzer sind dazu angehalten internes Expertenwissen zu entwickeln und zu erhalten, um mit der Sicherung von ICS-Netzwerken zu helfen oder sie sollten sich an einen Systemintegrator mit dem erforderlichen Wissen wenden. Benutzer finden es möglicherweise auch nützlich, die nachstehend aufgeführten Organisationen und Ressourcen zu kontaktieren, wenn sie eine Sicherheitsstrategie für ICS-Netzwerke entwickeln.

KEPServerEX kann für eine Verbindung zu vielen tausend industriellen Automatisierungsgeräten und -systemen verwendet werden. Aus diesem Grund sind sicher Geräte- und Systemkonfiguration nicht Gegenstand des vorliegenden Dokuments. Befolgen Sie die optimalen Vorgehensweisen bei der Bereitstellung und Verbindung von Geräten. Dazu zählt u.a., falls verfügbar, die ordnungsgemäße Authentifizierung von Verbindungen. Genau wie bei der ICS-Netzwerksicherheit, wird empfohlen, dass Benutzer internes Expertenwissen in diesem Bereich entwickeln oder mit einem qualifizierten Systemintegrator zusammenarbeiten, der sich mit den spezifischen Geräten in der Umgebung auskennt.

2.1 Ressourcen für ICS-Netzwerksicherheit

- U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS CERT) (<https://ics-cert.us-cert.gov>)
- National Institute of Standards and Technology (<https://www.nist.gov/>)
 - National Institute of Standards and Technology's Guide to Industrial Control System Security (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>)

- North American Electric Reliability Corp. Critical Infrastructure Protection Standards (<https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>)

2.2 Systemintegratoren

- Systemintegratoren für das Kepware® System Integrator Program (<https://www.kepware.com/en-us/partners/system-integrators/>)

3. Host-Betriebssystem

KEPServerEX sollte immer in der sichersten Umgebung bereitgestellt werden. Stellen Sie sicher, dass das Host-Betriebssystem (OS) von Anfang an sicher ist und ergreifen Sie alle durchführbaren Maßnahmen, um die Sicherheit des Betriebssystems für die Lebensdauer des Systems aufrecht zu erhalten. KEPServerEX sollte in einer Umgebung bereitgestellt werden, die eine "Defense-in-Depth"-Sicherheitsstrategie, d.h. ein mehrstufiges Sicherheitssystem, verwendet im Gegensatz zu einer Umkreis-orientierten Sicherheitsphilosophie. Zu den konkreten Aspekten eines sicheren Betriebssystems zählen u.a. Systemsicherheit, Benutzerverwaltung, Firewall-Einstellungen und Dateiverwaltung.

3.1 System

- Stellen Sie sicher, dass geeignete Zugriffssteuerungsmaßnahmen vorhanden sind, um den physischen Zugriff auf die Ziel-Hardware auf die entsprechenden Benutzer zu beschränken.
- Stellen Sie KEPServerEX immer auf einer aktiv unterstützten Version von Windows bereit und installieren Sie die Windows Sicherheitspatches gemäß der ICS Sicherheitsstandards. Das Industrial Control Systems Cyber Emergency Response Team empfiehlt im Wortlaut "[Organizations should develop a systematic patch and vulnerability management approach for ICS and ensure that it reduces the exposure to system vulnerabilities while ensuring ongoing ICS operations](#)". Organisationen sind dazu angehalten, einen systematischen Patch sowie einen Ansatz für das Schwachstellen-Management für ICS zu entwickeln, und sicherzustellen, dass die Anfälligkeit von Systemen reduziert wird und der laufende ICS-Betrieb gleichzeitig aufrecht erhalten wird.
- Verschlüsseln Sie die Festplatte des Hostrechners, um die ruhenden Daten zu sichern.
- Scannen Sie das Host-System regelmäßig mit namhafter Anti-Malware-Software mit aktuellen Signaturdateien.
- Deaktivieren Sie nicht verwendete Dienste auf dem Hostrechner.
- Vermeiden Sie gemeinsames Hosten von KEPServerEX und anderen Anwendungen, um die Angriffsfläche zu reduzieren.

3.2 Benutzerverwaltung

- Erstellen Sie einen Windows-Benutzer getrennt vom Administrator-Konto, um KEPServerEX zu konfigurieren und zu verwalten.
- Verwalten Sie das Administrator-Konto gemäß den von Windows empfohlenen Verfahrensweise.
- Benutzerpasswörter müssen der formellen Passwortrichtlinie für die entsprechende Domäne entsprechen.
- Passwörter und Anmeldeinformationen dürfen nicht von mehreren Benutzern gemeinsam genutzt werden.
- Bewahren Sie die Passwörter sicher auf.
- Überprüfen Sie das Zugriffssteuerungsmodell regelmäßig, um sicherzustellen, dass die Berechtigungen unter Verwendung des Prinzips der geringsten Rechte (d.h. Berechtigungen

werden nur denjenigen Benutzern, die bestimmte erforderliche Funktionen ausführen müssen, gewährt und widerrufen, wenn sie nicht länger benötigt werden) festgelegt werden.

3.3 Umfang

- Verwenden Sie eine Firewall, um den externen Fußabdruck zu minimieren und überprüfen Sie die Firewall-Einstellungen regelmäßig.
- Verwenden Sie ein Angriffserkennungssystem (Intrusion Detection System - IDS).
- Überwachen Sie den Remote-Zugriff auf das Host-Betriebssystem und protokollieren Sie die Aktivitäten.

3.4 Nicht-Produktions-Dateien

- Entfernen Sie Sicherungsdateien regelmäßig vom Produktionssystem.
- Entfernen Sie Beispiel- oder Testdateien sowie Skripts vom Produktionssystem.

4. Installation

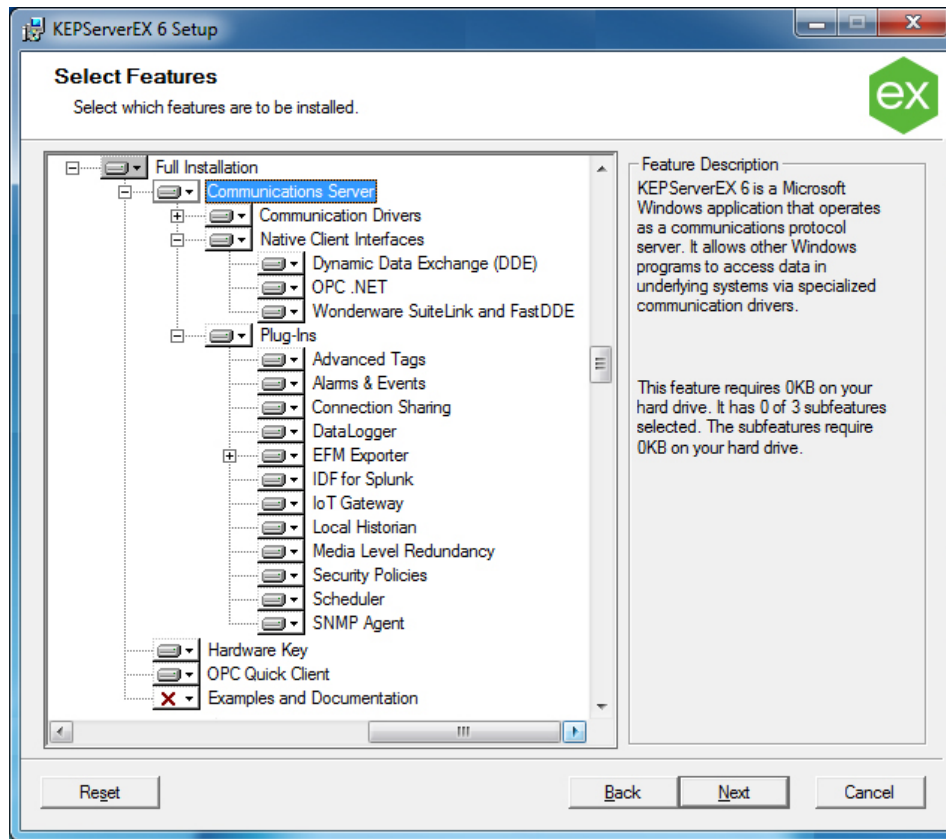
Benutzer sollten die KEPServerEX Installation validieren und nur die Funktionen installieren, die für eine bestimmte Anwendung erforderlich sind. Verwenden Sie während der Installation ein starkes Administrator-Passwort.

4.1 Validierung

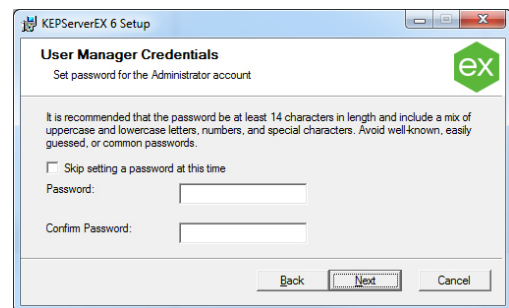
- 4.1.1 Kepware unterhält eindeutige Identifikationscodes für offiziell freigegebene Software. Kunden sollten diese Codes vergleichen, um sicherzustellen, dass nur zertifizierte ausführbare Dateien installiert werden.
- Befolgen Sie die Anweisungen unter: <https://www.kepware.com/digitalsignature>.

4.2 Installation

- 4.2.1 Wird während der Installation das Dialogfenster "Funktionen auswählen" angezeigt, installieren Sie nur die Funktionen, die für die vorliegende Umgebung erforderlich sind.



- 4.2.2 Wird während der Installation das Dialogfenster "Benutzermanager-Anmeldeinformationen" angezeigt, legen Sie ein starkes Administratorpasswort fest. Es wird empfohlen, ein Passwort aus mindestens 14 Zeichen zu verwenden. Das Passwort sollte große und kleine Buchstaben sowie Zahlen und Sonderzeichen enthalten. Vermeiden Sie beliebige, leicht zu ratende oder allgemeine Passwörter. Bewahren Sie die Passwörter sicher auf.

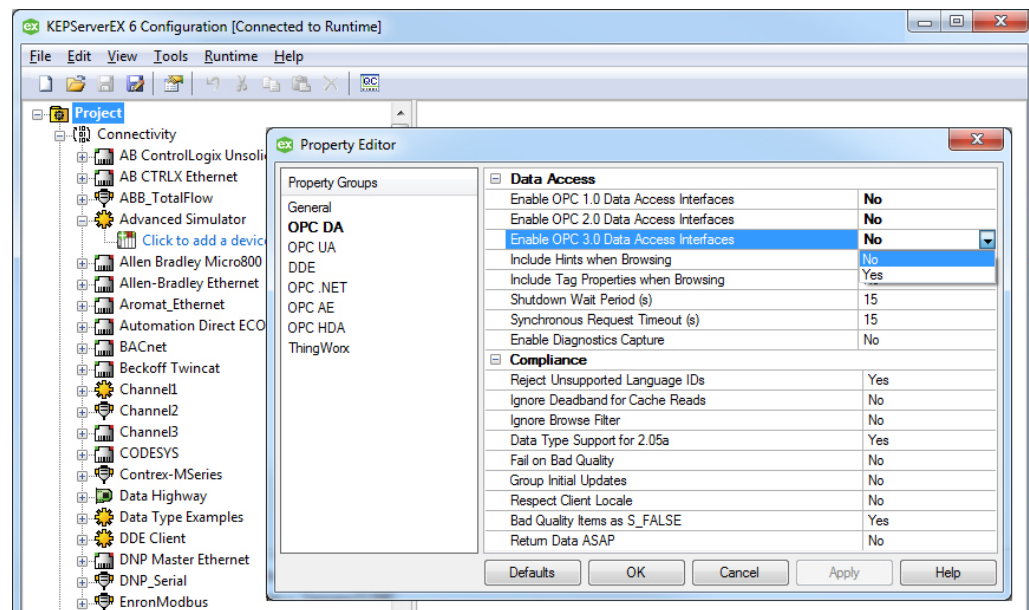


5. Nach der Installation

Nach der Installation des Produkts sollte der KEPServerEX Administrator mehrere Aktionen ausführen, um das höchste Sicherheitsniveau zu gewährleisten. Unsichere Benutzeroberflächen, die von Benutzern nicht verwendet werden, sollten deaktiviert werden und Benutzergruppen und Benutzer sollten unter Verwendung des Prinzips der geringsten Rechte konfiguriert werden.

5.1 Unsichere Benutzeroberflächen

- 5.1.1 Deaktivieren Sie die OPC DA-Benutzeroberfläche, wenn sie für die spezifische Anwendung nicht benötigt wird. Bei OPC DA handelt es sich um ein Legacy-Protokoll, das ohne ein angemessenes Sicherheitsniveau schwer bereitzustellen ist. Soweit mögliche sollten Benutzer eines der in diesem Dokument aufgeführten sicheren Protokolle verwenden.
1. Führen Sie die KEPServerEX Konfiguration aus.
 2. Klicken Sie mit der rechten Maustaste auf "Projekt" und wählen Sie **Projekteigenschaften** aus.



3. Wählen Sie Eigenschaftengruppe **OPC DA** aus.
4. Deaktivieren Sie die Datenzugriff-Benutzeroberflächen für OPC 1.0, 2.0 und 3.0, indem Sie die erstellen drei Eigenschaften auf "Nein" festlegen.

5.1.2 Wiederholen Sie diese Schritte jedes Mal, wenn ein neues Projekt erstellt wird, das keine OPC DA-Konnektivität benötigt.

- Wird die OPC DA Benutzeroberfläche deaktiviert, so wird der Zugriff auf das eingebaute Quick Client-Tool, das zum Testen der Konnektivität verwendet wird, verweigert. Verwenden Sie ein Drittpartei-Tool, wie z.B. [UA Expert](#), um die Konnektivität zu testen.

5.2 Server Users

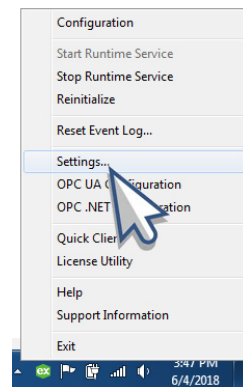
5.2.1 Erstellen Sie ein starkes Passwort für den Default User (Standardbenutzer) in der Benutzergruppe für Server Users (Serverbenutzer).

1. Öffnen Sie die administrativen Einstellungen durch Rechtsklick auf das KEPServerEX Symbol in der Taskleiste und klicken Sie auf **Einstellungen**.

2. Wählen Sie die Registerkarte **Benutzermanager** aus.

- Der für den Zugriff auf das Menü **Einstellungen** erforderlich Benutzername sowie das erforderliche Passwort mit der entsprechenden Berechtigungsebene ist in diesem Fall der Benutzername und das Passwort für den Administrator.

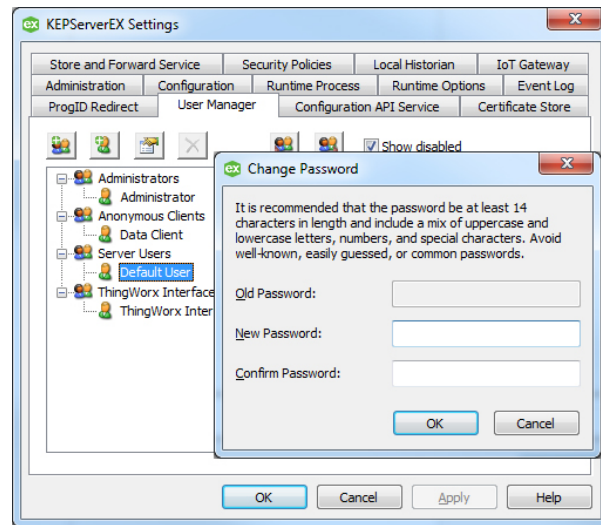
3. Doppelklicken Sie auf **Default User** unter der Gruppe "Server Users".



- Legen Sie ein starkes Passwort fest. Es wird empfohlen, ein Passwort aus mindestens 14 Zeichen zu verwenden. Das Passwort sollte große und kleine Buchstaben sowie Zahlen und Sonderzeichen enthalten. Vermeiden Sie beliebige, leicht zu ratende oder allgemeine Passwörter. Bewahren Sie die Passwörter sicher auf.

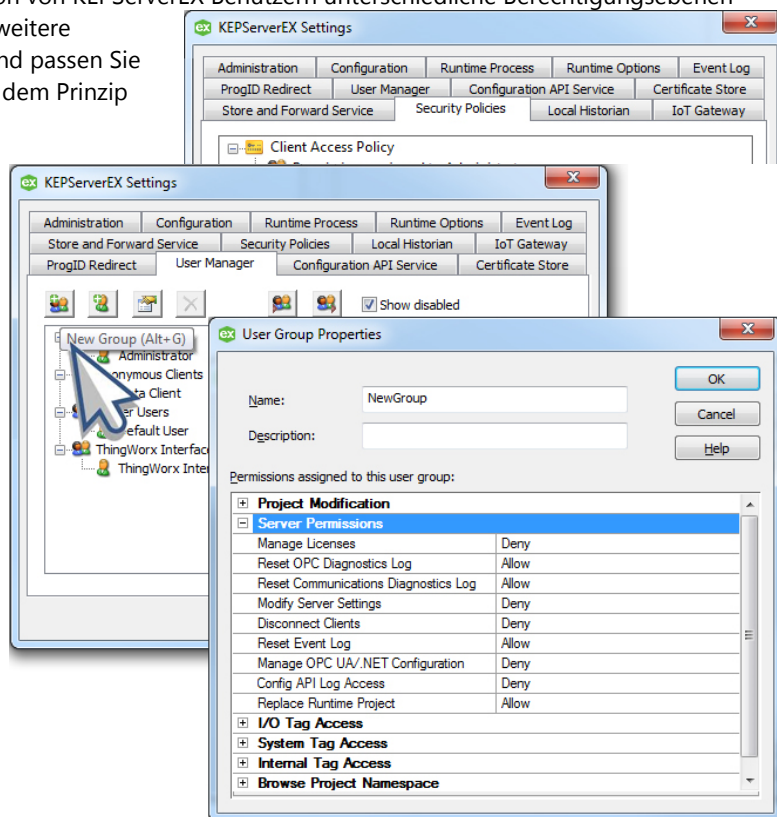
5.2.2 Passen Sie die Berechtigungen für den Default User gemäß dem Prinzip der geringsten Rechte (d.h. Berechtigungen werden nur denjenigen Benutzern, die bestimmte erforderliche Funktionen ausführen müssen, gewährt und widerrufen, wenn sie nicht länger benötigt werden) an.

- Öffnen Sie die Registerkarte **Sicherheitsrichtlinien** in "KEPServerEX - Einstellungen".
- Erweitern Sie die für Server Users zugewiesenen Berechtigungen und passen Sie sie gemäß dem Prinzip der geringsten Rechte an.



5.2.3 Werden für die Konfiguration von KEPServerEX Benutzern unterschiedliche Berechtigungsebenen benötigt, erstellen Sie ggf. weitere Gruppen für Server Users und passen Sie die Berechtigungen gemäß dem Prinzip der geringsten Rechte an.

- Öffnen Sie die Registerkarte **Benutzermanager** in "KEPServerEX - Einstellungen".
- Klicken Sie auf **Neue Gruppe (Alt+G)**.
- Weisen Sie der neu erstellten Gruppe Berechtigungen gemäß dem Prinzip der geringsten Rechte zu.
- Klicken Sie mit der rechten Maustaste auf die neue Gruppe.

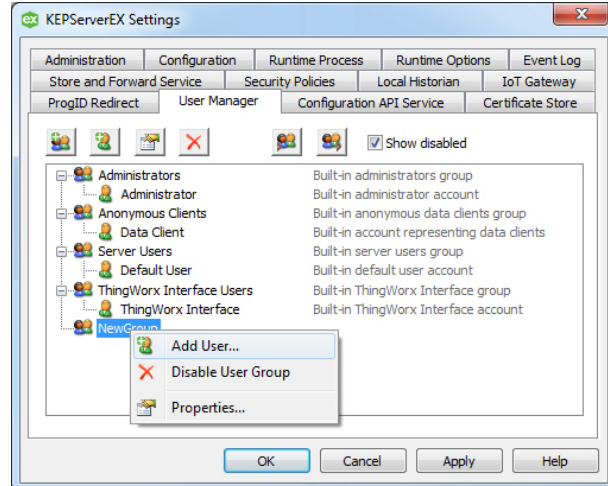


5. Klicken Sie auf **Benutzer hinzufügen...**

6. Legen Sie ein starkes Passwort fest. Es wird empfohlen, ein Passwort aus mindestens 14 Zeichen zu verwenden. Das Passwort sollte große und kleine Buchstaben sowie Zahlen und Sonderzeichen enthalten.

● Vermeiden Sie beliebige, leicht zu ratende oder allgemeine Passwörter. Bewahren Sie die Passwörter sicher auf.

● Benutzernamen und Anmeldeinformationen dürfen nicht von mehreren Benutzern gemeinsam genutzt werden! Erstellen Sie einen neuen Benutzer oder eine neue Gruppe, wenn Benutzer oder Gruppen unterschiedliche Berechtigungssebenen benötigen.



6. Sichere Benutzeroberflächen

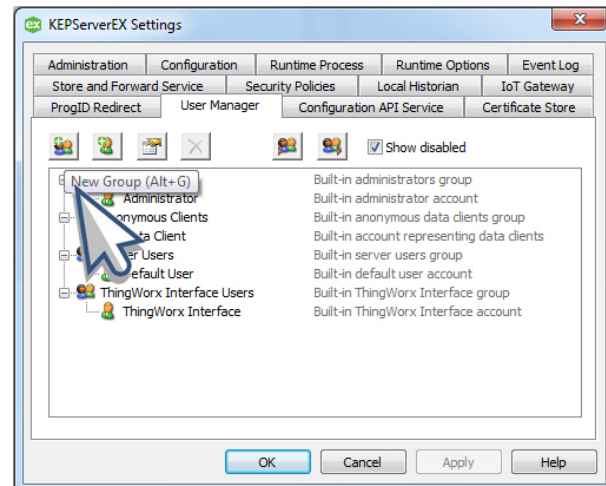
KEPServerEX wurde für die Kommunikation über Protokolle, die in der industriellen Automation und im Industrial Internet of Things (IIOT) häufig verwendet werden, entwickelt. Bestimmte Protokolle sind sicherer und verfügen über mehr Sicherheitsoptionen als andere Protokolle. OPC UA, MQTT und REST sind beliebte Protokolle, die so konfiguriert werden können, dass ein hohes Sicherheitsniveau aufrechterhalten wird. Es gibt auch noch andere Protokolle die ebenfalls sicher konfiguriert werden können (SNMP, Native ThingWorx Schnittstelle, etc.).

● Weitere Informationen zu anderen sicheren Protokollen finden Sie im *KEPServerEX Handbuch*.

6.1 OPC UA

6.1.1 Erstellen Sie eine Gruppe für Server Users für den spezifischen Zweck der Verwendung der OPC UA-Benutzeroberfläche und passen Sie die Berechtigungen für diese Gruppe gemäß dem Prinzip der geringsten Rechte an.

1. Öffnen Sie die Registerkarte "Benutzermanager" in "KEPServerEX - Einstellungen".
2. Klicken Sie auf **Neue Gruppe (Alt+G)**.



3. Weisen Sie der neuen Gruppe Berechtigungen gemäß dem Prinzip der geringsten Rechte zu.

4. Klicken Sie mit der rechten Maustaste auf die neue Gruppe.

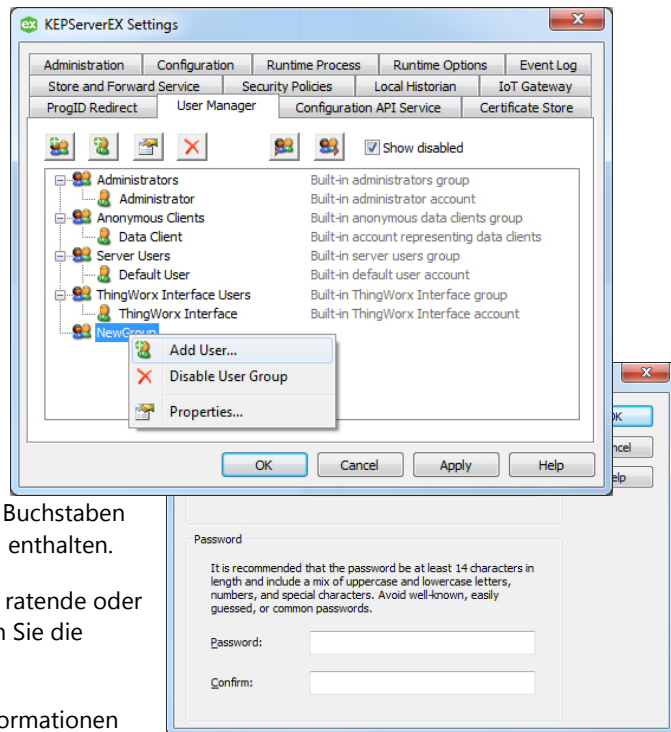
5. Klicken Sie auf **Benutzer hinzufügen...**

6. Legen Sie ein starkes Passwort fest. Es wird empfohlen, ein Passwort aus mindestens 14 Zeichen zu verwenden. Das Passwort sollte große und kleine Buchstaben sowie Zahlen und Sonderzeichen enthalten.

● Vermeiden Sie beliebte, leicht zu ratende oder allgemeine Passwörter. Bewahren Sie die Passwörter sicher auf.

● Benutzernamen und Anmeldeinformationen dürfen nicht von mehreren Benutzern gemeinsam genutzt werden! Erstellen Sie einen neuen Benutzer oder eine neue Gruppe, wenn Benutzer oder Gruppen unterschiedliche Berechtigungsebenen benötigen.

● Anonyme UA-Anmeldungen sind standardmäßig deaktiviert. Es wird empfohlen, niemals anonymen UA-Client-Zugriff zu gewähren.



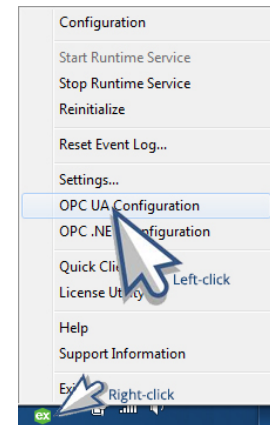
6.1.2 Verwenden Sie beim Erstellen des OPC UA-Server-Endpunkts die derzeit verfügbaren höchsten Sicherheitseinstellungen.

1. Öffnen Sie den "OPC UA Configuration Manager" durch Rechtsklick auf das KEPServerEX Symbol in der Taskleiste und wählen Sie anschließend **OPC UA Konfiguration**.

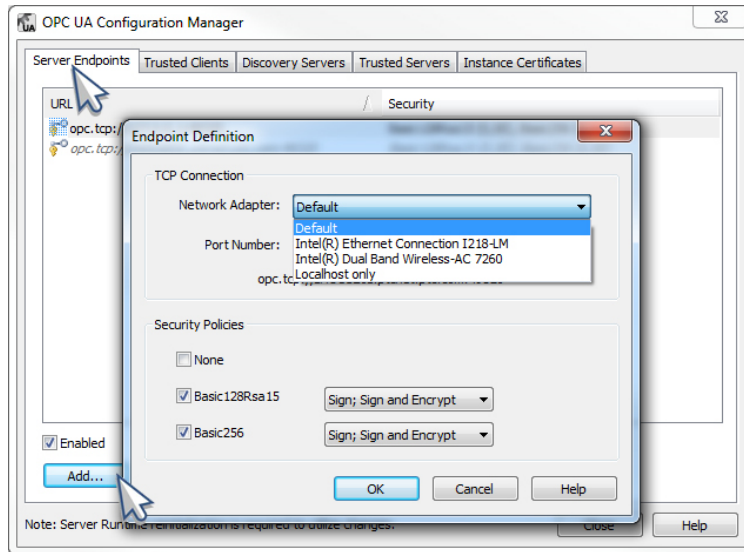
2. Klicken Sie auf die Registerkarte **Serverendpunkte**.

3. Klicken Sie auf die Schaltfläche **Hinzufügen...**, um einen neuen Endpunkt zu definieren.

4. Stellen Sie sicher, dass die aktuellsten Sicherheitsrichtlinien ausgewählt sind.

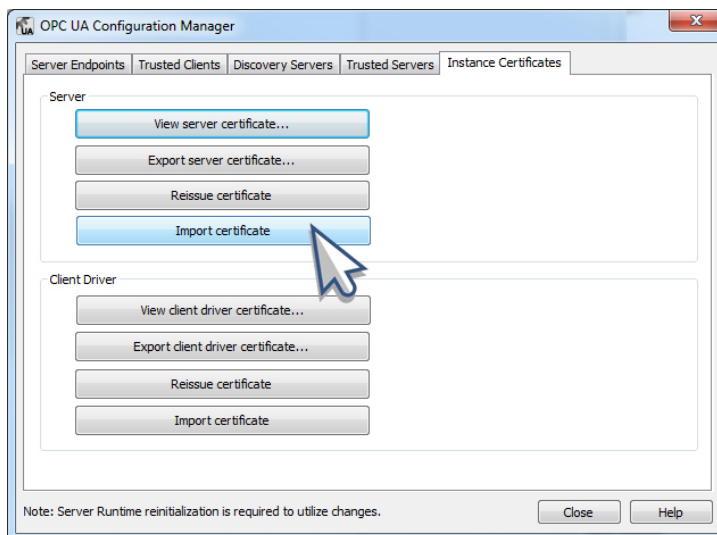


5. Klicken Sie auf **OK**.



- 6.1.3 Verwenden Sie, wenn möglich, ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat.

Klicken Sie auf der Registerkarte "Instanzzertifikate" im Dialogfenster "OPC UA Configuration Manager" auf **Zertifikat importieren** und importieren Sie ein von einer Zertifizierungsstelle

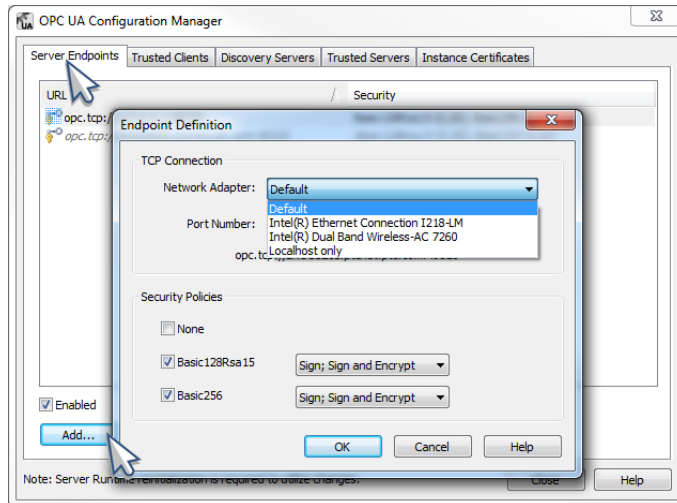


signiertes Zertifikat.

- Verwenden Sie beim Erstellen eines OPC-Server-Endpunkts einen Netzwerkadapter, auf den nur über ein Netzwerk zugegriffen werden kann, welches den OPC UA-Client ausführt, der auf KEPServerEX zugreift. (Verwenden Sie keinen Adapter, der über das Internet oder andere Netzwerke, die für die Konnektivität nicht erforderlich sind, zugänglich ist.)

1. Öffnen Sie den OPC UA Configuration Manager.

2. Fügen Sie einen neuen Endpunkt hinzu.



3. Stellen Sie sicher, dass nur über das Netzwerk, auf dem der OPC UA-Client ausgeführt wird, auf den verwendeten Netzwerkadapter zugegriffen werden kann.

6.2 MQTT

- 6.2.1 Legen Sie beim Konfigurieren des MQTT-Broker, zu dem KEPServerEX eine Verbindung herstellen wird, einen starken Benutzernamen und ein starkes Passwort fest, verwenden Sie starke und moderne Verschlüsselung und, wenn möglich, ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat.

- Die Konfiguration dieser Elemente ist abhängig vom verwendeten Broker.

6.3 REST-Client

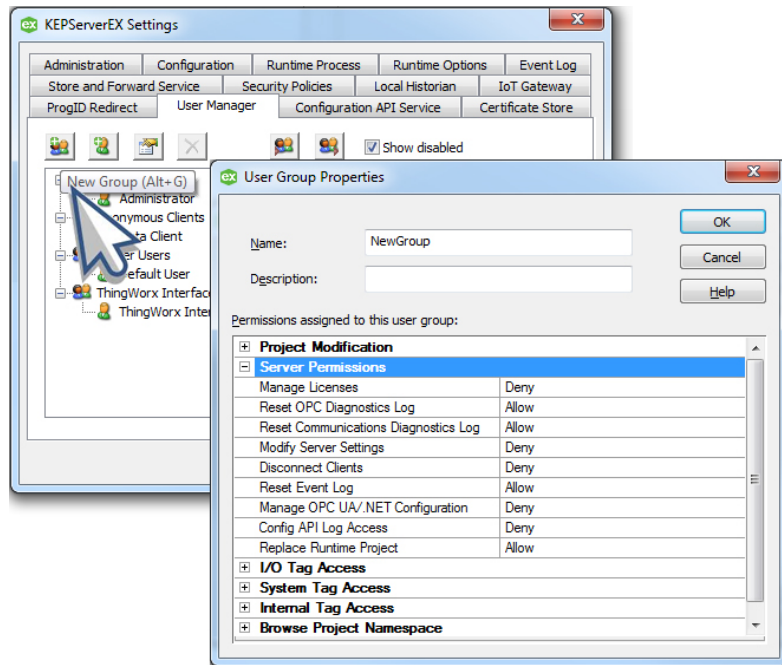
- 6.3.1 Legen Sie beim Konfigurieren des REST-Servers, zu dem KEPServerEX eine Verbindung herstellen wird, einen starken Benutzernamen und ein starkes Passwort fest, verwenden Sie starke und moderne Verschlüsselung und, wenn möglich, ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat.

- Die Konfiguration dieser Elemente hängt von dem spezifischen verwendeten Server ab.
- Eine Authentifizierung unter Verwendung des entsprechenden Zertifikats erfordert möglicherweise die Installation des Zertifikats auf dem Betriebssystem, auf dem KEPServerEX ausgeführt wird. (Weitere Informationen finden Sie im englischen Handbuch [IoT Gateway Manual](#)).

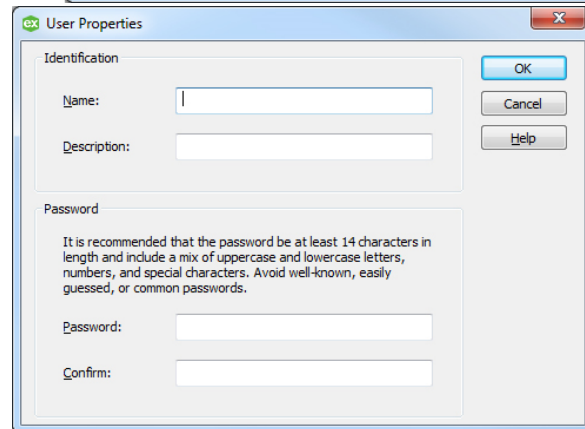
6.4 REST-Server

- 6.4.1 Erstellen Sie eine Gruppe für Server Users für den spezifischen Zweck der Verwendung des Rest-Server-Agenten, und passen Sie die Berechtigungen für diese Gruppe gemäß dem Prinzip der geringsten Rechte an.

1. Öffnen Sie die Registerkarte "Benutzermanager" in "KEPServerEX - Einstellungen", indem Sie mit der rechten Maustaste auf das KEPServerEX Symbol in der Taskleiste klicken.



2. Klicken Sie auf **Neue Gruppe (Alt+G)**.
3. Weisen Sie der neu erstellten Gruppe Berechtigungen gemäß dem Prinzip der geringsten Rechte zu.
4. Klicken Sie mit der rechten Maustaste auf die neue Gruppe und wählen Sie **Benutzer hinzufügen...** aus.
5. Legen Sie ein starkes Passwort fest.

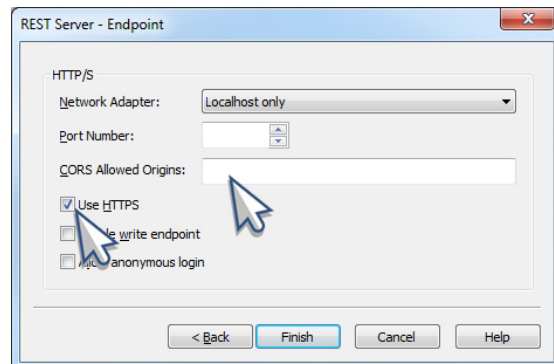


- Es wird empfohlen, ein Passwort aus mindestens 14 Zeichen zu verwenden. Das Passwort sollte große und kleine Buchstaben sowie Zahlen und Sonderzeichen enthalten.
- Vermeiden Sie beliebige, leicht zu ratende oder allgemeine Passwörter. Bewahren Sie die Passwörter sicher auf.
- Benutzernamen und Anmeldeinformationen dürfen nicht von mehreren Benutzern gemeinsam genutzt werden! Erstellen Sie einen neuen Benutzer oder eine neue Gruppe, wenn Benutzer oder Gruppen unterschiedliche Berechtigungsebenen benötigen.

- 6.4.2 Verwenden Sie bei der Konfiguration des REST-Server in KEPServerEX eine starke Verschlüsselung (HTTPS).

- Stellen Sie bei der Konfiguration eines REST-Server-Endpunkts sicher, dass das Kontrollkästchen **Use HTTPS** aktiviert ist.

- 6.4.3 Es wird empfohlen, dass Sie die Einstellungen für Cross-Origin Resource Sharing (CORS) mit spezifischen Domänen von der Positivliste füllen. Verwenden Sie kein Sternchen, um alle zu akzeptieren.



- Geben Sie bei der Konfiguration eines REST-Server-Endpunkts Domänen von der Whitelist in das Feld **Von CORS zugelassene Ursprünge** ein.

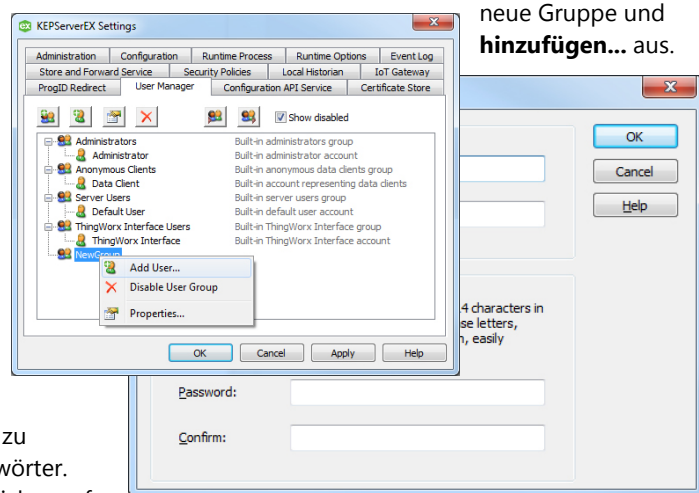
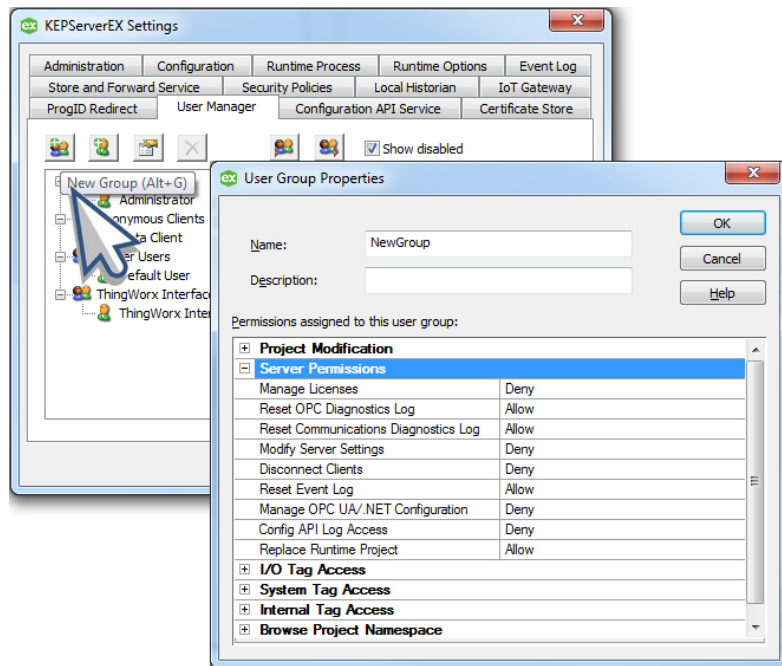
7. Konfigurations-API

Die Konfigurations-API erlaubt es Benutzern, bestimmte KEPServerEX Driver und Plugins programmatisch zu konfigurieren. Benutzer mit vielen KEPServerEX Instanzen oder sich ständig ändernden Produkten können Ihre Konfigurationen mithilfe der Konfigurations-API problemlos aktualisieren. Es ist wichtig, dass bei der Verwendung dieser Funktion ein Höchstmaß an Sicherheit verwendet wird.

7.1 Konfigurations-API

7.1.1 Erstellen Sie eine Gruppe für Server Users für den spezifischen Zweck der Verwendung der Konfigurations-API und passen Sie die Berechtigungen für diese Gruppe gemäß dem Prinzip der geringsten Rechte an.

- Öffnen Sie die Registerkarte "Benutzermanager" in "KEPServerEX - Einstellungen", indem Sie mit der rechten Maustaste auf das KEPServerEX Symbol in der Taskleiste klicken.
- Klicken Sie auf **Neue Gruppe (Alt+G)**.
- Weisen Sie der neu erstellten Gruppe Berechtigungen gemäß dem Prinzip der geringsten Rechte zu.
- Klicken Sie mit der rechten Maustaste auf die wählen Sie **Benutzer**
- Legen Sie ein starkes Passwort fest.
 - Es wird empfohlen, ein Passwort aus mindestens 14 Zeichen zu verwenden. Das Passwort sollte große und kleine Buchstaben sowie Zahlen und Sonderzeichen enthalten.
 - Vermeiden Sie beliebige, leicht zu ratende oder allgemeine Passwörter. Bewahren Sie die Passwörter sicher auf.
 - Benutzernamen und Anmeldeinformationen dürfen nicht von

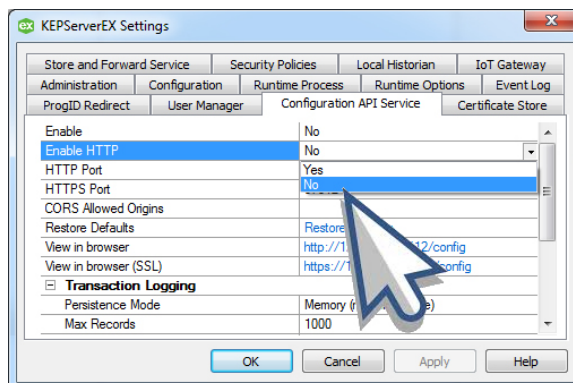


neue Gruppe und
hinzufügen... aus.

mehreren Benutzern gemeinsam genutzt werden! Erstellen Sie einen neuen Benutzer oder eine neue Gruppe, wenn Benutzer oder Gruppen unterschiedliche Berechtigungsebenen benötigen.

7.1.2 Es wird empfohlen, nur HTTPS zu verwenden. HTTP sollte für die Produktionsumgebung nicht aktiviert werden.

1. Öffnen Sie die Registerkarte "Konfigurations-API-Dienst" in "KEPServerEX - Einstellungen", indem Sie mit der rechten Maustaste auf das KEPServerEX Symbol in der Taskleiste klicken.

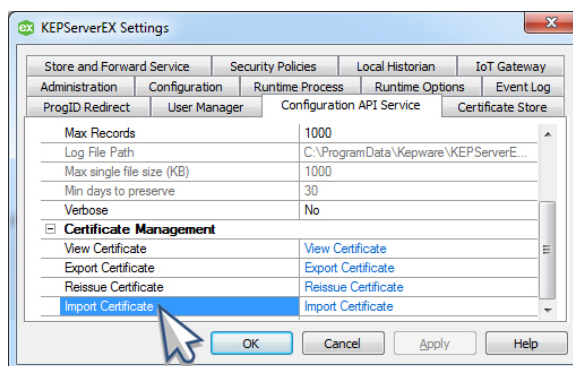


2. Deaktivieren Sie HTTP.

7.1.3 Verwenden Sie, wenn möglich, ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat.

Klicken Sie in den Einstellungen für "Konfigurations-API-Dienst" auf **Zertifikat importieren** und importieren Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat.

Geben Sie in den Einstellungen für "Konfigurations-API-Dienst" Domänen von der Whitelist in das Feld **Von CORS zugelassene Ursprünge** ein.



- Es wird empfohlen, Einstellungen für Cross-Origin Domain Sharing mit Domänen von der Whitelist zu füllen.

- Verwenden Sie KEIN Sternchen, um alle zu akzeptieren.

- Überwachen Sie Transaktionsprotokolle und das Serverereignis-Protokoll solange die Konfigurations-API verwendet wird.

Der Endpunkt für das Ereignisprotokoll ist /config/v1/event_log und kann via einer "get"-Anweisung zu diesem Endpunkt abgerufen werden.

8. Laufende Wartung

Bei der Bereitstellung in einer Produktionsumgebung ist es wichtig, die Systemsicherheit sowie die Sicherheit von KEPServerEX ständig zu auswerten sowie aufrechtzuerhalten. Dazu zählen u.e. ein schnellstmögliches Upgrade von KEPServerEX auf die neuste Version, die Überwachung externer Abhängigkeiten und die Anwendung optimaler Vorgehensweisen in Bezug auf die Sicherheit über den gesamten Lebenszyklus des Systems hinweg sowie in der Umgebung.

8.1 KEPServerEX Upgrades

- 8.1.1 Es ist unbedingt erforderlich, dass Benutzer, insbesondere Benutzer, die KEPServerEX in sicherheitskritischen Umgebungen bereitstellen, schnellstmöglich ein Upgrade auf die neuste Version vornehmen, um von Verbesserungen bei der Sicherheit zu profitieren.
- 8.1.2 Es ist wichtig, neuere Versionen der Software schnell validieren zu können, bevor diese in einer Produktionsumgebung bereitgestellt wird.
 - Benutzer sollten einen Plan parat haben, um neuere Versionen schnell zu validieren und zu implementieren, ohne dass sich dies nachteilig auf den Betrieb auswirkt. Das Industrial Control Systems Cyber Emergency Response Team (ICS CERT) empfiehlt, dass Systemadministratoren alle Patches offline in einer Testumgebung mit dem gleichen ICS-Modell und -Typ testen, um herauszufinden, ob der Patch negative Auswirkungen haben könnte.
 - Dieser Prozess kann durch eine Automatisierung dieser Tests beschleunigt werden.

8.2 Diagnose

- 8.2.1 Verwenden Sie die unterschiedlichen Diagnosefunktionen im Produkt nur wenn nötig und deaktivieren Sie die Diagnosemodi, wenn sie nicht in Gebrauch sind.

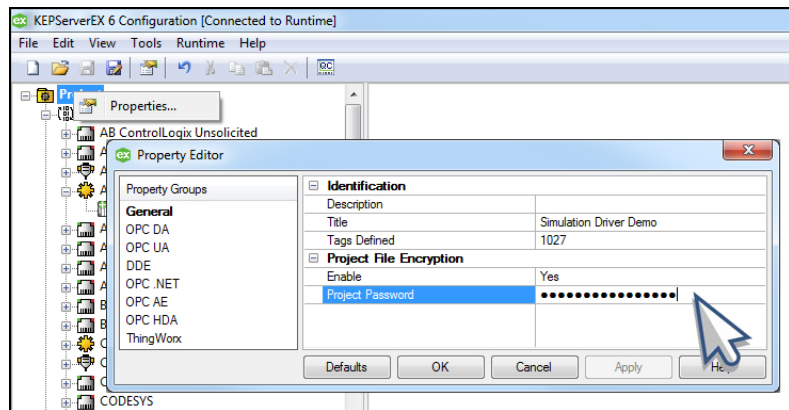
8.3 Externe Abhängigkeiten

- 8.3.1 Überwachen Sie alle externen Abhängigkeiten und führen Sie sobald als möglich ein Upgrade auf die neueste Version durch.

8.4 Projektdatei-Sicherheit

- 8.4.1 Verwenden Sie beim Speichern eines Projekts alle zur Verfügung stehenden Sicherheitsmechanismen.
 1. Öffnen Sie die KEPServerEX Konfiguration.
 2. Doppelklicken oder rechtsklicken Sie auf "Projekt" und öffnen Sie **Eigenschaften....**
 3. Öffnen Sie die Eigenschaftsgruppe **Allgemein**.

4. Legen Sie ein starkes Passwort fest, um die .opf-Projektdateien zu schützen. Es wird empfohlen, ein Passwort aus mindestens 14 Zeichen zu verwenden. Das Passwort sollte große und kleine Buchstaben sowie Zahlen und Sonderzeichen enthalten. Vermeiden Sie beliebte, leicht zu ratende oder allgemeine Passwörter. Bewahren Sie die Passwörter sicher auf. In JSON gespeicherte Projektdateien sind lesbar und können bearbeitet werden. Endbenutzer sollten bei der Verwendung dieses Formats Vorsicht walten lassen.



8.5 Dokumentation

- 8.5.1 Es wird empfohlen, alle Konfigurationsänderungen, administrativen Änderungen oder Änderungen zur Laufzeit, die an KEPServerEX vorgenommen wurden, zu dokumentieren sowie alle Änderungen an Systemen, die mit KEPServerEX interagieren.

Dies ermöglicht es, einen Rollback zu einem vorherigen Systemstatus durchzuführen und es kann jede gewünschte Konfiguration repliziert werden, sollte dies notwendig werden.
- 8.5.2 Überprüfen Sie die Systemkonfiguration regelmäßig und vergleichen Sie sie mit diesem Handbuch. Bestätigen Sie, dass eventuelle Abweichungen auf bewusst getroffenen Entscheidungen beruhen und die Sicherheit nicht kompromittieren.

9. Nächste Schritte

1. Weitere Informationen finden Sie im [KEPServerEX Version 6 Produkthandbuch](#).
2. Verwenden Sie die [Kepware Handbücher](#), um sich über erste Schritte mit KEPServerEX Funktionen zu informieren.
3. Senden Sie eine E-Mail an sales@kepware.com, um einen Termin für eine ausführliche Demonstration zu vereinbaren und um zu erfahren, wie KEPServerEX in einer bestimmten Umgebung eingesetzt werden kann.