Technical Note

Migrate to Kepware Server 7.0 from KEPServerEX 6 or ThingWorx Kepware Server 6

Kepware / PTC is re-branding KEPServerEX (KSE) and ThingWorx Kepware Server (TKS) to provide all users with a unified and optimized experience. This deprecates both products and replace them with single product, Kepware Server. All users are strongly encouraged to upgrade to the new product.

- *For detailed release notes, please visit: www.ptc.com/en/products/kepware.*

Automation has been added to assist users in upgrading to Kepware Server.

Follow the steps below to upgrade TKS (Versions 6.17-6.18) or KSE (Versions 6.17-6.18) to Kepware Server (7.0). If you are on a lower version, upgrade to version 6.17 or 6.18 before migration.

Get Started

- **Notes**:
  - TKS / KSE and Kepware Server cannot be installed on the same machine at the same time. You MUST follow these instructions to migrate from the prior product to the new product.
  - Valid active licenses for TKS / KSE continue to function with Kepware Server once migration is complete.
  - Invalid licenses or lapsed maintenance must be resolved to upgrade.
  - Project files and most data files can be automatically migrated. TKS / KSE projects are compatible with Kepware Server. (However, we suggest creating a backup of the project in case problems arise. Please see the tables below for details on what is and is not migrated.)
- **Tip**: If using a hardware key, the required certificate file can be re-downloaded at from MyKepware using the ID found on the physical key. The file must be re-imported after the upgrade is complete for licensing to function.

Collect an Application Report

- This step is optional, but recommended.

Use the Application Report Utility to collect a backup of the server configuration and associated settings and logs. This report is a useful reference to diagnose any issues that may arise during the upgrade and migration process.

- *Follow the steps in Generating an Application Report*

Export Certificates (if Applicable)

- This step is optional.

Imported instance certificates and external certificates in trust stores are not migrated. If these certificates are not accessible outside the TKS / KSE instance, export them prior to uninstalling so they can be imported into Kepware Server *(see the Certificates section below for further information)*.

Backup the Current Project

1. Open the existing software by double-clicking the desktop icon or selecting **Configuration** from the System Tray.
2. Select **File | Save As**.
3. Follow the prompts to save the current project to a local directory.

- For security, set a strong password.

Export User Data

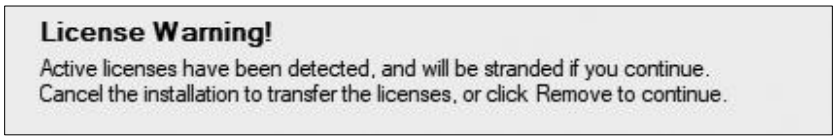
1. Navigate to **Settings** from the System Tray.
2. Select **User Manager** and **Export User Information** (Alt + E).
3. Follow the prompts to save the user data to a safe location.

- For security, set a strong password.

Uninstall TKS / KSE

- **Caution**: Running a prior version on the same system with Kepware Server is not supported. The previous version must be uninstalled prior to installing the update.
- **Caution**: Verify that the **Remove User Data** option is NOT selected. The option removes the current runtime project and custom server settings. This is de-selected by default.
- **Note**: If using a Windows workflow to uninstall (via Start menu, Settings, or Control Panel), user data is automatically preserved.

1. Right-click the **Start** menu and select **Apps and Features** (**Programs and Features** in Windows 7).
2. Locate and select TKS / KSE.
3. Click **Uninstall**.
4. If Kepware Server is being installed on the same computer, click **OK** on the active license warning pop-up.



5. Follow the prompts to completely uninstall the product.

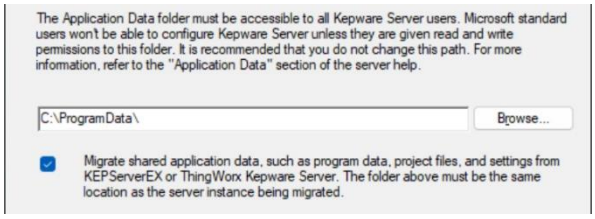
Download Kepware Server

Download the installer for Kepware Server Version 7.0 at MyKepware.com.

Install Kepware Server

- **Caution**: Ensure the Application Data folder is consistent with the path used during the previous installation of TKS / KSE. By default, this is C:\ProgramData\. If you choose a different location from the previous install, manually update the project file to the new location and copy the following files from the old TKS / KSE Application Data directory to the new Kepware Server Application Data directory:
  - default.opf
  - settings.ini
  - event.log
  - _EFM (folder)
  - Historical Data (folder)
  - ThingWorx (folder)
  - ua_gateway.json
  - IoT Gateway (folder)

1. Launch the Kepware Server installer wizard.
2. Follow the prompts, ensuring the migrate application data checkbox is selected during installation.



3. Launch Kepware Server Configuration.
4. Verify the project from the previous version is loaded (or locate and load).

Import User Data

1. Navigate to **Settings** from the System Tray.
2. Select the **User Manager** tab.
3. Select **Import User Information** (Alt + I).
4. Locate the exported user file.
5. Click **Open**.
6. Enter the correct password (if one is set, it is required to import the user data).
7. Verify the users and groups from the prior installation are present.

UA Gateway Considerations

None of the UA Gateway program data files from TKS are transferred to the new Kepware Server files.

If there are UA Gateway peer trust certificates you want to migrate to the new Kepware Server trust store, you must manually move them from the TKS program data store to the new Kepware Server program data store.

If you do not manually move the trust certificates, your UA clients and UA servers will prompt that the certificates are not trusted. Use the usual process of trusting UA certificates through the user interface.

Manually Migrate UA Trust Certificates

For the UA Gateway Server Interface Peer Trust certificates:

Old Path:

<program data path>\PTC\ThingWorx Kepware Server\V6\UA Gateway\Server Interface\pki\trusted

New Path:

<program data path>\PTC\Kepware Server\V7\UA Gateway\Server Interface\pki\trusted

For the UA Gateway Client Interface Peer Trust certificates:

Old Path:

<program data path>\PTC\ThingWorx Kepware Server\V6\UA Gateway\Client Interface\pki\trusted

New Path:

<program data path>\PTC\Kepware Server\V7\UA Gateway\Client Interface\pki\trusted

You also need to maintain any trusted user certificates for both interfaces.

For the UA Gateway Server Interface Trust User certificates:

Old Path:

<program data path>\PTC\ThingWorx Kepware Server\V6\UA Gateway\Server Interface\pki\trustedUser

New Path:

<program data path>\PTC\Kepware Server\V7\UA Gateway\Server Interface\pki\trustedUser

- **Notes**:
  - Any remaining files in the <program data path>\PTC\ThingWorx Kepware Server\V6\UA Gateway are stranded by the Kepware Server application.
  - If you would like to save the TKS files for archival purposes or delete the folder and its contents to save space, this must be done manually.

Re-establish Kepware Server Legacy UA Client Connections

If user data is not removed during the Kepware Server 7.0 installation, the OPC UA connection between the UA Gateway and the Legacy UA server will fail due to a "Bad User Access Denied" error. This is because the name of the client connection and user password are different for the new installation.

- *See "Default Connection to the OPC UA Server" in the server help file for documentation on how to set the correct password for the UA Gateway to the Legacy UA server.*

The client connection name must be modified as part of a PUT request:

"common.ALLTYPES_NAME": "Kepware Server",

The PUT request updates the client connection name and the user password.

- **Note**: Some drivers, such as OPC UA Client Driver and OPC DA Client Driver, or other utilities and connections, may need to be updated through the UA certificate trust process.

Certificates

To align with best security practices, Kepware Server uses certificates with 2048-bit public keys rather than the 1024-bit keys used in TKS / KSE. This change has varying impacts on different classes of certificates within Kepware Server.

Instance certificates generated by TKS / KSE cannot be migrated. Instead, these are automatically re-generated by Kepware Server. Clients using this class of certificates must trust the new certificates:

- OPC UA Server Interface Instance Certificate
- OPC UA Client Driver Instance Certificate
- IoT Gateway REST Server Instance Certificate

- ThingWorx Native Interface Instance Certificate
- Configuration API Service REST Server Instance Certificate
- IEC 61850 MMS Client Instance Certificate
- MQTT Client Driver Instance Certificate

Imported instance certificates are not migrated from TKS / KSE to Kepware Server and must be re-imported. This class of certificates includes:

- Imported OPC UA, IoT Gateway REST Server, ThingWorx Native Interface, Configuration API Service REST Server, IEC 61850 MMS Client, and MQTT Client Driver Instance Certificates (CA-Signed, Imported Self-Signed, etc.)
- IoT Gateway MQTT Agent Instance Certificate

Caution: It is strongly recommended to import 2048-bit certificates.

External certificates in trust stores are not migrated. These certificates must be manually imported into Kepware Server trust stores. If these certificates are not accessible outside TKS / KSE, it is recommended that they be exported from the trust stores before uninstalling.

Note: Trusted OPC UA client and server certificates may not need to be manually imported to Kepware Server *(see Re-Establishing Trust for OPC UA Connections)*.

The sections below detail the processes to import and export various certificates.

Importing / Exporting an External OPC UA Instance Certificate

1. Navigate to **OPC UA Configuration** in the System Tray.
2. Select **Instance Certificates**.
3. Select **Import certificate** or **Export [server/client driver] certificate** under "Server" for OPC UA Server Interface certificates or "Client Driver" for OPC UA Client Driver certificates.

Importing an IoT Gateway MQTT Agent Instance Certificate

1. Navigate to **Settings...** in the System Tray.
2. Select the **IoT Gateway** tab.
3. Select **Manage Certificate...** under "MQTT Agent".
4. Select **Import New Certificate**.

Note: IoT Gateway MQTT Agent Certificates cannot be exported.

Importing / Exporting IoT Gateway REST Server Instance Certificate

1. Navigate to **Settings...** in the System Tray.
2. Select the **IoT Gateway** tab.
3. Select **Manage Certificate...** under "REST Server".
4. Select **Import REST server certificate...** or **Export REST server certificate...**.

Importing / Exporting an MQTT Client Driver, ThingWorx Native Interface, and IEC 61850 MMS Client Driver Instance Certificate

1. Navigate to **Settings...** in the System Tray.
2. Select the **Certificate Store** tab.
3. Select the desired feature from the **Feature** drop-down menu.
4. Select **Export** or **Import** under “Instance Certificate”.

Importing / Exporting an MQTT Client Driver, Siemens S7 Plus Ethernet Driver, ThingWorx Native Interface, and IEC 61850 MMS Client Driver Trusted Certificate

1. Navigate to **Settings...** in the System Tray.
2. Select the **Certificate Store** tab.
3. Select the desired feature from the **Feature** drop-down menu.
4. Select **Export** or **Import** under “Manage Trust Store”.

Importing and Exporting a Configuration API Service Certificate

1. Navigate to **Settings...** in the System Tray.
2. Select the **Configuration API Service** tab.
3. Select **Import Certificate** or **Export Certificate** under “Certificate Management”.

Re-Establishing Trust for OPC UA Connections

Trust must be re-established for secure connections to the OPC UA Server Interface and OPC UA Client Driver. The certificates associated with Trusted Clients and Trusted Servers are not transferred from TKS / KSE to Kepware Server.

OPC UA Server Interface Connections

If the external client does not prompt certificate exchange with the OPC UA Server Interface, a certificate must be manually generated from the server and uploaded to the client. If the client automatically prompts certificate exchange, skip steps 2 and 3 below.

1. Navigate to **OPC UA Configuration** from the System Tray.
2. Select the **Instance Certificates** tab.
3. Select **Export server certificate** under “Server”.
4. Upload this certificate to the external OPC UA client.
5. Select the **Trusted Clients** tab.
6. Click on the name of the client to connect to and then select **Trust**.

OPC UA Client Driver Connections

If the OPC UA Client Driver does not automatically prompt certificate exchange with the external server, a certificate must be manually generated from the server and uploaded to Kepware Server. If the OPC UA Client Driver automatically prompts certificate exchange, skip steps 2 and 3 below.

1. Navigate to **OPC UA Configuration** from the System Tray.
2. Select the **Trusted Servers** tab.
3. Select **Import** and upload the server certificate.
4. If the server has a red X, click on the name of the server to connect and select **Trust**.

OPC UA Namespace Changes

The Namespace URI for index 2 has been updated. Clients that reference the URI (uns=) instead of the Namespace Index (ns=) may require configuration updates.

Previous URIs:

uns=KEPServerEX

uns=ThingWorx Kepware Server

New URI:

uns=Kepware Server

This change may affect any OPC UA client that uses URI-based references *(for more information, see: Article - CS443295. Login required.)*

What Is Migrated

Item	Details	Notes
Project Files	Automatically migrated; compatible with Kepware Server. Backup recommended.	Files with the following extensions are migrated: .ini, .log, .opf, .ptr, .bin, .dat, .csv, .idx, .tsd, .json
Settings.ini & Admin Settings	Copied during upgrade.	Not all settings in the Administration persist *(see below table for examples)*.
Driver/Plug-in File Paths	Automatically updated if default paths are used.	Features migrated are: ThingWorx Native Interface, Memory Based, Simulator, ABB TotalFlow, Datalogger. **Note**: The Local Historian Plug-In does not automatically update the path and requires manual correction *(see note below for additional details)*.
Application Data	Migrated if same path (e.g., C:\ProgramData) is used across versions.	*See the Kepware Server Install Guide.*
Project & Server Settings	Preserved	Preserved *unless* the **Remove User Data** checkbox is selected during uninstall.

What Is Not Migrated

Item	Details	Notes
Registry Settings	Not migrated.	Expected to have no impact outside of OPC ProgID Redirect.
OPC ProgID Redirects	Stored in registry settings and existing items are not migrated.	New entries are created for TKS V6 and/or KSE V6. *See note below for additional details.*
User Manager Settings	Must be manually exported and imported.	*See Export User Data section above for details.*
Certificates	Not migrated; new instance certificates are generated during installation.	*See Certificates section for more information.*
Simulator Data	If coming from TKS and using a simulator with the demo project, the simulator persistence .dat file may not be migrated.	*See Article - CS454596 for more information (login required).*

- **Note**: If using the Local Historian Plug-In and the Datastore location is set to Program Data, this path does not automatically updated during migration to Kepware Server. To review, verify, or update the Datastore location, navigate to the **Properties...** of the target Datastore.
- **Tip**: The OPC ProgID redirect mechanism enables Kepware Server to change the ProgID/CLSID of DCOM servers (OPC DA, OPC AE, OPC HDA) without breaking existing client configurations. This allows a client to use the legacy ProgID to connect and communicate even when the actual ProgID used by the server has changed. The server_admin.exe includes a ProgID Redirect tab to add or remove redirected ProgIDs.

TKS / KSE Program Data and Registry Entries

After migration is complete, TKS / KSE Program Data and registry entries remain in addition to the new Kepware Server entries. The TKS / KSE items can be deleted with no impact on the function of Kepware Server.