KRYON™

BE YOUR FUTURE

Installation & Upgrade Guide

Leo RPA Platform 5.17

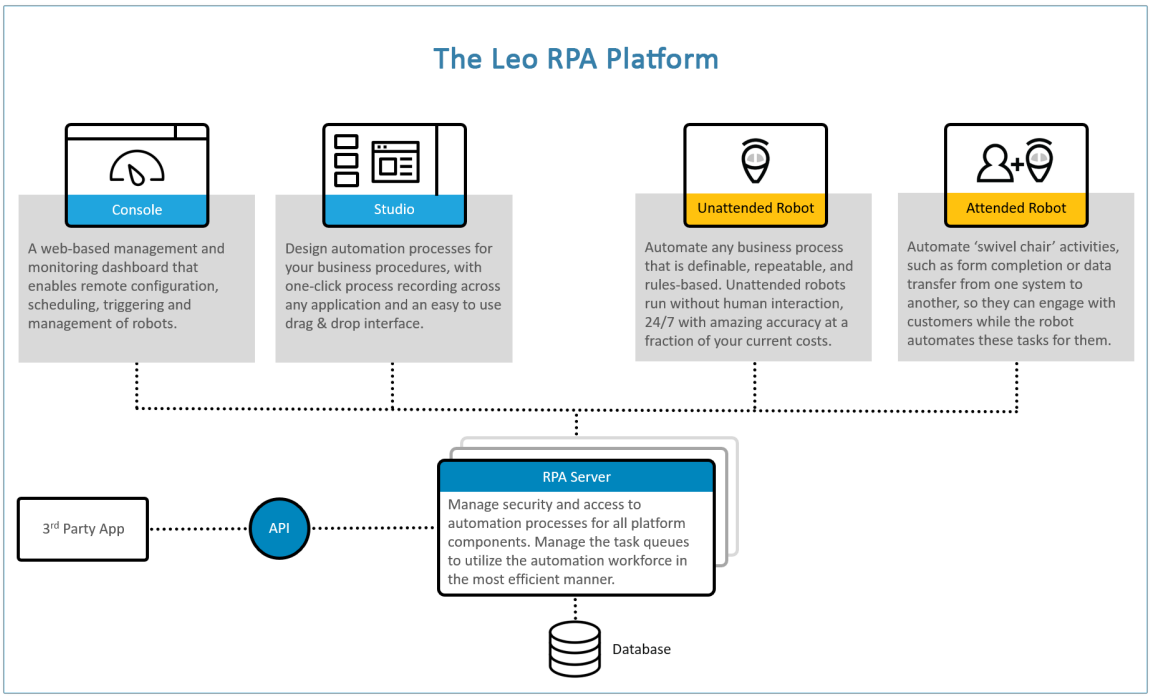
Contents

CHAPTER 1: Overview

This guide explains the steps required to install the components of the Leo RPA Platform:

- Server-side components –
  - Leo Application Server (including Leo Admin)
  - Leo Database
  - Leo Console
- Client applications
  - Leo Studio
  - Leo Unattended Robot
  - Leo Attended Robot

Platform architecture



Intended audience

The Leo Platform is an enterprise system involving multiple components and numerous 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
- SQL Server
- Internet Information Services (IIS)

This guide is intended for such IT personnel.

CHAPTER 2: Initial Considerations

Installation of the Leo RPA Platform can be customized based on 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

The Leo platform can be installed using either:

- **Domain Authentication –** client applications will connect to the Leo Application Server using network credentials defined in Windows Active Directory
- **Username & Password Authentication –** client applications (including unattended/attended robots, Studio, and Console) will connect to the Leo Application Server using usernames/passwords configured specifically for the RPA platform and defined in Leo Admin

RPA Authentication Look for this label in the guide to quickly identify instructions that vary depending on the RPA platform authentication method you choose.

Database authentication method

The Leo database can be configured to use either:

- **Windows Authentication –** the Leo Application Server will connect to the Leo database using network credentials defined in Windows Active Directory
- **SQL Server Authentication –** the Leo Application Server will connect to the Leo database server using a username/password configured specifically for the database server and defined in SQL Server Management Studio

NOTE

Either database authentication method can be used with either RPA platform authentication method.

DB Authentication Look for this label in the guide to quickly identify instructions that vary depending on the database authentication method you choose.

Automation context

If you will be using RPA in unattended or hybrid automation contexts, Leo Console is a required component of the platform. If you will be using Leo only with attended robots, Console (and the related Windows/IIS components) do **NOT** need to be installed.

Unattended/Hybrid Only Look for this label in the guide to quickly identify the sections you can skip if you are installing in an "attended only" context.

Attended/Hybrid Only Look for this label in the guide to quickly identify the sections you can skip if you are installing in an "unattended only" context.

TLS/SSL

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

- Currently, this option is supported only when the RPA platform authentication method is Domain Authentication

NOTE

If you will be installing with TLS/SSL, your organization must provide the required certificate.

TLS/SSL Look for this icon in the guide to quickly identify requirements applicable to installing with TLS/SSL and see Appendix A for detailed TLS/SSL configuration settings.

CHAPTER 3: System Requirements

	Test Server	Production Environment (minimum)	Production Environment (recommended)	
	Single Server	Single Server	Application Servers	Database Server
Machine role	Application Server + Database + Console	Application Server + Database + Console	Application Server + Console	Database
# of servers	1 physical or VM server	1 physical or VM server	2	According to organization policy – redundant or cluster
CPU	4 cores	4 cores + 1 core for each 1,000 concurrent attended/50 unattended robots	4 cores + 1 core for each 1,000 concurrent attended/50 unattended robots	4 cores
Memory	4 GB	4 GB +1 GB for each additional core (> 4)	8 GB	8 GB

	Test Server	Production Environment (minimum)	Production Environment (recommended)	
	Single Server	Single Server	Application Servers	Database Server
Robot capacity		**According to number of CPU cores –** *With 4 cores (minimum architecture)*: Max # of concurrent attended robots = 1,000 - or - Max # of concurrent unattended robots = 100 *With 4 additional cores*: Max # of concurrent attended robots = 5,000 - or - Max # of concurrent unattended robots = 300	**According to number of CPU cores –** *With 4 cores (minimum architecture)*: Max # of concurrent attended robots = 1,000 - or - Max # of concurrent unattended robots = 100 *With 8 additional cores*: Max # of concurrent attended robots = 9,000 - or - Max # of concurrent unattended robots = 500	
Disk	250 GB	250 GB	500 GB	500 GB

	Test Server	**Production Environment (minimum)**	**Production Environment (recommended)**	
	Single Server	**Single Server**	**Application Servers**	**Database Server**
Network	2 MB in/out	2 MB in/out	2 MB (in/out) per 5,000 concurrent attended or 300 concurrent unattended robots	
OS	Windows Server 2012/2016	Windows Server 2012/2016	Windows Server 2012/2016	
Windows components	**.NET Framework 4.5.1 or higher, including these features –** • TCP Port Sharing --- **Unattended/Hybrid Only** **Web Server (IIS) Server Role, including these features –** • Common HTTP Features: ○ Default Document ○ Directory Browsing ○ HTTP Errors ○ Static Content ○ HTTP Redirection	**.NET Framework 4.5.1 or higher, including these features –** • TCP Port Sharing --- **Unattended/Hybrid Only** **Web Server (IIS) Server Role, including these features –** • Common HTTP Features: ○ Default Document ○ Directory Browsing ○ HTTP Errors ○ Static Content ○ HTTP Redirection	**.NET Framework 4.5.1 or higher, including these features –** • TCP Port Sharing --- **Unattended/Hybrid Only** **Web Server (IIS) Server Role, including these features –** • Common HTTP Features: ○ Default Document ○ Directory Browsing ○ HTTP Errors ○ Static Content ○ HTTP Redirection	

	Test Server	Production Environment (minimum)	Production Environment (recommended)	
	Single Server	Single Server	Application Servers	Database Server
	• Health and Diagnostics: ∘ HTTP Logging ∘ Custom Logging ∘ Logging Tools ∘ Request Monitor • Performance • Security: ∘ Request Filtering ∘ Basic Authentication ∘ Client Certificate Mapping Authentication ∘ Digest Authentication ∘ IIS Client Certificate Mapping Authentication ∘ IP and Domain Restrictions	• Health and Diagnostics: ∘ HTTP Logging ∘ Custom Logging ∘ Logging Tools ∘ Request Monitor • Performance • Security: ∘ Request Filtering ∘ Basic Authentication ∘ Client Certificate Mapping Authentication ∘ Digest Authentication ∘ IIS Client Certificate Mapping Authentication ∘ IP and Domain Restrictions	• Health and Diagnostics: ∘ HTTP Logging ∘ Custom Logging ∘ Logging Tools ∘ Request Monitor • Performance • Security: ∘ Request Filtering ∘ Basic Authentication ∘ Client Certificate Mapping Authentication ∘ Digest Authentication ∘ IIS Client Certificate Mapping Authentication ∘ IP and Domain Restrictions	

	Test Server	Production Environment (minimum)	Production Environment (recommended)	
	Single Server	Single Server	Application Servers	Database Server
	○ URL Authorization ○ Windows Authentication • Application Development: ○ .NET Extensibility 4.5 (or above) ○ ASP.NET 4.5 (or above) ○ ISAPI Extensions ○ ISAPI Filters • Management Tools: ○ IIS Management Console ○ IIS Management Scripts and Tools ○ Management Service	○ URL Authorization ○ Windows Authentication • Application Development: ○ .NET Extensibility 4.5 (or above) ○ ASP.NET 4.5 (or above) ○ ISAPI Extensions ○ ISAPI Filters • Management Tools: ○ IIS Management Console ○ IIS Management Scripts and Tools ○ Management Service	○ URL Authorization ○ Windows Authentication • Application Development: ○ .NET Extensibility 4.5 (or above) ○ ASP.NET 4.5 (or above) ○ ISAPI Extensions ○ ISAPI Filters • Management Tools: ○ IIS Management Console ○ IIS Management Scripts and Tools ○ Management Service	

	Test Server	Production Environment (minimum)	Production Environment (recommended)	
	Single Server	Single Server	Application Servers	Database Server

Additional software	• Microsoft Visual C++ 2005 Redistributable (x64)
	• Microsoft Visual C++ 2013 Redistributable (x64)
	• Microsoft Visual C++ 2015 Redistributable (x64)
	• SQL Server Express 2012/2014/2016 ***(NO license required)***, including these components:
	  ◦ Database Engine Services
	  ◦ Basic Management Tools
		• Microsoft Visual C++ 2005 Redistributable (x64)
		• Microsoft Visual C++ 2013 Redistributable (x64)
		• Microsoft Visual C++ 2015 Redistributable (x64)
		• SQL Server 2012/2014/2016 (Standard edition and higher, ***license required***), including these components:
		  ◦ Database Engine Services
		  ◦ Basic Management Tools
			• Microsoft Visual C++ 2005 Redistributable (x64)
			• Microsoft Visual C++ 2013 Redistributable (x64)
			• Microsoft Visual C++ 2015 Redistributable (x64)
				SQL Server 2012/2014/2016 (Standard edition and higher, ***license required***), including these components:
				• Database Engine Services
				• Basic Management Tools

CHAPTER 4: Preparing the Environment

Follow these preliminary steps to prepare your environment for the installation of the Leo RPA Platform:

- Open required firewall ports
- Verify/create user
- Install required components
- Start port-sharing service

Open required firewall ports

Leo's default port configuration is as follows. (Server-side ports are fully configurable, and you will have the opportunity to specify them during Application Server installation):

Protocol	Server-side inbound port (configurable)	Client-side outbound port	Friendly name (for purposes of this guide)
HTTP	80	dynamic	***HTTP Port***
Net.TCP	443	dynamic	***Net.TCP Port***
HTTPS	8080	dynamic	***HTTPS Port***

Follow these steps to prepare your network for Leo installation:

1. Open ports for HTTP and Net.TCP protocols as shown in the table above (or using the port numbers you will specify during Application Server installation)
2. TLS/SSL If you are installing with TLS/SSL, open a port for the HTTPS protocol as shown in the table above (or using the port number you will specify during Application Server installation)
3. Unattended/Hybrid Only
   - Open an additional port of your choice to be used by Leo Console – let's call this ***Console Port***
   - Open an additional port of your choice to be used by the Leo Web Service API – let's call this one ***API Port***
     - This is required only if you will be using the API as a method of managing unattended robot tasks
   - Open Port 8090 if you will be installing Leo Application Server and Leo Console (IIS) on different machines

> **TIP**
>
> Be sure to write down the relevant port numbers; you will use them when configuring Console.

Verify/create user

RPA Authentication Ensure that there is a user (or create a user) with rights to run Leo services on the Application Server:

- If you will be using Domain Authentication, this user must:
  - be a member of the domain (in Active Directory); and
  - have local administrative rights for the machine on which Leo Application Server will be installed
- If you will be using Username & Password Authentication, this user must:
  - have local administrative rights for the machine on which Leo Application Server will be installed (can be either a domain user or a local system account)

Install required components

Install required Windows components and any additional required software on all machines as specified in System Requirements.

Start port-sharing service

Configure the Net.TCP Port Sharing service to `Automatic start` and start the service (on the machine on which Leo Application Server will be installed).

CHAPTER 5: Preparing the Leo Database Server

SQL Server instance

1. Ensure that an instance of SQL Server is installed on a machine that will be accessible over the network to the Leo Application Server
   - The Leo Database Server can be installed on the same machine as the Application Server if machine resources are sufficient
   - The supported database engine for the Leo Database Server is SQL Server 2012 and above
     - Required SQL components: Database Engine Services and Basic Management Tools
2. Open **SQL Server Management Studio** and connect to the database server

Create a login to the SQL Server

Create a login by which the Leo Application Server will access the database:

1. In the **Object Explorer**, right-click **Security** and select **New > Login**
2. DB Authentication Enter the following data to create the login:
   - If you are using Windows Authentication as your database authentication method:
     - **Authentication:** Windows authentication
     - **Login name:** the user with administrative rights to run Leo services (as verified/created in Preparing the Environment)
   - If you are using SQL Server Authentication as your database authentication method:
     - **Authentication:** SQL Server authentication
     - **Login name:** set as desired
     - **Password:** set as desired
     - **Enforce password policy:** disabled
3. Ensure that `sysadmin` is enabled on the **Server Roles** page of this login's properties

Create a database

Create a new empty database:

- **Database name:** set as desired (e.g., RPA_Database)
- **Owner:** login name created above

TIP

Hold on to that info!

You will need the database server's machine name, database name, and login information when Installing the Leo Application Server.

CHAPTER 6: Installing the Leo Application Server

Overview

Leo Application Server is based on Windows services. It consists of 17 different services that serve the Leo Robot and Leo Studio clients, as well as Leo Console.

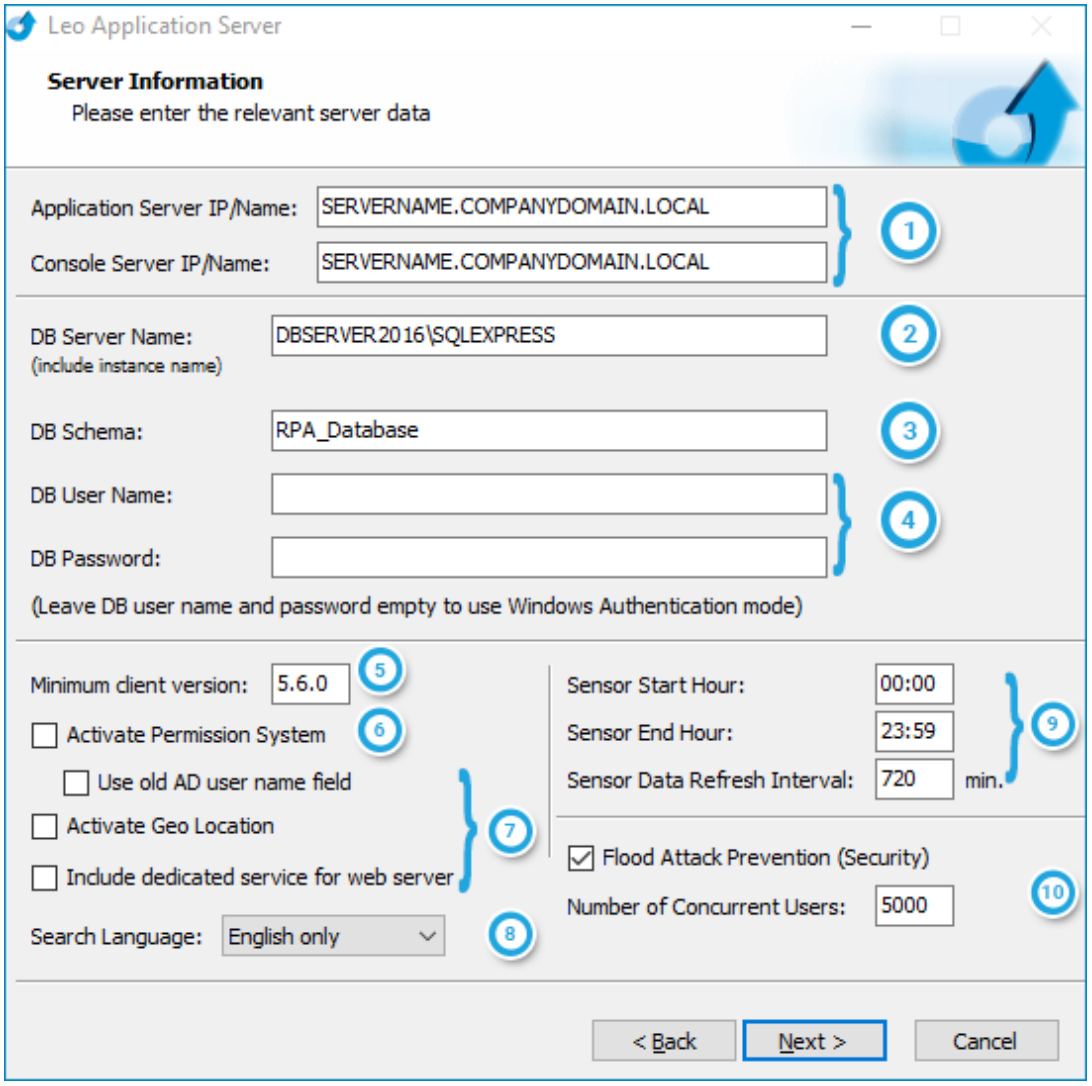
NOTE

Running the Leo Application Server installation kit requires administrator user permissions.

Installation

Follow these steps to install Leo Application Server:

1. Run the Leo Application Server installation kit **as administrator**
2. On the **Server Information** screen, enter the required information as follows:



1 **Application Server IP/Name:** the IP address of the application server or its full computer name as identified by Windows (including computer name and domain)

- Example: `USSERVER.OURCOMPANY.LOCAL`

2 **Database Server Name:** the name of the machine on which the Leo database was created, including the instance name in which the database is defined (syntax: `servername\instancename`)

3 **Database Schema:** the name of the Leo database (see Preparing the Leo Database Server)

4 **DB Authentication**

Database User Name & Database Password: login name and password created for the Leo database server (see Preparing the Leo Database Server)

- If you selected Windows Authentication as your database authentication method, these fields **should be left blank**

- If you are using SQL Server Authentication as your database authentication method, these fields **are required**

5 **Client Minimum Version:** minimum Leo client version required to connect to the Leo Application Server

- By default, the client version is the same as the version of the Leo Application Server you are installing
  - In general, clients should be maintained on the same version as the server (i.e., when you upgrade the server to a new version, clients should be updated as well)
- Clients include unattended/attended robots and Leo Studio

6 **Activate Permissions System:** tick this checkbox to enable the Leo RPA platform's internal permissions system

- This system enables the assignment of permissions (read/write/publish) to Studio users and robots with respect to specific catalogs and categories of automation workflows

7 **Use old AD user name field**, **Activate Geo Location**, and **Include dedicated service for web server**: deprecated (should not be used)

8 Attended/Hybrid Only **Search Language:** language(s) to be supported by the Leo search engine

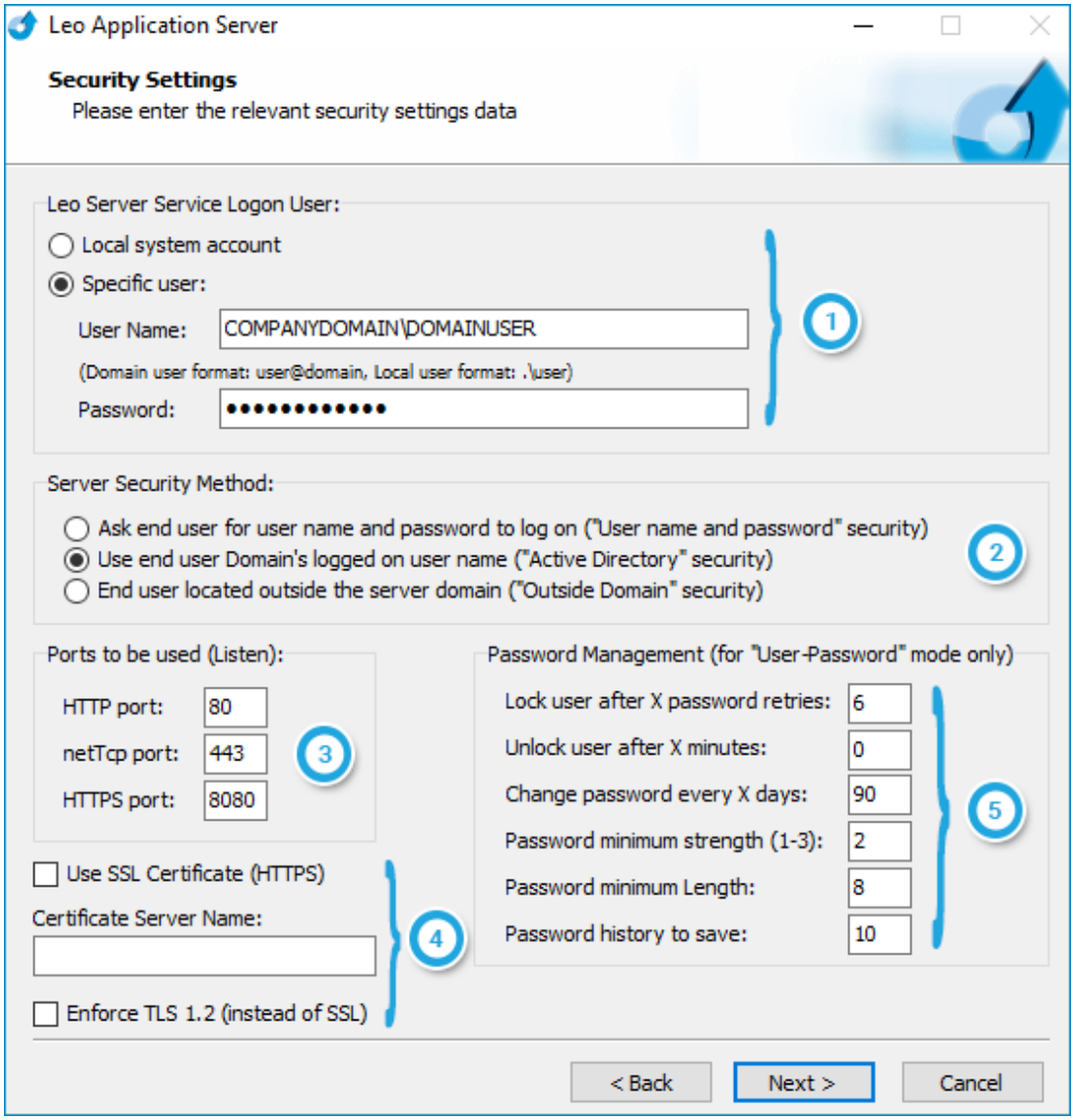
9 Attended/Hybrid Only

- **Sensor Start Hour:** daily scheduled start time for Leo sensors
- **Sensor End Hour:** daily scheduled end time for Leo sensors
- **Sensor Data Refresh Interval:** data refresh intervals for Leo sensors

10 **Flood Attack Prevention:** tick this checkbox to enable DDoS attack prevention

- **Number of concurrent users:** maximum number of concurrent users to be supported by the server (when flood attack prevention is enabled)

3. On the **Security Settings** screen, enter the required information as follows:



1 **RPA Authentication** **TLS/SSL**

Leo Server Service Logon User: the user verified/created when Preparing the Environment

- If you will be using Domain Authentication or when installing with TLS/SSL, choose the **Specific user** option
- If you will be using Username & Password Authentication, you can choose either option: **Local system account** or **Specific user**

When using the **Specific user** option, enter the user's credentials

- Domain user format = `domain\user` or `user@domain`
- Local user format = `.\user`

2 **RPA Authentication**

Server Security Method:

- For Domain Authentication, choose the **"Active Directory" security** option
- For Username & Password Authentication, choose the **"User name and password"** security option

NOTE: The **"Outside Domain" security** method has been deprecated and should not be used.

3 **Ports to be used (Listen):**

The port numbers for –

- the HTTP Port,
- the Net.TCP Port, and
- TLS/SSL the HTTPS Port

as opened when Preparing the Environment

4 TLS/SSL

Use SSL Certificate (HTTPS):

- Tick this checkbox if you will be using Leo with TLS/SSL; and
- supply the full computer name (as identified by Windows) of the Certificate Server

Enforce TLS 1.2:

- Tick this checkbox to require the use of only the TLS protocol (and disable the use of the SSL protocol)

5 RPA Authentication **Password Management:** password policy configuration

- These fields are applicable only when using Username & Password Authentication

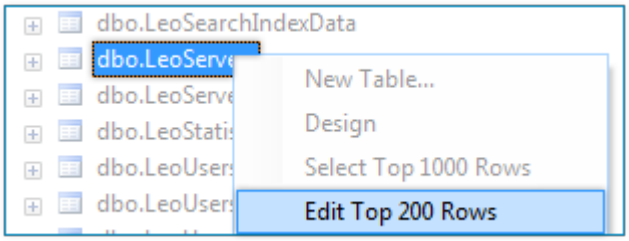
CHAPTER 7: Creating the Leo Application Database

Follow these steps to create the Leo application database:

1. From the Leo application server, open SQL Server Management Studio and connect to the database server
2. In Windows File Explorer, browse to the folder where the Leo application server files are installed and locate the file **Create Minimum DB.sql**
   - The default location is `C:\Program Files\Leo Application Server`
3. In SQL Server Management Studio, open a new query, drag the file into the **New Query** window and execute it

> **NOTES**
>
> - Make sure that you run the query on the correct schema by selecting it before opening the new query
> - Ensure that the query runs with no errors

4. Update the **dbo.LeoServers** table with the Application Server IP/Name 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='<Application Server IP or Name>';
       ```
       - 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 name or IP address of the application server

USDBSERVER\SQLEX...- dbo.LeoServers

	ServerID	ServerName	ProcessName	ServerType
	1	ComputerName	NULL	1
	2	ComputerName	NULL	2
▶*	NULL	NULL	NULL	NULL

5. Create the Software AG administrator login for **Leo Admin**:
   a. Locate the file **adminsag.sql** (provided to you separately)
   b. Open a new query, drag the file into the **New Query** window and run it
   c. Make note of the username and password
   - **username:** sagadmin
   - **password:** Sagadmin123!
6. Restart all Leo services:
   a. Navigate to `C:\Program Files\Leo Application Server`
   - Right-click `StopAll.bat`, and select **Run as administrator**
   - Right-click `StartAll.bat`, and select **Run as administrator**

CHAPTER 8: Configuring Leo Console

Unattended/Hybrid Only

Follow these steps to configure Leo Console:

- Define MIME types
- Define website #1 (Console)
- Define application (ConsoleApp)
- Define website #2 (WebAPI) – applicable only if you will be using the API as a method of managing unattended robot tasks
- Restart the server

Define MIME types

1. Ensure that the extensions **.woff** and **.woff2** appear in the list of defined MIME types
   - If these extensions do not appear, add them as follows:
     - **File name extension:** `.woff`

       MIME type: `font/x-woff`
     - **File name extension:** `.woff2`

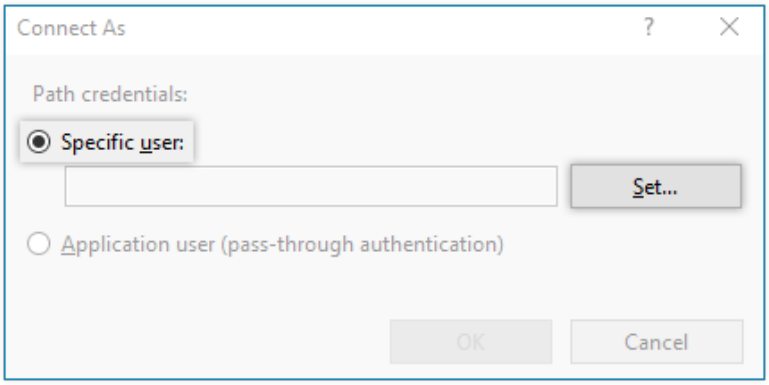
       MIME type: `application/font-woff2`

Define website #1 (Console)

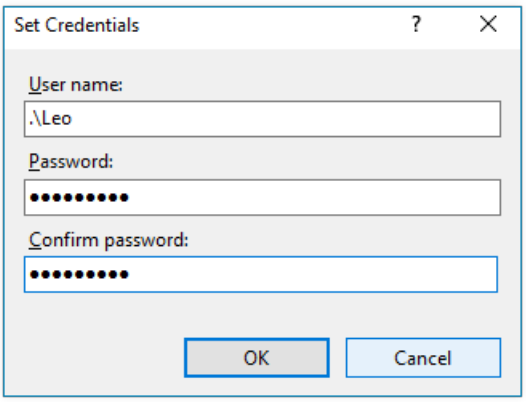
2. Under **Sites** in the **Connections** pane, add the **console** website as follows:
   - **Site name:** `console`
   - **Physical path:** `<Leo Application Server path>\Leo Web Server 64bit\Console\Client`
     - For example: `C:\Program Files\Leo Application Server\Leo Web Server 64bit\Console\Client`
   - **Port:** Port number of the Console Port (as opened when Preparing the Environment)
   - TLS/SSL **Binding Type:** If you will be using Leo with TLS/SSL, be sure to change the **Binding Type** to `https`

> **TIP**
>
> (Optional) If this server is dedicated to the Leo platform, you can remove the **Default Web Site**.

3. RPA Authentication If you are using Domain Authentication, configure connection to the **console** site as a specific user:
   a. Click the Connect as... button
   b. In the **Connect As** dialog, choose the **Specific user** option and click the **Set** button



   c. In the **Set Credentials** dialog, enter the user name and password for the Leo Server Service Logon User (i.e., the user verified/created when Preparing the Environment)



NOTE

Watch the syntax!

The characters `.\` should precede the user name in this dialog

d. Click **OK** to save the **Connect As** settings

e. Click the Test Settings... button to verify configuration

- Ensure that both the **Authentication** and **Authorization** tests are successful

Define application (ConsoleApp)

4. Under the **console** site you just created, add the **ConsoleApp** application as follows:
   - **Alias:** `ConsoleApp`
   - **Physical path:** `<Leo Application Server path>\Leo Web Server 64bit\Console\API`
     - For example: `C:\Program Files\Leo Application Server\Leo Web Server 64bit\Console\API`

5. RPA Authentication For Domain Authentication, follow the instructions in step 3 again to configure connection to the **ConsoleApp** application as a specific user

Define website #2 (WebAPI)

If you will be using the API as a method of managing unattended robot tasks –

6. Under **Sites** in the **Connections** pane, add the **WebAPI** website as follows:
   - **Site name:** `WebAPI`
   - **Physical path:** `<Leo Application Server path>\Leo Web Server 64bit\WebAPI`
     - For example: `C:\Program Files\Leo Application Server\Leo Web Server 64bit\WebAPI`
   - **Port:** Port number of the API Port (as opened when Preparing the Environment)
   - TLS/SSL **Binding Type:** If you will be using Leo with TLS/SSL, be sure to change the **Binding Type** to `https`
7. RPA Authentication For Domain Authentication, follow the instructions in step 3 again (last time!) to configure connection to the **WebAPI** site as a specific user
8. Ensure that **ONLY** Anonymous Authentication is enabled for the **WebAPI** site
   - Disable all other authentication methods for this site
9. RPA Authentication If you are using Username & Password Authentication, follow these steps to edit the API server configuration:
   - With a text editor, open the file `<Leo Application Server path>\Leo Automation Server 64bit\Controller\Config\appSettings.config`
     - The default file location is `C:\Program Files\Leo Application Server\Leo Automation Server 64bit\Controller\Config\appSettings.config`
   - Find the line that reads: `<add key="APIAuthenticationProvider" value="OutsideDomain" />` and change the value to `UserPassword`
     - The full line should now read: `<add key="APIAuthenticationProvider" value="UserPassword" />`

Restart the server

10. Restart the IIS Server

CHAPTER 9: Installing Leo Clients

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

- Run the appropriate installation package
- Configure the client application's connection to the Leo Application Server
- Unattended/Hybrid Only Enable unattended robot mode (applicable to unattended robots only)

NOTE

In certain situations, additional steps are required:

- If you are using the Leo SmartScan solution, see Configure SmartScan
- TLS/SSL If you are using Leo with TLS/SSL, see Configure clients for TLS/SSL

Run the installation package

Run the appropriate ***.msi** installation package on the client machine:

Client Application	Installation Package
Unattended/Attended Robot	LeoPlayerFullSetup_32bit.msi ***- or -*** LeoPlayerFullSetup_64bit.msi (as appropriate for the client machine) ***– or –*** LeoPlayerFullSetup_32bit64bit.exe (installation wizard will automatically install the appropriate version for the client machine)
Leo Studio	LeoStudioFullSetup_64bit.msi

TIP

Set up the server connection first

In the last step of the installation wizard, uncheck the option to run the client immediately. Configuring the server connection before running the client will save you some time (never a bad thing!)

Configure the server connection

1. With a text editor, open one of the following configuration files –
   - For robot clients: `C:\Program Files\Leo\Config\appSettings.config`
   - For Leo Studio: `C:\Program Files\Leo Studio\Config\appSettings.config`
2. Find the line that begins: `<add key="MainServerNames"`, and change the value to the Application Server IP/Name
   - The full line should now read: `<add key="MainServerNames" value="{Application Server IP or Name}" />`
3. Find the lines that read:
   - `<add key="NetComPort" value="443" />`
   - `<add key="HttpComPort" value="80" />`
   - `<add key="HttpsComPort" value="443" />`

   and change the values as follows:
   - `<add key="NetComPort" value="Net.TCP Port number" />`
   - `<add key="HttpComPort" value="HTTP Port number" />`
   - TLS/SSL `<add key="HttpsComPort" value="HTTPS Port number" />`

   (where port numbers are the ports opened when Preparing the Environment)

Unattended/Hybrid Only Enable unattended robot mode

For unattended robots, enable unattended robot mode:

1. With a text editor, open the file `C:\Program Files\Leo\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="RunAutomationEnabled" value="True" />`

Configure SmartScan

If you are using the Leo SmartScan solution, configure each Studio client as follows:

1. With a text editor, open one of the file `C:\Program Files\Leo Studio\Config\appSettings.config`
2. At the end of the file (but before the line that reads: `</appSettings>`), add a line that

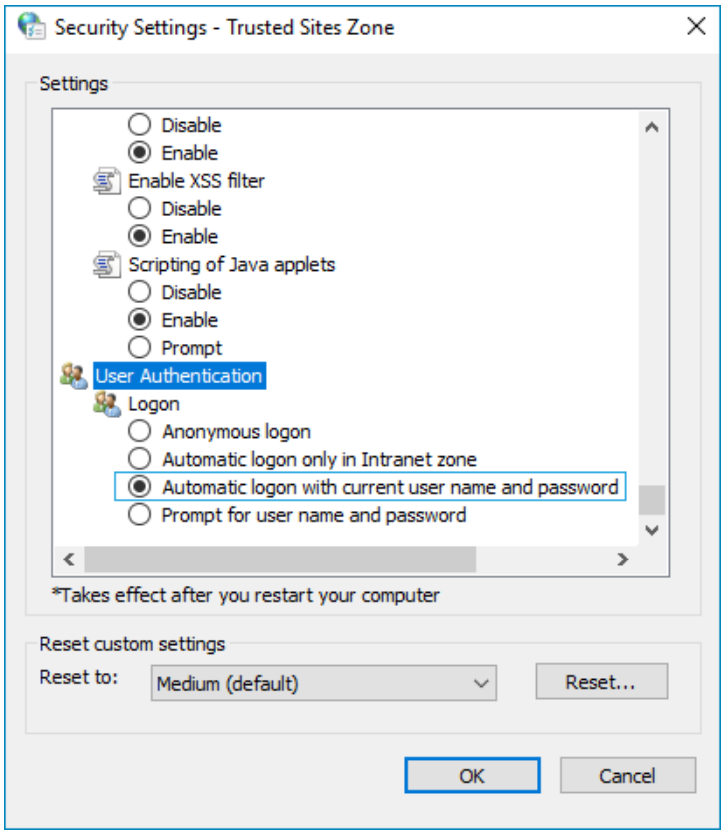
reads

```
<add key="EnableSmartScanAC" value="true" />
```

TLS/SSL Configure clients for TLS/SSL

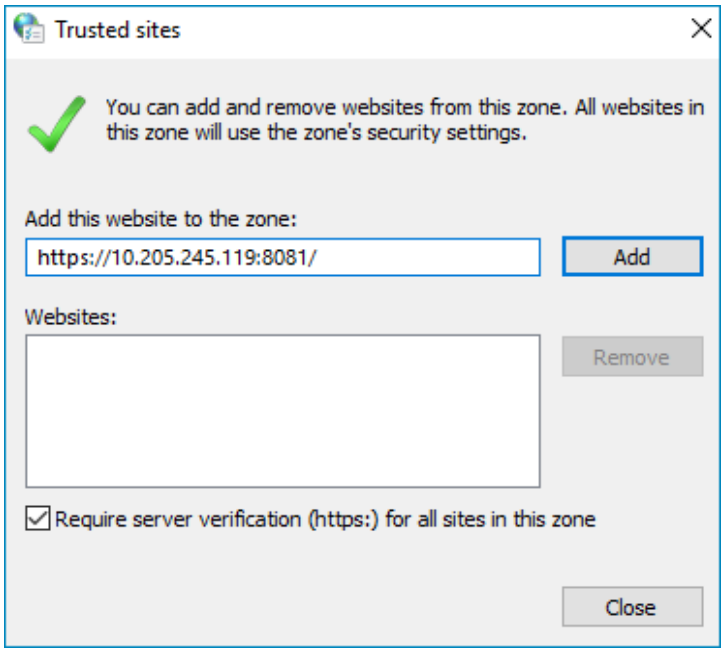
If you are using Leo with TLS/SSL, configure each client machine as follows:

1. Go to **(Control Panel > Internet Options > Security**
2. Click on the icon for the **Trusted sites** zone
   a. Change the **Security Settings** for this zone:
      - Click the Custom level... button
      - Scroll all the way down to the end of the long list, and under **User Authentication > Logon**, select **Automatic logon with current user name and password**



   b. Add the Leo Console URL to the **Trusted Sites** zone:
      - With the icon for the **Trusted Sites** zone still selected, click the Sites button

- Enter the Leo Console URL and click Add



CHAPTER 10: Upgrading to a New Version

Follow these steps to upgrade to a newer version of the Leo RPA Platform.

Upgrade server-side components

1. Back up the current Leo Application Server installation
   a. Copy the Leo application server folder (by default, `C:\Program Files\Leo Application Server`) to a different location (either locally or on a different machine)

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

2. Back up the Leo database:
   a. From the Leo application server, open SQL Server Management Studio and connect to the database server
   b. In the Object Explorer, right-click the Leo database and select **Tasks > Back Up**
   c. Give the **Backup set** a name and set the **Destination** to which the backup will be saved
3. Prepare the database for the new version:
   a. Obtain the necessary database upgrade scripts from Kryon Support
      - Run the following query on the database: `select * from LeoDBVersion order by 1 desc`. The result will be a list of Leo server versions.
      - Email this result to support@kryonsystems.com. The Kryon Support team will send you the required database script(s).
   b. Run the database scripts on the database, one by one, from the earlier version to the newer version

   > **CAUTION**
   >
   > Run the scripts in numerical order to avoid database corruption.

4. Install the new version of Leo Application Server (see Installing the Leo Application Server for complete instructions)
   - As part of the installation wizard, you will be prompted to uninstall the prior version
5. Migrate automation workflows to the new version

a. *Preliminary step:* allow multiple connections to the database

- Run the Leo Configuration Tool (`(C:\Program Files\Leo Application Server\Config Editor\LeoConfigEditor.exe)`
  - From the **Config Key** drop-down list, select `FloodAttackShield`
  - In the **New Value** field, enter `False`
  - Click Set Value
- Restart all Leo services:
  - Navigate to `C:\Program Files\Leo Application Server`
  - Right-click `StopAll.bat`, and select **Run as administrator**
  - Right-click `StartAll.bat`, and select **Run as administrator**

b. Run the Leo Migration Tool `(C:\Program Files\Leo Application Server\Migration Tool 64bit\LeoScriptsMigrationTool.exe)`

- Log in to the tool using Leo Studio credentials
- Select all wizards and/or sensors and click **Start**

c. *Final step:* disallow multiple connections to the database

- Run the Leo Configuration Tool (`(C:\Program Files\Leo Application Server\Config Editor\LeoConfigEditor.exe)`
  - From the **Config Key** drop-down list, enter `FloodAttackShield`
  - In the **New Value** field, type `True`
  - Click Set Value
- Restart all Leo services:
  - Navigate to `C:\Program Files\Leo Application Server`
  - Right-click `StopAll.bat`, and select **Run as administrator**
  - Right-click `StartAll.bat`, and select **Run as administrator**

6. Ensure that the names/settings/mappings/bindings for the sites and application defined in IIS exactly match the settings specified in Configuring Leo Console.

CAUTION

The required settings have changed for v.5.17 and later. Don't skip this step of conforming your settings to those specified!

Upgrading clients

1. Run the appropriate ***.msi** installation package on the client machine (see Installing Leo Clients for complete instructions)
   - As part of the installation wizard, you will be prompted to uninstall the prior version
2. For each client, configure the server connection and configure SmartScan (if relevant)

APPENDIX A: TLS/SSL Configuration

TLS/SSL

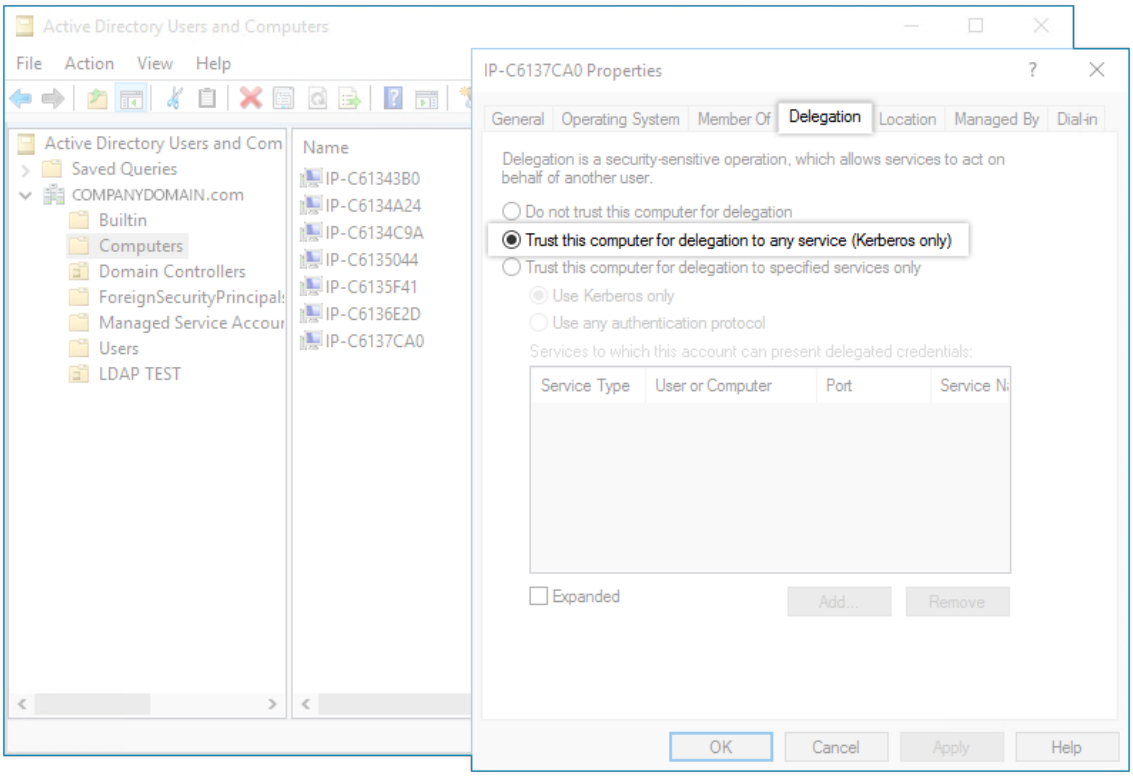
Follow these steps if you will be using Leo with TLS/SSL.

NOTES

- The settings described here are recommended settings based on tested configurations. Actual settings may vary based on your organization's security policies.
- The user completing this step must have relevant permissions to configure these settings (e.g., an IT manager)

Configure Domain Controller

1. Trust all computers that will run Leo components for delegation to any service (Kerberos).
   - Include all machine(s) that will run Leo Application Server and Leo Console, as well as any machine that will run Leo clients (unattended Robots, attended Robots, and Studio)



Configure Leo Application Server

1. From the Windows Command Prompt, use the `netsh http add sslcert` command to map the Net.TCP Port, the HTTPS port, and Port 8090 to the installed TLS/SSL certificate, for example:
   - `netsh http add sslcert ipport=0.0.0.0:443 certhash=`**`<Console Port's Certificate Hash value>`** `appid={00000000-0000-0000-0000-000000000000}`
   - `netsh http add sslcert ipport=0.0.0.0:8080 certhash=`**`<Console Port's Certificate Hash value>`** `appid={00000000-0000-0000-0000-000000000000}`
   - `netsh http add sslcert ipport=0.0.0.0:8090 certhash=`**`<Console Port's Certificate Hash value>`** `appid={00000000-0000-0000-0000-000000000000}`

TIPS

Finding the Console Port's Certificate Hash value

To find the Console Port's Certificate Hash value (to be used in the `netsh http add sslcert` commands shown above):

- Use the `netsh http show sslcert` command to retrieve a list of SSL Certificate bindings
- Scroll to the entry for the port number of the Console Port and copy the value of the Certificate Hash

Reviewing port mappings

After mapping the relevant ports to the TLS/SSL certificate, check the mappings with the `netsh http show sslcert` command. The resulting output should look similar to the following:

```
    IP:port                      : 0.0.0.0:443
    Certificate Hash             : b274a87233acaae4537a0d56fdffb0e670349b16
    Application ID               : {00000000-0000-0000-0000-000000000000}
    Certificate Store Name       : (null)
    Verify Client Certificate Revocation : Enabled
    Verify Revocation Using Cached Client Certificate Only : Disabled
    Usage Check                  : Enabled
    Revocation Freshness Time    : 0
    URL Retrieval Timeout        : 0
    Ctl Identifier               : (null)
    Ctl Store Name               : (null)
    DS Mapper Usage              : Disabled
    Negotiate Client Certificate : Disabled
    Reject Connections           : Disabled

    IP:port                      : 0.0.0.0:8080
    Certificate Hash             : b274a87233acaae4537a0d56fdffb0e670349b16
    Application ID               : {00000000-0000-0000-0000-000000000000}
    Certificate Store Name       : (null)
    Verify Client Certificate Revocation : Enabled
    Verify Revocation Using Cached Client Certificate Only : Disabled
    Usage Check                  : Enabled
    Revocation Freshness Time    : 0
    URL Retrieval Timeout        : 0
    Ctl Identifier               : (null)
    Ctl Store Name               : (null)
    DS Mapper Usage              : Disabled
    Negotiate Client Certificate : Disabled
    Reject Connections           : Disabled

    IP:port                      : 0.0.0.0:8090
    Certificate Hash             : b274a87233acaae4537a0d56fdffb0e670349b16
    Application ID               : {00000000-0000-0000-0000-000000000000}
    Certificate Store Name       : (null)
```

2. Use the `netsh http add urlacl` command to reserve the certificate server URL on the Net.TCP Port for non-administrator users and accounts, for example:
   - `netsh http add urlacl url=https://<certificate_server.com>:443/ user=Everyone listen=yes`
     - **NOTE:** In the above example, **`certificate_server.com`** would be replaced by the actual **Certificate Server Name** specified in the Security Settings window during Leo Application Server installation

TIP

Reviewing the reserved URL

After reserving the URL, check it with the `netsh http show urlacl` command. The resulting output should look similar to the following:

```
Reserved URL            : https://certificate_server.com:443/
    User: \Everyone
        Listen: Yes
        Delegate: No
        SDDL: D:(A;;GX;;;WD)
```

3. Define a service principal name (SPN) (by which a Kerberos client uniquely identifies an instance of a service for a given Kerberos target computer) with the following commands:
   - `setspn -a HTTP/<certificate_server.com> <domain>\<user>`
   - `setspn -a HOST/<certificate_server.com>:<Net.TCP port> <domain>\<user>`
   - `setspn -a HOST/<certificate_server.com>:<HTTPS port> <domain>\<user>`
   - `setspn -a HOST/<certificate_server.com>:8090 <domain>\<user>`

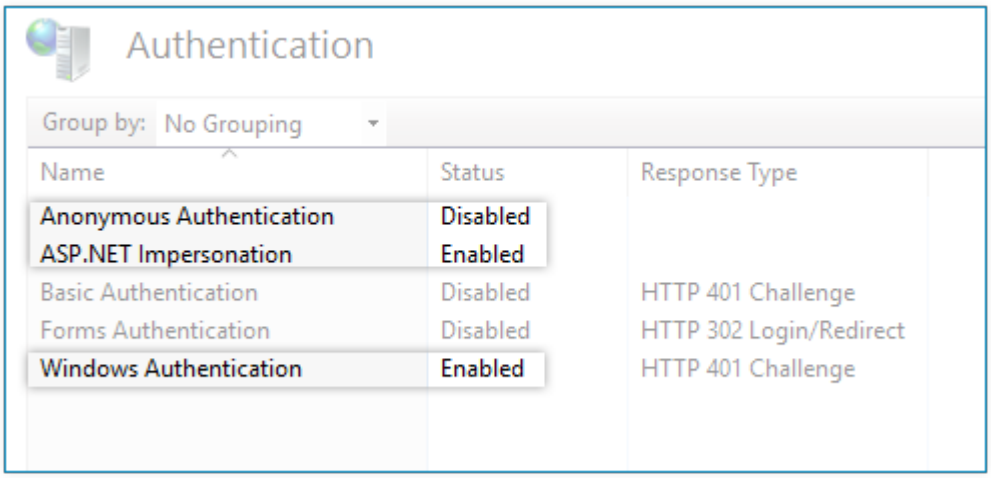
- **NOTE:** In the above examples:
  - `certificate_server.com` would be replaced by the actual **Certificate Server Name** specified in the Security Settings window during Leo Application Server installation
  - `<domain>\<user>` would be replaced by the Leo Server Service Logon User (i.e., the user verified/created when Preparing the Environment)

> **TIP**
>
> **Reveiwing SPN registrations**
>
> After creating SPN registrations, check them with the following command:
> `setspn -L <domain>\<user>`

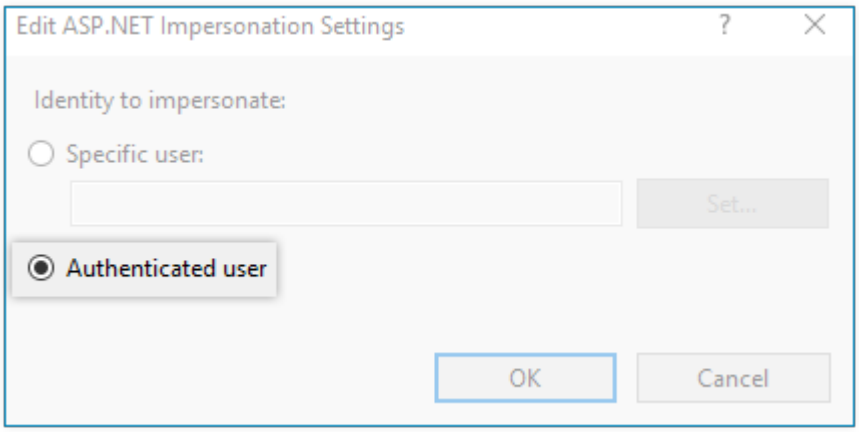
Configure Leo Console Authentication Settings

For the **Console** site defined when Configuring Leo Console, configure authentication settings as follows:

1. Disable **Anonymous Authentication**
2. Enable **ASP.NET Impersonation**
3. Enable **Windows Authentication** (required for clients to authenticate using the NTLM or Kerberos protocols)



4. Configure ASP.NET Impersonation Settings so that **Authenticated user** is selected as the **Identity to impersonate**



5. Enter the **Windows Authentication Advanced Settings** dialog, and uncheck **Enable Kernel-mode authentication**