Installation & Upgrade

Kryon RPA

v20.9.8

Document revision: 29-Sep-2021

Contents

Guide Overview

Guide Overview

Scope 7

Intended audience 7

How to approach this guide 8

Where do I start from? 8

Platform Architecture

System Requirements – Server

System Requirements – High Scale Server

System Requirements – Clients

Initial Considerations

RPA platform authentication method 21

Database authentication method 21

Automation context 21

System Hardening 22

SSL/TLS 22

Multiple RPA servers (High-Availability) 22

Before you start

Are you re-installing? 23

Planning to have SEQ on a remote server? 23

Need to review the ports we are going to use? 23

Create or verify a user that can run RPA services 23

Planning to use Kerberos authentication? 24

Planning to connect the RPA server to a remote Database Server? 24

Kryon RPA Server Installation

RPA Server Installation Steps Overview 25

Running the RPA Server Installation Wizard 26

Target Folder 26

Deployment type 27

Servers 27

High Availability 29

RPA Clients 32

Secured Connection (SSL/TLS) 32
Option 1: Without SSL/TLS Certificate 32
Option 2: Secured (provide an existing certificate) 33
Ports 35
SEQ – Centralized Log Repository 35
User Authentication 36
Service Credentials 36
Authentication Service Credentials 38
Connect to Active Directory 39
Active Directory Groups 41
Authentication Platform Security 42
Option 1: Provide KEYTAB file post installation 42
Option 2: Use existing KEYTAB file 43
Option 3: Generate a KEYTAB file 44
Connect to Database 45
Option 1: Install local SQL Server 45
Option 2: Configure the connection to your database server 45
RPA Authentication DB 46
Keycloak default user credentials 48
Support Tools 50
Components to Install 52
Executing Installation 52

Kryon RPA Clients Installation

RPA Clients Installation Steps Overview 53
Running the Client (Robot and Studio) Installation Packages 54
Configuring Connection to Server 54
Option to configure the client .exe file parameters for Robot silent installation 56
Configuring Client Connection to Seq 57
Enabling Unattended Robot Mode/LogonExpert 57
Enabling unattended robot mode 57
Enabling LogonExpert 58

Upgrading the RPA Server and Clients

Upgrading the RPA Server 59
Upgrading the RPA Clients 60

Backup Current Version & Database 61
Back up current version installation 61
Back up Kryon database 61
Configure Current SQL Instance 62
Prepare the Kryon Database for Upgrade 65
Remove the Current Console Configuration 66
Upgrading the database version 67
Migrating users to the new Authentication Platform 70
To migrate Kryon users to the new authentication platform: 70
Step 1: Configure user migration script options 70
Step 2: Run the user migration script 72
Step 3: Confirm successful migration 73
Encrypt the Credentials Vault 74
How do I know if the Credentials Vault was already encrypted? 74
Running the Migration Tool to encrypt the Credentials Vault 75
Confirming successful encryption 76
Automatic Client Update 77
Prerequisites 77
How to automatically deploy software updates 77

Rolling-back to Previous Version

APPENDICES

Kryon Network Ports 81
Default port configuration 81
Opening ports 81
Preparing the Kryon Database Server 83
Step 1: Install SQL Server Management Studio 84
Step 2: Prepare an SQL Server instance 85
Creating Database Manually 91
Connect to the SQL Server instance 91
Create the authentication platform database schema 91
Create the Kryon application database 92
Enter the RPA server addresses 92
About upgrading from Console to ConsoleX 94
Migrating data from Console to ConsoleX 96

Task with recurrences 96
Task with no recurrences, with single run in the past 97
Task with no recurrences, with multiple runs in the past 97
Task with no recurrences, with a future single run 98
Task with no recurrences, with future multiple runs 99
Task in the queue 99
SSL/TLS Certificates - Manually creating certificate files 100
Install OpenSSL 100
Manually creating individual certificate files 100
SSL/TLS Requirements 111
Enabling Kryon Connector Browser Extensions 112
Installing Kryon Java Bridge 113
Generating a KEYTAB file (Kerberos) 115
Restarting Kryon Services 116
Configuring Task Re-run 117
Changing Kryon Studio to Japanese 118
Changing SEQ default minimum level of 'log writes' 119
Why has this change been made? 119
Changing the default 'log writes' 119
Configuring Kryon Terminal Server Robot 120
Configure the tool 120
Install the tool 120
Managing the Tool 123
Logging 124
Configuring Non-Default Ports in a SSL/TLS Deployment 125
Non-default HTTPS and/or Discovery port: client configuration 125
Non-default Discovery port: Console configuration 125
Adding another LDAP user federation (Kerberos) 127
Connect to Windows Active Directory 128
Sync users to Kryon Admin 134
RPA System Hardening and Vulnerability Management 135
Before Installation 135
During Installation 135
After Installation 135

How to encrypt the database connection (tutorial) 136
Troubleshooting 145
AutoUpdate error 404 in Network Load-Balancer configuration 145
"The system administrator has set policies to prevent this installation" error 145

Guide Overview

Guide Overview

Scope

This guide explains the steps required to install (and upgrade) the components of the Kryon RPA Platform:

1. Installing server-side components
    - Kryon RPA Server (including Kryon Admin)
    - Kryon Database
    - Kryon Console
2. Installing client applications
    - Kryon Studio
    - Kryon unattended robots
    - Kryon attended robots
3. Upgrading Versions

Intended audience

The Kryon RPA Platform is an enterprise system involving multiple components and networking/security considerations. It is anticipated that installation will be performed by IT professionals with general knowledge of the following:

- Windows (server and desktop editions)
- Network security and protocols
- Microsoft SQL Server

This guide is intended for such IT personnel.

How to approach this guide

About the documentation of the installation and upgrade processes

As you go through the processes and instructions documented in here, you'll find cross-references to different appendices located at the end of this manual. The cross-references are named "**Read more about...**"/"**read about**"/"**See <topic>**".

Click a cross-reference to check out some more advance or customized configuration, to learn more about a specific configuration, or to review the relevancy and implications of some of the options.

Don't worry about navigating your way back and forth between the different appendices and the installation step or page you were at. We've inserted dedicated cross-references to take you back and forth between the sections. You'll find these links at the end of each relevant appendix, named: "**-Take me to the relevant step in the RPA Installation Guide-**".

About the screenshots

Screenshots are available sparingly; we include them as necessary and for further clarification. We've made sure to cover the required information for you in text.

The headlines in the RPA Server Installation chapter correspond to the headlines in the RPA server installation wizard.

Where do I start from?

I am installing from scratch

First, you take a look at the Platform Architecture to get a better idea of how the RPA services are laid out.

Then, go over the Server Systems Requirements, and Clients System Requirements to make sure everything is ready from your side.

For High-Scale Production Environment, review System Requirements – High Scale Server

After that, make sure you cover the Initial Considerations section to see if there is anything else you need to consider or maybe prepare.

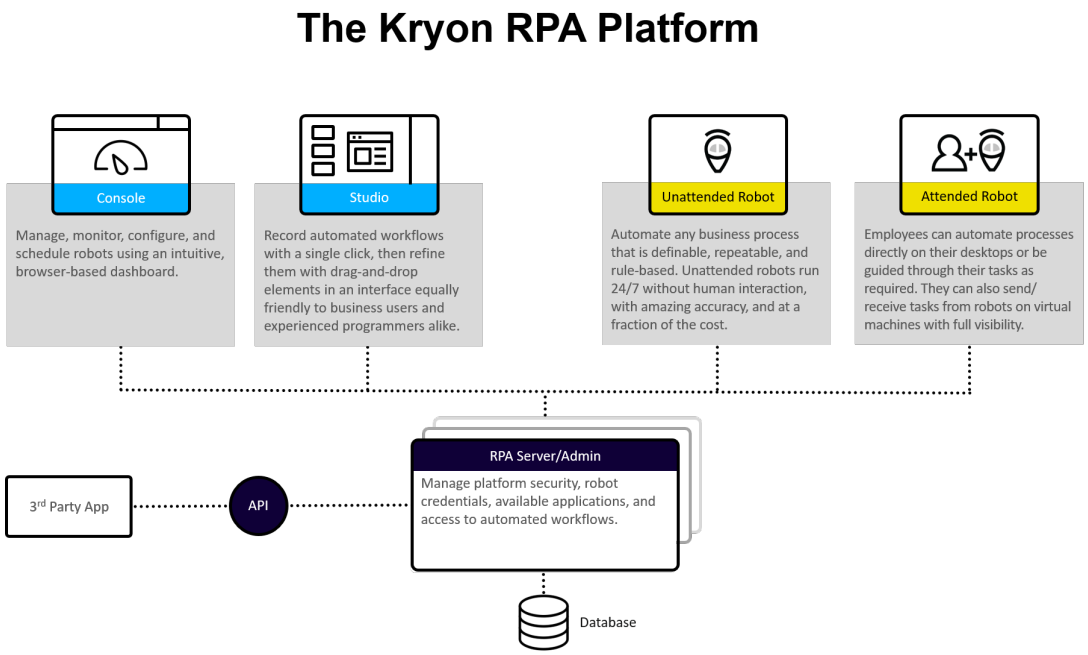
Got it all covered? You can start with the RPA Server Installation (make sure to read the 'Before you Start' and the short sections following it; prerequisites, installation steps overview, etc.).

Done with the server installation? Move to the RPA Client Installation to install Studio and Robot.

I want to upgrade

When it is time to upgrade, follow the instructions in the Upgrading Versions section.

Platform Architecture



System Requirements – Server

	Test Server	Production Environment (minimum)	Production Environment (recommended)		
	Single Server	Single Server	RPA Servers	Database Server	Centralized Log Repository Server (SEQ) *
Machine role	RPA Server + Database + Console	RPA Server + Database + Console	RPA Server + Console	Database	SEQ
# of servers	1 physical or VM server	1 physical or VM server	2 physical or VM servers	According to organization policy – redundant or cluster	According to organization policy – redundant or cluster
CPU	4 cores	4 cores + 2 cores for each 1,000 concurrent attended or 50 unattended robots	4 cores + 1 core for each 1,000 concurrent attended or 50 unattended robots	4 cores + 1 core for each 1,000 concurrent attended or 50 unattended robots	4 cores
Memory	8 GB	8GB + 512MB for each 1,000 concurrent attended or 50 unattended robots	8GB + 512MB for each 1,000 concurrent attended or 50 unattended robots	8GB + 512MB for each 1,000 concurrent attended or 50 unattended robots	16 GB RAM

	Test Server	Production Environment (minimum)	Production Environment (recommended)		
	Single Server	Single Server	RPA Servers	Database Server	Centralized Log Repository Server (SEQ) *
Robot capacity		**According to number of CPU cores –** *With 4 cores (minimum architecture)*: Max # of 1000 concurrent attended robots - or - Max # of 50 concurrent unattended robots *With 8 additional cores*: Max # of 1000 concurrent attended robots - or - Max # of 350 concurrent unattended robots	**According to number of CPU cores –** *With 4 cores (minimum architecture)*: Max # of 1,000 concurrent attended robots - or - Max # of 50 concurrent unattended robots *With 12 additional cores*: Max # of 15,000 concurrent attended robots - or -	**According to number of CPU cores –** *With 4 cores (minimum architecture)*: Max # of 1,000 concurrent attended robots - or - Max # of 50 concurrent unattended robots *With 12 additional cores*: Max # of 15,000 concurrent attended robots - or - Max # of 500	

	Test Server	Production Environment (minimum)	Production Environment (recommended)		
	Single Server	Single Server	RPA Servers	Database Server	Centralized Log Repository Server (SEQ) *
			Max # of 500 concurrent unattended robots	concurrent unattended robots	
Disk size (Local hard disk *only*)	250 GB	250 GB (minimum 100 GB required by the installer)	500 GB	500 GB	256 GB SSD
Network	20 Mbps in/out	20 Mbps in/out	Average of 30 Mbps (in/out) per 5,000 concurrent attended or 167 concurrent unattended robots		
OS	Windows Server 2012 R2 or higher	Windows Server 2012 R2 or higher	Windows Server 2012 R2 or higher		
Database software	Microsoft SQL Server 2012 or higher (Express edition, ***NO license required***), including these components:	Microsoft SQL Server 2012 or higher (Standard edition, ***license required***), including these components:		Microsoft SQL Server 2012 or higher (Standard edition or higher, ***license required***), including	

	Test Server	Production Environment (minimum)	Production Environment (recommended)		
	Single Server	Single Server	RPA Servers	Database Server	Centralized Log Repository Server (SEQ) *
	• Database Engine Services • Basic Management Tools ** *In test environments, Microsoft SQL Server 2017 Express Edition can be optionally installed by the RPA server installation package.*	• Database Engine Services • Basic Management Tools ** *In production environments, database software must be installed prior to RPA server installation*		these components: • Database Engine Services • Basic Management Tools ** *In production environments, database software must be installed prior to RPA server installation*	

*The information is based on SEQ System Requirements.

System Requirements – High Scale Server

	High Scale Production Environment 30K Attended/Server UP TO 60k/System		
	RPA Servers	**Database Server**	**Centralized Log Repository Server (SEQ) ***
Machine role	RPA Server + Console	Database	SEQ
# of servers	2 physical or VM servers	According to organization policy – redundant or cluster	According to organization policy – redundant or cluster
CPU (See the next table for CPU reference)	16 cores Intel® Xeon® Scalable Processors/AMD EPYC™ 2nd generation ***or;*** 24 cores Intel® Xeon® Processor E5 v4 Family ***or;*** 32 cores AMD EPYC™ 1st generation	16 cores Intel® Xeon® Scalable Processors/AMD EPYC™ 7002 series processor ***or;*** 24 cores Intel® Xeon® Processor E5 v4 Family ***or;*** 32 cores AMD EPYC™ 7001 series processor	8 cores
Memory	16 GB RAM	32 GB RAM	16 GB RAM
Robot capacity	**According to number of CPU cores:** ***Up to 15K concurrent Attended/500 Unattended***	**According to number of CPU cores:** ***Up to 15K concurrent Attended/500 Unattended***	

	High Scale Production Environment 30K Attended/Server UP TO 60k/System		
	RPA Servers	**Database Server**	**Centralized Log Repository Server (SEQ) ***
	Robots: • 8 x cores Intel® Xeon® Scalable /AMD EPYC™ 7002 series processor • 12 x Intel® Xeon® Processor E5 v4 Family • 16 x cores AMD EPYC™ 7001 series processor ***Up to 30K concurrent Attended/1K Unattended Robots:*** • 16 x cores Intel® Xeon® Scalable /AMD EPYC™ 7002 series processor • 24 x Intel® Xeon® Processor E5 v4 Family • 32 x cores AMD EPYC™ 7001 series processor	***Robots:*** • 8 x cores Intel® Xeon® Scalable /AMD EPYC™ 7002 series processor • 12 x Intel® Xeon® Processor E5 v4 Family ***Up to 30K concurrent Attended/1K Unattended Robots:*** • 16 x cores Intel® Xeon® Scalable /AMD EPYC™ 7002 series processor • 24 x Intel® Xeon® Processor E5 v4 Family ***Up to 60K concurrent Attended/2K Unattended Robots:*** • 32 x cores Intel® Xeon® Scalable /AMD EPYC™ 7002 series processor • 48 x Intel® Xeon® Processor E5 v4 Family	
Disk size (Local hard	500 GB	500 GB	256 GB SSD

	High Scale Production Environment 30K Attended/Server UP TO 60k/System		
	RPA Servers	**Database Server**	**Centralized Log Repository Server (SEQ) ***
disk *only*)			
Network	Average of 90 Mbps (in/out) per 15,000 concurrent attended or 500 concurrent unattended robots		
OS	Windows Server 2012 R2 or higher		
Database software		Microsoft SQL Server 2012 or higher (**Enterprise** edition, ***license required***), including these components: • Database Engine Services • Basic Management Tools **IMPORTANT:** In production environments, database software ***must*** be installed prior to RPA server installation. Max degree of parallelism ***must*** be set to 1 at database level (Kryon Database options - Max Dop set to 1).	

*The information is based on SEQ System Requirements.

High Scale Production Environment CPU Reference	
CPU Series	**RPA Server + Console**
Intel® Xeon® Scalable Processors	Xeon Platinum 8259CL (AWS EC2 M5 instance) Xeon Platinum 8275CL (AWS EC2 C5 instance) Xeon Platinum 8124M (AWS EC2 C5n instance) Xeon Platinum 8180
AMD EPYC™ 7002 series	Epyc 7R32 (AWS EC2 C5a instance)
Intel® Xeon® Processor E5 v4 Family	Xeon E5-2686 v4 (AWS EC2 M4 instance)
AMD EPYC™ 7001 series	Epyc 7571 (AWS EC2 M5a instance) Epyc 7601

System Requirements – Clients

	Unattended Robot		Attended Robot		Kryon Studio	
	minimum	recommended	minimum	recommended	minimum	recommended
Machine type	physical or virtual		physical or virtual		physical or virtual	
CPU	Intel® Core Duo 2 GHz (or similar)	Intel® i3/i5/i7 (or similar)	Intel® Core Duo 2 GHz (or similar) * Intel® i3/i5/i7 (or similar) – if using Kryon's sensor/push technology	Intel® i3/i5/i7 (or similar)	Intel® i3/i5/i7 (or similar)	
RAM	2 GB	4 GB	2 GB * 4 GB – if using Kryon's sensor/push technology	4 GB	4 GB	8 GB
Free memory	200-300 MB (or higher)		200-300 MB (or higher)		200-300 MB (or higher)	
Minimum disk space	50 MB		50 MB		50 MB	

	Unattended Robot		Attended Robot		Kryon Studio	
	minimum	recommended	minimum	recommended	minimum	recommended
OS	Windows 7 SP1/8.1/10 (most recent update – 64 bit Windows Server 2008 R2 SP1/2012/2016/2019 – 64 bit		Windows 7 SP1/8.1/10 (most recent update) – 32/64 bit Windows Server 2008 R2 SP1/2012/2016/2019 – 64 bit		Windows 7 SP1/8.1/10 (most recent update) – 64 bit Windows Server 2008 R2 SP1/2012/2016/2019 – 64 bit ** Best practice is for the Studio machine's OS to match as closely as possible the OS of the robot machine(s) on which the automation workflows will run.*	
Other requirements					**Minimum video resolution:** 1024x768	

Initial Considerations

You can customize the installation of the Kryon RPA Platform according to your organization's network and security policies. Throughout this guide, instructions and requirements will vary based on the following primary considerations:

RPA platform authentication method

You can install Kryon RPA Server using either:

- **Username & Password authentication:** Client applications (including unattended/attended robots, Studio, and Console) can connect to the Kryon RPA Server using usernames/passwords configured specifically for the RPA platform and defined in Kryon Admin
- **Domain authentication (also referred to as Kerberos):** Client applications can connect to the Kryon RPA Server using credentials defined in **Windows Active Directory**. Also referred to as Single Sign-on.

Database authentication method

You can configure the Kryon database to use either:

- **SQL authentication:** The Kryon RPA Server can connect to the Kryon database server using username and password configured specifically for the database server, and defined in SQL Server Management Studio.
- **Windows authentication –** The Kryon RPA Server can connect to the Kryon database using network credentials defined in **Windows Active Directory**.

> **NOTE:** Either database authentication method can be used with either RPA platform authentication method.

Automation context

There are three different automation contexts:

- Attended
- Unattended
- Hybrid (install in a context that supports both attended an unattended automation)

The installation in **Unattended** or **Hybrid** automation context *requires* the installation of **Console**/**ConsoleX** as well.

The installation in Attended automation context *doesn't require* the installation of **Console**/**ConsoleX**.

System Hardening

Consider RPA System Hardening to reduce IT vulnerability and the possibility of being compromised.

See RPA System Hardening and Vulnerability Management

SSL/TLS

The Kryon platform includes the option to secure communications using SSL/TLS .

If you want to install with SSL/TLS , you can provide the organization's CA and certificate or generate them using the RPA Server installation wizard (yes, we can do it for you).

If you already have the organization's CA and certificate, just make sure they meet the TSL/SSL requirements.

If you are planning to create a CA and certificate before installing the RPA Server and you need the guidance, see SSL/TLS Additional Procedures.

> **NOTE:** Only SSL/TLS v1.2 is supported.

Multiple RPA servers (High-Availability)

The Kryon platform supports the option to install two (2) or more RPA servers. This is the recommended configuration in a production environment.

Before you start

- For easy installation, make sure you have the setup files (RPA server, Studio, and Robots) in the same folder.
- Make sure to run the Kryon RPA Server installation kit **as administrator**.

For a smooth installation, we recommend you review the below list of possible and optional configurations you may encounter throughout the RPA Server installation wizard so you can be properly prepared.

Are you re-installing?

If you are re-installing Kryon RPA Platform for any reason, make sure to restart the server first right after uninstalling and before you start with the new installation.

Planning to have SEQ on a remote server?

If you are planning to install SEQ on a different server, make sure to (i) install SEQ on the different server, OR (ii) to run the Kryon's SEQ Installation Wrapper file on that server. The Kryon SEQ Installation Wrapper wraps SEQ with Kryon's configurations for easier installation of the RPA Server. Either way, make sure to configure retention policy for SEQ.

Need to review the ports we are going to use?

You can review the list of default ports the RPA server is set to use (you can also set different ports). If you don't have the specified ports open, don't worry about it as you can open them with a click through the installation wizard (provided they aren't in use).

See Kryon Default ports.

Create or verify a user that can run RPA services

Ensure that there is a user with the rights to run Kryon services on the RPA server:

- If you will be using Username & Password authentication, this user must have local administrative rights for the machine on which the Kryon RPA Server will be installed (can be either a domain user or a local system account).
- If you will be using Kerberos authentication (Single Sign-on), this user must be a member of the domain (in Active Directory) and have local administrative rights for the machine on which the Kryon RPA Server will be installed.

We recommend you create a user for the specific purpose of running Kryon services (i.e., a user that will not log in to the RPA server for any other purpose).

Planning to use Kerberos authentication?

Obtain a KEYTAB file from your Domain Administrator (optional at this stage; a KEYTAB can also be generated during or after RPA server installation).

Planning to connect the RPA server to a remote Database Server?

If you are planning to connect the RPA server to a remote database server, make sure to prepare the Kryon Database Server.

> **NOTE:** The RPA installer gives you the option to install a local SQL on the fly.

GOT IT, TAKE ME TO THE NEXT STEP: RPA INSTALLATION STEPS OVERVIEW.

Kryon RPA Server Installation

RPA Server Installation Steps Overview

1. Running the RPA Server Installation Wizard
2. Selecting the RPA Server target folder
3. Selecting the deployment and automation type (attended, un-attended, or hybrid)
4. Selecting Console installation type (no Console, or the new ConsoleX)
5. Selecting installation type (single-machine or high-avaiability)
    - Providing servers FDQNs for high-availability
6. Selecting supported languages for the RPA clients (Robots)
7. Configuring connection security (SSL/TLS)
    - Generating or providing CA and certificates
8. Configuring server-client communication ports
9. Configuring Centralized Log Repository (SEQ)
    - Installing SEQ locally or connecting to remote SEQ
10. Selecting user authentication (Single Sign-on [Kerberos] or Username&Password)
11. Configuring the service credentials of the user who runs the RPA
12. Selecting a user to run authentication services on the RPA server
13. Configuring communication and authentication with Active Directories, Active Directory Groups, and Platform Security (these steps are **relevant only to Single-Sign-on user authentication type**).
14. Configuring database (install SQL locally or configure the connection to a remote database)
15. Setting the RPA authentication database
16. Review the authentication platform (Keycloak) users credentials created by the installer
17. Generate Client MSI setup kits
18. Installing additional support tools if needed
19. Review the components to be installed
20. Executing installation, server reboot, and completing installation

Running the RPA Server Installation Wizard

Run the RPA Server Installation setup file provided by Kryon and consider the upcoming configuration and installation options to match your organization's needs.

IMPORTANT

For password, the allowed special characters are:

` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] / < > , . ; ? : | (space)

The disallowed special characters are:

" ' \

Optional for POC purposes only: Check the "**Express Installation**" check-box for fast and automatic installation.
This is a quick automatic installation with default values (skips all the installation wizard configuration).

- Installs a new database upon every new Express installation
- Client exe files (Robot and Studio) must be in the same folder as the server installation file
- Once the server installation completes, simply run the client exe setup files from the MSI Kit
- Clients can be taken from C:\Kryon\RPA-Clients as MSI files, and executed when already configured
- For each express installation execution new schema will be created (default name with TimeDate sufix)
- RPA deployed as unattended single machine, username/password authentication method, services run as LocalSystem, default ports apply.

Click **Next** in the wizard

Target Folder

The installer automatically shows the folder to which the Kryon RPA Server files should be installed. The default value is `Kryon` on the local drive with the most free space.

You can keep the default 'install folder' or change it. If you decide to change it, make sure the **Install folder**:

- on a local drive that has at least 100Gb free storage and at least 20Gb free storage on C:\
- isn't a root folder of a drive (e.g., `C:\`)
- has a full path that doesn't exceed 20 characters in length

Click **Next** in the wizard

Deployment type

Select the relevant deployment type:

- Unattended Automation
- Attended Automation
- Hybrid Automation

Click **Next** in the wizard

Servers

Application server name:
The FQDN of the RPA server is populated automatically

Console type: (visible only for Unattended automation deployment)

- **Do not install Console:** Install in an attended automation only context.
- **Install ConsoleX:** Install in an unattended or hybrid automation context.

  If you are doing an upgrade, make sure to read about moving from Console to ConsoleX.
  See Migrating data from Console to ConsoleX, and About upgrading from Console to ConsoleX

Console server name: (visible only for Unattended automation deployment)

- If you are installing **ConsoleX**, the FDQN in this field must be the same FDQN of the ConsoleX application server (which is the same FDQN of the RPA server since *ConsoleX installation is supported only if installed on the RPA server*). In this case, the FDQN of the ConsoleX/RPA Server is populated automatically in this field.

Click **Next** in the wizard

High Availability

Select the relevant installation type:

- **Single Machine Deployment:** Install on one server only
- **High Availability – Built-in LB:** Install in High Availability mode (on at least 2 servers) using Kryon's Client based built-in Load Balancer.
    - **High Availability – Built-in LB:** Install in High Availability mode (on at least 2 servers) using Kryon's Client based built-in Load Balancer.

      NOTES:
      - You can select this option and insert the relevant server FDQN(s) even if you haven't configured the server(s) yet.
      - You can begin the installation of each additional Server in HA *only after* the installation of the first server is complete. Installation of more than one server in parallel isn't supported.

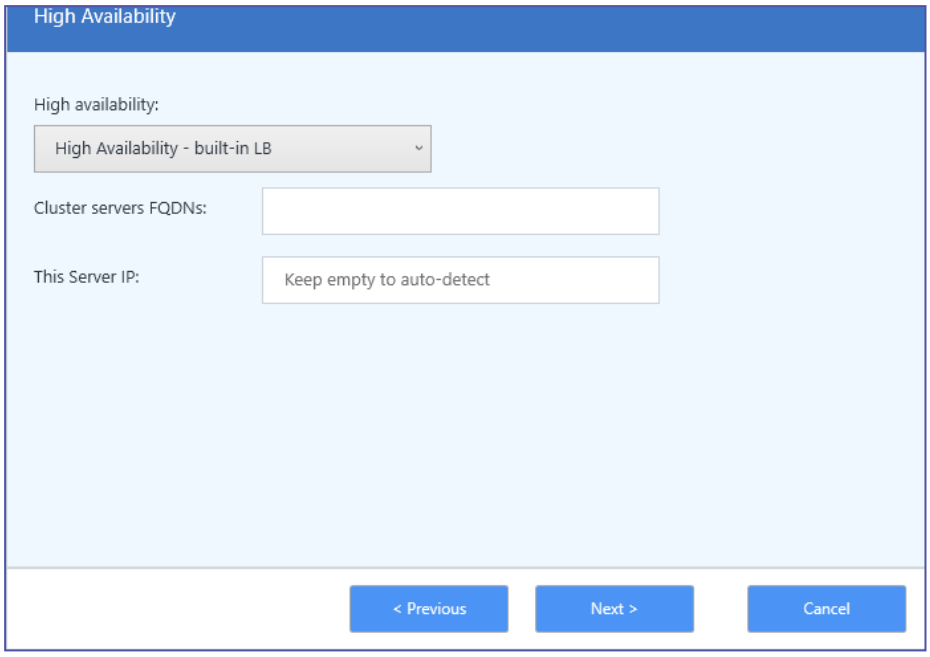
    - **Cluster Server FQDNs**: Insert the FQDN(s) of the server(s) on which you want to install RPA (main server and fallback servers). If you want to insert more than one server, separate the FQDNs using a comma (,) without space.

      Example: server1.com,server2.com

    - **This Server IP**: Keep empty. This field automatically populates.

      NOTE: If the server has more than one IP address, you can

manually insert the IP you want to use.



- **High Availability – Network LB:** (visible only for Attended automation deployment)
  Select this option ONLY with the guidance of your support team. This option allows you to configure a network load balancer instead of the built-in one.

  NOTE: When External/Network LB HA selected, the LeoServer table in the database should be populated with values of the LB FQDNs and not with the values or the participating servers.

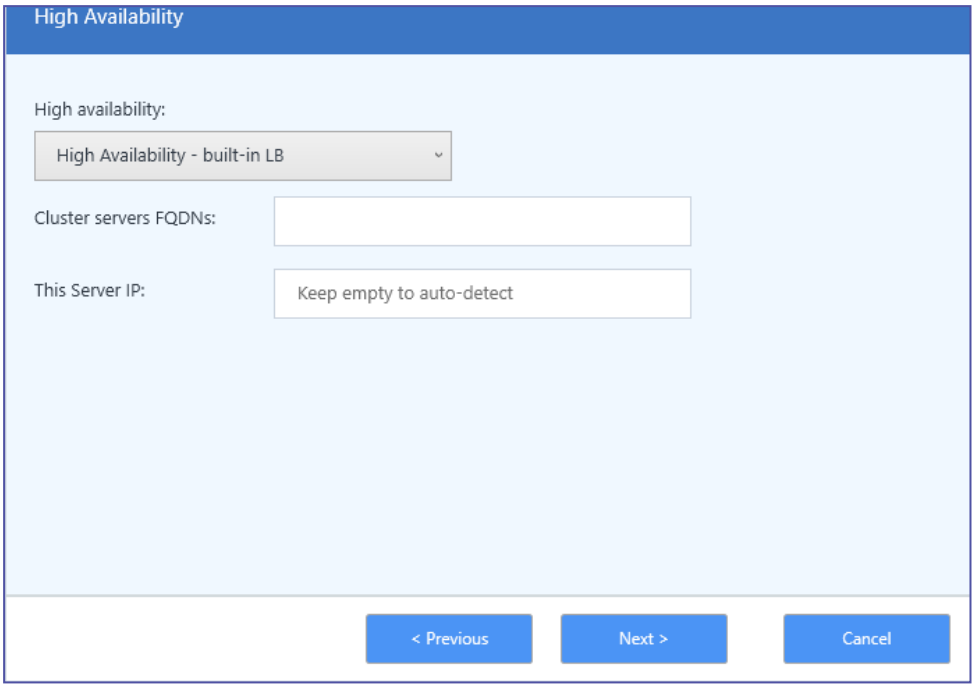
- **Cluster Server FQDNs**: Insert the FQDN(s) of the server(s) on which you want to install RPA (main server and fallback servers). If you want to insert more than one server, separate the FQDNs using a comma (,) without space.

  Example: server1.com,server2.com

- **This Server IP**: Keep empty. This field automatically populates.

  NOTE: If the server has more than one IP address, you can

manually insert the IP you want to use.



- **High Availability – Network LB:** (visible only for Attended automation deployment)
  Select this option ONLY with the guidance of your support team. This option allows you to configure a network load balancer instead of the built-in one.

NOTES:
- When External/Network LB HA selected, the LeoServer table in the database should be populated with values of the LB FQDNs and not with the values or the participating servers.
- In case of error 404, see AutoUpdate error 404 in Network Load-Balancer configuration

Click **Next** in the wizard

If RabbitMQ (open source message broker) isn't already installed on your server, the RPA Server Installation prompts you to install it and to create credentials for it.

If it is already installed, this step doesn't appear.

NOTE: Changing the default password is recommended for RPA System Hardening and Vulnerability Management

Click **Next** in the wizard

RPA Clients

Select the language(s) to be supported by the Kryon search engine (relevant only for **Attended** and **Hybrid** automation).

Click **Next** in the wizard

Secured Connection (SSL/TLS)

Select the relevant security option:

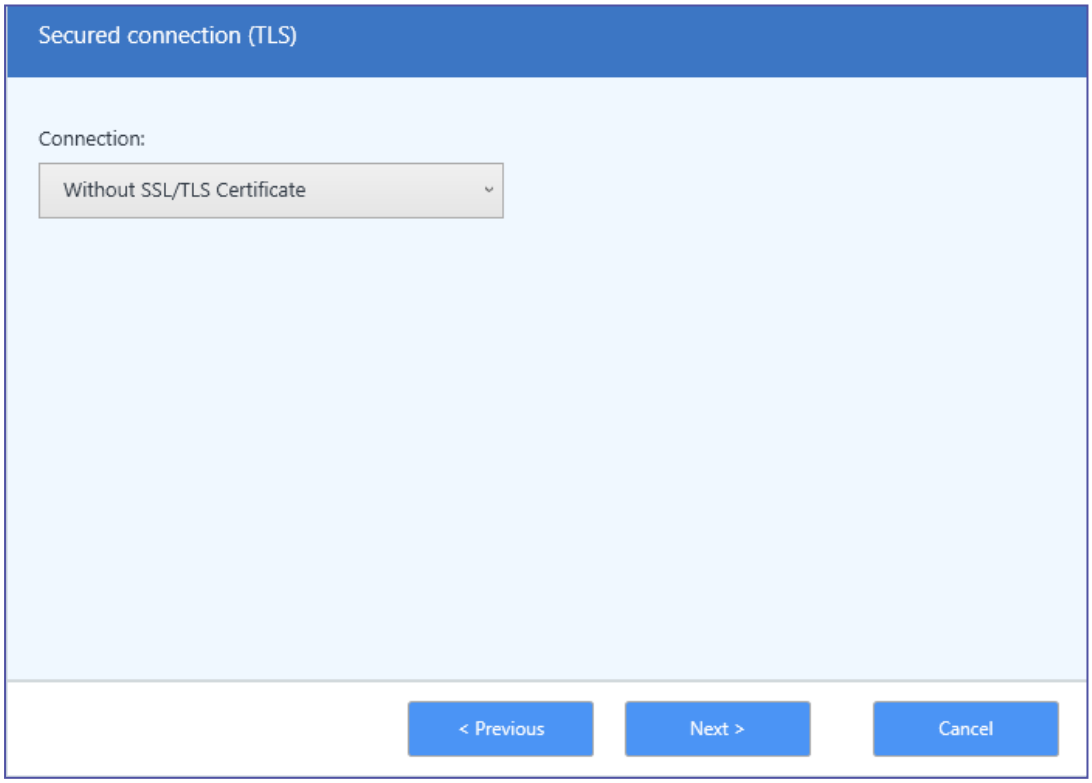
- Option 1 **Without SSL/TLS Certificate**
- Option 2 **Secured (provide an existing certificate)**

> **NOTE:** Only SSL/TLS v1.2 is supported.

Not sure what to select? Review the information below about each option.

Option 1: Without SSL/TLS Certificate

Run the installation in a 'simple' mode without SSL/TLS configuration; usually this option is used for a fast and simple installation for tests.



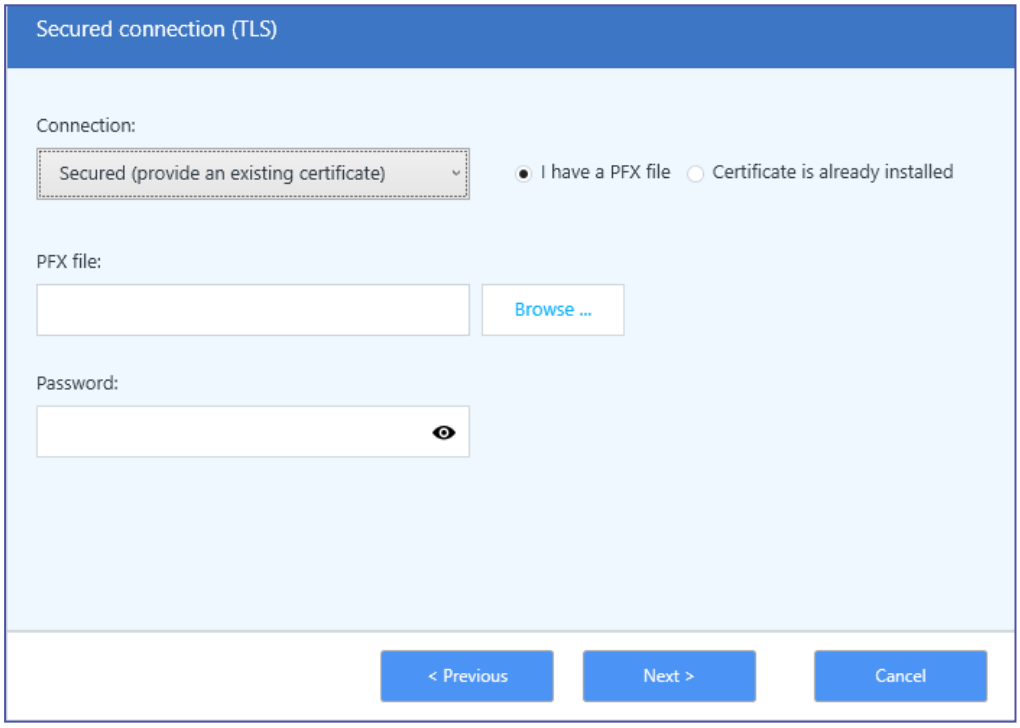
Option 2: Secured (provide an existing certificate)

Select the relevant option based on the format of your SSL/TLS certificate:

- **I have a PFX file:** You have a single file in ***.pfx** format. Browse the ***.pfx** file, and enter the certificate password.

  The installer will: (i) automatically install the ***.pfx** certificate in the Windows certificate store; and (ii) generate the individual required certificate files from the ***.pfx** file.

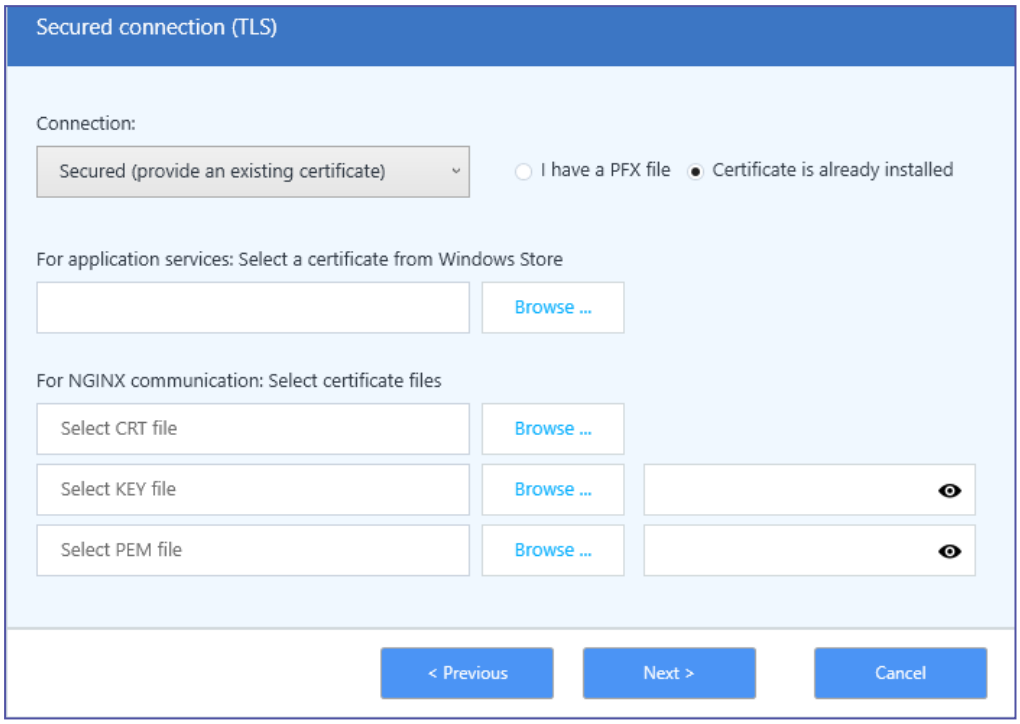
  NOTE: You can select this option even if the certificate has previously been installed in the Windows certificate store.



- **Certificate is already installed:** The ***.pfx** certificate has already been installed to the Windows certificate store and you have the following 3 required files: one in ***.key** format, one in ***.crt** format, and one named **ca-bundle.pem**.
  Browse to select the relevant certificate file from the Windows certificate store.
  Browse to select the relevant .CRT, .KEY, and .PEM files.

  NOTE: If you want to manually install the certificate in the Windows certificate store and generate the individual files, See Manually

creating individual certificate files.



Click **Next** in the wizard

Ports

The installer presents to you the default ports required for communication between server and clients.
Read more about the default ports opened and about opening ports manually.
The ports are:

- HTTPS port
- NGINX port
- Net.TCP port
- Discovery port (relevant/visible only for SSL/TLS deployments)

> **NOTE:** Only SSL/TLS v1.2 is supported.

Options to consider:

- You can change the default ports if needed - recommended for RPA System Hardening and Vulnerability Management .

- You can select to **Open all ports in Windows Firewall**.

Click **Next** in the wizard

SEQ – Centralized Log Repository

- Select **Install SEQ locally** if you want the installation package to automatically install a local copy of Seq (centralized logging package).
- Select **Use remote SEQ server** if you have installed SEQ on a different server. Before providing the information of the remote SEQ, we recommend you run the Kryon's SEQ Installation Wrapper on the server SEQ is installed on. The wrapper wraps SEQ with Kryon's configuration and allows establishing a successful connection between the RPA Server and the remote SEQ.

  After running the SEQ wrapper, insert the information of the remote SEQ.

  > **NOTE:** Inserting SEQ Server Ports isn't mandatory.

TIP:

- You can pull the remote SEQ information from the URL used to access Seq on the remote server. The URL structure is as follows: `{SEQ Protocol}://{SEQ server FQDN}:{SEQ Server Port}/{End point}`

- Check out the Seq developer's website to learn more about installing and working with Seq.

Click **Next** in the wizard

User Authentication

How will users/robots log in to Kryon application?

- For Domain authentication, select **Single sign on (Kerberos)**

  Note: Only domain users can configure SSO during installation.
- For Username & Password authentication, select **Require username and password**
- **Enable Kryon permissions system:** Select this checkbox to enable Kryon's internal permissions system (enables the assignment of read/write/publish permissions to Studio users and robots for specific libraries/categories of automation workflows).

Click **Next** in the wizard

Service Credentials

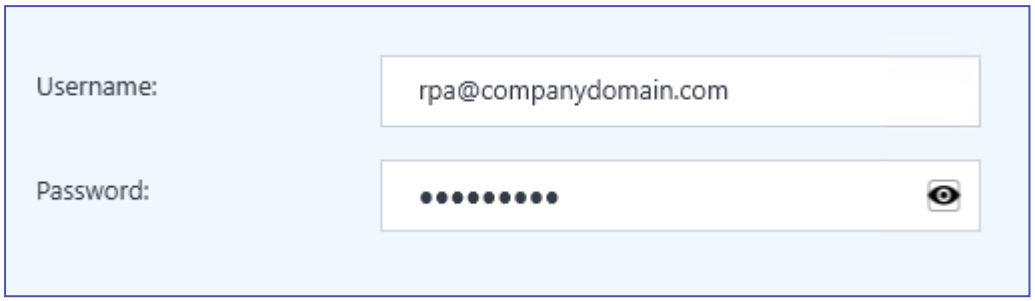
If you previously selected **Single sign on (Kerberos)**, enter the relevant credentials of the user who will run the RPA on the server.
The user must:

- have local administrative rights on the server
  Note: If you're logged-in with a different user, the installer will add a service-user to the user local Administrators group if permitted by the organization's policy. If the organization's policy doesn't permit this action, you need to add the service-user manually.
- be a domain account
- have access to database (if you are using SQL Windows Authentication connection to database schema)

IMPORTANT

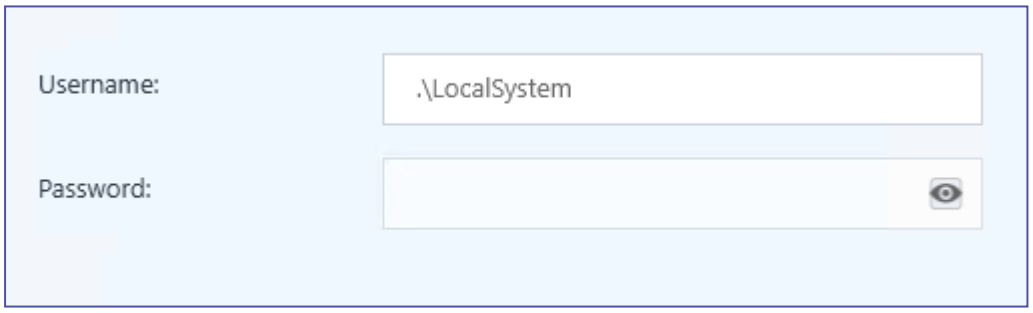
For password, special characters aren't supported. For example: `\ ; & "`

Note: You cannot use the default value `.\LocalSystem` for SSO (Kerberos).



If you previously selected **Username & Password authentication**, select one of the following options:

- Keep the default entry (`.\LocalSystem` with no password necessary); ***or***
- Enter the service user credentials:
  - Domain user format = `domain\user` or `user@domain`
  - Local user format = `.\user`
    Note: The user must have local administrative rights on the server.



NOTE

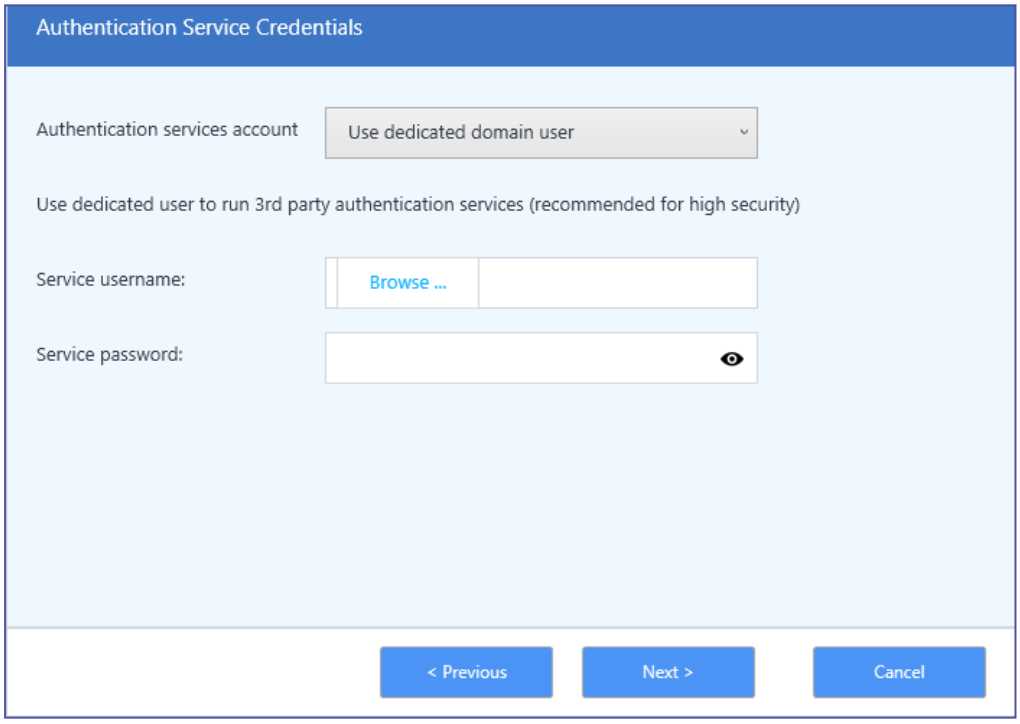
If you are running the installation using a Local Admin user and you insert a user that isn't a member of the local admin group, the installation will add it automatically to the group.

Click **Next** in the wizard

Authentication Service Credentials

Select a user to run authentication services on the RPA server. The available options are:

- **Use .\LocalSystem**: Use the same user that runs RPA services.
- **Use dedicated domain user** : i.e., a domain user that has been created especially for this purpose. For the highest possible security, the **dedicated domain user** option is recommended. When this option is selected, you must provide the credentials for the selected user. You can also **Browse** a user name.
- **Create new local user**: i.e., the installation package creates a new local user especially for the purpose of running authentication services (for Username & Password deployments only).

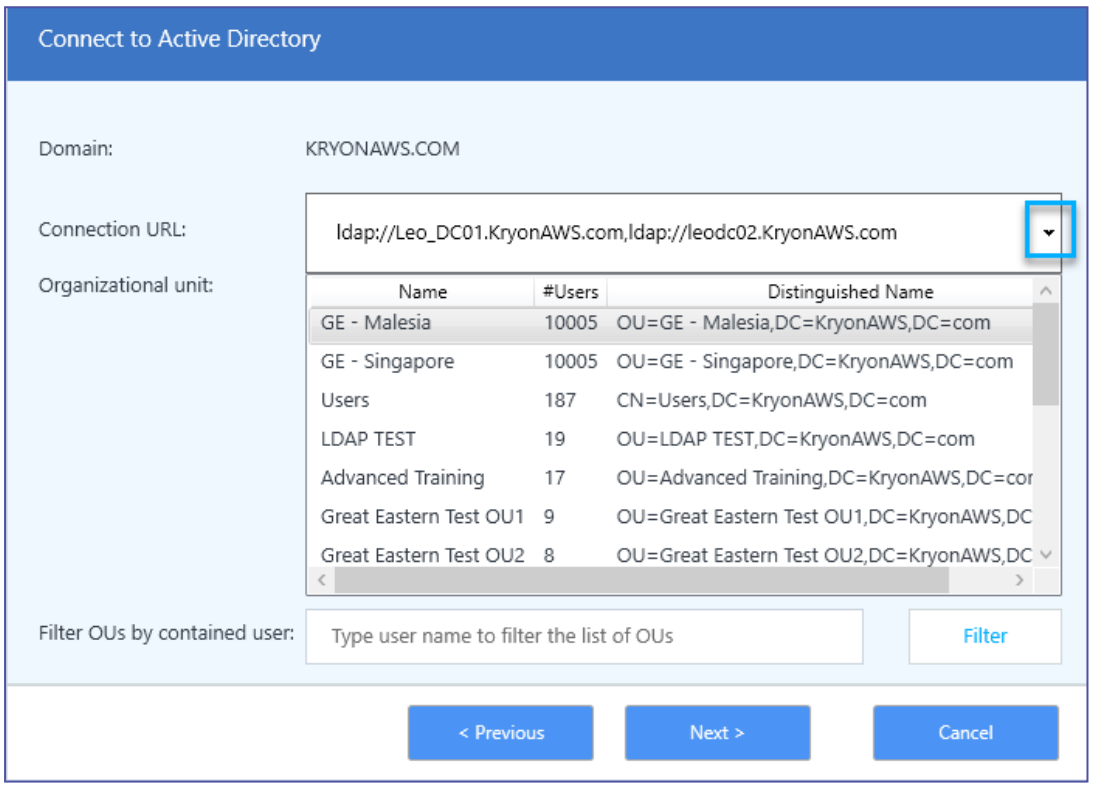


Click **Next** in the wizard

Before you proceed to the next step...

The next three steps are applicable to Kerberos deployments only. If you are installing with Username & Password authentication deployment, **skip to the step: Connect to Database**.

Connect to Active Directory



Domain: Auto-populated with the name of the domain on which you are installing the server

Connection URL: Auto-populated with the addresses of domain controllers located on the domain

- Initially, all available domain controllers are included in the **Connection URL**.
- Click the down-arrow to see the list of available domain controllers, and clear the checkboxes of any servers you don't want to include.

Organizational unit: Displays a list of all OUs in the Windows Active Directory. Select the OU(s) that contain your Kryon users.

- **NOTE**: Only OUs with users are displayed.

Filter OUs by contained user: (Optional) Type a user name in this field to filter the list of available OUs to show only the one that contains a specific user, then click the **Filter** button to activate the filter.

- **EXAMPLE:** You know that "RPAUser1" is one of your Kryon users, but you can't remember which OU they are in. Simply type "RPAUser1" in this field and click **Filter** to see only the OU that contains that user.

BEST PRACTICE

Managing Kryon users

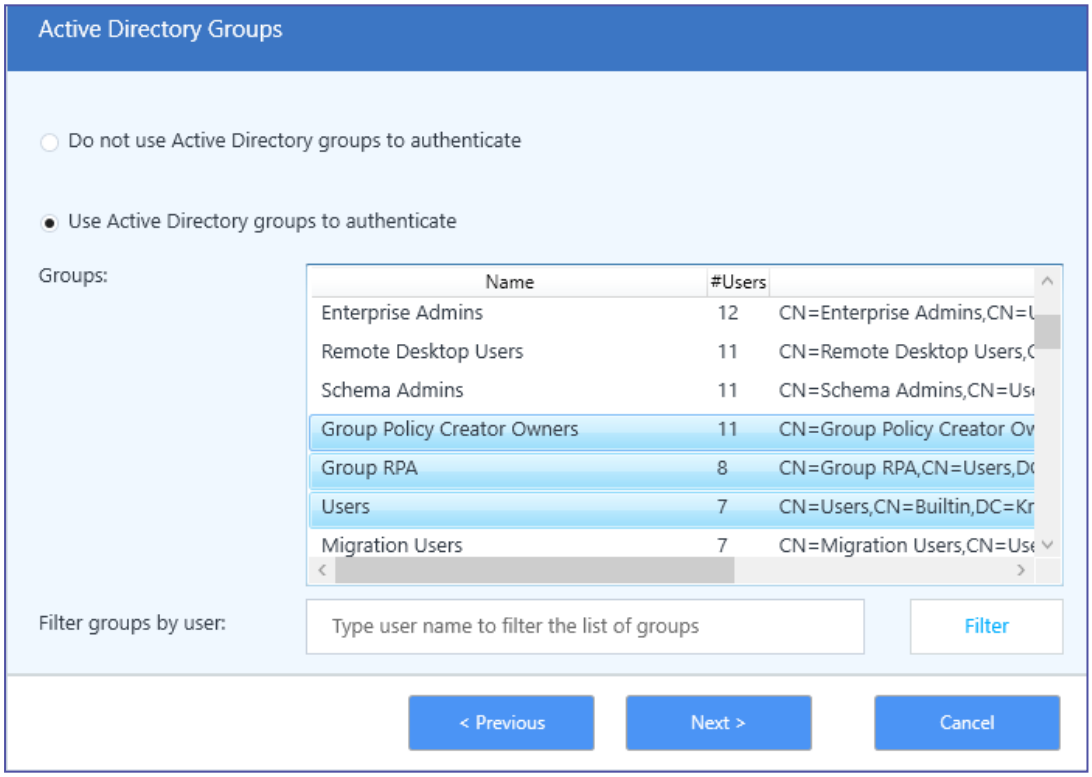
It's important to limit the users synced into the Kryon database to actual Kryon users.

Click **Next** in the wizard

Active Directory Groups

Select the relevant option:

- **Do not use Active Directory Groups to Authenticate**
- **Use Active Directory Groups to authenticate**:
  - Only the groups that belong to the previously selected OU are available.
  - Select the relevant group(s) to enable authentication by group(s).
  - Select **Filter** to filter Active Directory Groups by user.
    Filter OUs by contained user: (Optional) Type a user name in this field to filter the list of available AD to show only the one that contains a specific user, then click the **Filter** button to activate the filter.



Click **Next** in the wizard

Authentication Platform Security

KEYTAB generation: Select the option by which you will provide the KEYTAB file required for Kerberos.

- Option 1: **Provide KEYTAB file post installation**
- Option 2: **Use an existing KEYTAB file**
- Option 3: **Generate a KEYTAB file**

NOTE

When installing Kryon with multiple RPA servers (High-Availability mode), you must generate a **single KEYTAB file applicable to all servers.** This KEYTAB file must then be copied to each server and/or pointed to in each server's installation.

Option 1: Provide KEYTAB file post installation

Select this option to skip providing a KEYTAB file at this point.

If you use this option, a Domain Administrator must generate/provide a KEYTAB file post installation and move it to the required file path before using Kryon RPA. Please note that the installer provides you the option to easily copy the required KEYTAB commands.

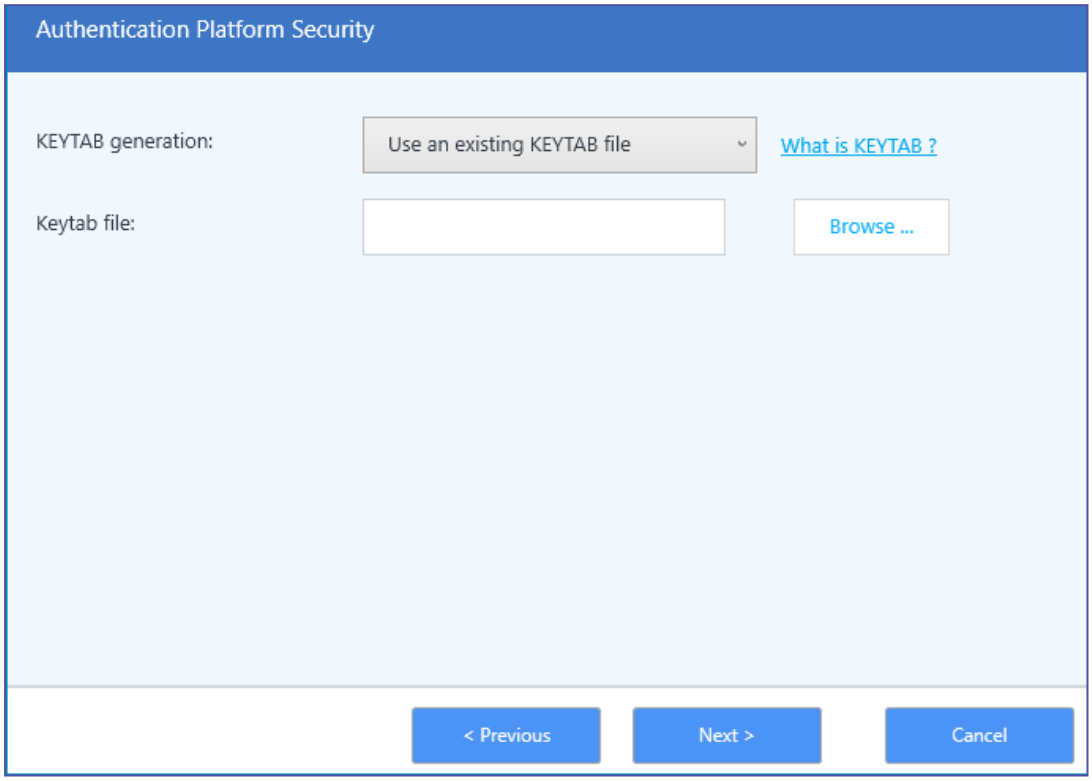
Copy command to clipboard / Save command to a batch file:Use one of these options to generate the script that allows you to generate a KEYTAB file later.

See Generating a KEYTAB file.

Option 2: Use existing KEYTAB file

Select this option if a KEYTAB file has been previously generated for this KryonRPA installation.

Enter or browse to the KEYTAB file.



Option 3: Generate a KEYTAB file

Select this option to generate a KEYTAB file during installation.

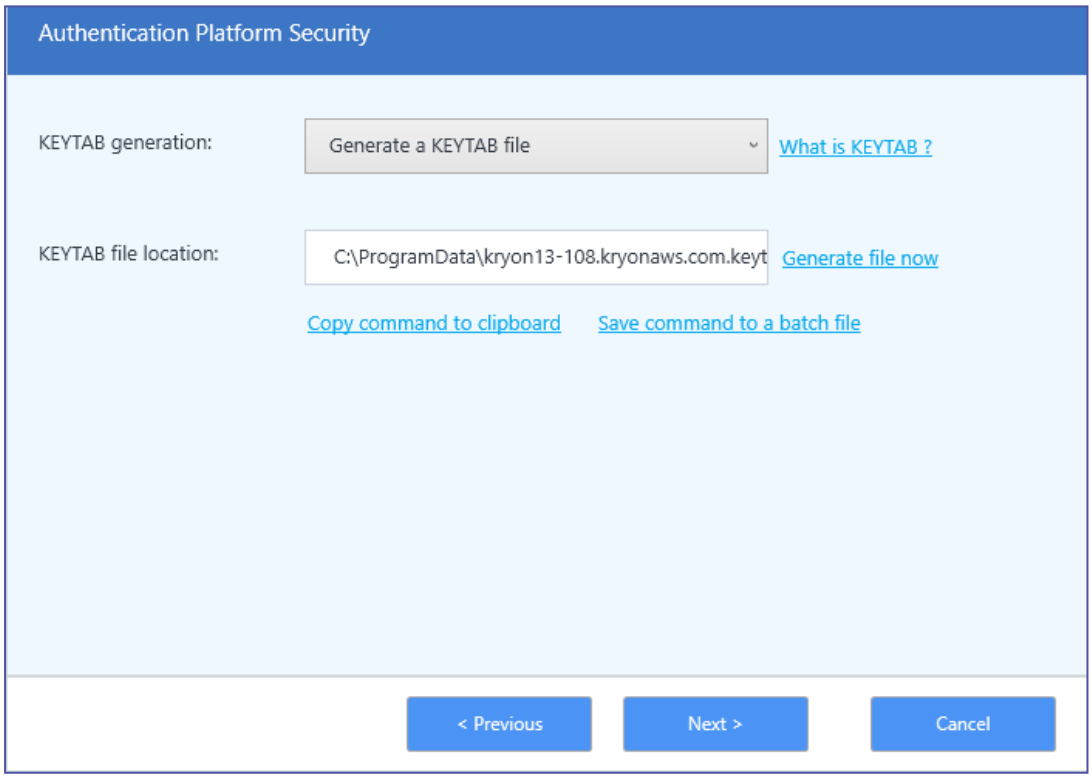
KEYTAB file location: This field is auto-populated with the location at which the KETYAB file will be generated.

See Generating a KEYTAB file.

You can click **Generate file now** to generate the KEYTAB file in real time.

- Using this option ensures that the KEYTAB file will be successfully generated prior to proceeding with installation.
- Upon successful generation of the KEYTAB file, the screen will automatically change to the **Use existing KEYTAB file** option, and the location of the KEYTAB file will be automatically populated.

Copy command to clipboard / Save command to a batch file: Click one of the options to generate the script for the KEYTAB.



Click **Next** in the wizard

Connect to Database

Option 1: Install local SQL Server

Select this checkbox if you want the installation package to automatically install a local instance of Microsoft SQL Server 2017 Express.

> **NOTE:** Not recommended for production environments.

When selected, you'll be required to **enter the password** you want to use for the **sa** (superadmin) user (this value defaults to `Kryon2020!`).

> **NOTE:** This option will not be visible if a local SQL instance is already installed.

Option 2: Configure the connection to your database server

Database server/port: You can identify the database instance on which the application database was created either by:

- entering the server name and instance name (syntax: `server_name\instance_name`); ***or***
- by selecting the network port used for communication with the database server

Encrypt DB: In case your database is secured, check this box to allow the connection.

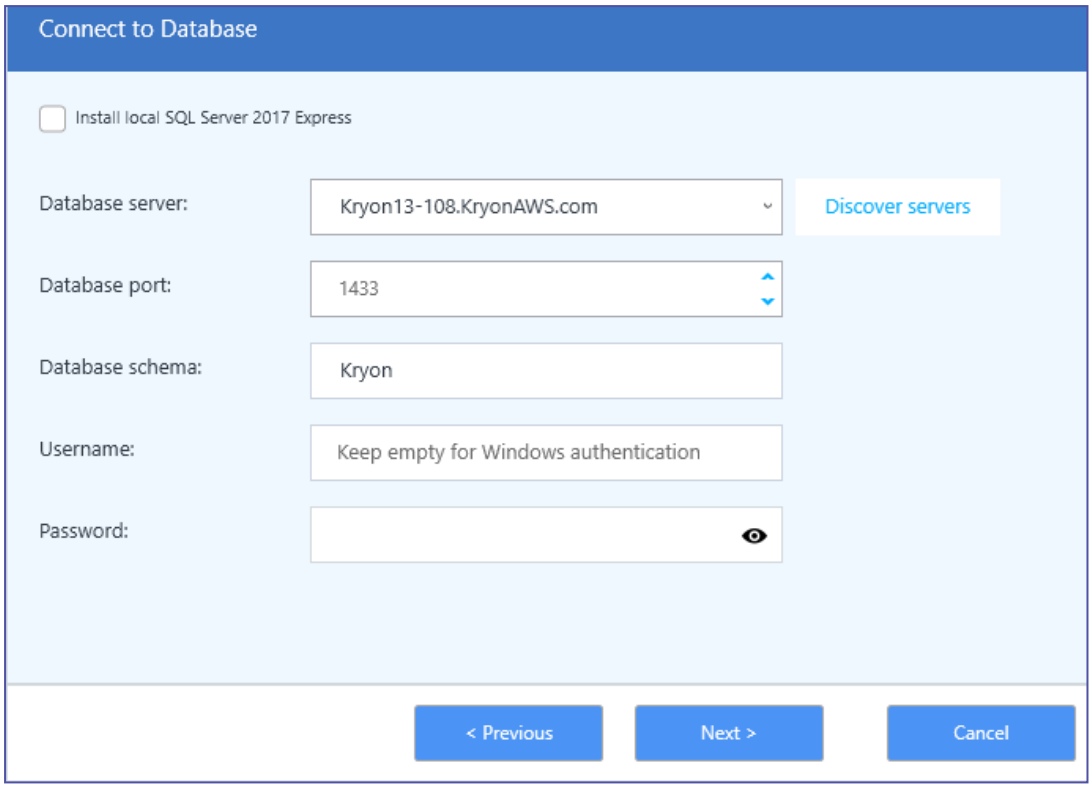
Alternatively, click **Discover servers** to identify all database instances on the network and to select the correct instance from the list.

Database schema: Enter the name you want to give the Kryon application database if not already created. Otherwise, type the name of the existing database schema.

Username & Password:

- If you selected **SQL authentication** when you created a login to the SQL server, enter the login name and password created for the Kryon database server.
- If you selected **Windows authentication** when you created a login to the SQL server, leave these fields empty.

  > **NOTE:** The current in use "Windows authentication" user must have access to database. See Minimum and recommended permissions to access database.



Click **Next** in the wizard

RPA Authentication DB

Database schema: Enter the name you want to give the authentication database if not created yet. Otherwise, type the name of the existing database schema.

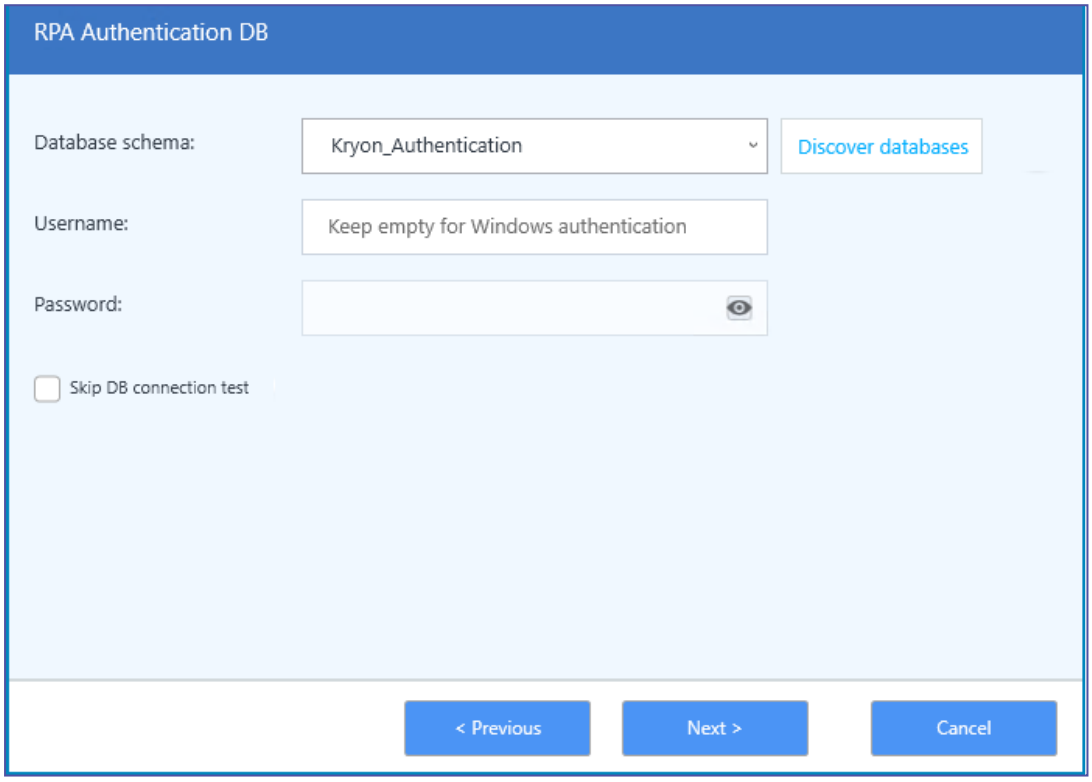
- You can use the **Discover databases** tool:
  1. Click **Discover Database**
  2. The dropdown list will be populated with all databases on the SQL Server instance
  3. Select the correct database from the list

Username & Password:

- If you selected **SQL authentication** when you created a login to the SQL server, enter the login name and password created for the Kryon database server.
- If you selected **Windows authentication** when you created a login to the SQL server, leave these fields empty

- If you selected the option to install a local instance of SQL Server Express in the previous step, these fields will be disabled and automatically be set to the same values as entered in that step.

By default, when you click **Next**, the installation package validates the database connection using the information you entered. Check the **Skip DB connection test checkbox** to skip.



Click **Next** in the wizard

Keycloak default user credentials

The installation package automatically creates 2 users for use with the Kryon authentication platform (also referred to as Keycloak). This screen gives you the option to change the default credentials for these users.

AuthAdmin: The administrator of the authentication platform; has permissions to manage user authentication and credentials.

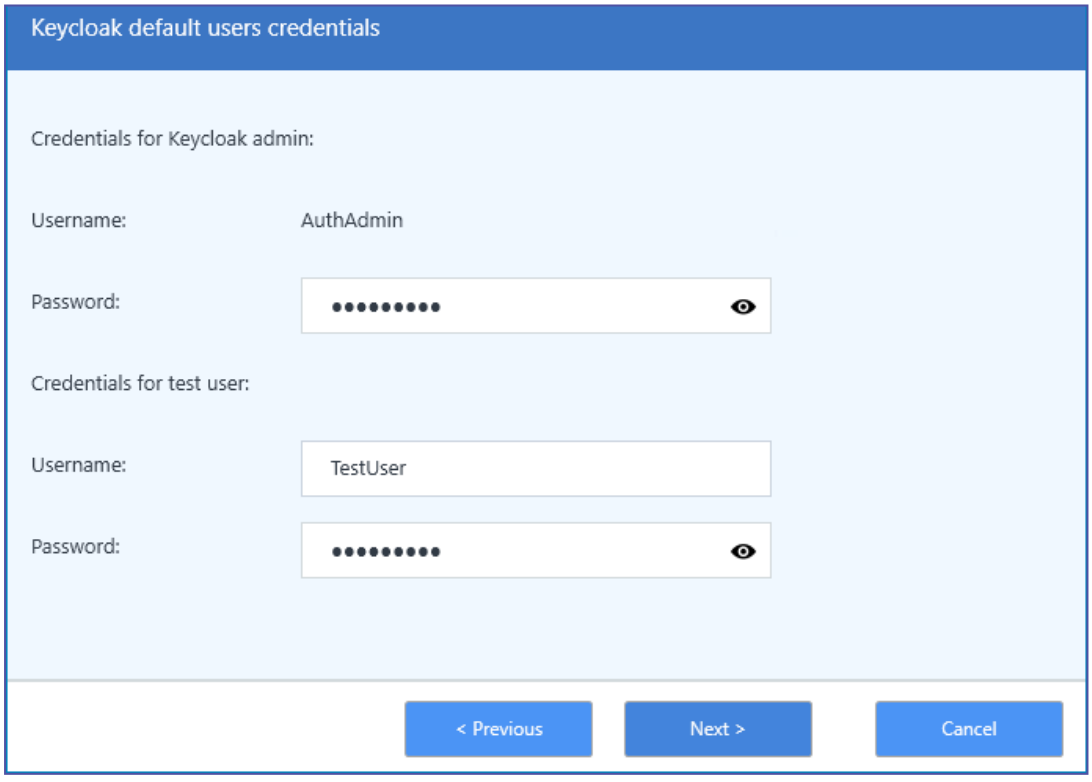
- You can change the password for this user from its default value of `Kryon123`. Changing the password is recommended for RPA System Hardening and Vulnerability Management

> **NOTE:** the username for this user cannot be changed

Test user: A user that can be used for testing and troubleshooting your authentication platform setup.

- You can change the username for this user from its default value of `TestUser` and/or its password from its default value of `Kryon123!`.

> **NOTE:** Changing the passwords in this step is recommended for RPA System Hardening and Vulnerability Management

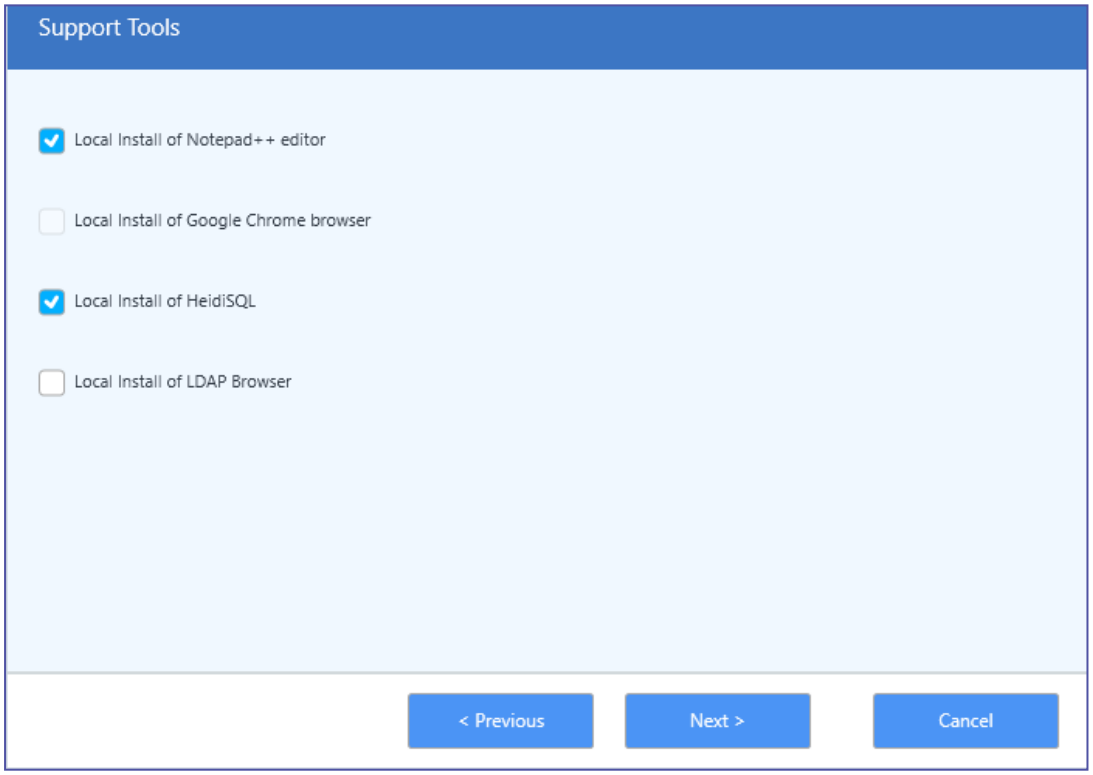


Click **Next** in the wizard

Support Tools

Select to install any or all of the optional support tools:

- **Notepad++ editor:** Handy editor for making any required changes to configuration files, etc.(Notepad++ documentation)
- **Google Chrome browser:** Supported browser for accessing the Kryon Console
- **HeidiSQL:** Database management tool, allowing you to work with your databases if you elect not to install Microsoft SQL Server Manager (HeidiSQL documentation)
- **Softerra LDAP Browser:** Tool for browsing and analyzing LDAP directories (Softerra LDAP Browser documentation)
  Note: This option is visible/enabled only if you are installing with Kerberos authentication



NOTE

If one of these tools is already installed on your server, its checkbox will be disabled.

Click **Next** in the wizard

Components to Install

Review the list of components to be installed, and click **Install** to begin Kryon RPA Server installation.

Executing Installation

The installation will run and the computer may prompt you to restart.

Following restart, the installation script will automatically resume.

When finished, the following message appears:
Kryon RPA Server is ready for use or, **required Reboot**.

NOTE

In case of a "The system administrator has set policies to prevent this installation" error message, follow the troubleshooting instructions here.

Done!

Take me to Clients Installation.

Kryon RPA Clients Installation

RPA Clients Installation Steps Overview

Follow these steps to install Kryon clients (unattended robots, attended robots, Kryon Studio):

1. Running client installation package
2. Configuring client connection to the Kryon RPA Server
3. Configuring client connection to Seq (centralized logging)
4. Enabling unattended robot mode/LogonExpert (for Unattended automation)
5. Making sure Kryon Browser Extension Connector is enabled

Optional configurations:

- Changing Kryon Studio language to Japanese
- Configuring Task-Rerun in case of Robot unexpected failure

Running the Client (Robot and Studio) Installation Packages

Before you start

To be able to use Java Advanced commands (as part of Kryon Studio), you need to have some Java elements setup properly so you can run the Kryon Java Bridge Script.

See Installing Java Bridge to make sure you have it configured right.

Run the Client MSI package

Run the relevant Client MSI installation package (Robot or Studio) generated by the RPA Installation wizard (MSI/WiX MSI) on the client machines. The MSI package contains the relevant client configurations.

Note: In client installation (Robot/Studio), make sure to enable the **Kryon Connector Browser Extension** when prompted. If you install Chrome/Firefox after the clients installation is complete, you need to manually enable the connector for the browsers.

You are Done!

Otherwise > >>

Run the client .exe files

If you didn't generate the Client MSI Package or you don't want to use it, you need to:

1. Manually configure the client.exe files and then run them.
   See Configuring Connection to Server
2. Configure client connection to SEQ
3. Configure non-default ports in SSL/TLS deployment

What else can you do in here?

By default, a Kryon Robot is installed as an attended robot. You can change this configuration from attended to unattended.

See Enabling Unattended Robot Mode.

Configuring Connection to Server

Follow these steps to configure the client's connection to the RPA server:

1. With a text editor, open the following configuration files –
   - For robot clients:
     `C:\Program Files\Kryon Robot\Config\appSettings.config`
   - For Kryon Studio:
     `C:\Program Files\Kryon Studio\Config\appSettings.config`
2. Find the line that begins: `<add key="MainServerNames"`, and change the value to the FQDN of the RPA server (full computer name).
   - The full line should now read: `<add key="MainServerNames" value="<FQDN of the RPA Server>" />`
3. **Ports**: If the server was installed using the default ports, the following values do not need to be changed.

   If you opened non-default ports when you installed the server, change the values of the following parameters:
   - `<add key="NetComPort" value="<server port number used for Net.TCP Port>" />`
   - `<add key="HttpComPort" value="<server port number used for HTTP Port>" />`
   - `<add key="HttpsComPort" value="<server port number used for NGINX Port>" />` (relevant to TSL/SSL only)

See Option to configure the client .exe file parameters for Robot silent installation

Option to configure the client .exe file parameters for Robot silent installation

By default, the Client MSI is automatically generated with all the relevant attributes. In case you need to override or modify any parameters, you can run the .exe file if the client installation through the command line and modify the desired parameters.

Open the command line and run the .exe file in the following format:

```
"[InstallationFile path]" [Parameters]
```

Example: `client.exe INSTALL_UPDATER=false HTTP_PORT=443`

Available Robot/Client Parameters

Parameter	Default Value
INSTALL_FOLDER:	c:\program files\
ADD_TO_STARTUP	true
INSTALL_UPDATER	true
INSTALL_PYTHON	true
INSTALL_JAVA_ACCESS_BRIDGE	false
INSTALL_WATCHDOG	true
REMOVE_LOGON_EXPERT	false
REMOVE_MIRROR_DRIVER	true/false
CLUSTER_NODES	
DISCOVERY_PORT	80
NET_COM_PORT	8082
HTTP_COM_PORT	8081
HTTPS_COM_PORT	8083
NGINX_PROTOCOL	http/https
HTTP_PORT	80
LEO_SERVER	Server FQDN

UPDATE_SERVER_FQDN	Server FQDN
UPDATE_DECRYPT_PASSWORD	
DEPLOYMENT_TYPE	attended/unattended
INSTALL_LOGON_EXPERT	true/false
INSTALL_MIRROR_DRIVER	true/false
ENABLE_JAVA_MANAGER	true/false

Configuring Client Connection to Seq

Follow these steps to configure the client's connection to Seq (centralized logging):

1. With a text editor, open the following configuration files –
   - For robot clients:
     `C:\Program Files\Kryon Robot\LogBeat\LogBeatConfig.json`
   - For Kryon Studio:
     `C:\Program Files\Kryon Studio\LogBeat\LogBeatConfig.json`
2. Find the line that reads:

   ```
   "SEQUri": "{NGINXProtocol}://{NGINXServer}/seq",
   ```

   and change it to read:

   ```
   "SEQUri": "http://FQDN_RPAServer/seq",
   ```

Enabling Unattended Robot Mode/LogonExpert

Enabling unattended robot mode

By default, a Kryon Robot is installed as an attended robot. Follow these steps to configure it as an unattended robot:

1. With a text editor, open the file:

   ```
   C:\Program Files\Kryon Robot\
   [version#]\Config\appSettings.config
   ```

2. Find the line that reads: `<add key="RunAutomationEnabled" value="False" />`, and change the value to `True`

- The full line should now read: `<add key="RIllegal character unAutomationEnabled" value="True" />`

Enabling LogonExpert

If the unattended robot will be permitted to unlock locked Windows sessions in order to run tasks, follow these steps to enable LogonExpert:

1. In the same file, find the line that reads: `<add key="EnableLogonExpert" value="False" />`, and change the value to `True`
   - The full line should now read: `<add key="EnableLogonExpert" value="True" />`

-Take me to the relevant step in the RPA Installation Guide-

Upgrading the RPA Server and Clients

Upgrading the RPA Server

Follow these steps to upgrade from an earlier version to **Kryon20.9.8**.

Each time you click a step it will take you to the relevant section in the guide. **At the end of the target section** you'll find a cross-reference "**-I came here while upgrading, take me back to the upgrading steps overview-**". Click this cross-reference to get back here.

1. Stop all the Kryon RPA Services
2. Back-up current version installation and database
3. Configure current SQL instance to ensure support for new version (**relevant only if your current version is 19.1.3 or above**)
4. Prepare the Kryon database for upgrade (**relevant only if your current version is below 5.25.0**)
5. Uninstall the current version of the Kryon RPA Server through Windows Control Panel.
6. Make sure that OpenSSL in uninstalled. If not, uninstall it manually like you would normally do.
   NOTE: This step is relevant when upgrading from any version prior to 20.9.
7. Open network ports if the default ports aren't relevant to you (check for changes from earlier versions)
8. Remove the current Console configuration (**relevant only if your current version is 19.3 or below**)
9. Go to Programs and Features and make sure that OpenSSL is uninstalled (**relevant only if your current version is 19.x or 20.3.x**)
10. Install the Kryon RPA Server by following the standard installation procedure while taking into consideration that the database version will also be upgraded.
    - See Upgrading the database version procedure (**Relevant to version 19.5 and later**)
11. Perform a one-time user migration procedures:
    a. Migrate users to the new authentication platform (**relevant only if your current version is 19.1.3 or below**)
    b. Encrypt the Credentials Vault (**relevant only if your current version is 19.3 or below**)

12. If you are upgrading from Console to ConsoleX, make sure to review the information below first:
    About upgrading from Console to ConsoleX
    Then, if you decide yo upgrade, contact Kryon support team for further instructions.

Upgrading the RPA Clients

Starting from Client version 19.5, you can automatically deploy software updates to Robots and Studio, on client machines. For more information, see Automatic Client Update.

If you are updating from a version before Client version 19.5, follow these steps:

1. Uninstall the current versions of Kryon attended/unattended Robots and Kryon Studio, as applicable, through Windows Control Panel.
2. Follow the regular client installation workflow to install and configure the new version of Kryon clients.

Backup Current Version & Database

Back up current version installation

1. Copy the current Kryon server install folder to a different location (either locally on a different machine)
   - By default, the server files are installed to the folder:
     - Up to v19.1.3: `C:\Program Files\Kryon Application Server`
     - For 19.3 and above: `C:\Kryon`

> **TIP**
>
> Save storage space by compressing the backup.

2. For 19.3 and above, backup KEYTAB file (for Kerberos authentication only) from C:\ProgramData.
3. For 19.3 and above, backup security certificate files (SSL/TLS) from C:\ProgramData.

Back up Kryon database

1. From SQL Server Management Studio, connect to the database server.
2. In the Object Explorer, right-click the Kryon database and select **Tasks > Back Up**.
3. Give the **Backup set** a name and set the **Destination** to which the backup will be saved.

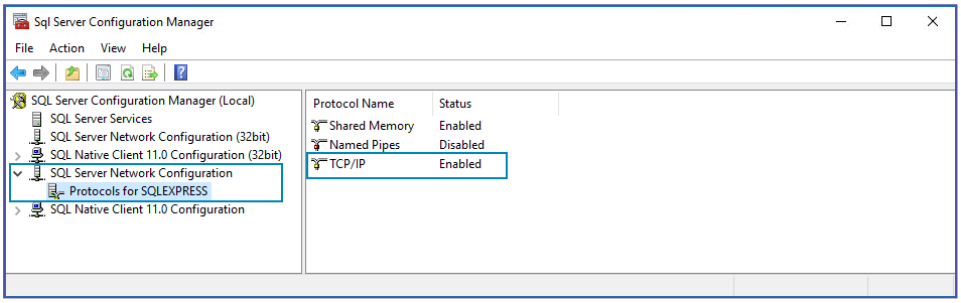
-I came here while upgrading, take me back to the upgrading steps overview-

Configure Current SQL Instance

If your current version is 19.1.3 or below, follow these instructions as part of the upgrade procedure. Otherwise, this procedure isn't relevant to your upgrade.

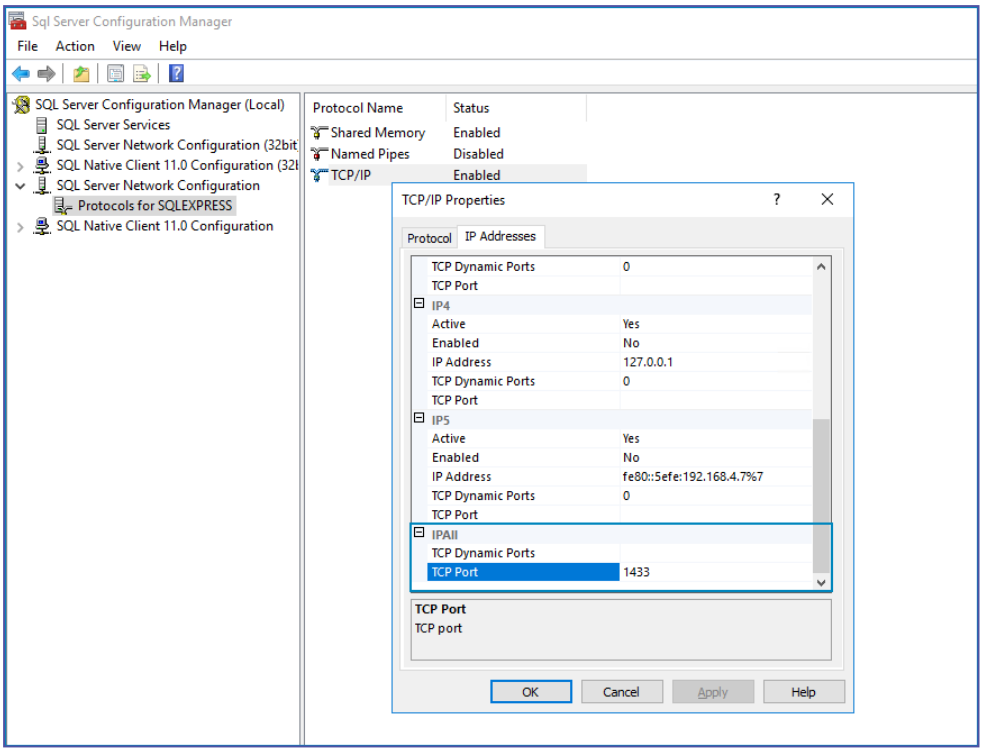
Open **SQL Server Configuration Manager** (a tool installed with SQL Server), and follow these steps to configure the database instance:

1. Enable and configure **TCP/IP**
   a. Under **SQL Server Network Configuration > Protocols for {Instance Name}**, enable **TCP/IP**

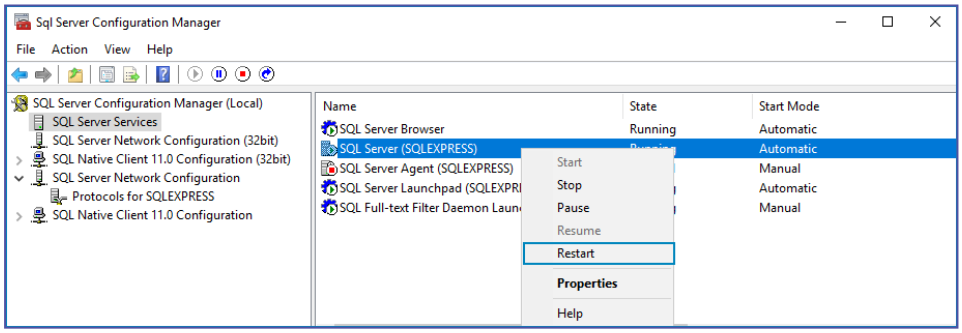


   b. Double click **TCP/IP** to open its configuration
   c. On the **IP Addresses** tab, scroll down to **IPAll**
   d. Remove the `0` value from **TCP Dynamic Ports** (so that it now appears blank)
   e. In **TCP Port**, enter the port number used to communicate with this database instance
      - To use the default value, enter `1433`

f. Click the **OK** button to save your changes



2. In **SQL Server Services**, right-click the **SQL Server** service for the relevant instance and select **Restart**

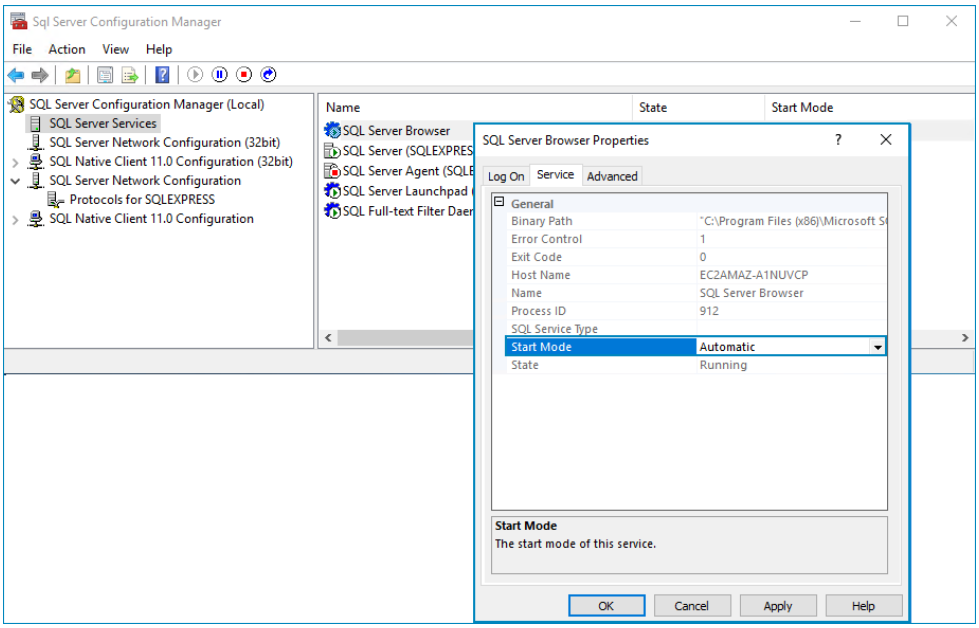


3. Configure and start the **SQL Server Browser**

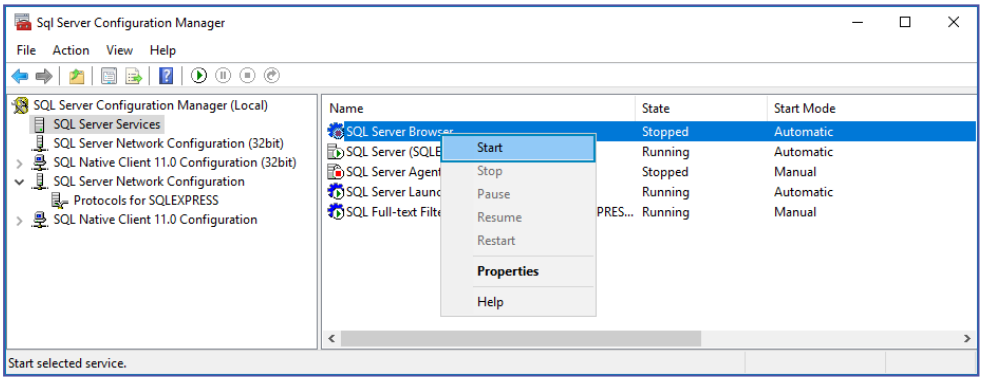
   a. In **SQL Server Services**, double click the **SQL Server Browser** service to open its configuration

   b. On the **Service** tab, set the **Start Mode** value to `Automatic`

   c. Click the **OK** button to save your changes



d. Right-click the **SQL Server Browser** service and select **Start**



-I came here while upgrading, take me back to the upgrading steps overview-

Prepare the Kryon Database for Upgrade

If your current version is below 5.25.0, follow these instructions as part of the upgrade procedure. Otherwise, this procedure isn't relevant to your upgrade.

Follow these steps to prepare the Kryon database for the new version:

1. Obtain the necessary database upgrade scripts from support team.
   - Run the following query on the database: `select * from LeoDBVersion order by 1 desc`. The result will be a list of Kryon server versions.
   - Email this result to you support team. The support team will send you the required database script(s).
2. Run the scripts on the database, one at a time and ***in numerical order***, from the earlier version to the newer version.

-I came here while upgrading, take me back to the upgrading steps overview-

Remove the Current Console Configuration

If your current version is 19.3 or below, follow these instructions as part of the upgrade procedure. Otherwise, this procedure isn't relevant to your upgrade.

Kryon RPA v19.3 introduced major changes to the structure of the IIS websites and applications that serve Kryon Console. For this reason, if you are upgrading from a version prior to 19.3, it is ***highly recommended*** that you delete the Console configuration applicable to prior versions and allow the RPA Server installation package to install Console with the new structure.

Follow these steps in **Internet Information Services (IIS) Manager** to remove the current Console structure:

1. In the left-side panel (**Connections**), under **Sites**:
   a. Right-click the **Console** site, and select **Remove**
   b. Right-click the **WebAPI** site, and select **Remove**

IMPORTANT

If you are upgrading from Console to ConsoleX, make sure to read about the implications and points of consideration before selecting this option.

See About upgrading from Console to ConsoleX.

-I came here while upgrading, take me back to the upgrading steps overview-

Upgrading the database version

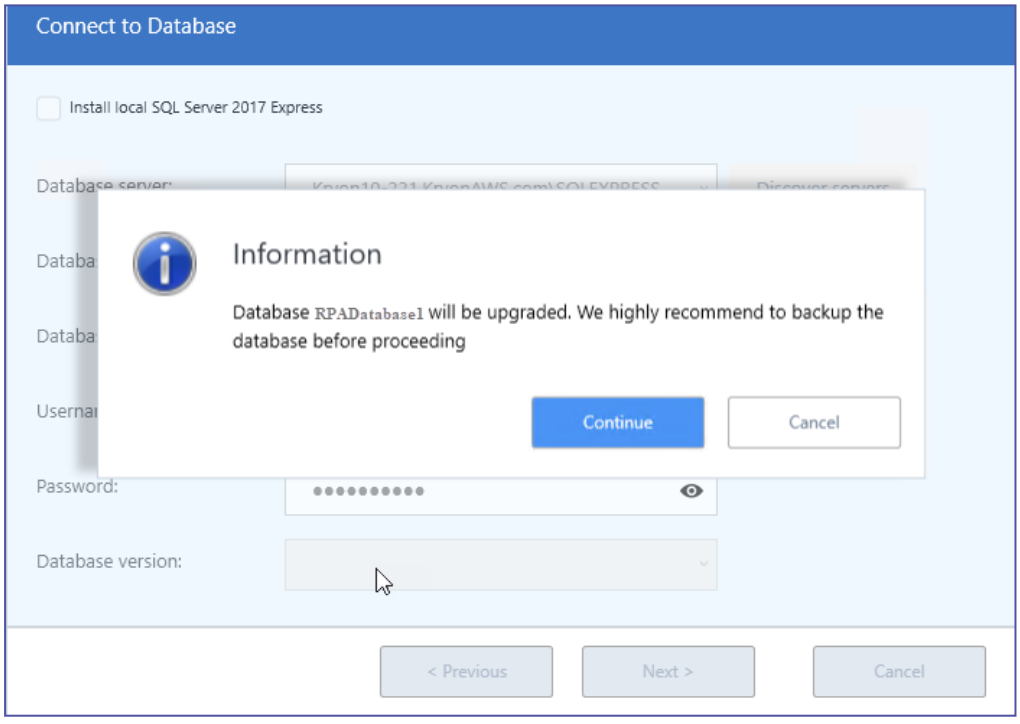
Starting from RPA version 19.5, you can perform an upgrade to the database through the RPA installation wizard.

During the RPA Server upgrade process, you'll reach the step in the wizard where you need to Connect to Database.

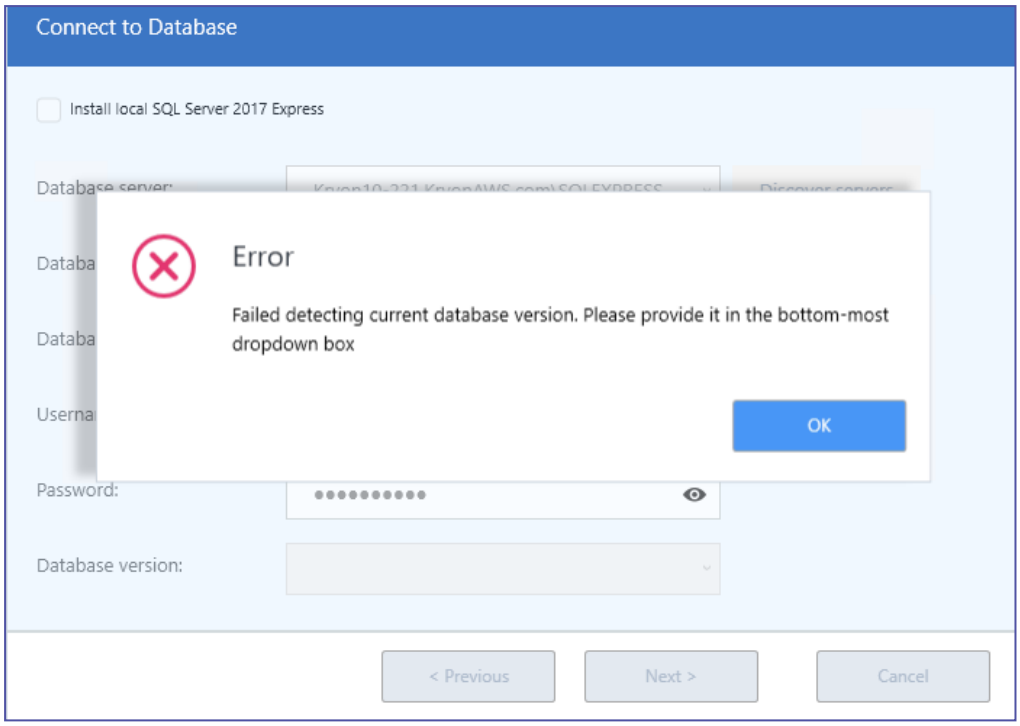
1. Once you insert the database schema, username and password, and you click Next, you'll receive the following message.
   Click **Continue**.

   What happens next depends on your current RPA version >
   If your current version is 19.5.0 and up, once you click Continue, the installer automatically performs the upgrade > you are done with this step. From this point, you can continue and follow the regular RPA Server installation procedure.

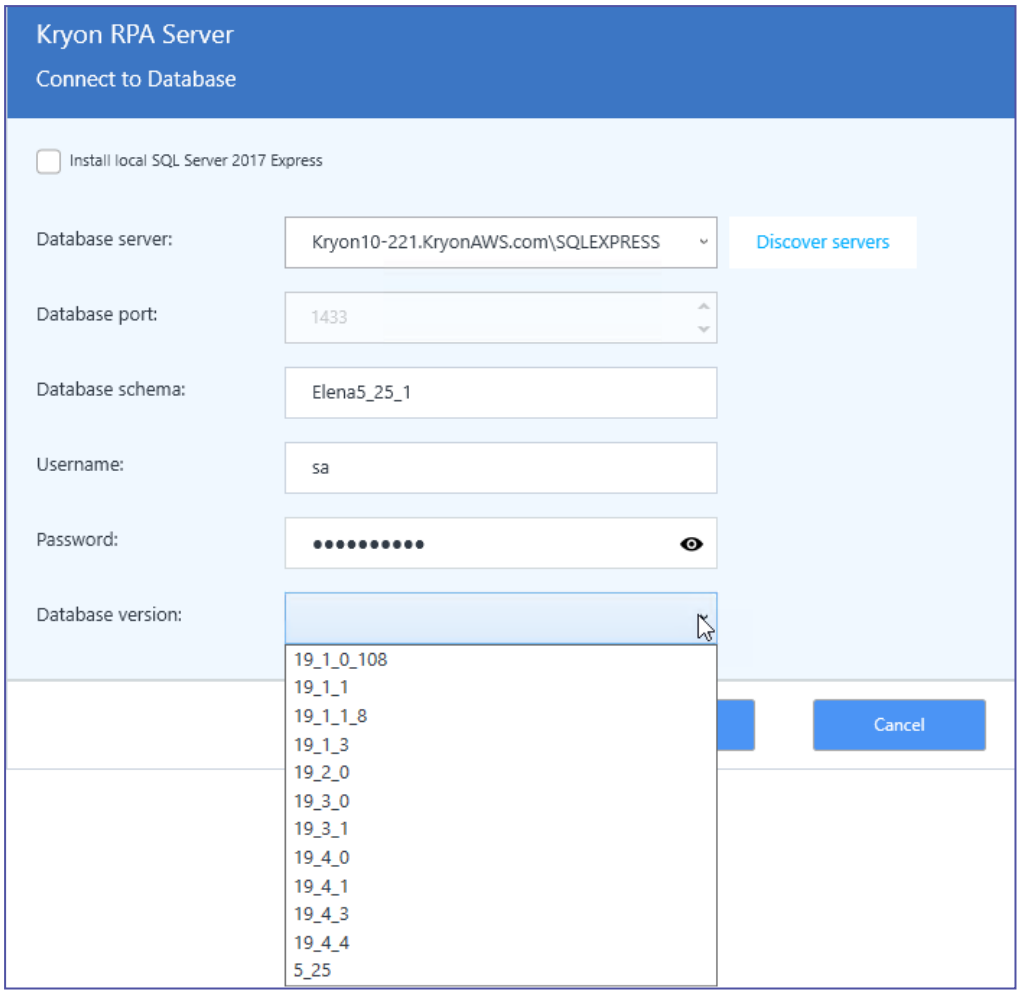
   Otherwise, continue to step 2.



2. The installer will attempt to look for a database version that matches the RPA version you are upgrading to. In an upgrade scenario, the expected result is an "error" since the current database version doesn't match the RPA version.
   Click **OK** to select your currently installed database version.



3. Select the currently installed database version from the drop-down list. Click **Next**.



4. Continue the RPA Server installation procedure.

-I came here while upgrading, take me back to the upgrading steps overview-

Migrating users to the new Authentication Platform

You only need to do this once!

Kryon RPA v19.3 introduced a new, robust, and flexible authentication platform. This topic describes the procedure for migrating your current Kryon users to the new platform.

If you have Kryon version 19.3 or above **before the current upgrade**, you can skip this step.

You need to follow this procedure when you upgrade from a Kryon version prior to 19.3 and:

1. If migrating from user-pass authentication: migration is mandatory
2. If migrating from Kerberos authentication: migration is mandatory in the following cases:
   a. You have robots defined and you want to save the user IDs assigned for each robot
   b. You have permissions defined in Admin, and you want to keep all the existing User IDs assigned with permissions
   c. You have a lot of different roles (for example: many Studio users) – using the migration tool will save you from having to assign roles (other that the automatic role assignment defined in Admin for new users)

To migrate Kryon users to the new authentication platform:

1. Configure user migration script options
2. Run the user migration script
3. Confirm successful migration

Step 1: Configure user migration script options

With Notepad++ (or another text editor), open the following file:
`{InstallFolder}\Support Tools\UsersMigrationTool\config.js`

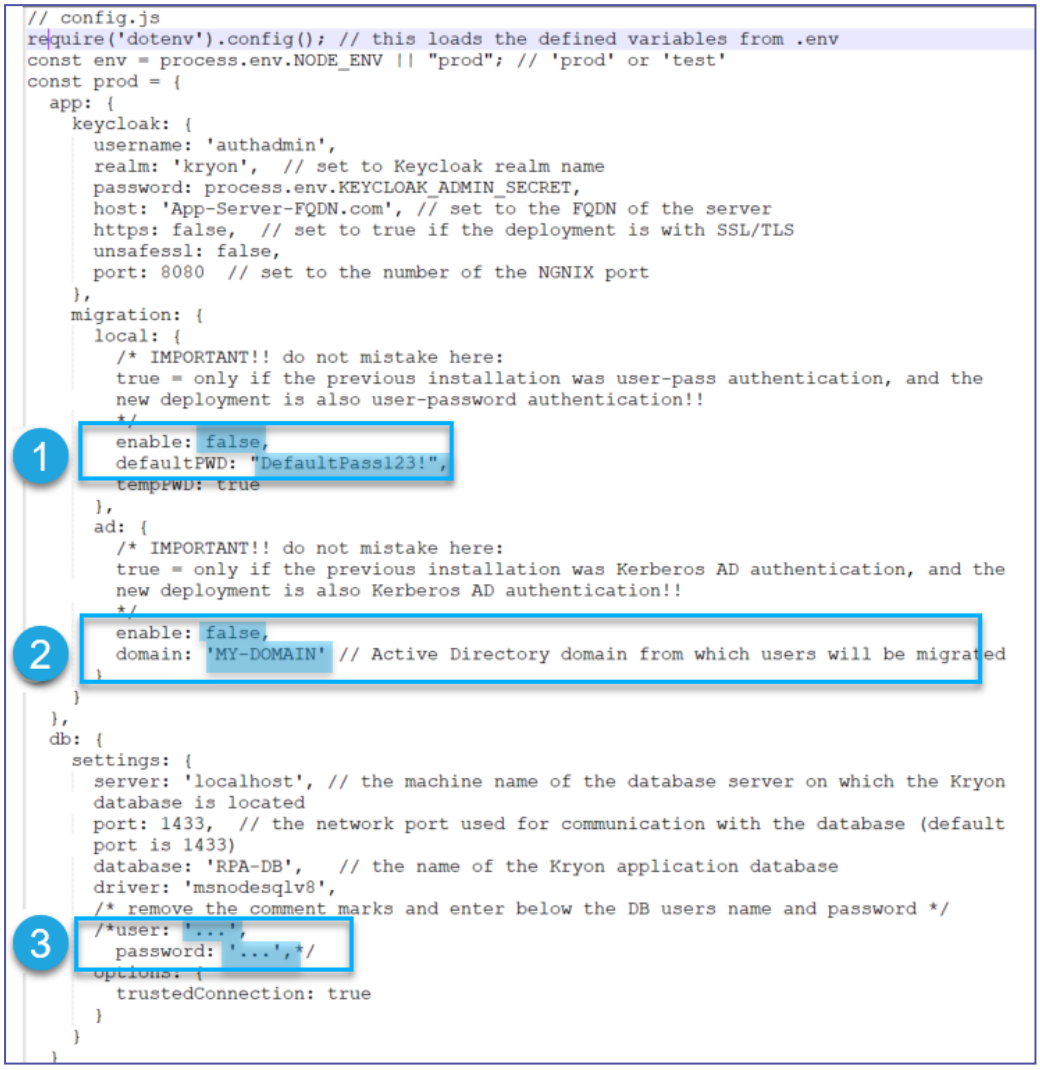
`TIPS:`

Narrow your focus...

In the `config.js` file, you'll set the options required for the user migration tool to run properly. Only the top half of the file is relevant to this mission. No need to pay any attention to the section below the line that reads: `const test = {.`

Keep the quotes...

When editing the file, be sure to keep the quotation marks for any value that currently appears within them.



1. Set migration option as follows for the **local:**
   enable: default is `false`
   - `true` = to migrate users from Kryon Admin (generally relevant to Username & Password deployments)
     IMPORTANT! Set to True only if the previous installation was user-pass authentication, and the new deployment is also user-password authentication.
   - `false` = to not migrate users from Kryon Admin
     defaultPWD: default is `DefaultPass123!` *(relevant only when local: enable = true)*
     Note: This is the initial password that will be set for all users when they are migrated from Kryon Admin to the authentication platform

2. Set the migration options as follows for the **ad:**
   enable:
   - `true` = you will be migrating users from Windows Active Directory (relevant to Kerberos deployments)
   - `false` = you will not be migrating users from Windows Active Directory
   - **domain***(relevant only when ad: enable = true)*
     - Active Directory domain from which users will be migrated
3. Set database options as follows:
   user and password:
   - Remove the `/*` characters from the beginning of the line that starts: `/*user`
   - Remove the `*/` characters from the end of the line that starts: `password`
   - Replace the ... characters in each of these 2 lines with the username and password of the (sysadmin) user authorized to access the Kryon database server.

Save your changes and close the file.

Step 2: Run the user migration script

1. Open a command prompt as administrator
2. Navigate to the drive on which the Kryon RPA Server is installed
3. Change directory to: `{InstallFolder}\Support Tools\UsersMigrationTool`
4. At the prompt, enter the following command:
   `{InstallFolder}\IDP\Modules\nodejs\node.exe migrate.js`

   As the script runs, you will see users being migrated. When it completes, you will be returned to the command prompt.

NOTE

No worries about warnings... but DO correct errors!

As the script runs, you may see warnings that looks something like the following:

```
warn:       Kryon AD users migration process skipped by config
(node:6072) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and
usability issues. Please use the Buffer.alloc(), Buffer.allocUnsafe(), or Buffer.from
() methods instead.
```

No need to worry about these warnings. The script should still run successfully.

On the other hand, a message marked error generally indicates that the script did not run as expected. Go back and check the options configured in Step 2 above.

Step 3: Confirm successful migration

When the script finishes running, confirm that users were migrated successfully by following these steps:

1. Log in to the **Kryon User Management Tool**
2. On the left navigation bar, click **Users**.
3. On the screen that opens, click **View all users** to see a list of all users in your organization. Use this list to confirm that your Kryon users were successfully migrated to the new authentication platform.

-I came here while upgrading, take me back to the upgrading steps overview-

Encrypt the Credentials Vault

You only need to do this once!

To provide an even higher level of security, Kryon added advanced encryption to the Credentials Vault. This topic describes the procedure for encrypting the Credentials Vault from prior versions. You need to follow this procedure only one time: when you upgrade from a Kryon version prior to 19.3.

If you were using a Kryon version 19.3 or higher **before the current upgrade**, you can skip this step.

CAUTION

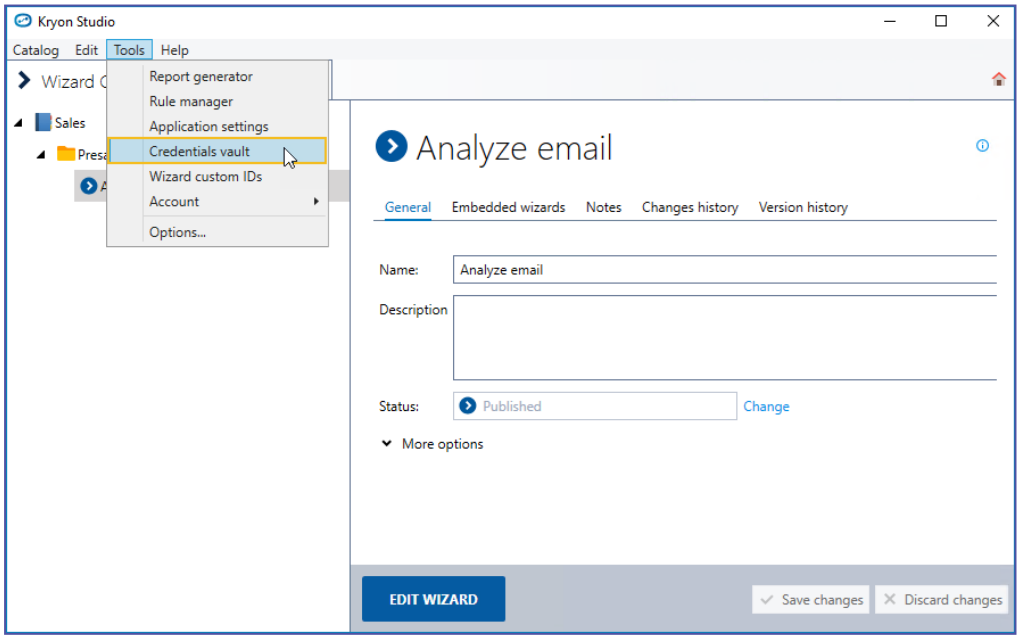
Avoid wizard failure!

Failure to encrypt the Credentials Vault will cause all wizards that utilize stored credentials to fail.

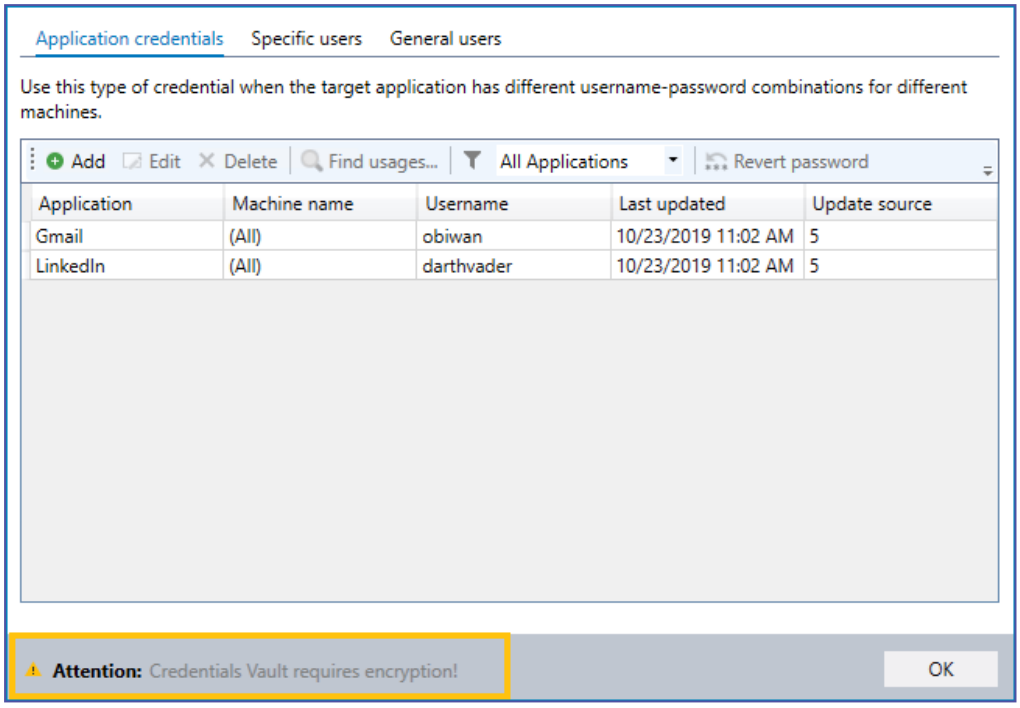
How do I know if the Credentials Vault was already encrypted?

To check if the Credentials Vault has been encrypted:

1. From the menu in Kryon Studio's main window, click **Tools > Credentials Vault**



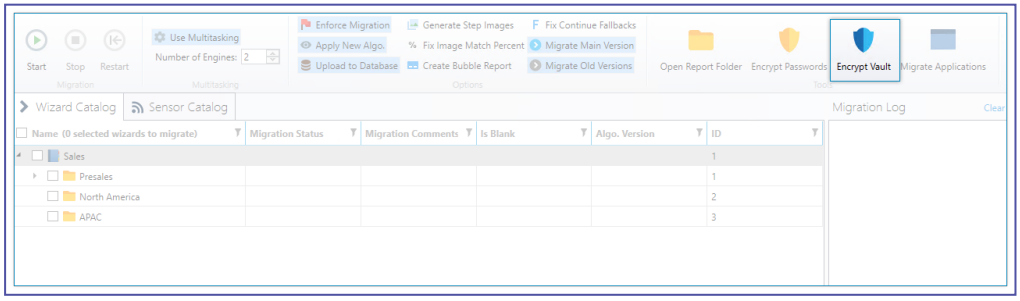
2. If the Credentials Vault requires encryption, a caution message will appear at the bottom of the Credentials Vault window



Running the Migration Tool to encrypt the Credentials Vault

To encrypt the Credentials Vault:

1. Close Kryon Studio
2. Navigate to `{InstallFolder}\RPA\Migration Tool 64bit`
3. Run the application `LeoScriptsMigrationTool.exe`
4. Log in a user with the Studio user role (to learn more about user roles, see the Kryon Admin User Guide – ***User Management: An Overview***)
5. In the ribbon, click the **Encrypt Vault** button



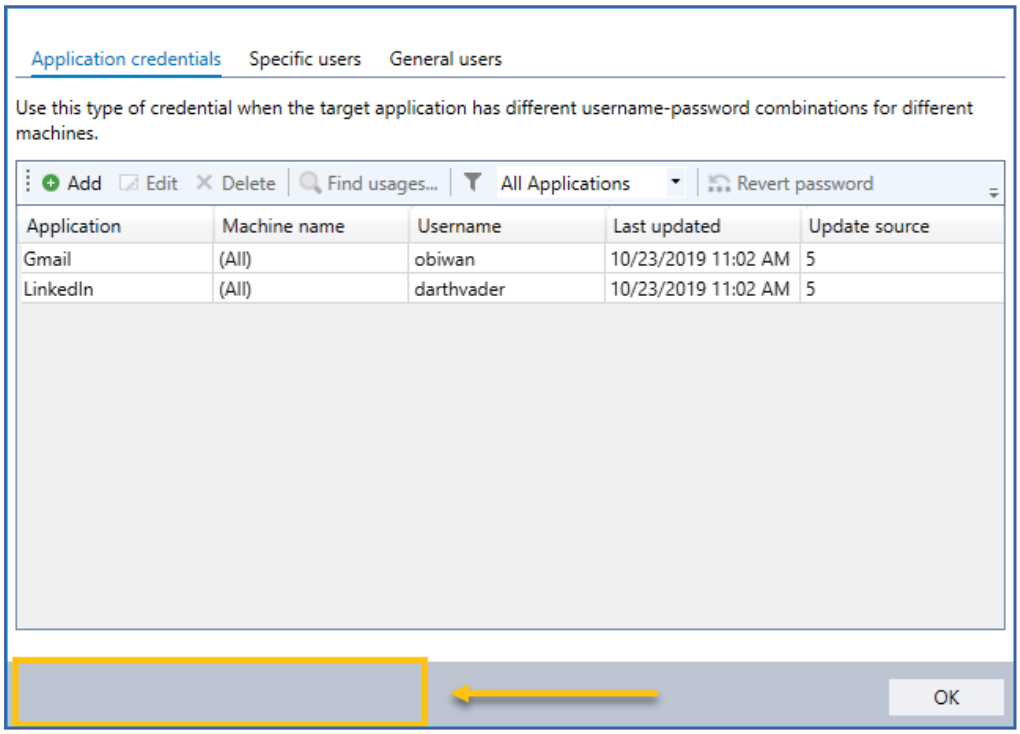
6. When the confirmation dialog appears, click the **Yes** button

7. The encryption process will begin, and its status will be displayed in the **Migration Log** pane (on the right-hand side of the window)
8. When the encryption process ends, confirm that it has completed successfully

Confirming successful encryption

To confirm successful Credentials Vault encryption:

1. Access the Credentials Vault from Kryon Studio, as described above
2. Check to be sure that the caution message no longer appears at the bottom of the Credentials Vault window



-I came here while upgrading, take me back to the upgrading steps overview-

Automatic Client Update

Starting from Client version 19.5.1 and onwards, you can automatically deploy software updates to client machines for Robot, Robot32, and Studio.

The procedure to deploy the update is simple. First, you download the updated files from the Kryon Updates Cloud. Then, you copy the files to their respective AutoUpdate destination folder (either Robot, Robot32 or Studio) on the RPA Server.

The deployment performs a silent install of the new version. No human intervention on the client machines is required.

The installation does not interfere if the robot is currently running a task. If a workstation is off, the update begins when it is restarted.

The automatic update mechanism handles more than one version at the same time. You can update client machines running different versions to the same new target version at one go.

Prerequisites

Client machines are upgraded automatically. However, you need to make sure you download and install .NET core 3.1 on all Robot clients machines before you run the Client-AutoUpdate.

How to automatically deploy software updates

TIP

Managing Versions

The files that you download and copy to initiate the update depends on the number of different versions running on your client machines.

If, for instance, all your machines are running on the same Robot version 19.1.2 and you want to update to version 19.5.8, you need to download these files:

1. `kryonrobot.19.5.2.to.19.5.8.wyu` (the update file from 19.5.2 to 19.5.8)
2. `kryonrobot.all.to.19.5.8` (the version file)
3. `wyserver.kryonrobot.wys` (the index file)

Now, say you also have some machines running Robot version 19.1.3, then, along with the files above you also need:

4. `kryonrobot.19.5.3.to.19.5.8.wyu` (the update file from 19.5.3 to 19.5.8)

and so on.

1. Based on the product you are upgrading (Robot, Robot32, Studio), download the Client-AutoUpdate files from the Kryon Updates Cloud as follows:
   a. The update file(s) for all the specific versions you require (for example, if some of your machines are running v19.5.2, others v19.5.3 and others v19.5.4, download `kryonstudio.19.5.2.to.19.5.8.wyu`, `kryonstudio.19.5.3.to.19.5.8.wyu`, and `kryonstudio.19.5.4.to.19.5.8.wyu`
   b. The product version file (for example, for Robot32, `kryonrobot32.all.to.19.5.8`)
   c. The product index file (for example, for Robot, `wyserver.kryonrobot.wys`)
2. Copy the files to the appropriate folder based on the product:
   a. **for Robot:** `C:\Kryon\AutoUpdate\Robot`
   b. **For Robot32:** `C:\Kryon\AutoUpdate\Robot32`
   c. **For Studio:** `C:\Kryon\AutoUpdate\Studio`

That's it. The update is all set!

-I came here while upgrading, take me back to the upgrading steps overview-

Rolling-back to Previous Version

If you want to rollback to the previous version of Kryon RPA Server, follow these steps:

1. a. If installation of Kryon RPA Server release 20.9.8 completed successfully, do the following, *otherwise,* skip to the next step:
    a. Stop **Kryon Services**
    b. Uninstall **Kryon RPA Server** release 20.9.8 through Windows Control Panel, *Add or Remove Programs*
2. **Ports**: if you opened additional ports for the new version, you can close them
3. Restore the Kryon database from the backup you made in Back up Kryon database
4. Reinstall the previous version (according to the installation instructions of the Kryon RPA Server version you are reinstalling)

TIP

If you need to access your previous configuration files, they are where you saved them in Backup Current Version & Database

APPENDICES

IN THIS CHAPTER:

Kryon Network Ports

Default port configuration

Kryon's default port configuration is as follows. Server-side ports are fully configurable, and you can the opportunity to specify them during RPA Server installation.

For standard deployments (without SSL/TLS):

Friendly name	Protocol	Server-side inbound port (configurable)	Client-side outbound port
HTTP port	HTTP	8081	dynamic
Net.TCP port	Net.TCP	8082	dynamic
NGNIX port	HTTP	80	N/A

For SSL/TLS deployments:

Friendly name	Protocol	Server-side inbound port (configurable)	Client-side outbound port
HTTPS port	HTTPS	8083	dynamic
Net.TCP port	Secured Net.TCP	8082	dynamic
NGNIX port	HTTPS	443	N/A
Discovery port	HTTP	80	N/A

NOTE: Only SSL/TLS v1.2 is supported.

Opening ports

You can open the relevant ports during the RPA Server installation by selecting the "open ports" check box.

If you miss the selection, you can open the ports manually.

Open the following ports in both the Windows Firewall and your hardware firewall to prepare your network for Kryon installation:

1. The ports listed in the relevant table above (or the port numbers you specified during RPA Server installation)
   Tip: Be sure to write down these port numbers; you will use them again!
2. **Port 8090** If you are installing with a multi-server configuration (i.e., with two RPA servers)

-Take me to the relevant step in the RPA Installation Guide-

-I came here while upgrading, take me back to the upgrading steps overview-

Preparing the Kryon Database Server

Preparing the Kryon Database Server consists of 2 main steps:

1. Install SQL Server Management Studio (if not previously installed); ***and***
2. Prepare SQL Server instance by following the instructions relevant to your situation:
   a. An SQL instance is not yet installed; ***or***
   b. An SQL instance is already installed

NOTES

- The supported database engine for the Kryon database server is SQL Server 2012 and above
- The Kryon database server can be installed on the same machine as the RPA server if machine resources are sufficient

Step 1: Install SQL Server Management Studio

SQL Server Management Studio is required in order to work with the Kryon database schema. If not yet installed:

1. Download Microsoft SQL Server Management Studio.
2. Run the installation package using the default installation options.

CAUTION

Be sure to restart if prompted!

You may be prompted to restart the sever after installation of SQL Server Management Studio. It is important to do so or an automatic restart will occur during RPA server installation.

Step 2: Prepare an SQL Server instance

The Kryon RPA Server utilizes 2 databases: the application database and the authentication platform database. Both of these database schema must reside in the same SQL Server instance (though it's perfectly fine if other schema also exist in this instance).

If an SQL Server instance is not yet installed

- You can choose for the Kryon RPA Server installation package to automatically install a local instance of Microsoft SQL Server 2017 Express. If you will elect this option, skip the remainder of this topic and proceed to RPA Server installation.
- If you wish to manually install SQL Server, follow the instructions in the Appendix Installing Microsoft SQL Server (Express Edition). Then, return here and follow the instructions for when an SQL instance is already installed.

If an SQL Server instance already installed

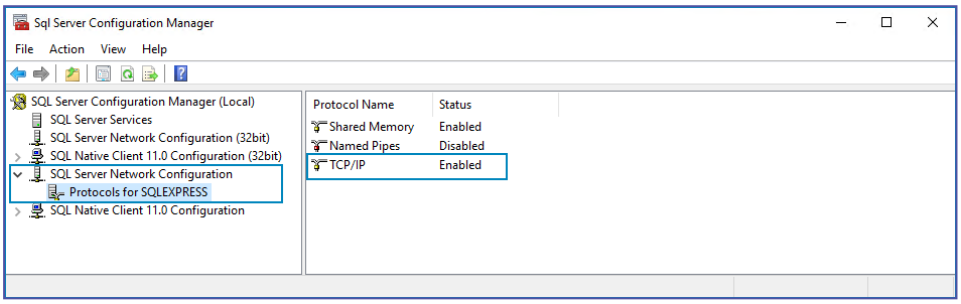
If an instance of SQL Server is already installed on a machine that will be accessible over the network to the Kryon RPA Server, proceed with the instructions in:

- Configuring the SQL Server instance
- Creating a login for the RPA server to access the database

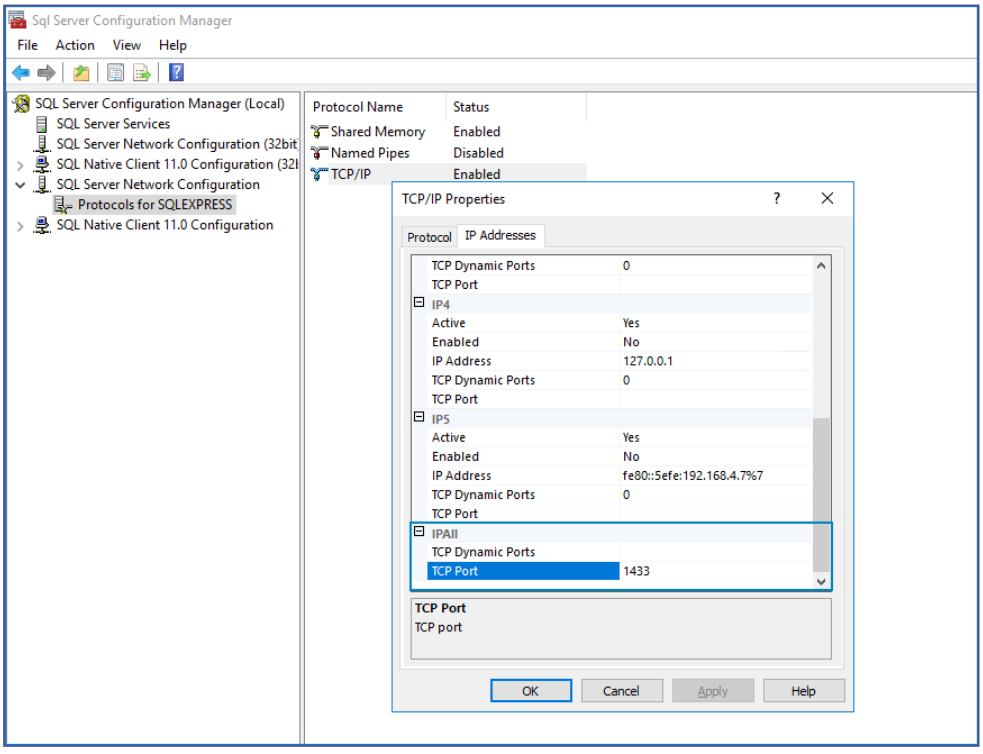
Configure SQL Server instance

Open **SQL Server Configuration Manager** (a tool installed with SQL Server), and follow these steps to configure the database instance:

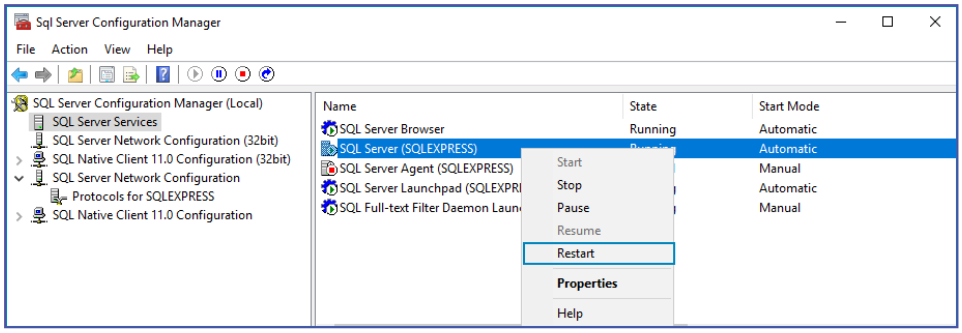
1. Enable and configure **TCP/IP**
   a. Under **SQL Server Network Configuration > Protocols for {Instance Name}**, enable **TCP/IP**



   b. Double click **TCP/IP** to open its configuration
   c. On the **IP Addresses** tab, scroll down to **IPAll**
   d. Remove the `0` value from **TCP Dynamic Ports** (so that it now appears blank)
   e. In **TCP Port**, enter the port number used to communicate with this database instance
      - To use the default value, enter `1433`
   f. Click the **OK** button to save your changes



2. In **SQL Server Services**, right-click the **SQL Server** service for the relevant instance and select **Restart**

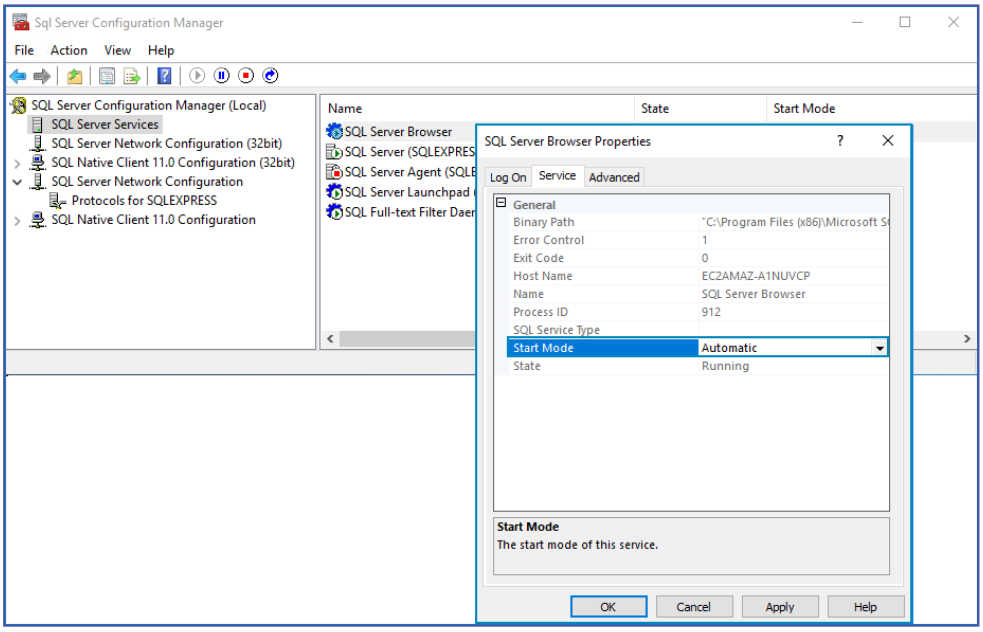


3. Configure and start the **SQL Server Browser**

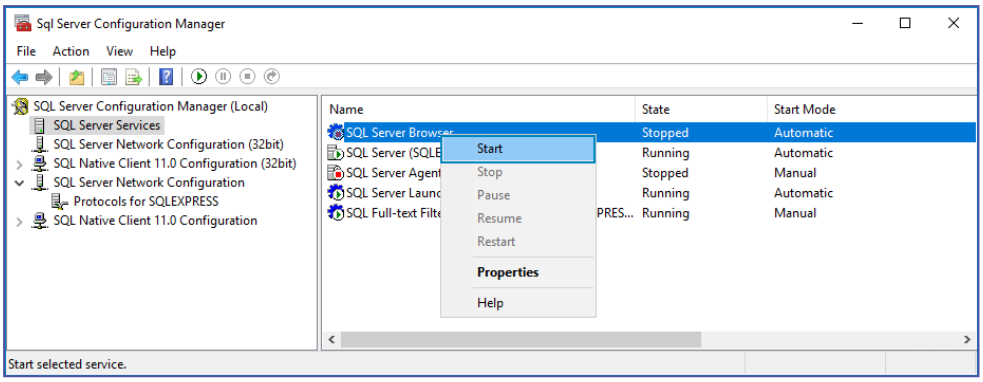
   a. In **SQL Server Services**, double click the **SQL Server Browser** service to open its configuration

   b. On the **Service** tab, set the **Start Mode** value to `Automatic`

   c. Click the **OK** button to save your changes



d. Right-click the **SQL Server Browser** service and select **Start**



Create a login to the SQL Server

Create a login by which the Kryon RPA Server will access the database:

1. Open **SQL Server Management Studio** and connect to the database server
2. In the **Object Explorer**, right-click **Security** and select **New > Login**
3. Enter the following data to create the login:
   - If you are using SQL authentication as your database authentication method:
     - **Authentication:** SQL Server authentication
     - **Login name:** set as desired
     - **Password:** set as desired (the following special characters aren't supported

       IMPORTANT

       For password, special characters aren't supported. For example: `\ ; & "`
     - **Enforce password policy:** disabled
   - If you are using Windows authentication as your database authentication method:
     - **Authentication:** Windows authentication
     - **Login name:** the user with rights to run Kryon services on the RPA server
4. Ensure that `sysadmin` is enabled on the **Server Roles** page of this login properties.

   IMPORTANT!

   What if I can't grant *sysadmin* rights to this login?

   The Kryon RPA Server installation package executes certain tasks that require `sysadmin` rights (e.g., creating database schema and building database tables). If the database doesn't have `sysadmin` rights at the time of installation, follow the additional steps in Creating Database Manually prior to the installation.

`Tip:` **Hold on to that info!**

Make your life easier when installing the RPA server by making note of:

- the FQDN of the database server
- the database instance name
- login credentials

-Take me to the relevant step in the RPA Server Installation Guide-

Creating Database Manually

If the database login doesn't have `sysadmin` rights at the time of installation, follow the procedures outlined below prior to RPA server installation:

1. Connect to the SQL Server instance
2. Create the authentication platform database schema
3. Create the Kryon application database
4. Enter the RPA server addresses

NOTES

- These procedures must be performed by a Database or IT Administrator (i.e., a user with administrative rights to the database server)
- The following required scripts are available in the location from which the Kryon RPA Platform installation files are downloaded:
  - `aerobase_db_and_user.sql`
  - `Create Minimum DB.sql`

Connect to the SQL Server instance

1. On the database server, open SQL Server Management Studio and connect to the relevant SQL Server instance

Create the authentication platform database schema

To create the authentication platform database:

1. Open a new query, and drag the `aerobase_db_and_user.sql` file into the **New Query** window
2. Execute the query, and ensure that it runs with no errors

Create the Kryon application database

To create the Kryon application database:

1. Create a new empty database with the following settings:
   - **Database name:** set as desired (e.g., Kryon)
     - **TIP:** Make note of this name, you'll need it when installing the RPA server
   - **Owner:** login name created when preparing database server
2. Select this newly-created database (be sure you are working with the correct DB schema!)
3. Open a new query, and drag the `Create Minimum DB.sql` file into the **New Query** window
4. Execute the query, and ensure that it runs with no errors.

Minimum and recommended permissions to access database

- **For Kryon_Authentication (default name)**: The minimum MSSQL role for a user is: `dbowner`
- **For Kryon RPA application**: The minimum MSSQL roles are: `dbdatareader`, `dbdatawriter`, and permission to Store Procedure (based on Microsoft SQL Guide).
  Note: To create database table, run the dedicated database script (located in `C:\Kryon\RPA\DB`) after the installation is complete. After running the script, stop and restart all Kryon services (through `C:\Kryon\RPA`).
- The recommended MSSQL role for both authentication and application is `dbowner` and up.

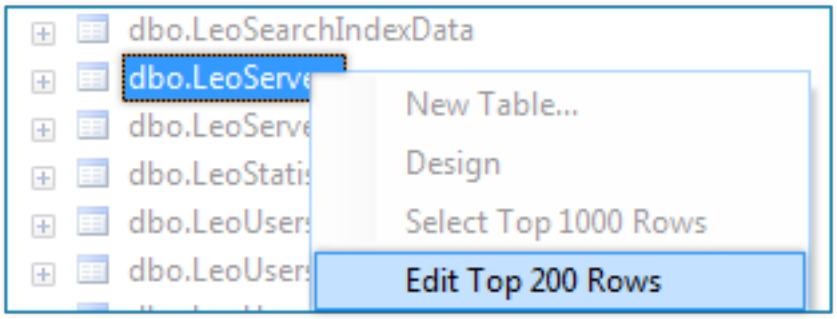
Enter the RPA server addresses

To enter the RPA server address in the Kryon database:

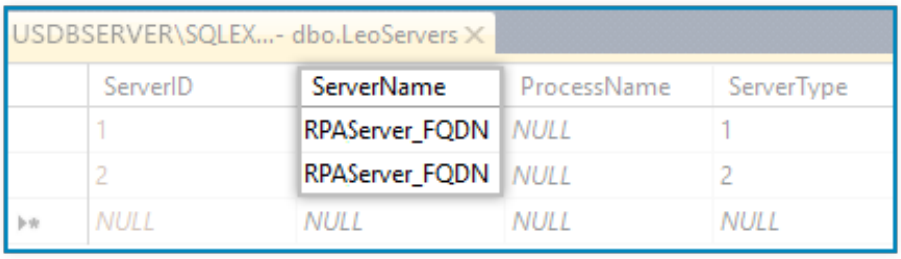
1. On the database server, open SQL Server Management Studio and connect to the SQL instance in which the Kryon database is defined
2. Select the Kryon database (be sure you are working with the correct DB schema!)
3. Update the **dbo.LeoServers** table with the FQDN of the RPA server using one of these two methods:
   - Option #1 – Update using a query:
     - Run the following command in a new query view:
       `UPDATE LeoServers SET ServerName='RPA Server FQDN';`

- OR -

- Option #2 – Update through the GUI:
  - Double-click the new database you created, then double-click **Tables**
  - Right-click **dbo.LeoServers** and select **Edit Top 200 Rows**



  - In the first and second rows, change **ServerName** to the **`RPA Server FQDN`**



IMPORTANT!

When you get to the next step of installing the RPA server, be sure to tick the checkbox labeled **Skip Aerobase DB creation**... otherwise, installation will fail.

-Take me to the relevant step in the RPA Installation Guide-

About upgrading from Console to ConsoleX

What should I consider before upgrading to ConsoleX?

- **ConsoleX** is supported only if you install it on the same server as the RPA application. If for any reason you must install the console on a different server, then install the regular-previous Console instead of **ConsoleX**.
- The database structure of **ConsoleX** is different than the previous console. **ConsoleX** uses new database tables to improve performance to adjust to new product requirements architecture. If you rely on the database structure of the previous console (for BI for example), you might need to apply some changes to your data query configuration.
  Read more about migrating from Console to ConsoleX.

Does all my data migrate from Console to ConsoleX automatically upon upgrade?

The *database schema* migrates automatically from the previous console to **ConsoleX** upon upgrade (during installation).

The *data of the console* (triggers definition, tasks definition, and tasks history) migrates by running a dedicated SQL script post the installation. To migrate your data, contact Kryon support team.

Can I run both consoles (older console and ConsoleX) at the same time?

No, you cannot run (install) both consoles at the same time.

What happens if I upgrade to ConsoleX but later on I decide to downgrade to the previous console?

In such case, you need to take into consideration that you can only migrate data from the previous console to **ConsoleX**, and not the other way around. This means that any new data or configuration saved on **ConsoleX** will not be migrated to the previous console.

Can I configure the SQL migration script to migrate only data from a specific date range?

No. The migration script migrates all data history, and it cannot be limited to a specific time rage (like last X months).

-Take me to the relevant step in the RPA Server Installation Guide-

-I came here while upgrading, take me back to the upgrading steps overview-

Migrating data from Console to ConsoleX

When upgrading from Console to ConsoleX, your database must be prepared using the data migration scripts provided by Kryon support.

During database migration, objects that are no longer supported will be modified to the new functionality.

The following changes in functionality from Console to ConsoleX impact the database structure when migrating:

Functionality	Console	ConsoleX
New task	Tasks assigned directly to robots	Tasks added to the queue
New task - # of runs	A task could be run: X times / Y hours / Forever	Task can run only once
New task - recurrence	Task recurrence available	Recurrence is supported only by triggers using CRON expression
Triggers - yearly recurrence	Available	Available only via 'custom' CRON expression

After migration, all triggers are set to inactive. You need to review your triggers and activate those you need activated.

The following explains specific changes:

Task with recurrences

New time trigger is created:

- The new Trigger Name is the same as the original Task Name with '(migrated)' added to it
- Recurrence is changed: daily, weekly, monthly is changed to time trigger CRON expression; yearly appears as a custom CRON expression.
    - **NOTE:** Since the new CRON does not support *weekly* recurrences greater than every one week or *daily* recurrences greater than every 31 days, these use cases are treated differently:
    - If the task offset was set with *weekly* recurrences greater than every one week, a new trigger is created with recurrence set to every 1 week.

    - If the task offset was set with *daily* recurrences greater than every 31 days, a new trigger is created with recurrence set to every 31 days
- The assigned Wizard is copied to the new trigger
- Robots are copied, if they exist; if not, set for first available robot
- Notifications are copied from task
- The change-log receives a new line: "Created during migration from older versions"
- For task history of the new trigger: Task names receive index ID (for example, `[Task name] #1`)

Example of log data for the change:

Task #123 migrated to a new trigger (#312)

- Task name
- Start time
- # of Runs / Hours / Forever
- Wizard
- Robot
- Variables
- Notifications
- 5 tasks were created: 111, 222, 333, 444, 555. Make sure to validate this trigger and activate it.

For task offset with recurrences set with weekly recurrences greater than every one week: Task #123 migrated to a new trigger (#312). The task offset was set to run every X weeks and converted to run every 1 week.

For task offset with recurrences set with daily recurrences greater than every 31 days: Task #123 migrated to a new trigger (#312). The task offset was set to run above 31 days and converted to run every 31 days.

Task with no recurrences, with single run in the past

Individual task does not change.

Task with no recurrences, with multiple runs in the past

Every run will be migrated as a separate task that appears in the HISTORY tab.

Task names receive index ID (for example, `[Task name] #1`)

Example of log data for the change:

Task #123 could not be migrated (number of runs not supported)

- Task name
- Start time
- # of Runs / Hours / Forever
- Wizard
- Robot
- Variables
- Notifications
- 5 tasks were created to keep history: 111, 222, 333, 444, 555.

Task with no recurrences, with a future single run

New time trigger is created:

- New Trigger Name is the same as the original Task Name with '(migrated)' added.
- The event is changed: time is changed to trigger CRON expression with same date as the original task.
- Robots are copied, if they don't exist set for first available robot.
- Notifications copied from task
- The change-log receives a new line: "Created during migration from older versions"

Example of log data for the change:

Task #123 migrated to a new trigger (#312)

- Task name
- Start time
- # of Runs / Hours / Forever
- Wizard
- Robot
- Variables
- Notifications

- 5 tasks were created: 111, 222, 333, 444, 555 Make sure to validate this trigger and activate it.

Task with no recurrences, with future multiple runs

New time trigger is created:

- This task will be migrated according to its start date, but will run only once.
- Example: A Task with start time at 20/05/2020 18:05, and number of Runs is 5, will be migrated to a Time Trigger that will be triggered only once at 20/05/2020 18:05.

Example of log data for the change:

Task #123 migrated to a new trigger (#312)

- Task name
- Start time
- # of Runs / Hours / Forever
- Wizard
- Robot
- Variables
- Notifications

Task in the queue

Tasks that are In Queue will remain the same:

Except for tasks whose number of runs is greater than 1. In this case:

1. Number of runs will be updated to 1. (only modified in memory when running the task and not saved to DB)
2. A warning message is sent to the logs

Example of log data for the warning message:

- Automation task queue #{taskId} had NumberOfRuns > 1, and was updated to NumberOfRuns = 1

-Take me to the relevant step in the RPA Server Installation Guide-

SSL/TLS Certificates - Manually creating certificate files

NOTE: Only SSL/TLS v1.2 is supported.

For reference, see SSL/SSL/TLS Requirements.

If required, these procedures must be completed prior to RPA server installation. Therefore, you should begin by downloading and installing OpenSSL (if not previously installed).

NOTE

Changing an SSL certificate after installation

If you need to change an SSL certificate after installation, contact the support team.

Install OpenSSL

1. Download the **OpenSSL** utility from this location:

   https://slproweb.com/products/Win32OpenSSL.html

   - Version to download: **Win64 OpenSSL v1.1.1c Light** (select the EXE file option)
2. Install using the default options provided by the installation package

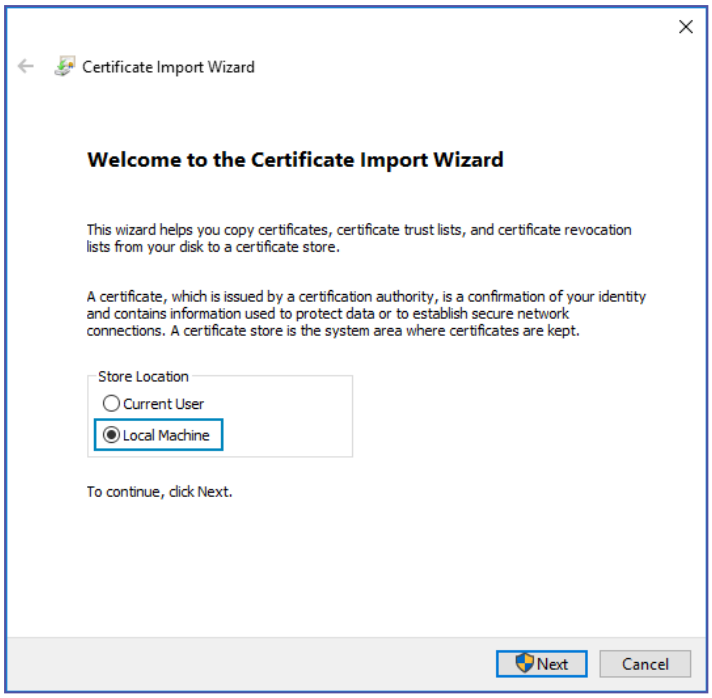
Manually creating individual certificate files

You can elect to manually prepare the additional certificate files required for RPA server installation (as opposed to letting the RPA server installation package do so). To manually prepare the certificate files, follow these steps:

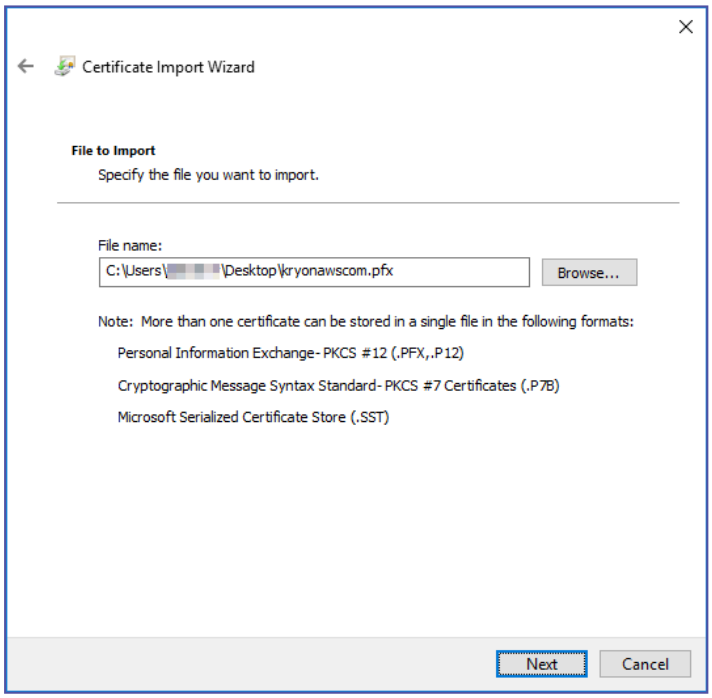
Step 1: Install the *.pfx certificate to the Windows certificate store

1. Copy the certificate (in ***.pfx** format) to an easy-to-access location (e.g., Desktop) on the machine on which you will install the RPA server
2. Double-click the ***.pfx** certificate

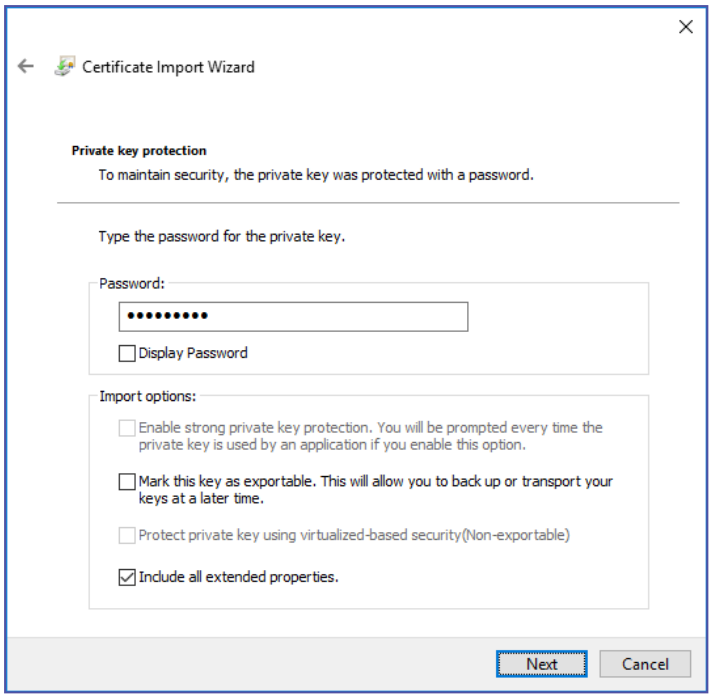
   The **Windows Certificate Import Wizard** will open
3. Select the **Local Machine** option



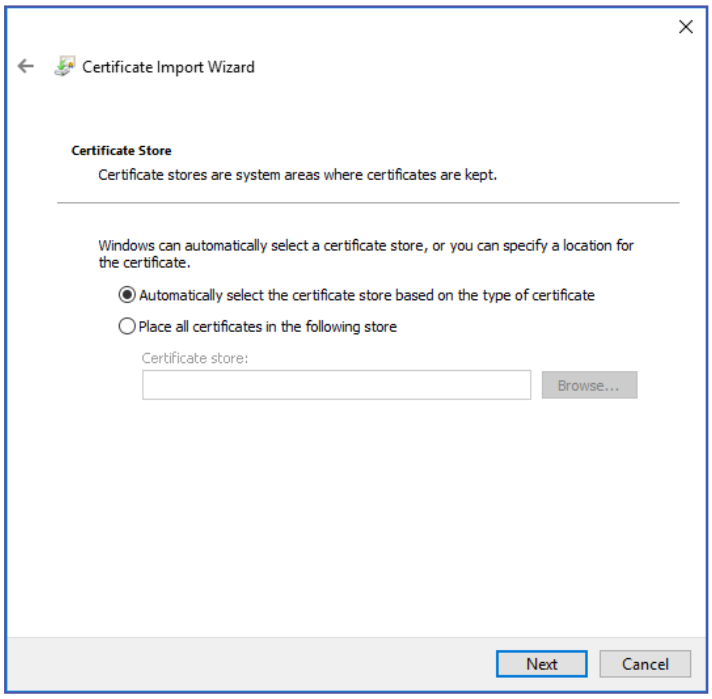
4. Confirm the file to import (the file you clicked on to open the wizard)



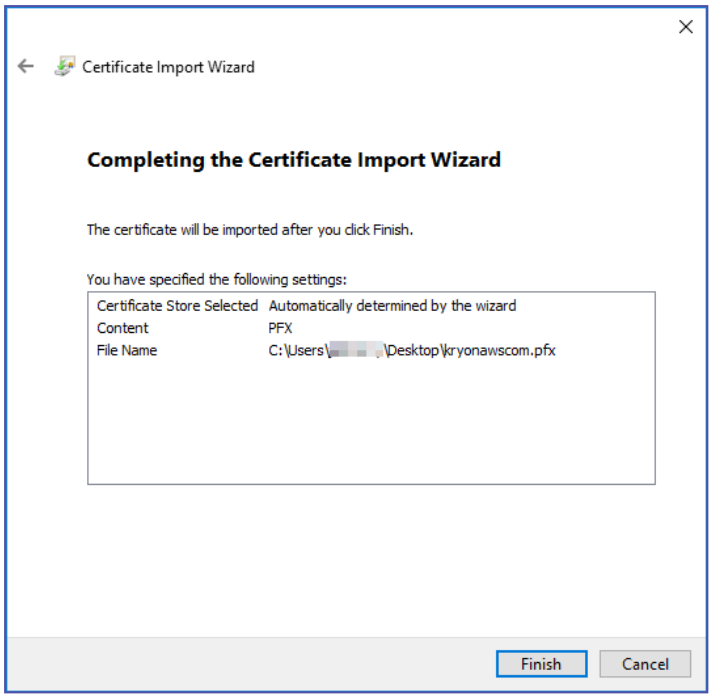
5. Enter the certificate password
6. Maintain the default **Import options** settings



7. Select the **Automatically select the certificate store** option



8. Review your settings and click the **Finish** button



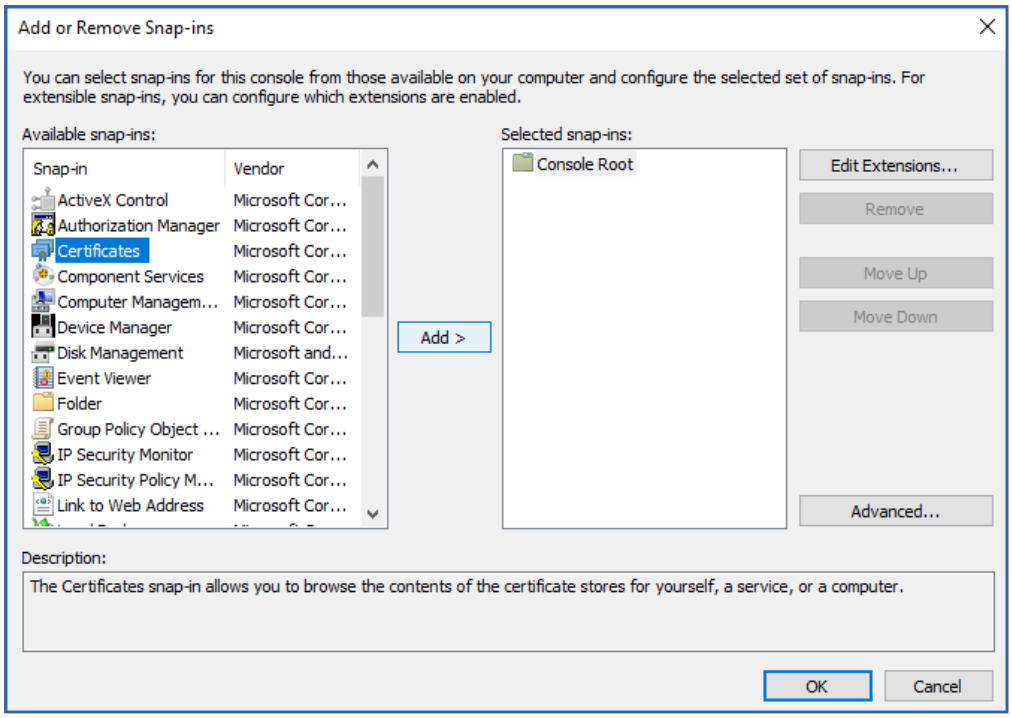
You will receive a confirmation that the certificate was imported successfully

Step 2: Export the certificate in *.p7b format

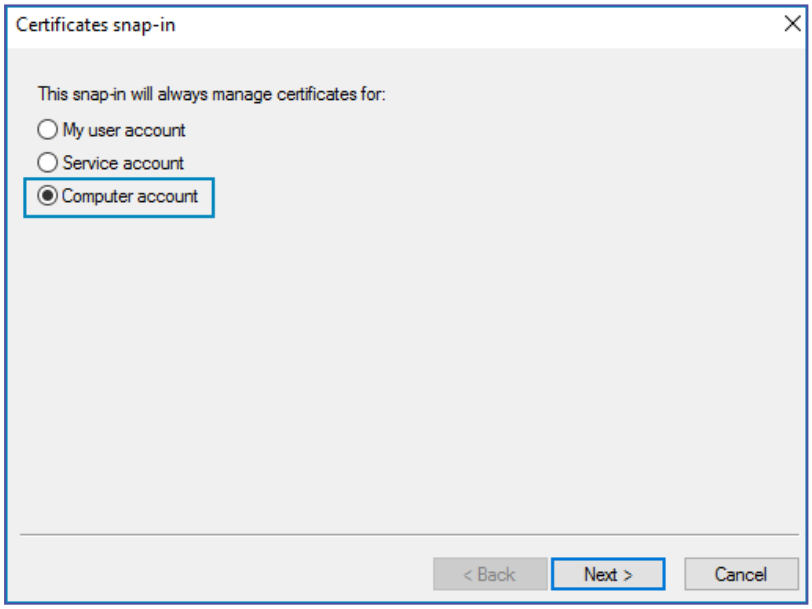
1. From the lower left corner **Windows** icon, run **MMC** (Microsoft Management Console) ***as administrator***

   TIP:
   If **MMC** does not pop up as an option when typing it from the **Windows** icon, open it instead by typing **Run**, then entering **MMC** in the **Run** dialog.

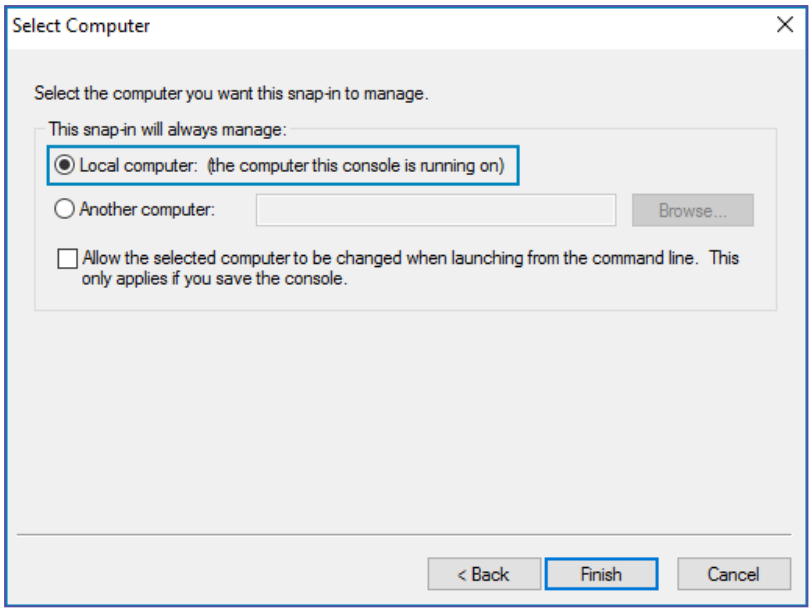
2. From the **File** menu, select **Add/Remove Snap-in...**
3. From the **Available snap-ins** list, select **Certificates**, and click the **Add >** button



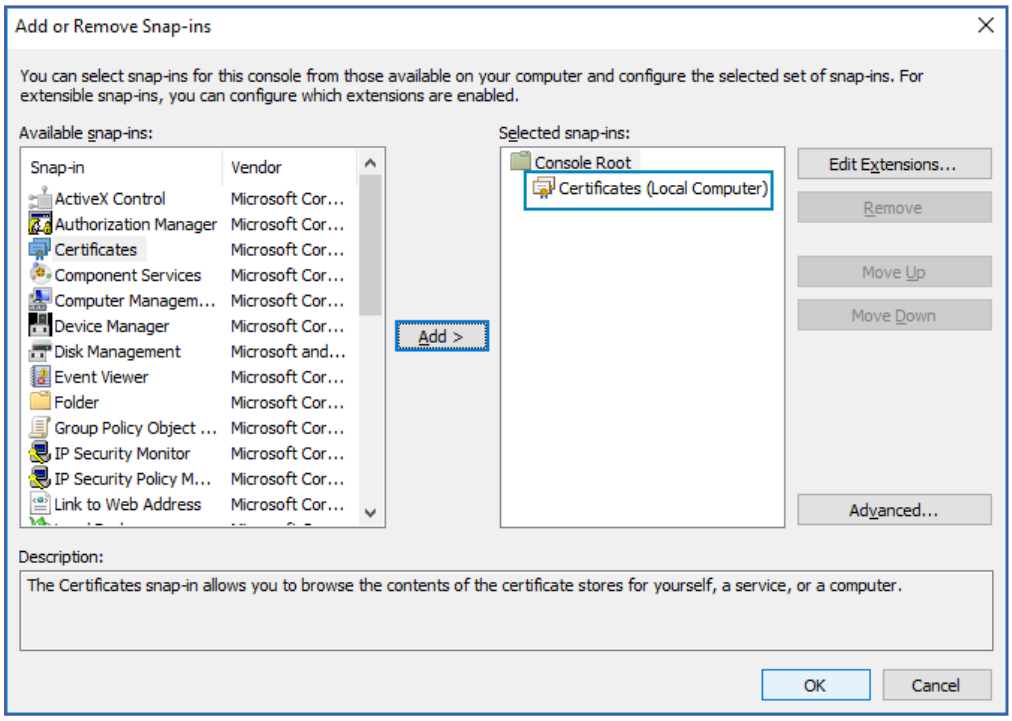
4. Select the **Computer account** option



5. Select the **Local computer** option, then click the **Finish** button

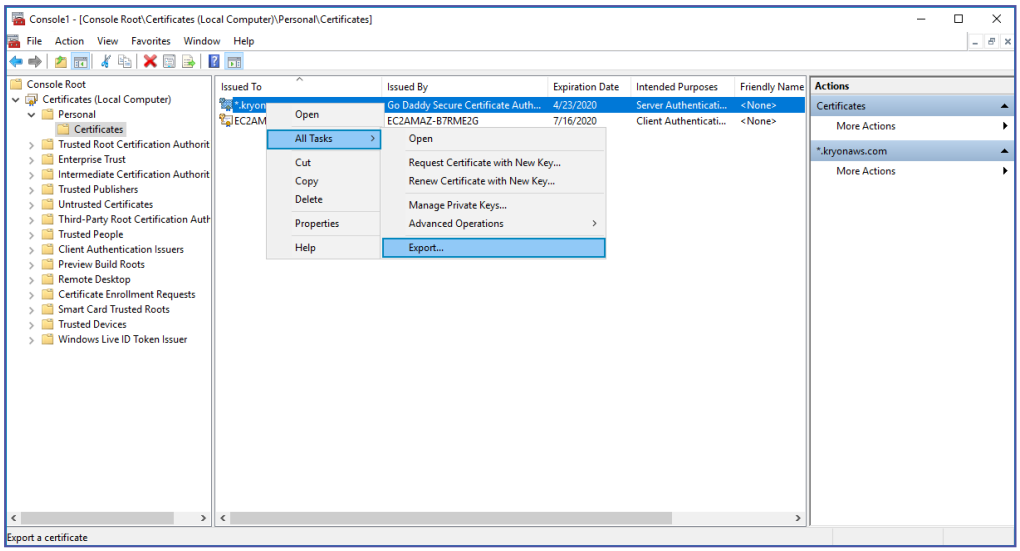


6. The **Certificates** snap-in will now appear in the left-hand column of the **Add or Remove Snap-ins window** under **Console Root**

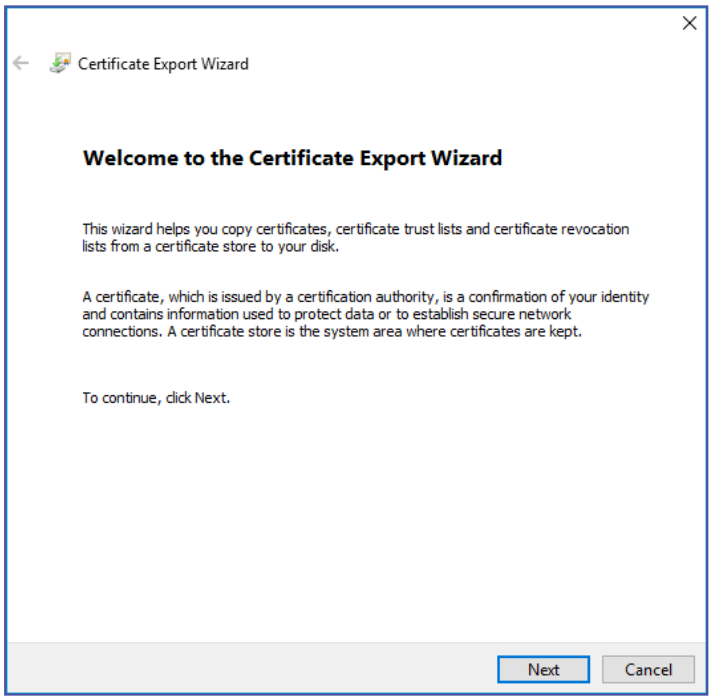


7. Click the **OK** button to return to the main **MMC** screen
8. From the left pane (the folder tree), navigate to **Console Root > Certificates (Local Computer) > Personal > Certificates**

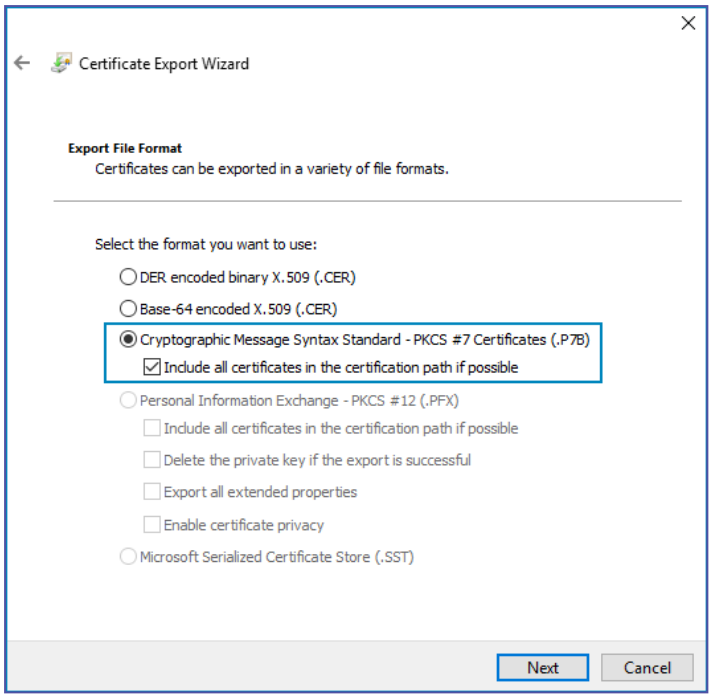
   A list of certificates will appear in the middle pane.
9. Right-click on the relevant certificate, select **All Tasks > Export...**



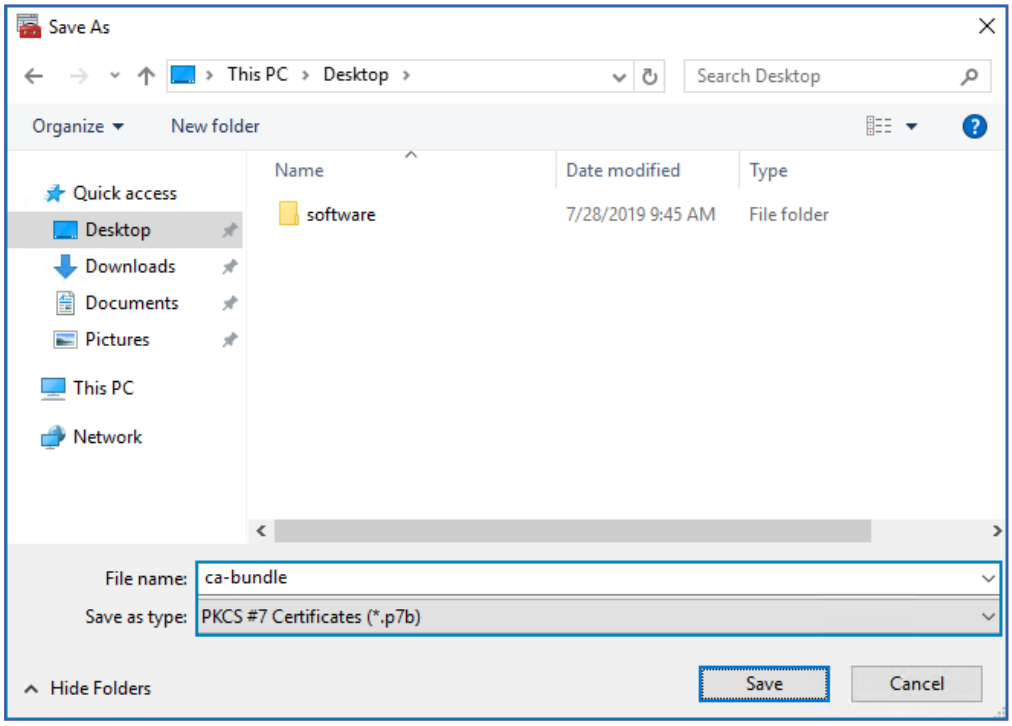
10. The **Windows Certificate Export Wizard** will open



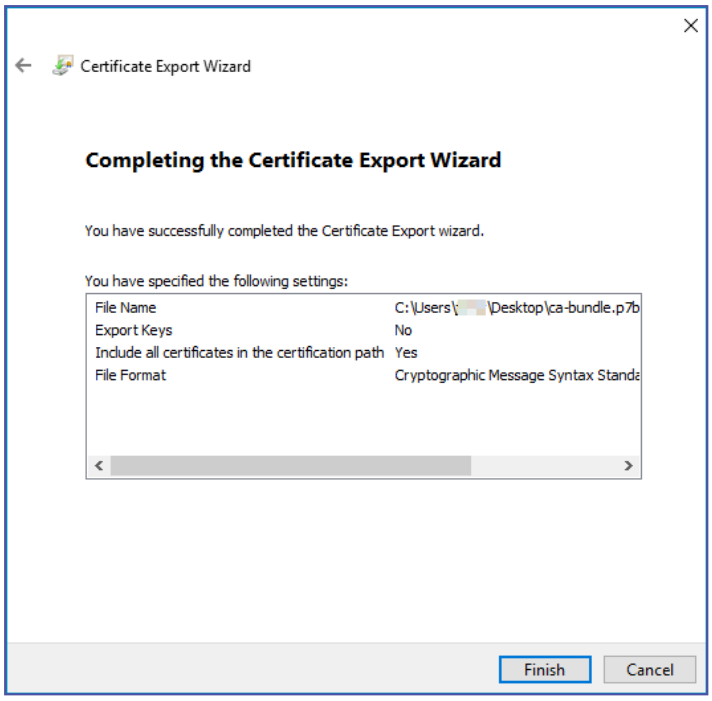
11. Select the **Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)** file format



12. Save the file to an easily-accessible location on the server with the name **`ca-bundle.p7b`**



13. Review your settings and click the **Finish** button



The file will be exported to the selected location, and you will receive a confirmation that the certificate was exported successfully

Step 3: Create the file: ca-bundle.pem

1. From Windows File Explorer, navigate to the folder: **C:\Program Files\OpenSSL-Win64\bin**
2. Run the file **openssl.exe *as administrator***
3. From the `OpenSSL>` command prompt, run the following command:

   ```
   pkcs7 -in {p7b file location}\ca-bundle.p7b -inform DER -print_certs -out {desired file location}\ca-bundle.pem
   ```

   - **Example:** `pkcs7 -in C:\Users\localadmin\Desktop\ca-bundle.p7b -inform DER -print_certs -out C:\Users\localadmin\Desktop\ca-bundle.pem`

   You will be returned to the `OpenSSL>` command prompt, and a file called `ca-bundle.pem` will be created in the specified location

Step 4: Create a CRT file

1. From the `OpenSSL>` command prompt, run the following command:

   ```
   pkcs12 -in {pfx file location}\{pfx filename}.pfx -clcerts -nokeys -out {desired file location}\{FQDN_of_RPA_Server}.crt
   ```

- **Example:** `pkcs12 -in C:\Users\localadmin\Desktop\companydomaincom.pfx -clcerts -nokeys -out C:\Users\localadmin\Desktop\RPAServer.companydomain.com.crt`

2. Enter the certificate password when prompted

   You will be returned to the `OpenSSL>` command prompt, and a file called `{FQDN_of_RPA_Server}.crt` will be created in the specified location

Step 5: Create a PEM file

1. From the `OpenSSL>` command prompt, run the following command:

   `pkcs12 -in {pfx file location}\{pfx filename}.pfx -nocerts -out {desired file location}\{FQDN_of_RPA_Server}.pem -nodes`

   - **Example:** `pkcs12 -in C:\Users\localadmin\Desktop\companydomaincom.pfx -nocerts -out C:\Users\localadmin\Desktop\RPAServer.companydomain.com.pem -nodes`

2. Enter the certificate password when prompted

   You will be returned to the `OpenSSL>` command prompt, and a file called `{FQDN_of_RPA_Server}.pem` will be created in the specified location

Step 6: Create a KEY file

1. From the `OpenSSL>` command prompt, run the following command:

   `rsa -in {pem file location}\{pem filename}.pem -out {desired file location}\{FQDN_of_RPA_Server}.key`

   NOTE: The PEM file referred to in this step is the file created in step #4 above (**NOT** `ca-bundle.pem` created in step #2)

   - **Example:** `rsa -in C:\Users\localadmin\Desktop\RPAServer.companydomain.com.pem -out C:\Users\localadmin\Desktop\RPAServer.companydomain.com.key`

   You will be returned to the `OpenSSL>` command prompt, and a file called `{FQDN_of_RPA_Server}.key` will be created in the specified location

TIP

Hang on to those certificate files!

Be sure to keep all the files utilized/created in this section in an easily accessible location until after RPA server installation. You should also save them to a safe location for backup purposes.

-Take me to the relevant step in the RPA Installation Guide-

SSL/TLS Requirements

If you want to install the Kryon RPA Platform using SSL/TLS , you have two options:

Option 1: Let the RPA installer generate the CA and certificate for you on the fly.

Option 2: Provide the organization's certificate. The certificate must meet the following requirements:

File format	PKCS #12 is PFX format (bundles a private key with its X.509 certificate) If PFX file is secured with password, customer must know it Certificate must be capable of being installed locally on server machine's personal certificate repository
Issuer	Signed by known, valid certifcate authority: public CA or private CA
Public key	RSA 2048+
Signature hash	SHA256
Enhanced key usage	*Server Authentication* or *Multipurpose*
Certificate expiration date	It is the customer's responsibility to make sure certificates are kept up to date

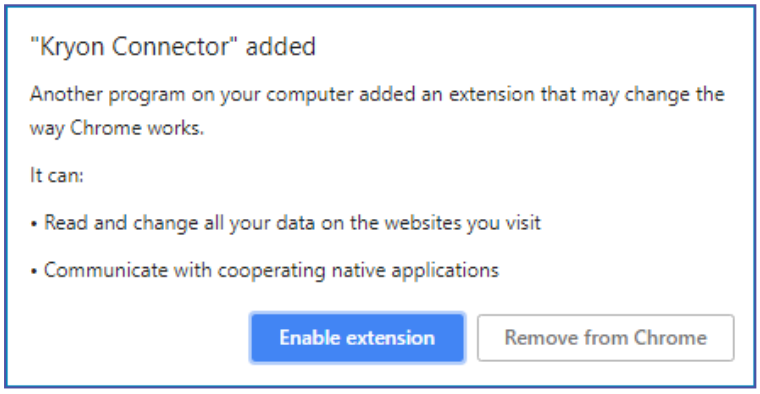
NOTE: Only SSL/TLS v1.2 is supported.

Enabling Kryon Connector Browser Extensions

To support wizards that run on Chrome and/or Firefox, enable/install the Kryon Connector Extension for the browser .

Chrome

The Kryon Connector extension will be automatically installed when you install or upgrade your Kryon Robot and Studio clients to version 5.21 or later. Be sure to enable it when prompted in Chrome:



Firefox

1. Open the relevant folder on the client machine:
   - For robot clients:
     `C:\Program Files\Kryon Robot\Firefox`
   - For Kryon Studio:
     `C:\Program Files\Kryon Studio\Firefox`
2. Double-click the file **Install.bat**
   - This file will be present only if Firefox was installed on the machine at the time of the client's installation
3. Open Firefox, and click on the icon that appears in the upper-right corner (next to the address bar)
4. Click on the notification that the Kryon Connector extension was installed, and follow the prompts to enable the extension

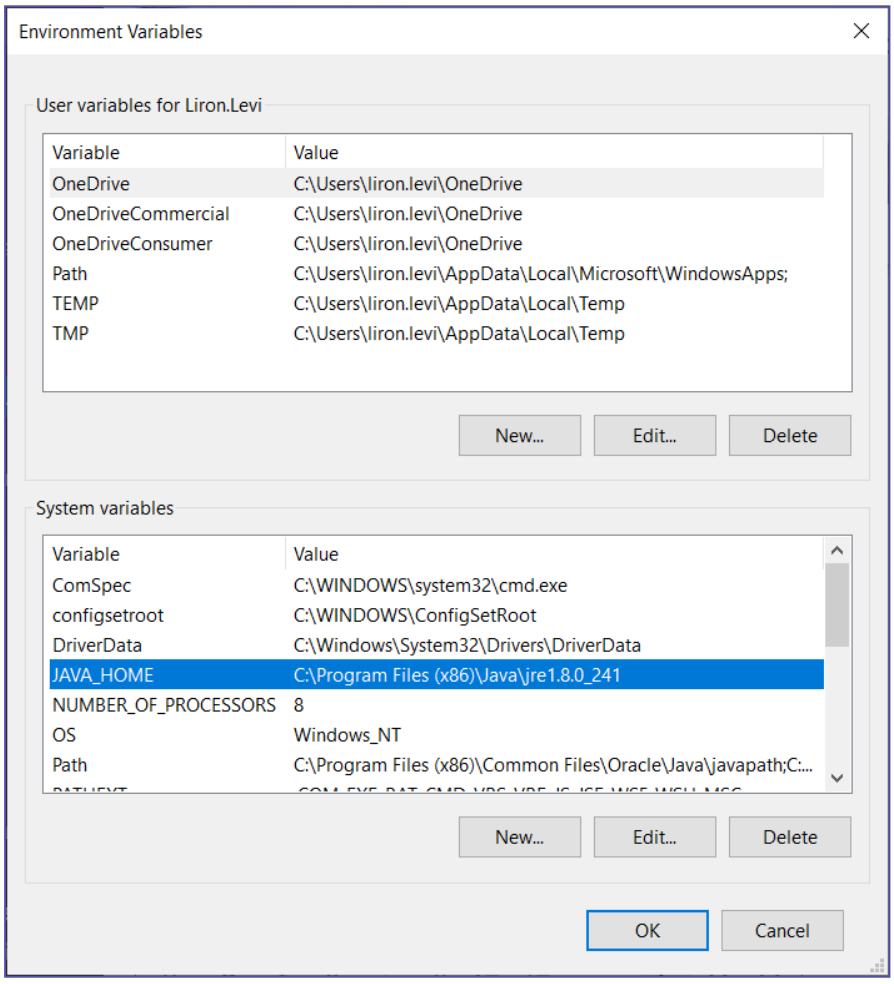
-Take me to the relevant step in the RPA Installation Guide-

Installing Kryon Java Bridge

Before running Studio and Robot installation package, you need to prepare the ground for Java Bridge and run the Java Bridge script.

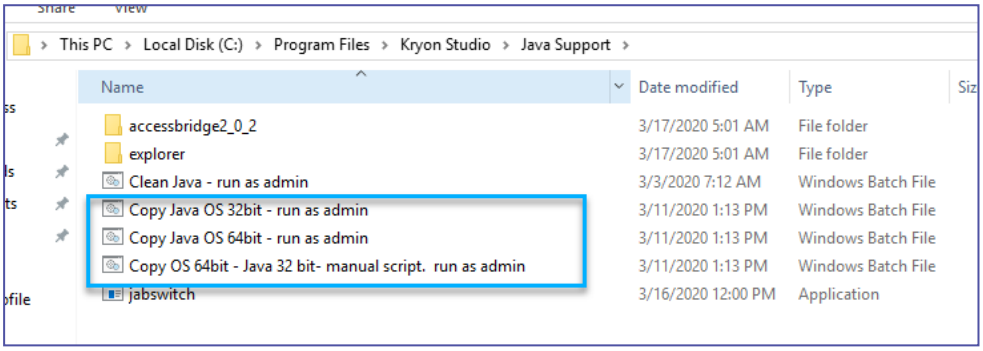
Java, Kryon Java Bridge, and JAVA_HOME are prerequisites to be able to use Java Automation Commands

1. Make sure you have Java installed. If not, download and install Java according to the Windows architecture (64 or 32 bit).
2. Make sure JAVA_HOME environment variable is configured for the installed Java:



3. **Install the Kryon Java Bridge** by running the Java Support Script (for Studio and Robot) *as admin* according to your architecture:
   - If you have 64bit architecture and you installed Java 64bit, run the script: "`Copy Java OS 64bit`".

- If you have 32bit architecture and you installed Java 32bit, run the script: "`Copy Java OS 32bit`".
- If you have 64bit architecture and you installed Java 32bit, run the scripts: "`Copy OS 64bit - Java 32 bit- manual scripts.`"
  Note: Make sure to run the relevant scripts for both Studio and Robot; navigate to both Studio and Robot folders > Java Support folder > run the relevant script.



NOTE

Contact Kryon support team for any additional or customizable Java configurations.

-Take me to the relevant step in the RPA Installation Guide-

Generating a KEYTAB file (Kerberos)

Best practice to generate a KEYTAB is during the RPA Server installation as the RPA Server wizard provides you with convenient tools to perform this action.

You can generate a KEYTAB file once you get to the Authentication Platform Security step in the RPA installation wizard.

1. To generate the KEYTAB script, you can use the "copy command to clipboard" or the "save command to batch file".
   - If you are installing on one primary machine, this is how the generic CLI script is formatted:
     ```
     ktpass -out filename.keytab -princ "HTTP/{FQDN}@DOMAIN" -
     mapUser "userPrincipalName" -mapOp set -pass "password" -
     crypto all -pType KRB5_NT_PRINCIPAL -setupn -setpass
     ```
   - If you are installing on more than one machine (High-Availability), the generated script adds a dedicated line for every additional serve and includes the FDQNs of the servers. This is how the generic CLI script for two machines is formatted:
     ```
     ktpass -out filename.keytab -princ "HTTP/{FQDN}@DOMAIN" -
     mapUser "userPrincipalName" -mapOp set -pass "password" -
     crypto all -pType KRB5_NT_PRINCIPAL -setupn -setpass -mapOp
     add -in filename.keytab
     ```
2. Store the KEYTAB file at `{InstallFolder}\IDP\Aerobase\Configuration\{filename}.keytab`

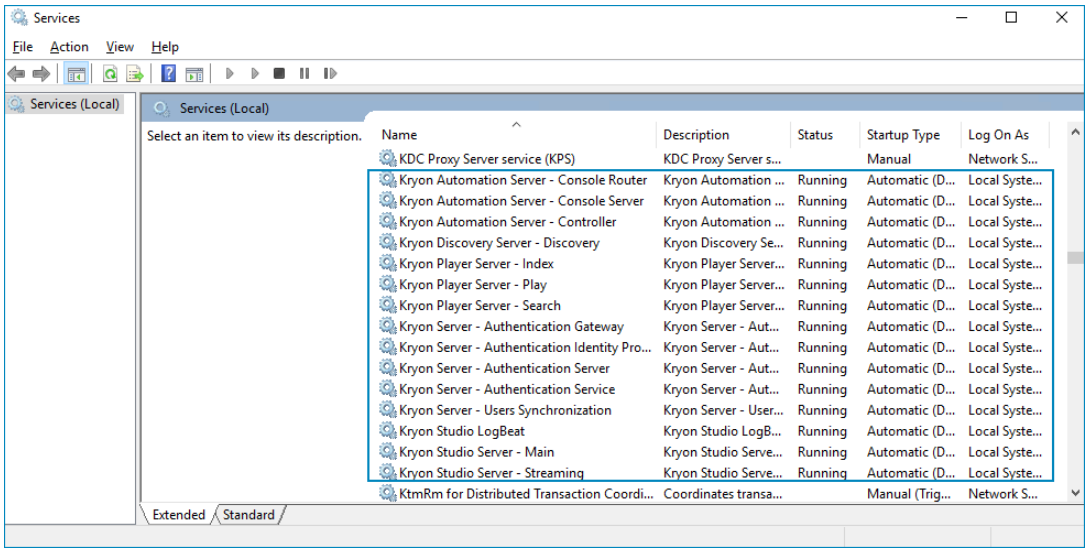
To use KEYTAB file for Single Sign-on (Kerberos) Authentication, please read Adding another LDAP user federation.

-Take me to the relevant step in the RPA Installation Guide-

Restarting Kryon Services

In certain circumstances (for example, after changes to database configuration), you may be required to restart all KryonRPA services. To do so:

1. Navigate to `{InstallFolder}\RPA`
2. Right-click `StopAll.bat`, and select **Run as administrator**
3. Right-click `StartAll.bat`, and select **Run as administrator**



Configuring Task Re-run

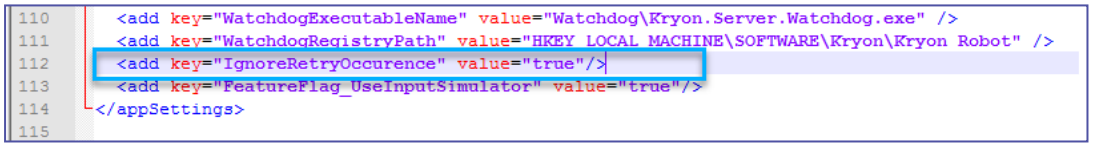
Starting from v20.3, the default configuration of task-rerun in case of a Robot/Client failure is to not re-run the task. This is to avoid running tasks twice which might result with duplicated tasks, hence duplicated results/outputs and even actions.

What can cause a Robot to fail/crash?

- Machine is down during Wizard run
- User runs 'kill task' to the bot during Wizard run
- User runs 'kill task' to the bot through a remote command (powershell)
- A critical error occurs during Wizard run

Configuration

The configuration is set in the `appSetting.config` file of the Robot. You can change the configuration from "true" to "false". See implications.



Configuration implications:

- If the value is "**true**", the Robot will report a failure and will not run the task again.
- If the value is "**false**", the Robot will run the wizard again, starting from step 1.

NOTE

The task will not run again in case more than 24 hours have passed since the Robot failure/crash.

Changing Kryon Studio to Japanese

If you want to change the Kryon Studio interface to Japanese, follow these instructions:

1. With a text editor, open the following file: `C:\Program Files\Kryon Studio\Config\appSettings.config`
2. Find the line that begins: `<add key="Locale"`, and change the value from `"en"` to `"ja-jp"`
   - The full line should now read:
     `<add key="Locale" value="ja-jp" />`
3. Restart Kryon Studio

You can revert to English at any time by following the same procedure and changing the value back to `"en"`.

Changing SEQ default minimum level of 'log writes'

Up to v19.5.x, the default minimum level of 'log writes' in clients (Robot and Studio) and server is "Verbose" (=all levels).

Starting from v20.3, the default minimum level of 'log writes' is "Information". This means that all the debug log writes from Robot/Studio and server don't write to SEQ by default.

Why has this change been made?

Based on our experience in the field, this change has led to significant improvements in the performance (memory and disk IO) on the client-side and on the serve-side.

Changing the default 'log writes'

In case you want to change back the config to write debug level (all levels), do the following:

1. In the "config" sub folder (of the Robot/Studio), open the `serilog.json` file to edit.
2. Replace the line:
   `"LevelSwitches": { "$controlSwitch": "Information" }`
   with the line:
   `"LevelSwitches": { "$controlSwitch": "Verbose" }`
3. Do the same for the server side (open the `serilog.json` file under the folder of the relevant service and apply the same change as above).

Configuring Kryon Terminal Server Robot

The Kryon Terminal Server Robot Tool supports a session scheduler feature. When enabled, the tool automatically maintains configured RDP sessions active. If a session is canceled – the tool will bring it back.

Configure the tool

Make configuration settings in only two files in the installation package, `appsettings.JSON` and `scheduled_rdp_sessions.JSON`.

Generally the tool should work with the default `appsetting.json` configuration.

Settings which may need to be changed in `appsetting.json` are:

- `DefaultRdpPort` – Default RDP port is 3389. You may need to change this if your company is using another one.
- The Session scheduler feature is enabled by default.

Further configuration for session scheduler are done in `scheduled_rdp_sessions.json`. Edit the following settings here to configure:

- `machineAddress`
- `UserName/UserPassword`

TO EDIT THE JSON FILES:

1. Open the JSON file with a text editor
2. Enter the value for the relevant parameter between the corresponding double-quotes, for example:

   ```
   "DefaultRdpPort": "3389",
   ```

   Note: The syntax for specifying folder and file locations in JSON uses a double backslash in each location in which Windows syntax would use a single backslash, for example:

   ```
   C:\\Program Files\\MariaDB\\
   ```

3. Save the JSON file

Install the tool

The following sets up the tool as a windows service:

Make sure you have custom or default system user account to create windows service. By default, a windows service will be created for next default user: 'Local System'.

Installation parameters details:

1. **{NAME}**

   Required. Service name. '`KryonRdpService`' is used below automation scripts as service name.

2. **{EXE FILE PATH}**

   Required. The app's executable path (for example, `C:\installation folder\company.RDPService.API.exe`). Include the executable file name with extension.

3. **{DOMAIN OR COMPUTER NAME\USER}**

   Optional. Service user account (for example, MyComputerName\ServiceUser). By default windows service will be created for next default user: 'Local System'.

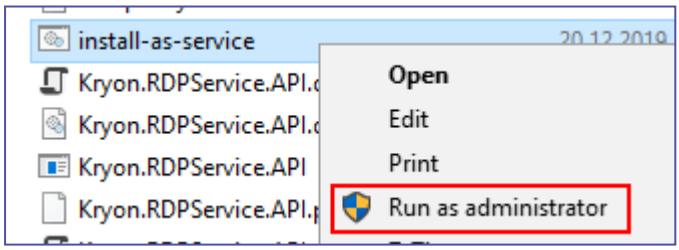
4. **{DISPLAY NAME}**

   Optional. Service display name (for example, Company RDP Management Service).

USING NSSM

This process is automated using '`install-as-service.bat`' script.

In order to install the service using NSSM, run '`install-as-service.bat`' as an administrator.



The installation package contains all the needed dependencies like nssm.exe, run-as-process.bat, etc. Once installed you'll see the service in the Windows Services list.

The installer sets the service to start automatically.

To verify: check that http://localhost:5000 is accessible.

USING WINDOWS SERVICE CONTROL MANAGER (SC.EXE)

1. **Create a service**

   Use sc.exe to create a service, passing the full path of the built executable.

   ```
   sc create {NAME} binPath= "{EXE FILE PATH}" type=own start=auto
   displayname="{DISPLAY_NAME}" obj={DOMAIN OR COMPUTER NAME\USER}
   ```

Command example

```
sc create "CompanyRdpService" binPath=
"C:\Projects\Company\rdp-
service\Company.RDPService.API\bin\Debug\netcoreapp2.2\win7-
x64\publish\Company.RDPService.API.exe" type=own start=auto
displayname="CompanyRDP management Service"
```

2. **Start/Stop/Pause a service**

   Use **sc.exe** to start the service (this needs to occur in a command prompt running as Administrator)

   sc start {NAME}

   sc stop {NAME}

   sc pause {NAME}

3. Get status of the service

   sc query {NAME}

4. Delete service

   sc delete {NAME}

USING POWERSHELL COMMANDS

1. **Create a service**

   New-Service -Name {*NAME*} –BinaryPathName "{*EXE FILE PATH*}" –StartupType Automatic –Displayname "{*DISPLAY_NAME*}" –Credential {*DOMAIN OR COMPUTER NAME\USER*}

   Command example

```
New-Service -Name "CompanyRdpService" -BinaryPathName
"C:\Projects\Company\rdp-
service\Company.RDPService.API\bin\Debug\netcoreapp2.2\win7-
x64\publish\Company.RDPService.API.exe" -StartupType Automatic
-Displayname="Company RDP management Service
```

2. **Start/Stop a service**

   Start-Service -Name {NAME}

   Stop-Service -Name {NAME}

3. **Get status of the service**

   Get-Service -Name {NAME}

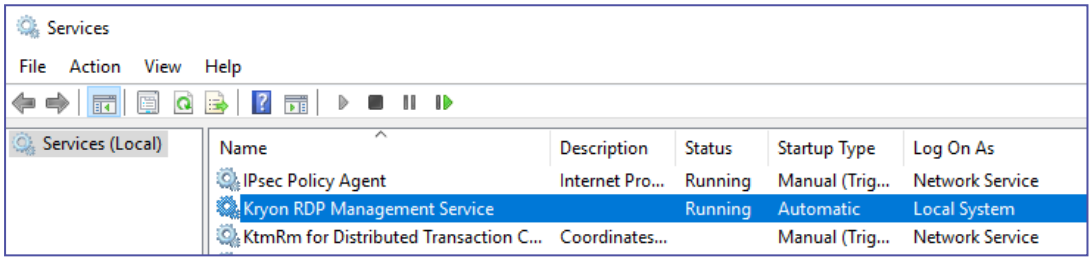
4. **Delete service**

   Remove-Service –Name {NAME}

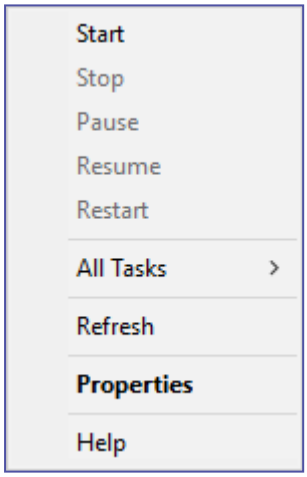
For more details, see here

Managing the Tool

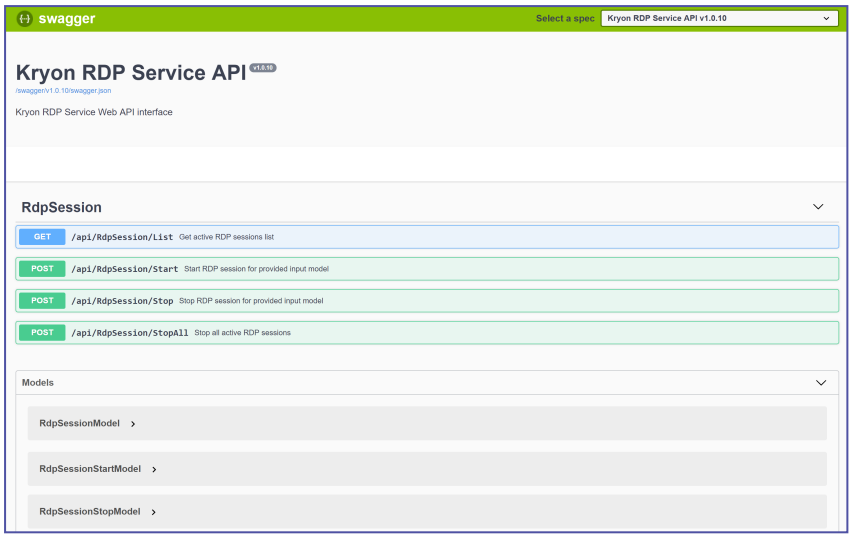
Once windows service is installed and started you should see the status of 'running' in Windows Services Manager, as follows:



Windows Services Manager can be used to manage the service:



You can access the API page from: http://localhost:5000.



Logging

In order to configure log file location, change `next appsettings.json` option:

- Absolute path: `LogFilePath: "c:\\company_rdp"`
- Relative path: (relative to exe file location) `LogFilePath: "./logs"`

Log file entries format can be configured in NLog configuration files: `nlog.Production.config`.

In particular log entries format can be changed be editing '`Layout`' variable in `nlog.Production.config`

```
<variable name="Layout"
          value="${date:format=dd-MM-yyyy HH\:mm\:ss}|${uppercase:${level}}|${message} ${exception:format=toString,StackTrace}"/>
```

The following is an example of the log file:

kryon_rdp_2019-08-21 - Notepad

File Edit Format View Help

```
21-08-2019 13:37:47|INFO|Environment: Production. Version: v1.0.14
21-08-2019 13:37:48|INFO|Session Scheduler: started.
21-08-2019 13:38:08|INFO|Session Scheduler: run: 21.08.2019 10:38
21-08-2019 13:38:08|INFO|Session Scheduler: reading session list from: c:\kryon_rdp\scheduled_rdp_sessions.json.
21-08-2019 13:38:08|INFO|FreeRdp start session command: '/w:500 /h:400 /cert-ignore -themes -wallpaper +compression
21-08-2019 13:38:08|INFO|Process started: Process ID: 17640; Process Name: wfreerdp; Active: True
21-08-2019 13:38:09|INFO|FreeRdp start session command: '/w:500 /h:400 /cert-ignore -themes -wallpaper +compression
21-08-2019 13:38:09|INFO|Process started: Process ID: 6812; Process Name: wfreerdp; Active: True
21-08-2019 13:39:09|INFO|Session Scheduler: run: 21.08.2019 10:39
21-08-2019 13:39:09|INFO|Session Scheduler: reading session list from: c:\kryon_rdp\scheduled_rdp_sessions.json.
21-08-2019 13:40:09|INFO|Session Scheduler: run: 21.08.2019 10:40
21-08-2019 13:40:09|INFO|Session Scheduler: reading session list from: c:\kryon_rdp\scheduled_rdp_sessions.json.
21-08-2019 13:40:24|INFO|Process stopped. ID: 17640
21-08-2019 13:41:09|INFO|Session Scheduler: run: 21.08.2019 10:41
21-08-2019 13:41:09|INFO|Session Scheduler: reading session list from: c:\kryon_rdp\scheduled_rdp_sessions.json.
21-08-2019 13:41:09|INFO|FreeRdp start session command: '/w:500 /h:400 /cert-ignore -themes -wallpaper +compression
21-08-2019 13:41:09|INFO|Process started: Process ID: 17176; Process Name: wfreerdp; Active: True
21-08-2019 13:42:09|INFO|Session Scheduler: run: 21.08.2019 10:42
21-08-2019 13:42:09|INFO|Session Scheduler: reading session list from: c:\kryon_rdp\scheduled_rdp_sessions.json.
21-08-2019 13:43:09|INFO|Session Scheduler: run: 21.08.2019 10:43
21-08-2019 13:43:09|INFO|Session Scheduler: reading session list from: c:\kryon_rdp\scheduled_rdp_sessions.json.
21-08-2019 13:43:25|INFO|Process stopped. ID: 17176
21-08-2019 13:44:09|INFO|Session Scheduler: run: 21.08.2019 10:44
```

Configuring Non-Default Ports in a SSL/TLS Deployment

If you selected a non-default HTTPS port (8083) and/or a non-default Discovery port (80) during RPA server installation for a SSL/TLS deployment, the additional procedures outlined below are required.

NOTE: Only SSL/TLS v1.2 is supported.

Non-default HTTPS and/or Discovery port: client configuration

If either port is non-default, follow these steps for every Kryon Studio and robot client:

1. With a text editor, open the following configuration files –
   - For robot clients:
     `C:\Program Files\Kryon Robot\Config\appSettings.config`
   - For Kryon Studio:
     `C:\Program Files\Kryon Studio\Config\appSettings.config`
2. Find the line that begins: `<add key="EnforceServerSchema" value="" />`, and change it to read:

   `<add key="EnforceServerSchema" value="https" />`
3. Find the lines that read:
   - `<add key="HttpsComPort" value=... />`
   - `<add key="DiscoveryPort" value=... />`

   and (if they are not correct), change the values to equal the actual port numbers used

Non-default Discovery port: Console configuration

If the Discovery port is non-default, follow these additional steps on the RPA server to configure Kryon Console:

1. With a text editor, open the following files:
   - `{InstallFolder}\RPA\Kryon Web Server 64bit\Console\API\Config\appSettings.config`
   - `{InstallFolder}\RPA\Kryon Web Server 64bit\WebAPI\Config\appSettings.config`

2. In each, find the line that reads `<add key="DiscoveryPort" value=... />`, and change the value to equal the actual port number used.

Adding another LDAP user federation (Kerberos)

There are 2 primary steps when configuring Kerberos (Domain Authentication) as your authentication method:

- Connect to Windows Active Directory; and
- Sync users to Kryon Admin (i.e., the Kryon database)

BEST PRACTICE:

Managing users

Consider the following, very likely scenario:

- Your Windows Active Directory contains thousands of users
- Your Kryon license covers 100 users, including Console users, Studio users, and robots

As explained above, the final result of configuring your Kryon deployment to work with Kerberos will be to import users into the Kryon database. In accordance with your Kryon license, only 100 users will be imported as active users. All remaining users will be imported as inactive. The active users would be the first 100 randomly imported users (which may or may not be the actual users you wish to be active in Kryon).

To avoid filling the Kryon database with inactive users and the need to search through them to activate the correct ones, it is highly recommended to create a container containing only Kryon users within your Active Directory, then sync only that container. Depending on the structure of your Active Directory, this container will often be a **CN** ("common name") within an **OU** ("organizational unit").

Connect to Windows Active Directory

To connect Kryon to your Windows Active Directory:

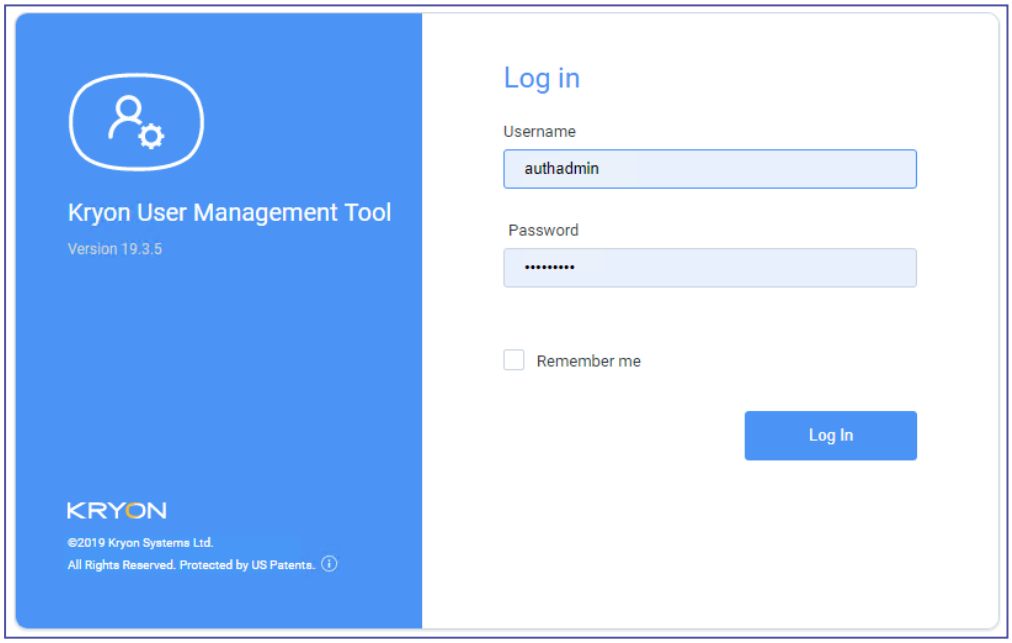
- Access the Kryon User Management Tool
- Configure a user federation
- Sync users to the user federation

Access the Kryon User Management Tool

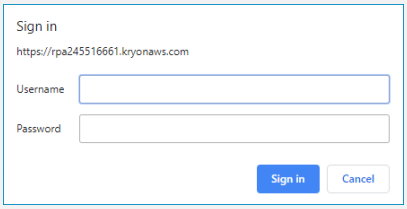
To access the Kryon User Management Tool:

1. Open an **incognito window** in Chrome
2. Enter the following URL: `http://{FQDN_RPA_SERVER}/auth/admin/kryon/console/#/realms/kryon`
   - Use `https://` in the URL if you installed with SSL/TLS

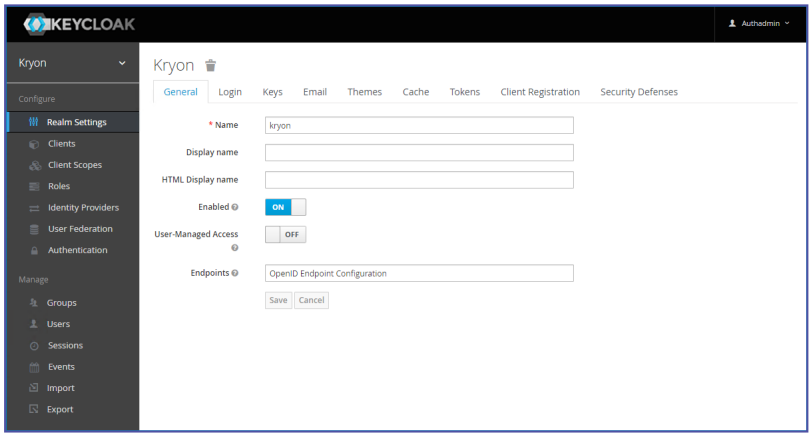
   The following screen will open:



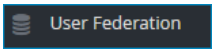
> **NOTE**
>
> If you receive a Chrome message asking you to sign in, just click **Cancel**.



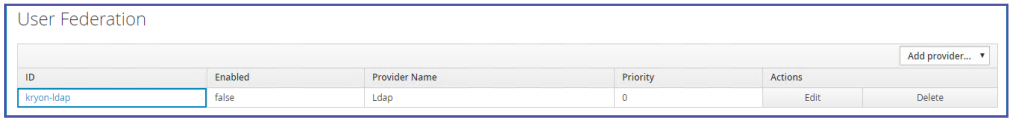
3. Log in to the **Kryon User Management Tool** with these credentials:
   - **Username:** authadmin
   - **Temporary password:** Kryon123!
     - You will be prompted to change the temporary password upon first login
4. The following screen will open:



Configure a user federation

1. From the left menu, click 

2. From the page that opens, click **kryon-ldap** (the default federation installed with Kryon)



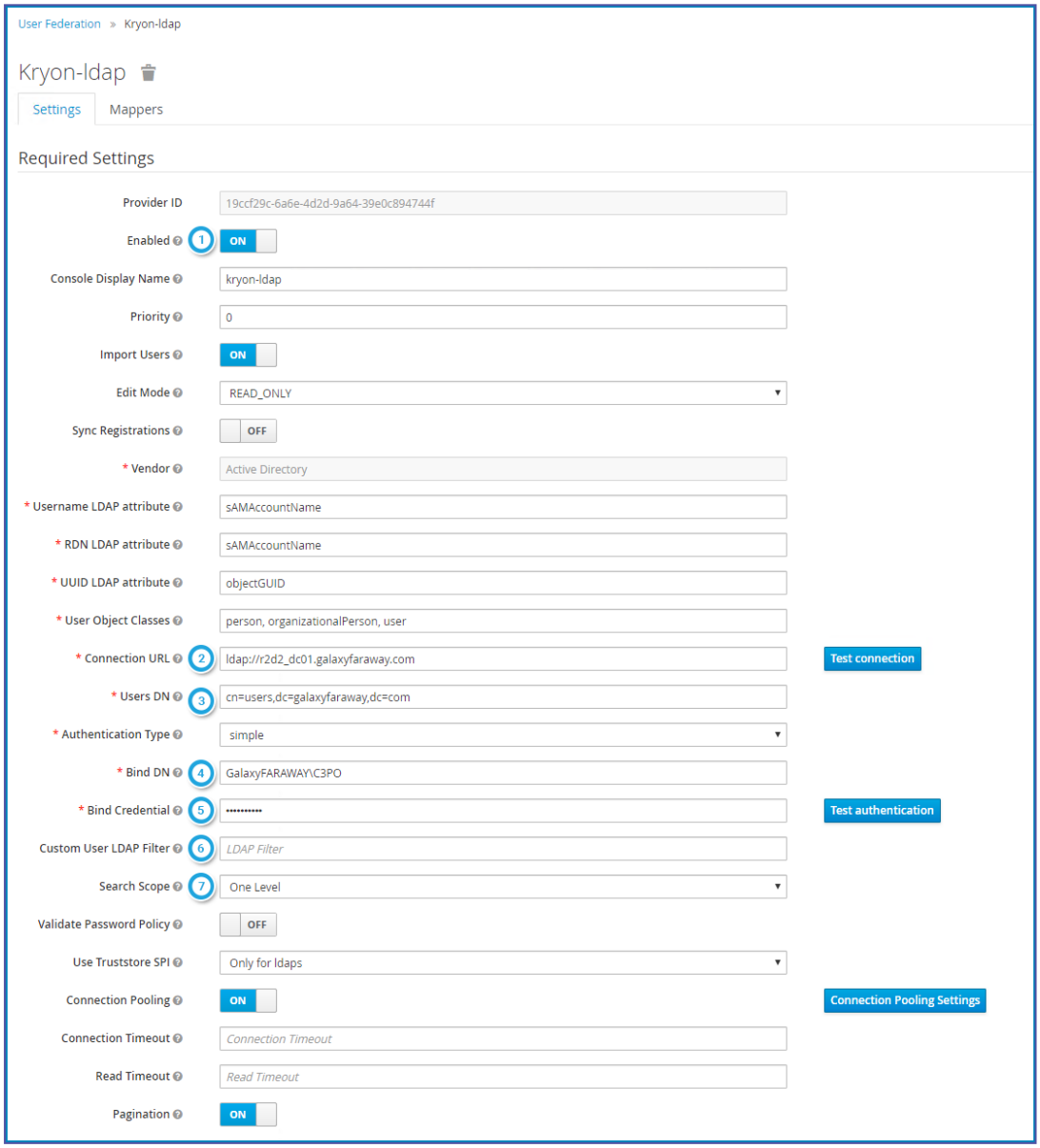
The page for defining the user federation settings will open.

NOTE

Take heart

There's no need to be intimidated by the long list of settings. Domain Administrators and other IT personnel who are experienced in working with Windows Active Directory are generally familiar with settings of this type. If you have questions about connecting to your Active Directory, consult with the Active Directory expert in your organization. If he or she can't answer your questions, get in touch with the Kryon Support team.

Required Settings section

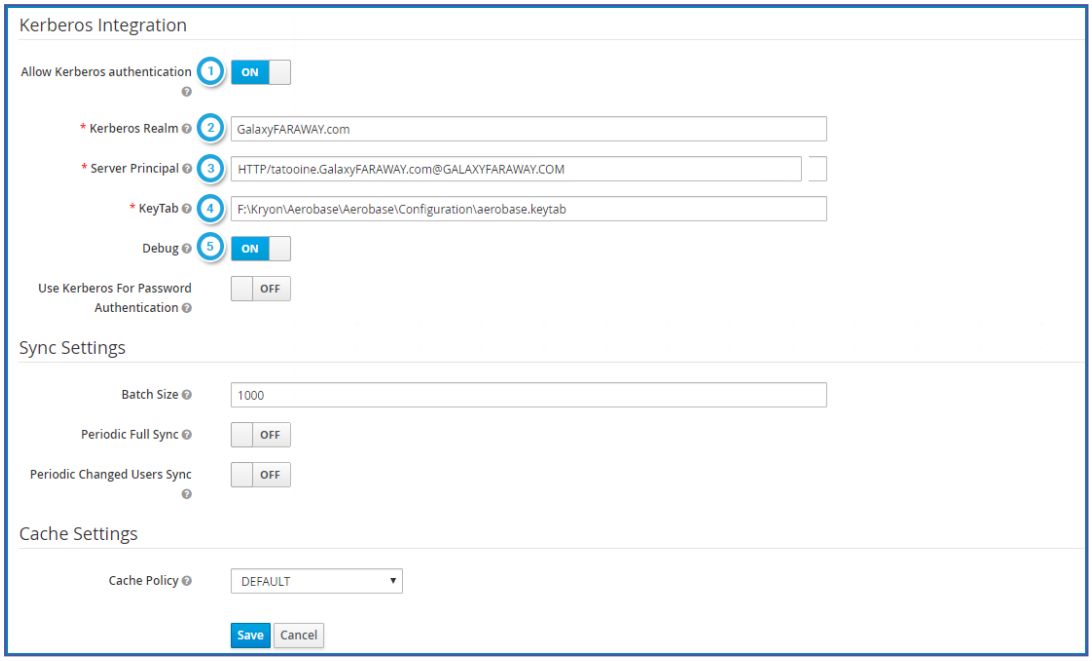


In the **Required Settings** section, these are the settings that need to be addressed. The other settings in this section can be left "as is" unless you are instructed otherwise:

1. **Enabled:** Turn this switch **ON** to enable this user federation to connect with your Active Directory.
2. **Connection URL:** `ldap://` followed by the fully qualified domain address (FQDN) of the domain controller
   - After entering the value in this field, click the **Test connection** button to confirm that the RPA server can connect to your Active Directory.
3. **Users DN:** A name that describes the path in the Active Directory where the users to sync are located. This could begin with an organizational unit (OU) or a common name (CN) and ends with one or more DCs (domain components). Learn more about the best practice of separating your Kryon users into a CN container for easier management.
   - **Example**: If your Kryon users are in an Active Directory container (CN) called `users`, and your Active Directory domain is `galaxyfaraway.com`, the entry in this field would be:

     ```
     cn=users,dc=galaxyfaraway,dc=com
     ```
4. **Bind DN:** The domain\username of the the user with rights to run Kryon services on the RPA server
5. **Bind Credential:** The password of the the user with rights to run Kryon services on the RPA server
   - After entering the **Bind DN** and the **Bind Credential**, click the **Test authentication** button to confirm that the RPA server can log in to your Active Directory.
6. **Custom User LDAP Filter:*(Optional)*** If you want to sync only specific users (by name or other attribute) from all users contained in the **Users DN**, you can set up a **Custom User LDAP Filter** (see this Microsoft article for examples of LDAP filters and syntax).
7. **Search Scope:** If your **Users DN** includes containers within it, set this value as follows:
   - **One level** → sync users from only the top level defined by the DN
   - **Subtree** → sync users from the top level defined by the DN and all its sub-levels

Kerberos Integration section



In the **Required Settings** section, these are the settings that need to be addressed. The other settings in this section can be left "as is" unless you are instructed otherwise:

1. **Allow Kerberos authentication:** Turn this switch **ON**.
2. **Kerberos Realm:** The domain name of your Active Directory
3. **Server Principal:** `HTTP/` followed by the `RPA_Server_FQDN@RPA_SERVER_DOMAIN` (exactly as defined; FQDN should be exactly as it appears in Control Panel)
   - **General format**: HTTP/ComputerFullName@DomainName@DOMAIN
   - **Exmaple:** HTTP/KSChrisLabT490.KSL.Local@ArvesSys.local@ARVESSYSLOCAL
4. **KeyTab:** The full path of the KEYTAB file on the RPA server. Following RPA server installation, the location should be as follows:

   `{InstallFolder}\IDP\Aerobase\Configuration\{filename}.keytab`

   - If the KEYTAB file was provided or generated during RPA server installation, the installation package will have copied the file to this location
   - If you generated the KEYTAB file following RPA server installation, you should have moved the file to this location as the final step in the process. See Generating a KEYTAB file.
5. **Debug:** Turn this switch **ON** to allow logging (enabling you to troubleshoot queries to the Active Directory).

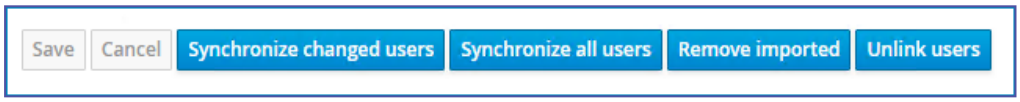
Sync Settings & Cache Settings section

The settings in this section can be left "as is" unless you are instructed otherwise.

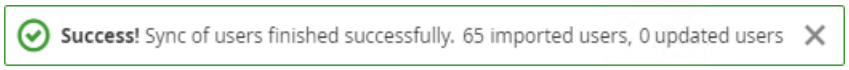
Sync users to the user federation

1. After completing all the federation settings, click the **Save** button. You should receive the following notification:

2. You will be presented with additional buttons, allowing you to sync the users from your Active Directory to the user federation:



3. Click the **Synchronize all users** button. You should receive a notification, letting you know the results of the sync:



Sync users to Kryon Admin

Now that your Active Directory users have been synced to the user federation, you can complete the Kerberos configuration process by syncing users to Kryon Admin (i.e., the Kryon database).

- For complete instructions, see ***Kryon Admin User Guide*** (Syncing from User Federation)

IMPORTANT!

Be sure to follow the steps in the ***Kryon Admin User Guide*** for creating a company and activating its license prior to syncing users to Kryon Admin.

If your license hasn't been activated prior to syncing, all users will come into the system in **Inactive** status.

RPA System Hardening and Vulnerability Management

System Hardening is ***a recommended*** process of securing a system's configuration and settings to reduce IT vulnerability and the possibility of being compromised. This can be done by reducing the attack surface and attack vectors which attackers continuously try to exploit for purpose of malicious activity.

Before Installation

- Enable Firewall:
  - Domain networks - ON
  - Guest / Public Network - ON

During Installation

- Install using a Secured Connection (SSL/TLS)
- Change the default ports
- Change the default passwords of Keycloak default user credentials:
  - Password of the Kycloack admin
  - Credentials of the test user.
- If you are using RabbitMQ, make sure to change its default password when prompted during the installation.

After Installation

- Secure Seq by enabling authentication

NOTE

You can also see the instructions on how to Encrypt database connection

How to encrypt the database connection (tutorial)

Tutorial overview:

1. Create certificate
2. Import PK to trusted root certificate
3. Import Certificate Into SQL Serve
4. Force Encryption In SQL Server
5. Verify SQL Server Connectivity Is Encrypted

Step 1: Creating certificate

NOTE

The certificate must be issued for Server Authentication. The name of the certificate must be the fully qualified domain name (FQDN) of the computer.

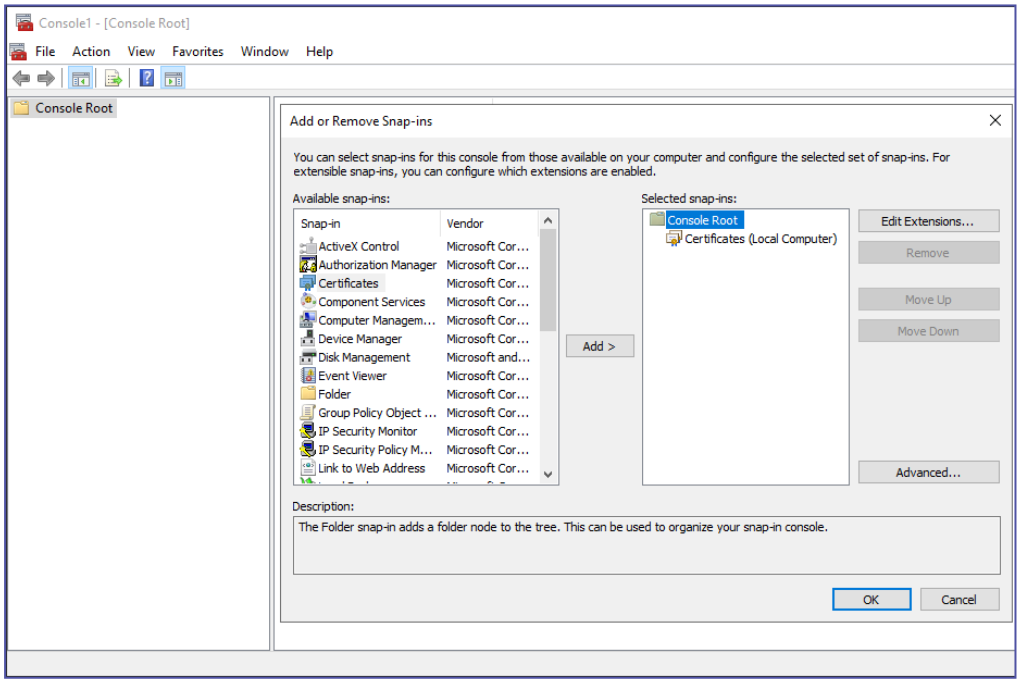
Before running the following PowerShell script, modify the `.pfk` output file location & DNS Names:

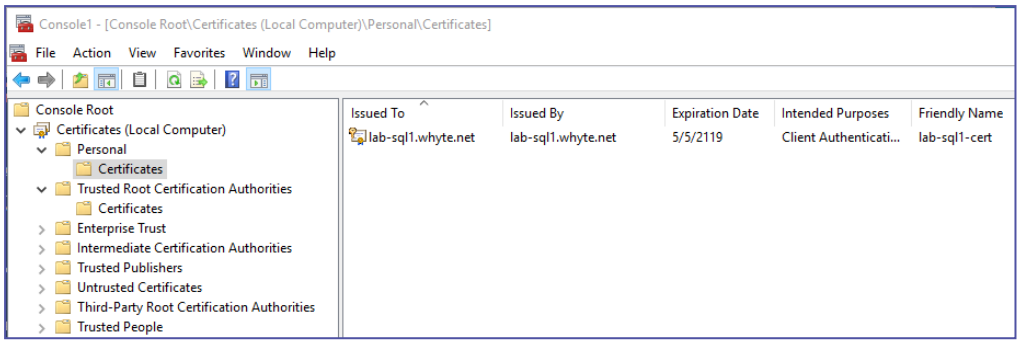
```
New-SelfSignedCertificate -DnsName lab-sql1.whyte.net -CertStoreLocation
cert:\LocalMachine\My -FriendlyName lab-sql1-cert -KeySpec KeyExchange -NotAfter (get-
date).AddYears(99)
$thumbprint = $(Get-ChildItem Cert:\LocalMachine\My).thumbprint
$Pwd = ConvertTo-SecureString -String "Str0ngePassword1!" -Force -AsPlainText
Export-PfxCertificate -Cert "Cert:\LocalMachine\My\$thumbprint" -FilePath "C:\temp_
certificates\lab-sql1pk.pfx" -Password $Pwd -Force
```

```
PS C:\Windows\system32> New-SelfSignedCertificate -DnsName lab-sql1.whyte.net -CertStoreLocation cert:\LocalMachine\My -FriendlyName lab-sql1
$thumbprint = $(Get-ChildItem Cert:\LocalMachine\My).thumbprint
$Pwd = ConvertTo-SecureString -String "Str0ngePassword1!" -Force -AsPlainText
Export-PfxCertificate -Cert "Cert:\LocalMachine\My\$thumbprint" -FilePath "C:\temp_certificates\lab-sql1pk.pfx" -Password $Pwd -Force


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
8D5A309BDE0F670DE60CD0E34550310815E22800  CN=lab-sql1.whyte.net

LastWriteTime : 5/5/2020 6:34:22 PM
Length        : 2725
Name          : lab-sql1pk.pfx
```

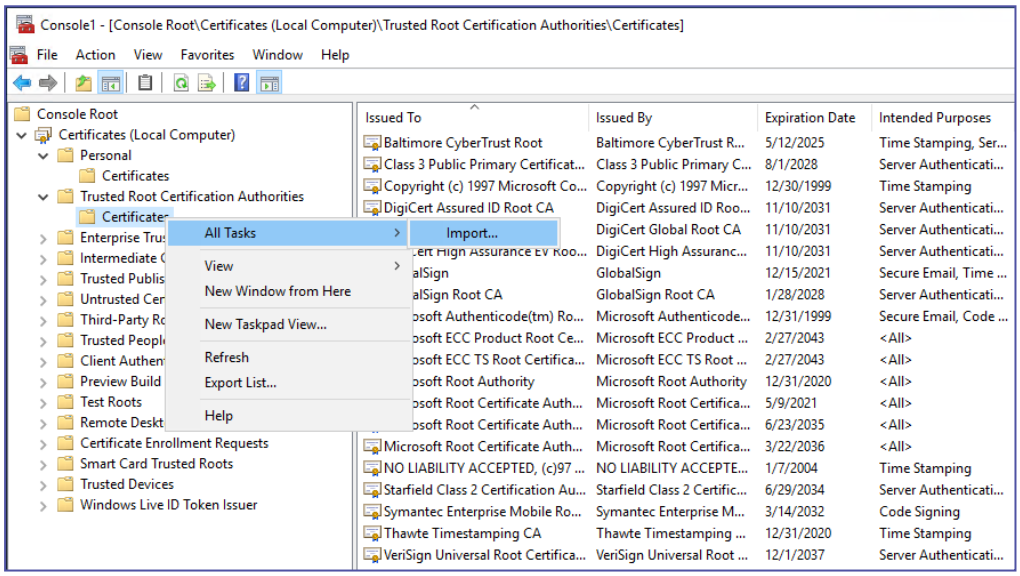
Step 2: Importing PK to trusted root certificates

a. Open Microsoft Management Console and add the Certificates (Local Computer) Snap-in:

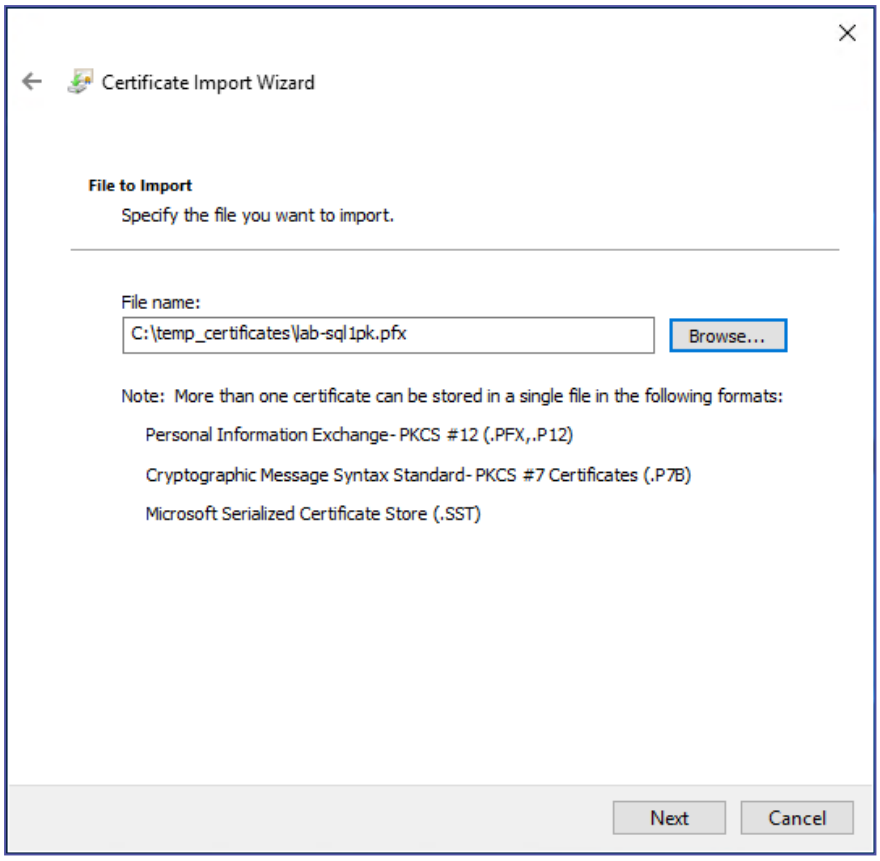




b. Expand Trusted **Root Certification Authorities** > right-click **Certificates** > **All Tasks** > **Import...**:

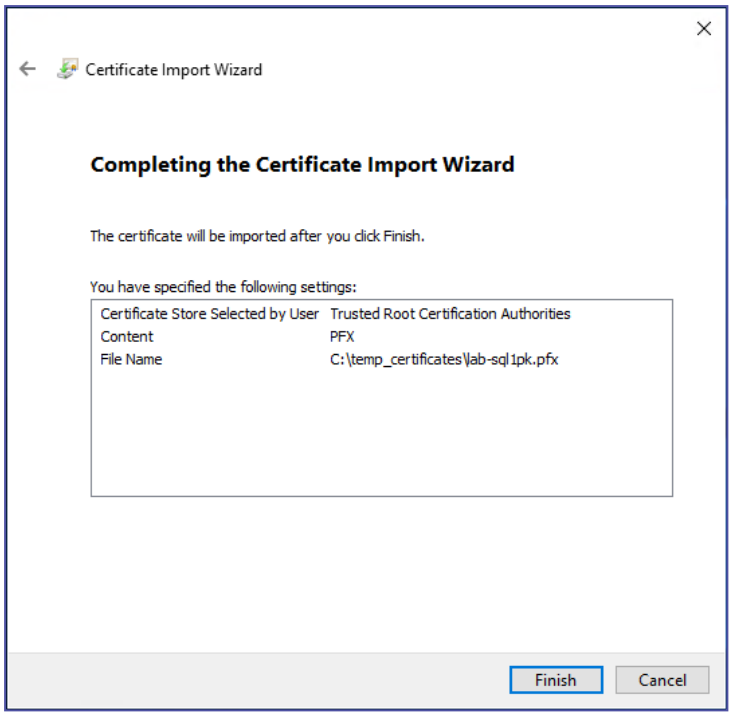


c. Navigate to the `.pfx` file:

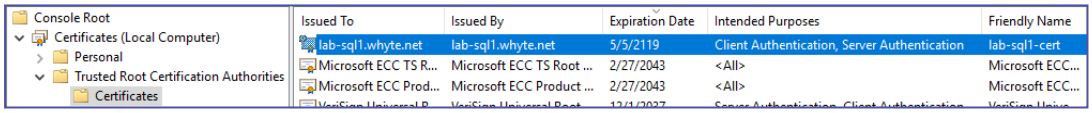


d. Enter password, check the **Include all extended properties** option, and click **Next**.

e. Click **Finish**

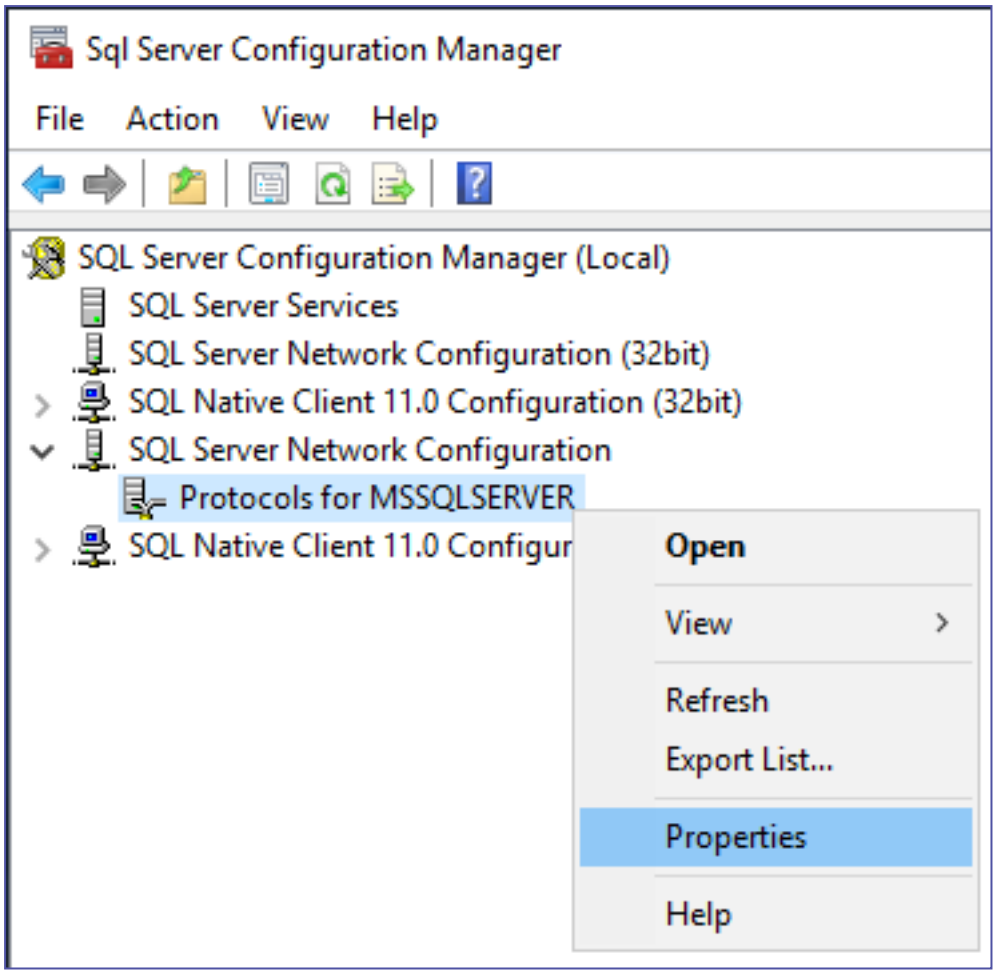


The new certificate is now available within the MMC:

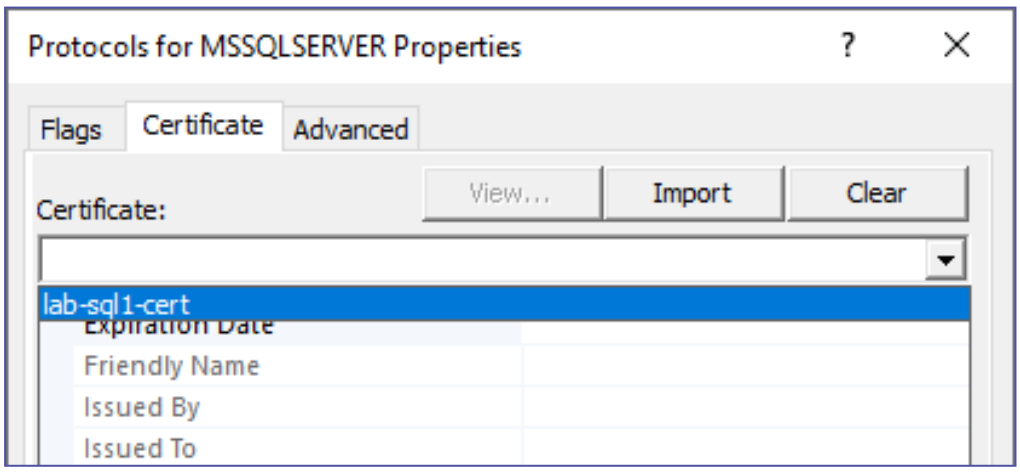


Step 3: Importing the certificate Into SQL Serve

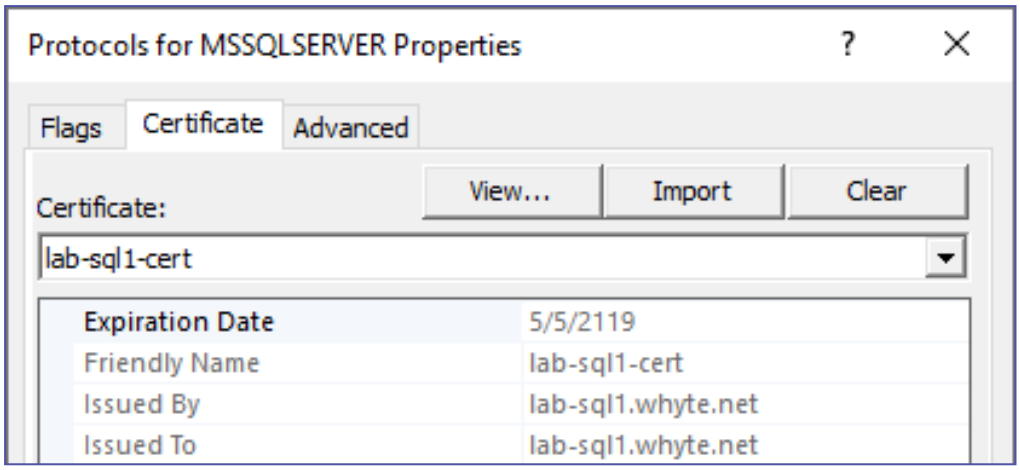
a. Open S**QL Server Configuration Manager** > right-click **Protocols for MSSQLSERVER** > **Properties**:



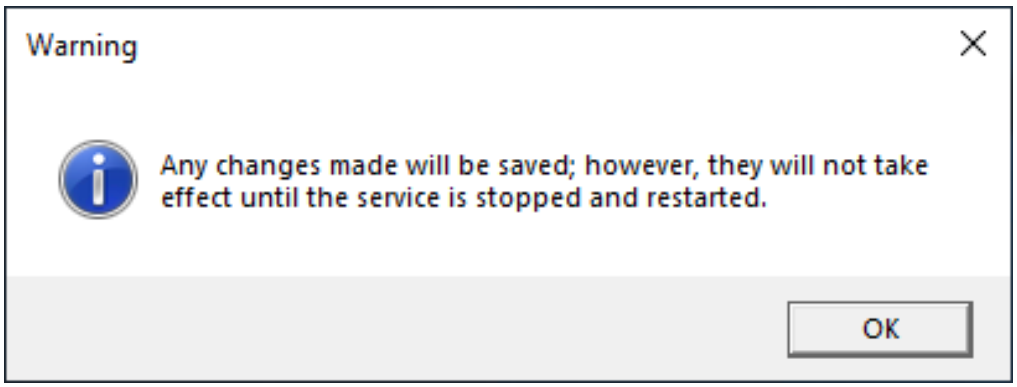
b. Open the **Certificate** tab and you should be able to view and select the new certificate from the drop-down menu:



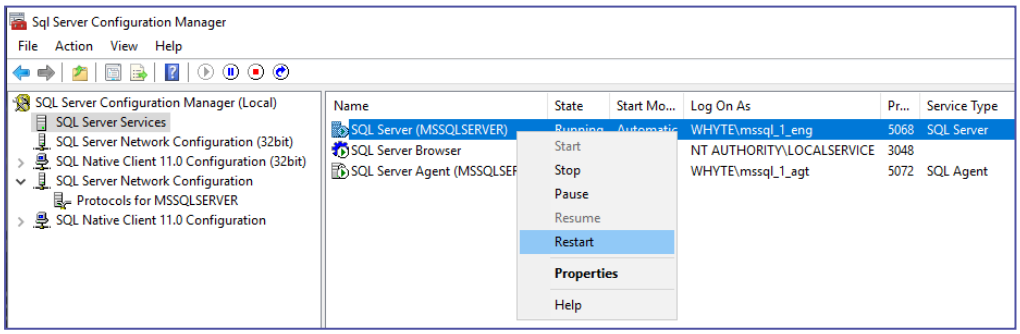
c. Click to Apply & Ok out of the window:



d. You'll get this prompt:

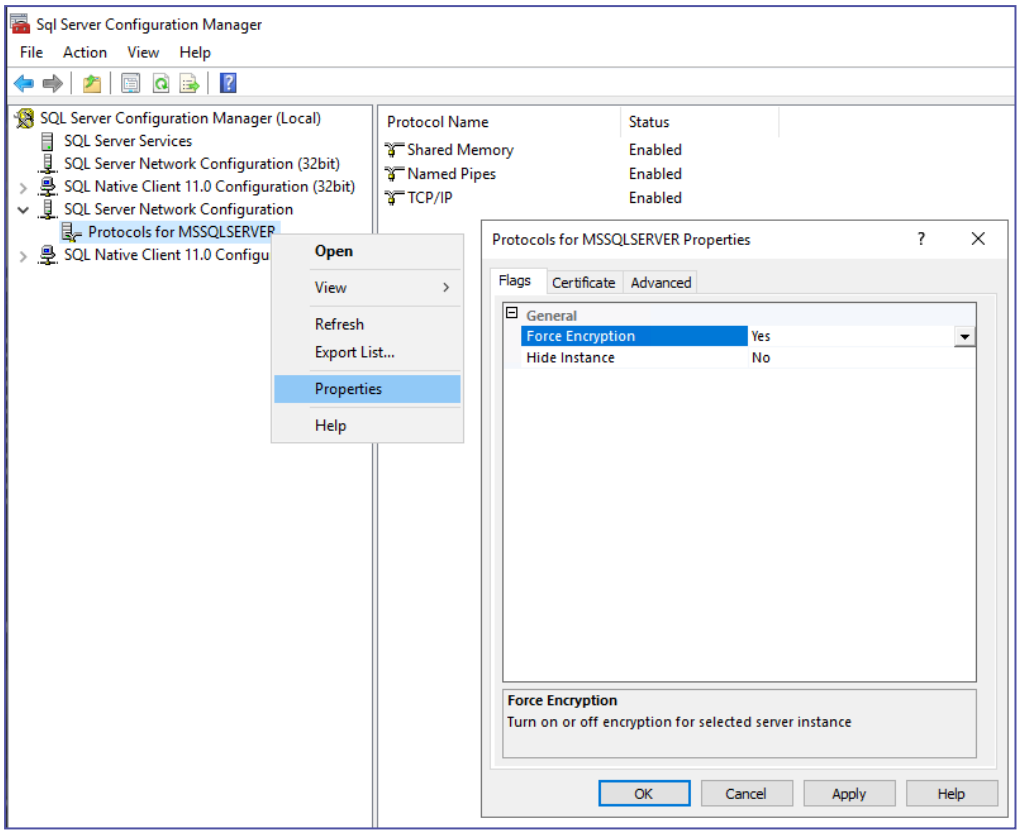


e. Restart the SQL Services from the configuration manager. If your services don't start back up again, then ensure the service accounts have the appropriate permissions. In this tutorial, the AD Service Accounts are members of the local Administrators group.

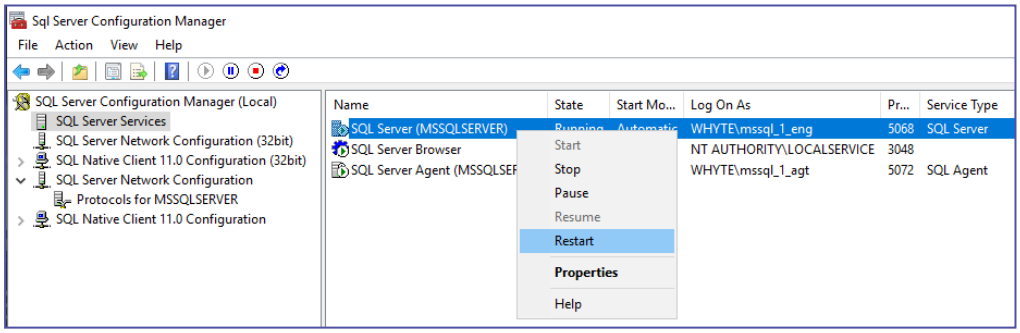


Step 4: Forcing the encryption in SQL server

a. Right-click **Protocols for MSSQLSERVER** > **Properties** > **Flags** tab > enable the **Force Encryption option**:

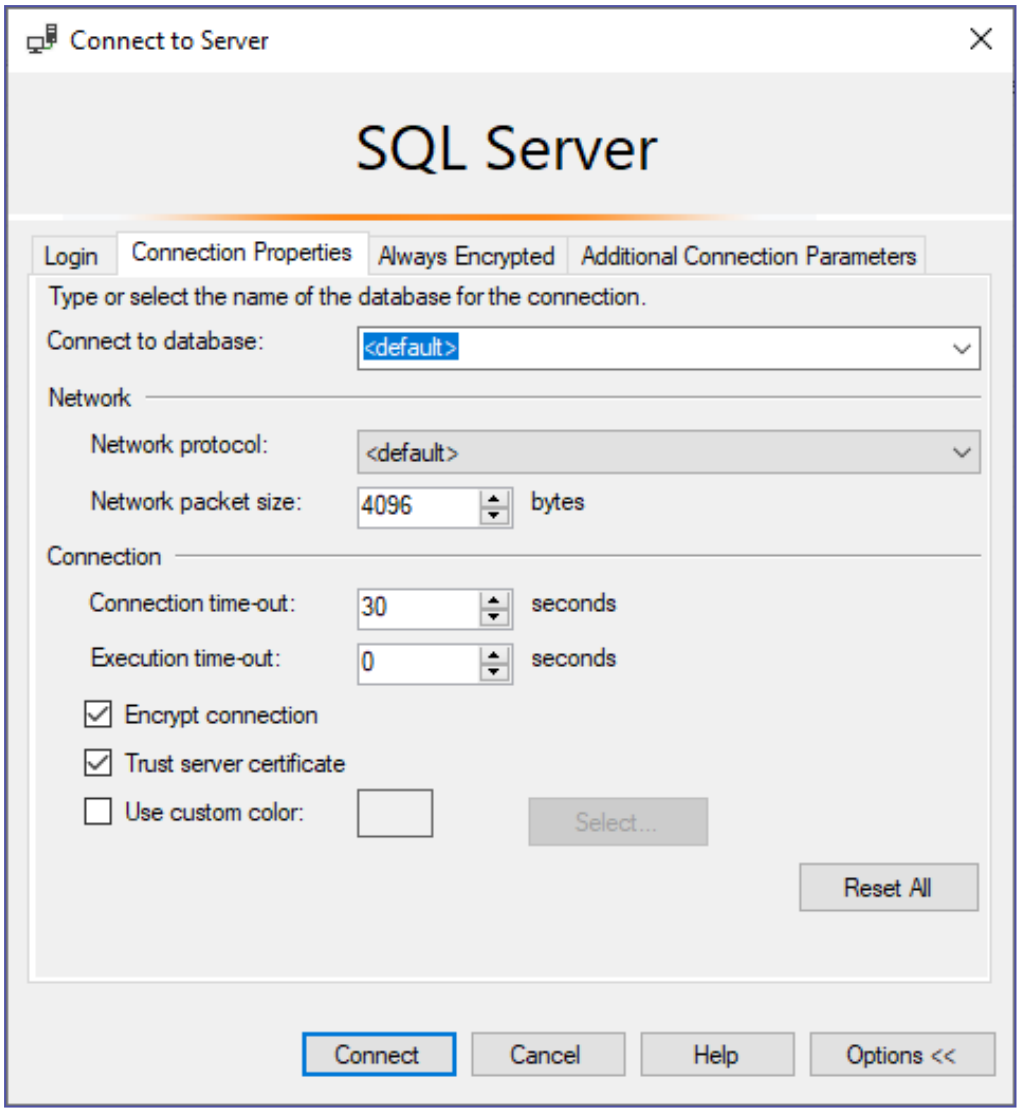


b. Restart the SQL Services:



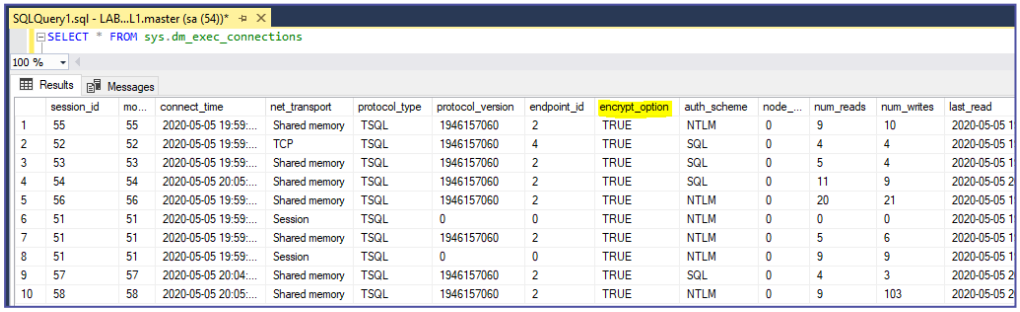
Step 5: Verifying SQL server connectivity in encrypted

a. Open a local and/or remote query session. You may have to ensure the Encrypt connection & Trust server certificate options are checked.



b. Query `sys.dm_exec_connections` to verify that the **encryption_option** is **TRUE** of all SQL connections:

```
SELECT * FROM sys.dm_exec_connections
```



	session_id	mo...	connect_time	net_transport	protocol_type	protocol_version	endpoint_id	encrypt_option	auth_scheme	node_...	num_reads	num_writes	last_read
1	55	55	2020-05-05 19:59:...	Shared memory	TSQL	1946157060	2	TRUE	NTLM	0	9	10	2020-05-05 1
2	52	52	2020-05-05 19:59:...	TCP	TSQL	1946157060	4	TRUE	SQL	0	4	4	2020-05-05 1
3	53	53	2020-05-05 19:59:...	Shared memory	TSQL	1946157060	2	TRUE	SQL	0	5	4	2020-05-05 1
4	54	54	2020-05-05 20:05:...	Shared memory	TSQL	1946157060	2	TRUE	SQL	0	11	9	2020-05-05 2
5	56	56	2020-05-05 19:59:...	Shared memory	TSQL	1946157060	2	TRUE	NTLM	0	20	21	2020-05-05 1
6	51	51	2020-05-05 19:59:...	Session	TSQL	0	0	TRUE	NTLM	0	0	0	2020-05-05 1
7	51	51	2020-05-05 19:59:...	Shared memory	TSQL	1946157060	2	TRUE	NTLM	0	5	6	2020-05-05 1
8	51	51	2020-05-05 19:59:...	Session	TSQL	0	0	TRUE	NTLM	0	9	9	2020-05-05 1
9	57	57	2020-05-05 20:04:...	Shared memory	TSQL	1946157060	2	TRUE	SQL	0	4	3	2020-05-05 2
10	58	58	2020-05-05 20:05:...	Shared memory	TSQL	1946157060	2	TRUE	NTLM	0	9	103	2020-05-05 2

Troubleshooting

AutoUpdate error 404 in Network Load-Balancer configuration

The **AutoUpdate** might throw error 404 in case of Network LoadBalancer configuration (Attended deployment)

Solution:

Open the file:

```
C:\Program
Files\
Kryon
Updater\Configuration\
KryonUpdaterServiceConfiguration.Production.json
```

And change the configuration as following:

From-

```
"UpdateServerPaths": ["http://*SERVER1_
FQDN*/AutoUpdate/Robot","http://*SERVER2_FQDN*/AutoUpdate/Robot"]
```

To -

```
"UpdateServerPaths": ["http://*LB_FQDN*/AutoUpdate/Robot"]
```

"The system administrator has set policies to prevent this installation" error

The installer might throw an "The system administrator has set policies to prevent this installation" error in case the corresponding register key is blocked.

Solution:

Set the value of the following register key to `0`:

```
HKLM\Software\Policies\Microsoft\Windows\Installer
```

- Name: "DisableMSI"
- Value: 0 (DWORD)