



TOC

Secure Deployment Guide —Kepware Server	3
Introduction	3
Network Environment and System Configuration	3
Resources on ICS Network Security	4
System Integrators	4
Host Operating System	4
System	4
User Management	4
Perimeter	5
Non- Production Files	5
Installation	5
Validation	5
Installation	5
Post- Installation	6
Application Data User Permissions	7
Unsecure Interfaces	7
Server Users	8
Secure Interfaces	11
OPC UA Server	11
OPC UA Gateway	13
UA Gateway Server Interface	13
UA Gateway Client Interface Connections	15
MQTT	16
REST Client	16

REST Server	17
MQTT Client SSL/ TLS Hostname Verification	18
Configuration API	18
Configuration API	18
Ongoing Maintenance	20
Upgrades	21
Diagnostics	21
External Dependencies	21
Project File Security	21
Documentation	21
Next Steps	22

Secure Deployment Guide —Kepware Server

September 2026

Version 1.019

Proprietary Notice This publication is provided by Velotic™ and/or its affiliates for informational purposes only and does not constitute legal, security or financial advice. The contents of the publication are based on information, data and sources made available by you to Velotic™ and while every effort has been made to ensure the accuracy of the report, Velotic™ does not guarantee the accuracy, completeness, or reliability of the information contained herein. No representations or warranties, express or implied, are made as to the accuracy, completeness, or reliability of the information contained herein and Velotic™ does not accept any responsibility for any loss or damage arising from the use of, or reliance on, the information presented in this report. You acknowledge that reliance upon the contents of this report is at your sole risk. No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of Velotic™. Information contained herein is subject to change without notice. ©2026 Velotic™ and/or its affiliates. All rights reserved. Trademark Notices Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries. All other trademarks are the property of their respective owners.

Introduction

Kepware Server enables communication for industrial automation and the industrial IoT. It is often used in production systems in discrete, process, and batch manufacturing; oil and gas production and distribution; building automation; energy production and distribution; and more. Safety and uptime are key components of these systems, but cybersecurity threats are increasing in both frequency and complexity. It is therefore paramount that when utilizing the software in a production environment, users deploy the application as securely as possible. This document guides users through the process of deploying Kepware Server with maximum security. It is recommended that administrators follow this guide as closely as possible when deploying in a production environment.

Kepware recommends new users utilize this guide for new production installations whenever practical.

Kepware also recommends existing users of the software compare existing configurations with the recommendations provided in this guide and adjust for best practices.

This document is a guide for installing and licensing Kepware Server.

Network Environment and System Configuration

Network security and Industrial Control System (ICS) network security is a highly complex subject. There is a set of best practices emerging that includes network segmentation, use of DMZs, traffic evaluation, maintaining up-to-date physical and logical inventories, advanced algorithms for anomaly and intrusion detection, and constant reexamination of the network from a security standpoint. However, best practices are changing constantly and implementation will vary based on the specific use case (e.g. operations network, satellite or cell network, or local network on a machine). The identification and implementation of these best practices are beyond the scope of this document. Users should develop and maintain in-house expertise to help secure the ICS networks or work with a systems integrator with the requisite expertise. Users may also find it valuable to consult the organizations and resources listed below when developing a security strategy for the ICS networks.

Kepware Server can be used to connect many thousands of different industrial automation devices and systems. As such, secure device and system configuration is beyond the scope of this document. Follow best practices when deploying and connecting any and all devices. These include, but are not limited to, proper authentication of connections whenever available. As with ICS network security, it is recommended that users develop internal expertise in this area or work with a qualified system integrator with knowledge of the specific devices in the environment.

Resources on ICS Network Security

- United States Computer Emergency Readiness Team (US-CERT) is an organization within the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) (<https://www.cisa.gov/cybersecurity>)
- 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/USRelStand.aspx>)

System Integrators

- System integrators connected with Kepware System Integrator Program (<https://www.kepware.com/en-us/partners/system-integrators/>)

Host Operating System

Kepware software should always be deployed in the most secure environment possible. Ensure the host operating system (OS) is secure from the outset and take all feasible measures to maintain the security of the OS for the life of the system. Kepware software should be deployed in an environment that utilizes the principles of “defense in depth” as opposed to one that utilizes a perimeter-oriented security philosophy. Specific aspects of a secure OS include, but are not limited to, system security, user management, firewall settings, and file management.

System

Ensure appropriate access control measures are in place to limit physical access to the target hardware to appropriate users.

Always deploy on an actively supported version of Windows and install Windows security patches in accordance with ICS security best practices. As outlined by the ICS-CERT, **“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”**.

Encrypt the hard drive of the host machine to secure all data at rest. Also ensure that the product Application Data folder is encrypted. By default, Kepware Server stores Application Data in C:\ProgramData\ . Regularly scan the host system using respected anti-malware software with up-to-date and supported signature files.

Turn off any unused services on the host machine.

To reduce the attack surface, avoid co-hosting Kepware software with any other applications.

User Management

Create a Windows user separate from the Administrator account to configure and manage the software. Manage the Administrator account according to Windows best practices.

The Administrator user account password cannot be reset, but additional administrative users can be added to the Administrator user group. Best practices suggest each user with administrative access be

assigned unique accounts and passwords to ensure audit integrity and continual access through role and staff changes.

User passwords must adhere to a formal password policy appropriate to the specific domain.

Do not share logins or passwords across multiple users.

Store passwords securely.

Set a machine inactivity limit by enabling the screen saver and requiring users to login to resume use.

Periodically review the access control model to ensure permissions are set using the principle of least privilege (i.e. permissions are granted only to users who need to perform required functions and are revoked when no longer necessary).

Configure event log viewing permissions with least-privilege principals to differentiate administrative and configuration users.

Perimeter

- Utilize a firewall to minimize external footprint and review firewall settings periodically.
- Utilize an intrusion detection system (IDS).
- Monitor remote access to the host operating system and log the activities.

Non-Production Files

Regularly remove any backup files from the production system.

Regularly remove any sample or test files or scripts from the production system.

Installation

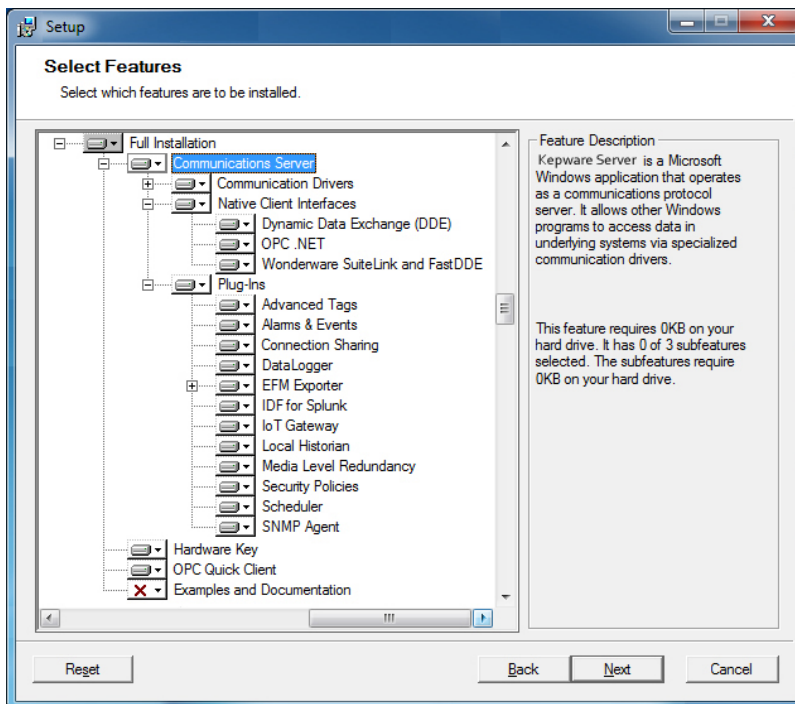
Users should validate the product installation files and only install the features required for the specific application. Set a strong administrator password during install.

Validation

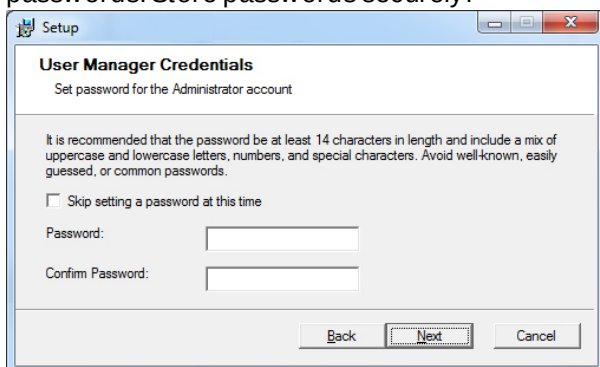
Kepware maintains unique identification codes for officially released software. Customers should verify against these codes to ensure that only certified executables are installed. Follow the instructions in article [CS278624](#) to validate the software (requires account login).

Installation

When presented with the Select Features dialog during the installation, install only the features required for the given production environment.



When presented with the User Manager Credentials dialog during the installation, set a strong administrator password. The password must be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid well known, easily guessed, or common passwords. Store passwords securely.



The Administrator user account password cannot be reset, but additional administrative users can be added to the Administrator user group. Best practices suggest each user with administrative access be assigned unique accounts and passwords to ensure audit integrity and continual access through role and staff changes.

Post- Installation

After the product has been installed, there are several actions that the product administrator should perform to maintain the highest level of security. This includes configuring permissions for Microsoft users, disabling any insecure interfaces that the user will not be using in the application, applying the appropriate permissions on the Application Data directory, and configuring user groups and users in a “least privilege” fashion. Finally, the administrator should log out or restart the computer to ensure user permissions are set correctly.

Application Data User Permissions

Configure the appropriate permissions on the product Application Data directory. This folder contains files critical to the proper functioning of the software, and permissions on this folder dictate which users are able to configure the product. By default, Kepware Server stores Application Data in `.\ProgramData\`. Using the Windows Security tab within the Properties of the Application Data folder, grant the appropriate user or user group **read** and **write** permissions on the Application Data folder. If you are editing permissions using the advanced window, apply the permissions to this folder, subfolders and files.

- Execute permission is not required to run Kepware Server.
- Only grant permissions to users or groups that require access to the application; do not grant permissions to all users.

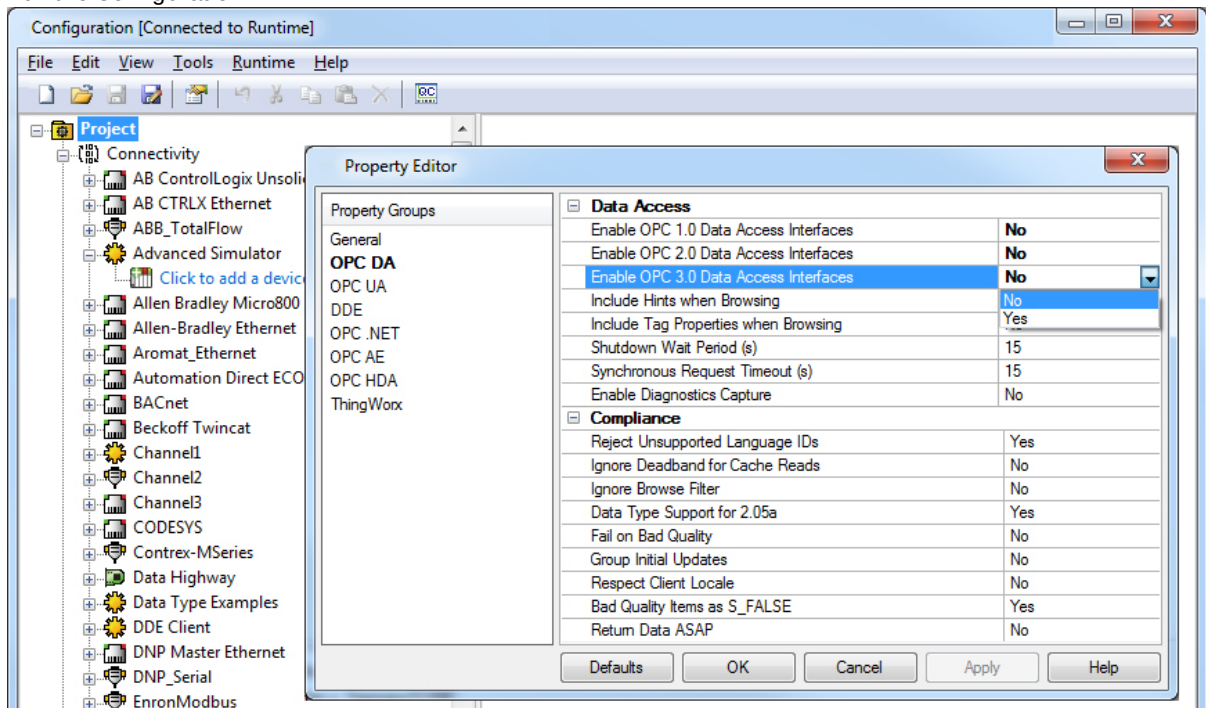
By default, the built in “Users” Windows group inherits read-only permissions on the Application Data Directory. Remove this inherited permission set unless all members of the Users group are trusted to configure Kepware Server.

Read and write permissions are required to open and change the configuration of the server.

Unsecure Interfaces

Disable the OPC DA Interface if not required for the specific application. OPC DA is a legacy protocol and is difficult to deploy with adequate levels of security. Where practical, users should utilize one of the secure protocols listed in this document.

1. Run the Configuration.



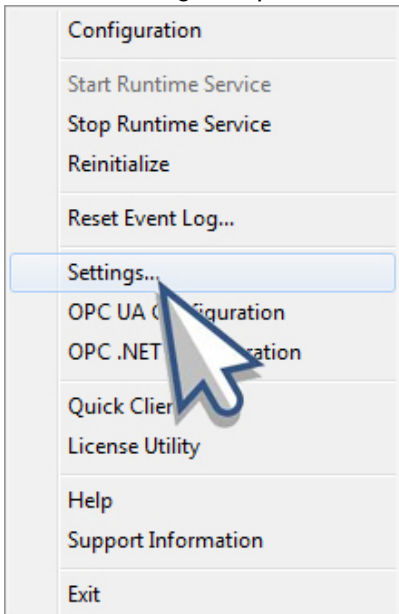
2. Right-click on Project and select **Project Properties**.
3. Select **OPC DA** Project Properties.
4. Disable OPC 1.0, 2.0, and 3.0 Data Access Interfaces by disabling the first three properties.

Repeat these steps any time a new project that does not require OPC DA connectivity is created.

Disabling the OPC DA interface will deny access to the built-in Quick Client tool used for testing connectivity. Utilize a third-party tool, such as [UA Expert](#), to test connectivity.

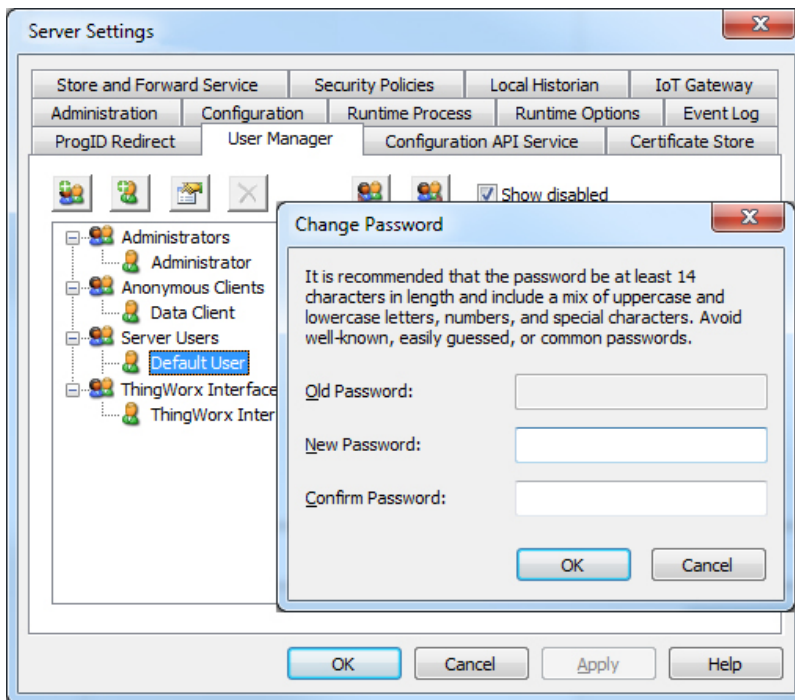
Server Users

Create a strong user password for the user Default User in the Server Users user group.



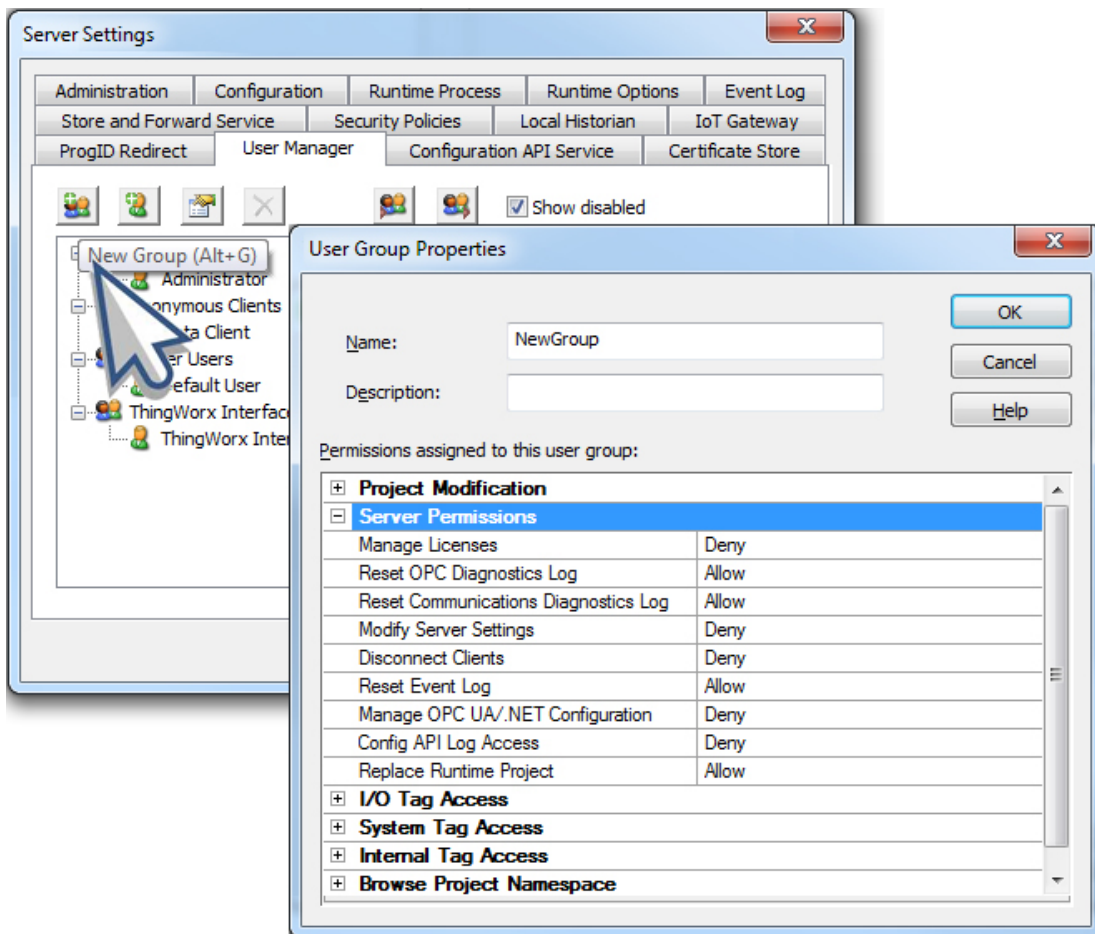
1. Open the Administrative Settings by right-clicking the product icon in the system tray and choosing **Settings**.
2. Select the **User Manager** tab.
3. The username and password required to access the **Settings** menu with the appropriate level of permissions in this instance will be the Administrator username and password.
4. Double-click on **Default User** under the Server Users group.
5. Set a strong password. The password must be at least 14 characters in length and include a mix of upper-case and lowercase letters, numbers, and special characters. Avoid well known, easily guessed, or common passwords. Store passwords securely.

Adjust permissions for the Default User according to the principles of least privilege (i.e. permissions are granted only to users who need to perform required functions and revoked when no longer necessary).

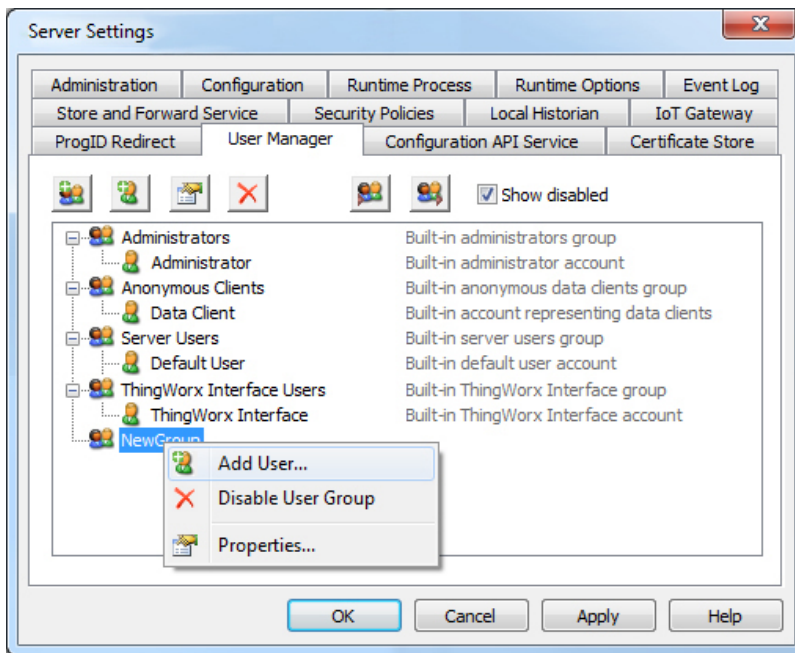


1. Open the Security Policies tab in Settings.
2. Expand Permissions assigned to Server Users and adjust permissions according to the principles of least privilege.

If configuring users requires varying levels of permissions, create additional server user groups as necessary and adjust the permissions according to the principles of least privilege.



1. Open the **User Manager** tab in Settings.
2. Click **New Group**.
3. Assign permissions to the newly created group according to the principles of least privilege.
4. Right-click on the new group.
5. Click **Add User**.
6. Set a strong password. The password must be at least 14 characters in length and include a mix of upper-case and lowercase letters, numbers, and special characters.



Avoid well known, easily guessed, or common passwords. Store passwords securely.

Do not share usernames or passwords across multiple users. Create a new user or a new group when users or groups need varying levels of permissions.

Secure Interfaces

Kepware Server is designed to communicate over protocols commonly used in industrial automation and the Industrial Internet of Things (IIOT). Certain protocols are more secure and have more options for security than others. OPC UA, MQTT, and REST are popular protocols that can be configured to use a high level of security. There are other protocols that can also be configured securely (SNMP, ThingWorx Native Interface, and others).

Refer to the user manual for more information on other secure protocols.

When using the UNC paths, ensure the path is a trusted and secure location.

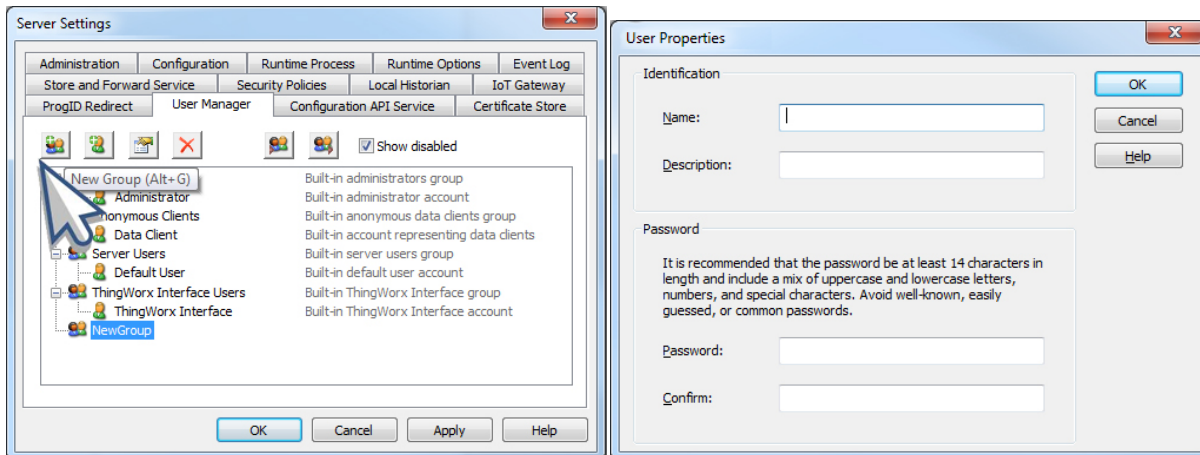
Some protocols are adding certificate authentication for secure communications. For those Kepware drivers where it is available, certificates are managed through the Administration.

OPC UA Server

Create a server user group for the specific purpose of using the OPC UA interface and adjust the permissions for that group according to the principle of least privilege.

1. Open the **User Manager** in Settings.
2. Click **New Group**.
3. Assign permissions to the new group according to the principles of least privilege.
4. Right-click on the new group.
5. Click **Add User**.

- Set a strong password. The password must be at least 14 characters in length and include a mix of upper-case and lowercase letters, numbers, and special characters.

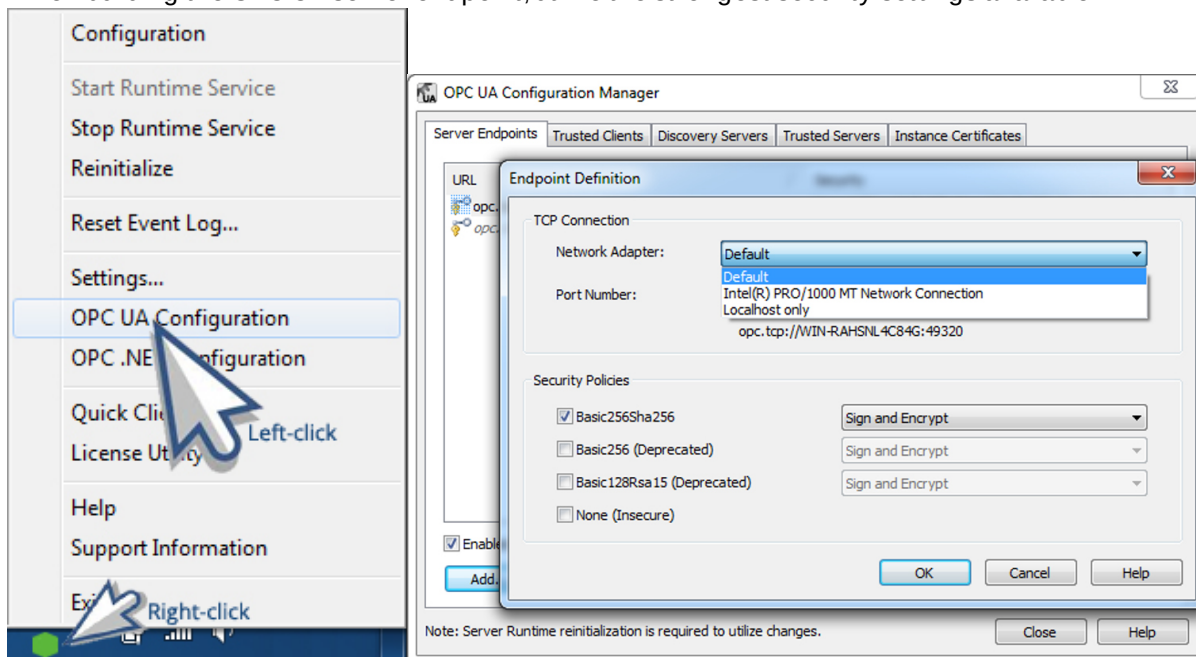


Avoid well known, easily guessed, or common passwords. Store passwords securely.

Do not share usernames or passwords across multiple users. Create a new user or a new group when users or groups need varying levels of permissions.

UA Anonymous logins are disabled by default. It is recommended to never permit anonymous UA client access.

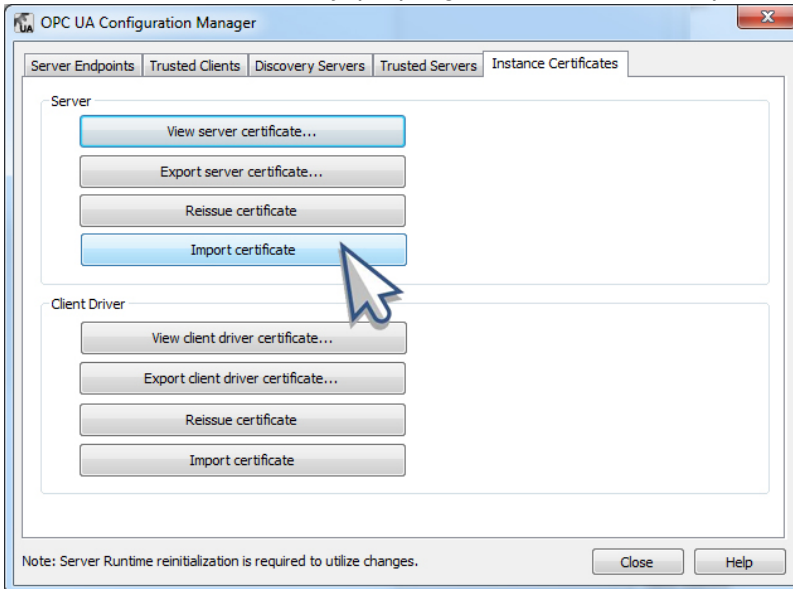
When building the OPC UA server endpoint, utilize the strongest security settings available.



- Open the OPC UA Configuration Manager by right-clicking the product icon in the system tray and choosing **OPC UA Configuration**.
- Click on the **Server Endpoints** tab.
- Click the **Add..** button to define a new endpoint.

4. For the most secure connection, ensure the network adapter used is accessible only from the network that is running the OPC UA Client.
5. Ensure the most up-to-date security policy options are checked. Less secure policies that have been deprecated will be clearly labeled.
6. Click **OK**.

Utilize a Certificate Authority (CA)-signed certificate when possible.



In the Instance Certificates tab of the OPC UA Configuration Manager, click **Import Certificate** and import a certificate signed by a CA.

Avoid importing certificates using a signature algorithm that is SHA1 or less secure.

Kepware Server is pre-loaded with a self-signed certificate. This certificate should be used for testing and proof-of-concepts only, and should not be used in production. In Version 6.7 and higher, this self-signed certificate is valid for three (3) years.

OPC UA Gateway

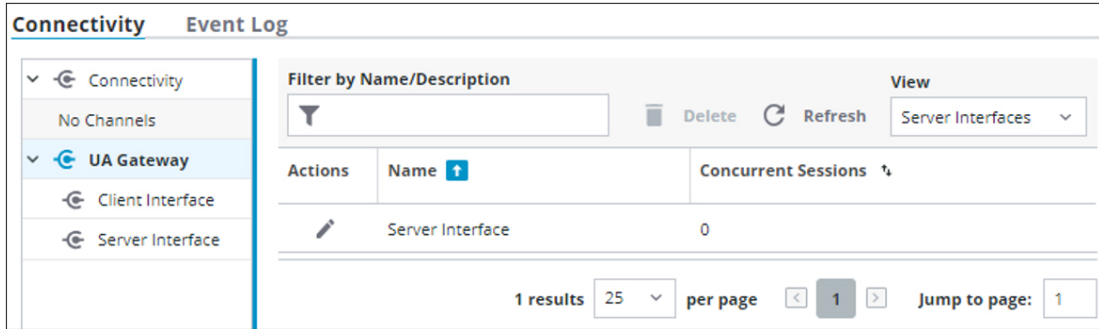
This section is only relevant for customers using Kepware Server, Kepware+, and OPC UA on devices in their environment.

UA Gateway Server Interface

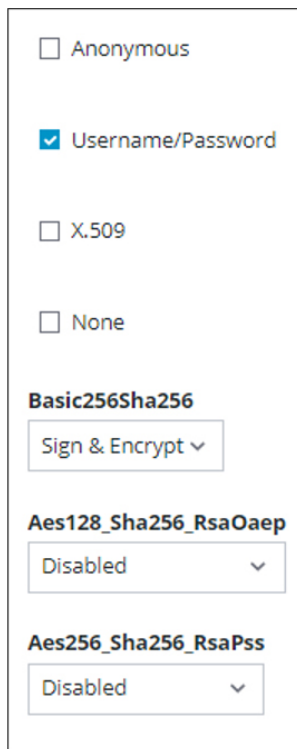
The UA Gateway has its own UA server Interface, separate from Kepware Server. This interface provides access to the aggregated devices connected via the UA Gateway client interface. By default, the UA Gateway does not expose the data collected by Kepware Server. The principle of Least Privilege should be applied; in all cases, utilize the strongest security settings available.

1. Access the Kepware+ user interface.
2. In the navigation tree, choose the **UA Gateway** node.
3. Select the Server Interface node. This populates the detail pane.

- Click the  (Edit) icon for Server Interface.



- In the Server Interface Property Editor, configure the security policies that apply to UA clients for successful connection to the UA Gateway.
- Select the appropriate authorization mechanism. **Anonymous** and **None** should not be used in production environments. For **Username/ Password**, create a Kepware Server user group for the specific purpose of using the OPC UA Gateway server interface and adjust the permissions for that group according to the principle of least privilege. The process of creating a new user group is described above.



- Select the message security policy to be used with the connected client(s). Use a policy which verifies the client using signing and encrypts the message.

Only connections from trusted UA Clients should be permitted access via the **Certificates View** of the **Server Interface** connectivity page. By default, new clients connecting to the UA Gateway are not trusted.

Connectivity		Event Log	
<ul style="list-style-type: none"> Connectivity No Channels UA Gateway Client Interface Server Interface 	<div> <div>+ New Server Endpoint</div> <div>Delete</div> <div>Refresh</div> <div>View Certificates</div> </div>		
	Actions	Trust Status	Application Name
			Valid To
			Thumbprint
		Trusted	UaExpert
			2027-11-01T13:45:00.000
			822addc35c2b559f8fddc9a5b58ca0a1b3e03f82

8. Select the new endpoint in the Detail pane.
9. From the View drop-down menu, select Certificates.
10. Click the (Edit) icon for the certificate.
11. From the Certificate Property Editor, examine the properties of the certificate to determine if the client should be trusted.
12. On determining a UA Client is authorized for access, change the Trust Status from Rejected to Trusted.

Trust Status

Trusted

Rejected

Trusted

MACKENZIEOL1A (822ADD)

Issuer

L = Portland

O = PTC

OU = Engineering

CN = UaExpert@PMACKENZIEOL1A

Subject

L = Portland

O = PTC

OU = Engineering

CN = UaExpert@PMACKENZIEOL1A

Application Name

UaExpert

URI

urn:PMACKENZIEOL1:UnifiedAutomation

UA Gateway Client Interface Connections

Connectivity to OPC UA devices is accomplished through the Client Connections view of the UA Gateway Client Interface.

1. Click the **New Client Connection** button.

Filter by Name/Description

+ New Client Connection

Delete

Refresh

Client Connections

View

0 Rows Selected

Actions

Name

URL Name

Status

Description

Identity Policy
 Username/Password ▾

User Name
 device82

User Password

Security Policy
 AES128_Sha256_RsaOaep ▾

Message Mode
 Sign & Encrypt ▾

2. Select **Username/ Password** as the Identity Policy.
3. Provide the User Name and User Password.
4. Select the **Security Policy** associated with the device. To allow connectivity to a broad range of devices, the UA Gateway supports Basic256 and Basic128Rsa15; however, these are not advisable in a production environment.
5. Select the **Message Mode** to be used with the device. Use a policy that verifies the identity of the device using signing and encrypts the message.

Only connections with trusted OPC UA devices should be permitted access via the Certificates View of the Client Interface connectivity page.

1. From the Connectivity node, choose **Client Interface**.
2. From the View drop-down menu, select **Certificates**.
3. Click the  (Edit) icon for the certificate.
4. From the Certificate Property Editor, examine the properties of the certificate to determine if the OPC UA device should be trusted.
5. On determining that the OPC UA device is authorized for access, change the **Trust Status** from **Rejected** to **Trusted**.

MQTT

When configuring the MQTT broker for Kepware connection; set a strong, unique username and password (uppercase and lowercase letters, numbers, and special characters), utilize strong and modern encryption, and utilize a Certificate Authority (CA)- signed certificate when possible.

Configuring these items depends on the specific broker utilized.

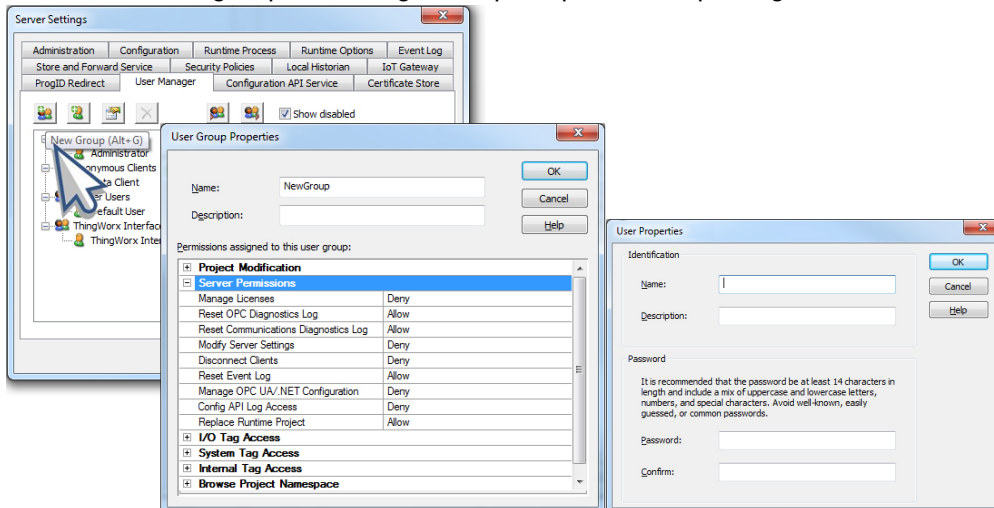
REST Client

When configuring the REST server for Kepware connections; set a strong, unique username and password (uppercase and lowercase letters, numbers, and special characters), utilize strong and modern encryption, and utilize a Certificate Authority (CA)- signed certificate when possible.

- Configuring these items depends on the specific server utilized.
- Authenticating with the appropriate certificate may require installing the certificate in the OS of the system running the software (see the [IoT Gateway Manual](#) for information).

REST Server

Create a server user group for the specific purpose of using REST Server agent, and adjust the permissions for that group according to the principle of least privilege.



1. Open the User Manager in Settings (accessible by right-clicking the product icon in the system tray).
2. Click **New Group**.
3. Assign permissions to the newly created group according to the principles of least privilege.
4. Right-click on the new group and choose **Add User...**
5. Set a strong password.

The password must be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters.

Avoid well known, easily guessed, or common passwords. Store passwords securely.

Do not share usernames or passwords across multiple users. Create a new user or a new group when users or groups need varying levels of permissions.

When configuring the REST server in the software, utilize strong encryption (HTTPS).

When configuring a REST Server endpoint, ensure the **Use HTTPS** property is enabled.

Use HTTPS will cause the REST Server to send data unencrypted in plain text.

It is recommended to populate CORS (Cross Origin Resource Sharing) settings with specific allow-listed domains; do not use the option of an asterisk to accept all.

When configuring a REST Server endpoint, input allow-listed domains into the **CORS Allowed Origins** property.

MQTT Client SSL/ TLS Hostname Verification

The IoT Gateway MQTT Client uses SSL/ TLS hostname verification to help ensure that the MQTT broker hostname matches the hostname identified in the broker certificate. This protection is enabled by default for new MQTT configurations.

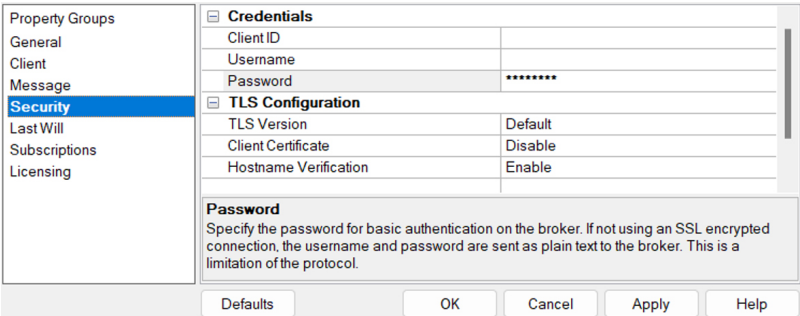
When configuring a new secure MQTT connection, use a broker hostname that matches a valid DNS name or IP address listed in the broker certificate Subject Alternative Name (SAN) field. Verify that the certificate is trusted and has not expired.

Connections may fail when using self- signed certificates, IP addresses without a matching IP SAN, or certificates whose hostname does not match the configured broker address. Correct the broker address or certificate configuration to establish a valid match.

Existing IoT Gateway projects retain hostname verification disabled after upgrade to preserve backward compatibility. No customer action is required for existing projects. Administrators should validate existing certificates and enable hostname verification when practical.

• The Paho MQTT Client upgrade also addresses a TLS hostname- verification security vulnerability.

• Refer to the applicable [Article - CS480493 - IoT Gateway's MQTT Agent Fails After Upgrade Because the IoT Gateway Host Entry Is Missing from settings.ini in Kepware Edge for PTC Kepware Products](#) for troubleshooting details and compatibility guidance (login required). [Article - CS480379 - PAHO MQTT Client Upgrade Introduces SSL/ TLS Hostname Verification For IoT Gateway in PTC Kepware Products](#) (login required).



Property Groups	
General	
Client	
Message	
Security	
Last Will	
Subscriptions	
Licensing	

Credentials	
Client ID	
Username	
Password	*****

TLS Configuration	
TLS Version	Default
Client Certificate	Disable
Hostname Verification	Enable

Password
Specify the password for basic authentication on the broker. If not using an SSL encrypted connection, the username and password are sent as plain text to the broker. This is a limitation of the protocol.

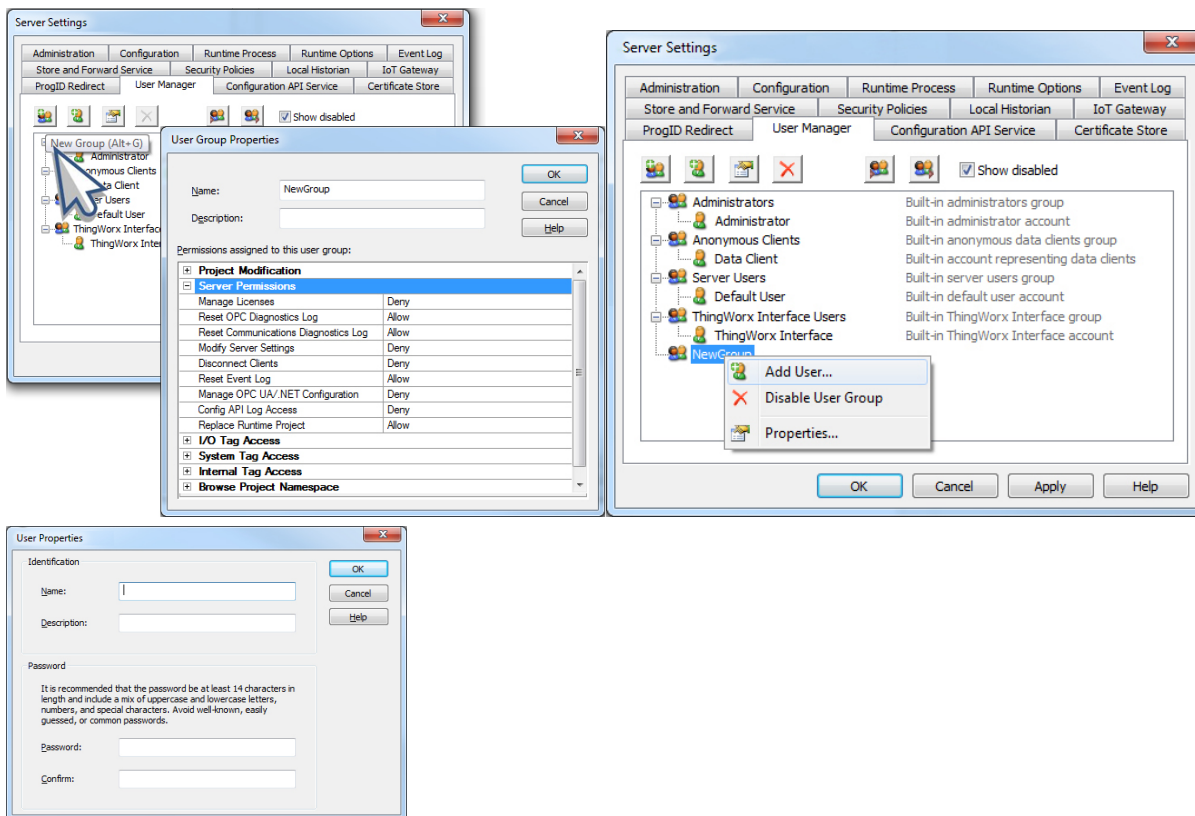
Defaults OK Cancel Apply Help

Configuration API

The Configuration API allows users to programmatically configure certain drivers and plug- ins. It allows users with many instances of Kepware Servers or constantly changing products to seamlessly update their configurations. It is important to utilize this feature using the highest level of security possible.

Configuration API

Create a server user group for the specific purpose of using the Configuration API and adjust the permissions for that group according to the principle of least privilege.



1. Open the User Manager in Settings (accessible by right-clicking product icon in the system tray).
2. Click **New Group**.
3. Assign permissions to the newly created group according to the principles of least privilege.
4. Right-click on the new group and choose **Add User...**
5. Set a strong password.

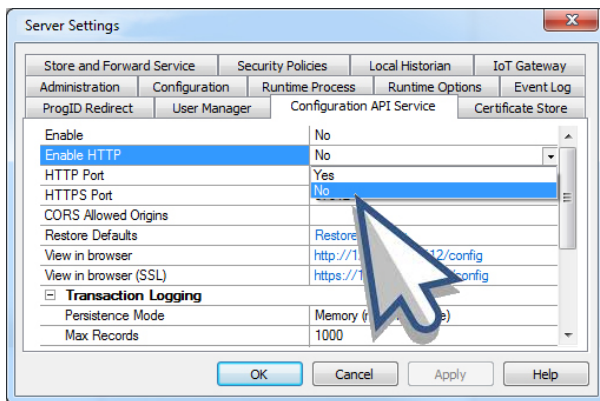
The password must be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters.

Avoid well known, easily guessed, or common passwords. Store passwords securely.

Do not share usernames or passwords across multiple users. Create a new user or a new group when users or groups need varying levels of permissions.

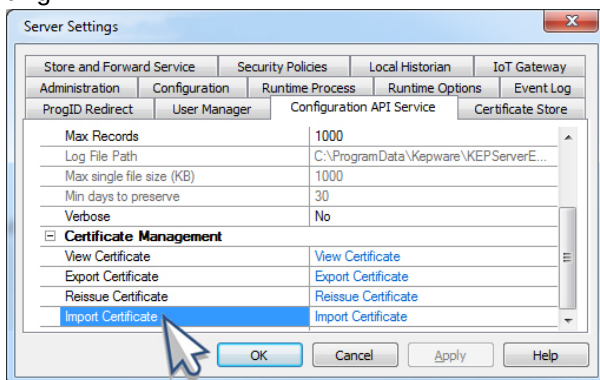
It is strongly recommended to only use HTTPS in both production and testing. HTTPS must be used for production.

1. Open the Configuration API Service Settings in Settings (right-click the product icon in the system tray).
2. Disable HTTP.



Utilize a Certificate Authority (CA)- signed certificate when possible.

In the Configuration API Service Settings, click **Import Certificate..** and import a certificate signed by a CA. In the Configuration API Service Settings, input allow- listed domains into the **CORS allowed origins** setting.



It is recommended to populate CORS (Cross Origin Domain Sharing) settings with allow- listed domains.

Do NOT use the option of an asterisk to accept all.

Monitor transaction logs and server event log as long as the Configuration API is in use.

The endpoint for the event log is /config/v1/event_log and can be retrieved by issuing a “get” to that endpoint.

Sanitize data both sent and received by the Configuration API.

Ensure that invalid scripting characters and other malicious inputs are not being passed to the server from clients.

As a best practice, clear the browser cache after each session of Configuration API interaction.

Ongoing Maintenance

It is important to constantly evaluate and maintain the security of the system and the server when deployed in a production environment. This includes, but is not limited to, upgrading to the latest version as soon as possible, monitoring external dependencies, and following security best practices throughout the lifecycle of the system and in the environment.

Upgrades

It is critical that users, especially users deploying this software in safety - critical environments, upgrade to the latest version as soon as possible to take advantage of security enhancements.

It is important to be able to quickly validate newer versions of the software before deploying in a production environment.

Users should have a plan in place to quickly validate and implement new versions without any impact to operations. The ICS CERT recommends that “system administrators should test all patches off-line in a test environment that contains the same model and type of ICS to determine whether the patch has unintended consequences.”

Automating these tests can expedite this process.

Diagnostics

Only utilize the various diagnostics features throughout the product when necessary and turn off diagnostic modes when not in use.

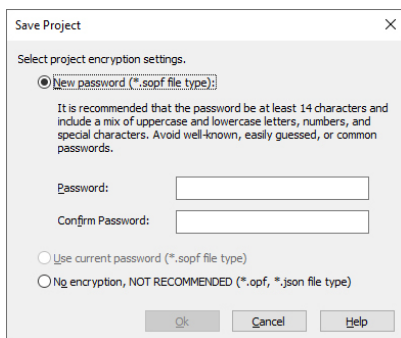
External Dependencies

Monitor all external dependencies and upgrade to the latest version as soon as possible.

Project File Security

When saving a project, utilize all available security mechanisms.

1. Open the Configuration.
2. Click **File | Save As**.
3. Choose the **New Password** option in the Save Project dialog.
4. Set a strong password to protect .sopf project files. The password must be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid well-known, easily guessed, or common passwords. Store passwords securely. Project files saved as JSON are human readable and editable. End users should exercise caution when using this format.



Documentation

It is recommended to document all configuration, administrative, or runtime changes made to the server, as well as all systems that interact with the server.

This enables roll-back to a previous system state as well as the ability to replicate any given configuration should it become necessary.

Regularly review the system configuration as compared to this guide and verify deviations are part of a conscious choice that does not compromise security.

Next Steps

1. Access additional information in the [user manual](#).
2. Access [Kepware's guides](#) for information on getting started with product features.
3. Email sales@kepware.com to schedule an in- depth demonstration and to learn how to use the server in your specific environment.