ADSS Web RA Server 2.9.6

Installation

Guide

ASCERTIA LTD

MARCH 2025

Document Version- 1.0.2

Table of Contents

1 Introduction

Registration Authority (RA) is another important component of PKI along with Certificate Authority (CA). CA is primarily responsible to create and revoke certificates, but complex business scenarios demand more than just the creation of certificates. Their responsibilities now include but not limited to managing users, certificate creation requests and revocation of certificates.

Businesses in the modern world require strong control over these processes along with the complete audit trail, to maintain the irrefutable evidence of these activities for future. Such additional controls and management are covered by an RA. An RA is therefore responsible to verify a user and their certificate request, and then inform the CA to issue the requested certificate.

An RA receives a request for digital certificate and verifies the user requesting the certificate. The user verification can be done manually through face to face interaction or electronically by using other mediums like phone, video conferencing, mail or courier that is acceptable to the RA as a secured medium. Once RA approves the user, it informs the CA to issue the certificate for the user. The RA then obtains the user certificate from the CA, and sends it to the user using a secure medium.

1.1 Scope

This manual describes how to install ADSS Web RA Server.

ADSS Web RA comprises five components and the installation procedure for all are covered herein:

- **Web** interface that provides user services on desktop browsers.
- **Admin** console that provides system administration and configuration.
- **API** that utilises the ASP.NET Web API framework to provide a REST architecture.
- **Device** is used to manage device enrolment for certificate creation.
- **Windows Enrolment** is used to manage certificate renewal or auto-enrolment on a Windows machine.

1.2 Intended Readership

This manual is intended for administrators responsible for installation and initial configuration. It is assumed that the reader has a good understanding of web applications running on IIS, digital signatures, digital certificates and IT security.

1.3 Technical Support

If technical support is required, Ascertia has a dedicated support team providing debugging and integration assistance as well as general customer support. Ascertia Support can be accessed through Ascertia Ticketing System or email address: support@ascertia.com

Ascertia provides formal support agreements with all product sales. Contact sales@ascertia.com for further details.

A Product Support Questionnaire should be completed in order to provide Ascertia Support having information about your system environment, along with details of any issues encountered. When requesting help, it is always important to confirm these details:

- System platform.
- ADSS Web RA version number.
- Details of the specific issue and relevant steps taken to reproduce it if possible.
- Database vendor, version and patch level.
- Product log files.

1.4 Glossary

ADSS Web RA	A short form of Unified Web Registration Authority
Cert	A short form of Digital Certificate
DBMS	Database Management System
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
HTTP/S	HTTP over SSL/TLS connection
SSL	Secure Sockets Layer

2 System Requirements

System Requirements includes hardware and software requirements both.

2.1 Hardware Prerequisites

Components	Requirements
Hard Disk Space	• 200 GB (Mínimum)
Memory	• 16 GB (Mínimum) • 24 GB (If the number of concurrent users is higher) • 32 GB (If the database is also deployed on the same system as the ADSS Web RA)
Processor	• A modern multi-core CPU such as Xeon E3-XXXX or E5-XXXX series is recommended
Processor Type	• x64
HSM (Optional)	• Thales Luna Network, PCIe, and USB • Entrust nShield Solo XC, Connect XC, and nShield EDGE • Utimaco CryptoServer SE Gen2 • Microsoft Azure Key Vault • Amazon Cloud HSM

2.2 Software Prerequisites

Component	Requirements
Operating Systems	• Follow this link to view details about supported OS: https://manuals.ascertia.com/WebRA/ADSS-WebRA-Server-Platform-Support.pdf
Microsoft IIS	• IIS 10 • Application Development feature in IIS
IIS Rewrite Module	• v2.1
.Net Framework	• .Net Framework 4.8.1 or above
.Net Core Runtime & Hosting Bundle	• ASP.NET Core Runtime 9.0 or above

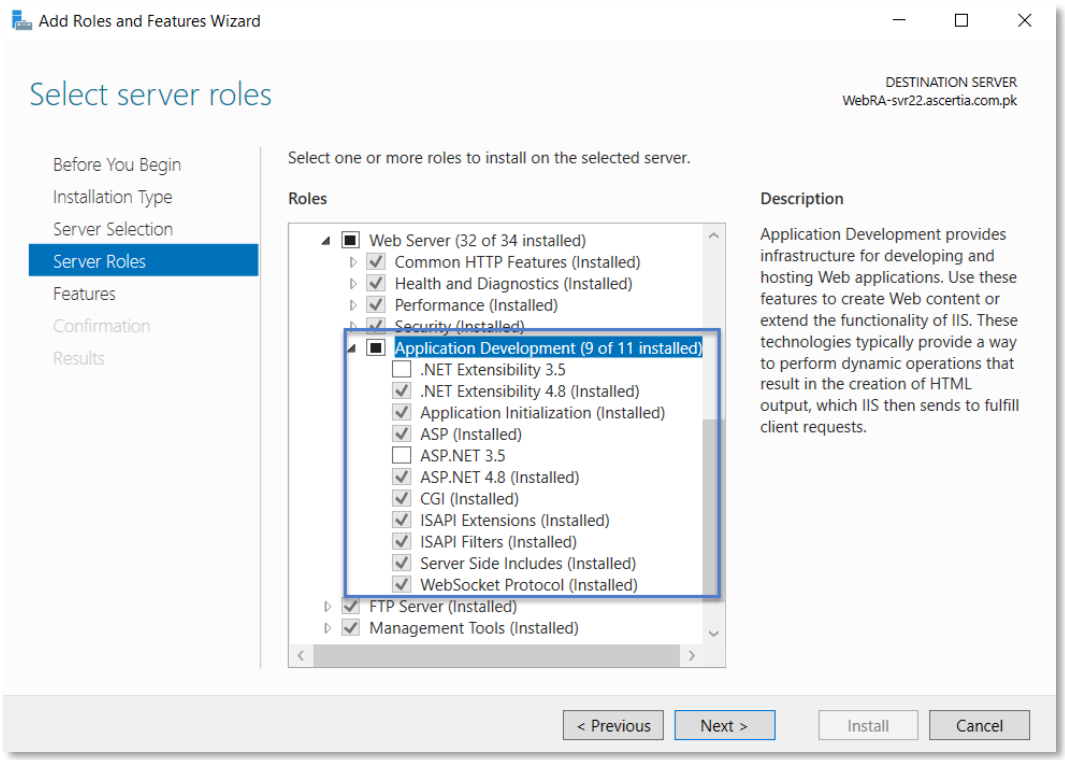
Database Server	• Follow this link to view details about Database Server: https://manuals.ascertia.com/WebRA/ADSS-WebRA-Server-Platform-Support.pdf
Web Brower **(for end-users and administrators)**	• Follow this link to view details about Web Browsers: https://manuals.ascertia.com/WebRA/ADSS-WebRA-Server-Platform-Support.pdf
ADSS Server	ADSS Web RA uses ADSS Server under the hood to create and manage certificates for the end user as a CA. ADSS Server can be installed on a separate machine or on the same machine for testing and proof of concept. It is recommended to keep the ADSS installation on a separate machine for a production environment. For further requirements related to the installation of ADSS Server, please refer to the installation guide of ADSS Server. • ADSS Server 6.6 or above
DMZ Proxy Systems	A DMZ proxy server is recommended to provide enhanced security for ADSS Web RA. Supported web servers are: • Windows Server + IIS, Apache or IBM HTTP Server • Linux + Apache or IBM HTTP Server It is recommended to use a reasonable CPU, 4 GB RAM (Minimum), 2000 MB Disk Space for the web server machine. ADSS Web RA and ADSS Server support network proxies to allow authenticated access to external services. Certificate generation with local smartcards or USB tokens requires ADSS Server Go>Sign Service.

For testing and proof of concepts, ADSS Server and ADSS Web RA can be installed on the same machine along with the database server. However, for optimal performance in a production environment, it is always recommended to install them on separately dedicated machines.

The details given above are the minimum set of requirements; for higher concurrent use of the application the system requirements may vary based on the load and performance expectations.

2.3 Application Development feature in IIS

Enable the following features in IIS on the deployment machine:

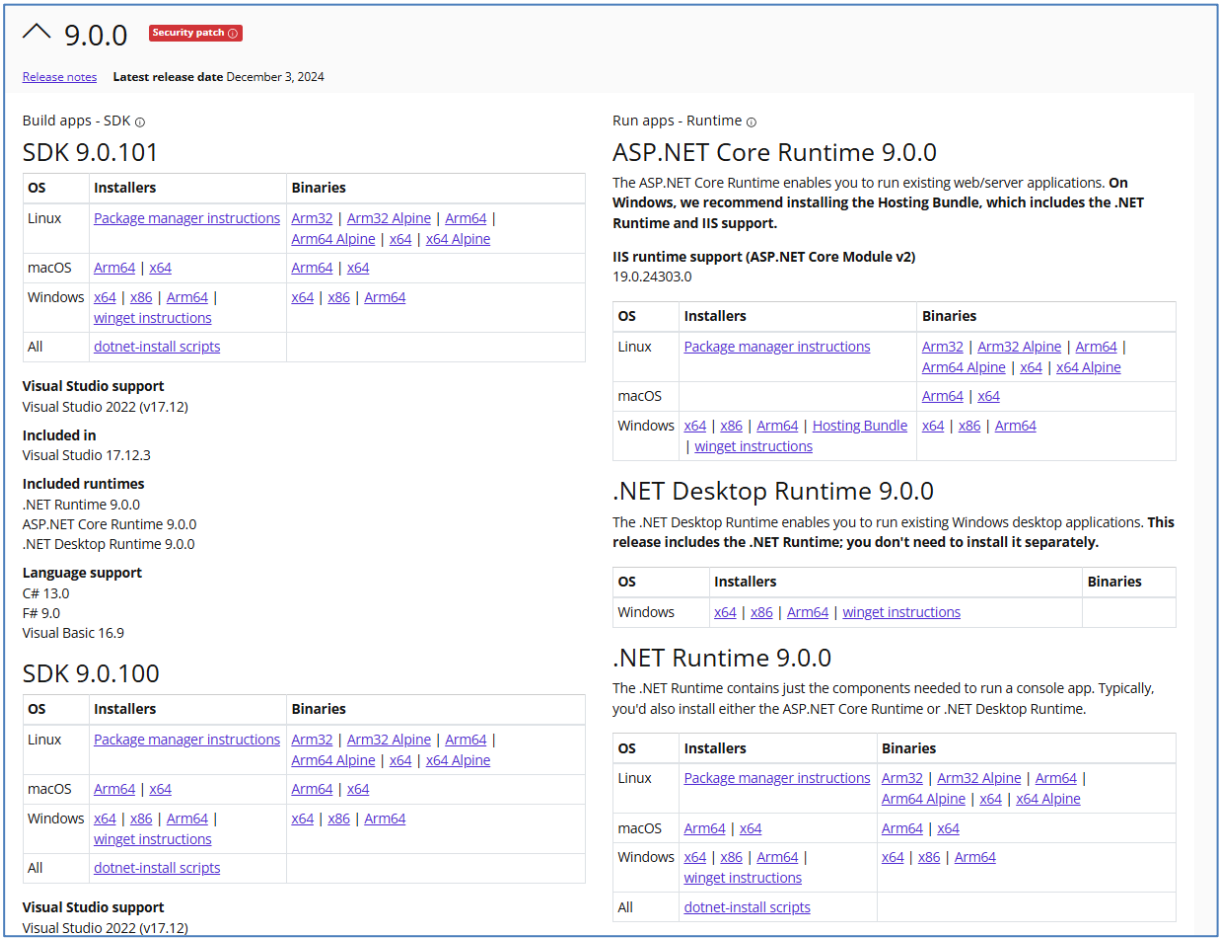


2.4 Microsoft .Net Core 9.0.0. Runtime & Hosting Bundle

2.4.1 Download the latest version of Microsoft .Net Core i.e. Microsoft .Net Core 9.0.0. Runtime and Hosting Bundle from the following link:

Microsoft .Net Core 9.0. Runtime & Hosting Bundle

2.4.2 Download the Hosting Bundle installer.



9.0.0 Security patch

Release notes **Latest release date** December 3, 2024

Build apps - SDK

SDK 9.0.101

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm32 Alpine | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS	Arm64 | x64	Arm64 | x64
Windows	x64 | x86 | Arm64 | winget instructions	x64 | x86 | Arm64
All	dotnet-install scripts	

Visual Studio support
Visual Studio 2022 (v17.12)

Included in
Visual Studio 17.12.3

Included runtimes
.NET Runtime 9.0.0
ASP.NET Core Runtime 9.0.0
.NET Desktop Runtime 9.0.0

Language support
C# 13.0
F# 9.0
Visual Basic 16.9

SDK 9.0.100

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm32 Alpine | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS	Arm64 | x64	Arm64 | x64
Windows	x64 | x86 | Arm64 | winget instructions	x64 | x86 | Arm64
All	dotnet-install scripts	

Visual Studio support
Visual Studio 2022 (v17.12)

Run apps - Runtime

ASP.NET Core Runtime 9.0.0

The ASP.NET Core Runtime enables you to run existing web/server applications. **On Windows, we recommend installing the Hosting Bundle, which includes the .NET Runtime and IIS support.**

IIS runtime support (ASP.NET Core Module v2)
19.0.24303.0

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm32 Alpine | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS		Arm64 | x64
Windows	x64 | x86 | Arm64 | Hosting Bundle | winget instructions	x64 | x86 | Arm64

.NET Desktop Runtime 9.0.0

The .NET Desktop Runtime enables you to run existing Windows desktop applications. **This release includes the .NET Runtime; you don't need to install it separately.**

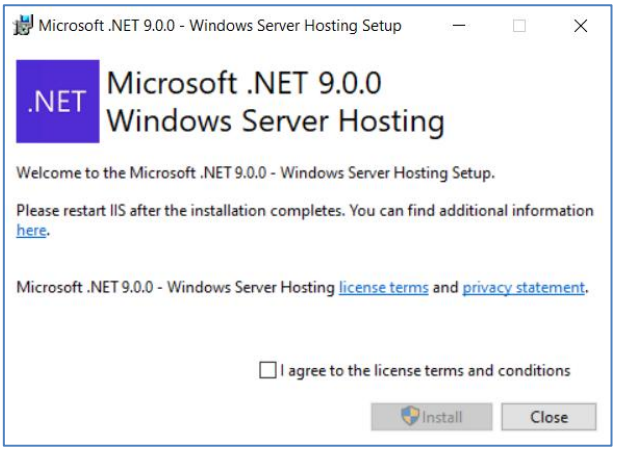
OS	Installers	Binaries
Windows	x64 | x86 | Arm64 | winget instructions	

.NET Runtime 9.0.0

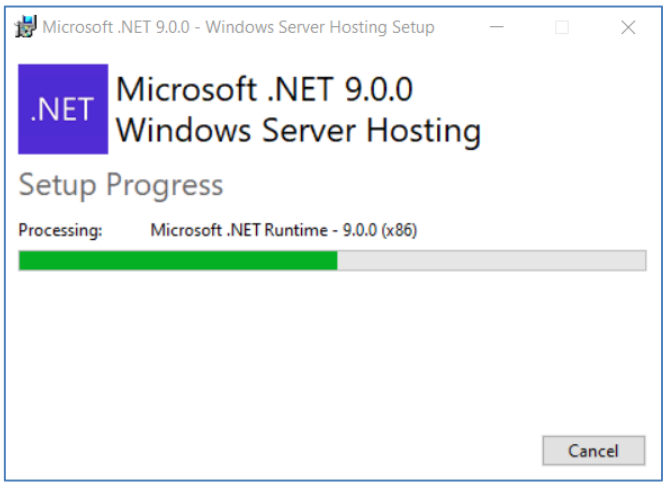
The .NET Runtime contains just the components needed to run a console app. Typically, you'd also install either the ASP.NET Core Runtime or .NET Desktop Runtime.

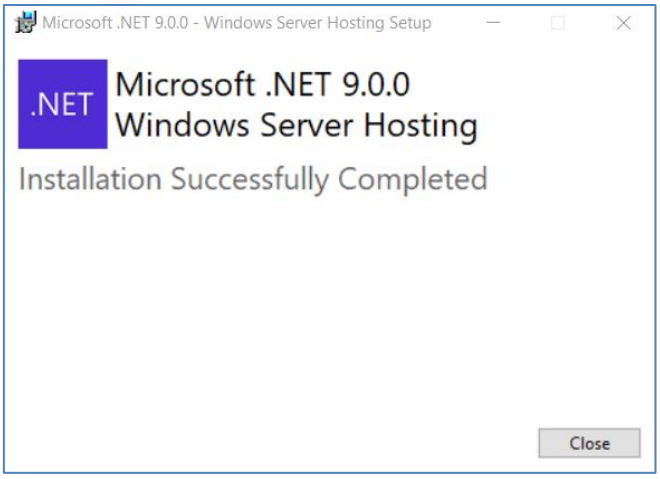
OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm32 Alpine | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS	Arm64 | x64	Arm64 | x64
Windows	x64 | x86 | Arm64 | winget instructions	x64 | x86 | Arm64
All	dotnet-install scripts	

2.4.1. Once downloaded, execute the installer by executing **dotnet-hosting-9.0.0-win.exe**



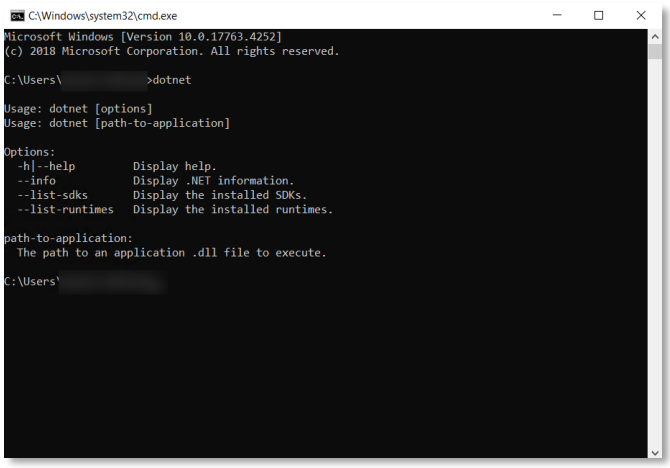
2.4.2. The setup will begin and take a few minutes to complete.





2.4.3. Once the installation process is complete, click **Close**.

2.4.4. To test if the installation was correct and components are reachable, run command line and type the following command:



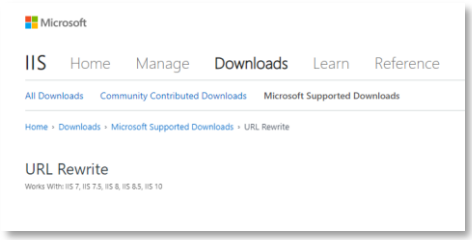
2.4.5. Now, restart your machine to apply these changes effectively.

2.5 Microsoft IIS URL Rewrite Module 2.1

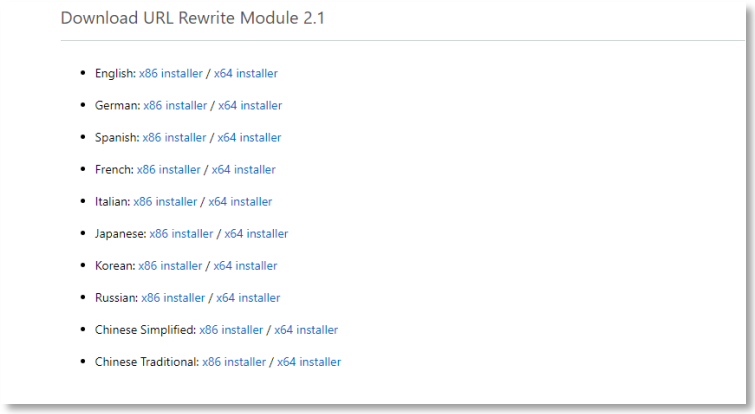
2.5.1. Download **Microsoft IIS URL rewrite module 2.1** from the following link:

[Microsoft IIS URL Rewrite Module 2.1]

2.5.2. Navigating to this URL will present with the following screen:

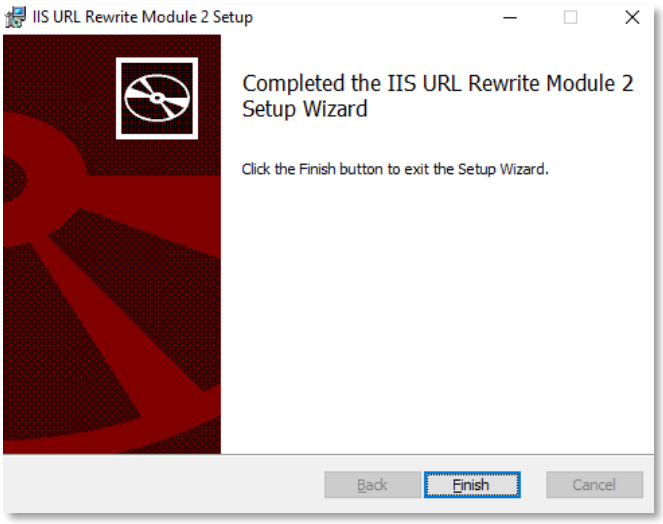


2.5.3. Scroll down to find a list of links available for download.



2.5.4. Download **x64 installer** with your preferred language. For this documentation it's **English**. Start the installation by executing the downloaded file in administrator mode.

2.5.5. Accept the terms in the license agreement and click **Install** to proceed, the installation will take few minutes:



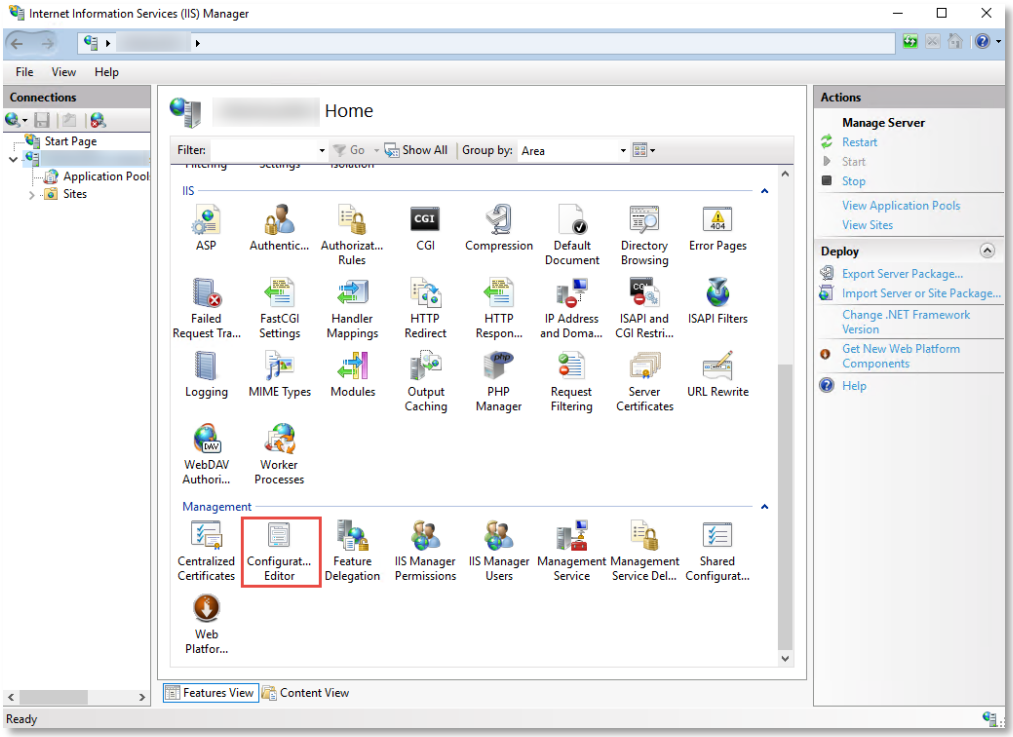
2.5.6. Click **Finish** once the installation process is complete.

2.6 Unlock system.webServer/serverRuntime section in IIS

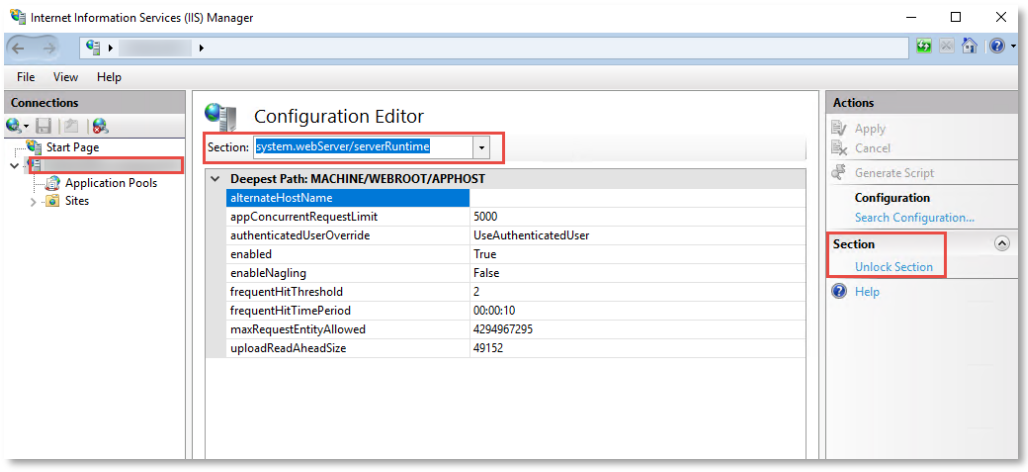
2.6.1. Launch the **IIS Manager**

2.6.2. Select **Server** from left panel

2.6.3. Open **Configuration Editor** from right pane under the Management section.



2.6.4. Unlock **system.webServer/serverRuntime** section in the Configuration Editor.



The installation process for prerequisites is complete.

2.7 SMTP Server

ADSS Web RA uses email as the primary notification medium. User registration, and all notifications are sent via SMTP. Hence, it is a critical part of the architecture and deployment. Details required are:

- Hostname/IP address of SMTP server
- Listening Port of SMTP server
- TLS/SSL authentication to communicate with SMTP server (if required)
- Username and password to authenticate to SMTP server (if required)
- Email from Address for notifications sent from ADSS Web RA
- Email to Address for alerts and warnings sent by ADSS Web RA
- Email Subject for alerts and warnings sent by ADSS Web RA

If there is no alternative it is possible to still use ADSS Web RA. However, this involves copying the notification emails directly from the database and manually running the links therein. This usage is strongly discouraged in favour of a standard deployment though.

2.8 Database

ADSS Web RA Server requires its own database. It is not required to create the schema or configure any other feature prior to the installation.

Permissions are required to allow the creation of database tables, and entry, modification, and removal of data within those tables.

3 Installation Modules

ADSS Web RA consists of the following modules. Note the API is the only non-mandatory ones for a working solution:

- **ADSS Web RA Admin**

Administration application that allows to manage the system wide configurations, service plans, user accounts and access controls, etc.

- **ADSS Web RA Desktop Web**

ADSS Web RA Web is used for managing certificates i.e. creation, renewal and revocation.

- **ADSS Web RA API (Restful Web Services)**

REST architecture API support that is used to integrate ADSS Web RA functionality within your own portal. The API uses JWT to implement authentication and authorization. There is a separate API Guide that provides full details of the REST architecture implementation.

- **ADSS Web RA Device**

ADSS Web RA Device is used to manage device enrolment for certificate creation, renewal and revocation.

- **ADSS Web RA SSL Device**

ADSS Web RA SSL Device is used to manage device enrolment over SSL for certificate creation, renewal and revocation e.g. EST Protocol

- **Windows Enrolment**

ADSS Web RA Windows Enrolment is used to manage certificate renewal or auto-enrolment on a Windows machine.

4 ADSS Web RA Installation on Windows Server

4.1 Fresh Installation of ADSS Web RA

Before starting the ADSS Web RA installation process, make sure the following:

Prerequisites must be installed on the ADSS Web RA machine. If these are not installed, ADSS Web RA will not open and even cannot display any page when accessed.
An empty database is created on the DMBS (SQL Server) with privileges for ADSS Web RA.

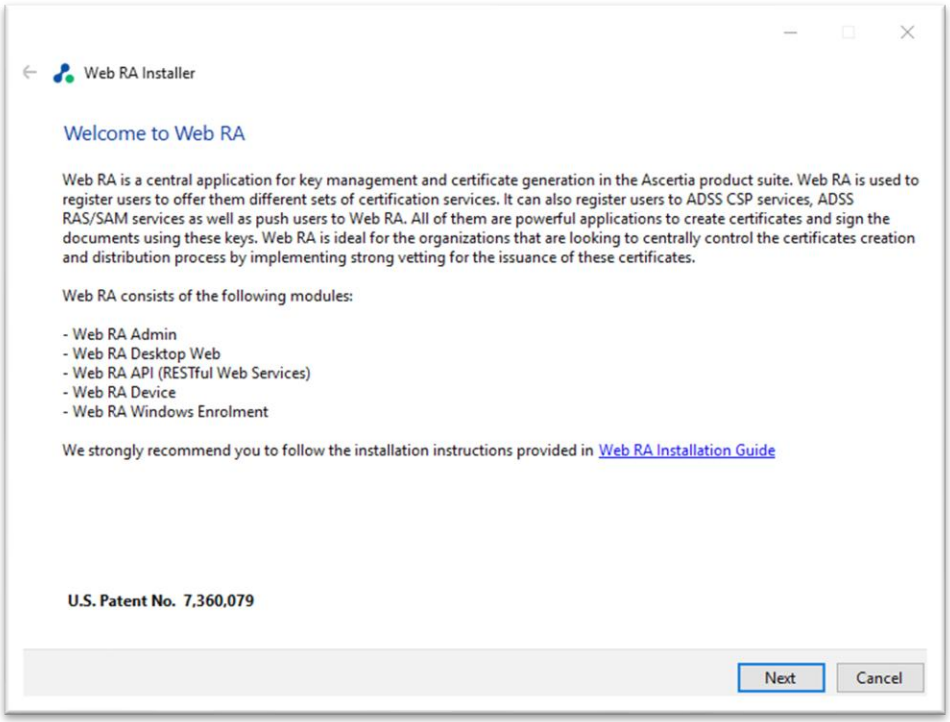
The ADSS Web RA package MUST be unzipped on to a disk that has sufficient space – a minimum of **100GB** is recommended. This is because the product is installed and runs from where the installation package is extracted to. Hence, choose a suitable location and naming structure. If you extract the installer on Desktop, it will not work so choose a proper drive to extract it.

Do not include spaces in the installation folder name and path – use hyphen or underscore characters instead, if required. Spaces will cause functional problems with ADSS Web RA installation. The installer must be run from a user account with the Windows Administrator privileges.

ADSS Web RA installer generates all the required database tables and populates the default data required to run the system. Therefore, there is no requirement for separate SQL scripts or equivalent for non-SQL databases.

4.1.1 Once the above conditions are satisfied, launch the installer by right-clicking the file **[WEBRA Installation-Dir]/setup/install** and select Run as administrator from the menu will present the welcome screen.

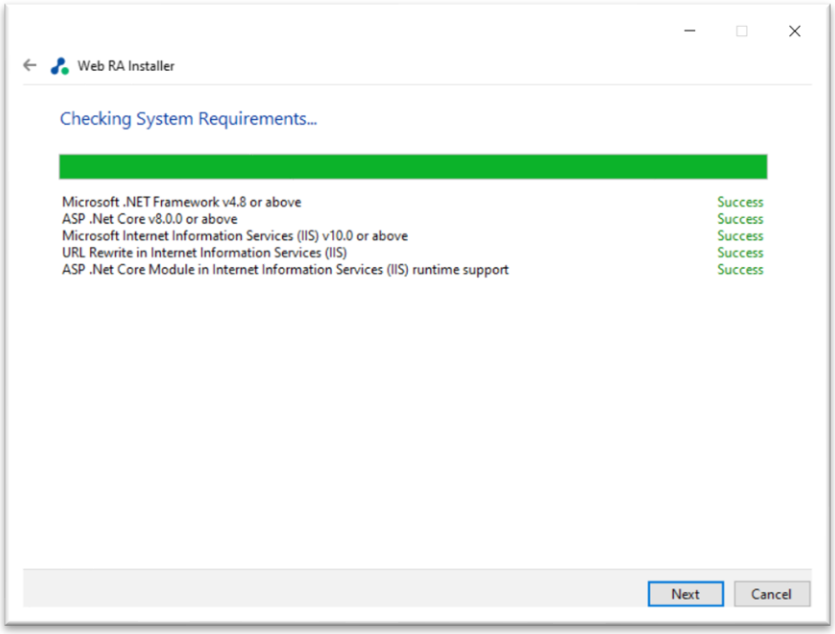
The following welcome screen is shown:



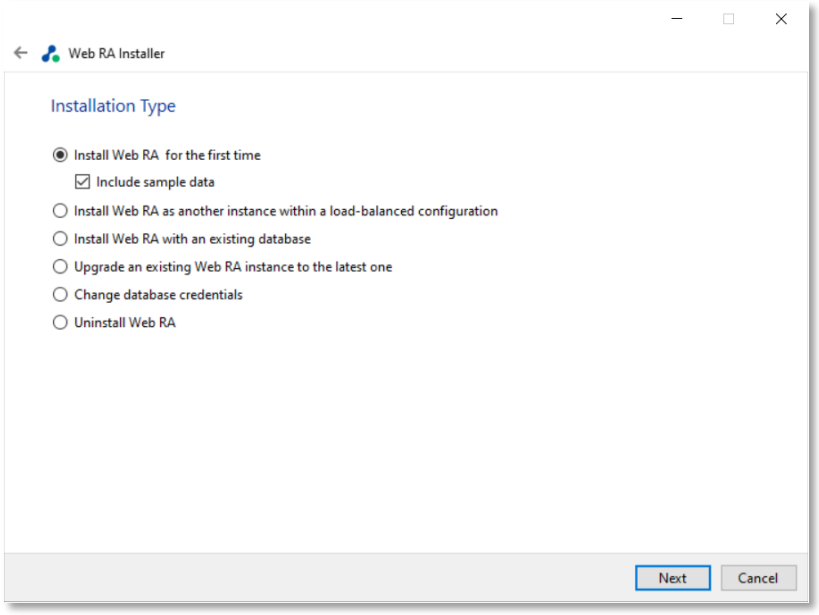
4.1.2 Click the **'Next'** button to continue.

4.1.3 System requirements screen will appear next to validate if all the required prerequisites are installed or not. If any of ADSS Web RA system dependencies are not found, or not functioning, then Failed status will be shown corresponding to that component on the screen.

You can only proceed with the installation process once all issues related to system dependencies are resolved as shown below:



4.1.4 Click the **'Next'** button to select an installation type.



If you are installing ADSS Web RA for the first time or you wish to deploy a fresh installation with a new database, then select "**Install Web RA for the first time**". The "**Install Web RA as another instance within a load-balanced configuration**" option will install the ADSS Web RA instance in a load-balanced mode. If you wish to upgrade an older system to the latest version, then select **"Upgrade" an existing ADSS Web RA instance to the latest one".** Installer supports the upgrade when the base (current) installation is v2.1.1 or higher.

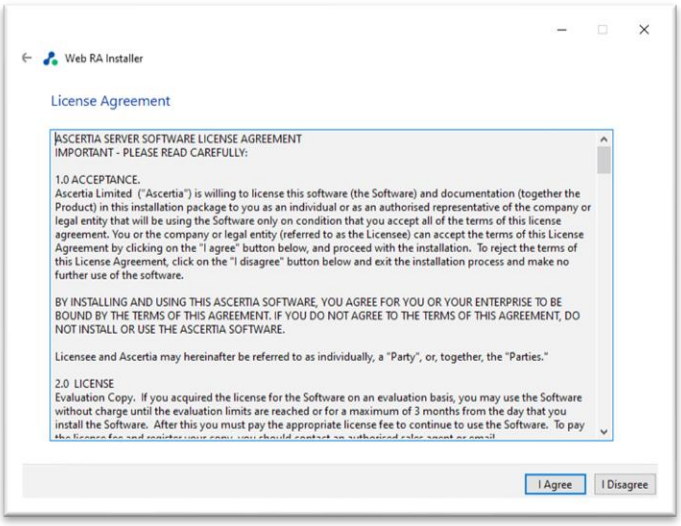
The **Install Web RA with an existing database** option will install ADSS Web RA against an existing ADSS Web RA database. For example, this option can be used to recover a system from a database back-up. The **Change database credentials** option is used if the database password, user, database name and/or server is changed, and it needs to be updated in ADSS Web RA installation. Select the last option **Uninstall Web RA** if you wish to uninstall ADSS Web RA from the system.

4.1.5 Select the option **Install Web RA for the first time**.
You can include sample data in application during fresh installation. Sample data includes following data:

- Default ADSS Connector
- Default SMTP Connector
- Default ADSS Service Profile
- Default Subscriber Agreement
- Default Vetting Form
- Default Service Plan
- Default Authentication Profile

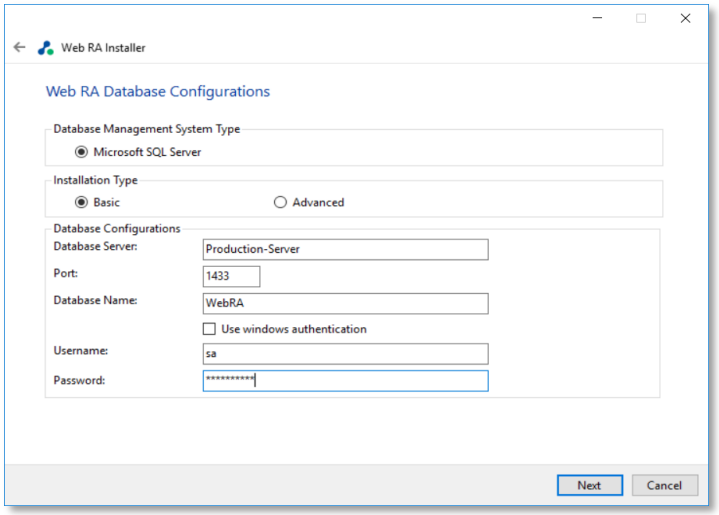
If “Include Sample Data” is not selected then above data will not be added when application installed.

4.1.6 Click the **Next** button to show the **License Agreement**.



4.1.3. Click the **I Agree** button to proceed.

4.1.7 The **Readme screen** will be displayed with new features list. Click **Next** button to proceed.
The following screen for **Database Configurations** will be displayed.



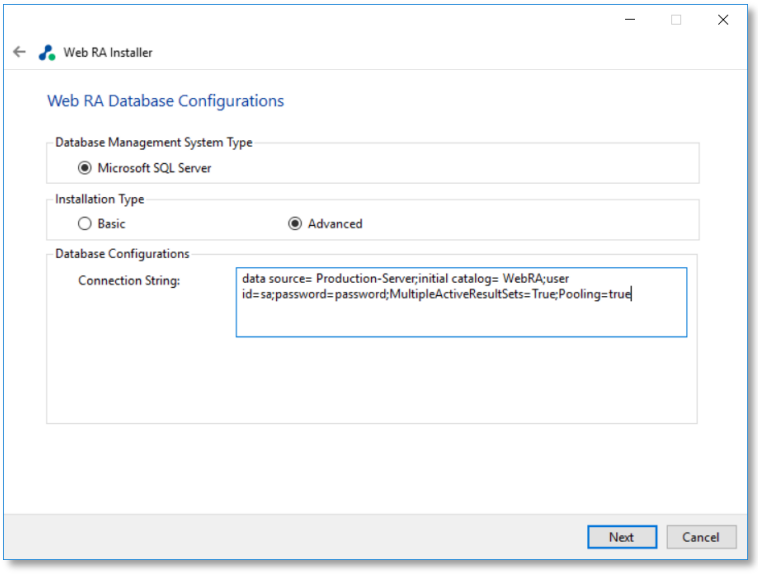
Furthermore, you can either choose to do a basic installation or use an advanced one. If this is a basic installation, then use the first option **Basic** and provide the appropriate ADSS Web RA database credentials. The information displayed above is an example and you should configure the relevant settings for your own environment.

Once you enter the database credentials and select Next, the installer uses the information to test the connectivity to the database. If the installer can establish the connection with the database, then it will proceed with the installation.

The following table explains the **Database Configurations**.

Item	Description
Database Server / Host Name	Database server IP or DNS name.
Port	Database listening port. For SQL Server the default port is **1433.**
Database Name	Name of the database instance. Note this must exist prior to the installation.
Use Windows Authentication	If enabled, installer will use the Windows logged in user to communicate with database. You are required to enter password because it will be used in Application Pool to set the Identity against this user for all websites. By default, the current logged in user will be configured in the Application Pool Identity. If you wish to run ADSS Web RA under a different windows user, then you need to change it manually. If your requirement is to use SQL Server authentication, then type SQL Server Username and Password in the underneath fields without enabling this option.
Username	Name of the database user. Note this must exist prior to the installation. It is not required in the case of Windows Authentication.
Password	Password credential of the database user. Note this must exist prior to the installation. In case of Windows Authentication, type the password of domain user shown in the Username field to configure the Application Pool Identity in IIS Server for successful communication with SQL Server.

If you have chosen **Advanced** for database configurations, then the following screen will be shown.



The information displayed above is an example and you should configure the relevant settings for your own environment.

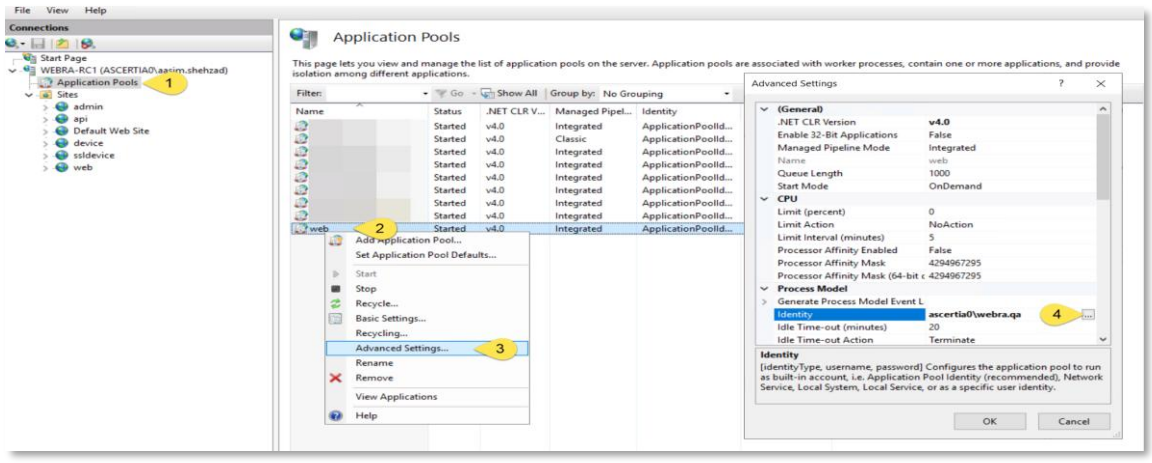
Once you complete the options and select **Next**, the installer uses the information provided to test the connectivity to the database. If the installer can establish the connection with the database, then it will proceed with the installation.

The following table entails details of the **Advanced Installation type**:

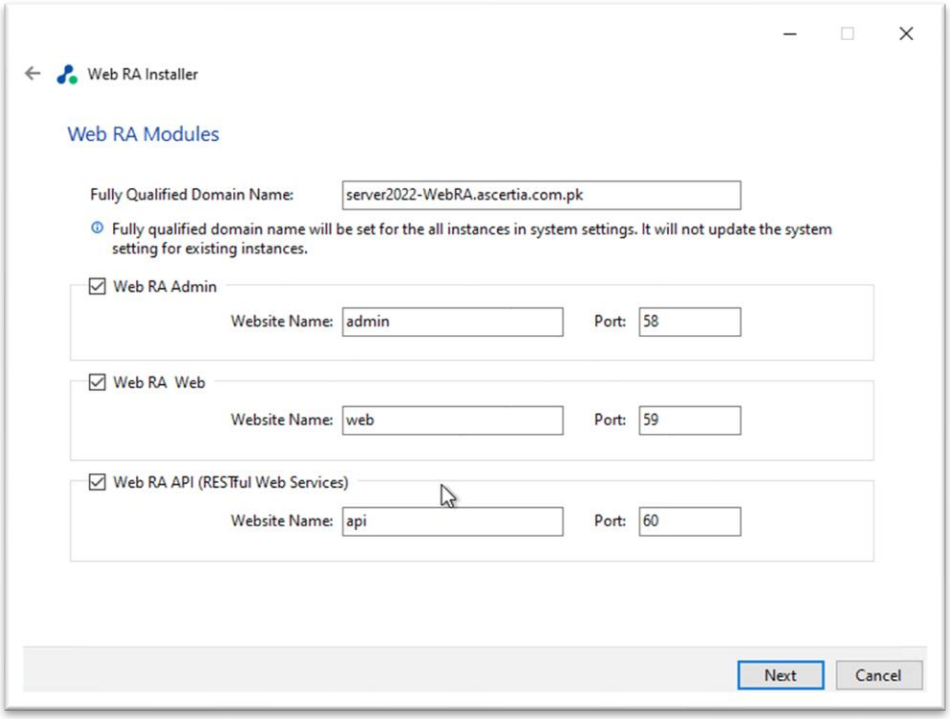
Item	Description
ADSS Web RA Connection String	The following are sample connection strings for SQL Server: • **Simple One** - "data source= **[Database Server Address]**;initial catalog= **[Database Name]**;user id=**[Database User Name]**;password=**[Database User Password]**;MultipleActiveResultSets=True;Pooling=true" • **For Named instance** - "data source= **[Database Server Address]\[SQL Server Instance Name]**;initial catalog=**[Database Name]**;user id=**[Database User Name]**;password**[Database User Password]**;MultipleActiveResultSets=True;Pooling=true" • **For Windows Authentication** - "data source= **[Database Server Address]**;initial catalog=**[Database Name]**;integrated security=SSPI;MultipleActiveResultSets=True;Pooling=true
Username	Field will only be shown in case of Windows Authentication while for SQL Server Authentication, username will be provided in the connection string.
Password	In case of Windows Authentication, type the password of domain user shown in the Username field to configure the Application Pool Identity in IIS Server for successful communication with SQL Server. In case of SQL Server authentication, password will be provided in the connection string.

*If Windows authentication is enabled in connection string, installer will use the Windows logged in user to communicate with database upon clicking the **Next** button. You are required to enter password because it will be used in Application Pool to set the Identity against this user for all websites.*

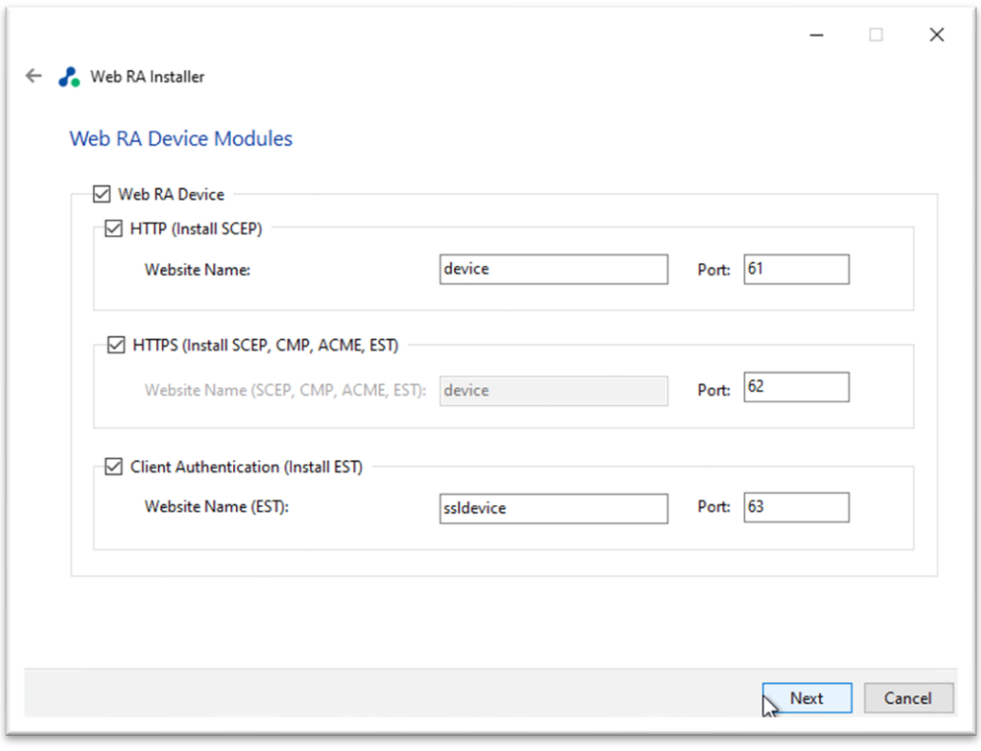
By default, the current logged in user will be configured in the Application Pool Identity. If you wish to run ADSS Web RA under a different Windows user, then you need to change it manually. As shown in the following Screen:



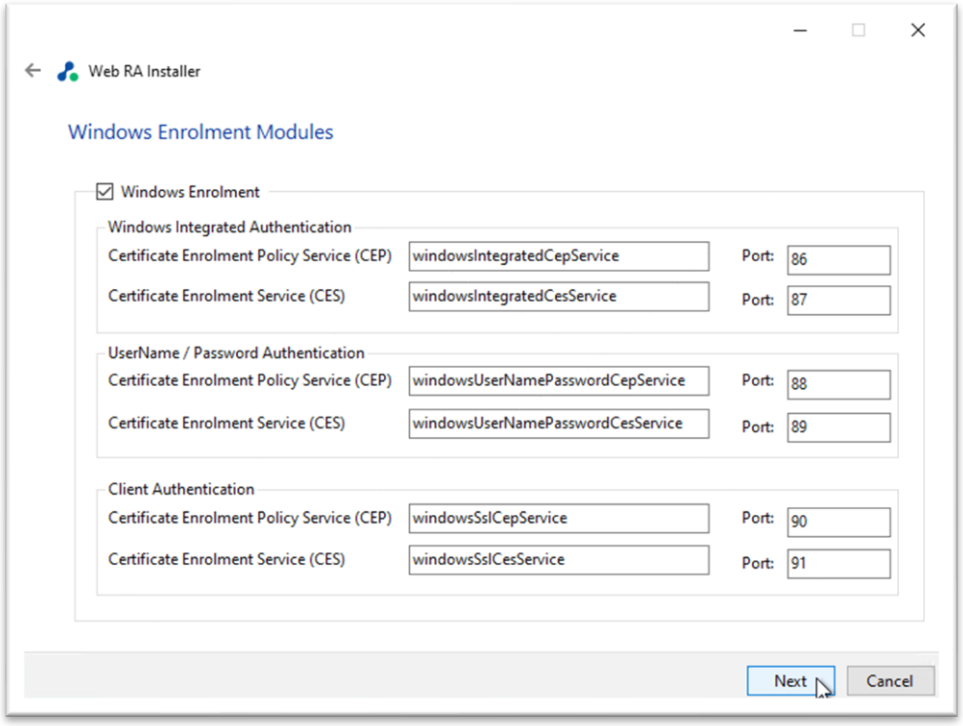
4.1.8 Click the Next button to select specific modules:



4.1.9 Select **Device Modules** to install the required features. The fully qualified domain name field will be auto-filled with complete computer name. For each selected application, provide the web application name and port. A typical in-house installation of ADSS Web RA should only include Admin, Desktop Web, and the API. However, the device will be added at the end. Click Next to proceed.



Select Windows Enrolment**. For each selected application, provide the web application name and port. Then click** Next**.**

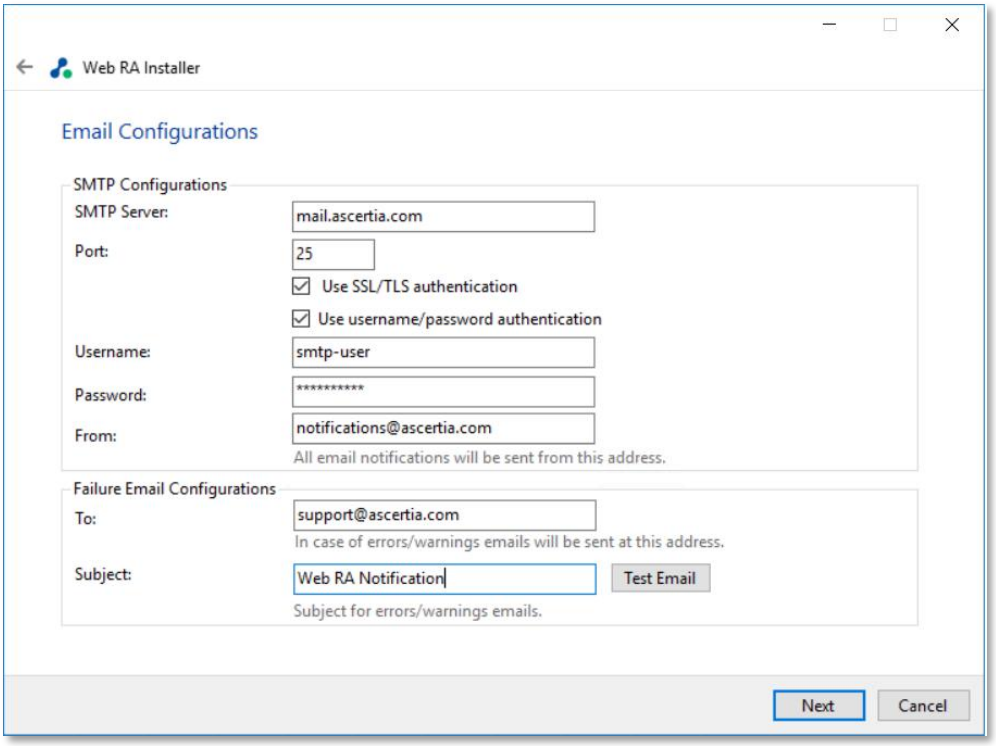


The information displayed above is an example, which you may change suiting to your environment and organisation preferences. However, the example shown is sufficient. The names will appear as websites under **IIS Manager**.

The following table entails details of the **Windows Enrolment** modules.

Item	Description
ADSS Web RA Admin	ADSS Web RA Admin is used by the administrators to manage the system wide configurations, service plans, user accounts and access control etc.
ADSS Web RA Web	ADSS Web RA Web is used to manage certificates for creation, renewal and revocation.
ADSS Web RA API	**REST API** is used to integrate ADSS Web RA functionality within your own portal.
ADSS Web RA Device	ADSS Web RA device is used to manage device enrolment for certificate creation, renewal and revocation. This site will be deployed with http and https bindings.
ADSS Web RA SSL Device	ADSS Web RA SSL device is used to manage device enrolment over SSL for certificate creation, renewal and revocation e.g. EST Protocol. This site will be deployed with https SSL.
Windows Enrolment	Windows Enrolment is used to manage certificate renewal or auto-enrolment on a windows machine.

4.1.10 Click the **Next** button to configure the **SMTP Server** and **Email Settings**.



Configure SMTP Server and email settings for your environment. ADSS Web RA must have access to a suitable SMTP Server without which users will not be able to receive registration emails that are required to complete the user registration process.

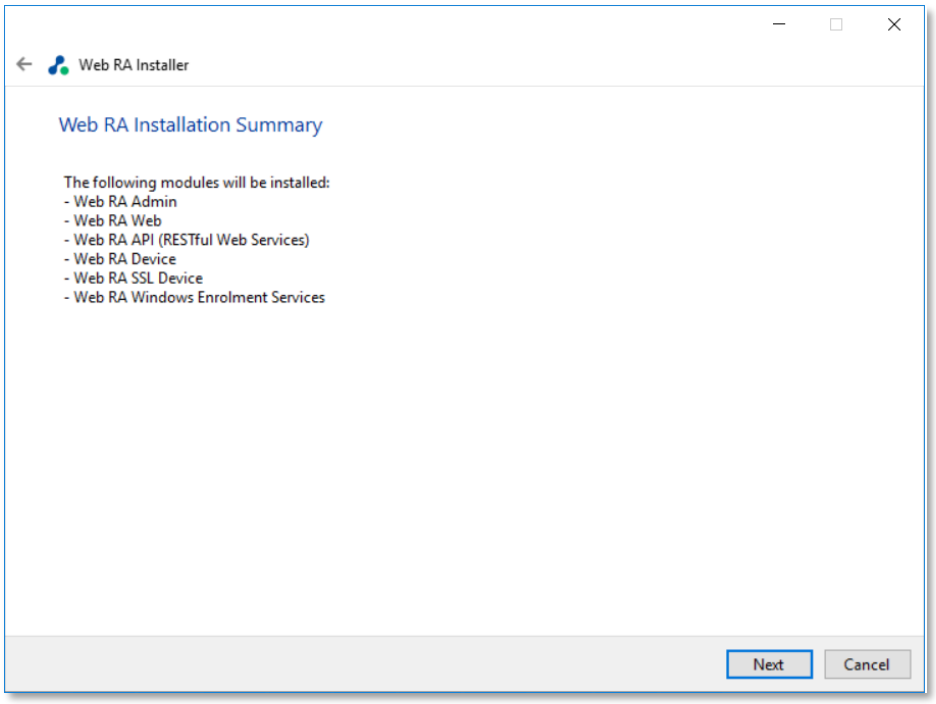
Additionally, system generated email notifications will not be received either. Although the latter will not prevent functionality, but it is not a recommended approach. The information displayed above is an example and you should setup configurations for your own environment.
The configuration items are explained in the following table:

Item	Description
SMTP Server	Defines the email server address. This email server is used to send email notifications to users as required, such as for account registration, data sharing etc. It is also used for sending notification emails to ADSS Web RA administrators.
Port	Define the service port for the SMTP mail server.
Use SSL/ TLS authentication	Select this option if the SMTP mail server requires SSL/TLS.
Username	Configure the SMTP mail server username that is used to send ADSS Web RA generated emails.
Password	Define the password to authenticate the SMTP server.
From	Configure the **From** email address that should be used to send notification emails to users and administrators.
To	Configure the email address where error notifications should be sent. This is usually the IT support team address.
Subject	Define a subject line for the notification emails that are sent to the administrator, e.g. ADSS Web RA Alert.

After configuring these SMTP settings, click the **Test Email** button to verify that SMTP configurations are valid.

If "Include Sample Data" is not selected then SMTP configuration screen will not be shown.

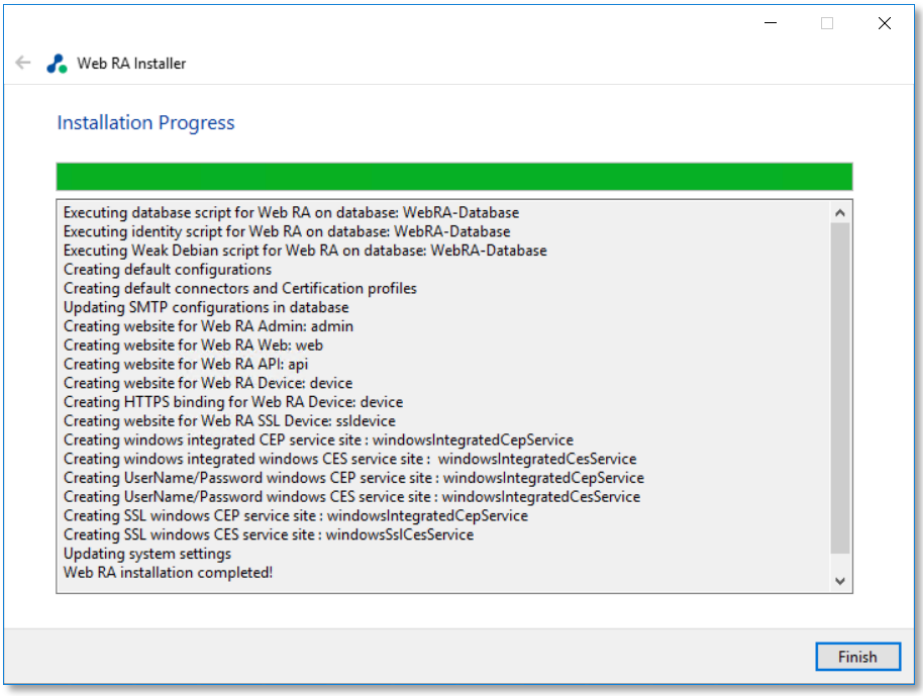
4.1.11 Click the **Next** button to see the **Installation Summary** and complete the installation process.



This screen shows the installation summary by listing different product modules that will be installed.

If you think any listed item is incorrect then use the Back button (arrow towards the top-left of the dialogue box) to correct your choices before proceeding ahead.

Otherwise, click the **Next** button to continue with the installation.



4.1.12 Click **Finish** to complete the installation process.

4.1.13 ADSS Web RA URLs

Use the following URLs to access the ADSS Web RA Server web sites:

Service	URL Format	Example
ADSS Web RA Admin	https://<machine-name>:PORT	https://localhost:443
ADSS Web RA Desktop Web	https://<machine-name>:PORT	https://localhost:81
ADSS Web RA API	https://<machine-name>:PORT	https://localhost:82
ADSS Web RA Device	https://<machine-name>:PORT	http://localhost:83 https://localhost:84
ADSS Web RA SSL Device	https://<machine-name>:PORT	https://localhost:85 https://localhost:86
ADSS Web RA Windows Integrated CEP Service	https://<machine-name>:PORT	https://localhost:87
ADSS Web RA Windows Integrated CES Service	https://<machine-name>:PORT	https://localhost:88
ADSS Web RA Windows SSL CEP Service	https://<machine-name>:PORT	https://localhost:89
ADSS Web RA Windows SSL CES Service	https://<machine-name>:PORT	https://localhost:90
ADSS Web RA Windows User Name Password CEP Service	https://<machine-name>:PORT	https://localhost:91
ADSS Web RA Windows User Name Password CES Service	https://<machine-name>:PORT	https://localhost:92

Where necessary (i.e. browsing Admin website) your web browser will prompt you to select the appropriate certificate for authentication purposes. The installation process places the necessary certificates into the Windows Security Store, Internet Explorer, Edge, Chrome and related browsers that rely on the security store, can use them as such.

If you wish to use Firefox and similar web browsers that utilize their own respective security stores you will need to import **adss-default-admin.pfx** and **WebRA-default-admin.cer** from **[WebRAInstallationDirectory]/setup/certs** directory.

There are two options to set secure binding against each ADSS Web RA site:

- Using standard IIS web server HTTP redirects. This means the basic installation is done with various ADSS Web RA sites, where each site has their respective default port/binding but no host name. You can then add new sites for each web site and bind this to the desired external public facing host name and secure port, likely to be 443. Each site can be configured in such a fashion.

Each default ADSS Web RA site can then be configured to permanently redirect to the secure version.

- Once the deployment of ADSS Web RA is completed, the bindings of each site can be changed to use a secure (443) port. The new binding will include the appropriate public facing host name.

Once the bindings of IIS web sites have been put in place, access the ADSS Web RA Administration console and make changes to the general configuration settings. This means changing the public and private URLs for the Desktop Web and API sites accordingly. Once it is complete, save the changes and publish them.

The second option is recommended.

Note: Microsoft Windows Server: TLS 1.3 is enabled by default for installations of Windows Server 2022, integrated applications should support this version of TLS. For application integrations that do not support this and need to be updated, customers can disable TLS 1.3 over TCP in the IIS Bindings

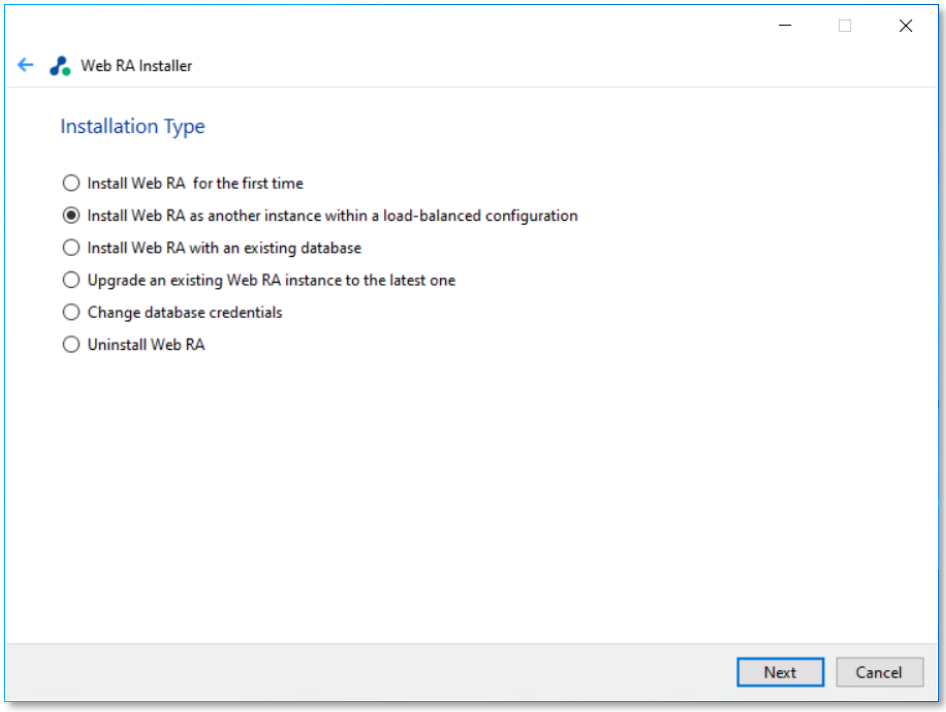
4.2 Installing ADSS Web RA with A Load-Balanced Configuration

Follow these instructions to install ADSS Web RA with a load-balanced configuration.

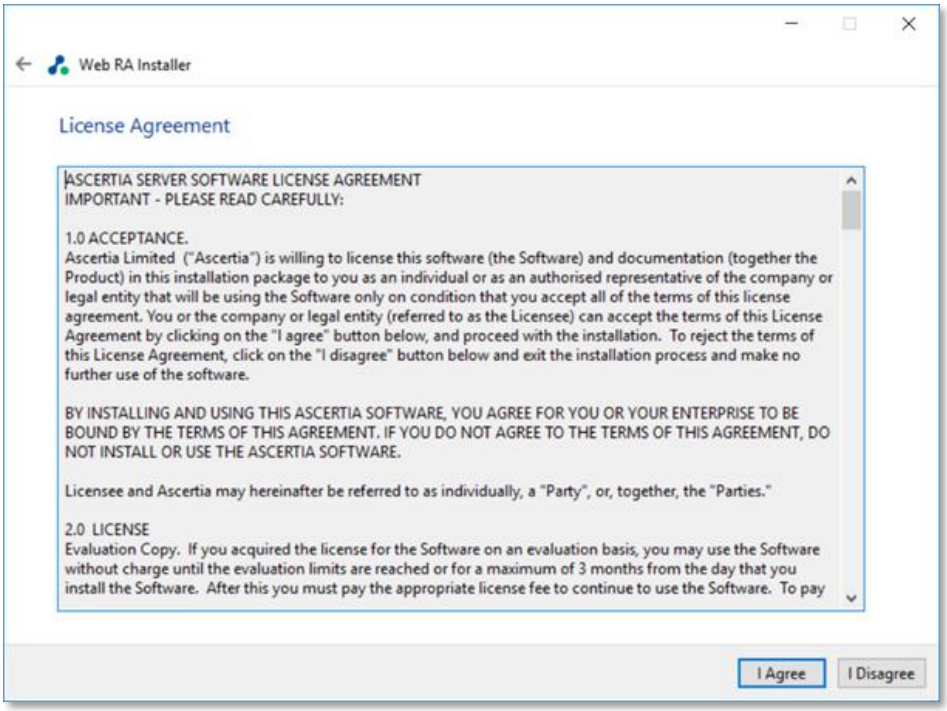
4.2.1 Launch the installer by right-clicking on the file name [Web RA Installation Directory]/setup/install.bat and select Run as administrator.

Follow the installation wizard as described previously until the **Installation Type** screen is shown:

4.2.2 Select the **option Install ADSS Web RA as another instance within a load-balanced configuration**.



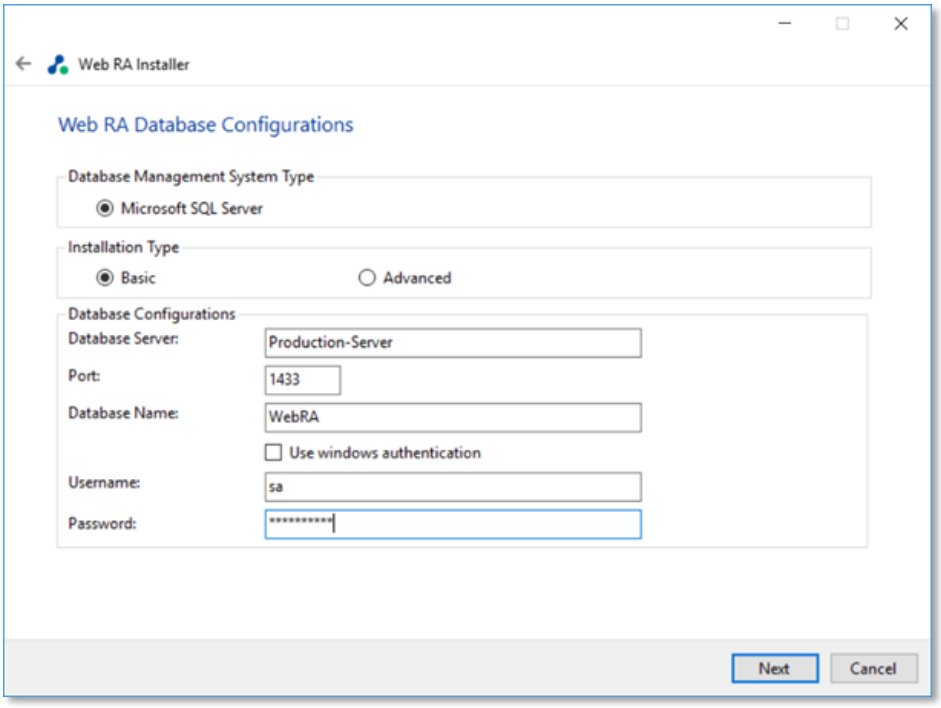
4.2.3 Click the **Next** button to show the **License Agreement**.



4.2.4 Click the **I Agree** button to continue.

4.2.5 The **Readme screen** will be displayed with new features list. Click Next to proceed.

4.2.6 The following screen for **Database Configurations** will be displayed. Enter the required fields and click **Next**.



The information displayed above is an example and you should configure the relevant settings for your own environment.

The ADSS Web RA database schema and the version required by the installer must be the same.

*If the current ADSS Web RA database schema is older than the version required by the installer, and you click **Next,** the installer will prompt you that ADSS Web RA database schema will be upgraded to the latest version. Click **OK** to authorise the schema update.*

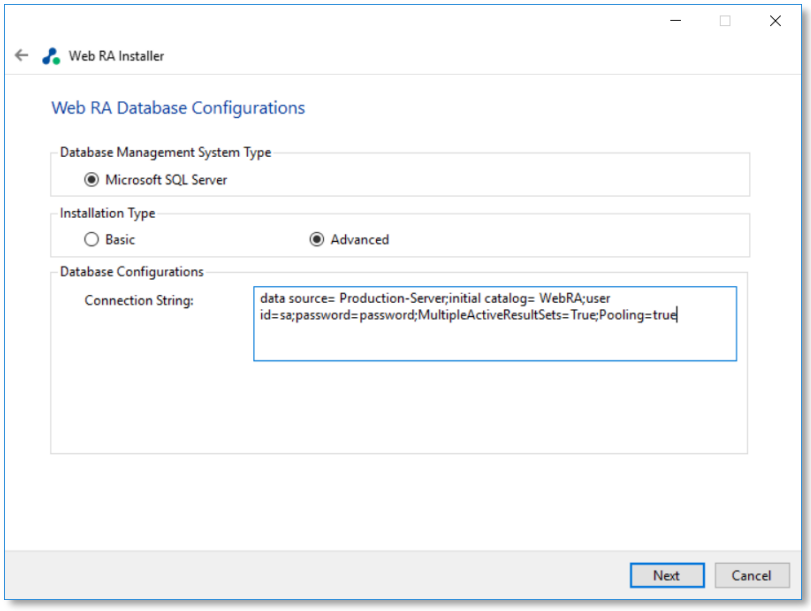
Furthermore, you can either choose to do a basic installation or use an advanced one. If this is a basic installation, then use the first option **Basic** and provide the appropriate ADSS Web RA database credentials. The information displayed above is an example and you should configure the relevant settings for your own environment.

Once you have entered the database credentials and select Next, the installer uses the information to test the connectivity to the database. If the installer can establish the connection with the database, then it will proceed with the installation.

The following table explains the **Database Configurations** screen.

Item	Description
Database Server / Host Name	Database server IP or DNS name.
Port	Database listening port. For SQL Server the default port is **1433.**
Database Name	Name of the database instance. Note this must exist prior to the installation.
Use Windows Authentication	If enabled, installer will use the Windows logged in user to communicate with database. You are required to enter password because it will be used in Application Pool to set the Identity against this user for all websites. By default, the current logged in user will be configured in the Application Pool Identity. If you wish to run ADSS Web RA under a different windows user, then you need to change it manually. If your requirement is to use SQL Server authentication, then type SQL Server Username and Password in the underneath fields without enabling this option.
Username	Name of the database user. Note this must exist prior to the installation. It is not required in the case of Windows Authentication.
Password	Password credential of the database user. Note this must exist prior to the installation. In case of Windows Authentication, type the password of domain user shown in the Username field to configure the Application Pool Identity in IIS Server for successful communication with SQL Server.

If this is not a basic installation and you choose the second option to "**Advanced"** then the following screen is shown:



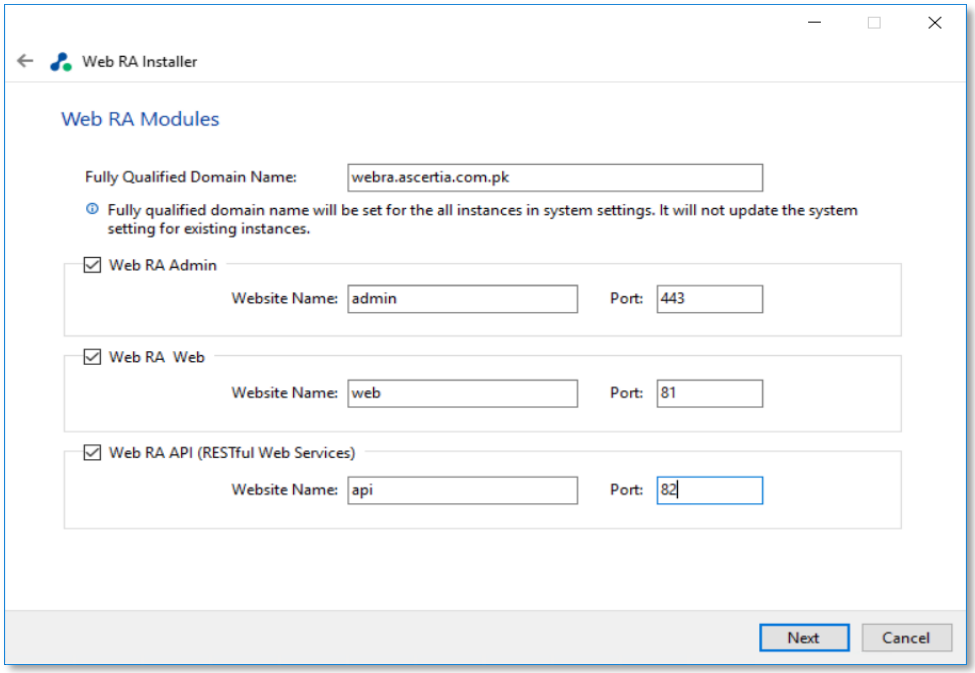
The information displayed above is an example and you should configure the relevant settings for your own environment.

Once you complete the options and select **Next**, the installer uses the information provided to test the connectivity to the database. If the installer can establish the connection with the database, then it will proceed with the installation.

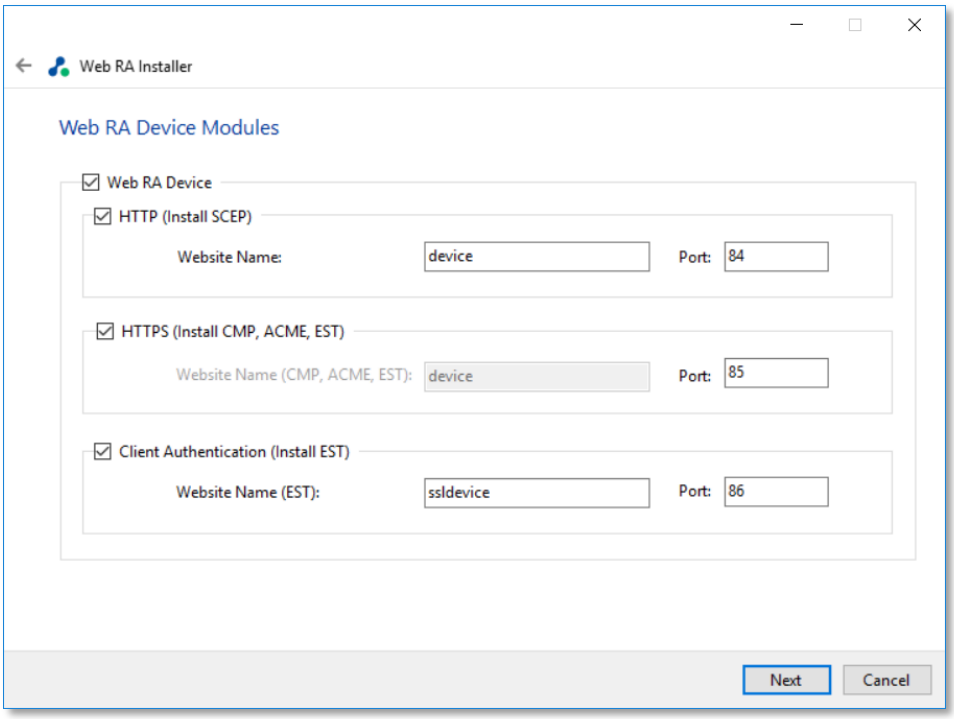
The following table entails details of the configuration options:

Item	Description
ADSS Web RA Connection String	The following are sample connection strings for SQL Server: • **Simple One** - "data source= **[Database Server Address]**;initial catalog= **[Database Name]**;user id=**[Database User Name]**;password=**[Database User Password]**;MultipleActiveResultSets=True;Pooling=true" • **For Named instance** - "data source= **[Database Server Address]\[SQL Server Instance Name]**;initial catalog=**[Database Name]**;user id=**[Database User Name]**;password**[Database User Password]**;MultipleActiveResultSets=True;Pooling=true" • **For Windows Authentication** - "data source= **[Database Server Address]**;initial catalog=**[Database Name]**;integrated security=SSPI;MultipleActiveResultSets=True;Pooling=true
Username	Field will only be shown in case of Windows Authentication while for SQL Server Authentication, username will be provided in the connection string.
Password	In case of Windows Authentication, type the password of domain user shown in the Username field to configure the Application Pool Identity in IIS Server for successful communication with SQL Server. In case of SQL Server authentication, password will be provided in the connection string.

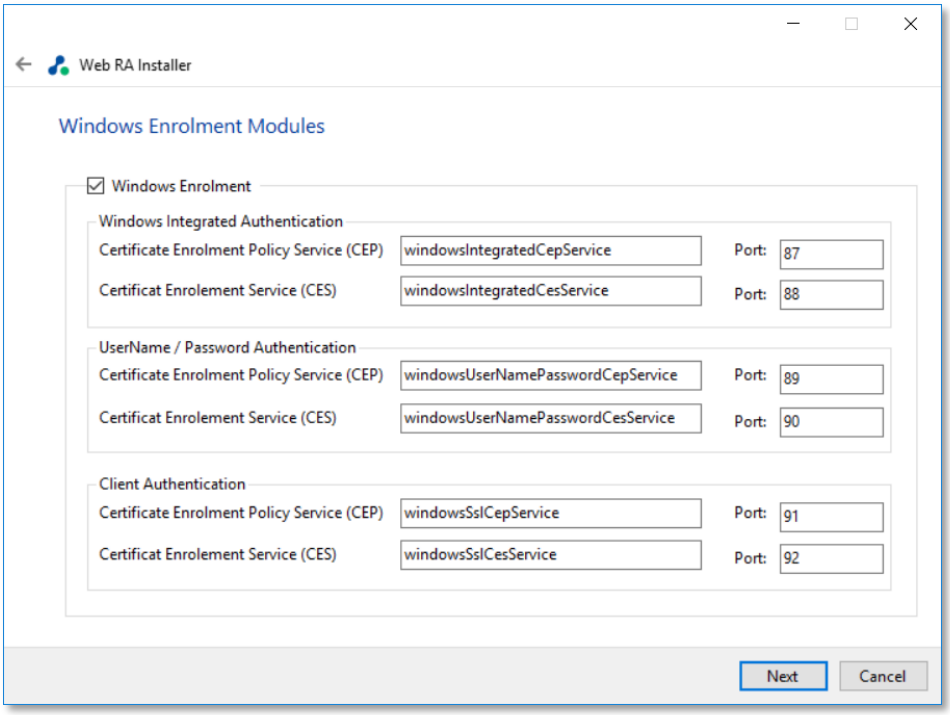
4.2.7 Click the **Next** button to select **Web RA Modules**.



4.2.8 Select the appropriate modules to install the required features. For each selected application, provide the web application name and port and click **Next**. A typical in-house installation of ADSS Web RA should only include Admin, Desktop Web, and the API and lastly, the device will be added.



4.2.9 Select **Windows Enrolment**. For each selected application, provide the web application name and port. Then click **Next**.

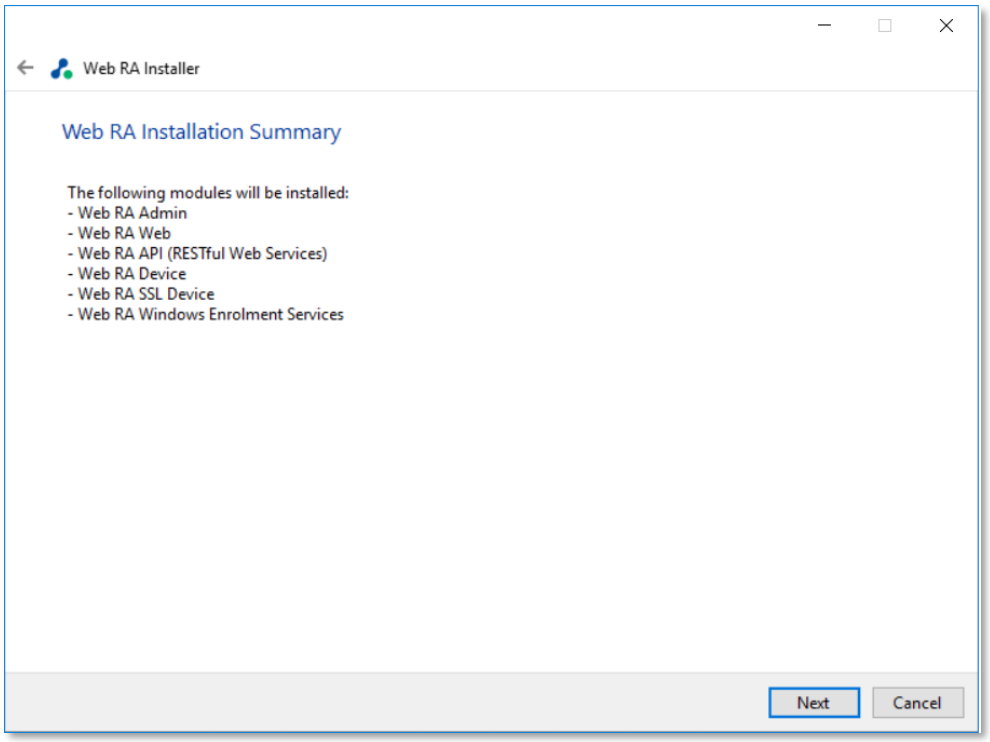


The information displayed above is an example, which you may change to suit your environment and organisation preferences. However, the example shown is sufficient. The names will appear as websites under IIS Manager.

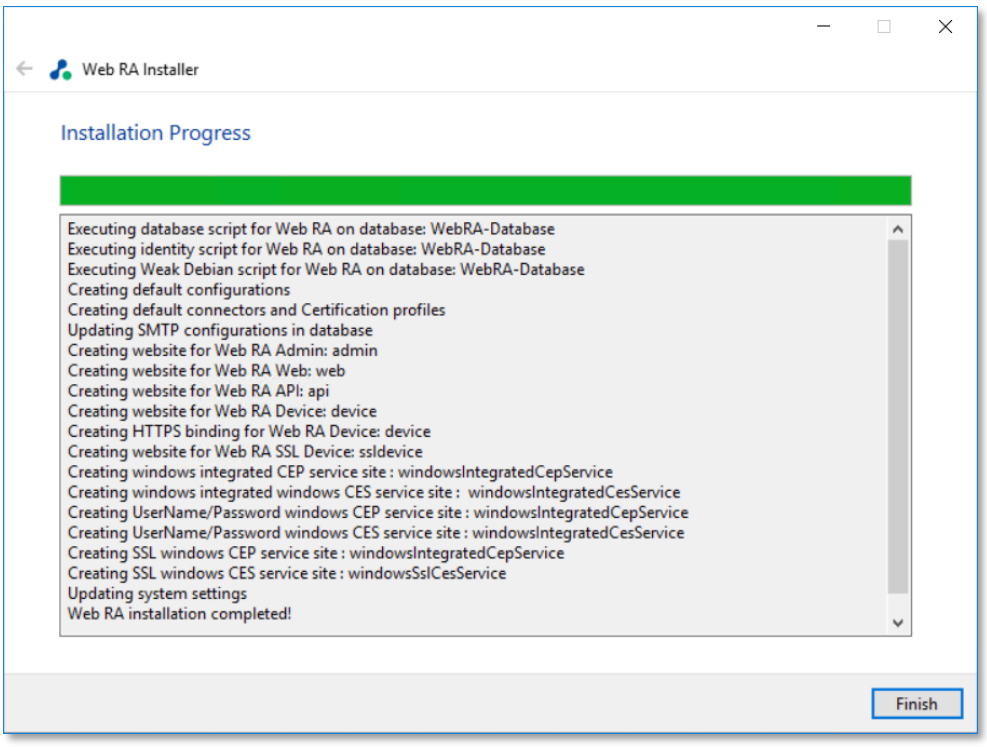
The following table explains the **Windows Enrolment** section.

Item	Description
ADSS Web RA Admin	ADSS Web RA Admin is used by the administrators to manage the system wide configurations, service plans, user accounts and access control etc.
ADSS Web RA Web	ADSS Web RA Web is used to manage certificates for creation, renewal and revocation.
ADSS Web RA API	**REST API** is used to integrate ADSS Web RA functionality within your own portal.
ADSS Web RA Device	ADSS Web RA device is used to manage device enrolment for certificate creation, renewal and revocation. This site will be deployed with http and https bindings.
ADSS Web RA SSL Device	ADSS Web RA SSL device is used to manage device enrolment over SSL for certificate creation, renewal and revocation e.g. EST Protocol. This site will be deployed with https SSL.
Windows Enrolment	Windows Enrolment is used to manage certificate renewal or auto-enrolment on a windows machine.

4.2.10 Click the **Next** button to show the **Installation Summary** and complete the installation.



This screen shows the installation summary by listing the different product modules that will be installed. If you think any listed item is incorrect then use the **Back** button (arrow towards the top-left of the dialogue box) to correct your choices before proceeding.



4.2.11 Click **Finish** to complete the installation process.

4.2.12 **ADSS Web RA URLs**

Use the following URLs to access the ADSS Web RA Server Web sites:

Service	URL Format	Example
ADSS Web RA Admin	https://<machine-name>:PORT	https://localhost:443
ADSS Web RA Desktop Web	https://<machine-name>:PORT	https://localhost:81
ADSS Web RA API	https://<machine-name>:PORT	https://localhost:82
ADSS Web RA Device	https://<machine-name>:PORT	http://localhost:83 https://localhost:84
ADSS Web RA SSL Device	https://<machine-name>:PORT	https://localhost:85 https://localhost:86
ADSS Web RA Windows Integrated CEP Service	https://<machine-name>:PORT	https://localhost:87
ADSS Web RA Windows Integrated CES Service	https://<machine-name>:PORT	https://localhost:88
ADSS Web RA Windows SSL CEP Service	https://<machine-name>:PORT	https://localhost:89
ADSS Web RA Windows SSL CES Service	https://<machine-name>:PORT	https://localhost:90

ADSS Web RA Windows User Name Password CEP Service	https://<machine-name>:PORT	https://localhost:91
ADSS Web RA Windows User Name Password CES Service	https://<machine-name>:PORT	https://localhost:92

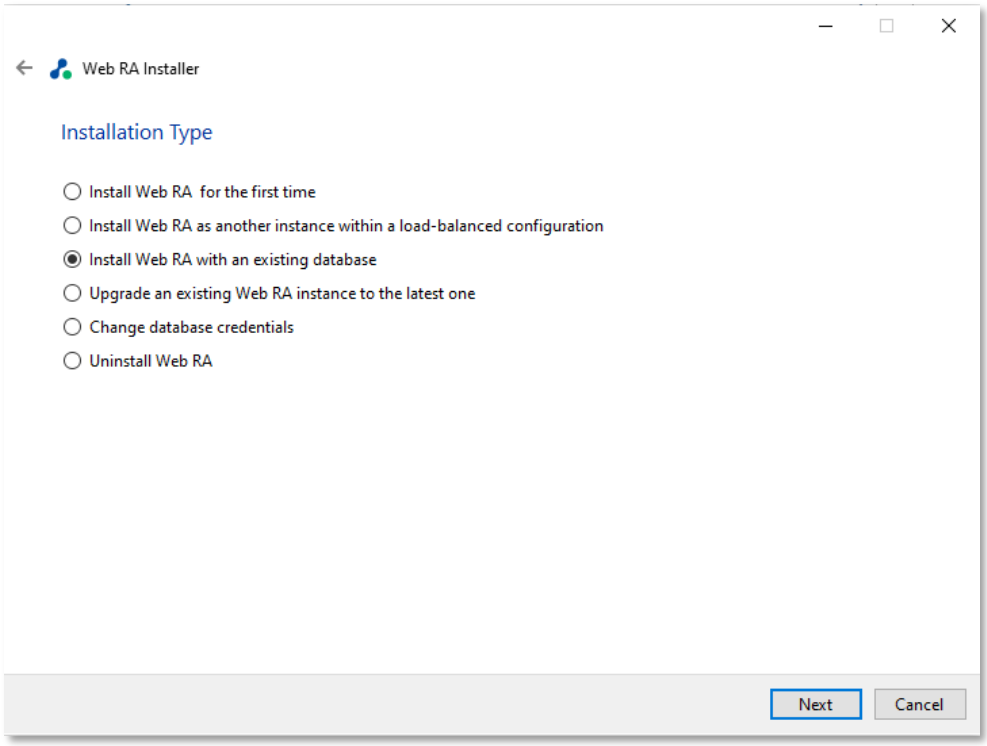
The site IDs of deployed IIS websites should be the same across all the instances in a load balanced environment to run Web RA application properly. Therefore, to ensure a successful load-balanced installation, you should check that the required site IDs on the primary instance are also available on the secondary instance(s). If the site IDs are already used on the secondary instance(s), the load-balanced installations will not be able to complete successfully.

4.3 Installing ADSS Web RA with an Existing Database

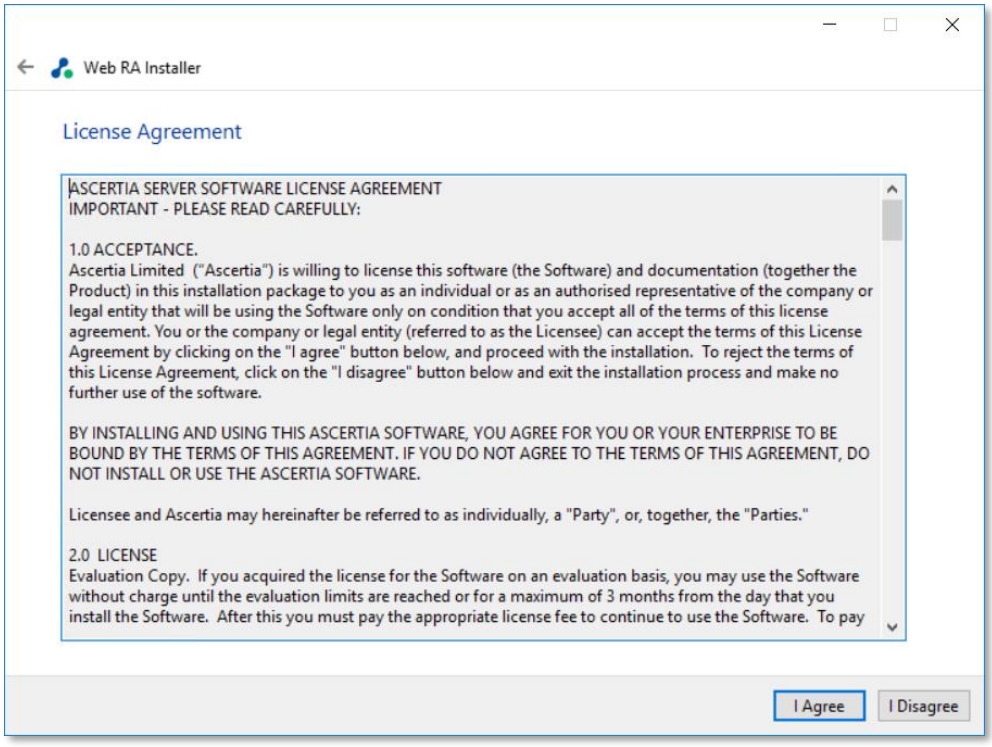
In order to install the ADSS Web RA with an existing database, follow the below mentioned installation instructions:

4.3.1 Launch the installer by right-clicking on the file name **[ADSS Web RA Installation Directory]/setup/install.bat** and select **Run** as administrator. Follow the installation wizard as described previously until the Installation Type screen is shown:

4.3.2 Select the option **Install ADSS Web RA within an existing database**.

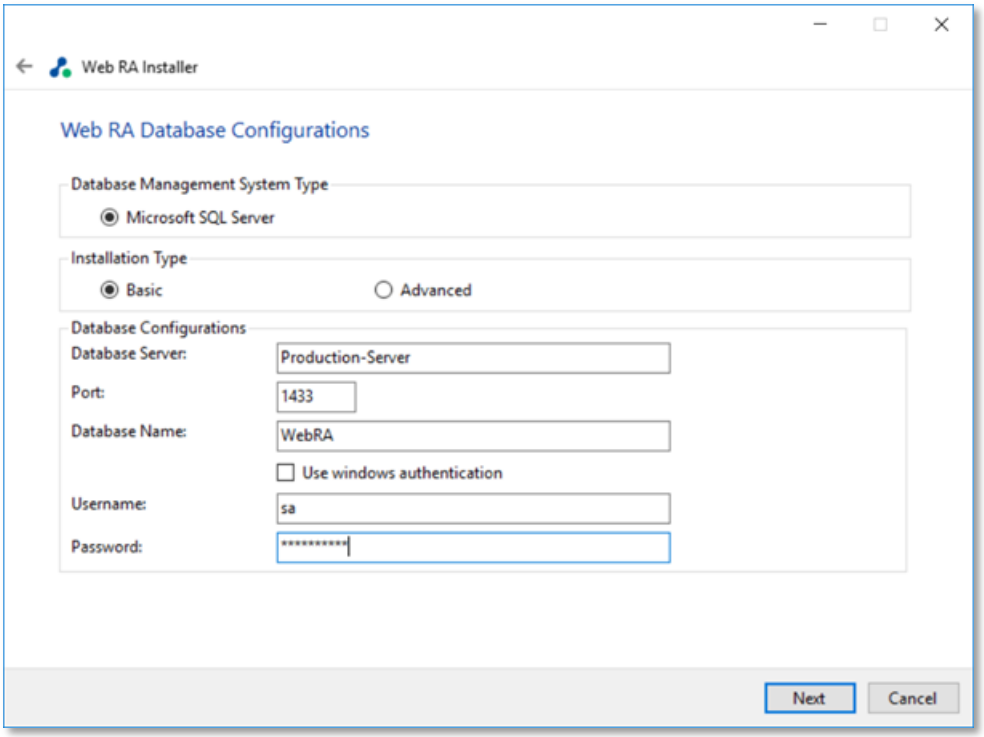


4.3.3 Click the **Next** button to show the **License Agreement**.



4.3.4 Click the **I Agree** button to continue.

4.3.5 The **Readme screen** will be displayed with new features list. Click **Next** to proceed. The following screen for **Database Configurations** will be displayed:



The information displayed above is an example and you should configure the relevant settings for your own environment.

The ADSS Web RA database schema and the version required by the installer must be the same.

*If the current ADSS Web RA database schema is older than the version required by the installer, and you click **Next,** the installer will prompt you that ADSS Web RA database schema will be upgraded to the latest version. Click **OK** to authorise the schema update.*

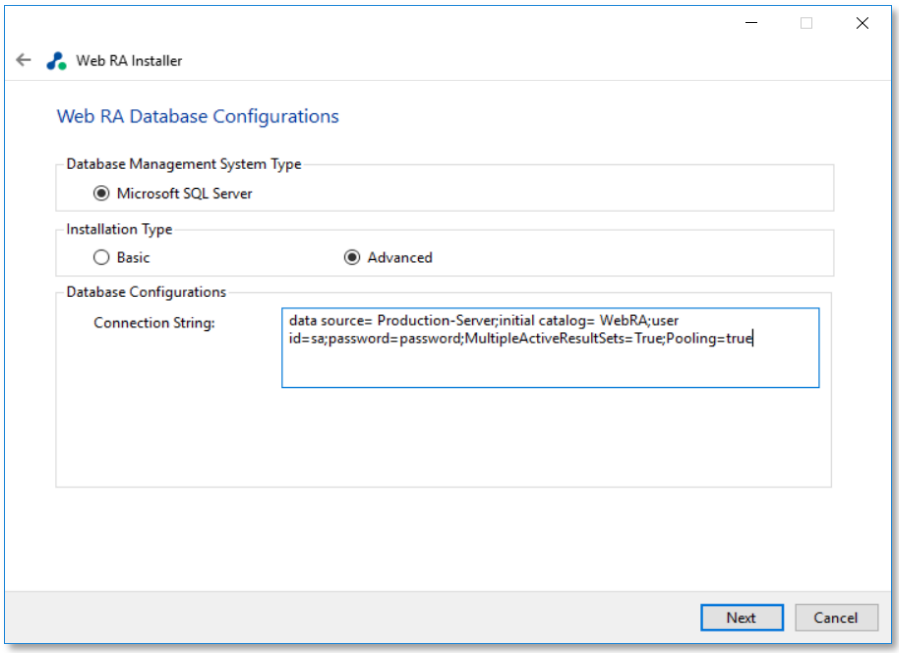
Furthermore, you can either choose to do a basic installation or use an advanced one. If this is a basic installation, then use the first option **Basic** and provide the appropriate ADSS Web RA database credentials. The information displayed above is an example and you should configure the relevant settings for your own environment.

Once you have entered the database credentials and select Next, the installer uses the information to test the connectivity to the database. If the installer can establish the connection with the database, then it will proceed with the installation.

The following table explains the **Database Configurations**.

Item	Description
Database Server / Host Name	Database server IP or DNS name.
Port	Database listening port. For SQL Server the default port is **1433.**
Database Name	Name of the database instance. Note this must exist prior to the installation.
Use Windows Authentication	If enabled, installer will use the Windows logged in user to communicate with database. You are required to enter password because it will be used in Application Pool to set the Identity against this user for all websites. By default, the current logged in user will be configured in the Application Pool Identity. If you wish to run ADSS Web RA under a different windows user, then you need to change it manually. If your requirement is to use SQL Server authentication, then type SQL Server Username and Password in the underneath fields without enabling this option.
Username	Name of the database user. Note this must exist prior to the installation. It is not required in the case of Windows Authentication.
Password	Password credential of the database user. Note this must exist prior to the installation. In case of Windows Authentication, type the password of domain user shown in the Username field to configure the Application Pool Identity in IIS Server for successful communication with SQL Server.

If this is not a basic installation and you choose the second option to "**Advanced"** then the following screen is shown.



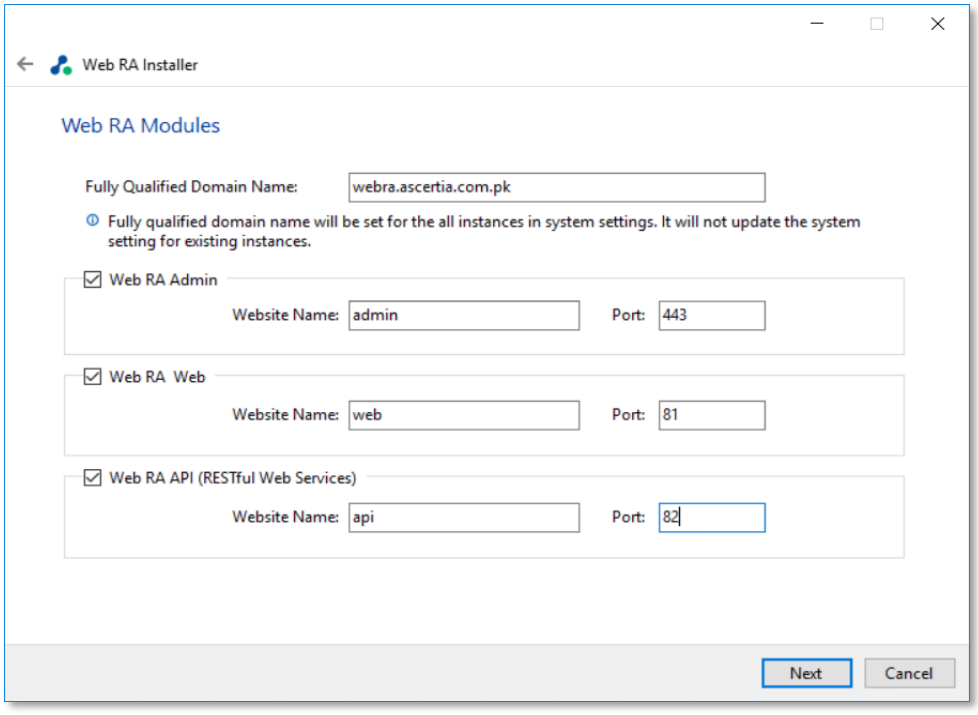
The information displayed above is an example and you should configure the relevant settings for your own environment.

Once you complete the options and select **Next**, the installer uses the information provided to test the connectivity to the database. If the installer can establish the connection with the database, then it will proceed with the installation.

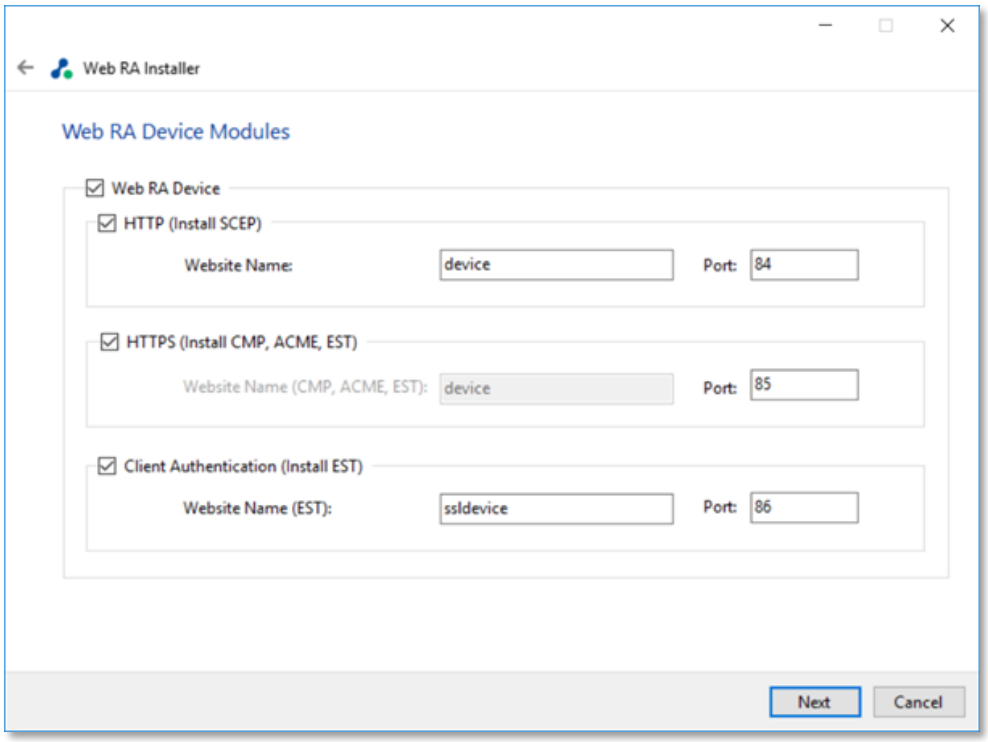
The following table explains the **Advanced Database Configurations**.

Item	Description
ADSS Web RA Connection String	The following are sample connection strings for SQL Server: • **Simple One** - "data source= **[Database Server Address]**;initial catalog= **[Database Name]**;user id=**[Database User Name]**;password=**[Database User Password]**;MultipleActiveResultSets=True;Pooling=true" • **For Named instance** - "data source= **[Database Server Address]\[SQL Server Instance Name]**;initial catalog=**[Database Name]**;user id=**[Database User Name]**;password**[Database User Password]**;MultipleActiveResultSets=True;Pooling=true" • **For Windows Authentication** - "data source= **[Database Server Address]**;initial catalog=**[Database Name]**;integrated security=SSPI;MultipleActiveResultSets=True;Pooling=true
Username	Field will only be shown in case of Windows Authentication while for SQL Server Authentication, username will be provided in the connection string.
Password	In case of Windows Authentication, type the password of domain user shown in the Username field to configure the Application Pool Identity in IIS Server for successful communication with SQL Server. In case of SQL Server authentication, password will be provided in the connection string.

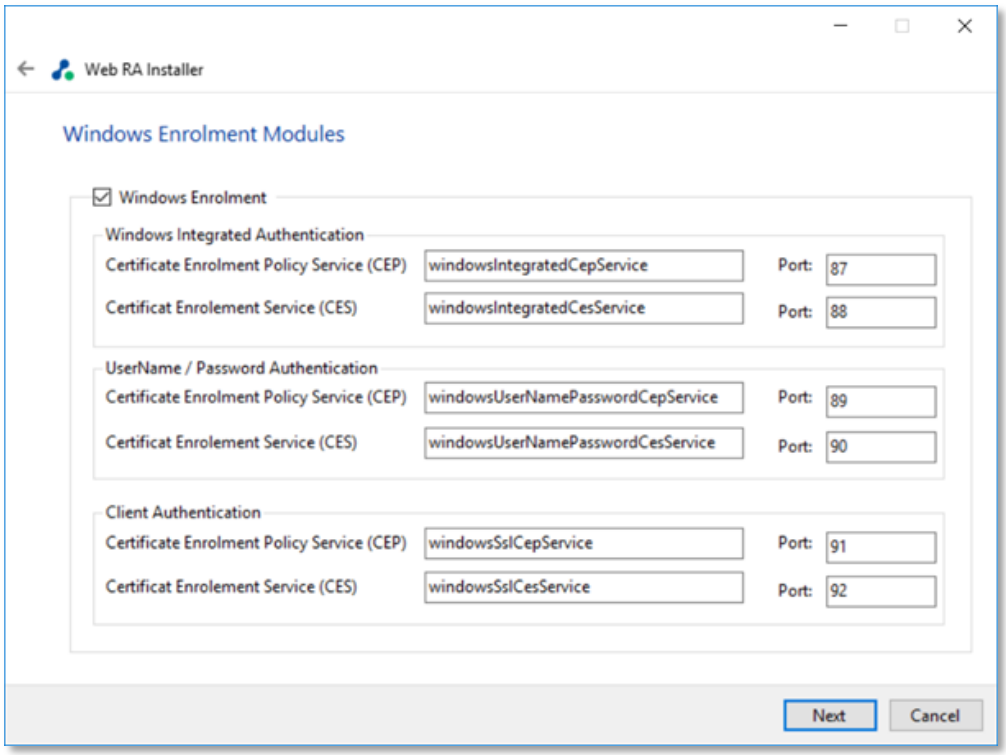
4.3.6 Click the **Next** button to select **Web RA Modules**.



4.3.7 Select **modules** to install the required features. For each selected application, provide the web application name and port. A typical in-house installation of ADSS Web RA should only include Admin, Desktop Web, and the API. However, the device will be added at the end. Click **Next** to proceed.



4.3.8 Select **Windows Enrolment**. For each selected application, provide the web application name and port. Then click **Next**.

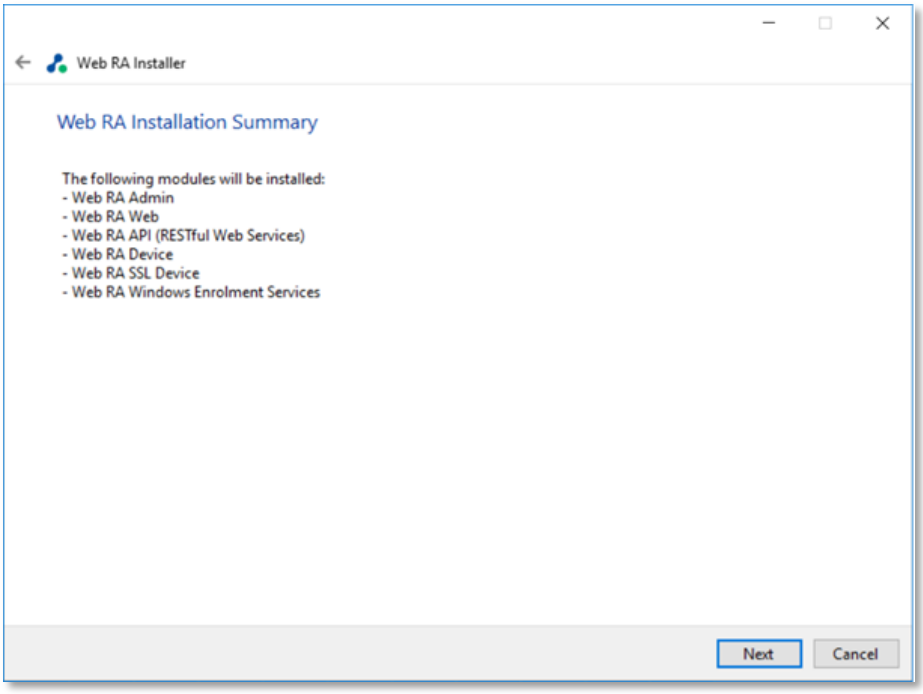


The information displayed above is an example, which you may change to suit your environment and organisation preferences. The names will appear as websites under IIS.

The following table explains the **Windows Enrolment Modules**.

Item	Description
ADSS Web RA Admin	ADSS Web RA Admin is used by the administrators to manage the system wide configurations, service plans, user accounts and access control etc.
ADSS Web RA Web	ADSS Web RA Web is used to manage certificates for creation, renewal and revocation.
ADSS Web RA API	**REST API** is used to integrate ADSS Web RA functionality within your own portal.
ADSS Web RA Device	ADSS Web RA device is used to manage device enrolment for certificate creation, renewal and revocation. This site will be deployed with http and https bindings.
ADSS Web RA SSL Device	ADSS Web RA SSL device is used to manage device enrolment over SSL for certificate creation, renewal and revocation e.g. EST Protocol. This site will be deployed with https SSL.
Windows Enrolment	Windows Enrolment is used to manage certificate renewal or auto-enrolment on a windows machine.

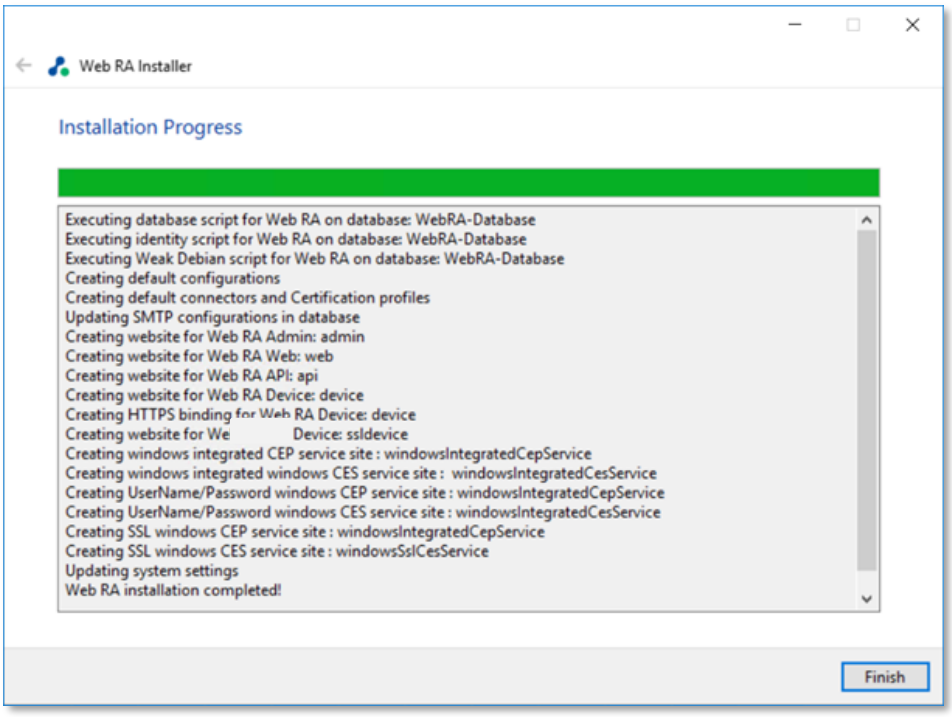
4.3.9 Click the **Next** button to see the summary and complete the installation.



This screen shows the installation summary by listing the different product modules that will be installed.

If you think any listed item is incorrect then use the **Back** button (arrow towards the top-left of the dialogue box) to correct your choices before proceeding ahead.

4.3.10 Click the **Next** button to continue with the installation.



Click the **Finish** button to complete the installation process.

4.3.11 ADSS Web RA URLs

See these URLs to access the ADSS Web RA web sites:

Service	URL Format	Example
ADSS Web RA Admin	https://<machine-name>:PORT	https://localhost:443
ADSS Web RA Desktop Web	https://<machine-name>:PORT	https://localhost:81
ADSS Web RA API	https://<machine-name>:PORT	https://localhost:82
ADSS Web RA Device	https://<machine-name>:PORT	http://localhost:83 https://localhost:84
ADSS Web RA SSL Device	https://<machine-name>:PORT	https://localhost:85 https://localhost:86
ADSS Web RA Windows Integrated CEP Service	https://<machine-name>:PORT	https://localhost:87
ADSS Web RA Windows Integrated CES Service	https://<machine-name>:PORT	https://localhost:88
ADSS Web RA Windows SSL CEP Service	https://<machine-name>:PORT	https://localhost:89
ADSS Web RA Windows SSL CES Service	https://<machine-name>:PORT	https://localhost:90

ADSS Web RA Windows User Name Password CEP Service	https://<machine-name>:PORT	https://localhost:91
ADSS Web RA Windows User Name Password CES Service	https://<machine-name>:PORT	https://localhost:92

4.4 Upgrading ADSS Web RA

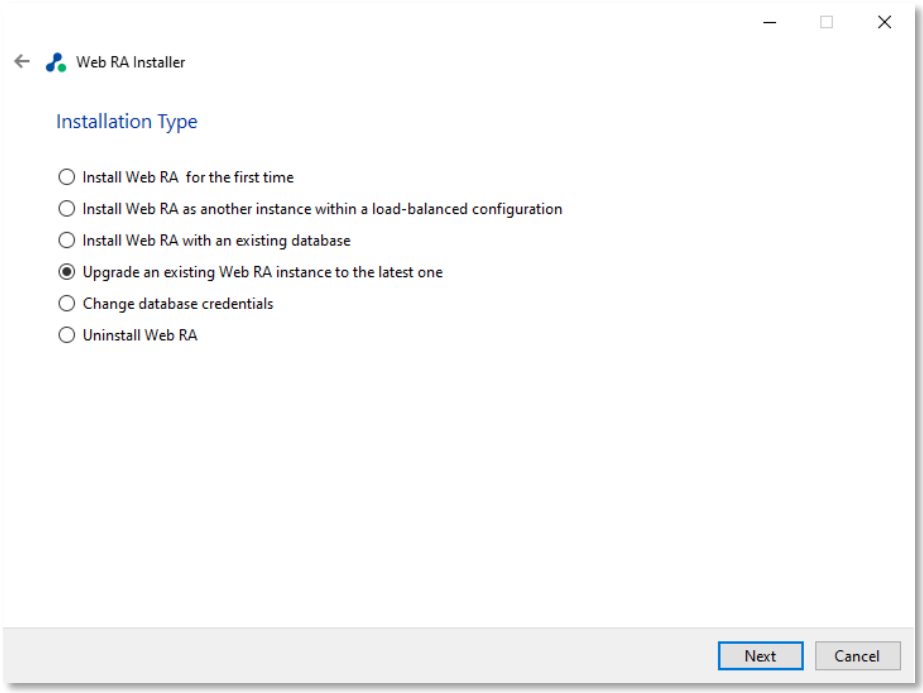
The upgrade process for ADSS Web RA is quick and easy. The existing data files, database schema and database entries are automatically upgraded during the process.

Follow these instructions to upgrade an older version of ADSS Web RA to the latest version.

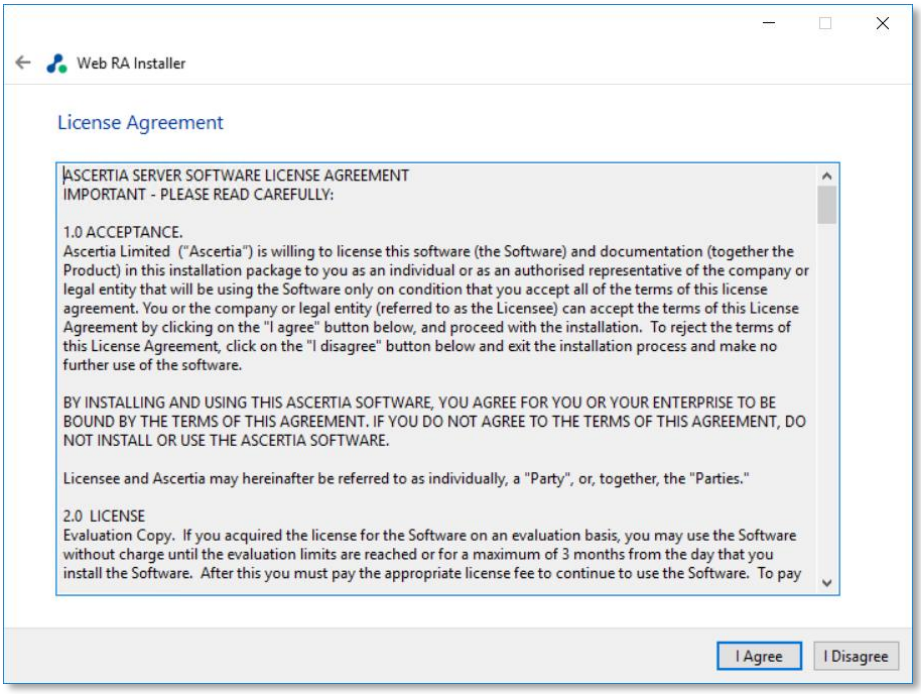
4.4.1. Launch the installer by right-clicking on the file name **[ADSS Web RA Installation Directory]/setup/install.bat** and select **Run as administrator**.

Follow the installation wizard as described previously until the **Installation Type** screen is shown:

4.4.2. Select the option **Upgrade an existing ADSS Web RA instance to the latest one**

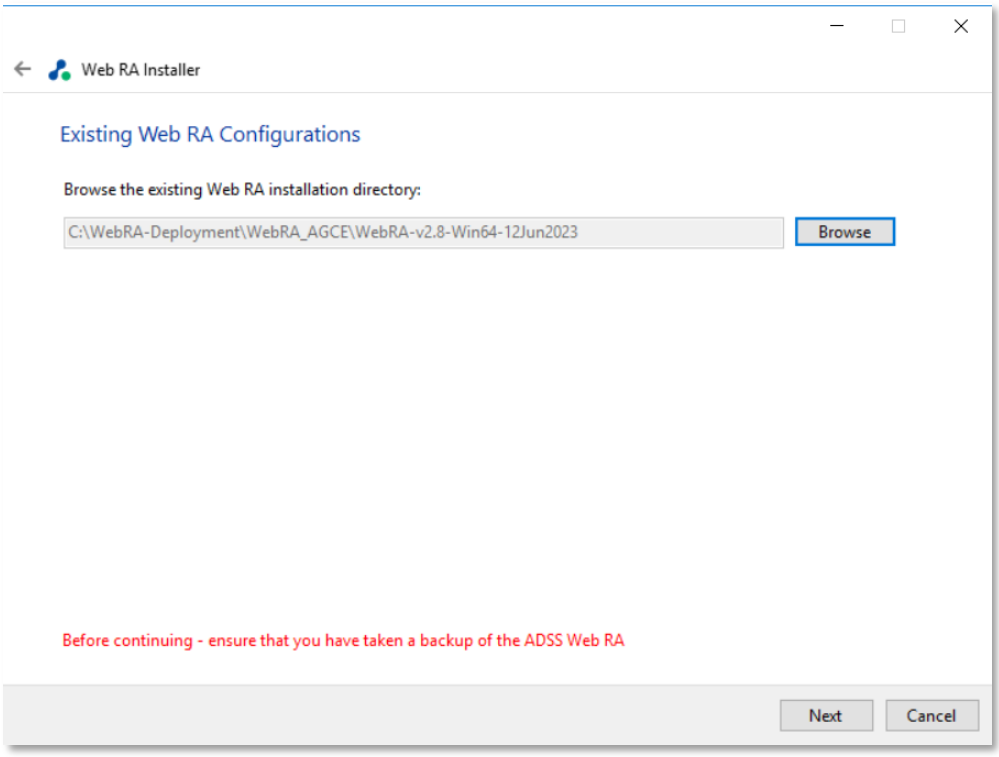


4.4.3. Click the **Next** button to view and accept the **License Agreement**.



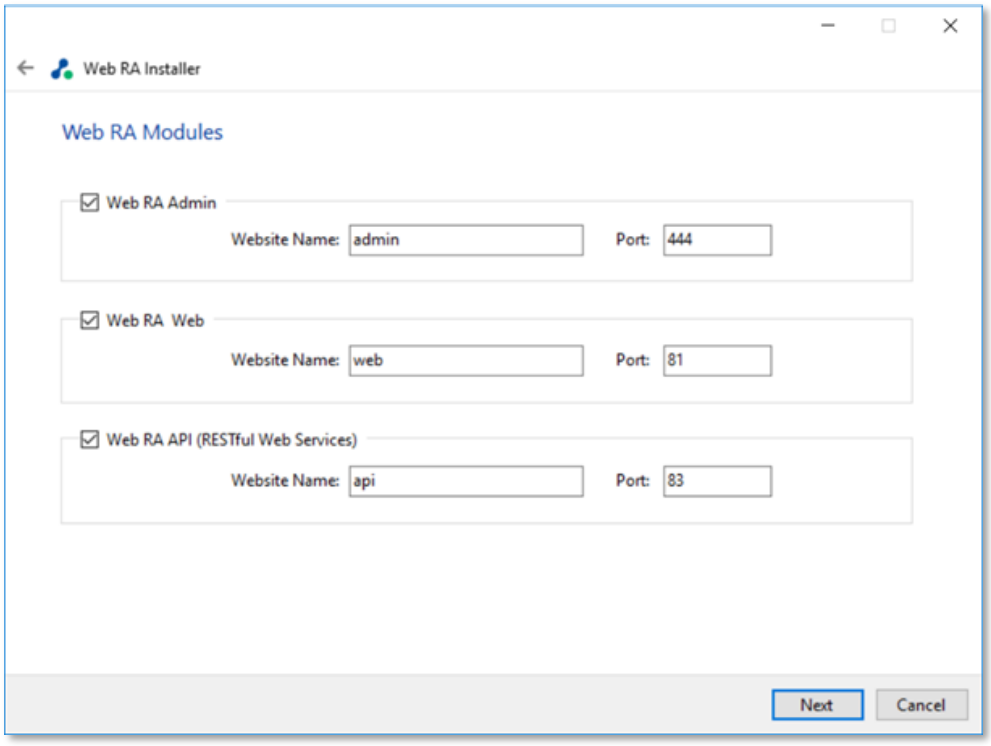
4.4.4. Click the **I Agree** button to proceed

4.4.5. The next appearing screen will be for ReadMe text. This includes all features of current version. Click **Next** to proceed.

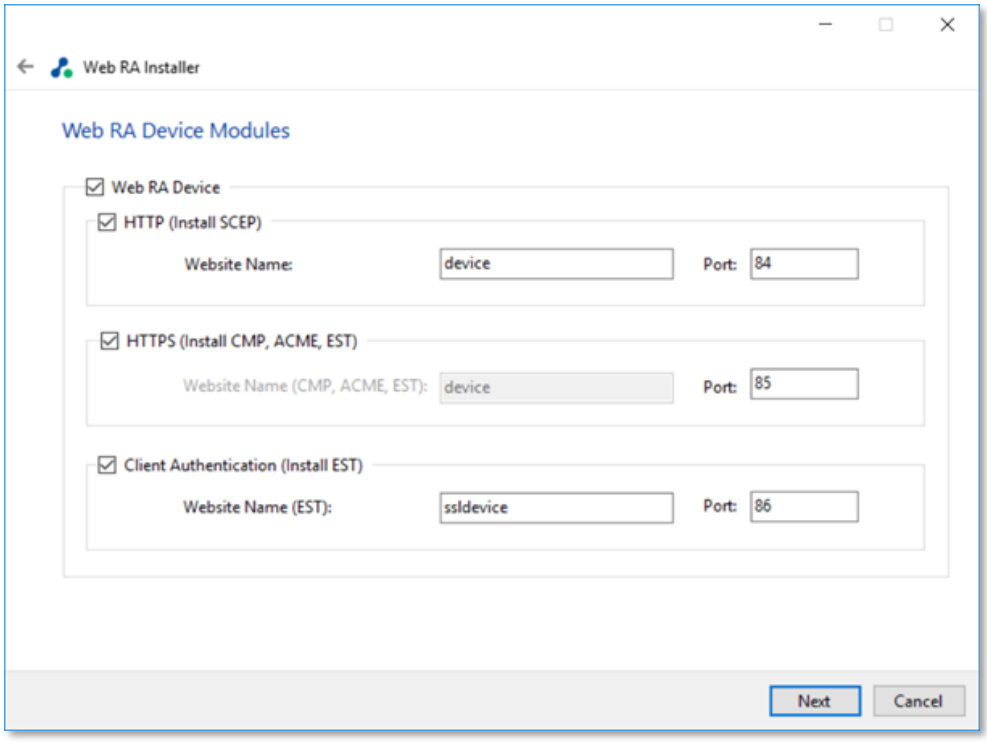


4.4.6. Click **Browse** and define the path to the existing ADSS Web RA installation directory.

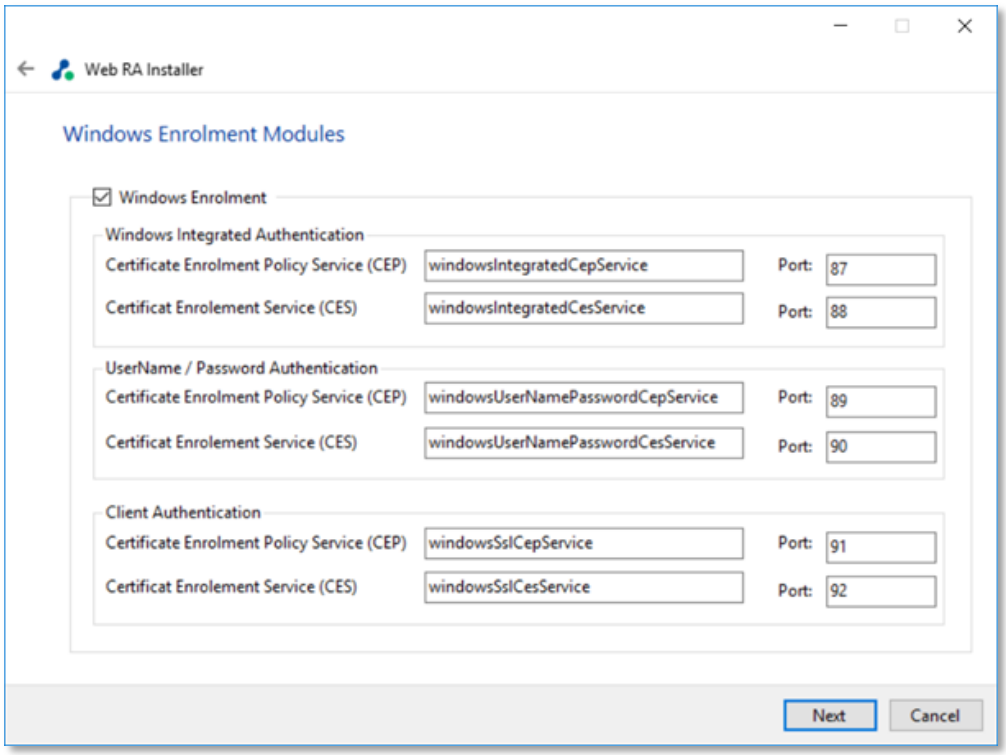
4.4.7. Click the **Next** button to select **Web RA Modules**.



4.4.1. Select **Device Modules** to install the required features. For each selected application, provide the web application name and port. A typical in-house installation of ADSS Web RA should only include Admin, Desktop Web, and the API. However, the device will be added at the end. Click **Next** to proceed.

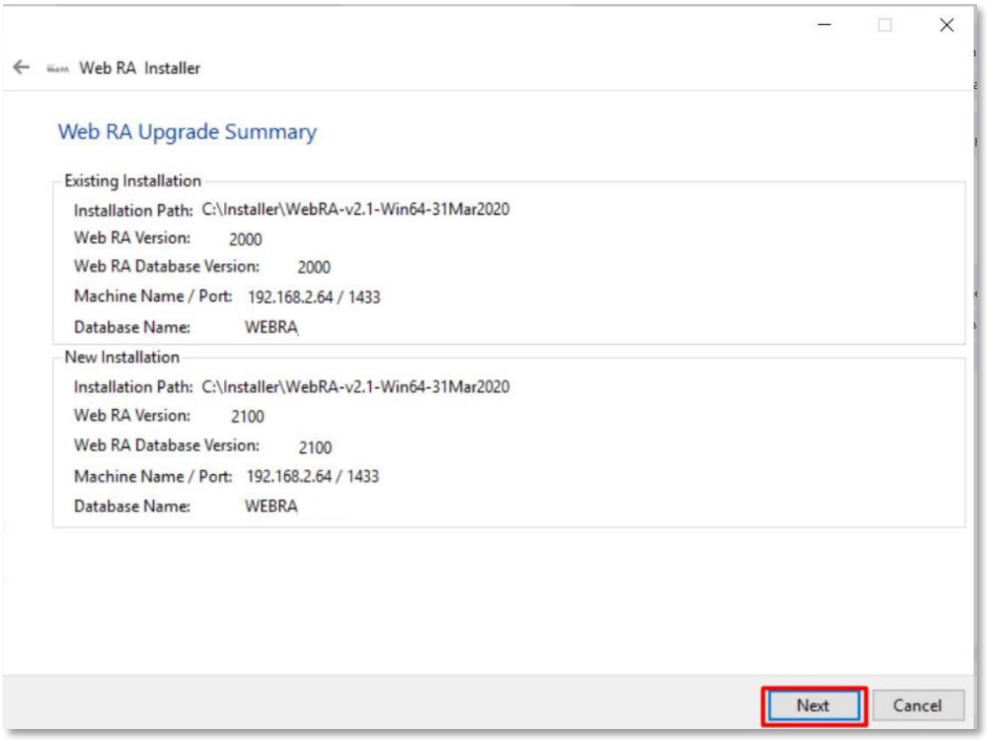


4.4.2. Select **Windows Enrolment**. For each selected application, provide the web application name and port. Then click **Next**.

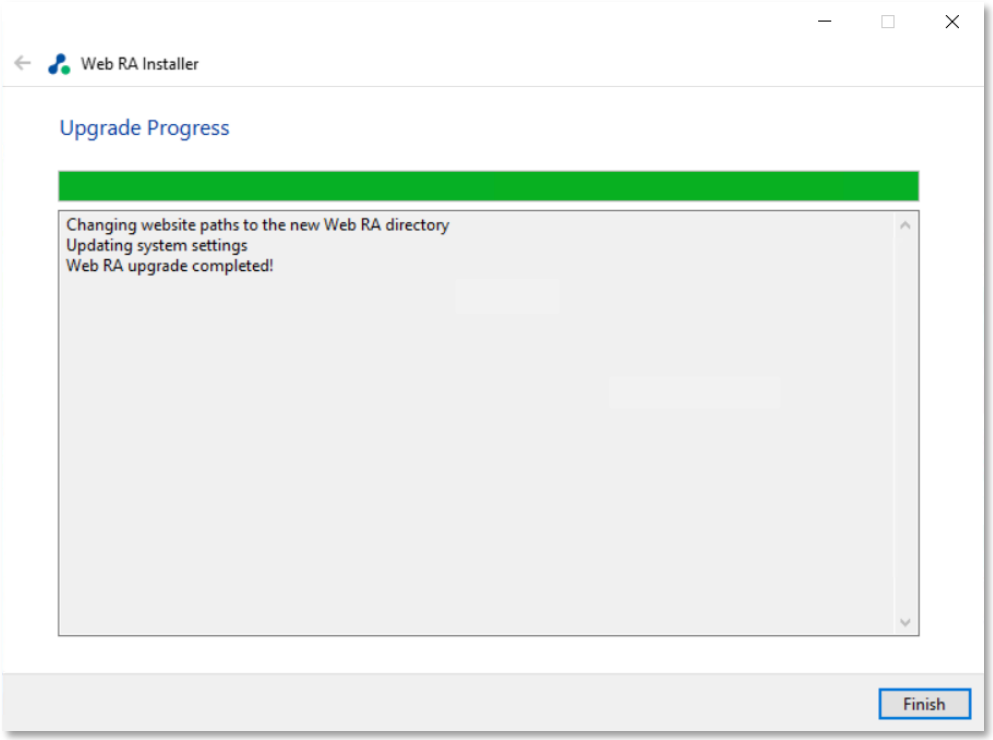


This screen shows a list of all ADSS **Web RA modules**. Components that are already installed are displayed but **greyed** out, while any ADSS Web RA module(s) that have not been installed previously can be selected for installation during the upgrade.

4.4.3. Click the **Next** button to see the **Upgrade Summary**.



4.4.4. Click the **Next** button to start the upgrade progress.



4.4.5. Click the **Finish** button to complete the ADSS Web RA upgrade process.

It is recommended to restart IIS after upgrade installation of ADSS Web RA.

4.5 Upgrade Web RA by adding modules

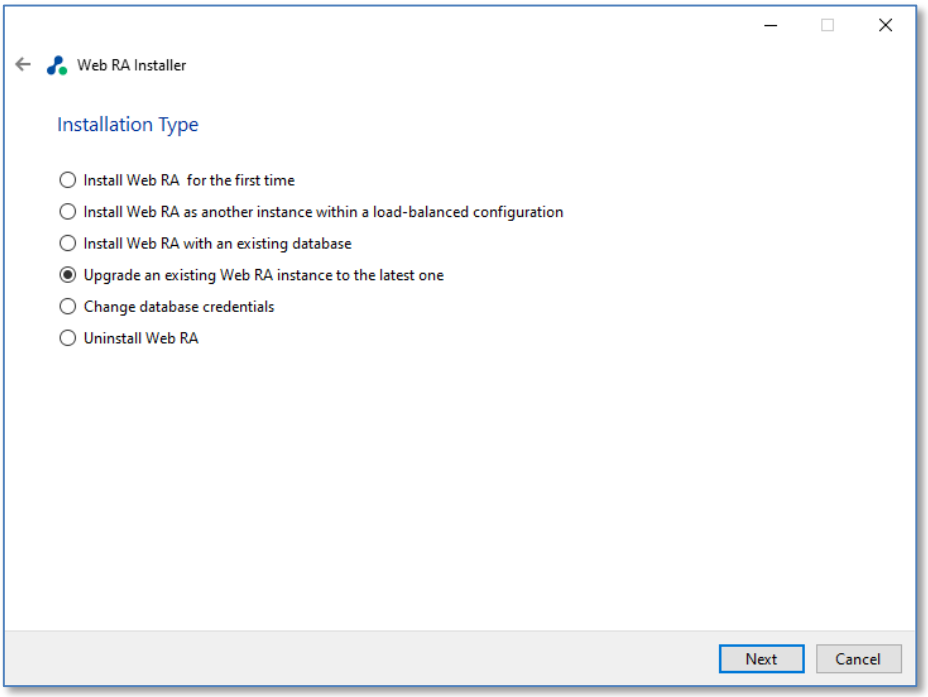
The Web RA installer allows you to add modules to your deployment at a later time if they were not installed initially. For example, if a user installs the Web RA application with the Admin, Web, and API modules but skips the Device Enrolments or Windows Enrolments modules, he can upgrade the existing deployment by adding these skipped modules when needed.

For example base version is v2.9 then follow the below steps:

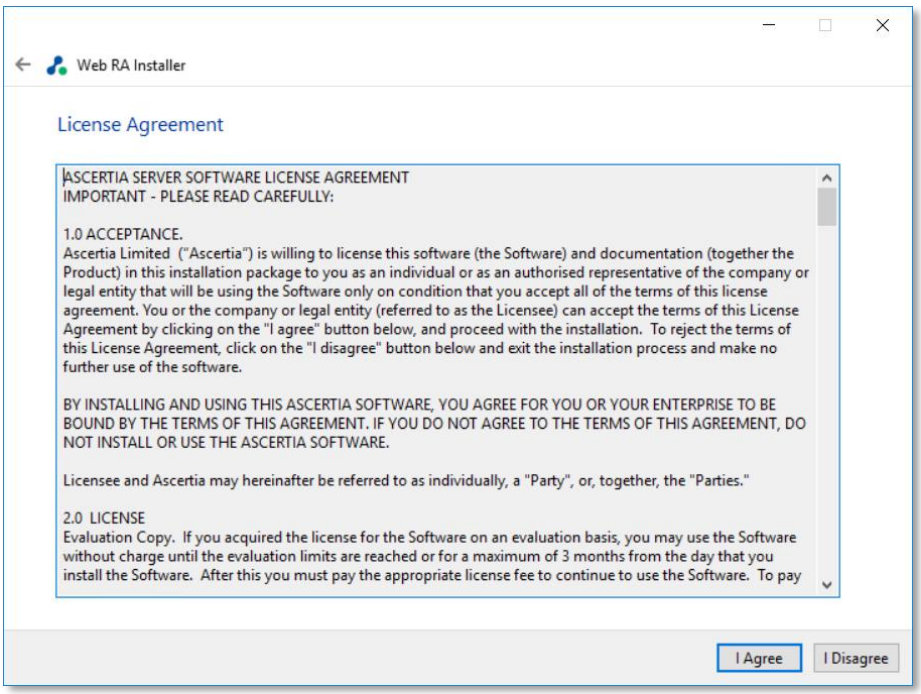
4.5.1. Launch the installer by right-clicking on the file name **[ADSS Web RA Installation Directory]/setup/install.bat** and select **Run as administrator**.

Follow the installation wizard as described previously until the **Installation Type** screen is shown:

4.5.2. Select the option **Upgrade an existing ADSS Web RA instance to the latest one**

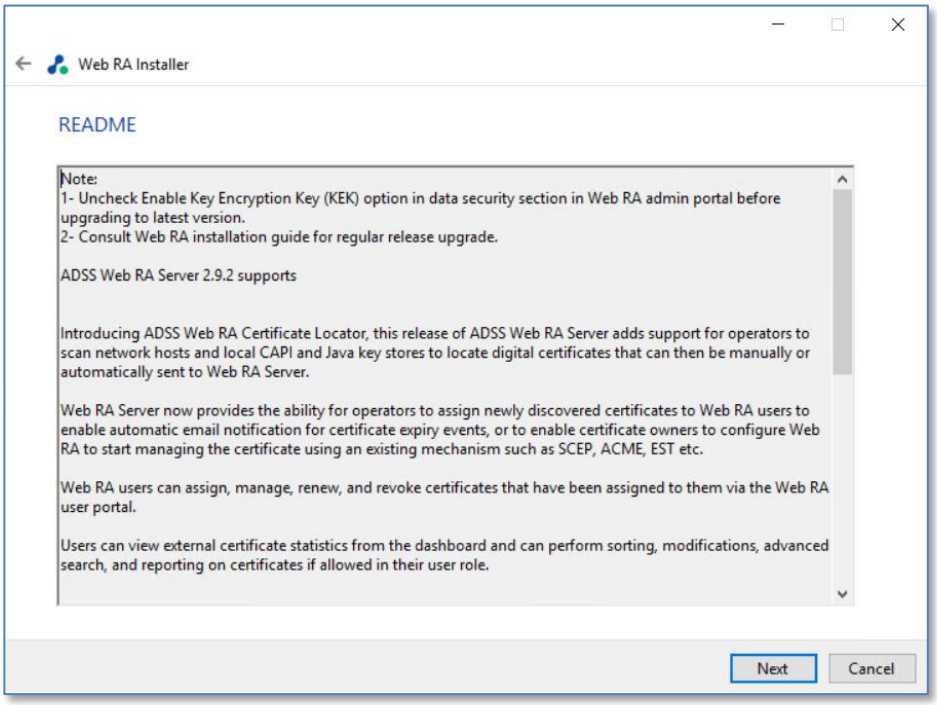


4.5.3. Click the **Next** button to view and accept the **License Agreement**.

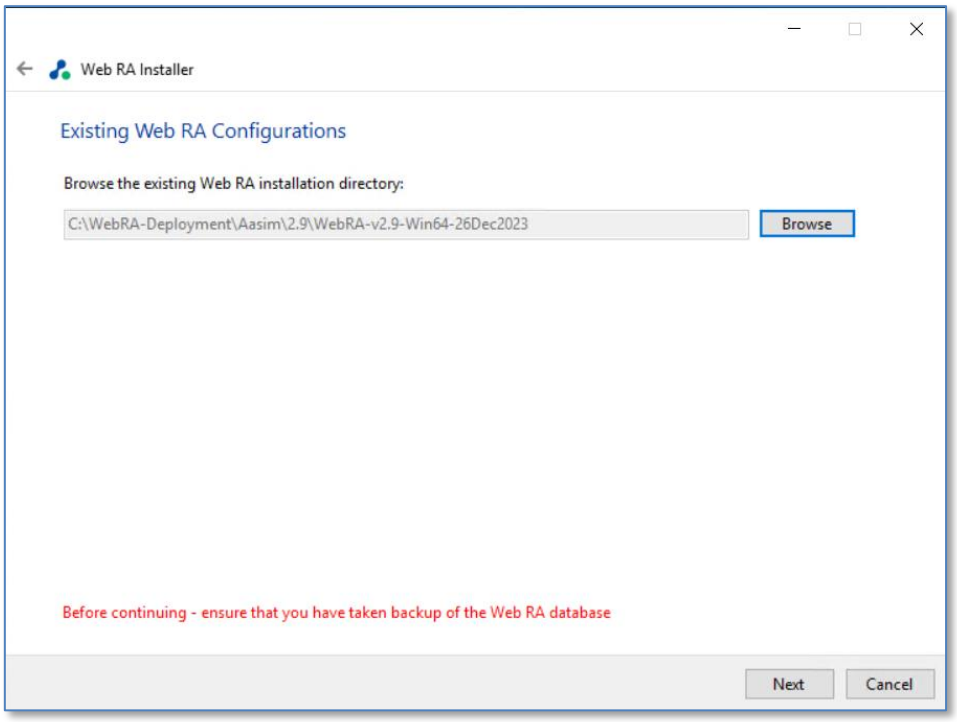


4.5.4. Click the **I Agree** button to proceed

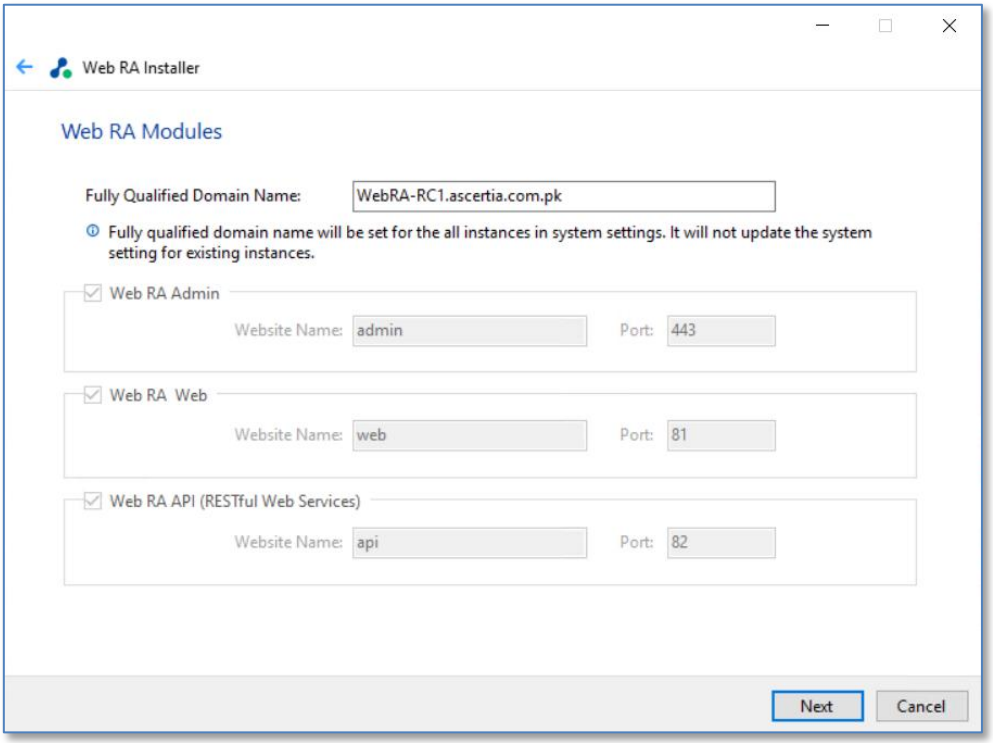
4.5.5. The next appearing screen will be for Readme text. This includes all features of current version. Click **Next** to proceed.



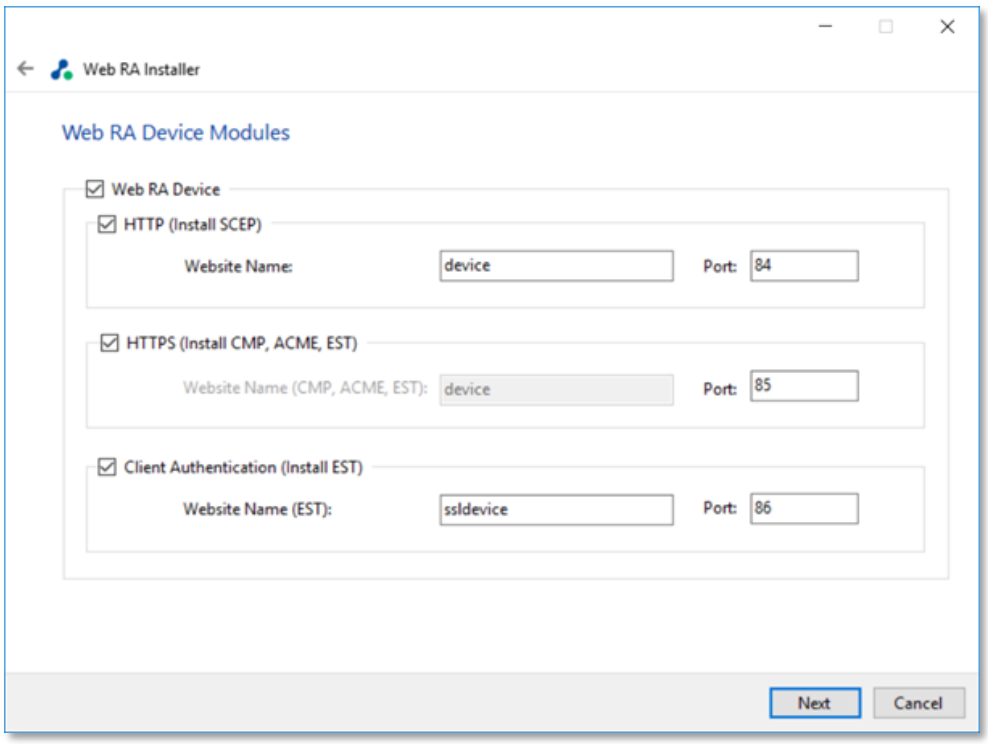
4.5.6. Click **Browse** and define the path to the existing ADSS Web RA installation base directory.



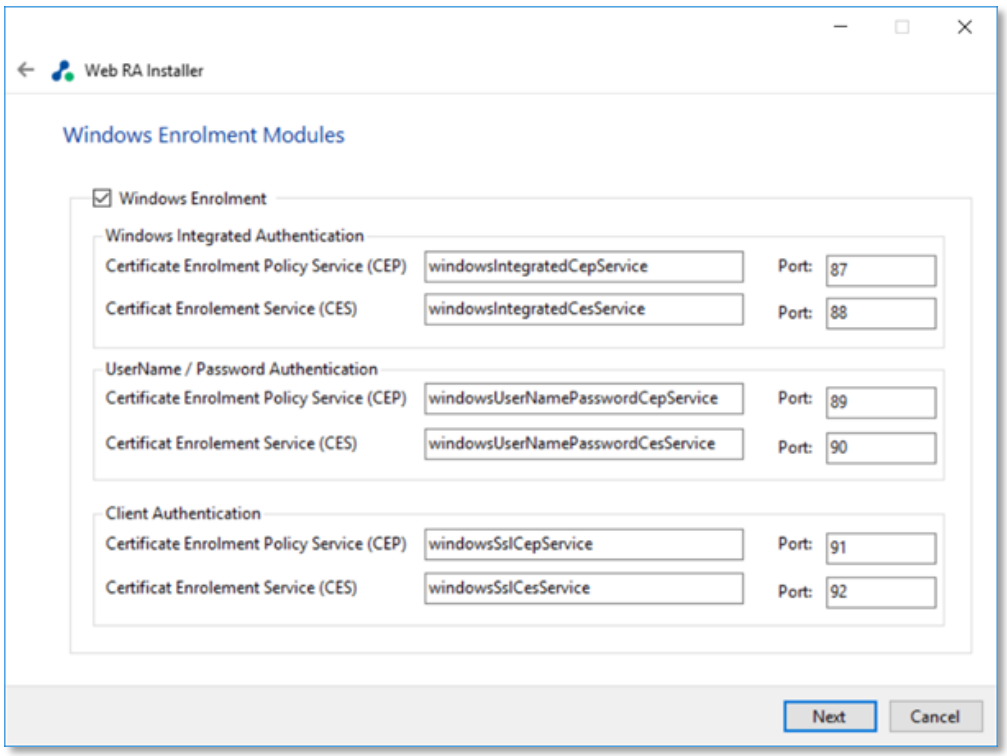
4.5.7. Click the **Next** button to select **Web RA Modules**. The already installed modules will be look like disabled fields e.g. Admin, Web and API modules are already installed.



4.5.8. Click **Next** and Select **Device Modules** to install the required features if not installed already. For each selected application, provide the web application name and port. The modules which are not previously installed will look like editable fields. Click **Next** to proceed.

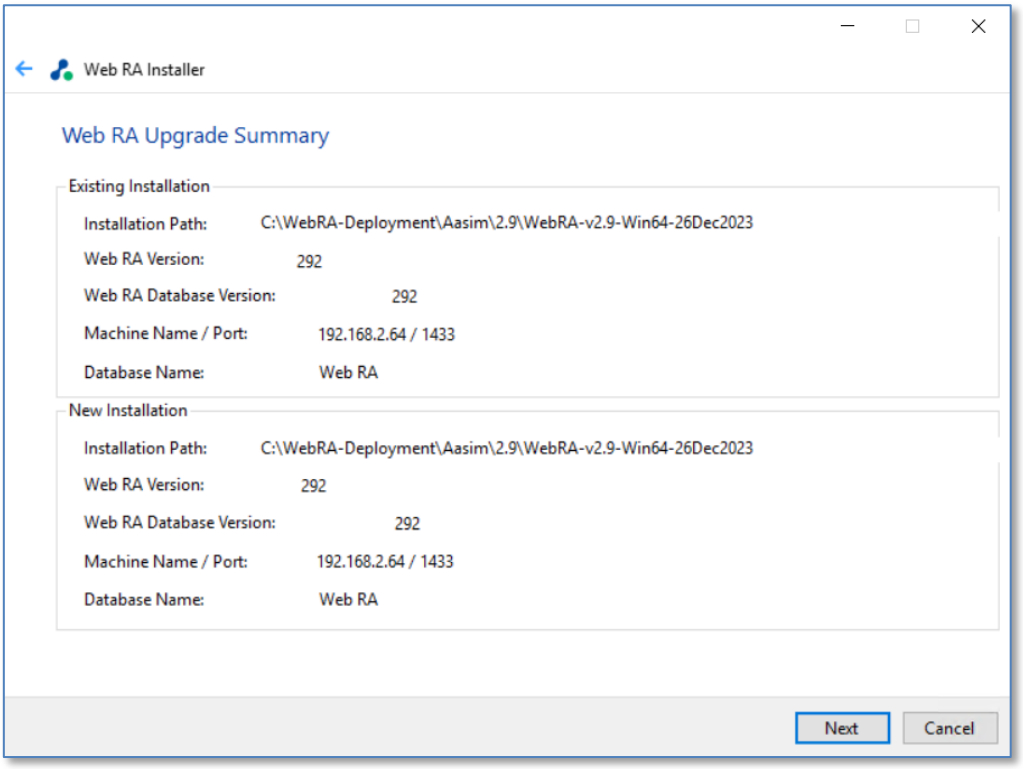


4.5.9. Select **Windows Enrolment** if not already installed. For each selected application, provide the web application name and port. Then click **Next**.

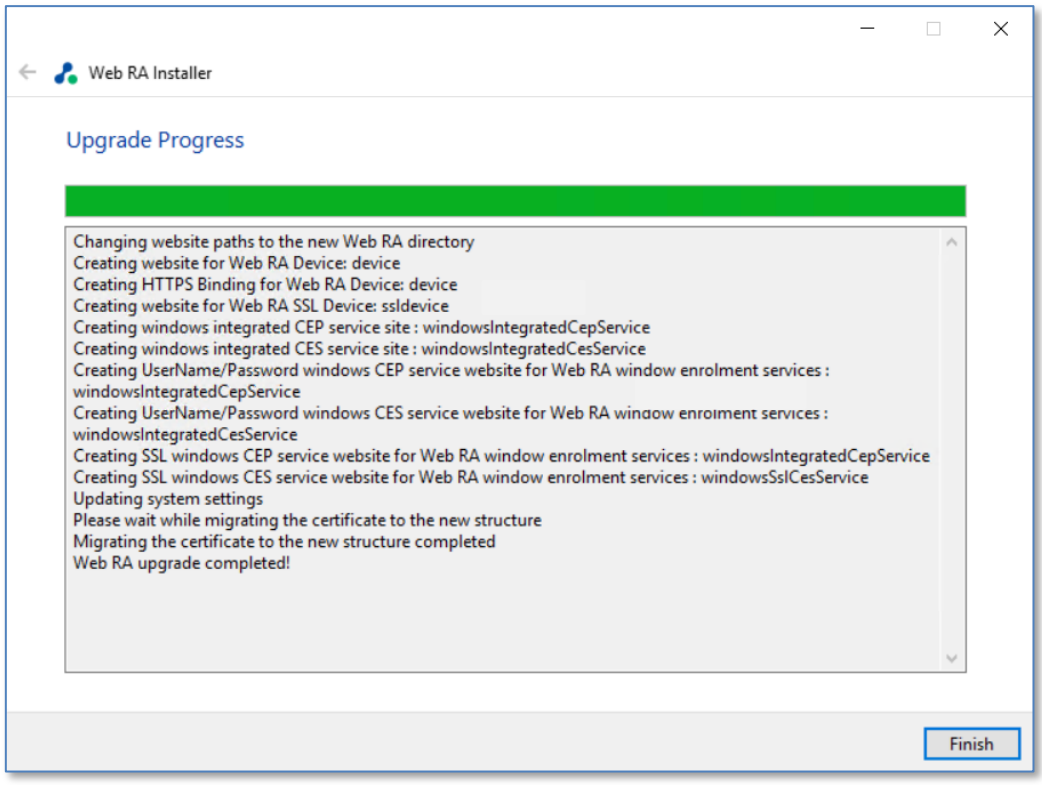


This screen shows a list of all ADSS **Web RA modules**. Components that are already installed are displayed but **greyed** out, while any ADSS Web RA module(s) that have not been installed previously can be selected for installation during the upgrade.

4.5.10. Click the **Next** button to see the **Upgrade Summary**.



4.5.11. Click the **Next** button to start the upgrade progress.



4.5.12. Click the **Finish** button to complete the ADSS Web RA upgrade process. Newly added modules will be deployed in IIS.

It is recommended to restart IIS after upgrade installation of ADSS Web RA.

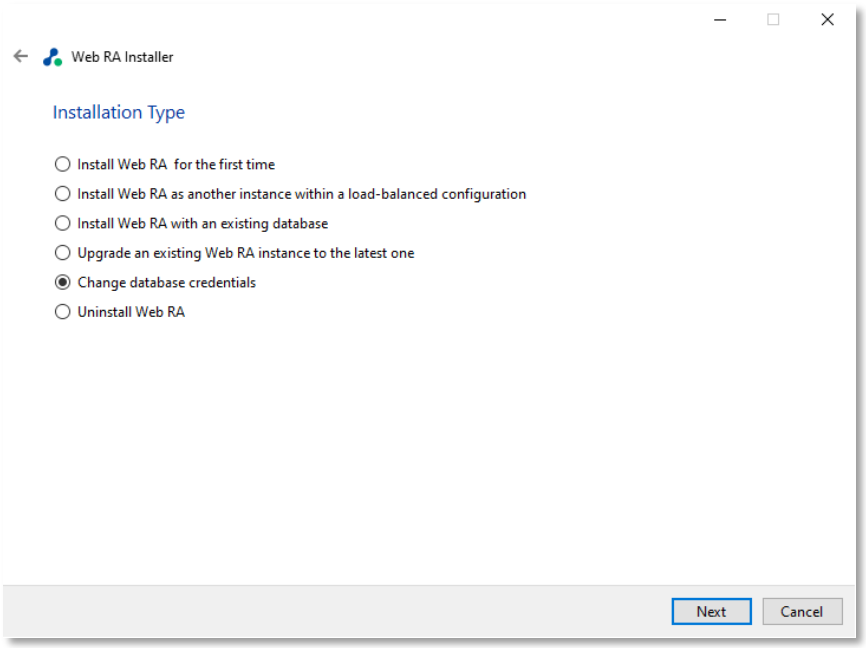
4.6 Changing Database Credentials for an Existing Installation

Database credentials stored by ADSS Web RA are encrypted for security purpose. If you need to make changes in your database server configurations, then these changes must be reflected in the ADSS Web RA installation for the signing operations to continue.

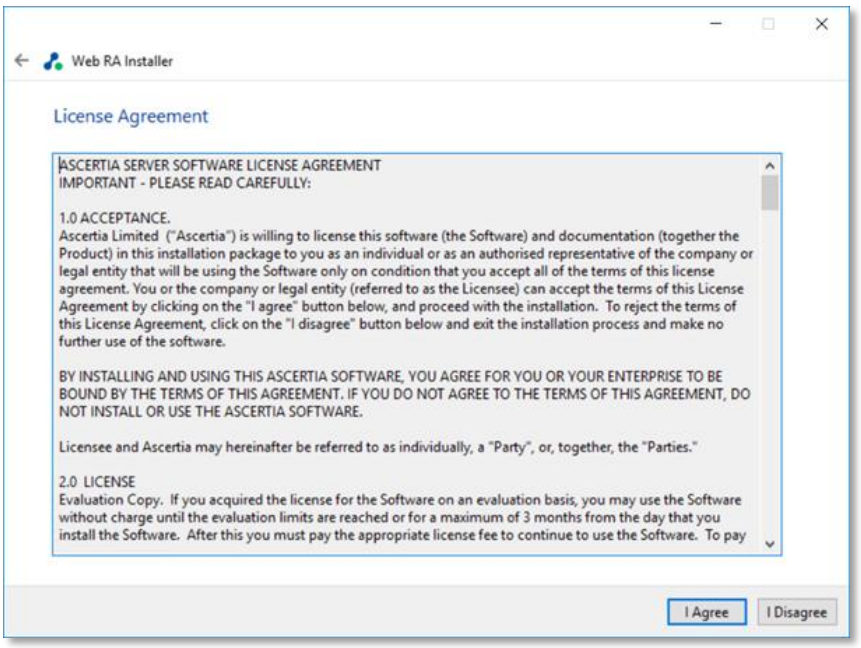
ADSS Web RA provides an option through the installer to update the following types of database related information:

- **Database username** and **password.**
- **Database name** and/or **server** (in case if database is restored from production database otherwise you need to install with existing database option).
- **Authentication types** (from SQL Server to Windows authentication and vice versa)

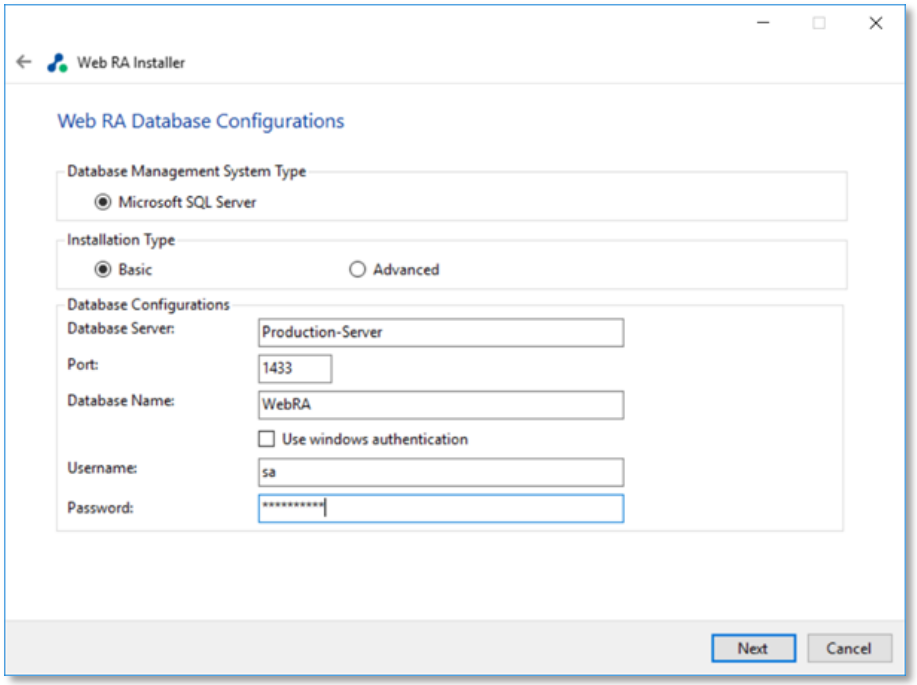
4.6.1. Follow the installation wizard, and select the **"Change database credentials"** option, when the **Installation Type** screen is shown:



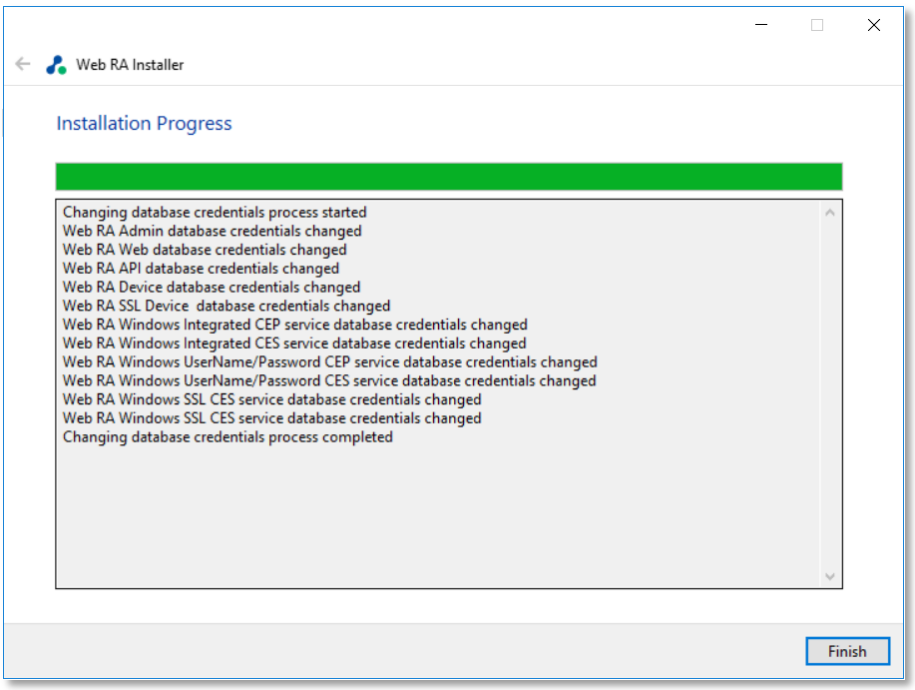
4.6.1. Click the **Next** button to show the **License Agreement**.



4.6.1. Click the **I Agree** button to proceed. The following screen for **Database Configurations** will be displayed.



4.6.1. Click the **Next** button to update the database configurations.



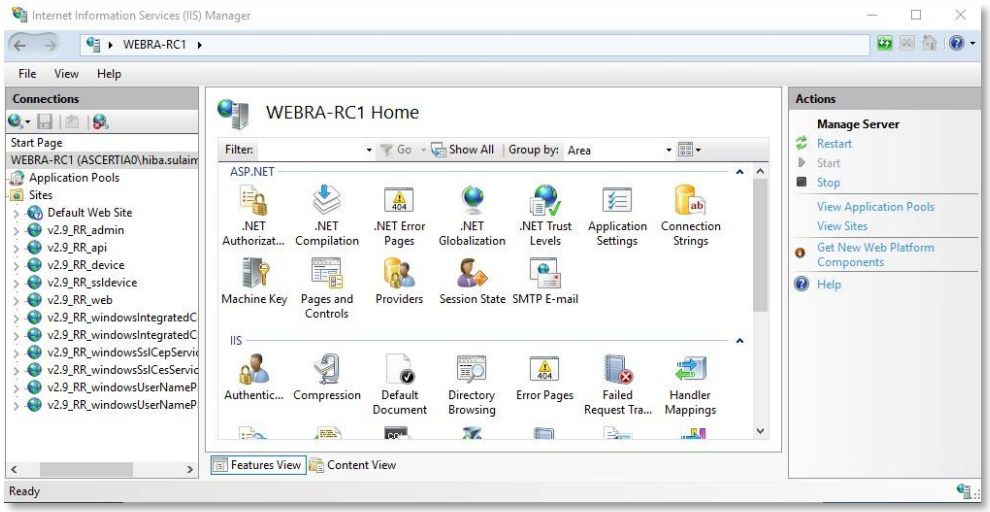
4.6.1. Click the **Finish** button to update the database configurations.

4.7 Regular Release Installation

Note: *If you are upgrading from v2.9 to v2.9.6, ensure that your v2.9 deployment is functioning properly by accessing it in a browser.*

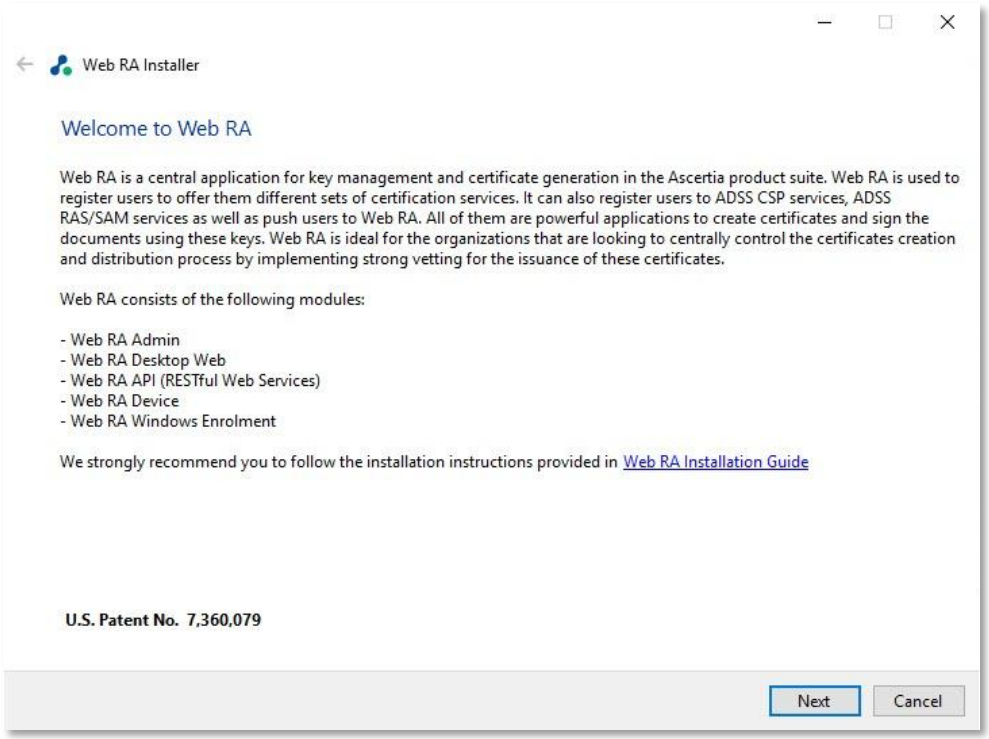
Follow the instructions below to install ADSS Web RA's regular release. Before starting the installation make sure that you have taken a backup of the Web RA database and have stopped the IIS Server.

To stop the IIS Server, launch the IIS Server and click Stop under the Manage Server action.

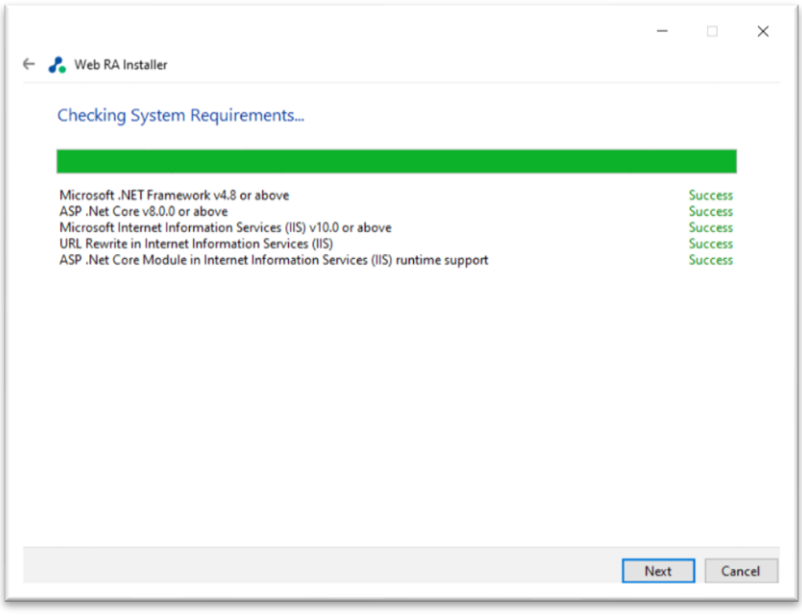


4.7.1 Launch the installer by right-clicking the file name [Web RA Regular Release Installation Directory]/setup/install.bat and select Run as administrator. Follow the installation wizard as described below:

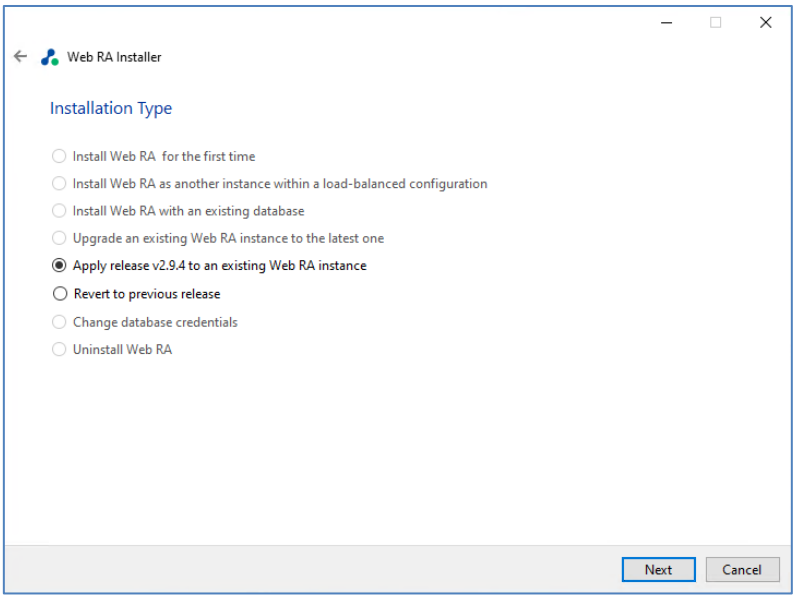
The Welcome screen will appear:



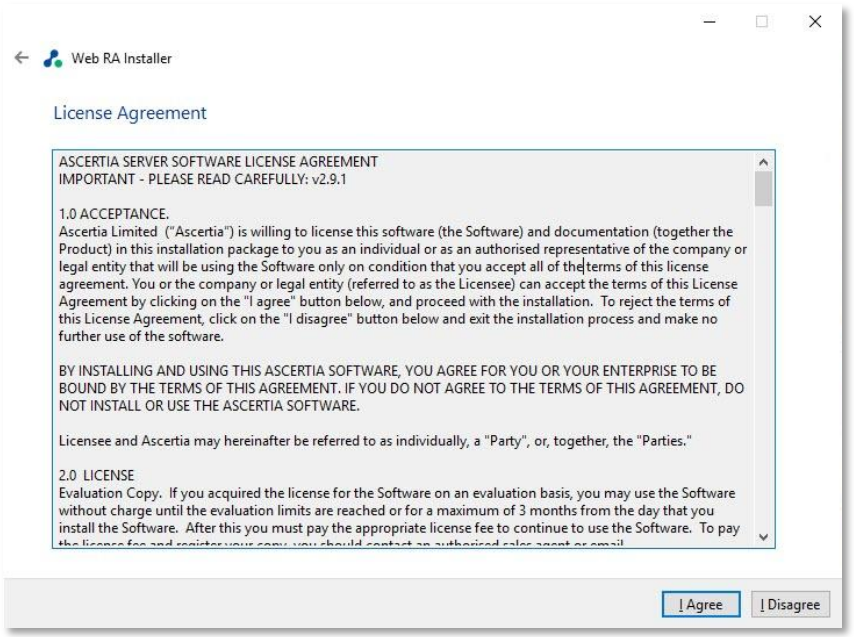
4.7.2 Click the Next button to continue. The system requirements screen will appear next to validate if all the required prerequisites are installed.



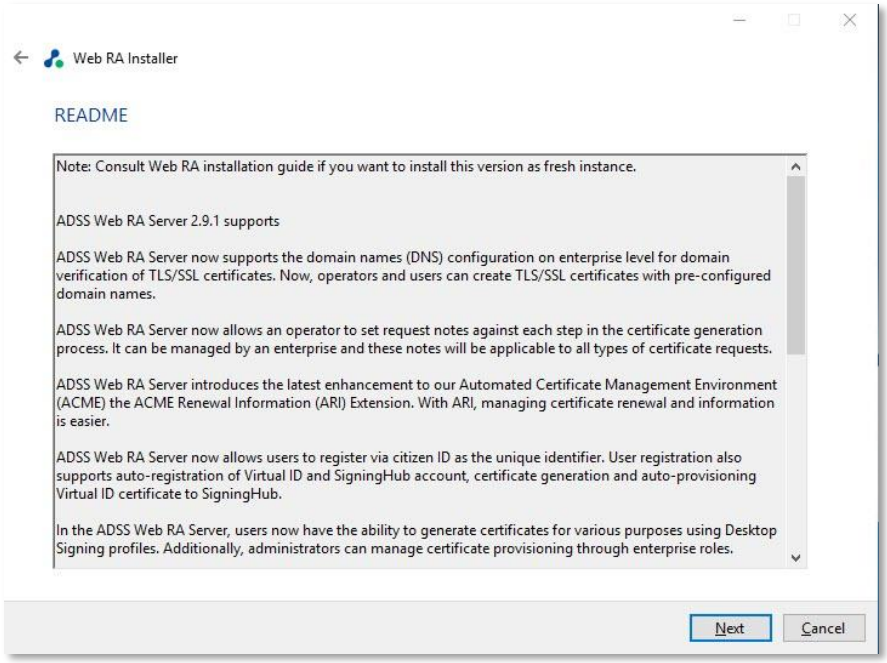
4.7.3 Click the Next button to show the Installation Type.



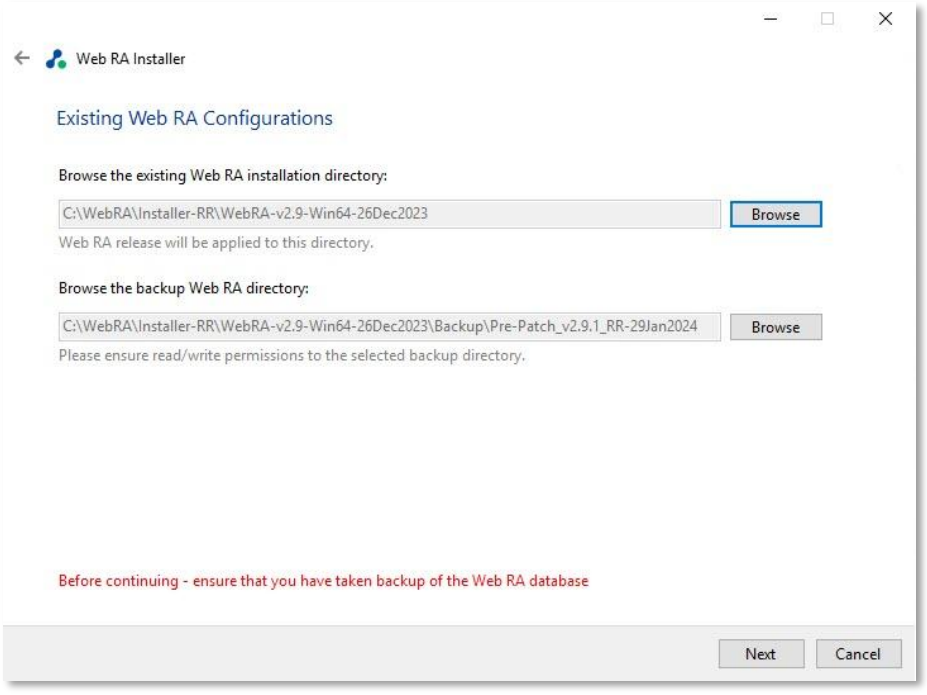
4.7.4 Click Next button to view and accept the License Agreement.



4.7.5 Click the I Agree button to proceed to the Read Me.

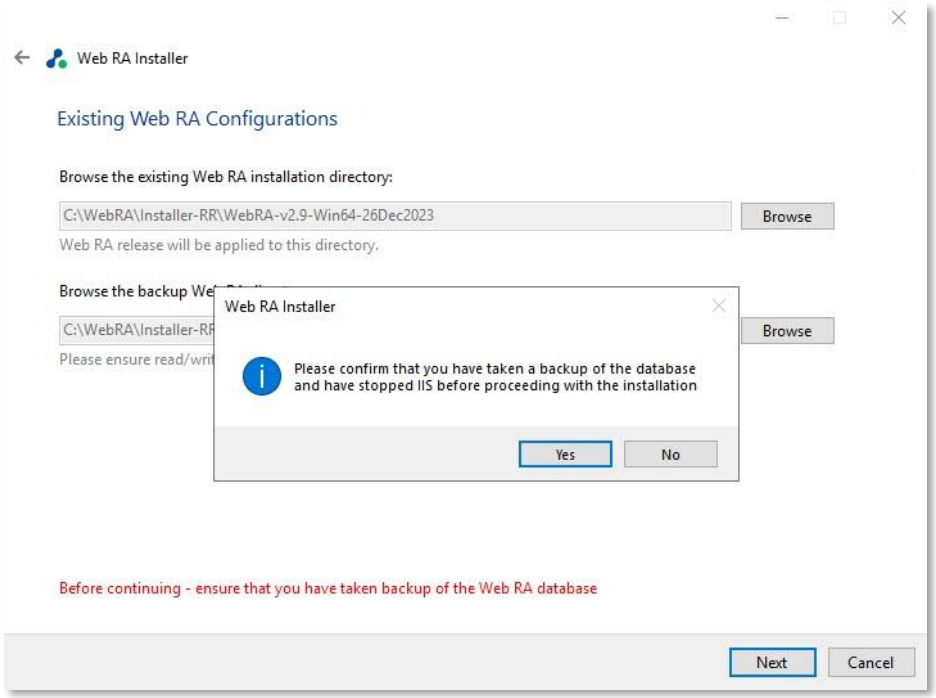


4.7.6 Click the Next button to provide the existing Web RA directory addresses:

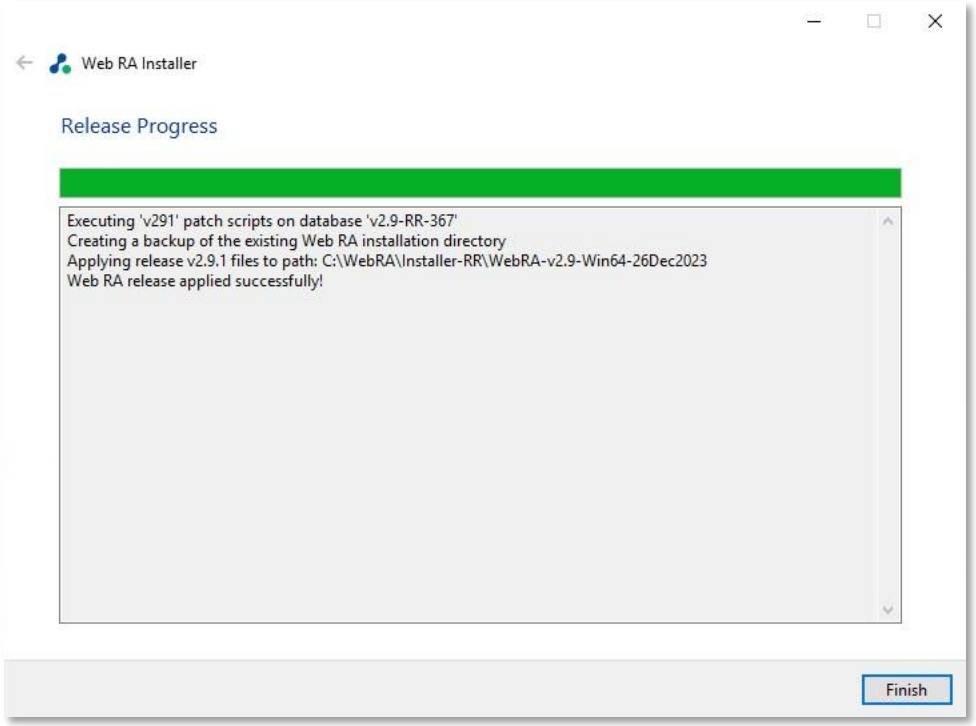


Click the Browse button against the existing Web RA installation directory.
Then click the Browse button against the backup Web RA directory, to browse to the addresses for the respective directories:
By default, when the existing Web RA installation directory address is selected, the installer will automatically create a backup Web RA folder and select it as backup directory. However, if the user wants to change the backup directory, they can click "Browse" and manually select the backup directory.

Click the Yes button to confirm that you have taken a backup of the database and have stopped the IIS before proceeding with the installation:

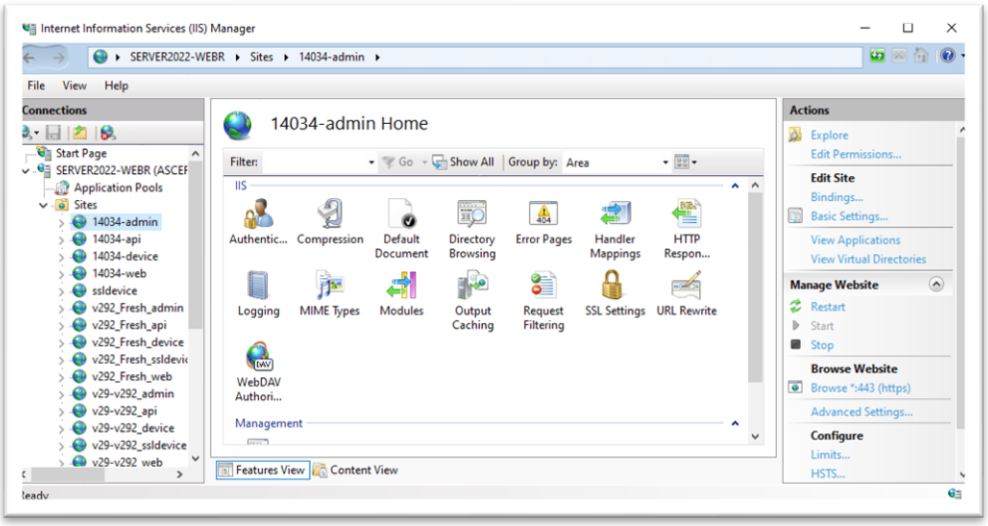


4.7.7 Click the Finish button to complete the installation process.



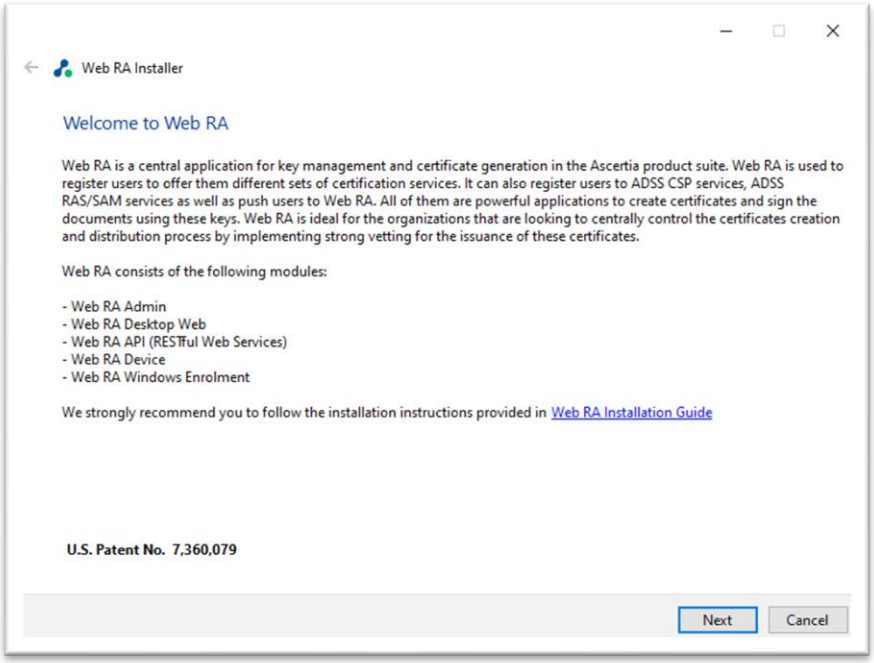
4.8 Uninstalling Regular Release

Follow the instructions below to uninstall ADSS Web RA's regular release. Before starting the uninstallation make sure that you have taken a backup of the Web RA database and have stopped the IIS Server.
To stop the IIS Server, launch the IIS Server and click Stop under the Manage Server action.

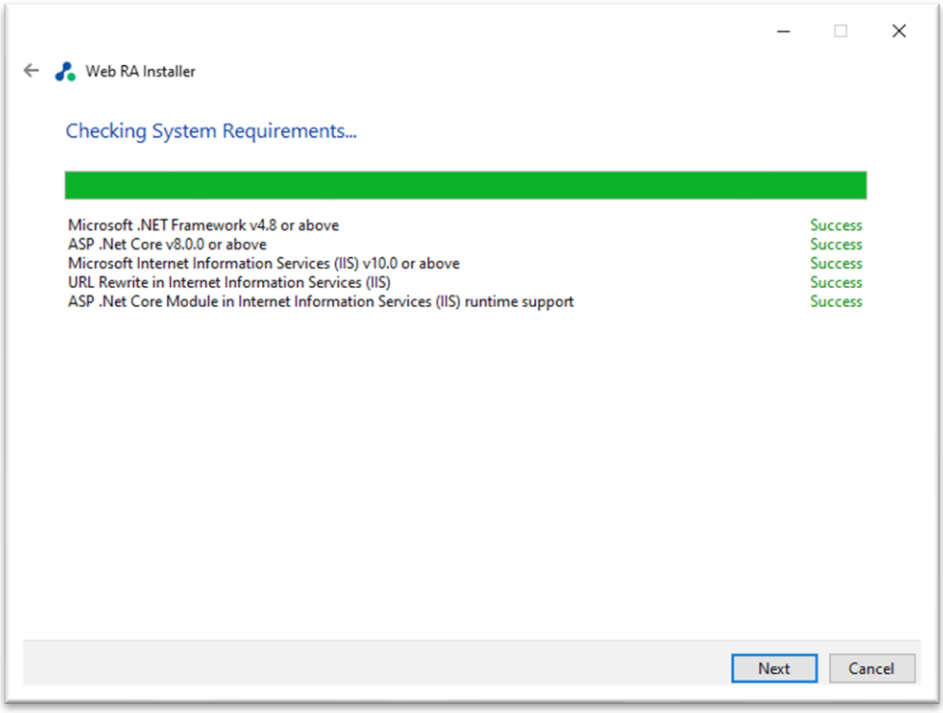


4.8.1 Launch the installer by right-clicking the file name [Web RA Regular Release Installation Directory]/setup/install.bat and select Run as administrator. Follow the installation wizard as described below:

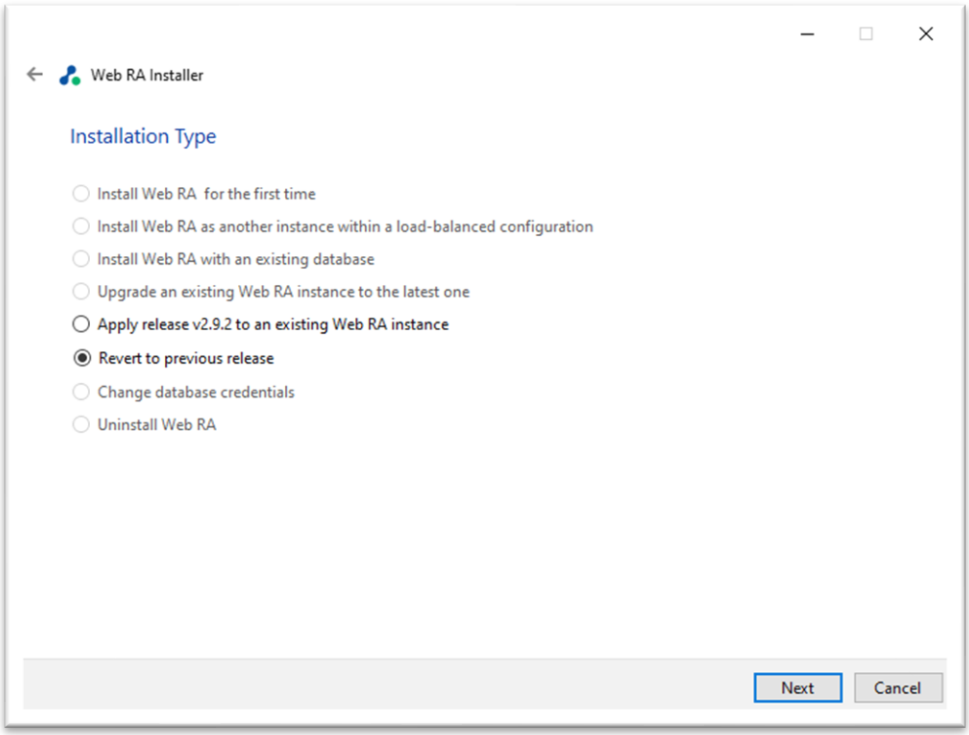
The Welcome screen will appear:



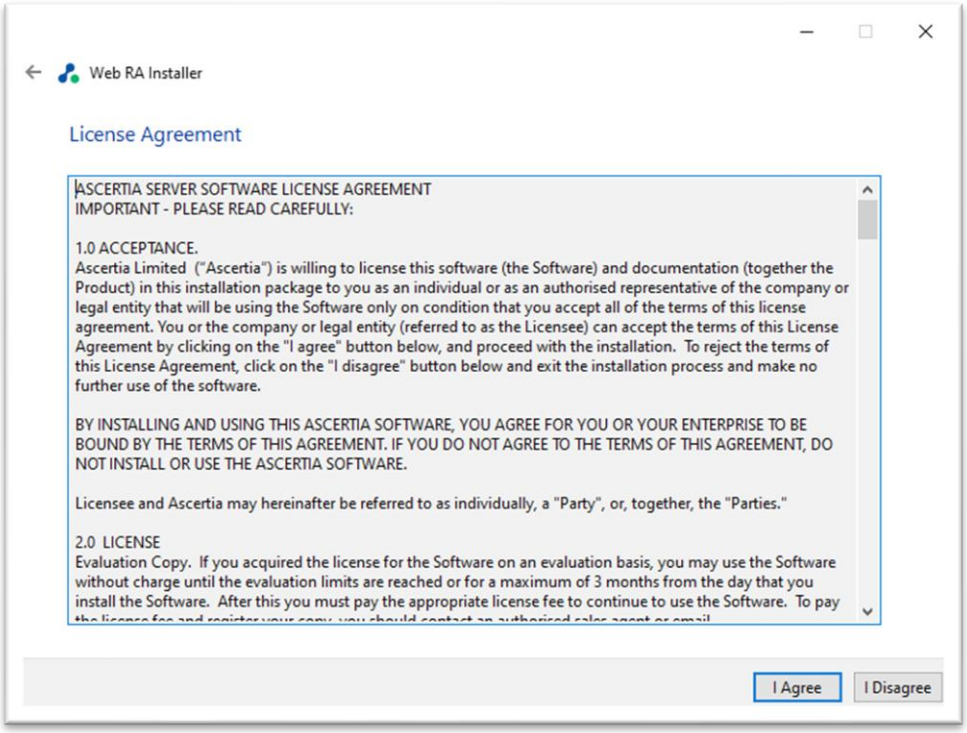
4.8.2 Click the Next button to continue. The system requirements screen will appear next to validate if all the required prerequisites are installed.



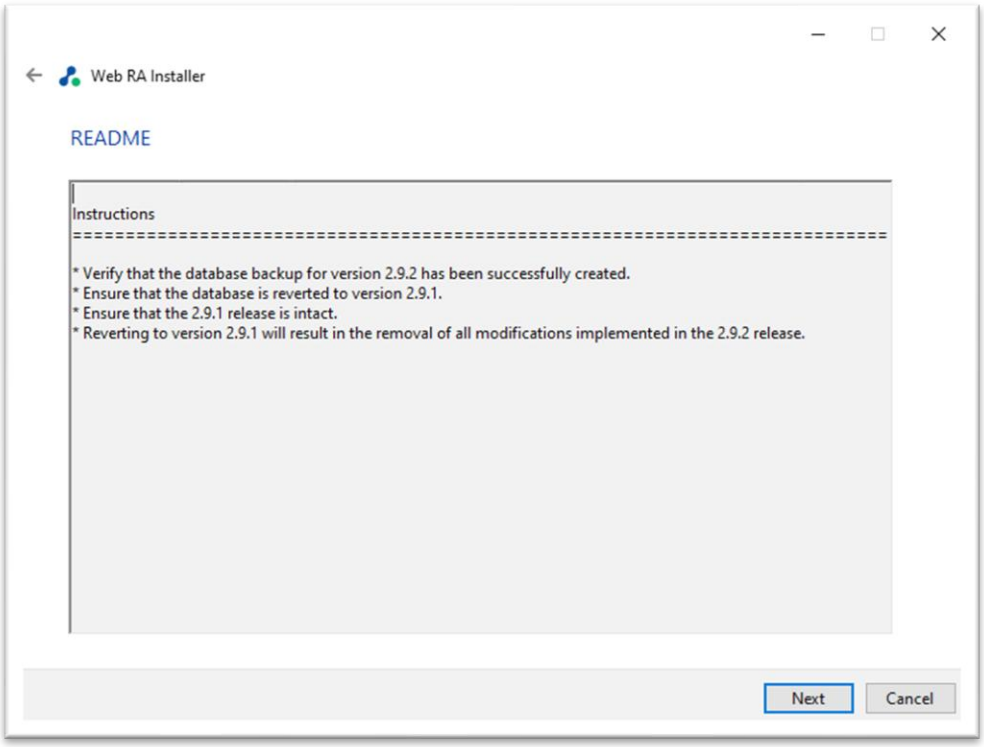
4.8.3 Click the Next button to show the Revert option.



4.8.4 Click Next button to view and accept the License Agreement.

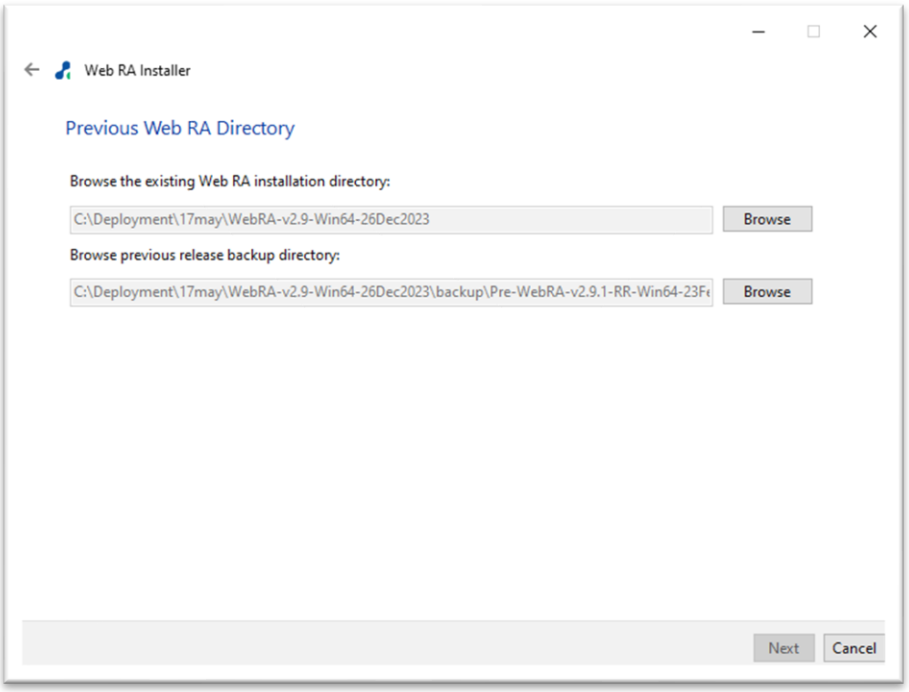


4.8.5 Click the I Agree button to proceed to the Read Me.

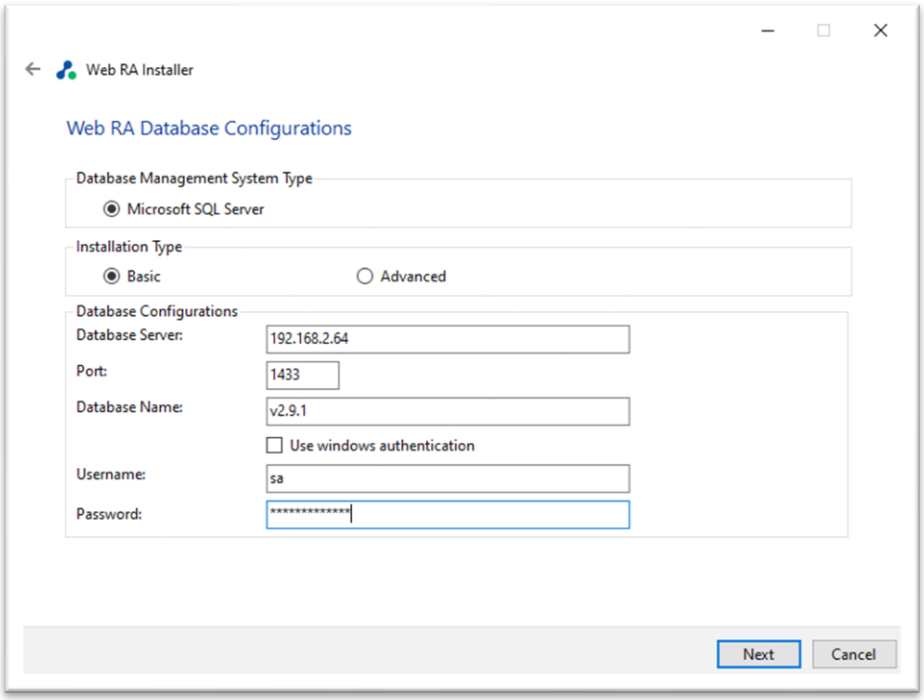


4.8.6 Click the Next button to provide:

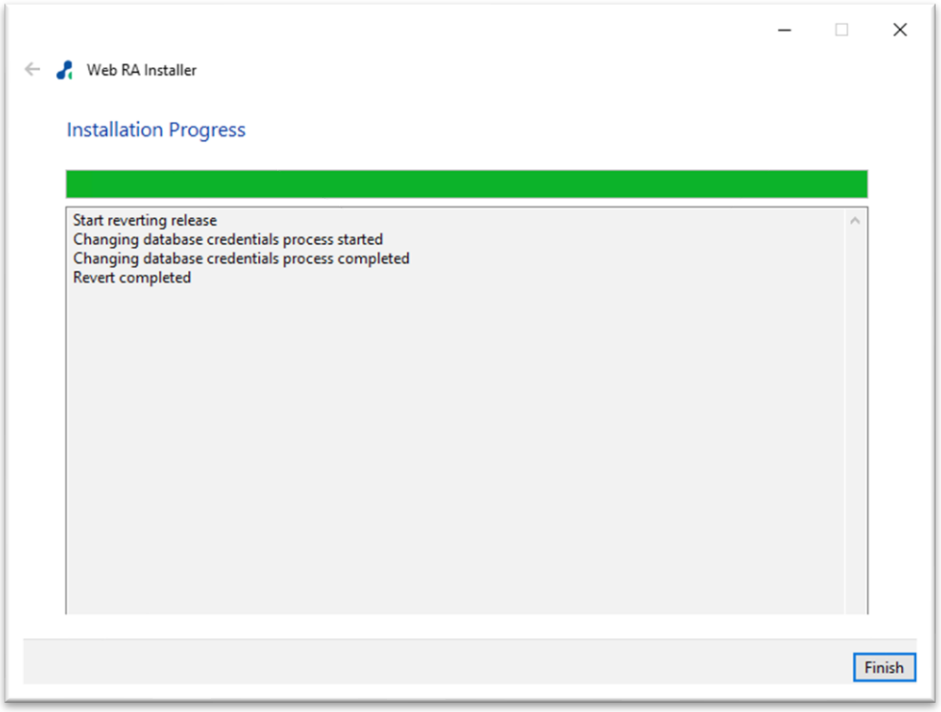
1. Browse the existing Web RA installation directory
2. Previous release backup directory will be set automatically. You also have the option to browse and select your own path.



4.8.7 Click next to view database details:



4.8.8 Click the Finish button to complete the installation process.

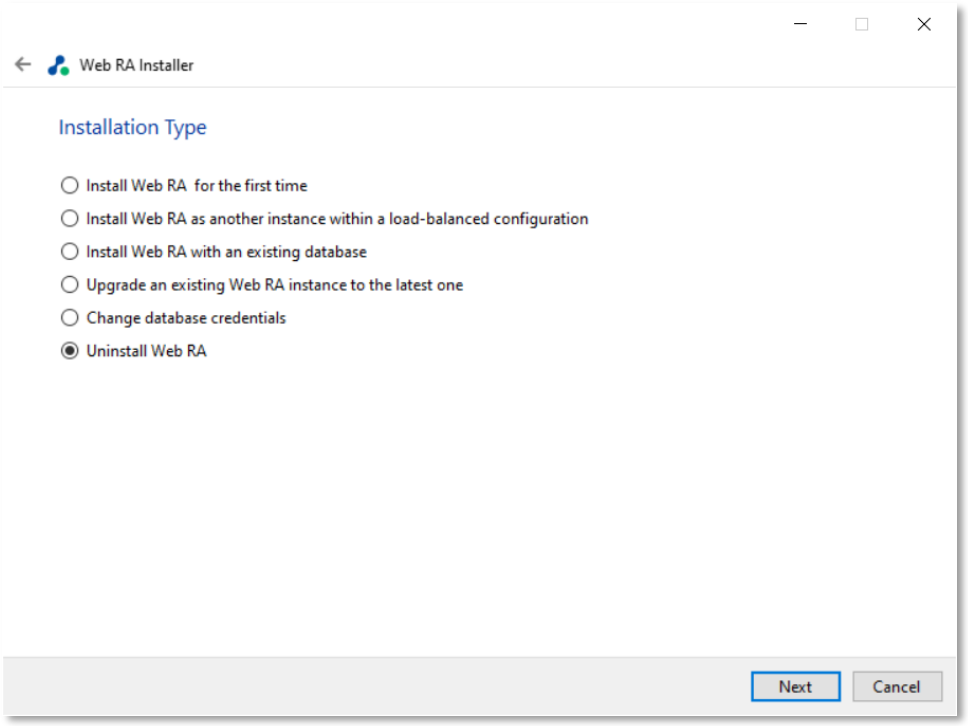


4.9 ADSS Web RA Uninstallation

Though we will not be pleased to let you go, but sometimes we have to say goodbye. You may uninstall ADSS Web RA Installer anytime.

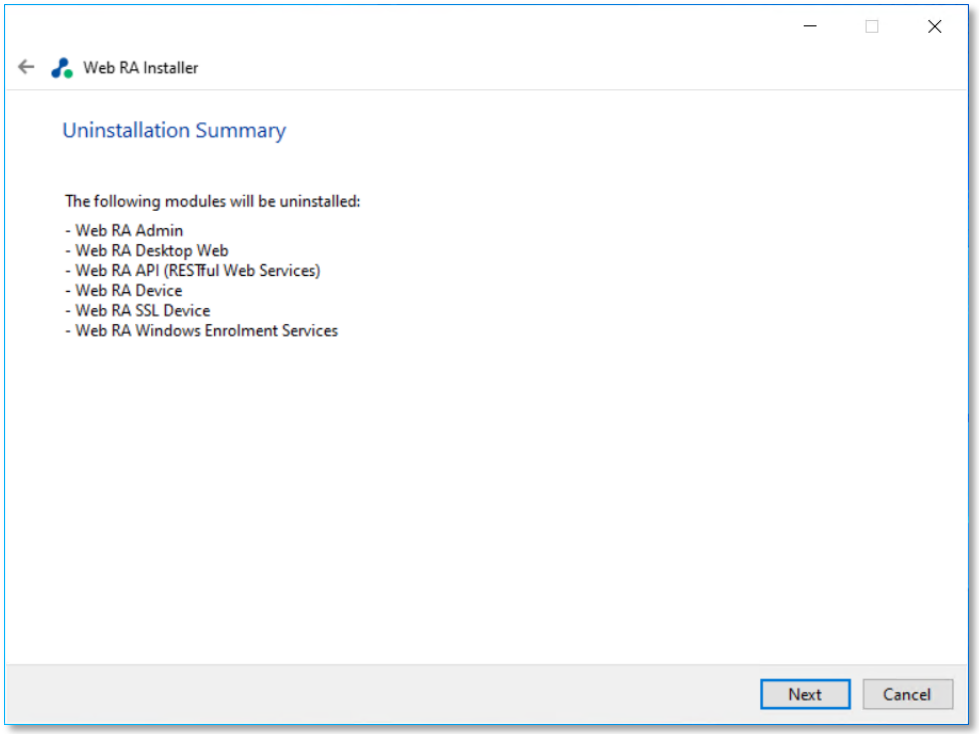
4.9.1 Right-click on the [ADSS Web RA Directory]/setup/install file and click Run as administrator.

4.9.2 Follow the installation wizard until the Installation Type screen is shown.

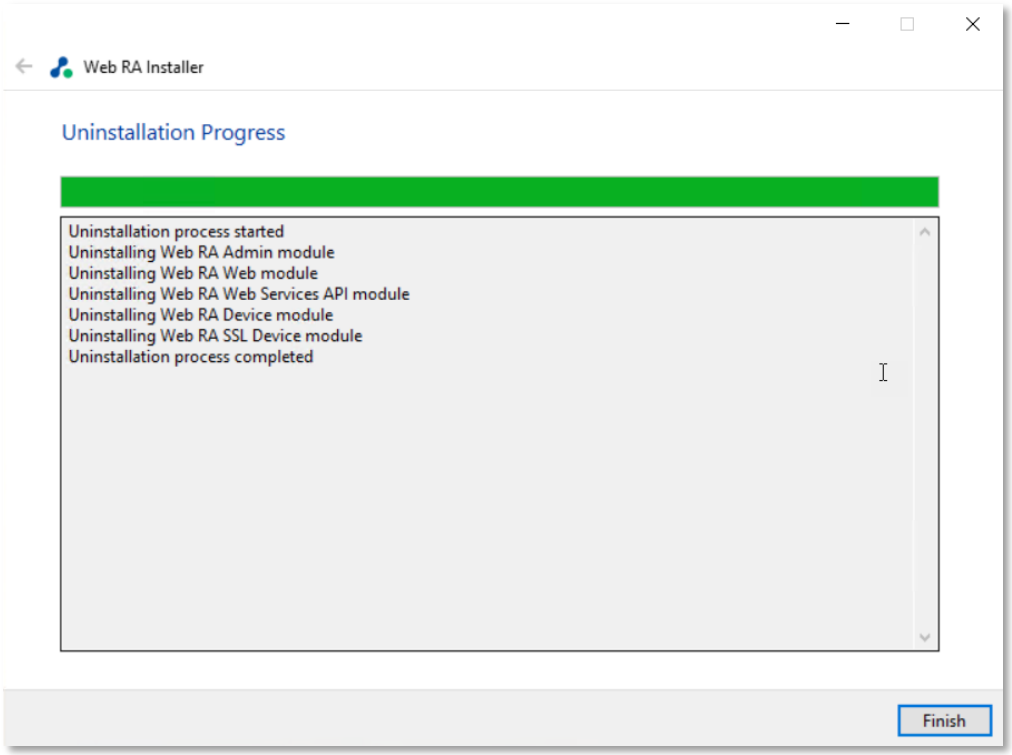


Select "**Uninstall Web RA**" to remove all websites from IIS mapped and this directory.

4.9.3 Click the Next button to proceed further. The following screen is shown.



4.9.4 Click the Next button to proceed with the uninstallation process.



4.9.5 Click the Finish button to complete the process.

This procedure does not remove the system database and its respective contents. You need to remove database manually.

5 ADSS Web RA Installation on Linux System

5.1 Prerequisites for Linux Installation

5.1.1 Install and Setup .Net Runtime 9

Source: Install .NET on RHEL and CentOS Stream - .NET | Microsoft Learn

The ASP.NET Core Runtime allows you to run .Net applications that do not include the runtime. The following command installs the ASP.NET Core Runtime, which is the most compatible runtime for .NET.

Installation

In your terminal, run the following command:

```
Bash: sudo dnf install aspnetcore-runtime-9.0
```

Verify Installation by running the following command:

```
Bash: dotnet --info
```

5.1.2 Install and Setup MSSQL Server 2022

Source: RHEL: Install SQL Server on Linux - SQL Server | Microsoft Learn

Install SQL Server (RHEL: Install SQL Server on Linux - SQL Server | Microsoft Learn)

To configure SQL Server on RHEL 9, run the following commands in the terminal to install the mssql-server package:

```
Bash: sudo curl -o /etc/yum.repos.d/mssql-server.repo
https://packages.microsoft.com/config/rhel/9/mssql-server-2022.repo
```

Download the SQL Server 2022 (16.x) Red Hat 9 repository configuration file:

```
Bash: sudo curl -o /etc/yum.repos.d/mssql-server.repo
https://packages.microsoft.com/config/rhel/9/mssql-server-2022.repo
```

- Run the following command to install SQL Server:

  ```
  Bash: sudo yum install -y mssql-server
  ```

- After the package installation is complete, run mssql-conf setup using its full path and follow the prompts to set the SA password and select your edition. The following SQL Server editions are available under a free license: Evaluation, Developer, and Express.

  ```
  Bash: sudo /opt/mssql/bin/mssql-conf setup
  ```

- Once the configuration is complete, verify that the service is running:

  ```
  Bash: systemctl status mssql-server
  ```

- To allow remote connections, open the SQL Server port on the RHEL firewall. The default SQL Server port is TCP 1433. If you're using FirewallD for your firewall, you can use the following commands:

```
Bash: sudo firewall-cmd --zone=public --add-port=1433/tcp --permanent

Bash:  sudo firewall-cmd –reload
```

At this point, the SQL Server is running on your RHEL machine and is ready for use!

5.1.3 Install and Setup Nginx

Source: nginx: Linux packages

- First, start by ensuring your system is up-to-date.

```
Bash: sudo dnf clean all
Bash: sudo dnf update
Bash: sudo dnf groupinstall "Development Tools"
```

- **Installing Nginx on AlmaLinux 9.**

By default, Nginx is available on the AlmaLinux 9 base repository. Simply install the Nginx package by using the dnf command:

```
Bash: sudo dnf install nginx
```

- After the installation is complete, start the service of the Nginx server. Then, enable it so that it starts itself automatically with the system reboot:

```
Bash: sudo systemctl restart nginx
Bash: sudo systemctl status nginx
Bash: sudo systemctl enable nginx
```

- Configure Firewall.

```
Bash: sudo firewall-cmd --permanent --add-service=http
Bash: sudo firewall-cmd --permanent --add-service=https
Bash: sudo firewall-cmd --reload
```

- Accessing Nginx Web Interface

ⓘ Once the installation is successful, verify that the webserver is running and accessible by entering your server's IP address in a browser: http://your-server-ip-address. If you see this page, it means that your Nginx web server is correctly installed and is running on AlmaLinux 9.

5.2 Pre-Installation Steps

5.2.1 Access the Root Directory

On a Linux machine, the **root directory** (/) is the highest-level directory that contains all system files and user directories.

5.2.2 Locate the `/var` Folder

- The /var directory is used to store variable data such as logs, cache, and web files.
- Navigate to this directory inside the root folder (/var).

5.2.3 Check for the `www` Folder

- Inside /var, check for the **www** folder.
- Some Linux distributions automatically create this folder, but in some cases, you might need to create it manually.

If the www folder is not present:

- Create a new www folder inside /var.
- Ensure appropriate permissions are set so that the installation can proceed without issues.

5.2.4 Place the Installation Package

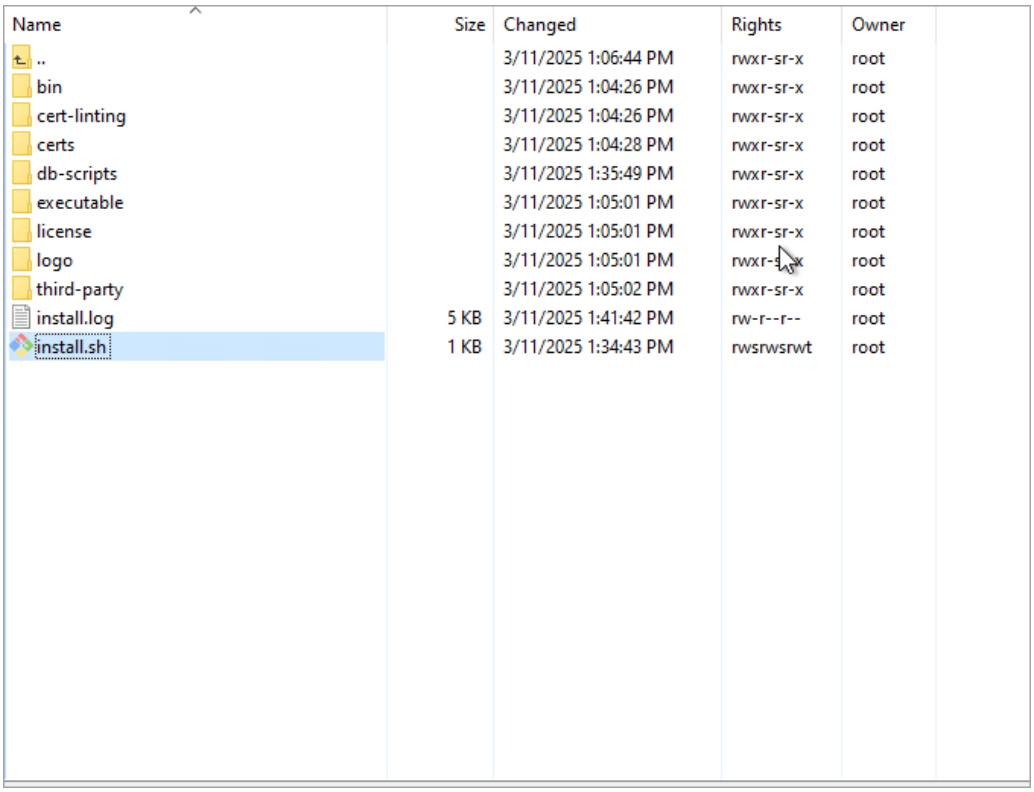
- Copy the extracted WebRA installation package into the /var/www/ directory.

5.2.5 Access the Installation Folder

- In the extracted package, navigate to the LinuxFresh folder.
- Then, go to **/var/www/LinuxFresh/setup/bin/** to access the install.json file.
- Each parameter in the install.json file must be correctly configured before proceeding with the installation.

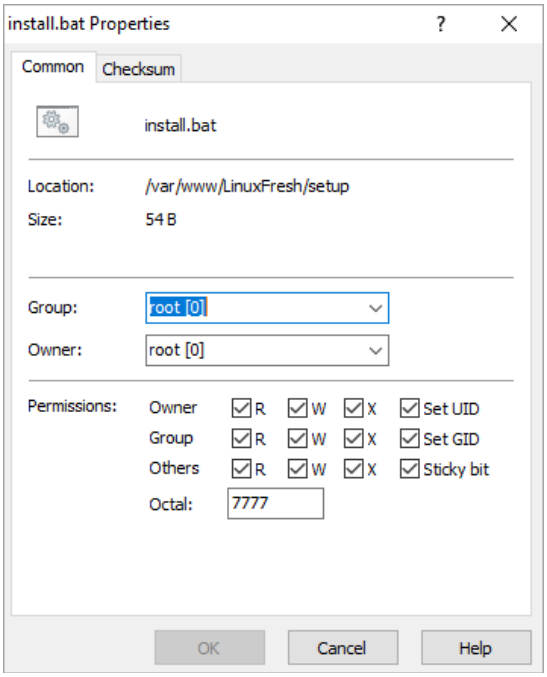
5.2.6 Set Execution Permissions for the Installation Script

Before starting the installation, the install.sh file must have execution permissions enabled.



To grant execution permissions:

- Locate the install.sh file inside **/var/www/LinuxFresh/setup/**.
- Right-click the file and select Properties.
- Go to the Permissions section.
- Grant permissions and click Ok.



5.3 Configuring Installation Parameters in install.json file

The install.json file contains all the required settings for the WebRA installation. The operator must define these configurations correctly before proceeding with the installation. The installation process reads this file to determine how the setup should be performed.

Each parameter in install.json must be configured according to your system requirements. The following sections explain each parameter in detail:

5.3.1 Set Agreement Parameter

- The LicenseAgreement parameter must be set to true if you want to include an agreement confirmation step in the installation process. This confirms acceptance of Ascertia's licensing terms and conditions.
- Possible values: true or false.
- If set to false, the installation will proceed without an explicit agreement confirmation.

```
{
  "Agreement": {
    "LicenseAgreement": true,
    "comment": "possible values are TRUE/FALSE"
  },
```

5.3.2 Installation Modes

Defines the type of installation to be performed. Choosing the correct mode is essential for a successful setup.

Possible values:

- **FIRST_TIME**: A fresh installation of WebRA.
- **LOAD_BALANCE**: Adds a new WebRA node to an existing setup.
- **UPGRADE**: Upgrades an existing WebRA installation.
- **EXISTING_DATABASE**: Connects to an already configured database.
- **REGULAR_RELEASE**: Installs a regular update package.
- **UNINSTALL_REGULAR_RELEASE**: Removes a previously installed update.
- **CHANGE_DB_CREDENTIALS**: Updates database credentials.
- **UNINSTALL**: Completely removes WebRA and its configurations.

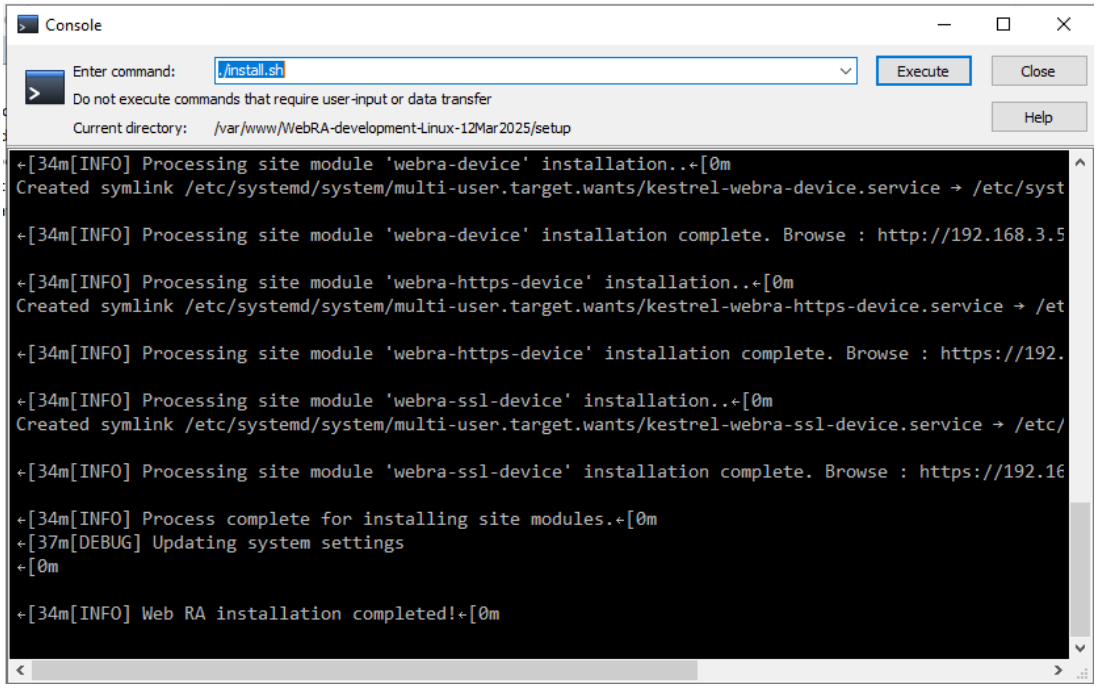
5.3.2.1 First Time Installation

When installing ADSS WebRA for the first time, set the “Type” value under “InstallationMode” to:

```
  },
  "InstallationMode": {
    "Type": "FIRST TIME",
    "comment": "possible values are
FIRST_TIME/LOAD_BALANCE/UPGRADE/EXISTING_DATABASE/REGULAR_RELEASE/UNINSTALL_REGULAR_RELEASE/CHANGE_DB_CREDENTIALS/UNINSTALL"
  },
```

After setting the Type, save the file and close it. Then navigate to **the /var/www/LinuxFresh/setup/** folder and run the install.sh script using the following command

```
sudo ./install.sh
```



Note: *For a FIRST_TIME installation, a new database is required. Ensure that no existing database is used to prevent conflicts with DB versions.*

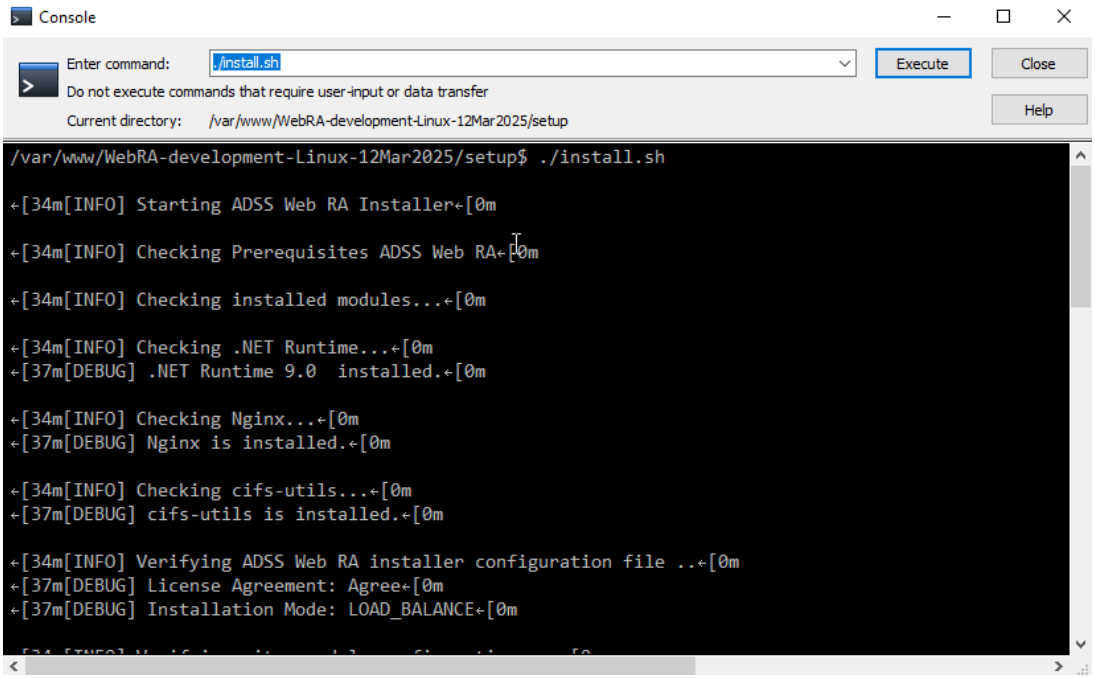
5.3.2.2 Installing in Load Balanced Mode

When installing ADSS WebRA in a load-balance environment, set the “Type” value under “InstallationMode” to:

```
  },
  "InstallationMode": {
    "Type": "LOAD_BALANCE",
    "comment": "possible values are
FIRST_TIME/LOAD_BALANCE/UPGRADE/EXISTING_DATABASE/REGULAR_RELEASE/UNINSTALL_REGULAR_RELEASE/CHANGE_DB_CREDENTIALS/UNINSTALL"
  },
```

After setting the Type, save the file and close it. Then navigate to **the /var/www/LinuxFresh/setup/** folder and run the **/install.sh** script using the following command:

```
sudo ./install.sh
```



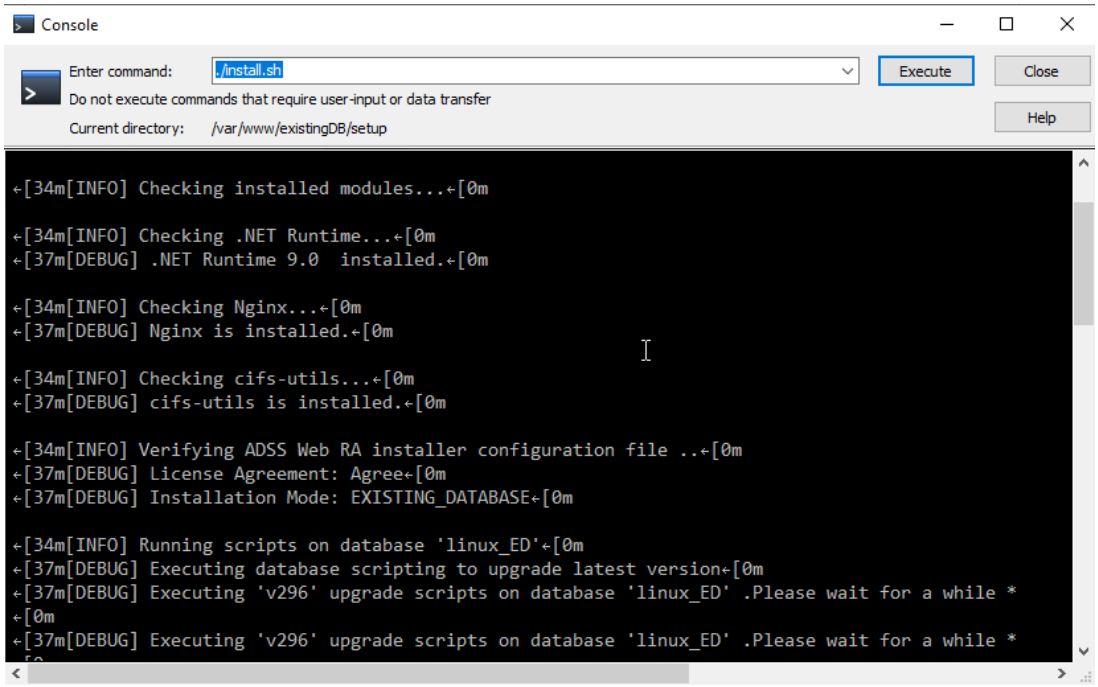
5.3.2.3 Installing WebRA with an Existing Database

To install WebRA while connecting it to an already configured database, set the Type value under “InstallationMode” to:

```
  },
  "InstallationMode": {
    "Type": "EXISTING_DATABASE",
    "comment": "possible values are
FIRST_TIME/LOAD_BALANCE/UPGRADE/EXISTING_DATABASE/REGULAR_RELEASE/UNINSTALL_REGULAR_RELEASE/CHANGE_DB_CREDENTIALS/UNINSTALL"
  },
```

After setting the Type, save the file and close it. Then navigate to **the /var/www/LinuxFresh/setup/** folder and run the **/install.sh** script using the following command:

```
sudo ./install.sh
```



5.3.2.4 Changing Database Credentials in WebRA

To update the database connection details without modifying other configurations, set the Type value under “InstallationMode” to "CHANGE_DB_CREDENTIALS", and update the following parameters under the Database Configuration section:

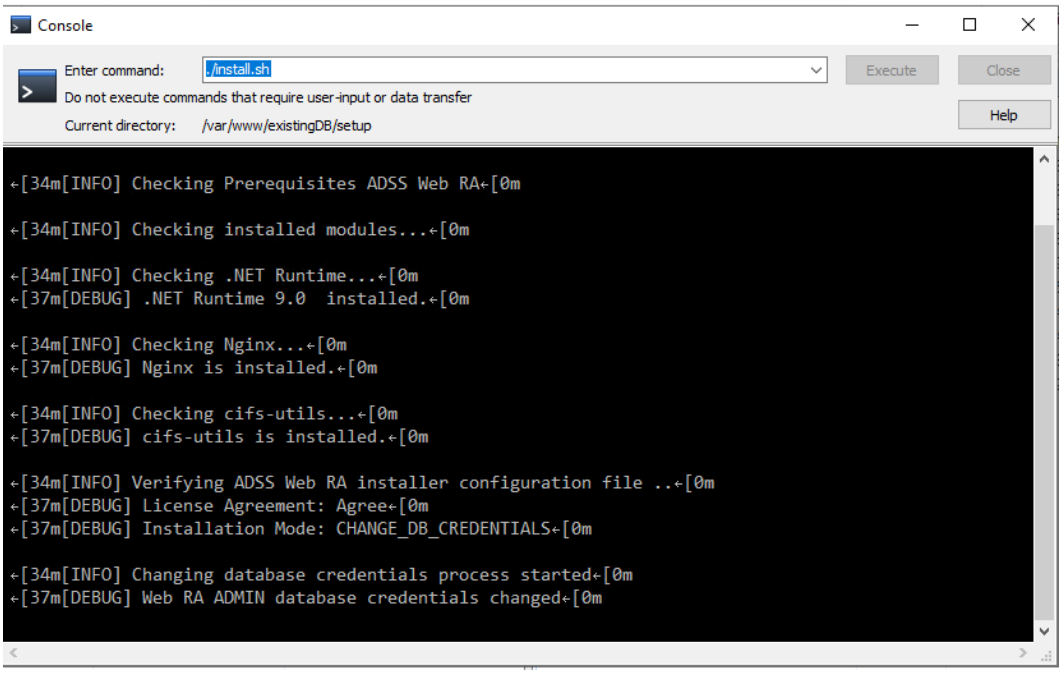
- DatabaseType
- MachineName
- Port
- Authentication
- UserId
- Password

Save and close the file install.json file after making the changes.

```
  },
  "InstallationMode": {
    "Type": "CHANGE_DB_CREDENTIALS",
    "comment": "possible values are
FIRST_TIME/LOAD_BALANCE/UPGRADE/EXISTING_DATABASE/REGULAR_RELEASE/UNINSTALL_REGULAR_RELEASE/CHANGE_DB_CREDENTIALS/UNINSTALL"
  },
  "ExistingInstallation": {
    "BackupDirectory": ""
  },
  "RegularInstallation": {
    "ExistingWebRAPath": "",
    "RegularBackupPath": ""
  },
  "SampleData": true,
  //"comment": "possible values are True or false",
  "DatabaseConfiguration": {
    "DatabaseType": "",
  //  "comment": "possible values are MSSQL",
    "ConfigurationType": {
      "Type": "",
      //"comment": "possible values are TYPICAL and ADVANCED",
      "TypicalDatabaseConfiguration": {
      "MachineName": "",
        "Port": "",
        "Authentication": "",
       //"comment": "possible Values are SERVER_AUTH, WINDOW_AUTH",
       "DatabaseName": "",
       "UserId": "",
       "Password": ""
      }
    },
    "AdvancedDatabaseConfiguration": {
```

Then navigate to **the /var/www/LinuxFresh/setup/** folder and run the **/install.sh** script using the following command:

```
sudo ./install.sh
```



5.3.3 Existing Installation Parameter

BackupDirectory: Specifies where to store backup files before upgrading or uninstalling WebRA. If left empty, no backup is created, which may lead to data loss.

```
  },
  "ExistingInstallation": {
    "BackupDirectory": ""
  },
  "RegularInstallation": {
    "ExistingWebRAPath": "",
    "RegularBackupPath": ""
```

5.3.4 Regular Installation Parameter

- **ExistingWebRAPath**: Specifies the file path where the currently installed WebRA instance is located.
- **RegularBackupPath**: Directory where a backup of the current WebRA instance will be stored before installation.

```
  },
  "ExistingInstallation": {
    "BackupDirectory": ""
  },
  "RegularInstallation": {
    "ExistingWebRAPath": "",
    "RegularBackupPath": ""
```

5.3.5 Sample Data

- If set to **True**, the installation will include sample data to help with testing and initial configuration.
- If set to **False**, the installation will proceed without adding sample data and you will have to create everything by scratch.

5.3.5.1 Database Configuration

- **DatabaseType**:

  Specifies the type of database WebRA will use. Currently, only MSSQL is supported.

- **ConfigurationType**:

  - TYPICAL: Uses default settings for database configuration, requiring minimal user input.
  - ADVANCED: Allows manual customization of the database connection settings.

***Note**: You can either use Typical or Advanced Database Configuration, but not both simultaneously.*

5.3.5.1.1 Typical Database Configuration

- **MachineName**: The hostname or IP address of the database server where WebRA's database will be hosted.
- **Port**: The port used for database connections (e.g., 1433 for MSSQL by default).
- **Authentication**: Defines how WebRA connects to the database.

  - **SERVER_AUTH**: Requires entering a username and password to connect to the database.

  - **WINDOW_AUTH:** Uses Windows authentication, eliminating the need to manually enter credentials.

- **DatabaseName**: The name of the database WebRA will use.
- **UserId**: The username for database authentication.
- **Password**: The password for database authentication.

```
},
"SampleData": true,
//"comment": "possible values are True or false",
"DatabaseConfiguration": {
  "DatabaseType": "",
//  "comment": "possible values are MSSQL",
  "ConfigurationType": {
    "Type": "",
    //"comment": "possible values are TYPICAL and ADVANCED",
    "TypicalDatabaseConfiguration": {
    "MachineName": "",
      "Port": "",
      "Authentication": "",
     //"comment": "possible Values are SERVER_AUTH, WINDOW_AUTH",
     "DatabaseName": "",
     "UserId": "",
     "Password": ""
    }
```

5.3.6 Advanced Database Configuration

Allows specifying a direct connection string for finer control over database connectivity.

- Example for **SQL Authentication**:

data source=[server];initial catalog=[database];user id=[user];password=[password]

- Example for **Windows Authentication**:

data source=[server];initial catalog=[database];trusted_connection=true

```
      }
    },
    "AdvancedDatabaseConfiguration": {
   //   "connectionString": "windows Authentication",
      "comment": " Possible  values are SQL Auhentication and windows Authentication"
      //SQL Authentication
      //data source=[server address];initial catalog=[database name];user
id=[user_id];password=[password];MultipleActiveResultSets=True;Pooling=true;",
      // Windows Authentications
     //"RAEntities": "data source=[server address];initial catalog=[database
name];trusted_connection=true;MultipleActiveResultSets=True;Pooling=true;"
    }
```

5.3.7 Custom Installation Parameter

Defines the modules to be installed and their respective configurations.

- **FullyQualifiedDomainName:** Specifies the full domain name of the server.

Each module has settings for site name, installation status, and ports.

- **AdminModule**:
  - Site name: admin
  - Install: true
  - Port: “Port Number” (default HTTPS port)
  - Application Port: “Port Number”

- **WebModule**:
  - Site name: web
  - Install: true
  - Port: “Port Number”
  - Application Port: “Port Number”

- **ApiModule**:
  - Site name: api
  - Install: true
  - Port: “Port Number”
  - Application Port: “Port Number”

- **DeviceModule** (SCEP support):
  - Site name: device
  - Install: true
  - Port: “Port Number”
  - Application Port: “Port Number”

- **HTTPSDeviceModule** (Secure communication for SCEP, CMP, ACME, EST):
  - Site name: https-device
  - Install: true
  - Port: “Port Number”
  - Application Port: “Port Number”

- **SSLDeviceModule** (EST on client authentication-based setup):
  - Site name: ssl-device
  - Install: true
  - Port: “Port Number”
  - Application Port: “Port Number”

```
  },
  "CustomInstallation": {
    "FullyQaulifiedDomainName": "",
    "AdminModule": {
      "siteName": "admin",
      "install": true,
      "port": [redacted],
      "applicationPort": [redacted]
    },
    "WebModule": {
      "siteName": "web",
      "install": true,
      "port": [redacted],
      "applicationPort": [redacted]
    },
    "ApiModule": {
      "siteName": "api",
      "install": true,
      "port": [redacted],
      "applicationPort": [redacted]
    },
```

```
    },
    //SCEP
    "DeviceModule": {
      "siteName": "device",
      "install": true,
      "port": [redacted],
      "applicationPort": [redacted]
    },
    //Install SCEP,CMP,ACME,EST
    "HTTPSDeviceModule": {
      "siteName": "https-device",
      "install": true,
      "port": [redacted],
      "applicationPort": [redacted]
    },
    //Instal EST on client Authentications based
    "SSLDeviceModule": {
      "siteName": "ssl-device",
      "install": true,
      "port": [redacted],
      "applicationPort": [redacted]
    }
```

5.3.7.1 Port Usage Guidelines

- The same port number cannot be assigned to multiple modules. If a port is already in use, a different number must be selected for another module.
- In the application ports, if using a sequential series (e.g., **5001, 5002, 5003**), the next installation should use a different series (e.g., **4001, 4002, 4003**) to prevent conflicts.

Constraints

- *Windows Enrolment and Active Directory are not supported in Linux deployment.*

5.3.7.2 Allowing Ports on Ubuntu

If the Linux server is running **Ubuntu**, use the following command to allow a specific port:

```
sudo ufw allow <port>/tcp
```

For example, *to allow* ***port 81****:*

```
sudo ufw allow 81/tcp
```

To verify the firewall status:

```
sudo ufw status
```

5.3.7.3 Allowing Ports on AlmaLinux

If the server is running **AlmaLinux**, use the following command:

```
sudo firewall-cmd –permanent –add-port=<port>/tcp
```

For example, to allow **port 443**:

```
sudo firewall-cmd –permanent –add-port=443/tcp
```

After making changes, reload the firewall settings:

```
sudo firewall-cmd –reload
```

5.3.8 SMPT Configuration

Defines email settings for notifications:

- **Host**: SMTP server address (e.g., smtp.example.com).
- **Port**: SMTP connection port (e.g., 587 for TLS, 465 for SSL).
- **FromAddress**: Sender's email address.
- **Username** and **Password**: SMTP authentication credentials.
- **UseSsl**: Determines if SSL/TLS encryption is enabled.

Note: *When SMTP settings are configured in the installation process, an SMTP connector is automatically created upon running the installer.*

```
  },
  "SmtpConfiguration": {
    // The hostname or IP address of the SMTP server (e.g., [redacted])
    "Host": "",
    // The port number used for the SMTP connection (e.g., [redacted])
    "Port": [redacted],
    // The email address that appears as the sender
    "FromAddress": "",
    // Default subject line for the email
    "DefaultSubject": "",
    // The default recipient email address
    "DefaultRecipient": "",
    // The username for authenticating with the SMTP server
    "Username": "",
    // The password for authenticating with the SMTP server
    "Password": "",
    // Indicates if authentication is required for the SMTP server
    "IsAuthenticationRequired": true,
    // Indicates if SSL/TLS should be used for the SMTP connection
    "UseSsl": true
  }
}
```

After configuring all necessary parameters in the install.json file, launch the /install.sh file to install ADSS WebRA with the required set of configurations.
Before executing /install.sh, run the following commands:

```
dos2unix install.sh
```

```
cat -A install.sh
```

After running the above given commands, launch the /install.sh file by running the following command:

```
sudo ./install.sh
```

Note: *Before running the install.sh file, ensure it has the necessary execution permissions. To do this, open the file properties and grant execution rights.*

5.3.9 Uninstallation Process

To uninstall ADSS WebRA, update the install.json file by modifying the “Type” value under the “InstallationMode” parameter before running the uninstallation process. The following options determine the type of uninstallation:

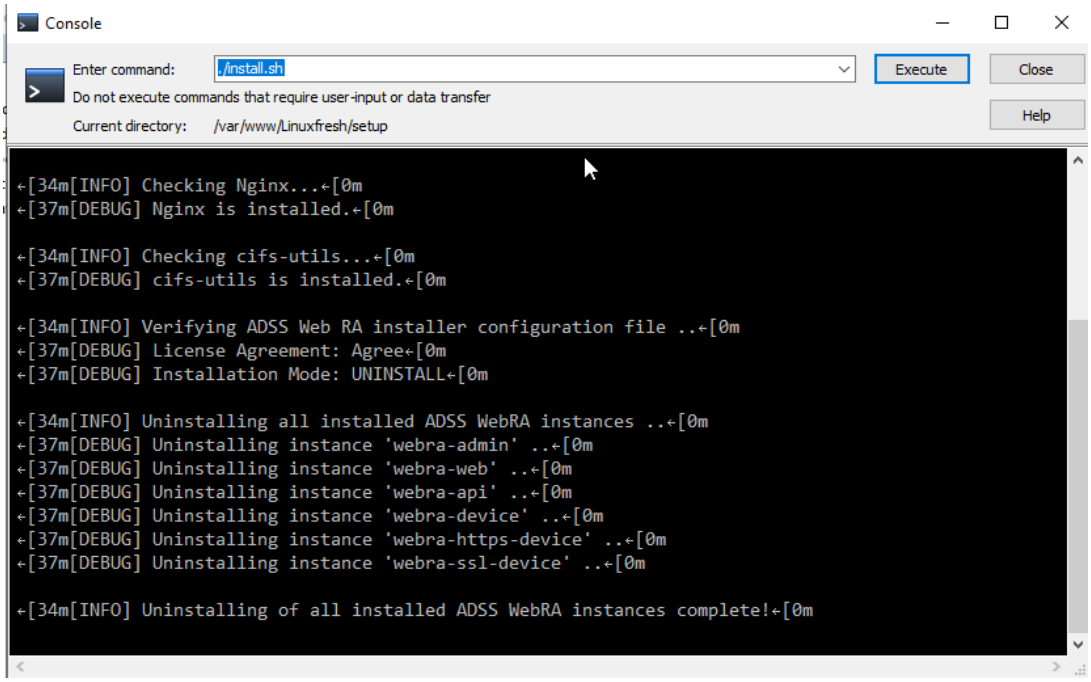
5.3.9.1 Uninstalling a Simple Installation

In the install.json file, set the “Type” value under “InstallationMode” to:

```
  },
  "InstallationMode": {
    "Type": "UNINSTALL",
    "comment": "possible values are
FIRST_TIME/LOAD_BALANCE/UPGRADE/EXISTING_DATABASE/REGULAR_RELEASE/UNINSTALL_REGULAR_RELEASE/CHANGE_DB_CREDENTIALS/UNINSTALL"
  },
```

After setting the Type, save the file and close it. Then navigate to **the /var/www/LinuxFresh/setup/** folder and run the install.sh script using the following command

```
sudo ./install.sh
```



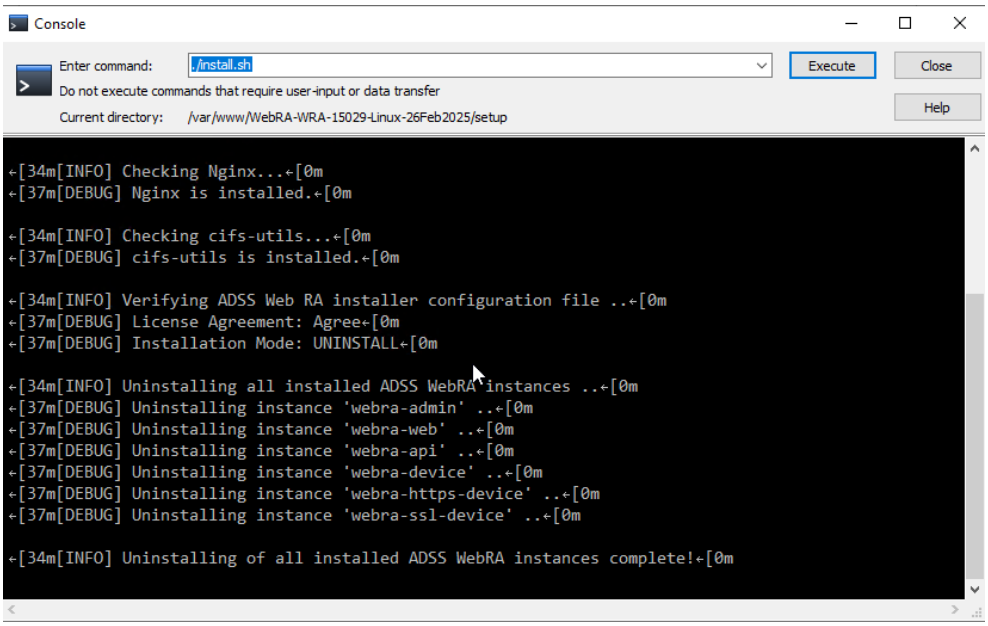
5.3.9.2 Uninstalling a Regular Release

To remove a previously installed regular release update modify the **install.json** file and set the Type under “InstallationMode” to:

```
  },
  "InstallationMode": {
    "Type": "UNINSTALL_REGULAR_RELEASE",
    "comment": "possible values are
FIRST_TIME/LOAD_BALANCE/UPGRADE/EXISTING_DATABASE/REGULAR_RELEASE/UNINSTALL_REGULAR_RELEASE/CHANGE_DB_CREDENTIALS/UNINSTALL"
  },
```

After setting the Type, save the file and close it. Then navigate to **the /var/www/LinuxFresh/setup/** folder and run the install.sh script using the following command:

```
sudo ./install.sh
```



6 Appendix

6.1 Troubleshooting

6.1.1 If ADSS Web RA Admin module is installed on Windows 2012 R2, then the HTTP 403.16 error code may occur when you access the ADSS Web RA Admin console from web browser.

Follow these instructions to solve this issue:

a. Open registry and add the key:

KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\ SCHANNEL

b. Create a new key with **Value Type: REG_DWORD (32-bit)**

c. Set **Value Name: ClientAuthTrustMode**

d. Edit the field and set **Value Data: 2**

If you are interested to know more details about it, browse the Microsoft KB link: https://support.microsoft.com/en-us/kb/2464556.

6.1.2 If you receive the HTTP error code 500.19 whilst accessing Admin, Web or API then:

a. Open IIS Management Console.

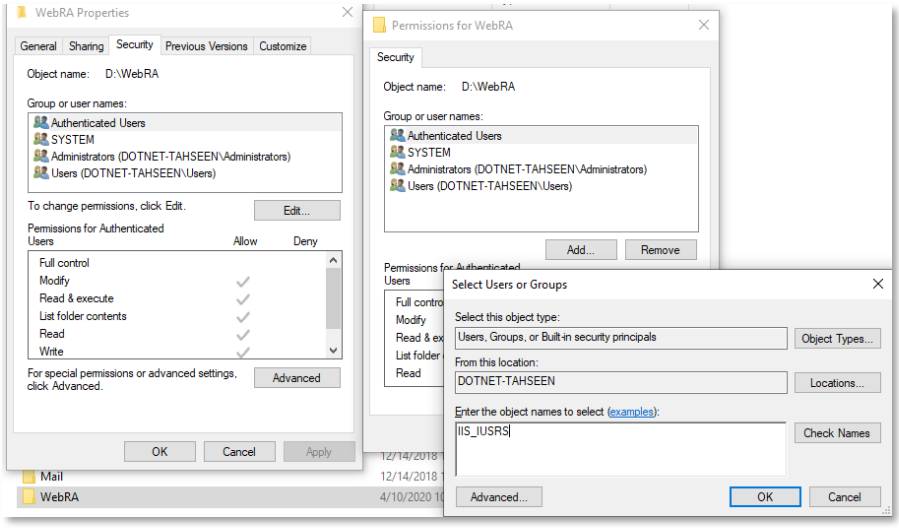
b. Go to Application Pools.

c. Select a site and click Advanced Setting.

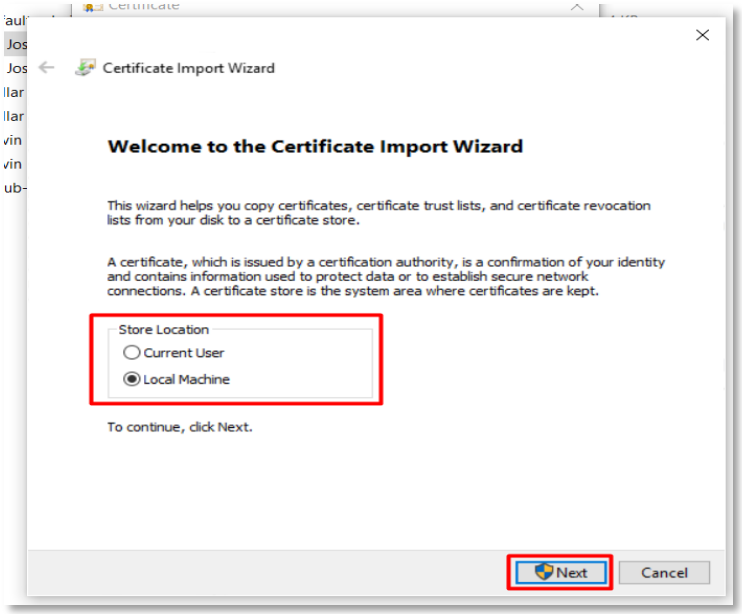
d. In General, make sure that Enable 32-Bit Applications is set to False.

6.1.3 If you cannot start ADSS Server from Windows Services panel on Azure, then make sure that you are not starting those services under Windows user that you have created while creating the Azure instance. You must create another Windows user with Administrative rights and start the services under that user.

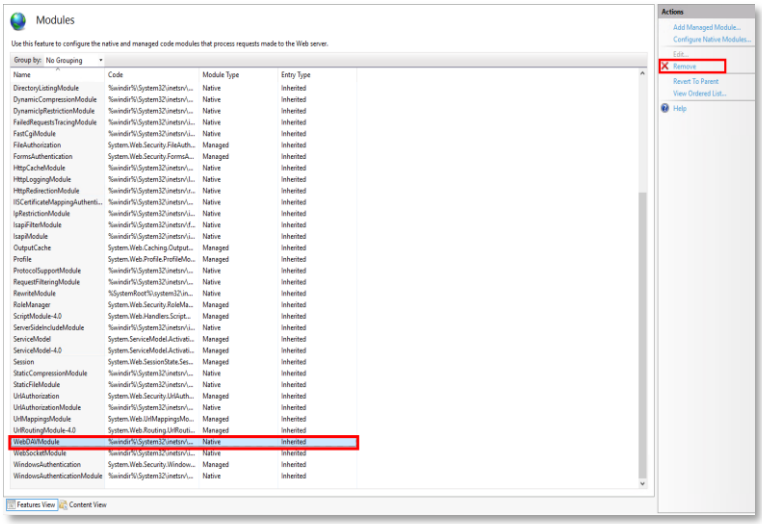
- Upon deploying to the server, you must keep in mind that the firewall and ports are open so that user can access the application from outside.
  - In **Firewall > Outbound Rules**. Open the ports if you want to 80-90, 440-450.
- Make sure the Directory has IIS permissions where code files are published.



- **Add / Install the SSL Server certificate** in **Microsoft Management Console** which will be imported to IIS so, connection between server and application can be established successfully.



- For API to work against all Verbs (GET,POST,DELETE,PUT etc) without **405** error, make sure WebDav Module remove against the API site.To do this click on "**API**" site in IIS ,select "**Modules**", find the "**WebDAVModule**" and remove it.



Troubleshooting for Linux

- **Deployment Stops Unexpectedly**

If the deployment process halts during execution, it may be due to Linux security settings preventing the installation from proceeding. To resolve this issue:

1. Temporarily disable Linux security enforcement by running the following command:

   ```
   sudo setenforce 0
   ```

   This forces the security module to be turned off.

2. Restart the **Nginx** service to ensure proper functionality:

   systemctl restart nginx

- **A Specific WebRA Service Is Not Running**

If the deployment completes but a specific service (such as **Admin**, **Web**, or **API**) is not running, restart the affected service using the following command:

systemctl restart kestrel-webra-{service name}.service

Replace {service name} with the actual service name (e.g., **admin**, **web**, **api**).

- **Installation Fails Due to Spaces in Folder Name**

Issue:

The installation process fails or encounters errors if the folder name where the installation package is placed contains spaces.

Solution:

Ensure that the installation folder name does not contain spaces. Rename the folder using underscores (_) or remove spaces before proceeding with the installation.

6.2 Configurations used for Simple Certificate Enrollment Protocol (SCEP)

6.2.1 Make sure that following tag is added in “web.config” of web module:

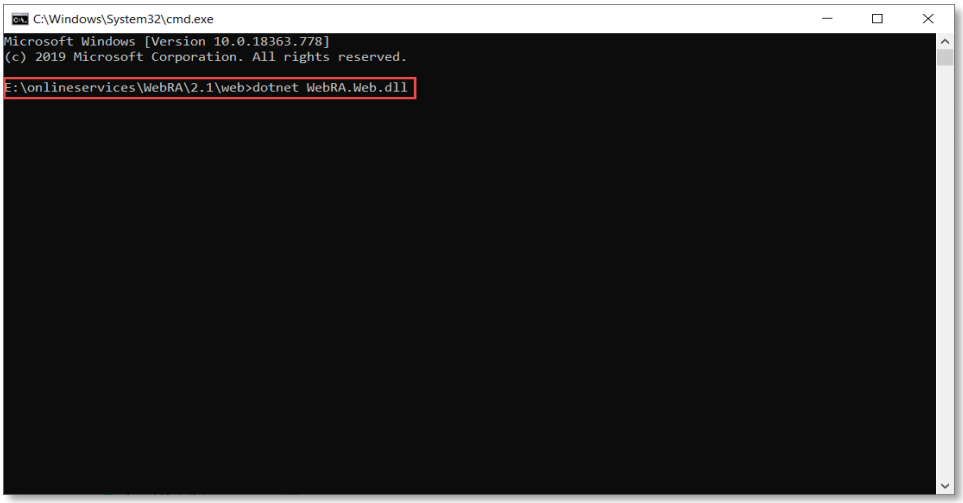
```
<security>
   <requestFiltering>
     <requestLimits maxQueryString=”8192”/>
      </requestFiltering>
   </security>
```

```
<configuration>
  <location path="." inheritInChildApplications="false">
    <system.webServer>
      <handlers>
        <add name="aspNetCore" path="*" verb="*" modules="AspNetCoreModuleV2" resourceType="Unspecified" />
      </handlers>
      <aspNetCore processPath="dotnet" arguments=".\WebRA.Protocol.dll" stdoutLogEnabled="true" stdoutLogFile=".\logs\stdout">
      </aspNetCore>
      <security>
        <requestFiltering>
          <requestLimits maxQueryString="8192" />
        </requestFiltering>
      </security>
    </system.webServer>
  </location>
</configuration>
<!--ProjectGuid: 31d1b205-525a-481e-bd32-4378e4f6559d-->
```

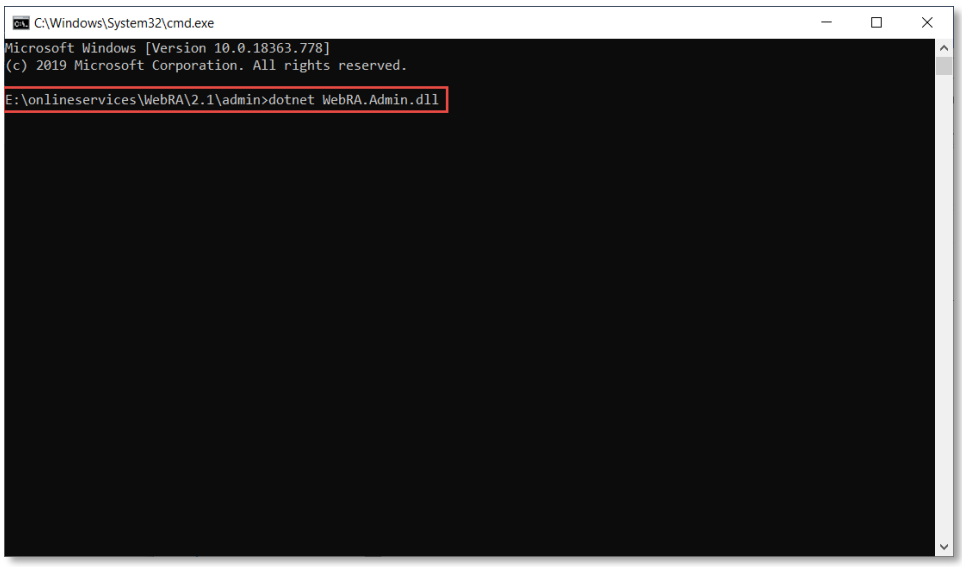
SCEP server URL that will be used for router will be:

- “[Server URL]/scep” e.g “https://beta.web.ra.signinghub.com/scep
- Update URL value in Expect-CT header in “**web.config**” for web and admin modules according to your deployment URL. e.g. **<add name="Expect-CT" value="max-age=0, report-uri='https://adminra.signinghub.com'" />**

To test if the code is working properly for web, run command line in [installation-dir]/web and type following command:



To test if the code is working properly for admin, run command line in [installation-dir]/admin and type following command:



6.3 SSL Certificates

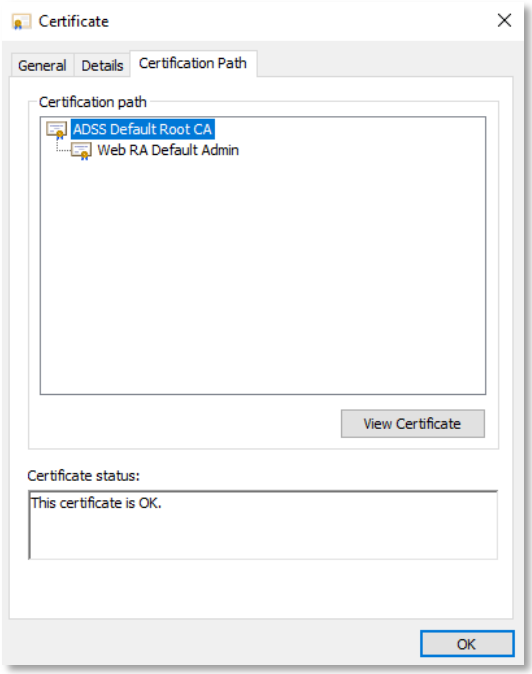
ADSS Web RA is a web application that is hosted in IIS. It is recommended to secure the communication between the server and browsers by using SSL over HTTPS. It is also recommended to use an SSL certificate issued by a well-known certificate authority (CA) e.g., Comodo, Symantec, Digicert, etc.

The Administrators portal can be accessed only via TLS client authentication. A default TLS client certificate is already packaged into ADSS Web RA.

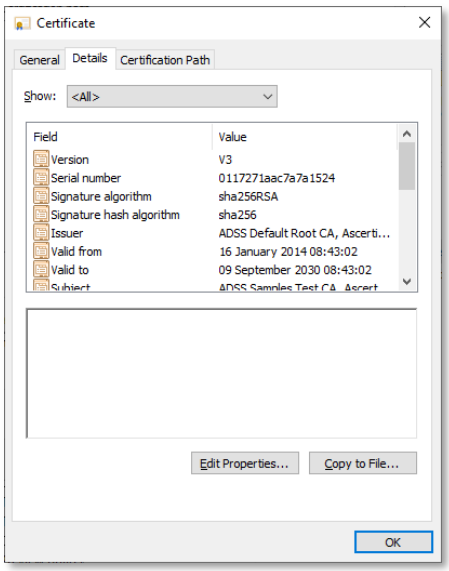
6.3.1 Exporting Root and Intermediate Certificates

6.3.2 In the [installation_dir]/setup/certs directory there are two files with the name *web-ra-default-admin.cer* and *web-ra-default-admin.pfx*. TLS certificate is installed, but root certificates are not validated by the machine. To validate it, root certificate needs to be imported in the certificate store.

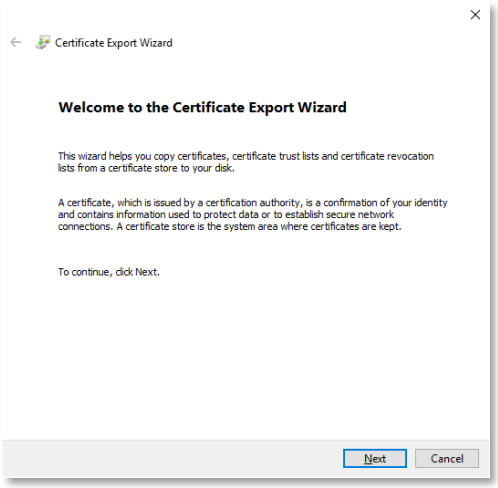
6.3.3 Double click the web-ra-default-admin.cer file



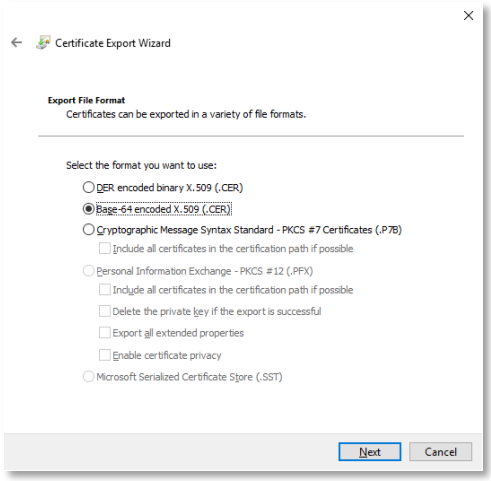
6.3.4 Select the Certification Path tab from the top. The default ADSS Web RA TLS certificate has one root certificate. Select the root certificate and click the View Certificate button. A new window will appear showing general details of the intermediate certificate.



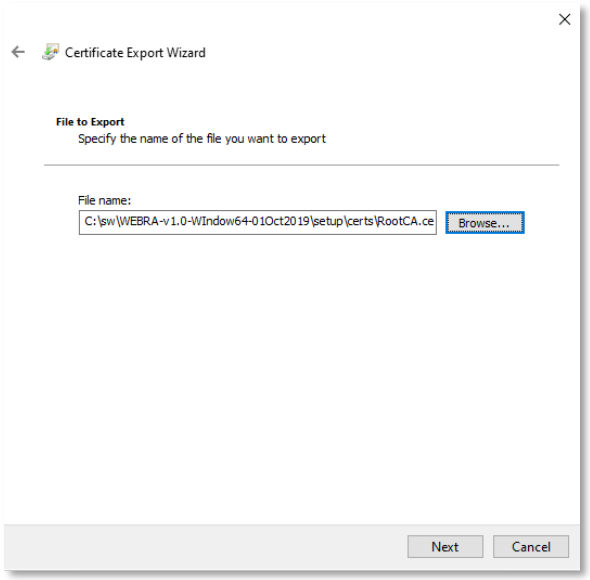
6.3.5 Select the Details tab from the top and click Copy to File. This will initiate the certificate export wizard.



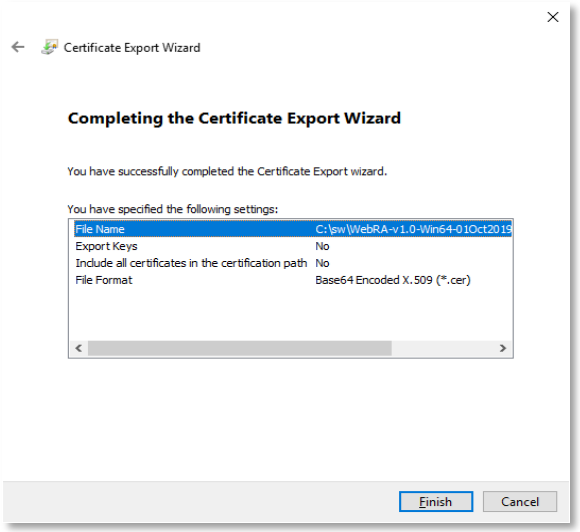
6.3.6 Click Next.



6.3.7 Select the Base-64 encoded X.509 (.CER) option and click Next



6.3.8 Choose a path where you want to save the certificate file for the intermediate certificate, and click Next.



6.3.9 Click Finish to complete the root certificate export process.

6.4 SSL Configuration for Linux

After installation, SSL certificates must be configured to enable secure communication for WebRA. Follow these steps to configure SSL:

6.4.1 Navigate to the Nginx configuration directory:

The configuration for the SSL device module is stored in the **sites-available** directory. Open the file with a text editor:

```
sudo nano /etc/nginx/sites-available/webra-ssl-device
```

6.4.2 Locate the SSL Configuration Block:

Inside this file, find the section where the SSL certificate and key are defined. It should look similar to this:

- ssl_certificate "/var/www/Linux_ED/setup/certs/EST-Server.crt";
- ssl_certificate_key "/var/www/Linux_ED/setup/certs/EST-Server.key";

6.4.3 Update the Certificate Paths:

Modify these lines to point to the correct certificate and key locations:

```
ssl_certificate "/var/www/Linux_Fresh/setup/certs/EST-Server.crt";
ssl_certificate_key "/var/www/Linux_Fresh/setup/certs/EST-Server.key";
```

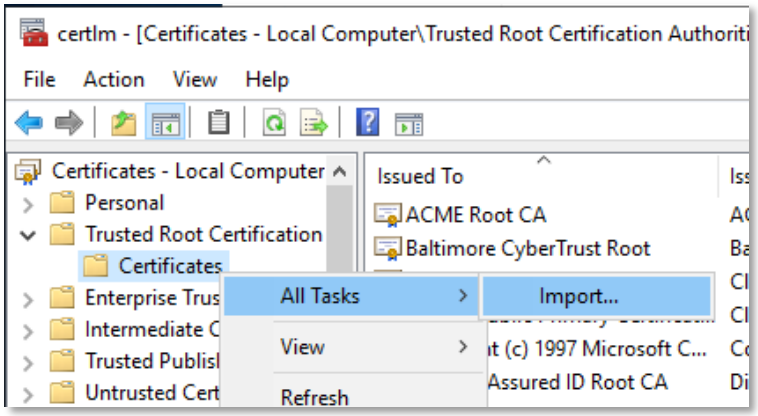
After updating the paths, save and exit the file**.** Once the configuration is updated, restart Nginx to load the new certificate. By following these steps, the WebRA module will be properly configured to use the provided SSL certificates.

6.5 Importing Root and Intermediate Certificates

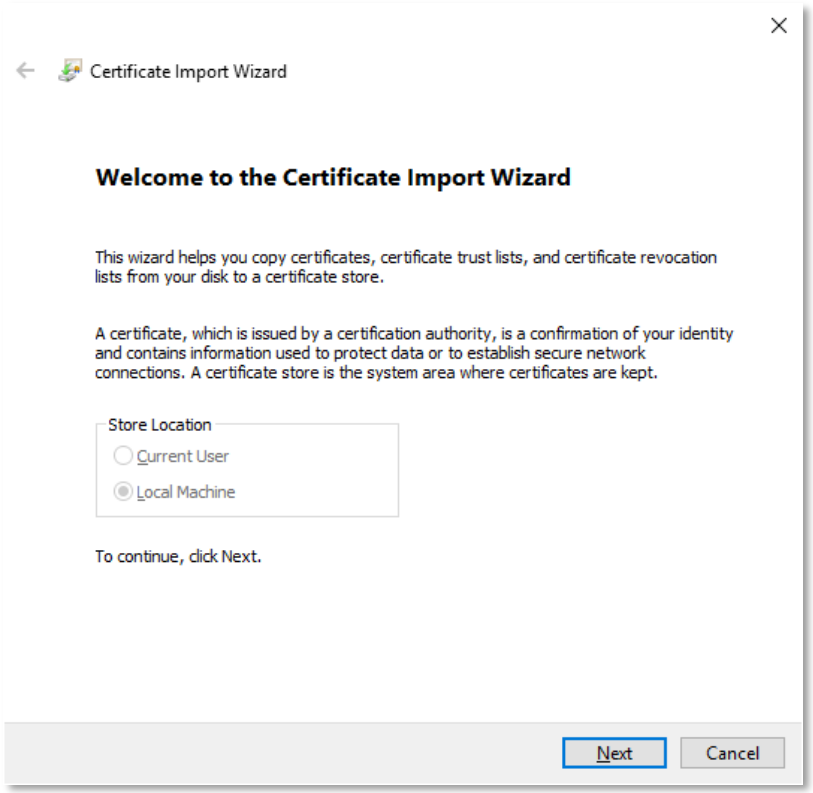
Now that we have the intermediate and root certificates exported and saved in a local file, we can import it to the certificate store.

6.5.1 Launch **certlm.msc** from the command prompt.

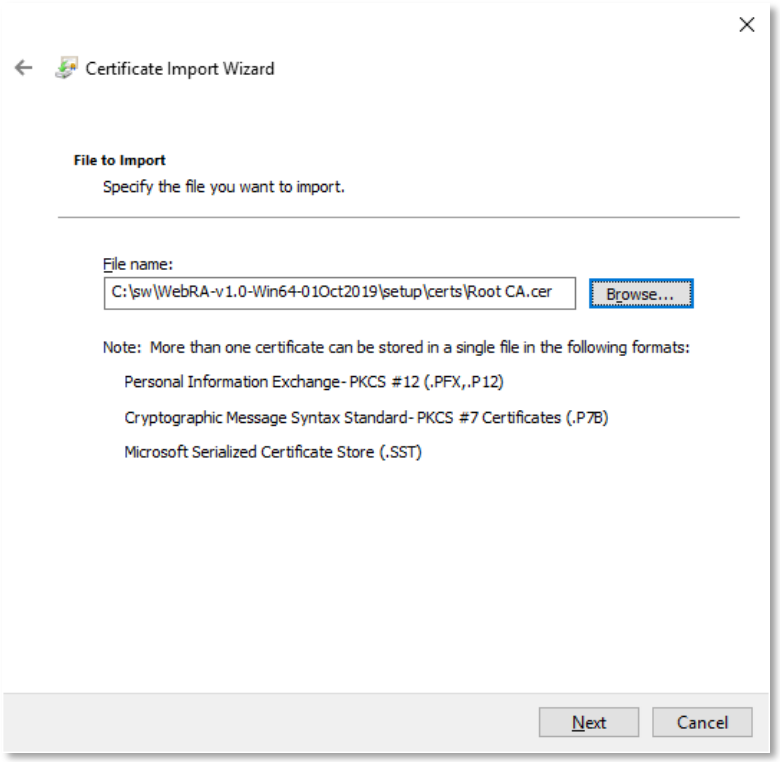
6.5.2 Expand the **Trusted Root Certification Authorities** folder from the left panel and right-click on **Certificates**. Now select **All Tasks** and then **Import...**



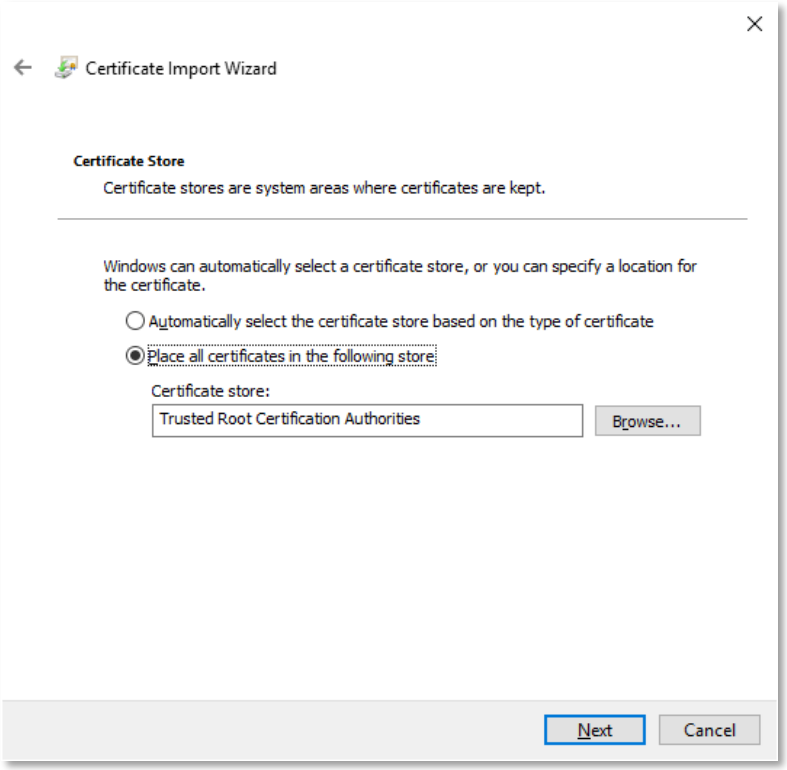
6.5.3 A certificate import wizard appears, Click **Next** to proceed.



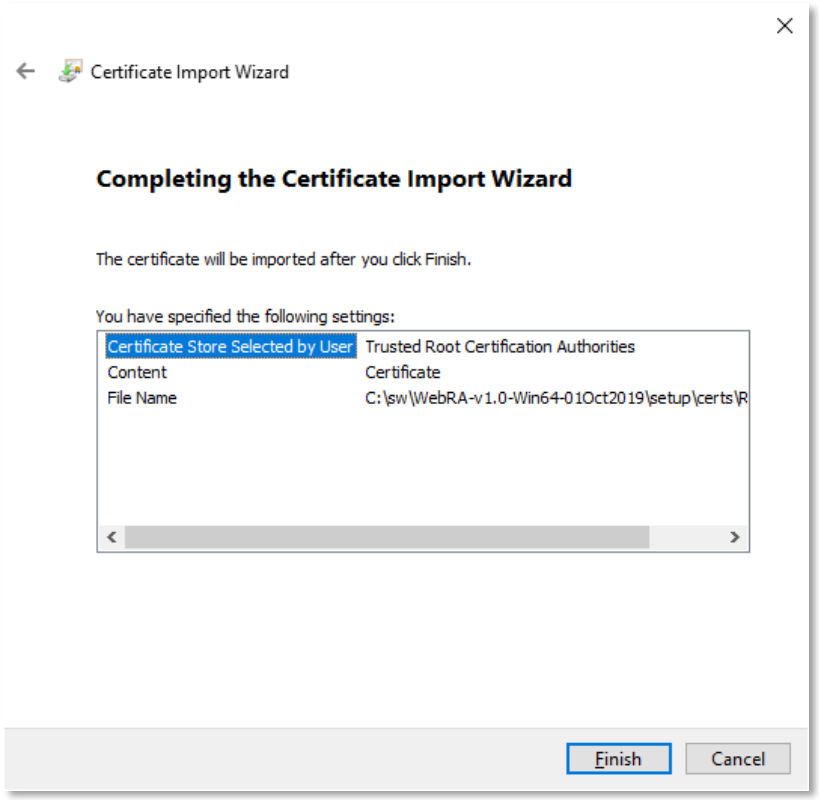
6.5.4 Browse the root certificate that we recently exported and click **Next** to proceed.



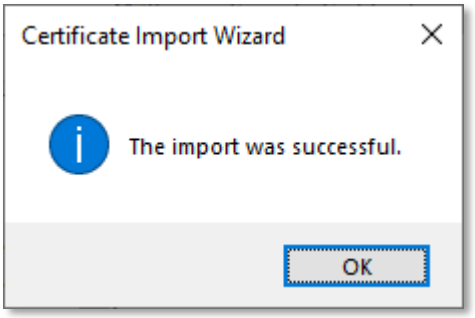
6.5.5 Click **Next** to proceed.



6.5.6 The root certificate is imported to the certificate store, click **Finish**.



6.5.7 A prompt will appear informing about the successful import of the certificate.

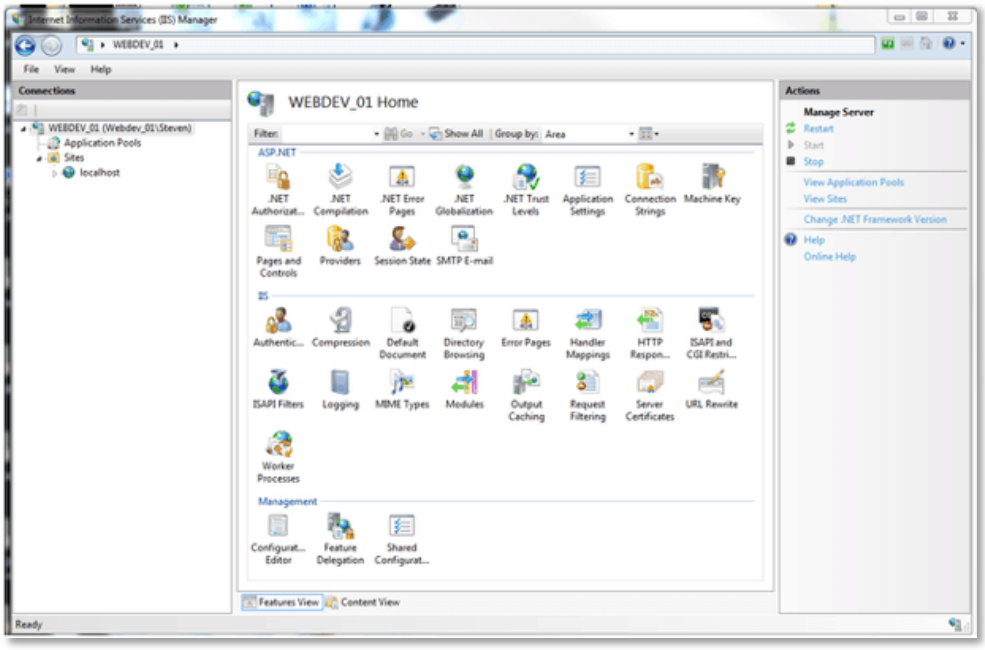


If you want to deploy the application for testing purpose you may want to use a self-signed certificate for proof of concept.

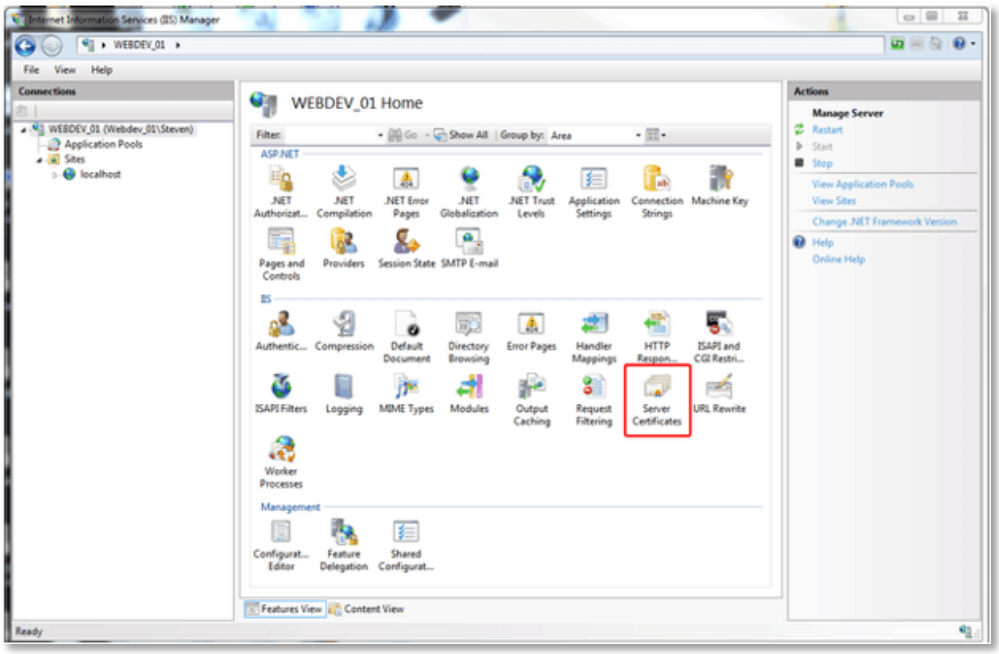
6.6 Generate a Self -Signed Certificate

For testing purpose or proof of concept, mostly a self-signed certificate will be required. It is easy to create a self-signed certificate with IIS.

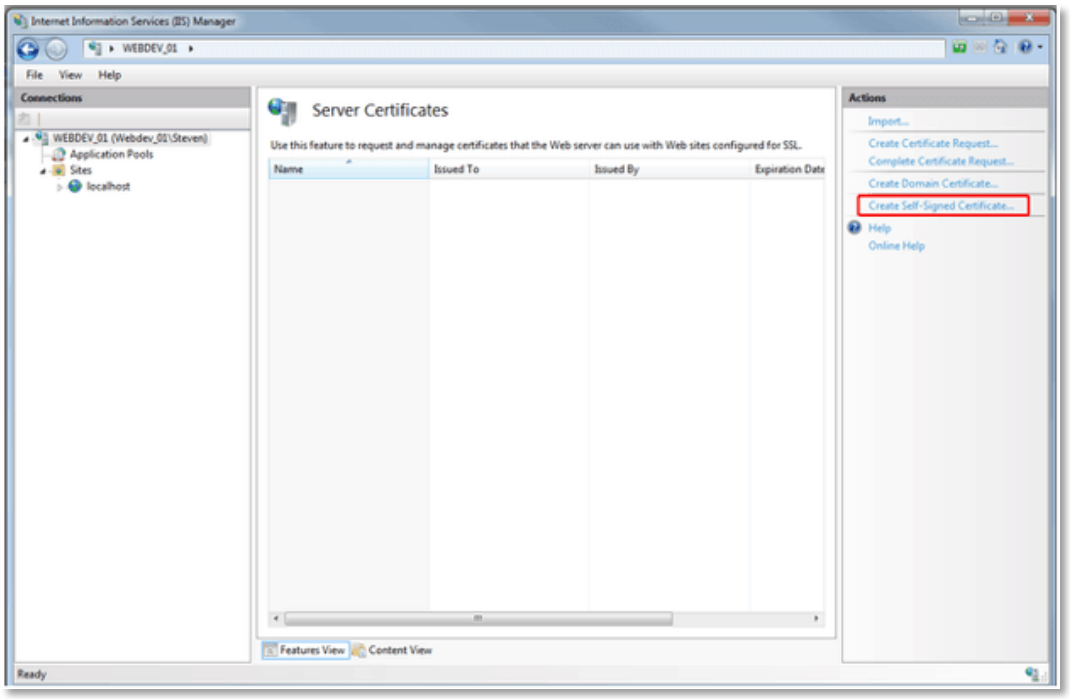
6.6.1 Launch the **IIS Manager**.



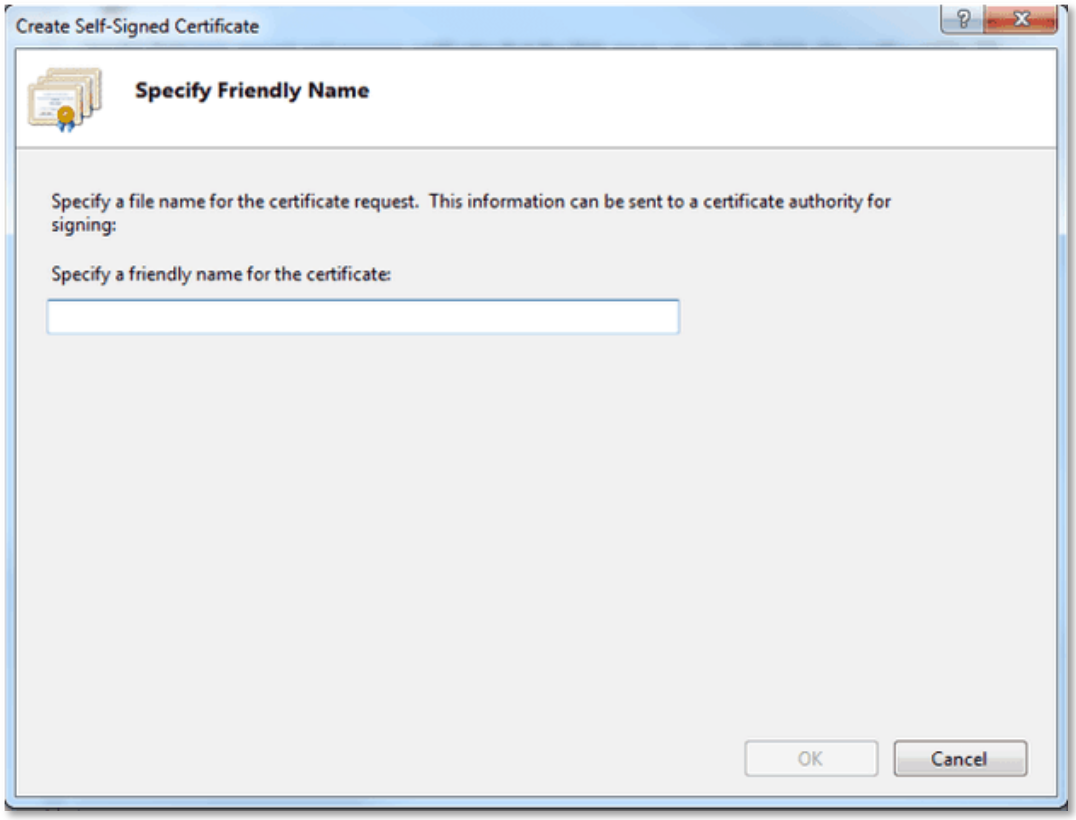
6.6.2 Click the **Server Name** from the **Server Connections**.



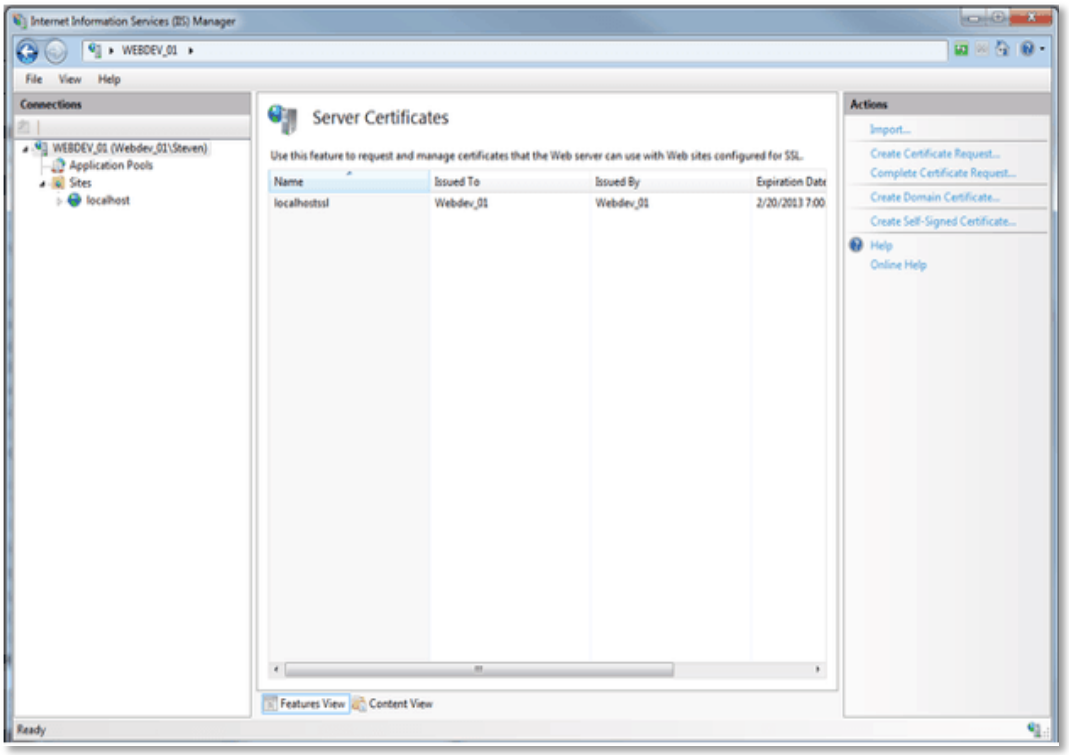
6.6.3 Double-click on **Server Certificates** from the IIS section in the middle panel.



6.6.4 Click **Create Self-Signed Certificate**... under the right Actions column.



6.6.5 Provide a meaningful name and press **OK**.

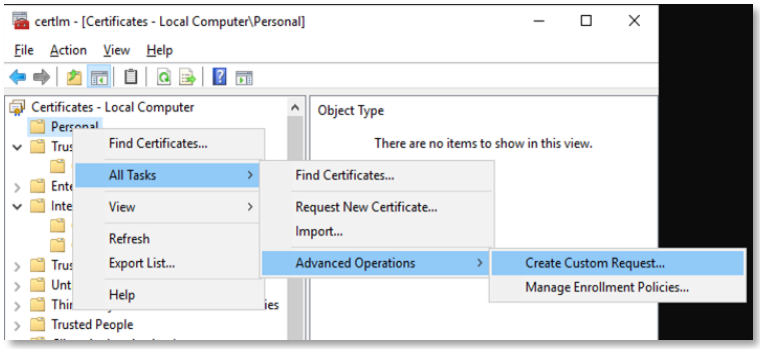


Now you have an SSL certificate that is self-signed and is valid for one year. You can select this certificate for creation of HTTPS binding for testing and proof of concept purposes.

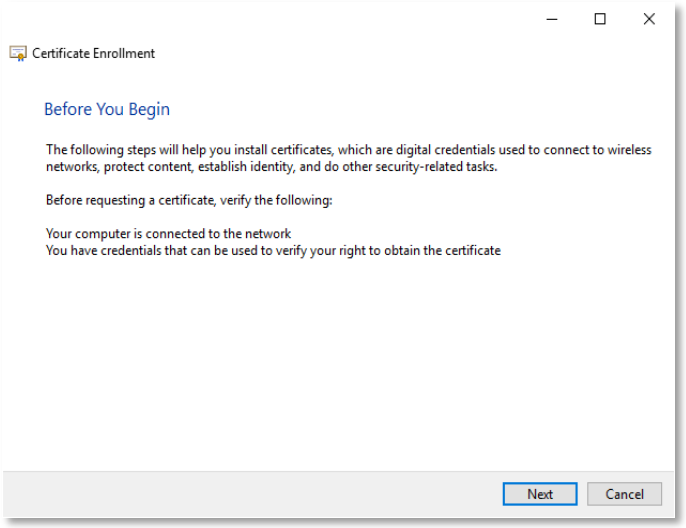
6.7 Generate a CSR for an SSL Certificate

To generate a self-signed SSL certificate follow the steps below:

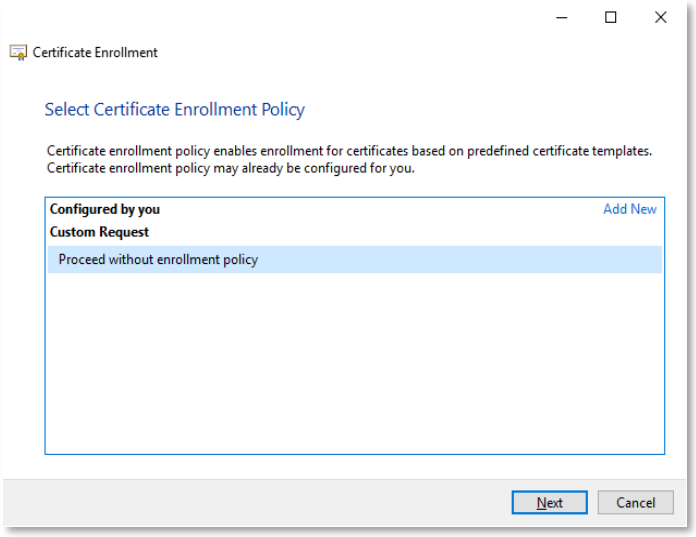
6.7.1 Launch **certlm.msc** from the command prompt.



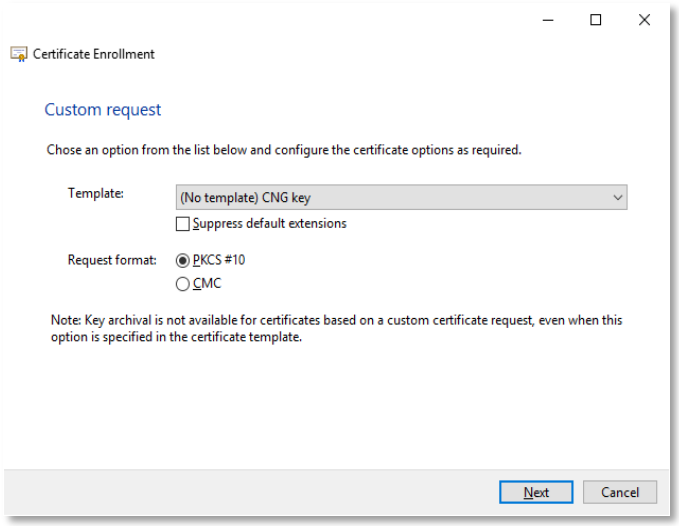
6.7.2 From the left menu, select and right-click the **Personal** folder. From the context menu, select **All Tasks** > **Advanced Operations** > **Create Custom request**. A new dialog will appear for certificate enrollment.



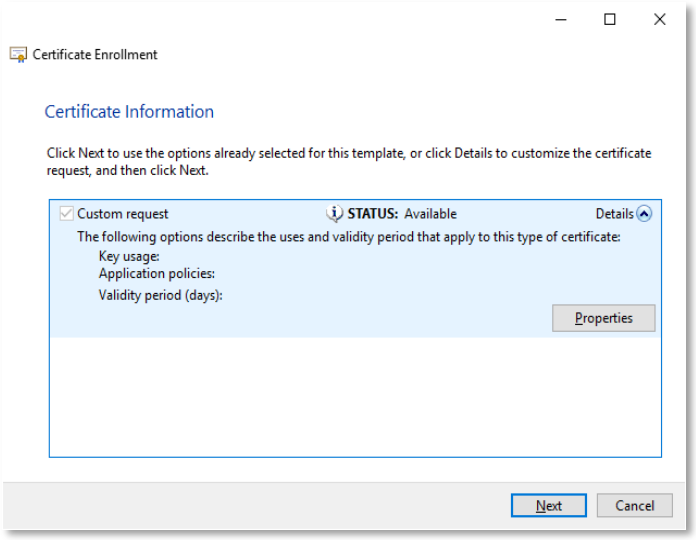
6.7.3 Press **Next** to proceed.



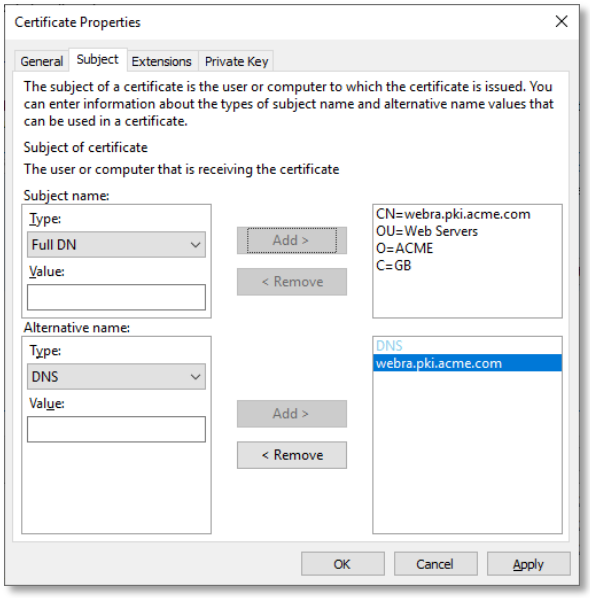
6.7.4 Select Proceed without enrollment policy then click **Next**.



6.7.5 Accept the default values and press **Next** without changing anything

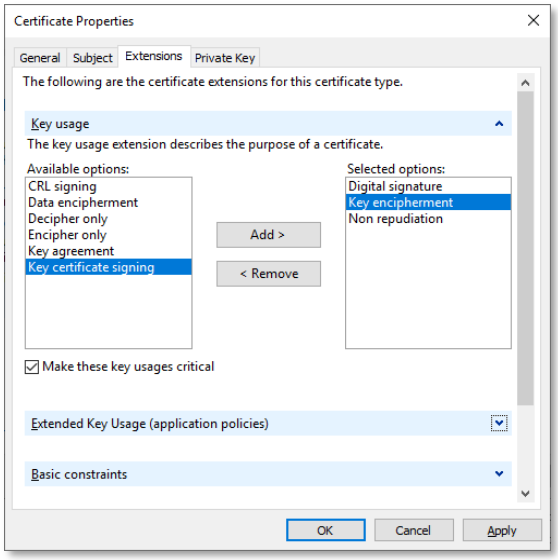


6.7.6 Click **Details** and the Properties button will appear. Click **Properties**.



6.7.7 Select the Subject tab from the top. For subject name enter CN=webra.pki.acme.com, OU=Web Servers, O=ACME, C=GB in the value and press Add >. For Alternate name enter DNS value as webra.pki.acme.com.

These values are the sample values used for certificate creation and can be replaced with the realistic data.

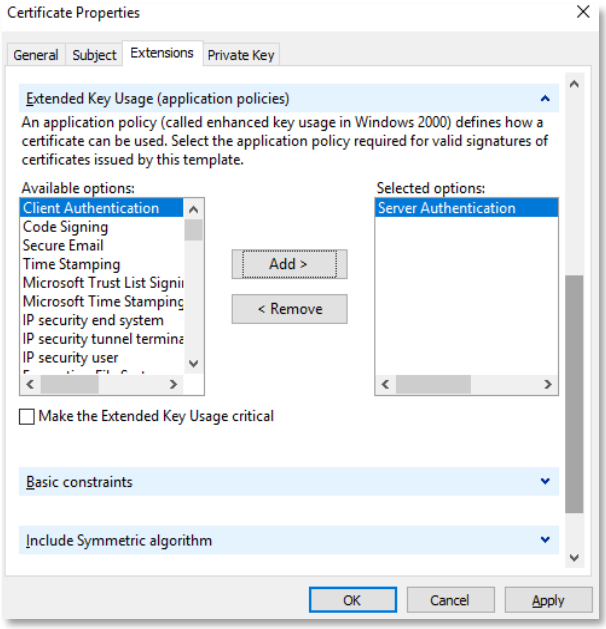


6.7.8 Select the Extensions tab from the top. Select the Key usage option from the drop down extensions. Now from the Available options, choose the following:

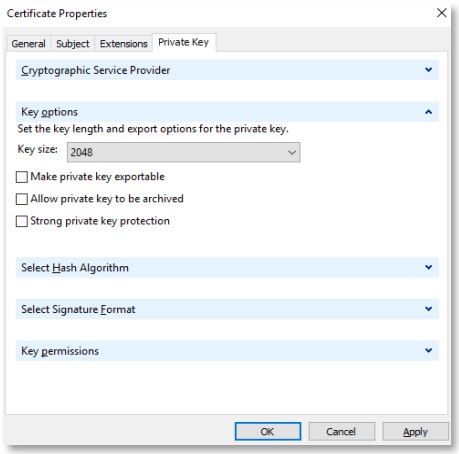
- Digital signature
- Key encipherment
- Non repudiation

Make sure you tick the **Make these key usages critical** checkbox.

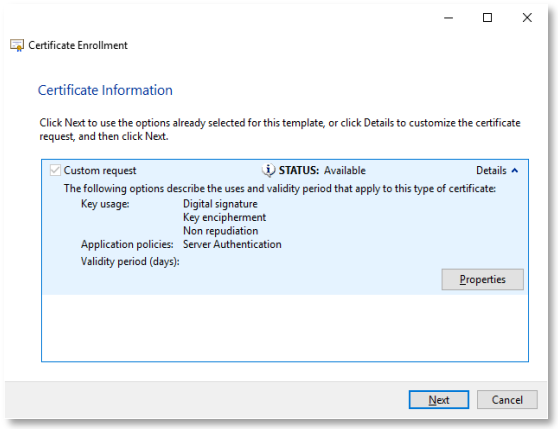
6.7.9 Now select the Extended Key Usage (application policies) from the drop down, and Server Authentication from the list.



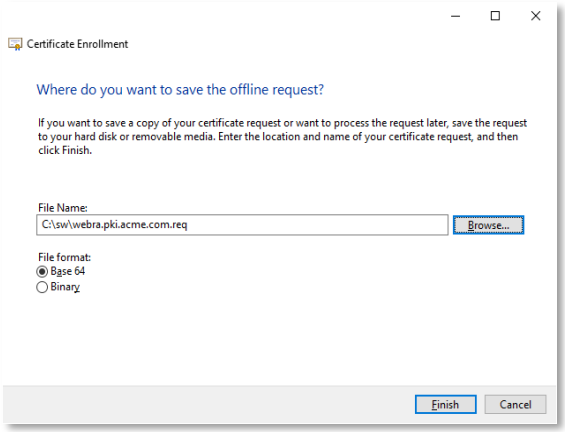
6.7.10 Select the Private Key tab from the top. Select the Cryptographic Service Provider option from the first drop down and Key options from the second drop down. Change the Key size to 2048 and click OK. The Certificate Enrollment screen will appear again.



6.7.11 Press Next to proceed.



6.7.12 Browse the location to save the request file and select the Base 64 file format. Press Finish. This request file can be submitted to any CA to create a certificate against this request. Every CA processes the request and generates a certificate as per their own policy. Once the certificate is received from a CA it can be imported into the certificates.



For further details contact us on sales@ascertia.com or visit www.ascertia.com

*** End of Document ***