Guide

Secure ThingWorx Kepware Server Deployment

August 2021
Ref. 1.012

Table of Contents

1. Introduction

ThingWorx® 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 of ThingWorx Kepware Server deploy the application as securely as possible. This document guides users through the process of deploying the server with maximum security. It is recommended that administrators follow this guide as closely as possible when deploying the server in a production environment.

Kepware/PTC recommends new users utilize this guide for new production installs of ThingWorx Kepware Server whenever practical. Kepware/PTC also recommends existing users of the software compare existing configurations with the recommendations provided in this guide and adjust for best practices.

2. 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.

ThingWorx 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.

2.1 Resources on ICS Network Security

- 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 System Integrators

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

3. Host Operating System

ThingWorx Kepware Server 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. ThingWorx Kepware Server 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.

3.1 System

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

Always deploy ThingWorx Kepware Server 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. Additionally, ensure that the ThingWorx Kepware Server Application Data folder is encrypted. By default, the server stores application data in C:\ProgramData\ThingWorx Kepware Server.

Regularly scan the host system using respected anti-malware software with up-to-date signature files.

Turn off any unused services on the host machine.

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

3.2 User Management

Create a Windows user separate from the Administrator account to configure, manage, and run ThingWorx Kepware Server. Manage the Administrator account according to Windows best practices.

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).

3.3 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.

3.4 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.

4. Installation

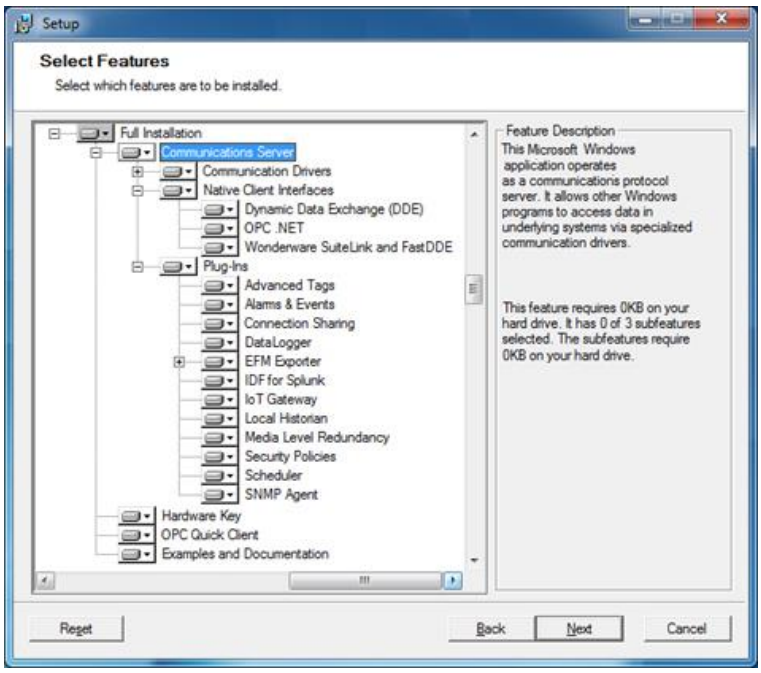
Users should validate the ThingWorx Kepware Server install and only install the features required for the specific application. Set a strong administrator password during install.

4.1 Validation

4.1.1 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 to validate the software at: https://www.kepware.com/digitalsignature.

4.2 Installation

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



4.2.2 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.

5. Post-Installation

After the product has been installed, there are several actions that the ThingWorx Kepware Server 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 his or her 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.

5.1 Application Data User Permissions

5.1.1 Configure the appropriate permissions on the ThingWorx Kepware Server Application Data directory. This folder contains files critical to the proper functioning of ThingWorx Kepware Server, and permissions on this folder dictate which users are able to configure the product. By default, ThingWorx Kepware Server stores Application Data in 'C:\ProgramData\Kepware'.

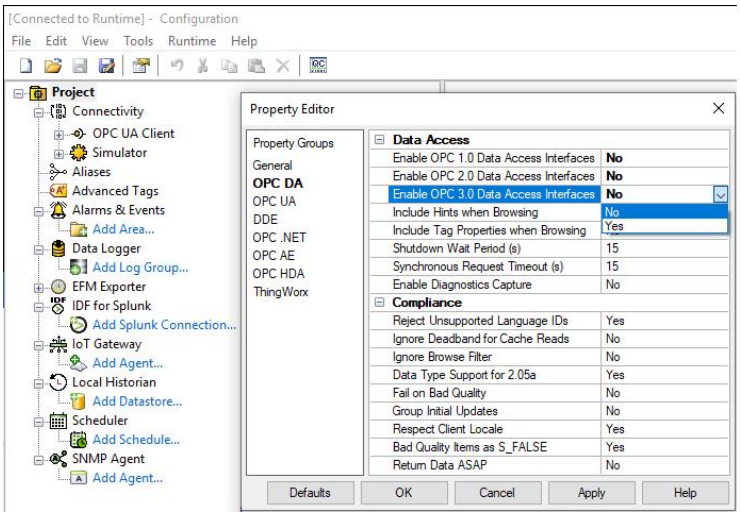
1. Using the Windows Security tab within the Properties of the Application Data folder, grant the appropriate user or user group **read** and **write** permissions on the Application Data folder. If you are editing permissions using the advanced window, apply the permissions to this folder, subfolders and files.
   - The execute permission is not required to run ThingWorx Kepware Server.
   - Only grant permissions to users or groups that require access to the application; do not grant permissions to all users.
2. 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 ThingWorx Kepware Server.

Both read and write permissions are required to open and change the configuration of ThingWorx Kepware Server.

5.2 Unsecure Interfaces

5.2.1 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 ThingWorx Kepware Server Configuration.
2. Right-click on Project and select **Project Properties**.



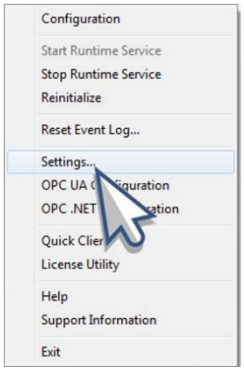
3. Select **OPC DA** Project Properties.
4. Disable OPC 1.0, 2.0, and 3.0 Data Access Interfaces by disabling the first three properties.

5.2.2 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.

5.3 Server Users

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

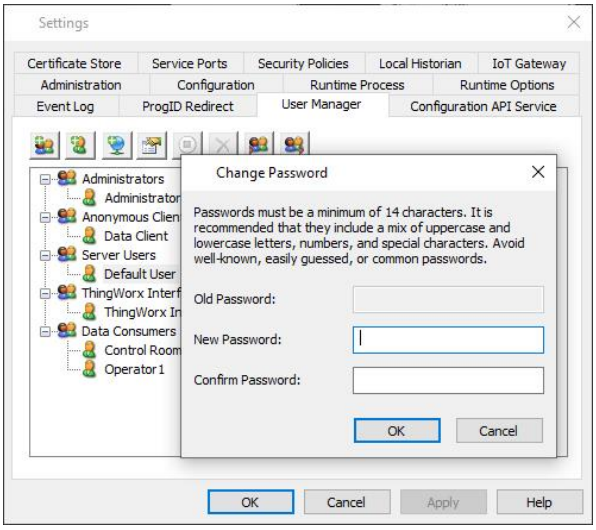


1. Open the Administrative Settings by right-clicking the ThingWorx Kepware Server icon in the system tray and choosing **Settings**.
2. Select the **User Manager** tab.

- 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.

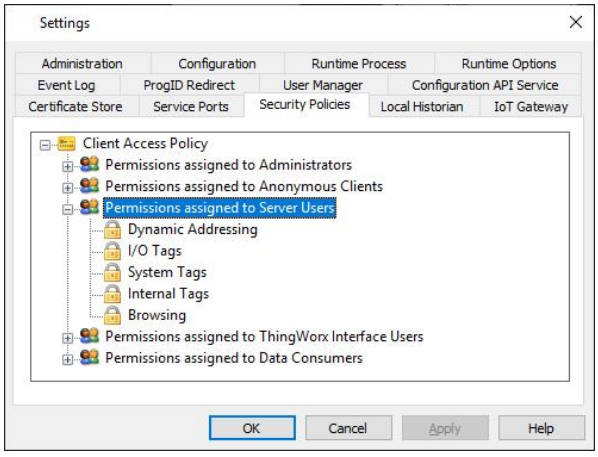
3. Double-click on **Default User** under the Server Users group.
4. Set a strong password. The password must be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid well known, easily guessed, or common passwords. Store passwords securely.

5.3.2 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).



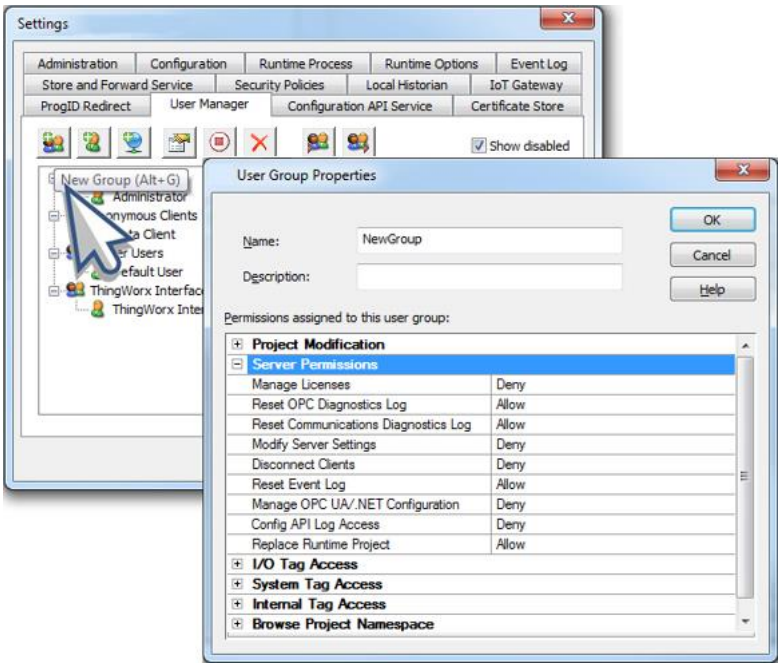
1. Open the **Security Policies** tab in ThingWorx Kepware Server Settings.
2. Expand Permissions assigned to Server Users and adjust permissions according to the principles of least privilege.

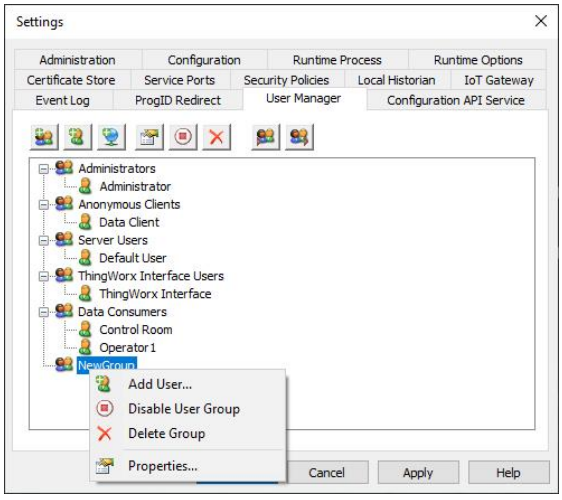
5.3.3 If configuring users of ThingWorx Kepware Server requires varying levels of permissions, create additional server user groups as necessary and adjust the permissions according to the principles of least privilege.



- When adding Active Directory users or groups, do not select any local users or groups that could allow unintended access to any user on the device, such as the 'Everyone' group.

1. Open the **User Manager** tab in ThingWorx Kepware Server 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 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.

6. Secure Interfaces

ThingWorx 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 ThingWorx Kepware Server manual for more information on other secure protocols.*

6.1 OPC UA

6.1.1 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.

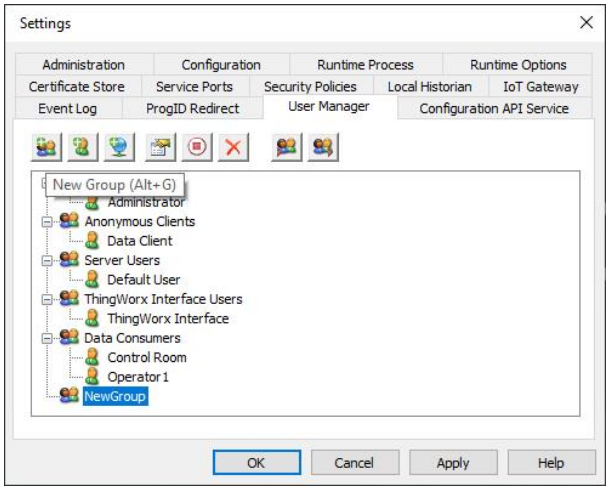
1. Open the User Manager in the server Settings.
2. Click **New Group**.

3. Assign permissions to the new group according to the principles of least privilege.

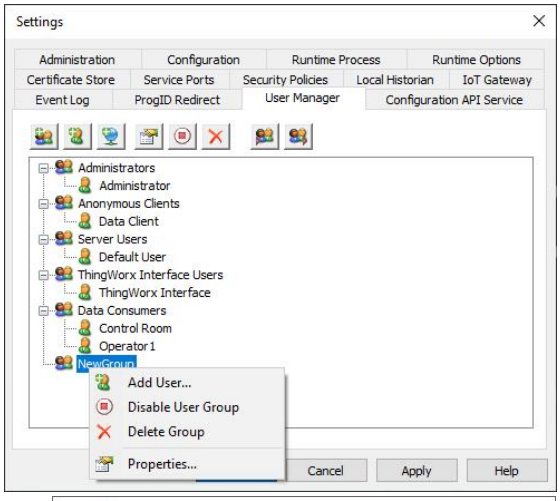
4. Right-click on the new group.

5. Click **Add User**.

6. 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.
- UA Anonymous logins are disabled by default. It is recommended to never permit anonymous UA client access.

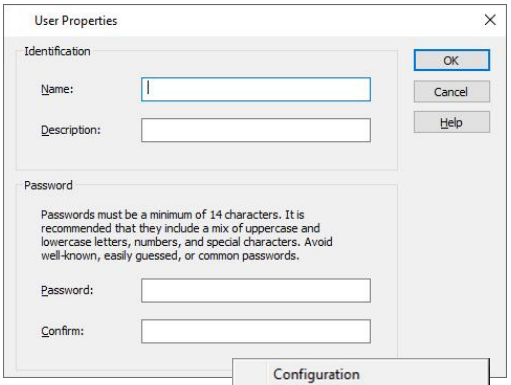


6.1.2 When building the OPC UA server endpoint, utilize the strongest security settings currently available.

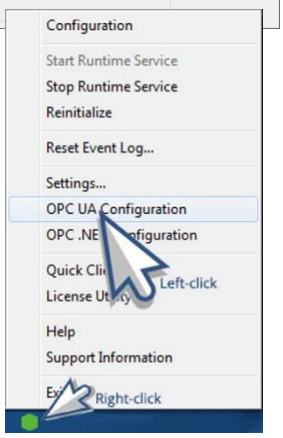
1. Open the OPC UA Configuration Manager by right-clicking the server icon in the system tray and choosing **OPC UA Configuration**.

2. Click on the **Server Endpoints** tab.

3. 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.

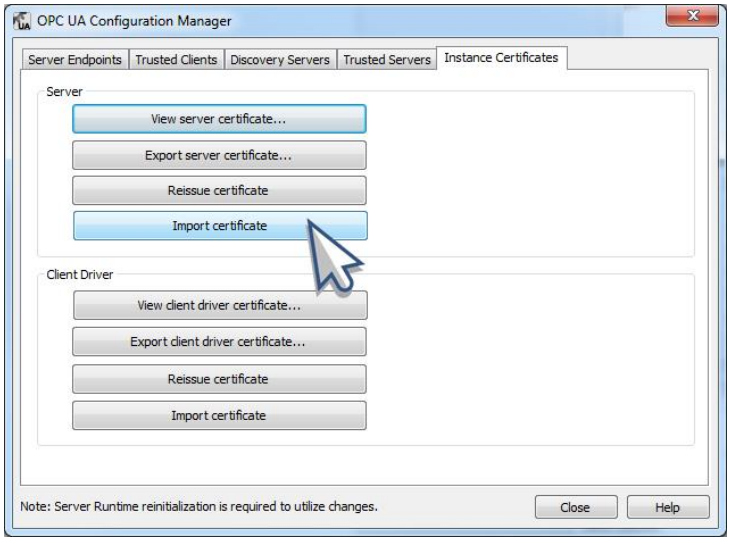


5. Ensure the most up-to-date security policy options are checked. Less secure policies that have been deprecated will be clearly labeled.

6. Click **OK**.

6.1.3 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.

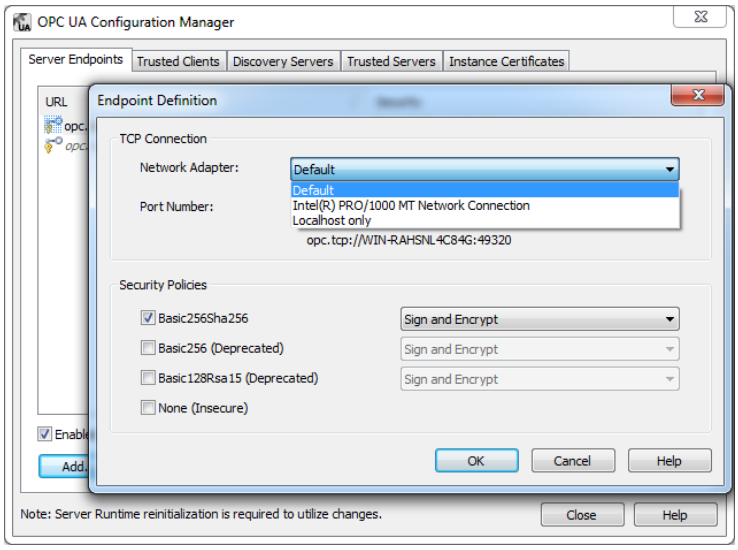


- Avoid importing certificates using a signature algorithm that is SHA1 or less secure.
- ThingWorx Kepware Server is pre-loaded with a self-signed certificate. This certificate should be used for testing and proof-of-concepts only; not in production. In ThingWorx Kepware Server Version 6.7 and higher, this self-signed certificate is valid for 3 years.

6.2 MQTT

6.2.1 When configuring the MQTT broker that ThingWorx Kepware Server will connect to, 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.



6.3 REST Client

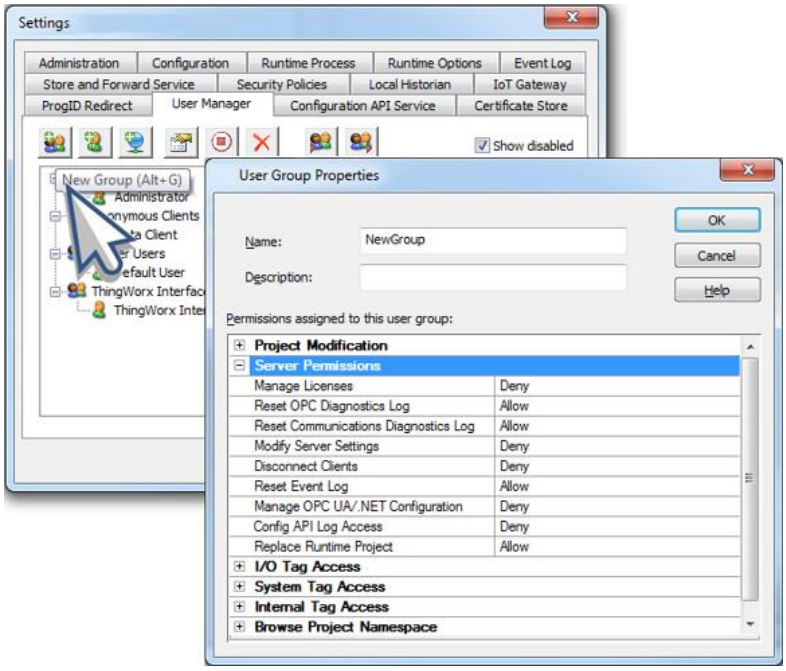
6.3.1 When configuring the REST Server that ThingWorx Kepware Server will connect to, set a strong, unique username and password (uppercase and lowercase letters, numbers, and special characters), utilize strong and modern encryption, and utilize a Certificate Authority (CA)-signed certificate when possible.

- Configuring these items will depend on the specific server utilized.
- Authenticating with the appropriate certificate may require installing the certificate in the OS of the system running the server *(see the IoT Gateway Manual for information)*.

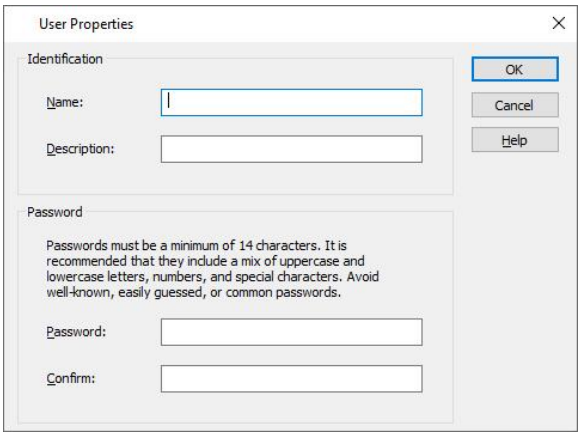
6.4 REST Server

6.4.1 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 ThingWorx Kepware Server Settings (accessible by right-clicking the ThingWorx Kepware Server 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....**



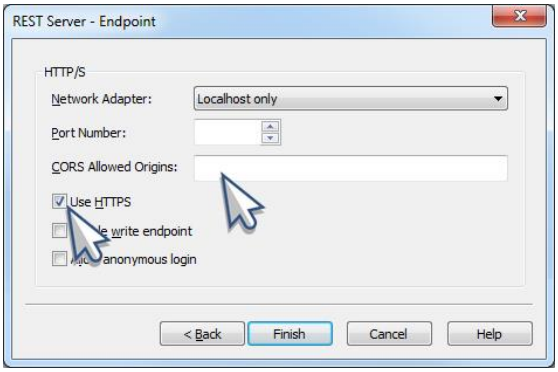
5. Set a strong password.



- 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.

6.4.2 When configuring the REST Server in ThingWorx Kepware Server, 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.



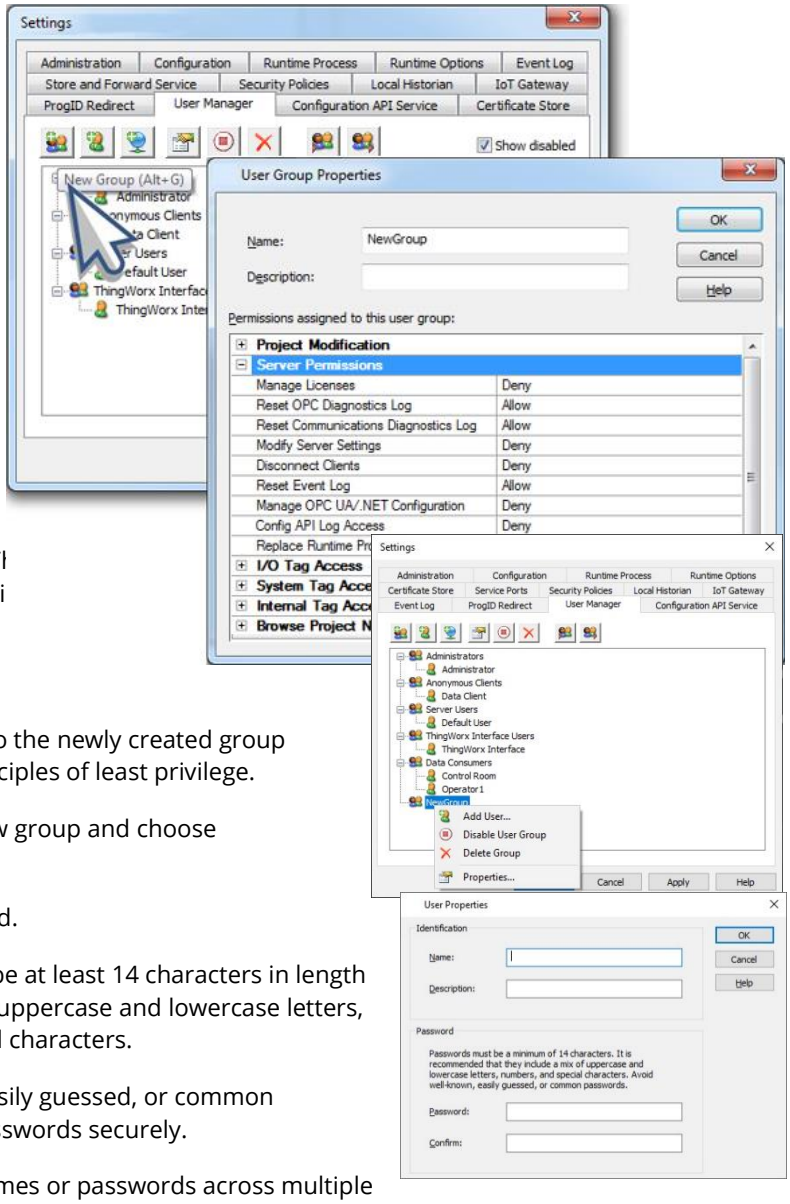
It is recommended to populate CORS (Cross Origin Resource Sharing) settings with specific allow-listed domains; do not use the option of an asterisk to accept all.

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

7. Configuration API

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

7.1 Configuration API



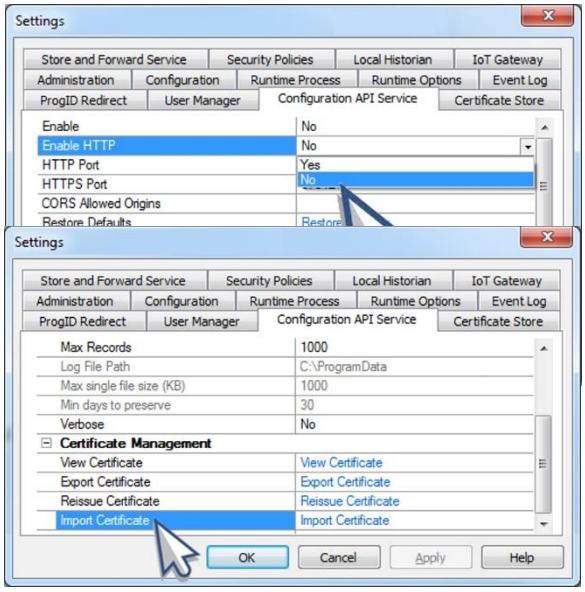
7.1.1 Create a server user group for the specific purpose of using the Configuration API and adjust the permissions for that group according to the principle of least privilege.

1. Open the User Manager in ThingWorx Kepware Server Settings (accessible by right-clicking the TI Kepware Server icon i 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.

7.1.2 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 ThingWorx Kepware Server Settings (accessible by right-clicking the ThingWorx Kepware Server icon in the system tray).
2. Disable HTTP.



7.1.3 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.

7.1.4 Sanitize data that is sent and received by the Configuration API

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

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

8. Ongoing Maintenance

It is important to constantly evaluate and maintain the security of the system and of ThingWorx Kepware Server when deployed in a production environment. This includes, but is not limited to, upgrading ThingWorx Kepware Server 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.

8.1 ThingWorx Kepware Server Upgrades

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

8.1.2 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.

8.2 Diagnostics

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

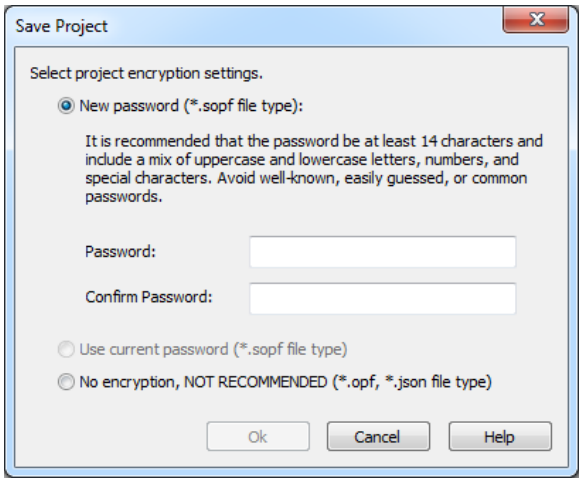
8.3 External Dependencies

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

8.4 Project File Security

8.4.1 When saving a project, utilize all available security mechanisms.

1. Open the ThingWorx Kepware Server 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.



8.5 Documentation

8.5.1 It is recommended to document all configuration, administrative, or runtime changes made to ThingWorx Kepware Server, as well as all systems that interact with ThingWorx Kepware Server.

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

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

9. Next Steps

1. Access additional information in the ThingWorx Kepware Server product manual.
2. Access Kepware's guides for information on getting started with ThingWorx Kepware Server features.
3. Email sales@kepware.com to schedule an in-depth demonstration and to learn how to use ThingWorx Kepware Server in the specific environment.

