Migrace na Kepware Server 7.0 z KEPServerEX 6 nebo ThingWorx Kepware Server 6

Společnost Kepware / PTC přechází na nové označení produktů KEPServerEX (KSE) a ThingWorx Kepware Server (TKS), aby všem uživatelům poskytla sjednocené a optimalizované prostředí. Tím dochází k ukončení obou produktů a jejich nahrazení jediným produktem Kepware Server. Všem uživatelům se důrazně doporučuje provést upgrade na nový produkt.

- *Podrobné poznámky k vydání naleznete na webu: www.ptc.com/en/products/kepware.*

Byla doplněna automatizace, která uživatelům pomáhá s upgradem na Kepware Server.

Postupujte podle níže uvedených kroků pro upgrade TKS (verze 6.17–6.18) nebo KSE (verze 6.17–6.18) na Kepware Server (7.0). Pokud používáte nižší verzi, před migrací nejprve upgradujte na verzi 6.17 nebo 6.18.

Postup

- **Poznámky**:
  - TKS / KSE a Kepware Server nelze mít nainstalované na stejném počítači zároveň. Pro migraci z předchozího produktu na nový MUSÍTE postupovat podle těchto pokynů.
  - Platné aktivní licence pro TKS / KSE budou po dokončení migrace nadále fungovat i s Kepware Serverem.
  - Neplatné licence nebo propadlá údržba (maintenance) musí být před upgradem vyřešeny.
  - Projektové soubory a většinu datových souborů lze migrovat automaticky. Projekty TKS / KSE jsou s Kepware Serverem kompatibilní. (Doporučujeme však vytvořit zálohu projektu pro případ, že by nastaly problémy. Podrobnosti o tom, co se migruje a co ne, najdete v tabulkách na konci.)
- **Tip**: Pokud používáte hardwarový klíč, požadovaný certifikátový soubor lze znovu stáhnout z MyKepware pomocí ID uvedeného na fyzickém klíči. Po dokončení upgradu je nutné soubor znovu importovat, aby licencování fungovalo.

Vytvoření aplikačního reportu

- Tento krok je volitelný, ale doporučený.

Pomocí nástroje **Application Report Utility** shromážděte zálohu konfigurace serveru a souvisejících nastavení a logů. Tento report je užitečným podkladem pro diagnostiku případných problémů, které se mohou objevit během procesu upgradu a migrace.

- *Postupujte podle kroků v části Generating an Application Report*

Export certifikátů (pokud je to relevantní)

- Tento krok je volitelný.

Importované instance certifikáty a externí certifikáty v úložištích důvěryhodných certifikátů (Trust Stores) se nemigrují. Pokud tyto certifikáty nejsou přístupné mimo instanci TKS / KSE, exportujte je před odinstalací, aby je bylo možné importovat do Kepware Serveru *(další informace viz níže kapitola Certifikáty)*.

Záloha aktuálního projektu

1. Otevřete stávající software dvojklikem na ikonu na ploše nebo výběrem **Configuration** ze System Tray.
2. Vyberte **File | Save As**.
3. Podle pokynů uložte aktuální projekt do lokálního adresáře.

- Z bezpečnostních důvodů nastavte silné heslo.

Export uživatelských dat

1. V System Tray přejděte do **Settings**.
2. Vyberte **User Manager** a **Export User Information** (Alt + E).
3. Podle pokynů uložte uživatelská data na bezpečné místo.

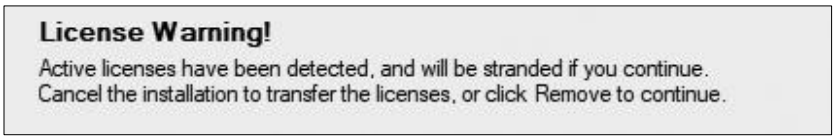
- Z bezpečnostních důvodů nastavte silné heslo.

Odinstalace TKS / KSE

- **Upozornění**: Provoz předchozí verze na stejném systému současně s Kepware Serverem není podporován. Před instalací aktualizace je nutné předchozí verzi odinstalovat.
- **Upozornění**: Ověřte, že NENÍ zaškrtnuta volba **Remove User Data**. Tato volba by odstranila aktuální runtime projekt a vlastní nastavení serveru. Ve výchozím stavu není vybrána.
- **Poznámka**: Pokud k odinstalaci použijete standardní postup ve Windows (přes nabídku Start, Settings nebo Control Panel), uživatelská data se automaticky zachovají.

1. Klikněte pravým tlačítkem na nabídku **Start** a vyberte **Apps and Features** (**Programs and Features** ve Windows 7).

2. Vyhledejte a vyberte TKS / KSE.
3. Klikněte na **Uninstall**.
4. Pokud se Kepware Server instaluje na stejném počítači, potvrďte varovné okno o aktivní licenci kliknutím na **OK**.



5. Postupujte podle pokynů pro úplnou odinstalaci produktu.

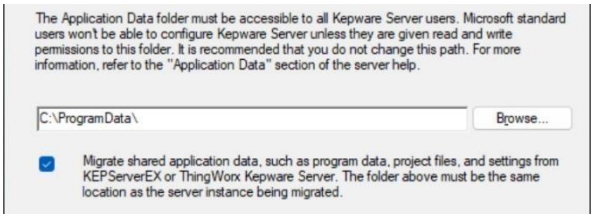
Stažení Kepware Serveru

Instalátor Kepware Server verze 7.0 stáhněte na MyKepware.com.

Instalace Kepware Serveru

- **Upozornění**: Ujistěte se, že složka **Application Data** odpovídá cestě použité při předchozí instalaci TKS / KSE. Ve výchozím stavu je to *C:\ProgramData*. Pokud zvolíte jiné umístění než při předchozí instalaci, ručně aktualizujte projektový soubor na nové umístění a zkopírujte následující soubory ze starého adresáře **TKS / KSE Application Data** do nového adresáře **Kepware Server Application Data**:
  - default.opf
  - settings.ini
  - event.log
  - _EFM (složka)
  - Historical Data (složka)
  - ThingWorx (složka)
  - ua_gateway.json
  - IoT Gateway (složka)

1. Spusťte průvodce instalací Kepware Server.
2. Postupujte podle pokynů a během instalace se ujistěte, že je zaškrtnuté políčko **Migrate application data**.



3. Spusťte **Kepware Server Configuration**.
4. Ověřte, že se načetl projekt z předchozí verze (případně jej vyhledejte a načtěte).

Import uživatelských dat

1. V System Tray přejděte do **Settings**.
2. Vyberte kartu **User Manager**.
3. Zvolte **Import User Information** (Alt + I).
4. Vyhledejte exportovaný uživatelský soubor.
5. Klikněte na **Open**.
6. Zadejte správné heslo (pokud je nastavené, je pro import uživatelských dat vyžadováno).
7. Ověřte, že jsou přítomni uživatelé a skupiny z předchozí instalace.

UA Gateway – důležité informace

Žádné soubory programových dat **UA Gateway** z TKS se do nových souborů Kepware Serveru nepřenášejí.

Pokud chcete migrovat certifikáty důvěry protistrany (peer trust certificates) UA Gateway do nového úložiště důvěry (trust store) v Kepware Serveru, musíte je ručně přesunout z úložiště programových dat TKS do úložiště programových dat Kepware Serveru.

Pokud certifikáty důvěry ručně nepřesunete, vaši UA klienti a UA servery budou hlásit, že certifikáty nejsou důvěryhodné. Použijte standardní postup pro důvěryhodné schválení UA certifikátů přes uživatelské rozhraní.

Ruční migrace UA trust certifikátů

Pro certifikáty důvěry UA Gateway – Server Interface (Peer Trust):

Původní umístění:

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

Nové umístění:

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

Pro certifikáty důvěry UA Gateway – Client Interface (Peer Trust):

Původní umístění:

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

Nové umístění:

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

Také je potřeba zachovat veškeré důvěryhodné uživatelské certifikáty pro obě rozhraní.

Pro certifikáty Trust User (důvěryhodný uživatel) pro UA Gateway Server Interface:

Původní umístění:

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

Nové umístění:

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

Poznámky:

- Veškeré zbývající soubory v *<program data path>\PTC\ThingWorx Kepware Server\V6\UA Gateway* zůstávají pro aplikaci Kepware Server nepoužívané.
- Pokud chcete soubory TKS uložit pro archivaci, nebo naopak složku a její obsah smazat kvůli úspoře místa, je nutné to provést ručně.

Obnovení připojení původního UA klienta v Kepware Serveru

Pokud během instalace Kepware Server 7.0 nejsou odstraněna uživatelská data, OPC UA spojení mezi UA Gateway a původním UA serverem selže a oznámí chybu "**Bad User Access Denied**". Důvodem je, že název klientského připojení a heslo uživatele jsou pro novou instalaci jiné.

Viz "Default Connection to the OPC UA Server" v nápovědě serveru, kde je popsáno, jak nastavit správné heslo pro spojení UA Gateway na původní UA server.

Název klientského připojení je nutné upravit jako součást PUT requestu:

"common.ALLTYPES_NAME": "Kepware Server",

PUT request aktualizuje název klientského připojení a uživatelské heslo.

Poznámka: Některé ovladače (například OPC UA Client Driver a OPC DA Client Driver) nebo jiné utility a připojení mohou vyžadovat aktualizaci přes proces důvěry (trust) UA certifikátů.

Certifikáty

V souladu s nejlepšími bezpečnostními postupy používá Kepware Server certifikáty s 2048bitovými veřejnými klíči namísto 1024bitových klíčů používaných v TKS / KSE. Tato změna má různé dopady na různé třídy certifikátů v rámci Kepware Serveru.

Instance certifikáty vygenerované v TKS / KSE nelze migrovat. Místo toho je Kepware Server automaticky znovu vygeneruje. Klienti používající tuto třídu certifikátů musí novým certifikátům důvěřovat (trust):

- 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

Importované instance certifikáty se z TKS / KSE do Kepware Serveru nemigrují a je nutné je znovu importovat. Tato třída certifikátů zahrnuje:

- Importované instance certifikáty pro OPC UA, IoT Gateway REST Server, ThingWorx Native Interface, Configuration API Service REST Server, IEC 61850 MMS Client a MQTT Client Driver (CA-Signed, Imported Self-Signed apod.)
- IoT Gateway MQTT Agent Instance Certificate

Upozornění: Důrazně se doporučuje importovat 2048bitové certifikáty.

Externí certifikáty v trust store se nemigrují. Tyto certifikáty je nutné ručně importovat do trust store v Kepware Serveru. Pokud tyto certifikáty nejsou dostupné mimo TKS / KSE, doporučuje se je před odinstalací vyexportovat z trust store.

Poznámka: Důvěryhodné certifikáty OPC UA klientů a serverů možná nebude nutné ručně importovat do Kepware Serveru (viz *Obnovení připojení původního UA klienta v Kepware Serveru*).

Import / export instance certifikátu externího OPC UA

1. V System Tray přejděte do **OPC UA Configuration**.
2. Vyberte **Instance Certificates**.
3. Vyberte **Import certificate** nebo **Export [server/client driver] certificate** v části **Server** pro certifikáty OPC UA Server Interface, nebo v části **Client Driver** pro certifikáty OPC UA Client Driver.

Import instance certifikátu IoT Gateway MQTT Agent

1. V System Tray přejděte do **Settings…**
2. Vyberte kartu **IoT Gateway**.
3. V části **MQTT Agent** zvolte **Manage Certificate…**
4. Zvolte **Import New Certificate**.

Poznámka: Certifikáty IoT Gateway MQTT Agent nelze exportovat.

Import / export instance certifikátu IoT Gateway REST Server

1. V System Tray přejděte do **Settings…**
2. Vyberte kartu **IoT Gateway**.
3. V části **REST Server** zvolte **Manage Certificate…**
4. Zvolte **Import REST server certificate…** nebo **Export REST server certificate…**.

Import / export instance certifikátu pro MQTT Client Driver, ThingWorx Native Interface a IEC 61850 MMS Client Driver

1. V System Tray přejděte do **Settings…**
2. Vyberte kartu **Certificate Store**.
3. V rozbalovacím menu **Feature** vyberte požadovanou funkci.
4. V části **Instance Certificate** zvolte **Export** nebo **Import**.

Import / export důvěryhodného (Trusted) certifikátu pro MQTT Client Driver, Siemens S7 Plus Ethernet Driver, ThingWorx Native Interface a IEC 61850 MMS Client Driver

1. V System Tray přejděte do **Settings…**
2. Vyberte kartu **Certificate Store**.
3. V rozbalovacím menu **Feature** vyberte požadovanou funkci.
4. V části **Manage Trust Store** zvolte **Export** nebo **Import**.

Import a export certifikátu pro Configuration API Service

1. V System Tray přejděte do **Settings…**
2. Vyberte kartu **Configuration API Service**.
3. V části **Certificate Management** zvolte **Import Certificate** nebo **Export Certificate**.

Obnovení důvěry (trust) pro OPC UA připojení

Pro bezpečná připojení k OPC UA Server Interface a OPC UA Client Driver je nutné znovu nastavit důvěru (trust). Certifikáty související s Trusted Clients a Trusted Servers se z TKS / KSE do Kepware Serveru nepřenášejí.

Připojení rozhraní OPC UA serveru

Pokud externí klient nevyvolá výměnu certifikátů s rozhraním OPC UA Server, je nutné certifikát ručně vygenerovat na serveru a nahrát jej do klienta. Pokud klient výměnu certifikátů vyvolá automaticky, přeskočte kroky 2 a 3 níže.

1. Navigate to **OPC UA Configuration** from the System Tray.
2. V System Tray přejděte do **OPC UA Configuration**.
3. Vyberte kartu **Instance Certificates**.
4. V části **Server** zvolte **Export server certificate**.
5. Nahrajte tento certifikát do externího OPC UA klienta.
6. Vyberte kartu **Trusted Clients**.
7. Klikněte na název klienta, ke kterému se chcete připojit, a poté zvolte **Trust**.

Připojení ovladače OPC UA Client

Pokud ovladač OPC UA Client automaticky nevyvolá výměnu certifikátů s externím serverem, je nutné certifikát ručně vygenerovat na serveru a nahrát jej do Kepware Serveru. Pokud ovladač OPC UA Client výměnu certifikátů vyvolá automaticky, přeskočte kroky 2 a 3 níže.

1. V System Tray přejděte do **OPC UA Configuration**.
2. Vyberte kartu **Trusted Servers**.
3. Zvolte **Import** a nahrajte certifikát serveru.
4. Pokud má server červené X, klikněte na název serveru, ke kterému se chcete připojit, a zvolte **Trust**.

Změny v OPC UA Namespace

Namespace URI pro index 2 byl aktualizován. Klienti, kteří odkazují na URI (uns=) místo na Namespace Index (ns=), mohou vyžadovat úpravu konfigurace.

Předchozí URI:

uns=KEPServerEX

uns=ThingWorx Kepware Server

Nové URI:

uns=Kepware Server

Tato změna může ovlivnit jakéhokoli OPC UA klienta, který používá odkazy založené na URI (více informací viz: *Article - CS443295, přístupné po přihlášení)*

Co se migruje

Položka	Popis	Poznámka
Projektové soubory (Project Files)	Migrováno automaticky; kompatibilní s Kepware Serverem. Doporučuje se vytvořit zálohu.	Migrují se soubory s následujícími příponami: .ini, .log, .opf, .ptr, .bin, .dat, .csv, .idx, .tsd, .json
settings.ini a administrátorská nastavení (Settings.ini & Admin Settings)	Kopíruje se během upgradu.	Ne všechna nastavení v části Administration se zachovají (*příklady viz tabulka níže*).
Cesty k souborům ovladačů / plug-inů (Driver/Plug-in File Paths)	Automaticky se aktualizují, pokud jsou použity výchozí cesty.	Migrují se tyto funkce: ThingWorx Native Interface, Memory Based, Simulator, ABB TotalFlow, Datalogger. **Poznámka**: Local Historian Plug-In cestu automaticky neaktualizuje a vyžaduje ruční opravu (*další podrobnosti viz poznámka níže*).

Položka	Popis	Poznámka
Aplikační data (Application Data)	Migruje se, pokud je mezi verzemi použita stejná cesta (např. *C:\ProgramData*).	*Viz Kepware Server Install Guide.*
Nastavení projektu a serveru (Project & Server Settings)	Zachováno	Zachováno, *pokud* při odinstalaci není zaškrtnuto políčko **Remove User Data**.

Co se nemigruje

Položka	Popis	Poznámka
Nastavení registru (Registry Settings)	Nemigruje se.	Očekává se, že to nebude mít dopad mimo OPC ProgID Redirect.
Přesměrování OPC ProgID (OPC ProgID Redirects)	Je uloženo v nastavení registru a stávající položky se nemigrují.	Nové položky se vytvoří pro TKS V6 a/nebo KSE V6 *(další podrobnosti viz poznámka níže)*.
Nastavení User Manageru (User Manager Settings)	Je nutné je ručně exportovat a importovat.	*Viz kapitola: Export uživatelských dat.*
Certifikáty (Certificates)	Nemigruje se; během instalace se vygenerují nové instance certifikáty.	*Viz kapitola: Certifikáty.*
Data simulátoru (Simulator Data)	Pokud migrujete z TKS a používáte simulátor s demo projektem, .dat soubor perzistence simulátoru se nemusí migrovat.	*Více informací viz Article - CS454596 (přístupné po přihlášení).*

Poznámka: Pokud používáte **Local Historian Plug-In** a umístění **Datastore** je nastaveno na **Program Data**, tato cesta se při migraci na Kepware Server automaticky neaktualizuje. Pro kontrolu, ověření nebo změnu umístění **Datastore** otevřete **Properties…** cílového **Datastore**.

Tip: Mechanismus **OPC ProgID redirect** umožňuje Kepware Serveru změnit **ProgID/CLSID** DCOM serverů (OPC DA, OPC AE, OPC HDA) bez narušení stávajících konfigurací klientů. Díky tomu může klient používat původní (legacy) **ProgID** pro připojení a komunikaci i v případě, že se skutečný **ProgID** používaný serverem změnil. Nástroj **server_admin.exe** obsahuje kartu **ProgID Redirect**, kde lze přidávat nebo odebírat přesměrované **ProgID**.

Programová data a položky registru TKS / KSE

Po dokončení migrace zůstanou v systému programová data a položky registru pro TKS / KSE zachována, a to vedle nových položek pro Kepware Server. Položky související s TKS / KSE lze odstranit bez dopadu na funkčnost Kepware Serveru.