



ADSS Web RA Installation Guide

ASCERTIA LTD

JULY 2022

Document Version - 2.6

© Ascertia Limited. All rights reserved.

This document contains commercial-in-confidence material. It must not be disclosed to any third party without the written authority of Ascertia Limited.

Commercial-in-Confidence

1	Introduction	3
1.1	Scope	3
1.2	Intended Readership	3
1.3	Technical Support.....	3
1.4	Glossary	4
2	System Requirements.....	5
2.1	Hardware Prerequisites	5
2.2	Software Prerequisites.....	6
2.3	Application Development feature in IIS	8
2.4	Microsoft .Net Core 5.0.9 Runtime & Hosting Bundle.....	9
2.5	Microsoft IIS URL Rewrite Module 2.1	11
2.6	Unlock system.webServer/serverRuntime section in IIS	14
	SMTP Server	15
2.7	Database	15
3	Installation Modules	16
4	ADSS Web RA Installation	17
4.1	Fresh Installation of ADSS Web RA.....	17
4.1.1	ADSS Web RA URLs.....	28
4.2	Installing ADSS Web RA with A Load-Balanced Configuration	29
4.3	Installing ADSS Web RA with an Existing Database	37
4.4	Upgrading ADSS Web RA	43
4.4.1	Upgrade Procedure.....	43
4.5	Changing Database Credentials for an Existing Installation	50
5	ADSS Web RA Uninstallation	54
6	Appendix.....	57
6.1	Troubleshooting	57
6.2	SSL Certificates	61
6.2.1	Exporting Root and Intermediate Certificates	61
6.3	Importing Root and Intermediate Certificates	68
6.4	Generate a Self -Signed Certificate	72
6.5	Generate a CSR for an SSL Certificate.....	75

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.

ADSS Web RA comprises four 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.

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	<ul style="list-style-type: none">• 200 GB (Minimum)
Memory	<ul style="list-style-type: none">• 16 GB (Minimum)• 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	<ul style="list-style-type: none">• A modern multi-core CPU such as Xeon E3-XXXX or E5-XXXX series is recommended
Processor Type	<ul style="list-style-type: none">• x64
HSM (Optional)	<ul style="list-style-type: none">• SafeNet Luna SA, Luna PCI, Luna G5• SafeNet Protect Server (PCI or External)• Thales nShield Solo or Connect HSMs• Utimaco HSMs• Azure Keyvault• Amazon AWS Cloud HSM

2.2 Software Prerequisites

Component	Requirements
Operating Systems	<ul style="list-style-type: none"> Windows Server 2019 Windows Server 2016
Microsoft IIS	<ul style="list-style-type: none"> IIS 10 Application Development feature in IIS
IIS Rewrite Module	<ul style="list-style-type: none"> v2.1
.Net Framework	<ul style="list-style-type: none"> .Net Framework 4.7.2 or above
.Net Core Runtime & Hosting Bundle	<ul style="list-style-type: none"> ASP.NET Core Runtime 5.0.9
Database Server	<ul style="list-style-type: none"> Microsoft SQL Server 2019 Microsoft SQL Server 2017 Microsoft SQL Server 2016 Microsoft SQL Server 2014
Database Management Studio	<ul style="list-style-type: none"> Microsoft SQL Server Management Studio 2019 Microsoft SQL Server Management Studio 2017 Microsoft SQL Server Management Studio 2016 Microsoft SQL Server Management Studio 2014
Web Brower (for end-users and administrators)	<p>The following browsers are supported:</p> <ul style="list-style-type: none"> Google Chrome 40+ Mozilla Firefox 35+ Microsoft Edge 14+ IE 11 (Not supported by Microsoft anymore) Apple Safari 8+ Opera 26+
ADSS Server	<p>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.</p> <ul style="list-style-type: none"> ADSS Server 6.6 or above

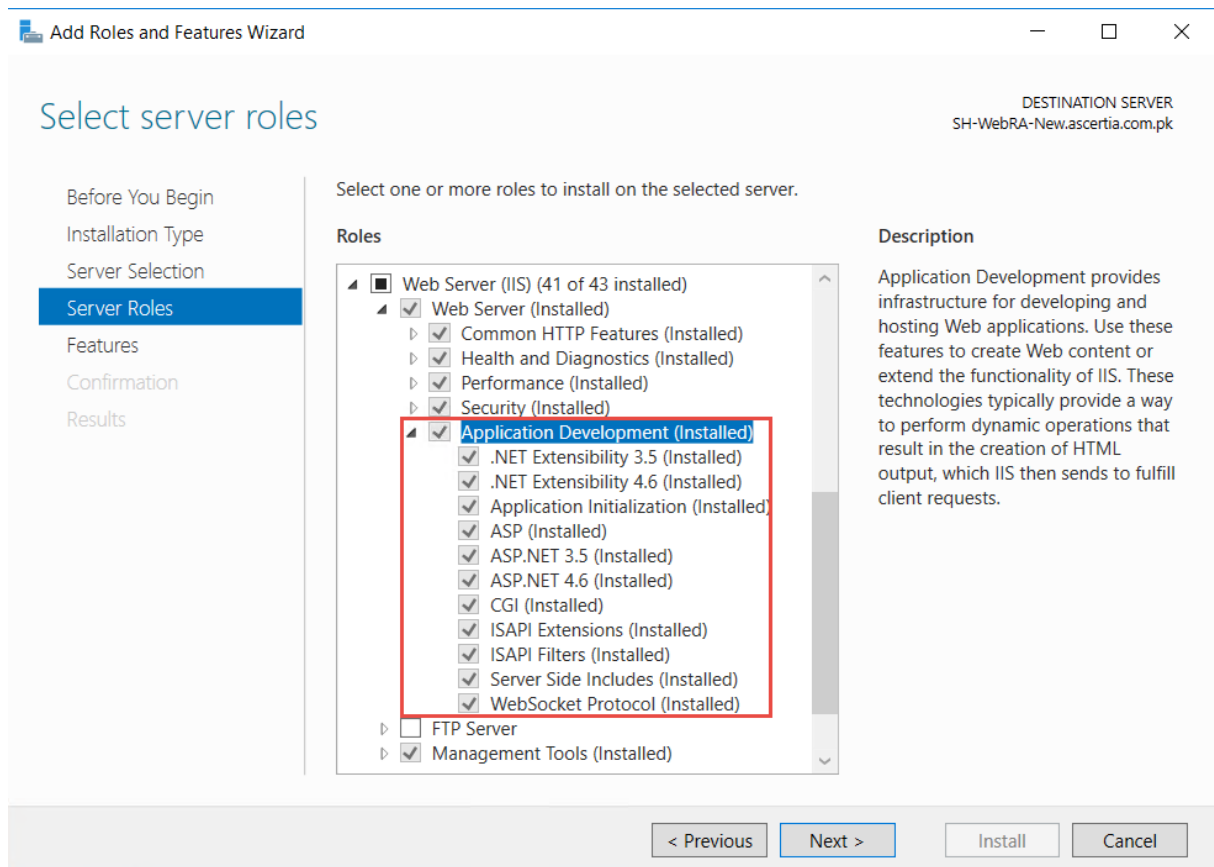
DMZ Proxy Systems	<p>A DMZ proxy server is recommended to provide enhanced security for ADSS Web RA. Supported web servers are:</p> <ul style="list-style-type: none">• Windows Server + IIS, Apache or IBM HTTP Server• Linux + Apache or IBM HTTP Server <p>It is recommended to use a reasonable CPU, 4 GB 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.</p>
--------------------------	--

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 feature in IIS of the deployment machine:



2.4 Microsoft .Net Core 5.0.9 Runtime & Hosting Bundle

Download the Microsoft .Net Core 5.0.9 runtime and hosting bundle from the following link:

- [Microsoft .Net Core 5.0.9 Runtime & Hosting Bundle](#)

Scroll down to 5.0.9 version and download the highlighted hosting bundle installer

5.0.9 Security patch

[Release notes](#) Latest release date August 10, 2021

Build apps - SDK

SDK 5.0.400

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

Visual Studio support
Visual Studio 2019 (v16.11)
Visual Studio 2019 for Mac (v8.10)

Included in
Visual Studio 16.11.0

Included runtimes
.NET Runtime 5.0.9
ASP.NET Core Runtime 5.0.9
.NET Desktop Runtime 5.0.9

Language support
C# 9.0
F# 5.0

Run apps - Runtime

ASP.NET Core Runtime 5.0.9

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)
15.0.21196.9

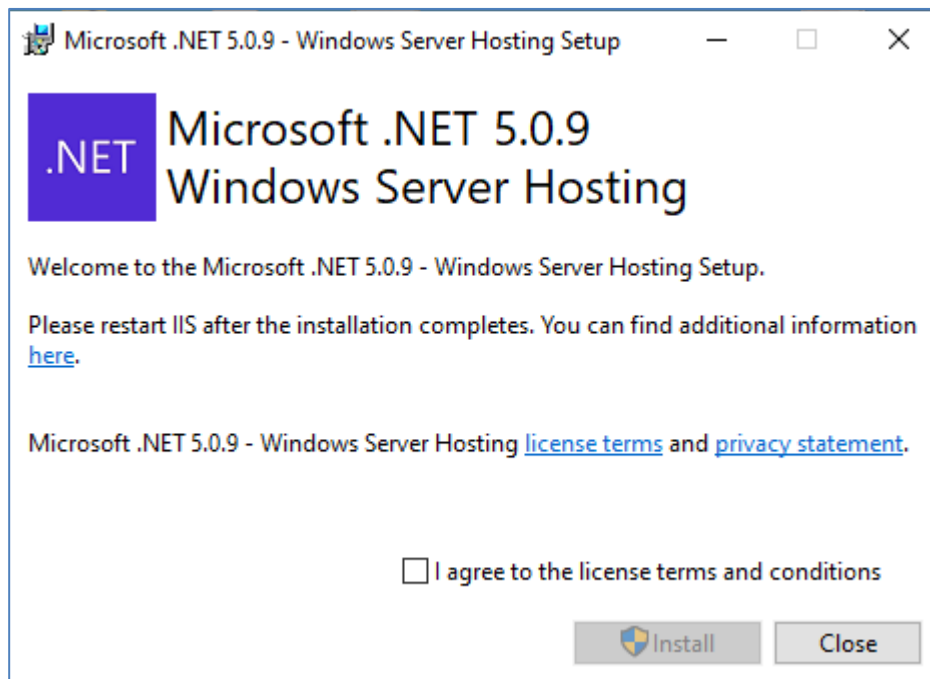
OS	Installers	Binaries
Linux	Package manager instructions	Arm32 Arm32 Alpine Arm64 Arm64 Alpine x64 x64 Alpine
macOS		x64
Windows	Hosting Bundle x64 x86	Arm64 x64 x86

.NET Desktop Runtime 5.0.9

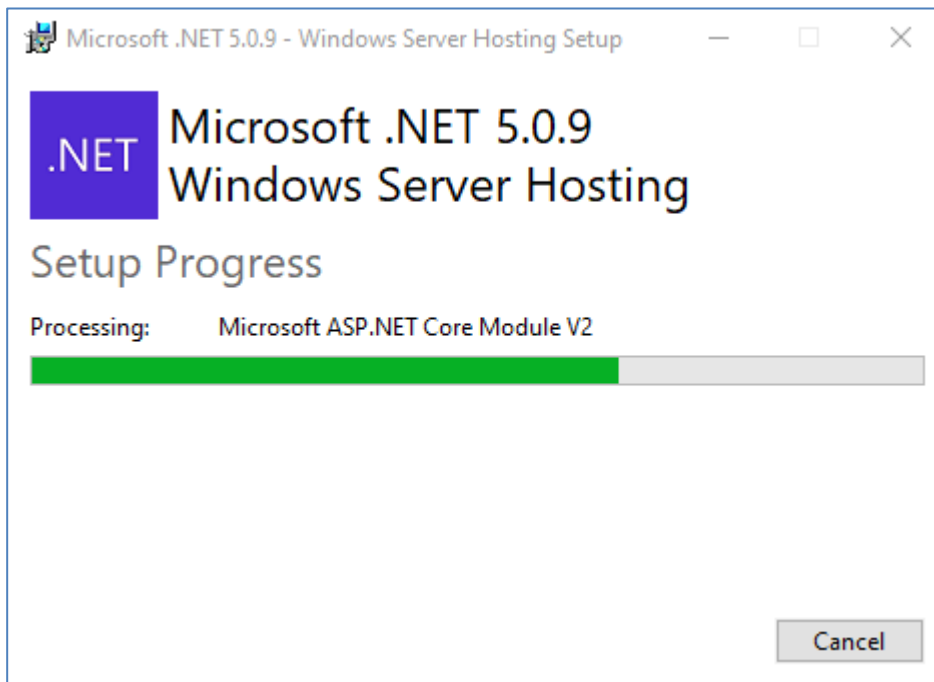
The .NET Desktop Runtime enables you to run existing Windows desktop applications. **This release includes the .NET Runtime; you don't need to install it separately.**

OS	Installers	Binaries
Windows	Arm64 x64 x86	

Once downloaded execute the installer by executing **dotnet-hosting-5.0.9-win.exe**

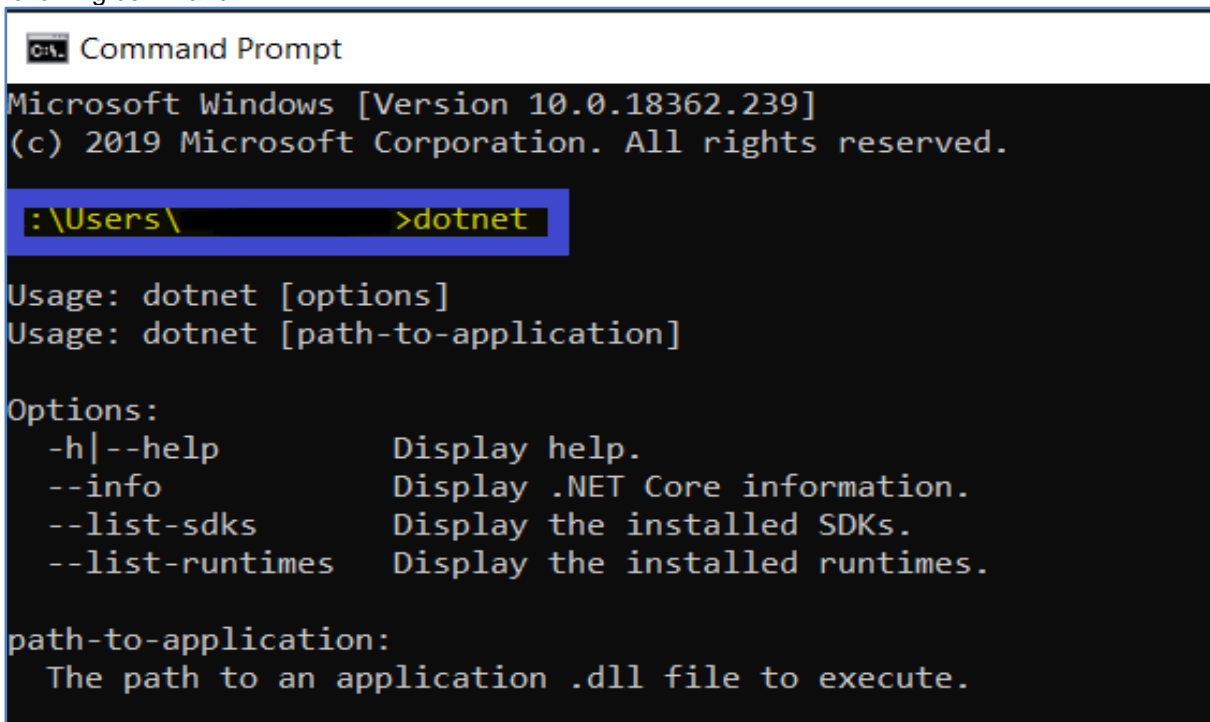


Agree to the license terms and conditions and press Install, it will take a few minutes to complete.



And after successful completion of the installation press **Close**.

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



```
Microsoft Windows [Version 10.0.18362.239]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[user]>dotnet

Usage: dotnet [options]
Usage: dotnet [path-to-application]

Options:
  -h|--help           Display help.
  --info              Display .NET Core information.
  --list-sdks         Display the installed SDKs.
  --list-runtimes     Display the installed runtimes.

path-to-application:
  The path to an application .dll file to execute.
```

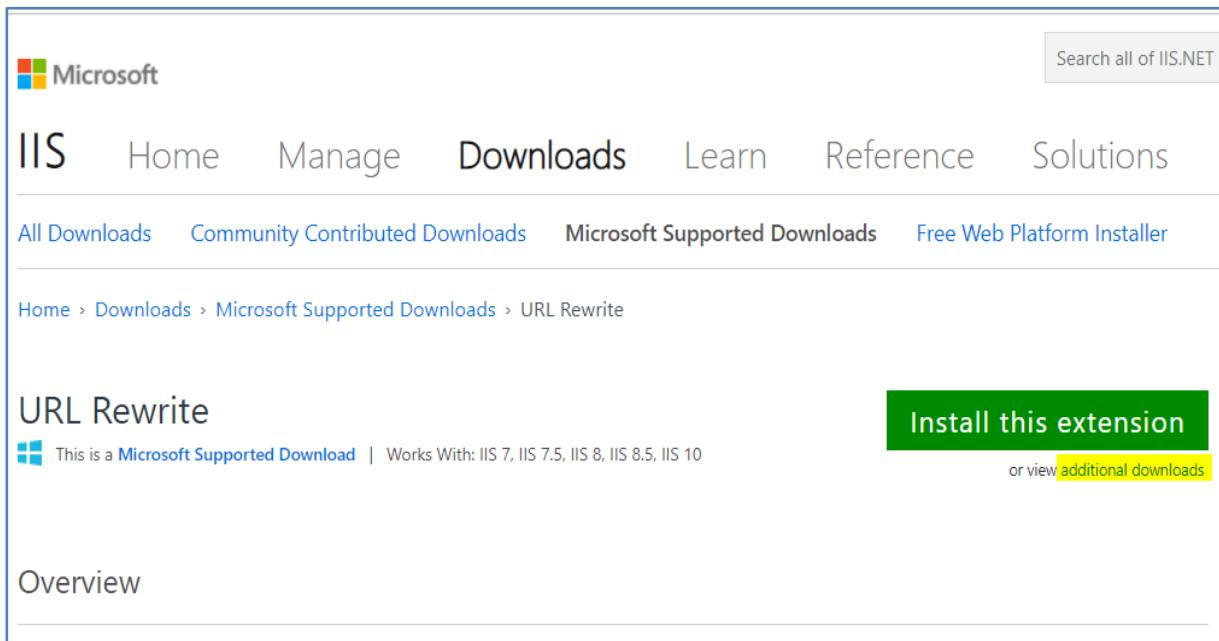
At this point, system is required to **restart** to apply these changes effectively.

2.5 Microsoft IIS URL Rewrite Module 2.1

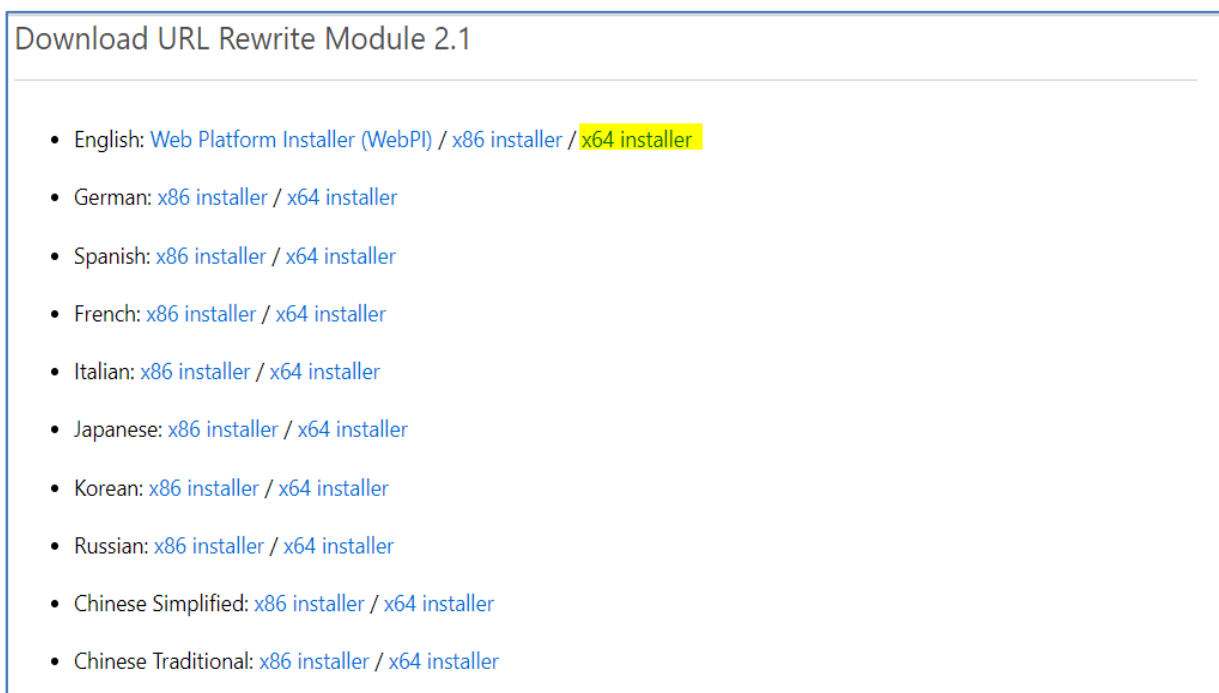
Download Microsoft IIS URL rewrite module 2.1 from the following link:

- [Microsoft IIS URL Rewrite Module 2.1](#)

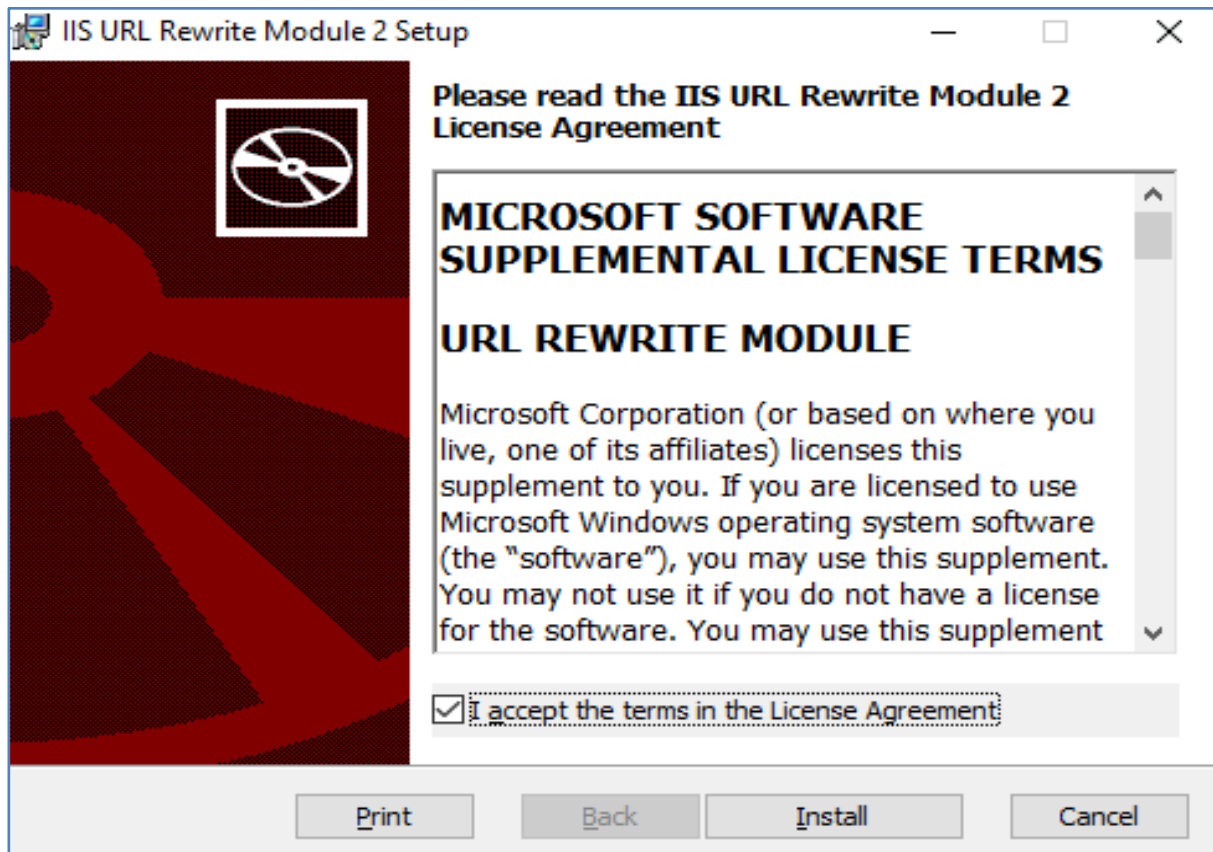
Navigating to this URL will present with the following screen:



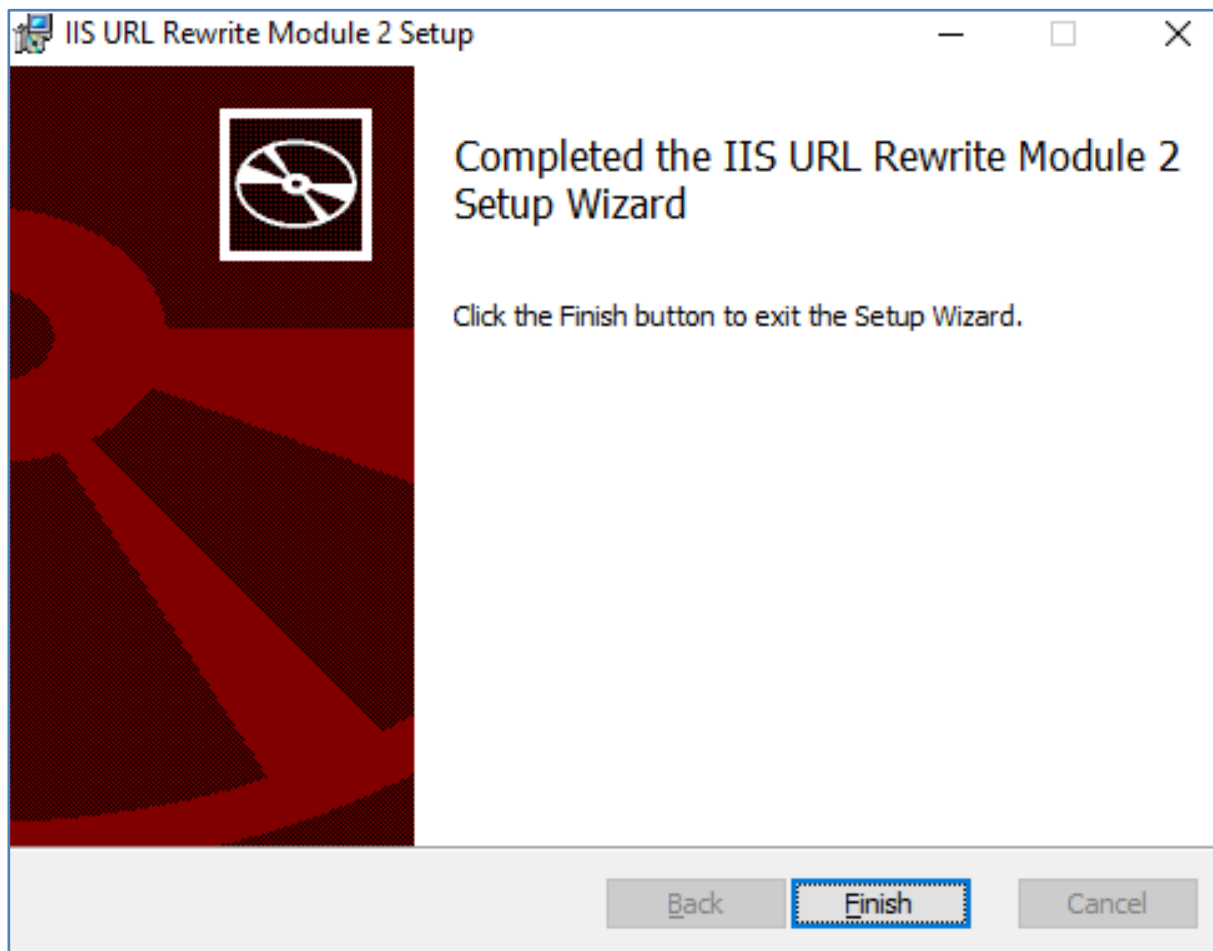
Clicking on the green **Install this extension** will install the extension on the current machine. For offline installers click **Additional Downloads** which will bring you down to the list of the installers



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



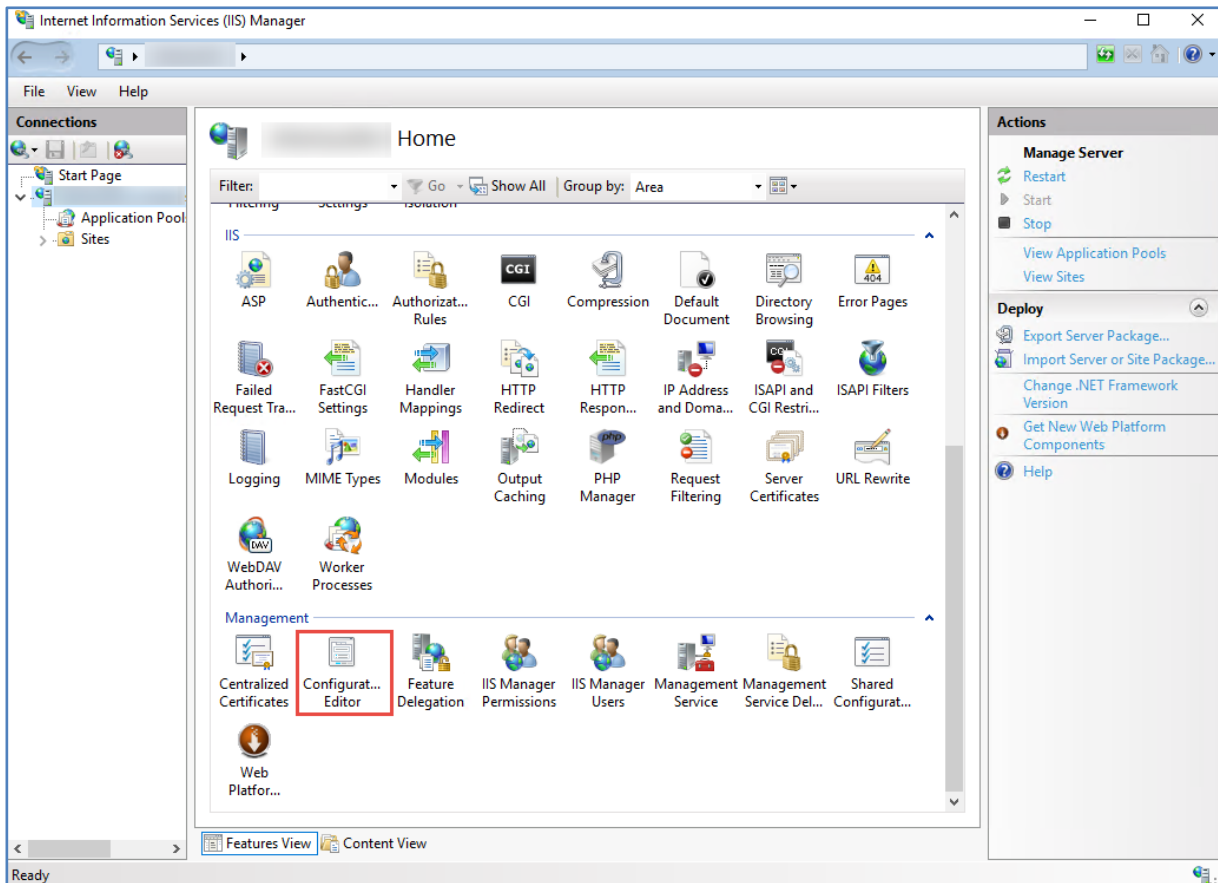
Accept the terms in the license agreement and click **Install** to proceed, the installation will take few minutes:



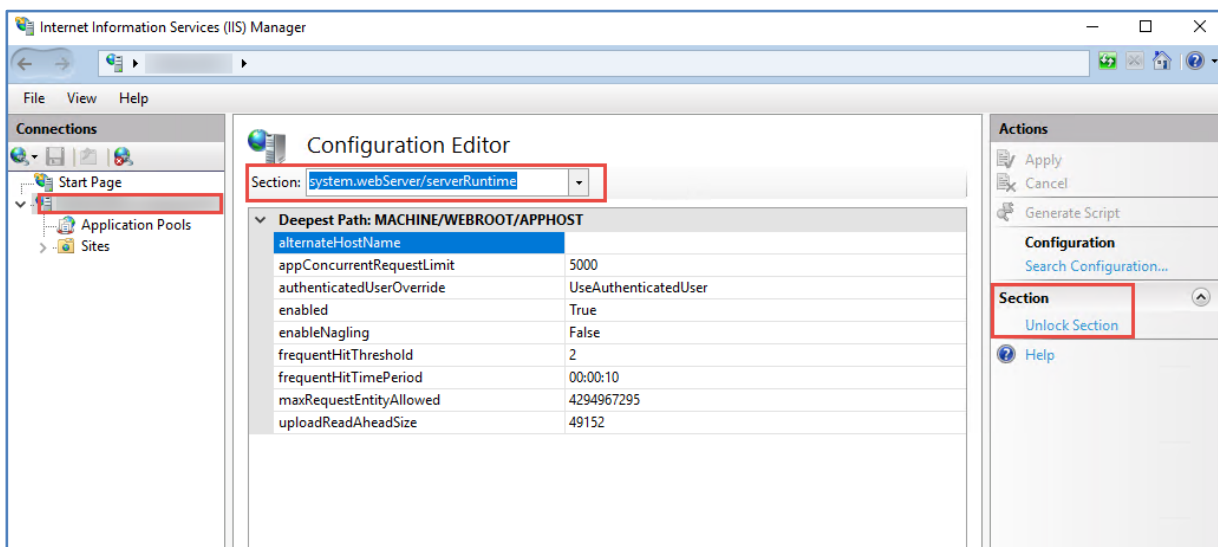
Click **Finish** once the installation is complete

2.6 Unlock system.webServer/serverRuntime section in IIS

1. Open IIS
2. Select Server from left panel
3. Open Configuration editor from right pane under Management section



4. Unlock system.webServer/serverRuntime section in configuration editor of IIS.



The installation process for prerequisites is complete.

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.

2.7 Database

Both ADSS Web RA and ADSS Server require their own respective databases. It is not needed 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 to manage certificates for 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, see details.
- **ADSS Web RA Device**
ADSS Web RA Device is used to manage device enrolment for certificate creation, renewal and revocation.

4 ADSS Web RA Installation

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.

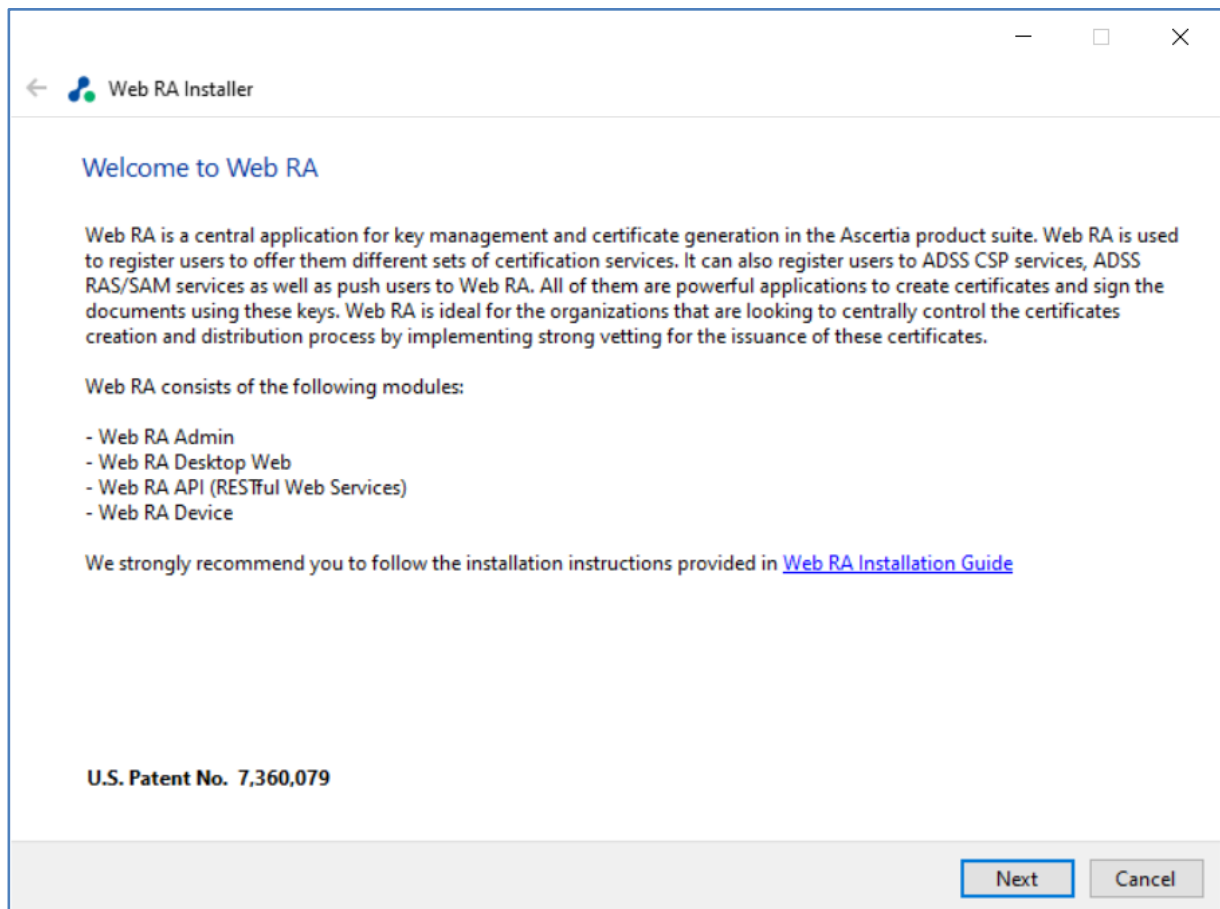
The ADSS Web RA package MUST be unzipped on to a disk that has sufficient space – a minimum of **100GB** is recommended. This is because the product is installed and runs from where the installation package is extracted to. Hence, choose a suitable location and naming structure. If you extract the installer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

Note: 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.

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

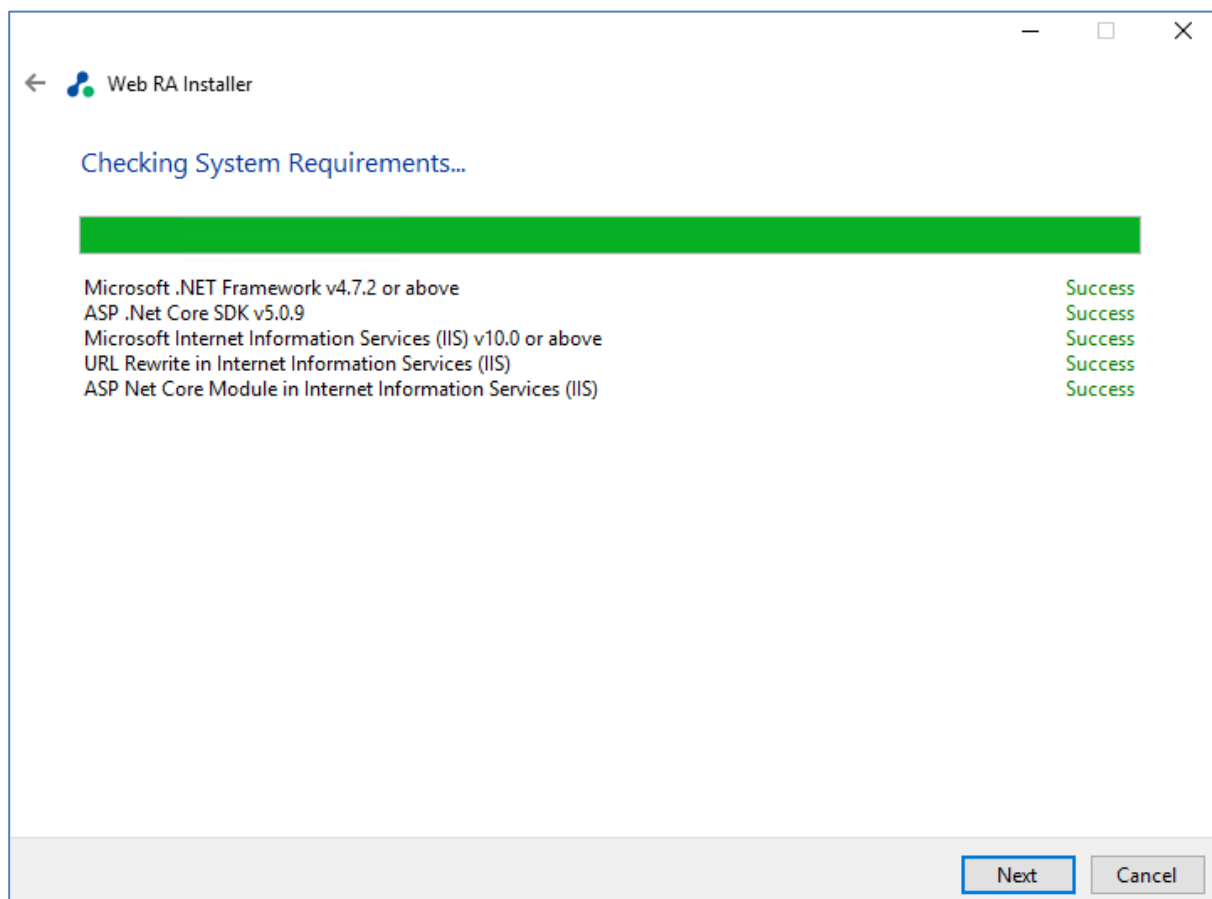
The following welcome screen is shown:



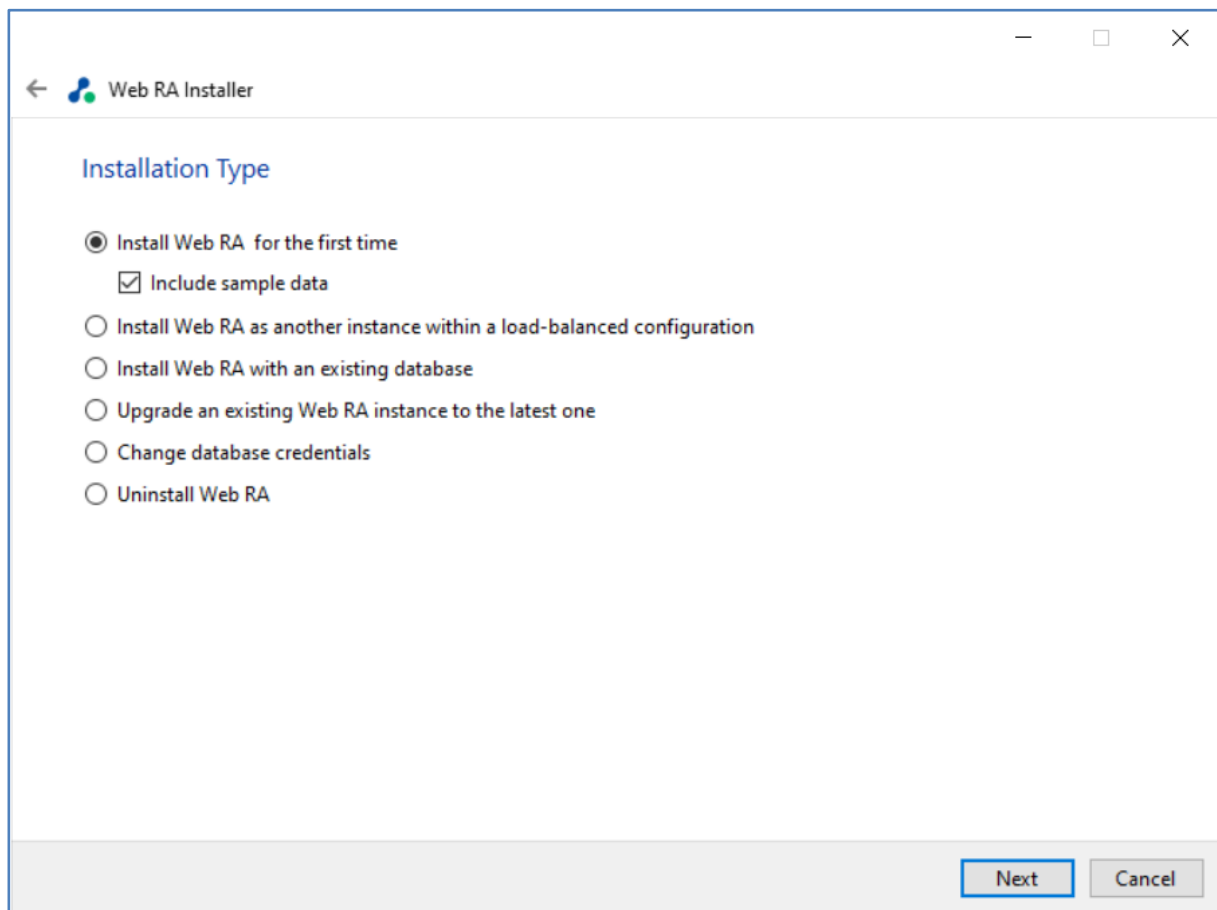
Click the '**Next**' button to continue.

A check of various operating system requirements is performed to check if the required prerequisites are installed or not. If any of the ADSS Web RA system dependencies is not found, or not functioning, then this will be reported on the screen.

Note you can only proceed with the installation once all issues related to system dependencies are resolved as shown here:



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.

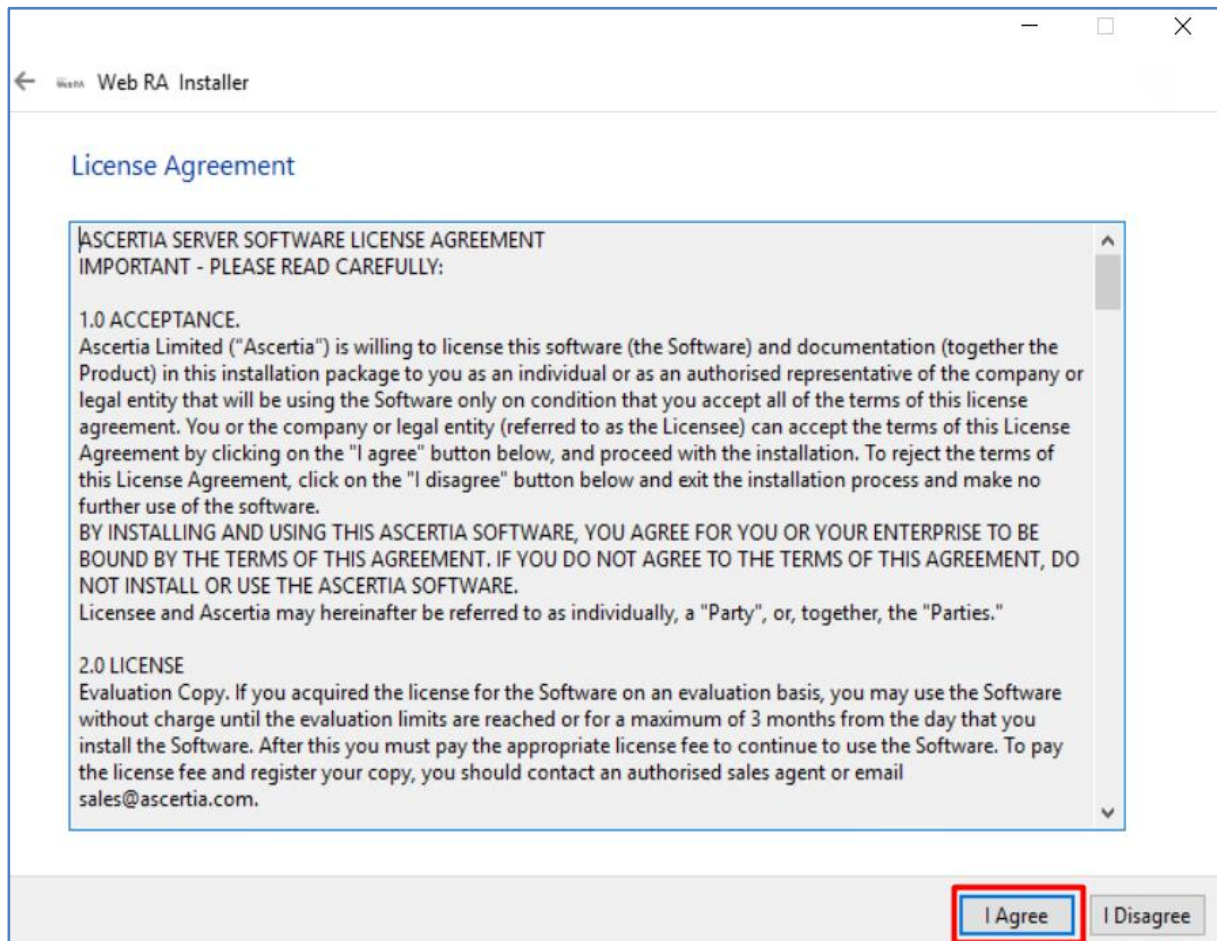
Select the option **Install Web RA for the first time**.

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.

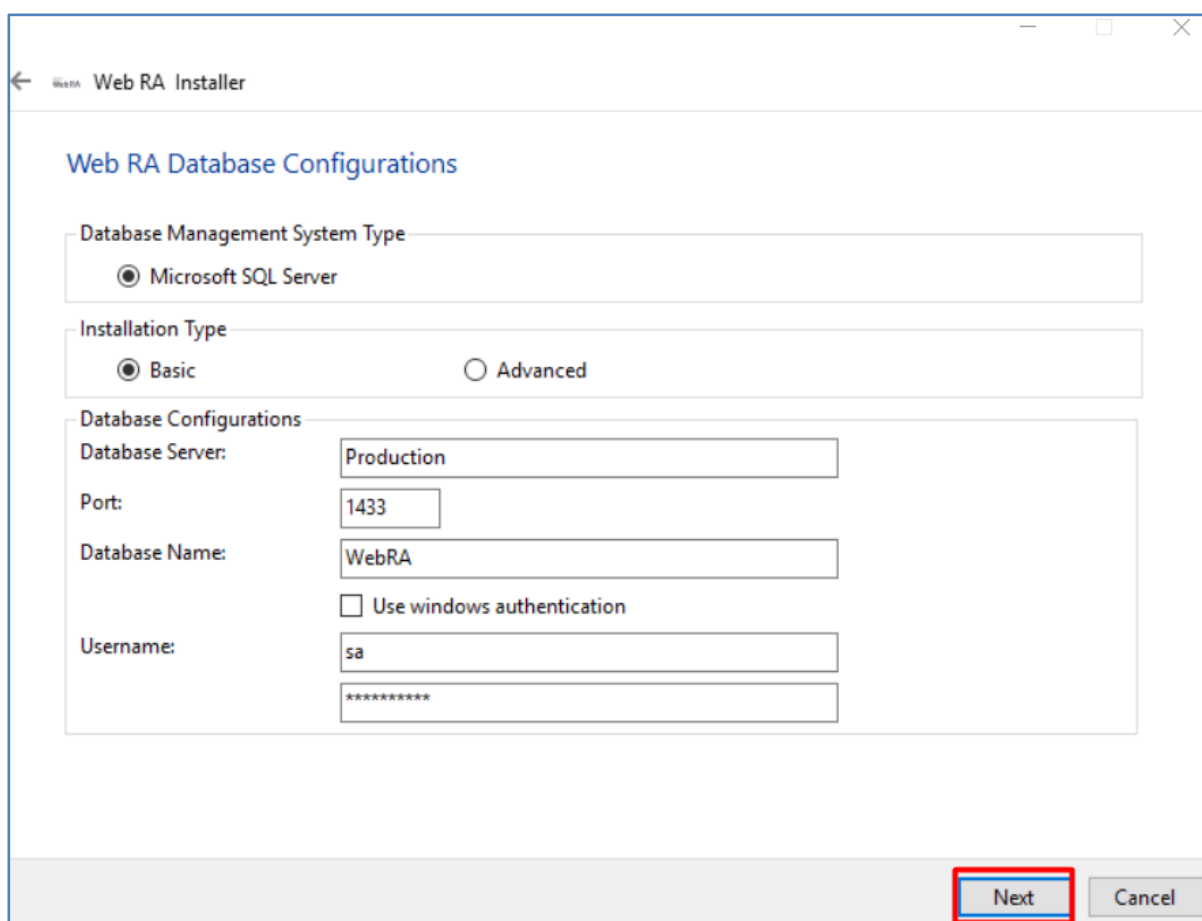
Click the **Next** button to show the License Agreement:



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

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

The following screen for database details will be displayed:



The image shows a screenshot of the 'Web RA Database Configurations' window from the 'Web RA Installer'. The window has a title bar with a back arrow, the text 'Web RA Installer', and standard window controls. The main content area is titled 'Web RA Database Configurations' in blue. It contains three sections: 'Database Management System Type' with a radio button selected for 'Microsoft SQL Server'; 'Installation Type' with radio buttons for 'Basic' (selected) and 'Advanced'; and 'Database Configurations' which includes text boxes for 'Database Server' (containing 'Production'), 'Port' (containing '1433'), 'Database Name' (containing 'WebRA'), 'Username' (containing 'sa'), and a password field (containing '*****'). There is an unchecked checkbox for 'Use windows authentication'. At the bottom right, there are 'Next' and 'Cancel' buttons, with the 'Next' button highlighted by a red rectangle.

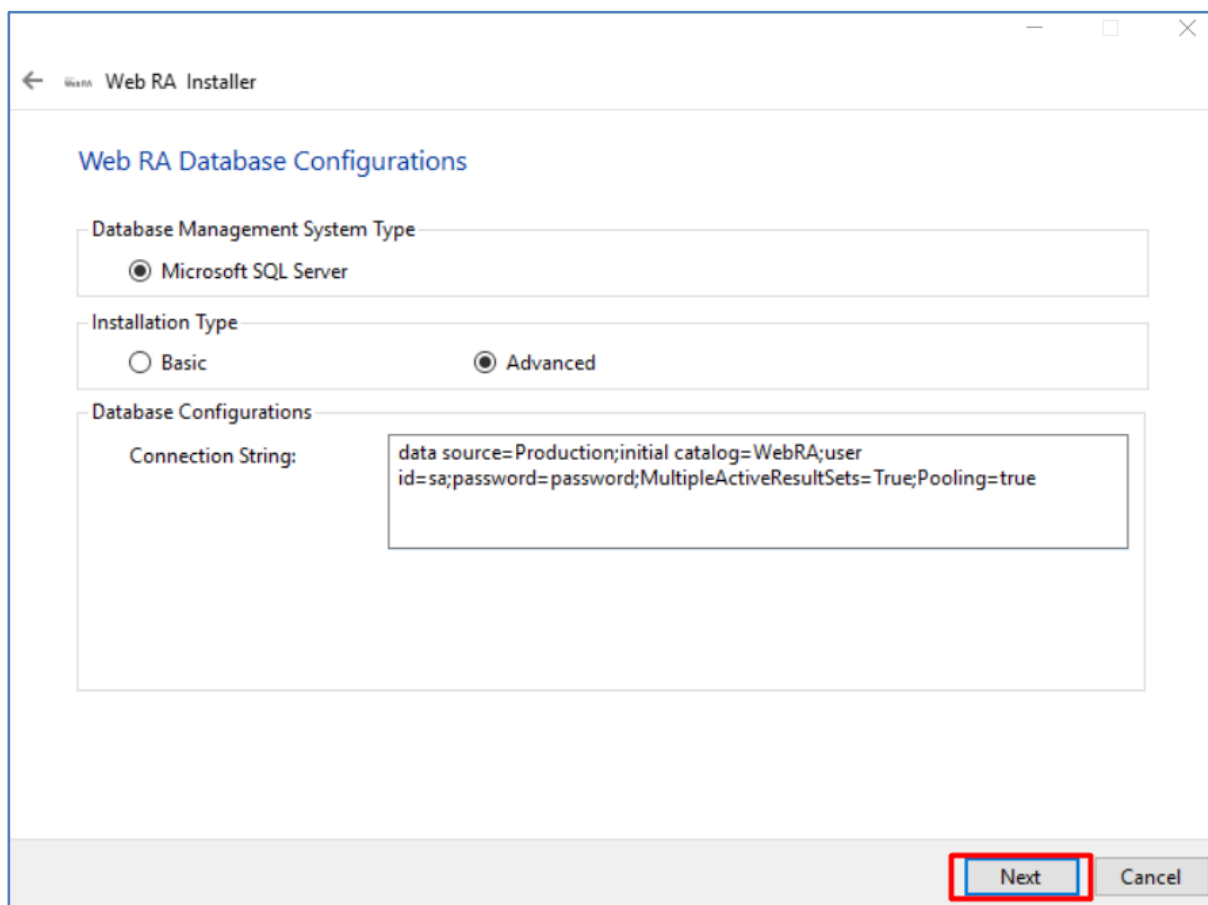
Furthermore, you can either choose to do a basic installation or use an advanced one. If this is a basic installation, then use the first option **Basic** and provide the appropriate ADSS Web RA database credentials. The information displayed above is an example and you should configure the relevant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

Note that 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 details the configuration options:

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	<p>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.</p> <p>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.</p> <p>If your requirement is to use SQL Server authentication, then type SQL Server Username and Password in the underneath fields without enabling this option.</p>
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 image shows a screenshot of the 'Web RA Database Configurations' window in the 'Web RA Installer'. The window has a title bar with a back arrow, 'Web RA Installer', and standard window controls. The main content area is titled 'Web RA Database Configurations' and contains three sections:

- Database Management System Type:** A radio button is selected for 'Microsoft SQL Server'.
- Installation Type:** Two radio buttons are present: 'Basic' and 'Advanced'. The 'Advanced' radio button is selected.
- Database Configurations:** A text box labeled 'Connection String:' contains the following text:


```
data source=Production;initial catalog=WebRA;user id=sa;password=password;MultipleActiveResultSets=True;Pooling=true
```

At the bottom right of the window, there are two buttons: 'Next' and 'Cancel'. The 'Next' button is highlighted with a red rectangular box.

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 details the configuration options:

Item	Description
ADSS Web RA Connection String	<p>The following are sample connection strings for SQL Server:</p> <ul style="list-style-type: none"> • 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"

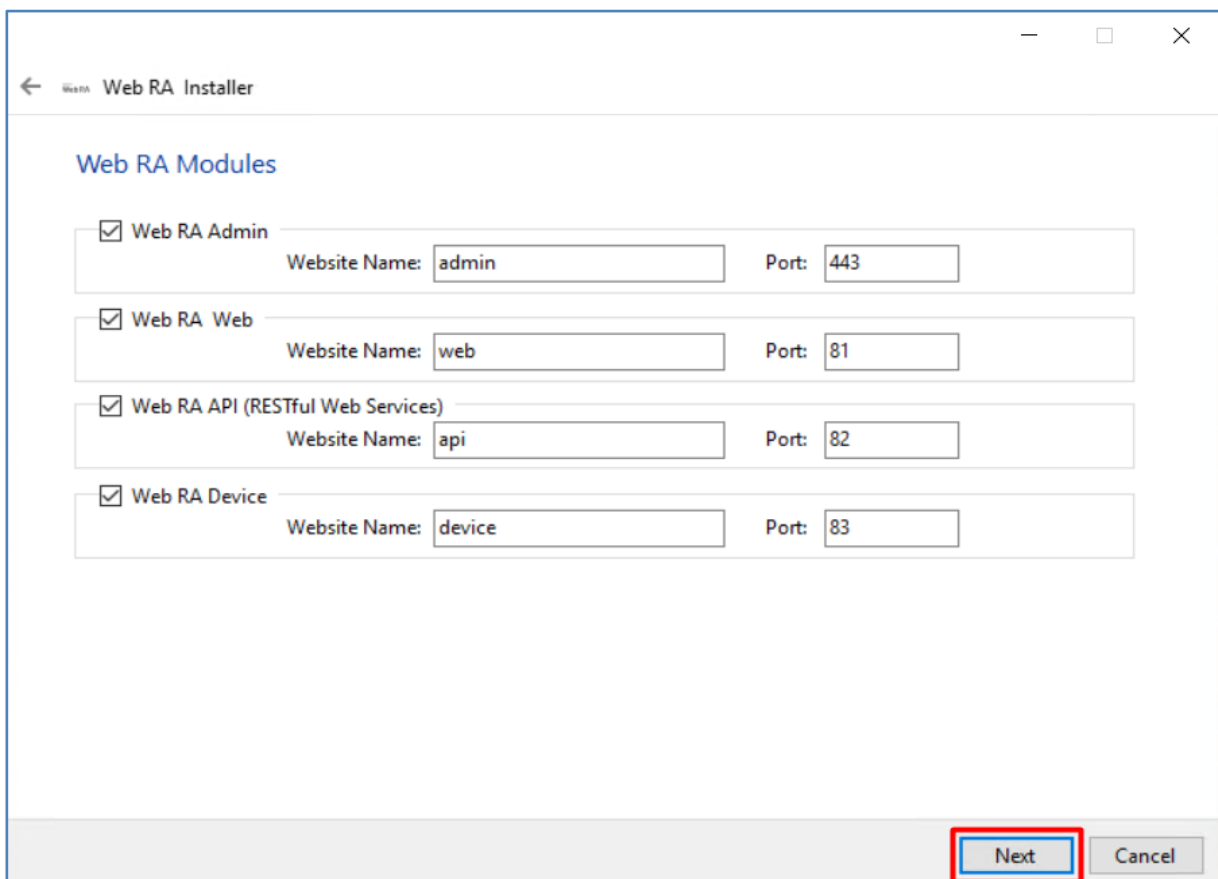
Username	Field will only be shown in case of Windows Authentication while for SQL Server Authentication, username will be provided in the connection string.
Password	In case of Windows Authentication, type the password of domain user shown in the Username field to configure the Application Pool Identity 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:

Click the **Next** button to select specific modules:



The screenshot shows the 'Web RA Modules' section of the 'Web RA Installer' window. It contains four rows, each with a checked checkbox, a label, a 'Website Name' text box, and a 'Port' text box. The 'Next' button at the bottom right is highlighted with a red rectangle.

Module	Website Name	Port
<input checked="" type="checkbox"/> Web RA Admin	admin	443
<input checked="" type="checkbox"/> Web RA Web	web	81
<input checked="" type="checkbox"/> Web RA API (RESTful Web Services)	api	82
<input checked="" type="checkbox"/> Web RA Device	device	83

Next Cancel

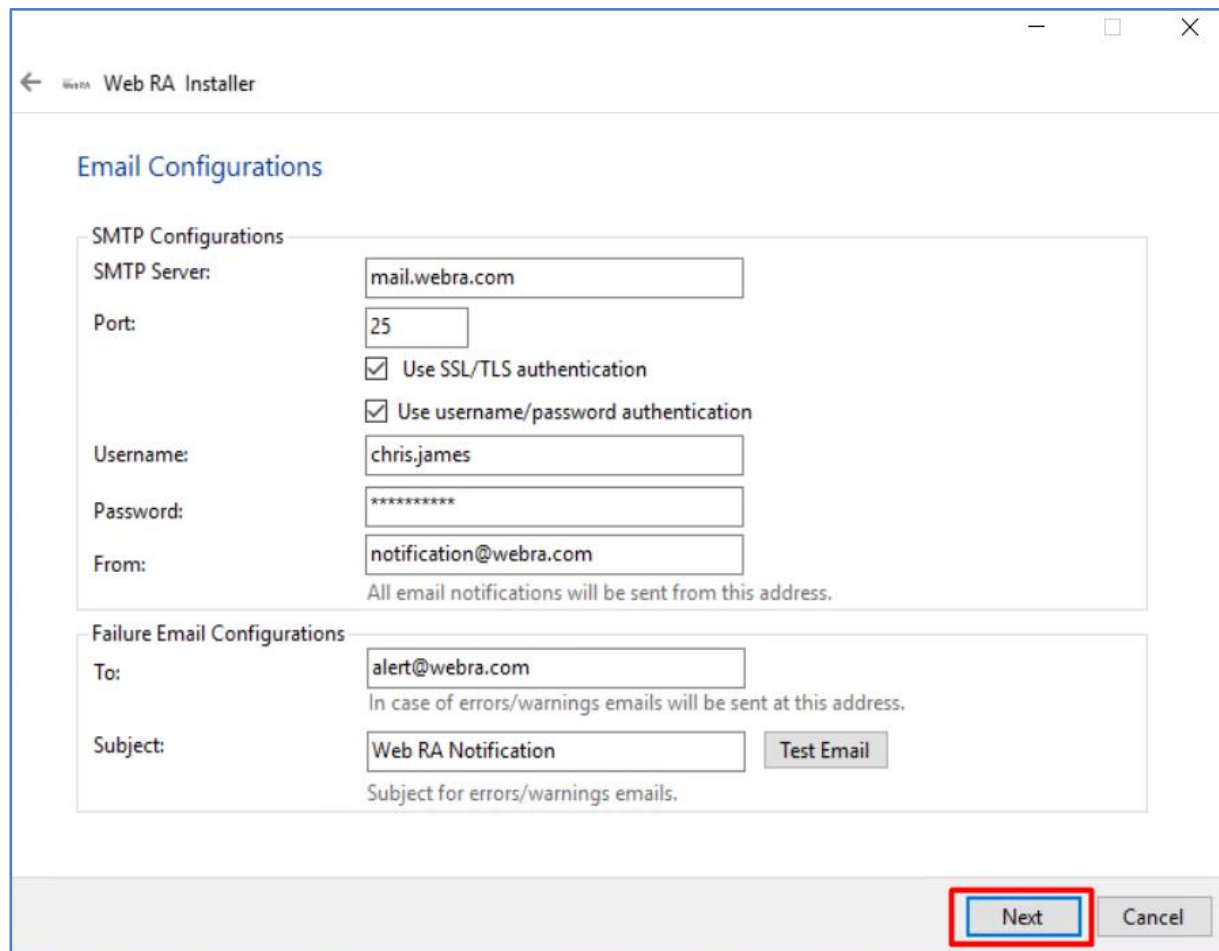
Select the appropriate modules to install the required features. For each selected application, provide the web application name and port. A typical in-house installation of ADSS Web RA should only include Admin, Desktop Web, and the API and lastly, the device will be added.

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.

The following table details the modules options:

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

Click the **Next** button to configure the SMTP server and email settings:



Web RA Installer

Email Configurations

SMTP Configurations

SMTP Server: mail.webra.com

Port: 25

☒ Use SSL/TLS authentication

☒ Use username/password authentication

Username: chris.james

Password: *****

From: notification@webra.com
All email notifications will be sent from this address.

Failure Email Configurations

To: alert@webra.com
In case of errors/warnings emails will be sent at this address.

Subject: Web RA Notification Test Email
Subject for errors/warnings emails.

Next Cancel

Configure the 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 sign-up process. In addition, administration notification and alert emails will also not be sent. Although the latter will not prevent functionality, but it is not a recommended approach. The information displayed above is an example and you should configure the relevant settings for your own environment.

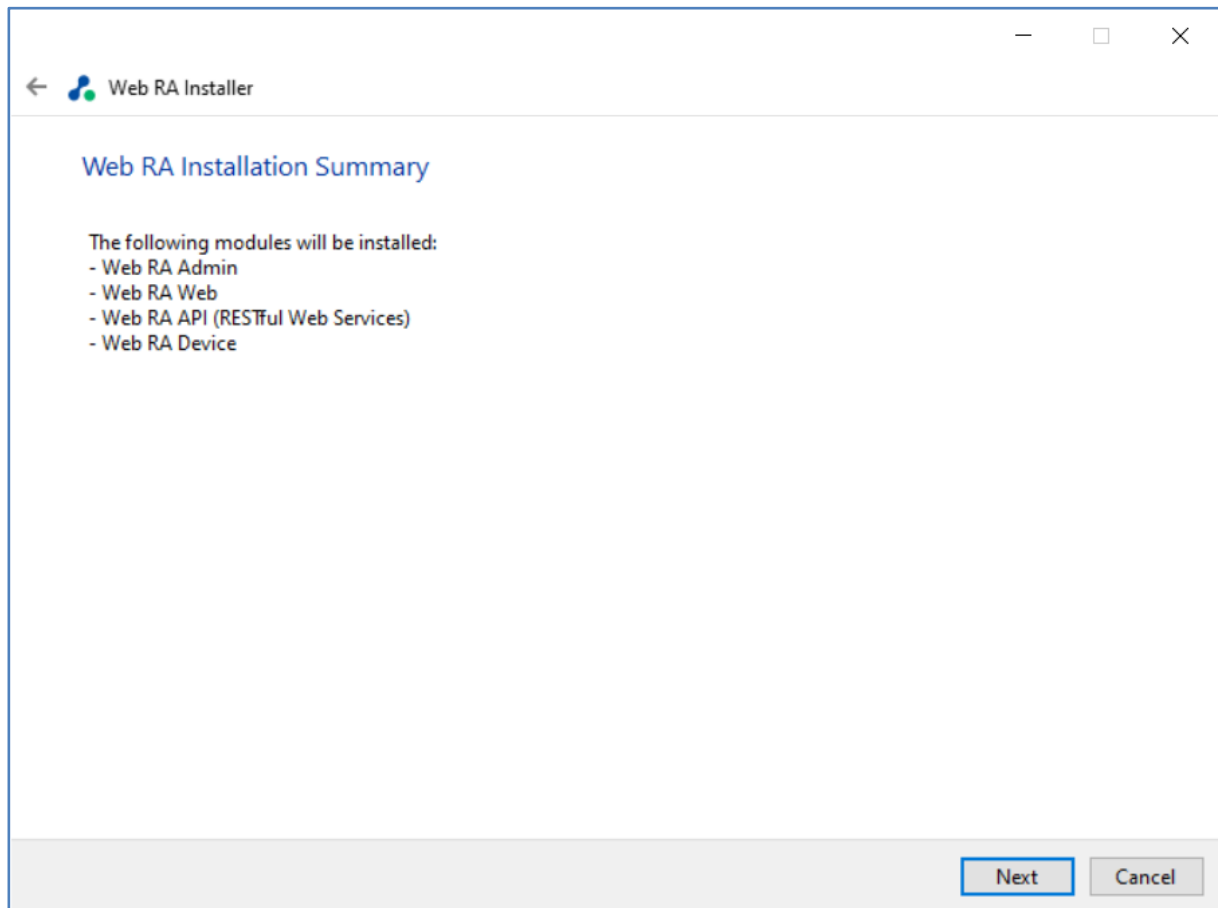
The configuration items are explained in the following table:

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.
Email 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.

Note: If “Include Sample Data” is not selected then SMTP configuration screen will not be shown.

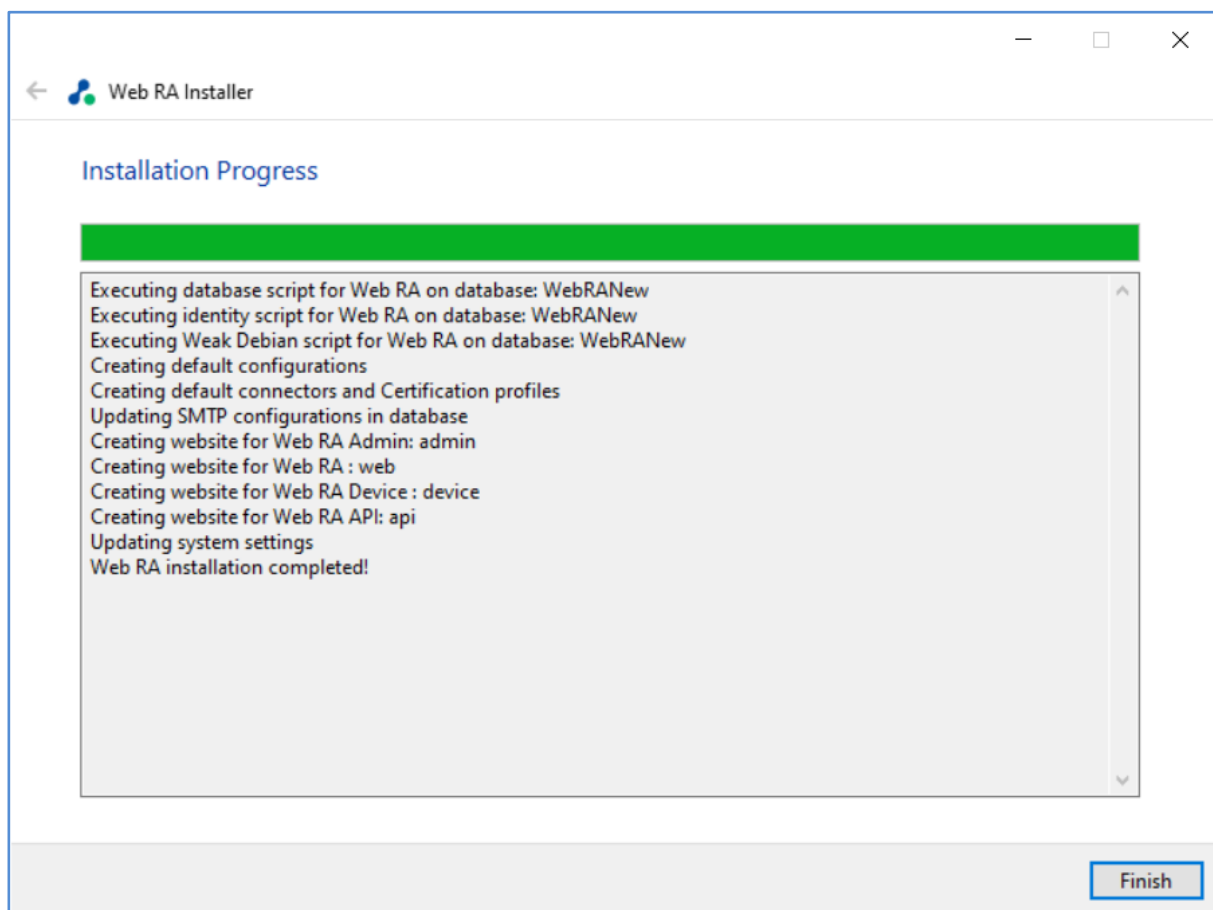
Click the **Next** button to see the summary and complete the installation:



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.

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



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

4.1.1 ADSS Web RA URLs

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

Service	URL Format	Example
ADSS Web RA Admin	<a href="https://<machine-name>:PORT">https://<machine-name>:PORT	https://localhost:443
ADSS Web RA Desktop Web	<a href="https://<machine-name>:PORT">https://<machine-name>:PORT	https://localhost:81
ADSS Web RA API	<a href="https://<machine-name>:PORT">https://<machine-name>:PORT	https://localhost:82
ADSS Web RA Device	<a href="https://<machine-name>:PORT">https://<machine-name>:PORT	https://localhost:83

Where necessary (i.e. browsing Admin website) your web browser will prompt you to select the appropriate certificate for authentication purposes. Note 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:

1. 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.
2. 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 done save the changes and publish them.



Option 2 is recommended.

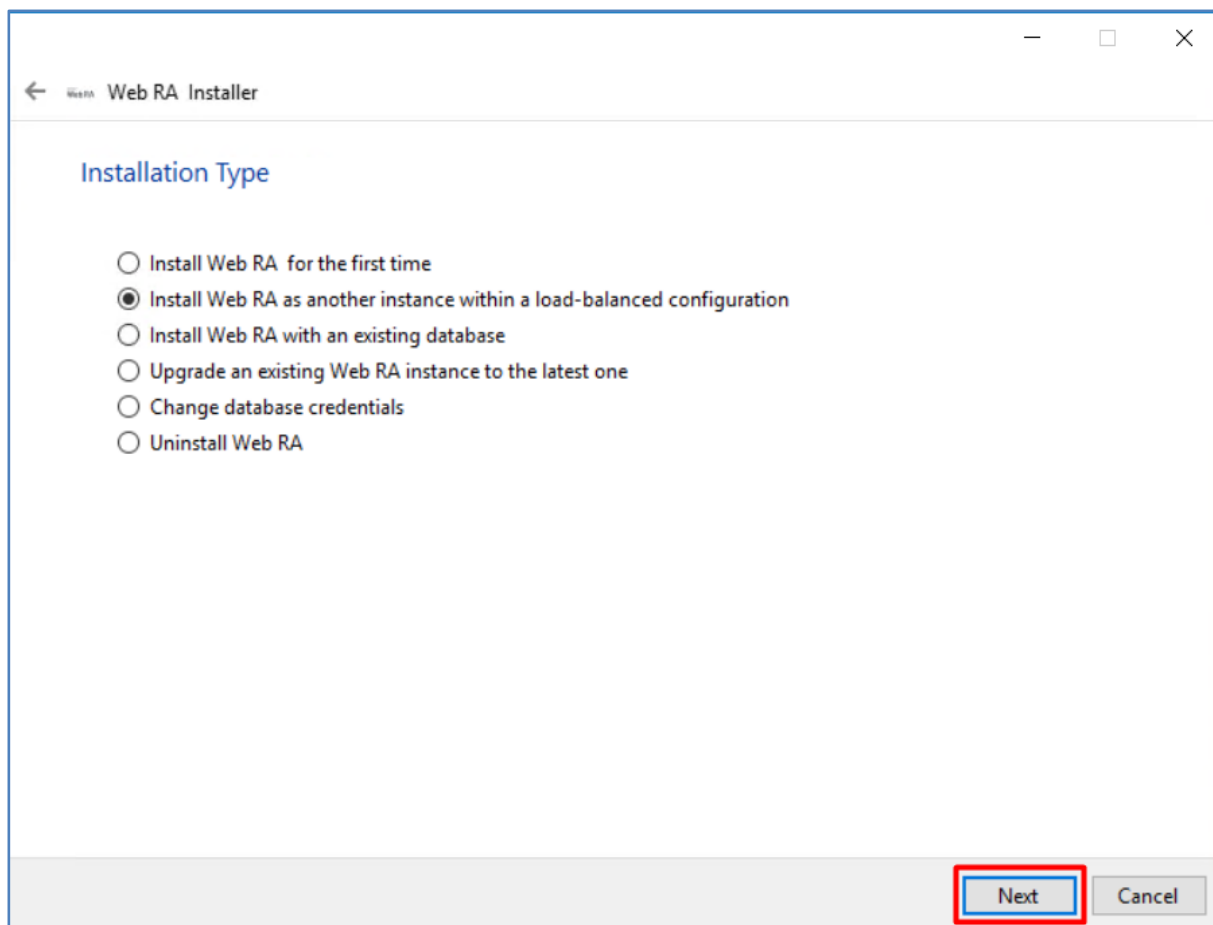
4.2 Installing ADSS Web RA with A Load-Balanced Configuration

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

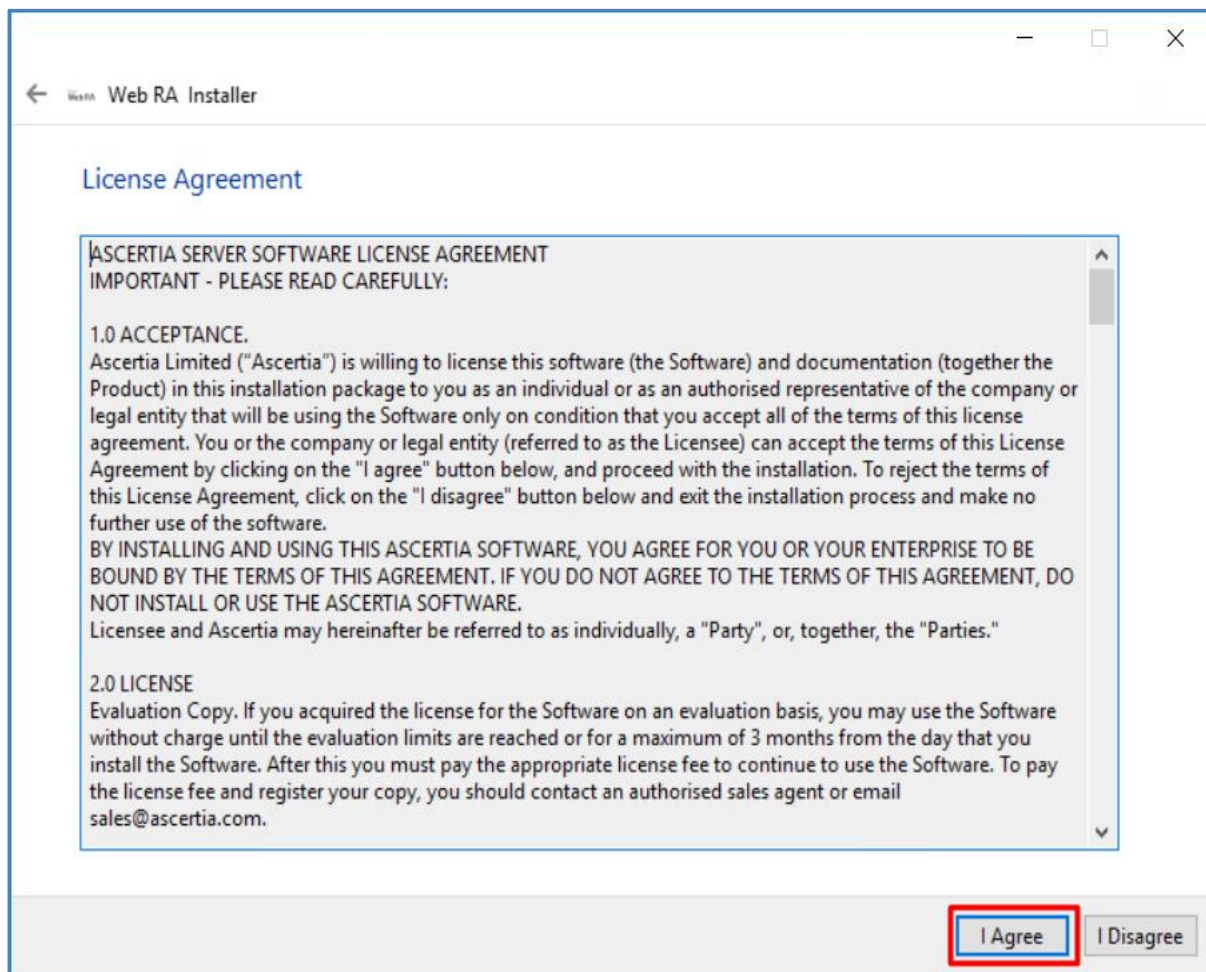
Launch the installer by right-clicking the file name **[Web RA Installation Directory]/setup/install.bat** and select **Run as administrator**.

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

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



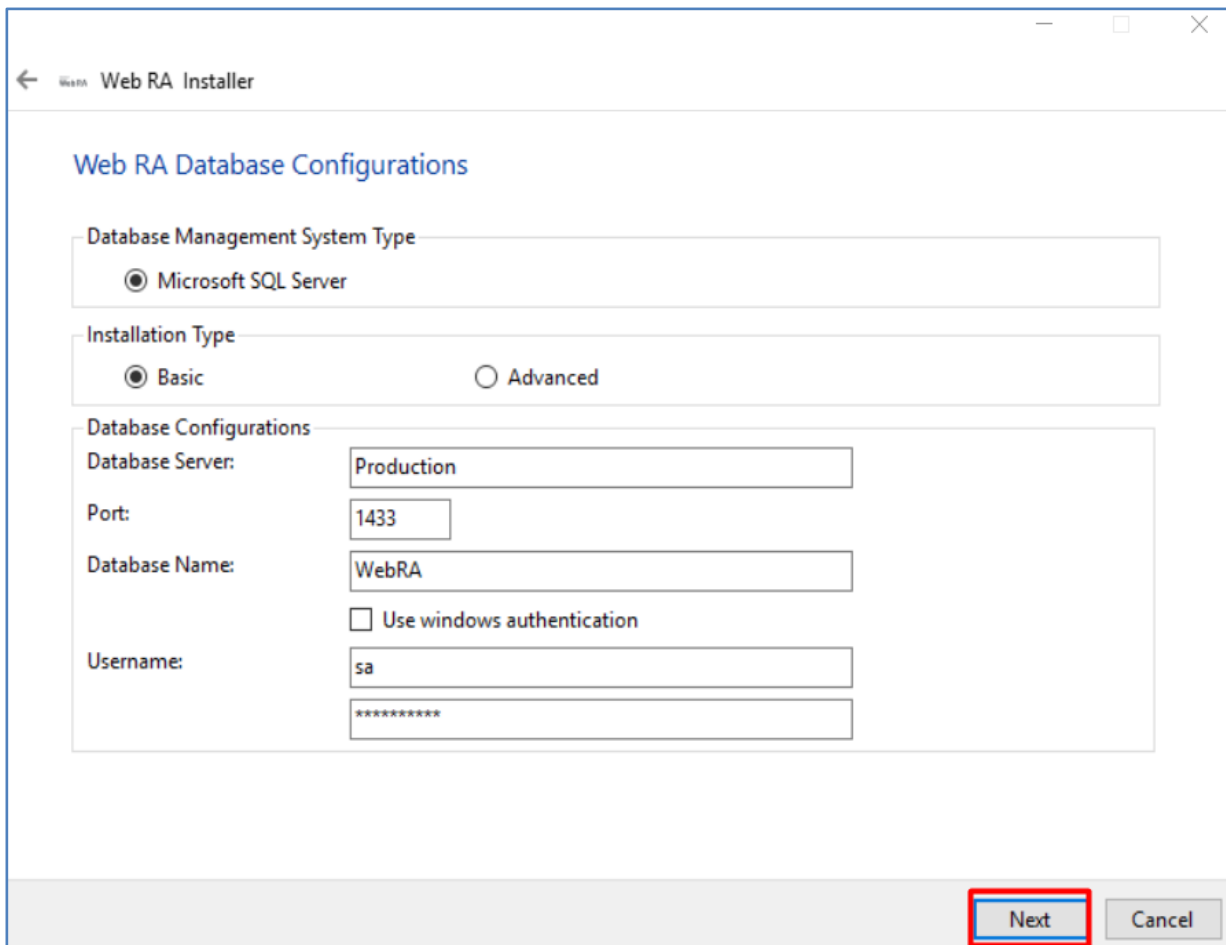
Click the **Next** button to show the License Agreement:



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

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

The following screen for database details will be displayed:



The screenshot shows the 'Web RA Database Configurations' window of the 'Web RA Installer'. The window has a title bar with a back arrow, 'Web RA', and 'Web RA Installer'. The main content area is titled 'Web RA Database Configurations' and contains three sections: 'Database Management System Type' with a radio button for 'Microsoft SQL Server'; 'Installation Type' with radio buttons for 'Basic' (selected) and 'Advanced'; and 'Database Configurations' which includes fields for 'Database Server' (Production), 'Port' (1433), 'Database Name' (WebRA), a checkbox for 'Use windows authentication' (unchecked), 'Username' (sa), and a password field (masked with asterisks). At the bottom right, there are 'Next' and 'Cancel' buttons, with the 'Next' button highlighted by a red rectangle.

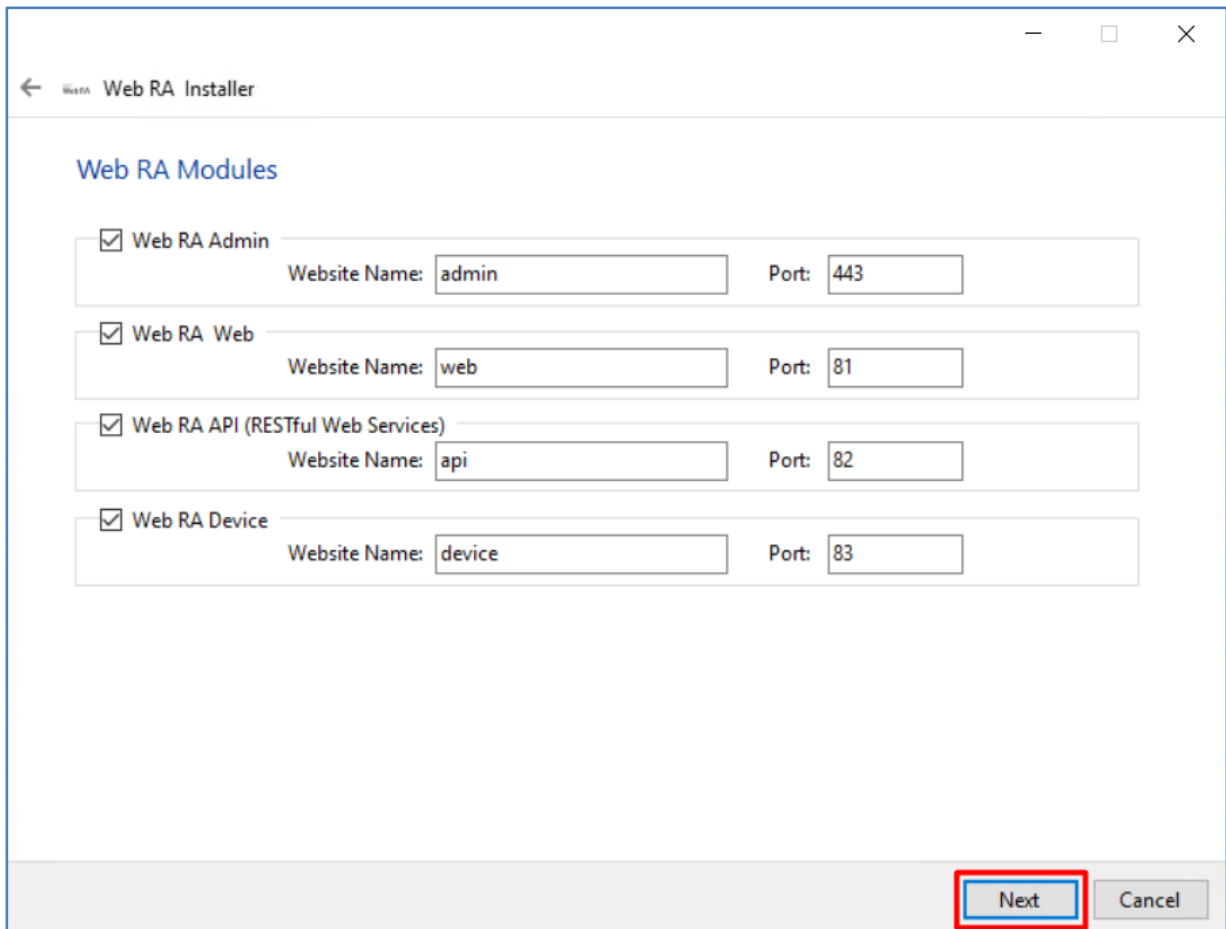
The information displayed above is an example and you should configure the relevant settings for your own environment.



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.*

Click the **Next** button to select specific modules.



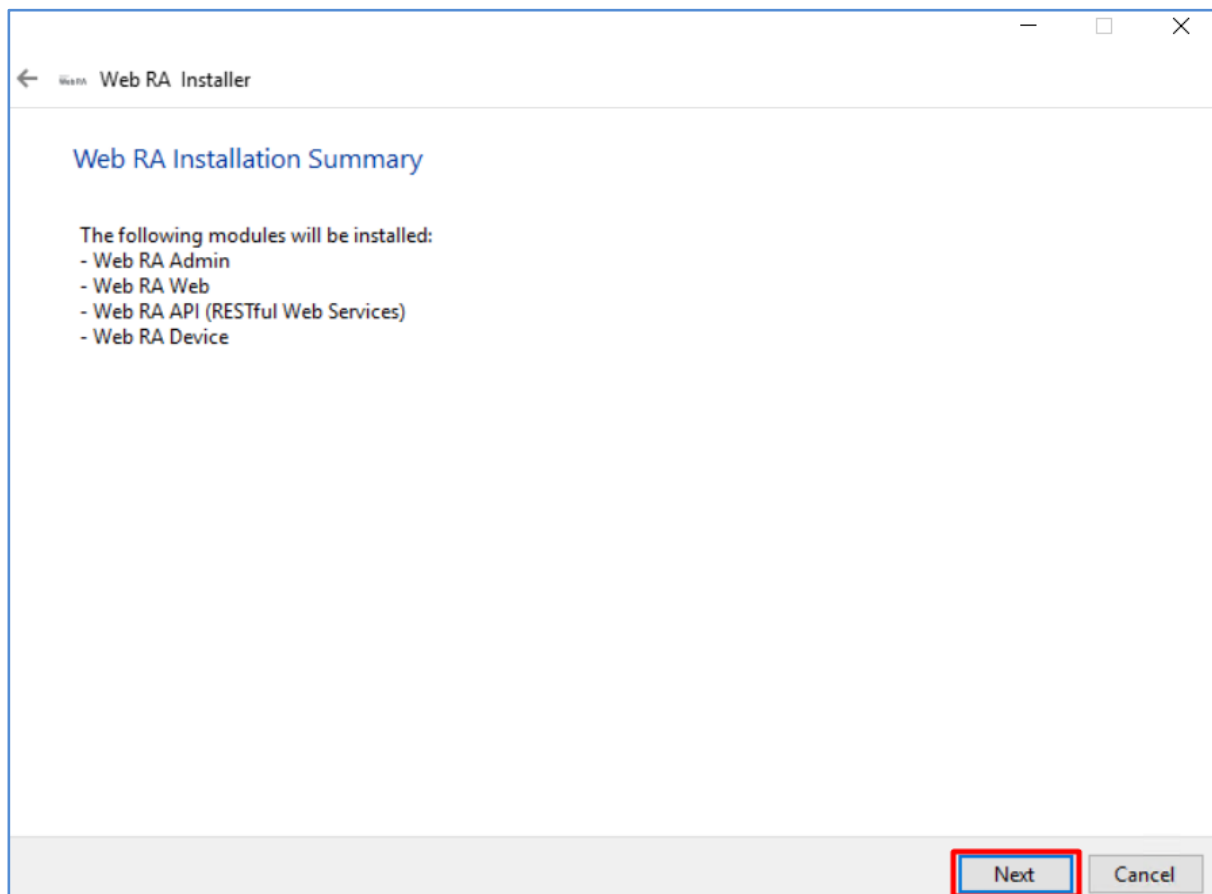
The image shows a screenshot of the 'Web RA Installer' window. The window has a title bar with a back arrow, the text 'Web RA Installer', and standard window controls (minimize, maximize, close). Below the title bar, the text 'Web RA Modules' is displayed. There are four modules listed, each with a checked checkbox, a 'Website Name' field, and a 'Port' field:

- ☒ Web RA Admin: Website Name: admin, Port: 443
- ☒ Web RA Web: Website Name: web, Port: 81
- ☒ Web RA API (RESTful Web Services): Website Name: api, Port: 82
- ☒ Web RA Device: Website Name: device, Port: 83

At the bottom right of the window, there are two buttons: 'Next' and 'Cancel'. The 'Next' button is highlighted with a red rectangular box.

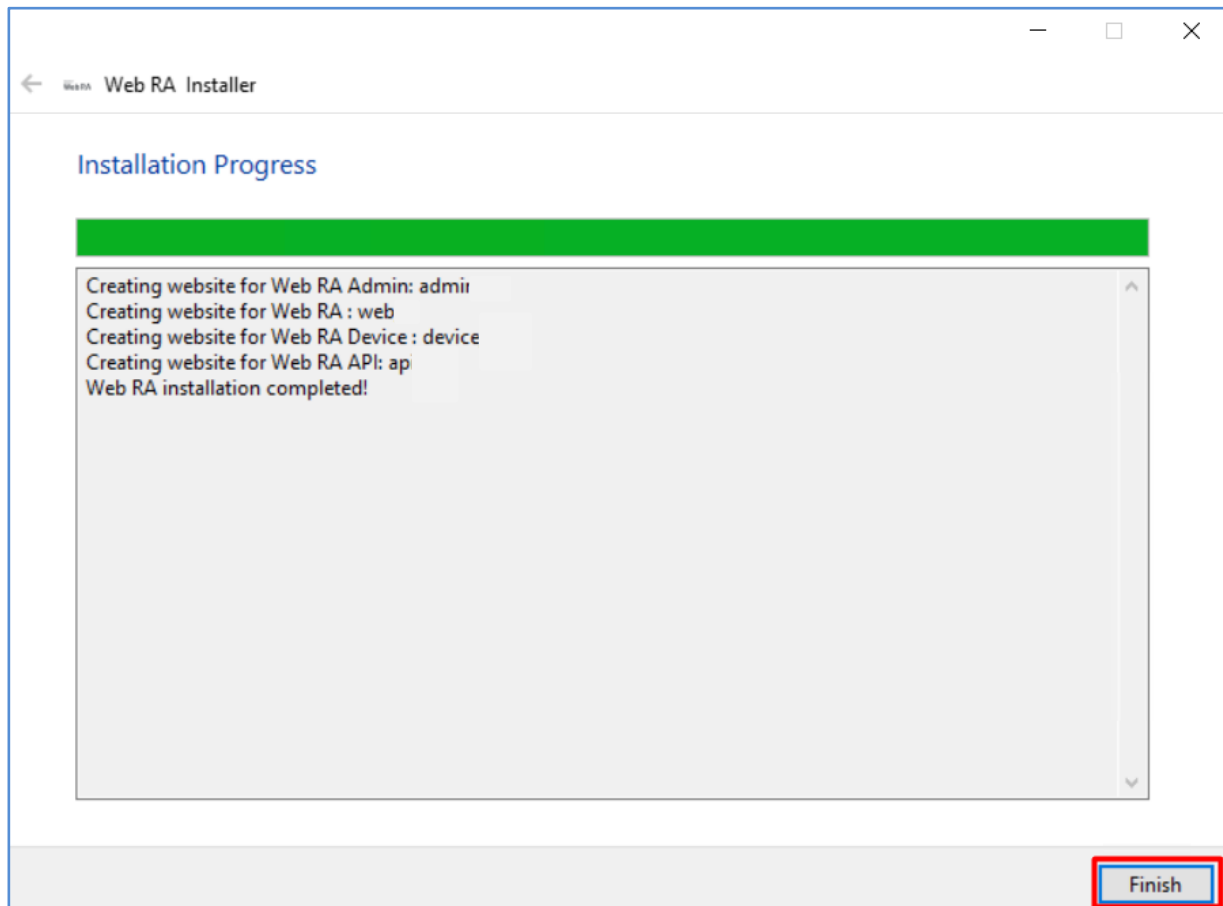
Select the appropriate modules to install the required features.

Click the **Next** button to show the summary and complete the installation:



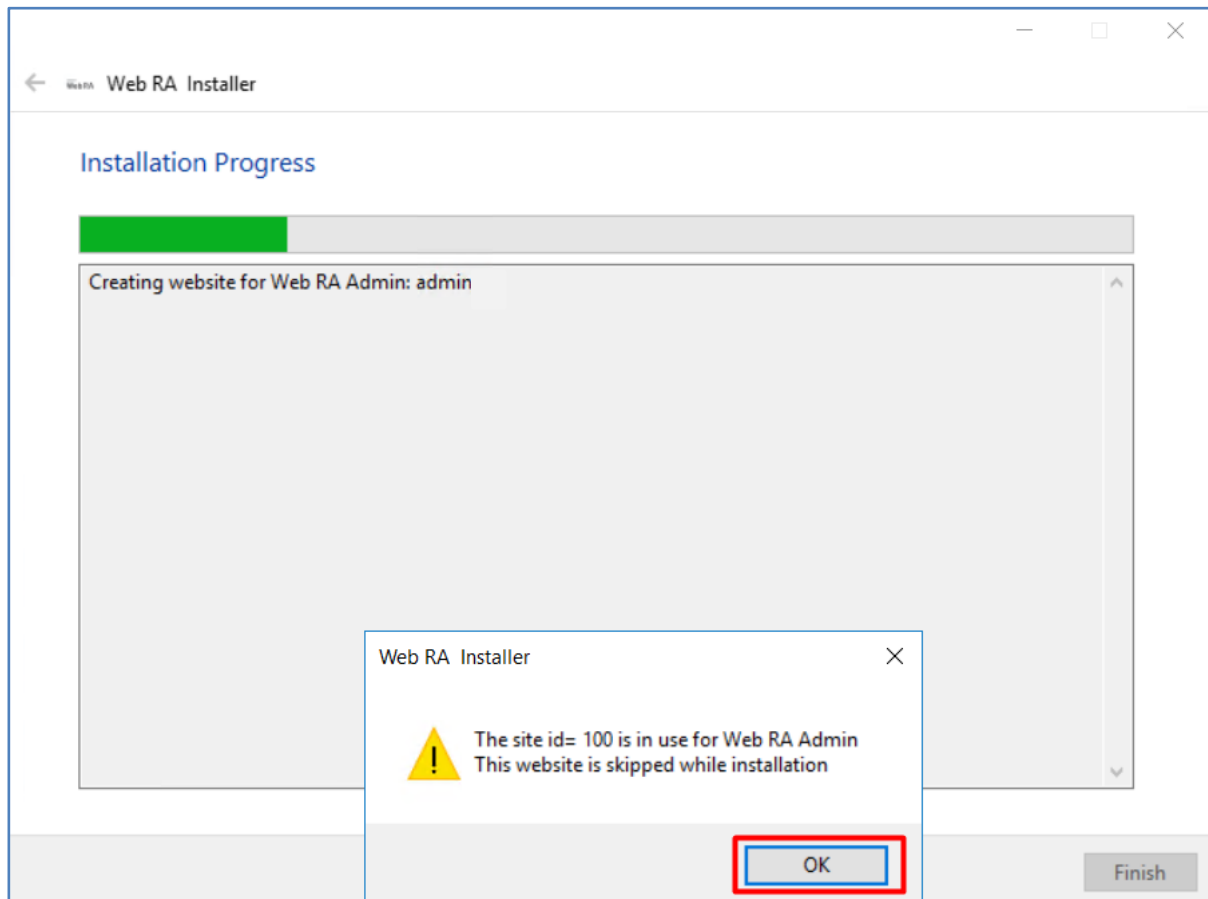
This screen shows the installation summary by listing the different product modules that will be installed.

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.



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

In case of an error message, as shown below, click **OK** to continue.



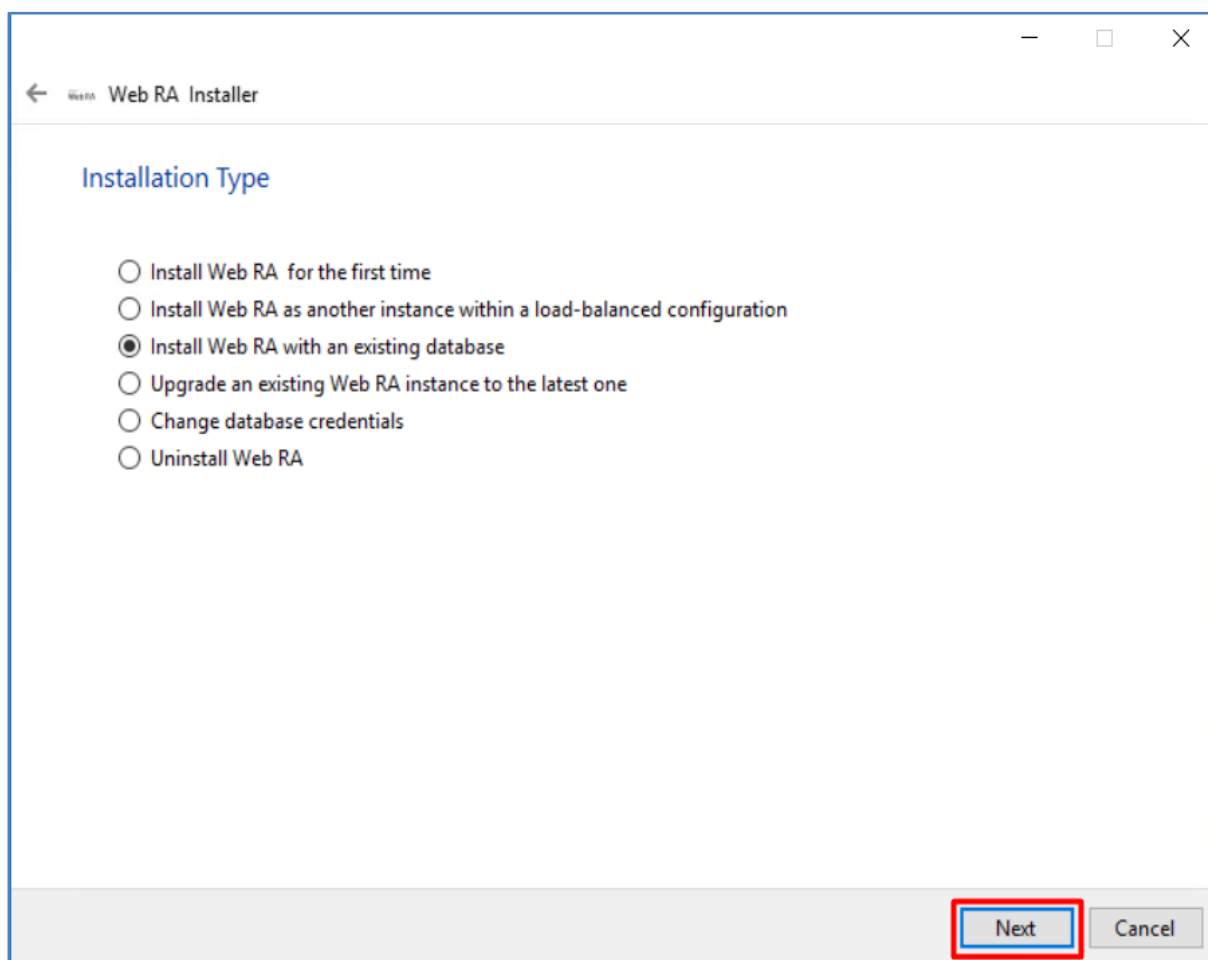
Click the **Finish** button to complete the installation process.

4.3 Installing ADSS Web RA with an Existing Database

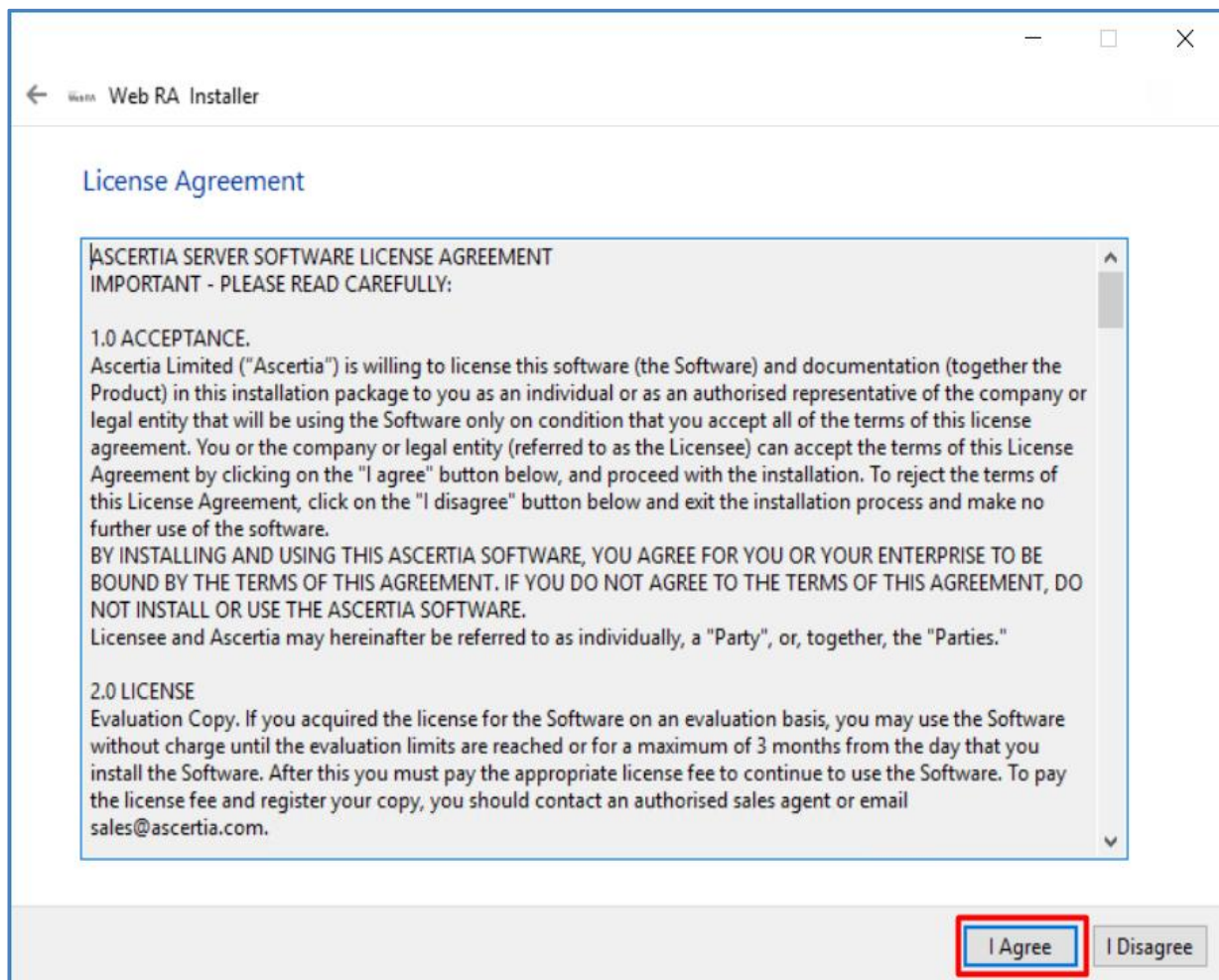
In order to install the ADSS Web RA with an existing database, follow the below mentioned installation instructions:

Launch the installer by right-clicking 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:

Select the option **Install ADSS Web RA within existing database**



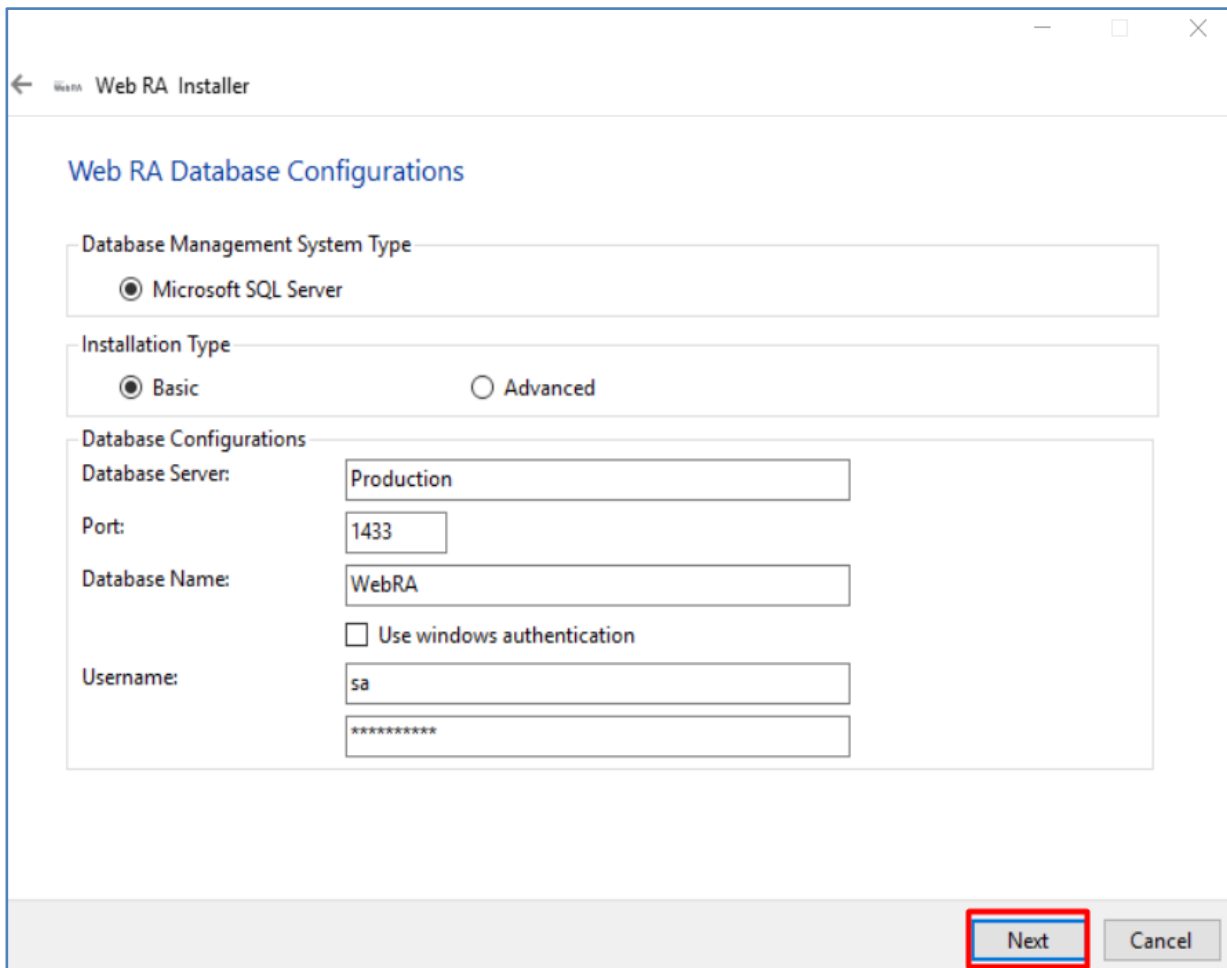
Click the **Next** button to show the License Agreement:



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

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

The following screen for database details will be displayed:



The screenshot shows the 'Web RA Database Configurations' window of the 'Web RA Installer'. The window has a title bar with a back arrow, 'Web RA Installer', and standard window controls. The main content area is titled 'Web RA Database Configurations' and contains three sections: 'Database Management System Type' with a radio button for 'Microsoft SQL Server'; 'Installation Type' with radio buttons for 'Basic' (selected) and 'Advanced'; and 'Database Configurations' which includes fields for 'Database Server' (Production), 'Port' (1433), 'Database Name' (WebRA), a checkbox for 'Use windows authentication' (unchecked), 'Username' (sa), and a password field (masked with asterisks). At the bottom right, there are 'Next' and 'Cancel' buttons, with the 'Next' button highlighted by a red rectangle.

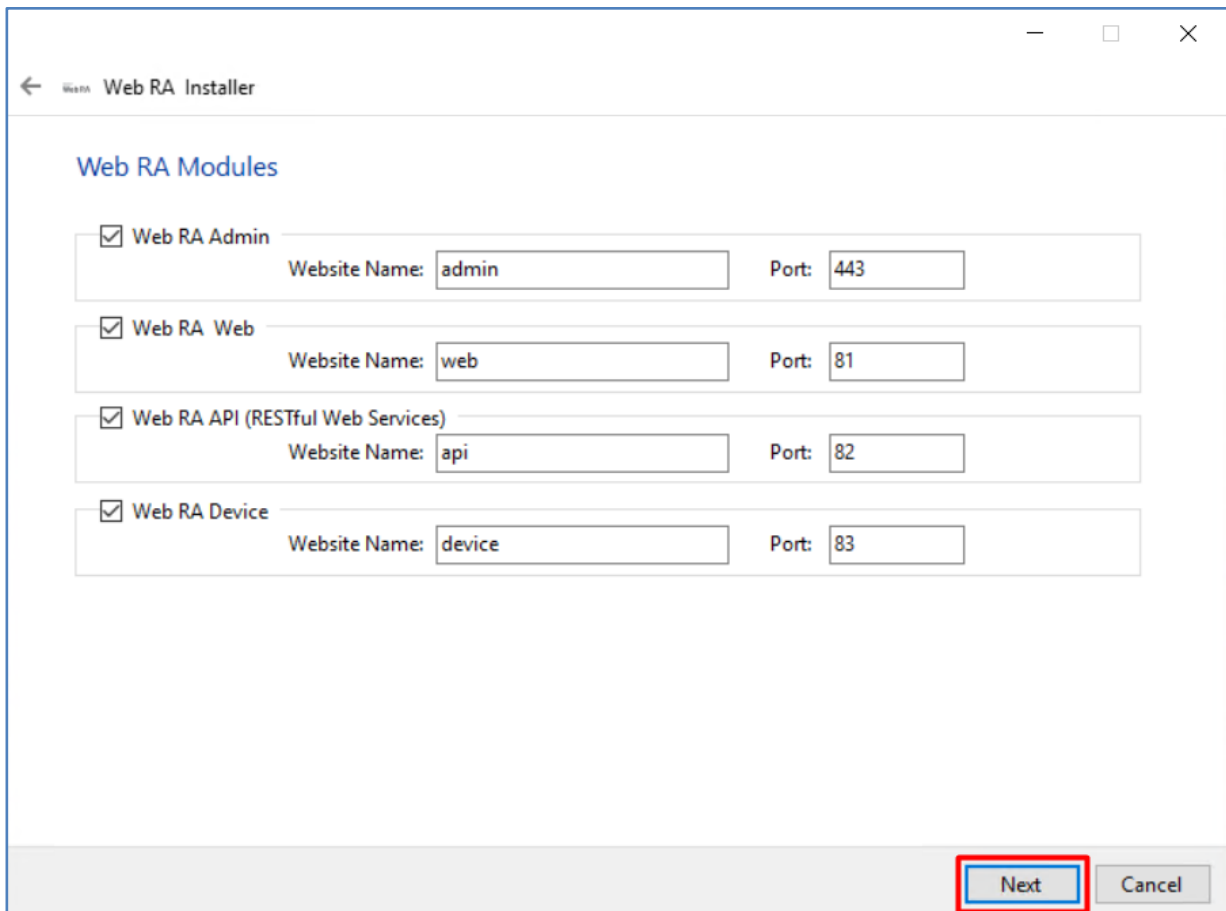
The information displayed above is an example and you should configure the relevant settings for your own environment.



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.*

Click the **Next** button to select specific modules.

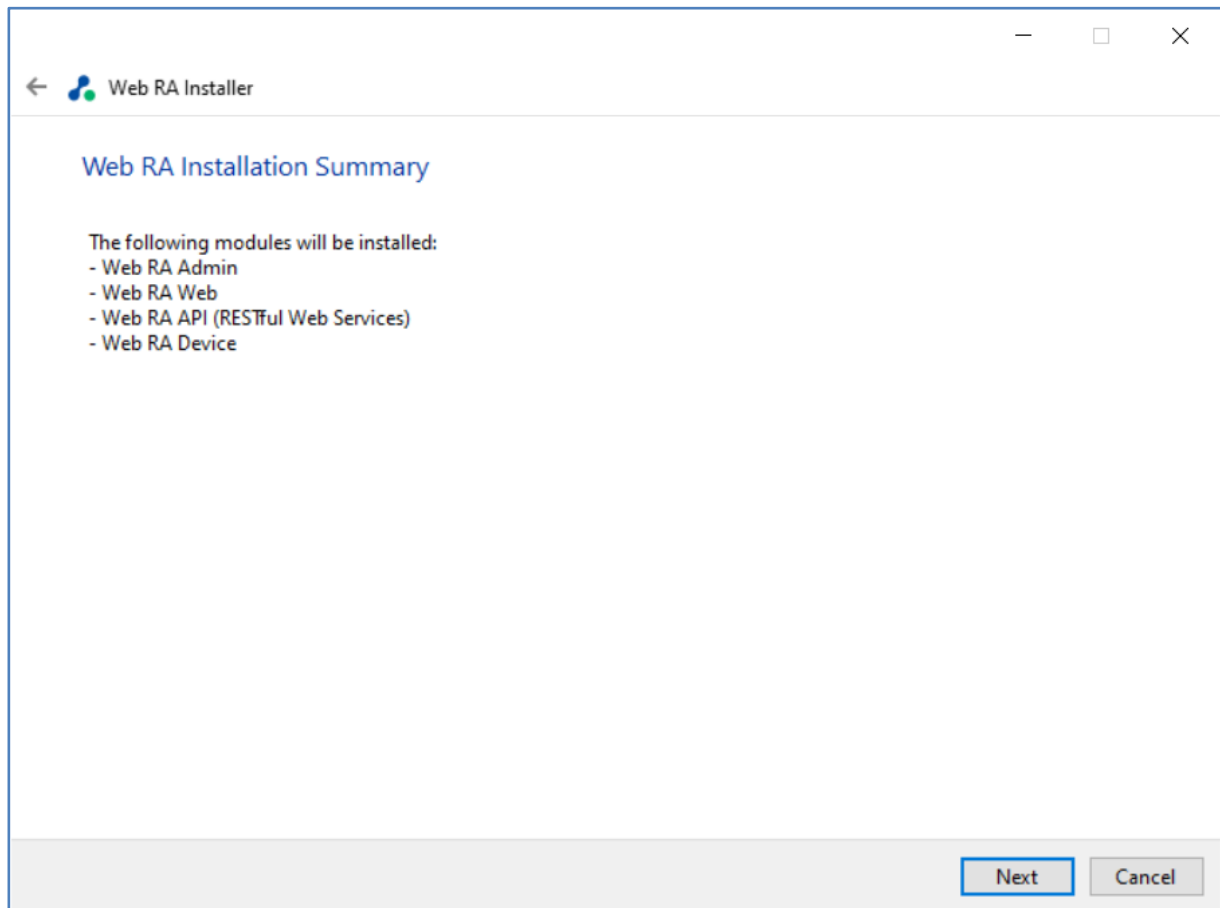


The image shows a screenshot of the 'Web RA Installer' window. The title bar includes a back arrow, the text 'Web RA', and the window title 'Web RA Installer'. The main content area is titled 'Web RA Modules' and contains four rows of module selection options. Each row has a checked checkbox, a label, a 'Website Name' text box, and a 'Port' text box. The modules are: 'Web RA Admin' (Website Name: admin, Port: 443), 'Web RA Web' (Website Name: web, Port: 81), 'Web RA API (RESTful Web Services)' (Website Name: api, Port: 82), and 'Web RA Device' (Website Name: device, Port: 83). At the bottom right, there are 'Next' and 'Cancel' buttons. The 'Next' button is highlighted with a red rectangular border.

Module	Website Name	Port
<input checked="" type="checkbox"/> Web RA Admin	admin	443
<input checked="" type="checkbox"/> Web RA Web	web	81
<input checked="" type="checkbox"/> Web RA API (RESTful Web Services)	api	82
<input checked="" type="checkbox"/> Web RA Device	device	83

Select the appropriate modules to install the required features.

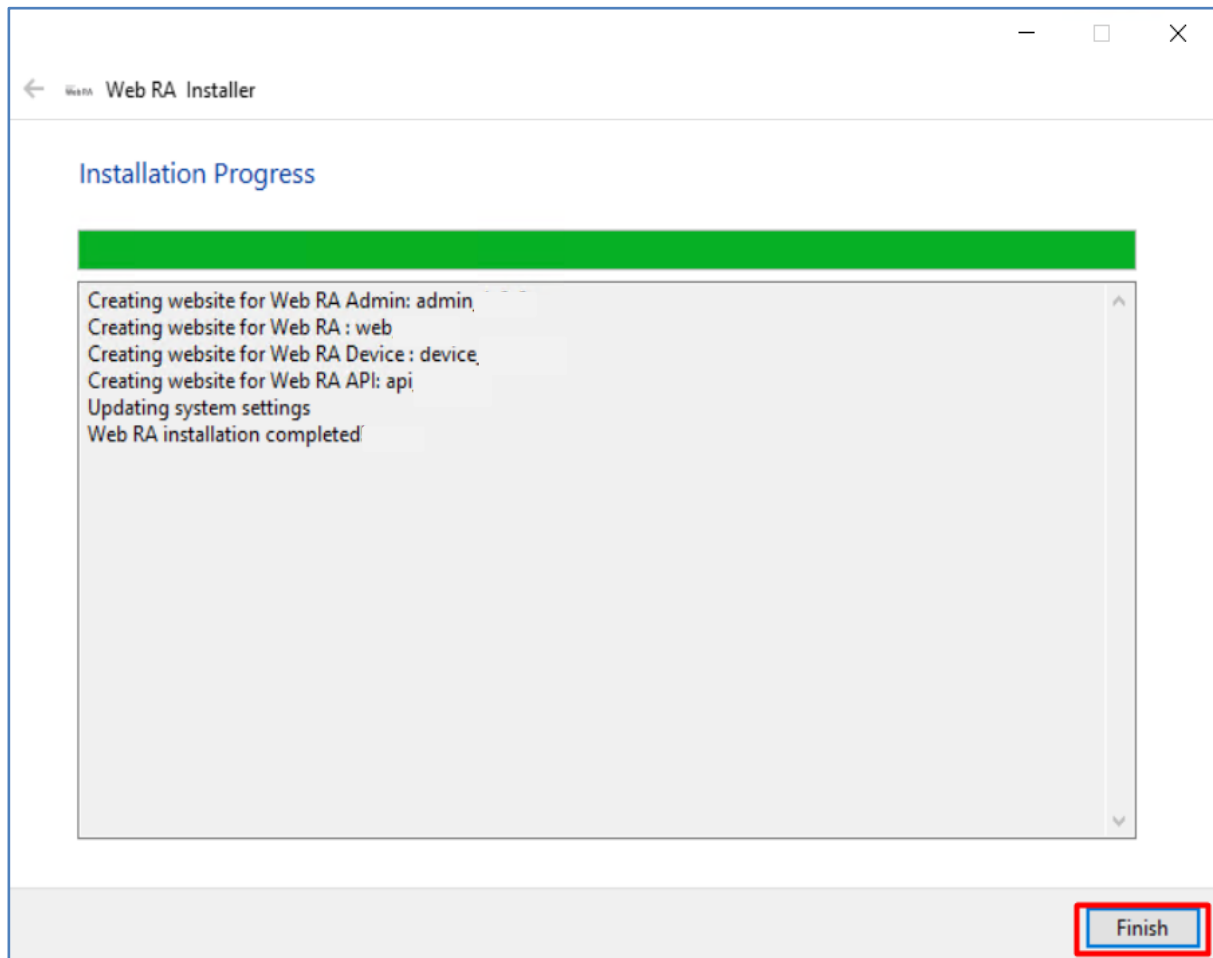
Click the **Next** button to show the summary and complete the installation:



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.

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



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

4.4 Upgrading ADSS Web RA

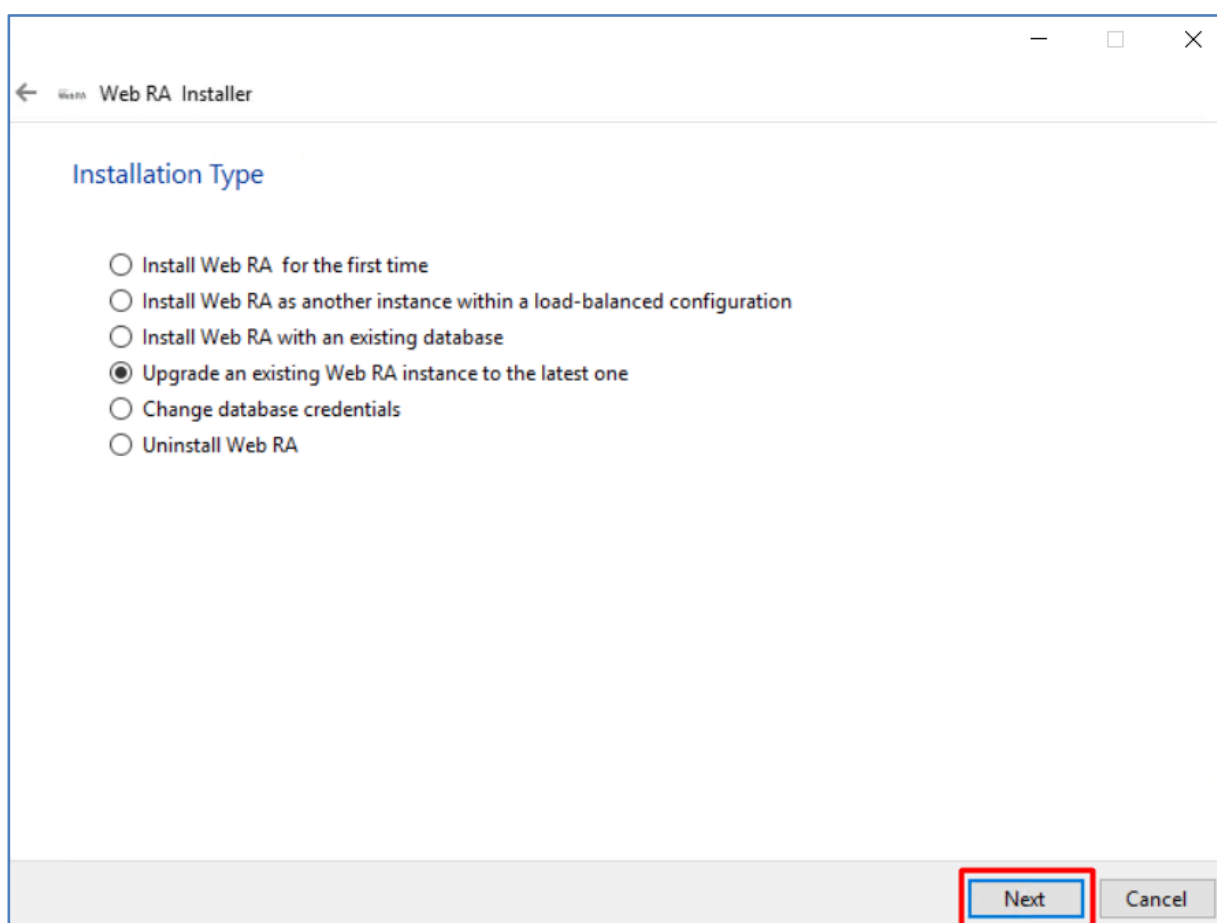
The upgrade process for ADSS Web RA is quick and easy. The existing data files, database schema and database entries are automatically upgraded during the process.

4.4.1 Upgrade Procedure

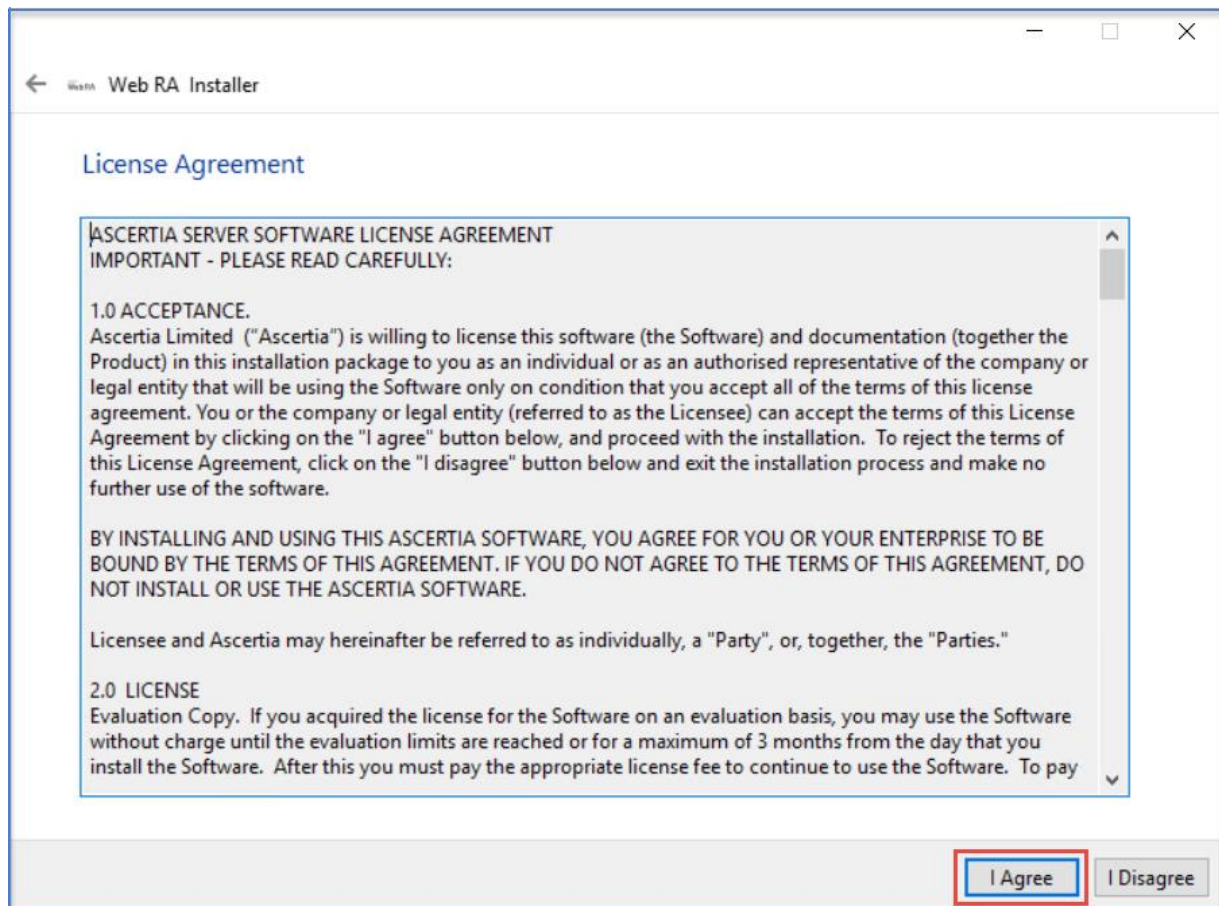
Follow these instructions to upgrade an older version of ADSS Web RA to the latest version. Launch the installer by right-clicking the file name **[ADSS Web RA Installation Directory]/setup/install.bat** and select **Run as administrator**.

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

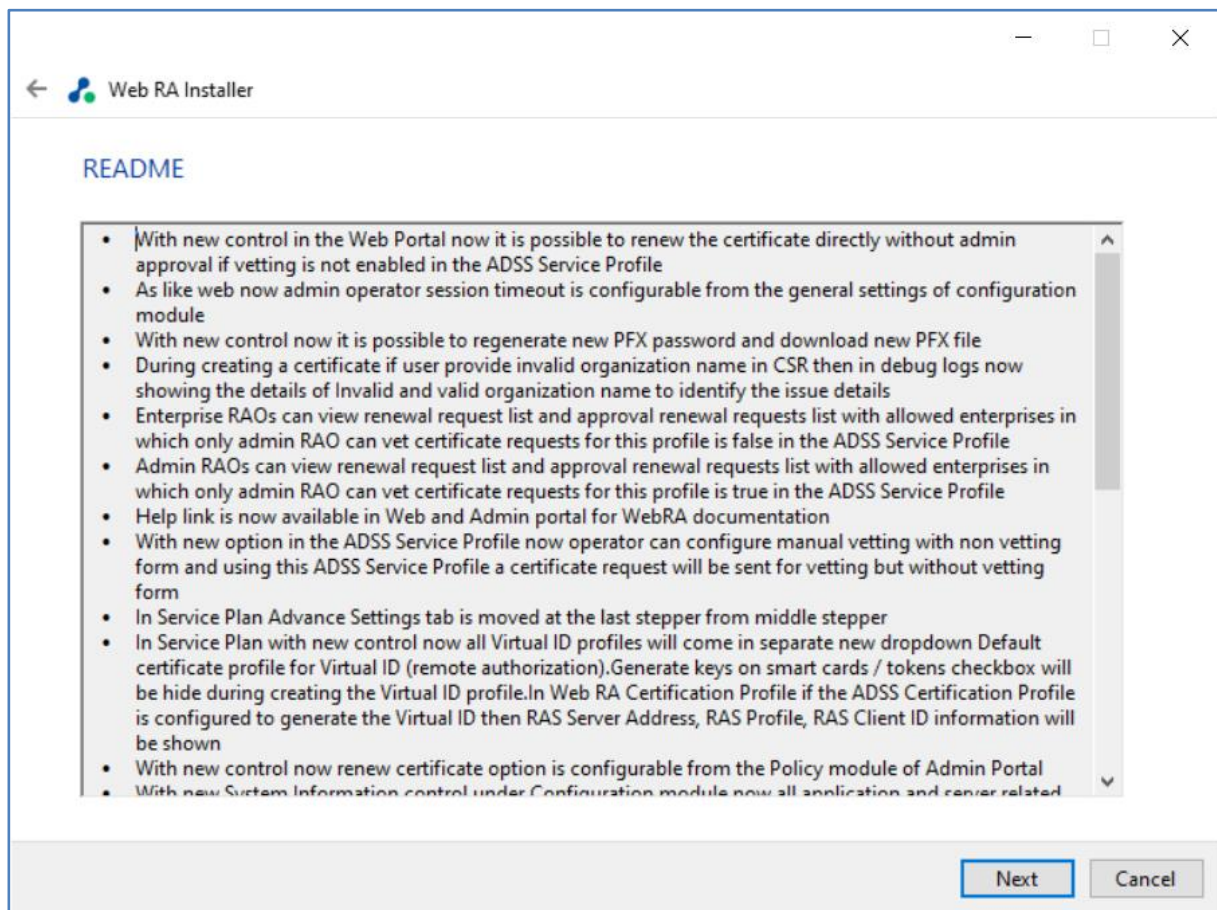
Select the option **Upgrade an existing ADSS Web RA instance to latest one**



Click the **Next** button to view and accept the license agreement:

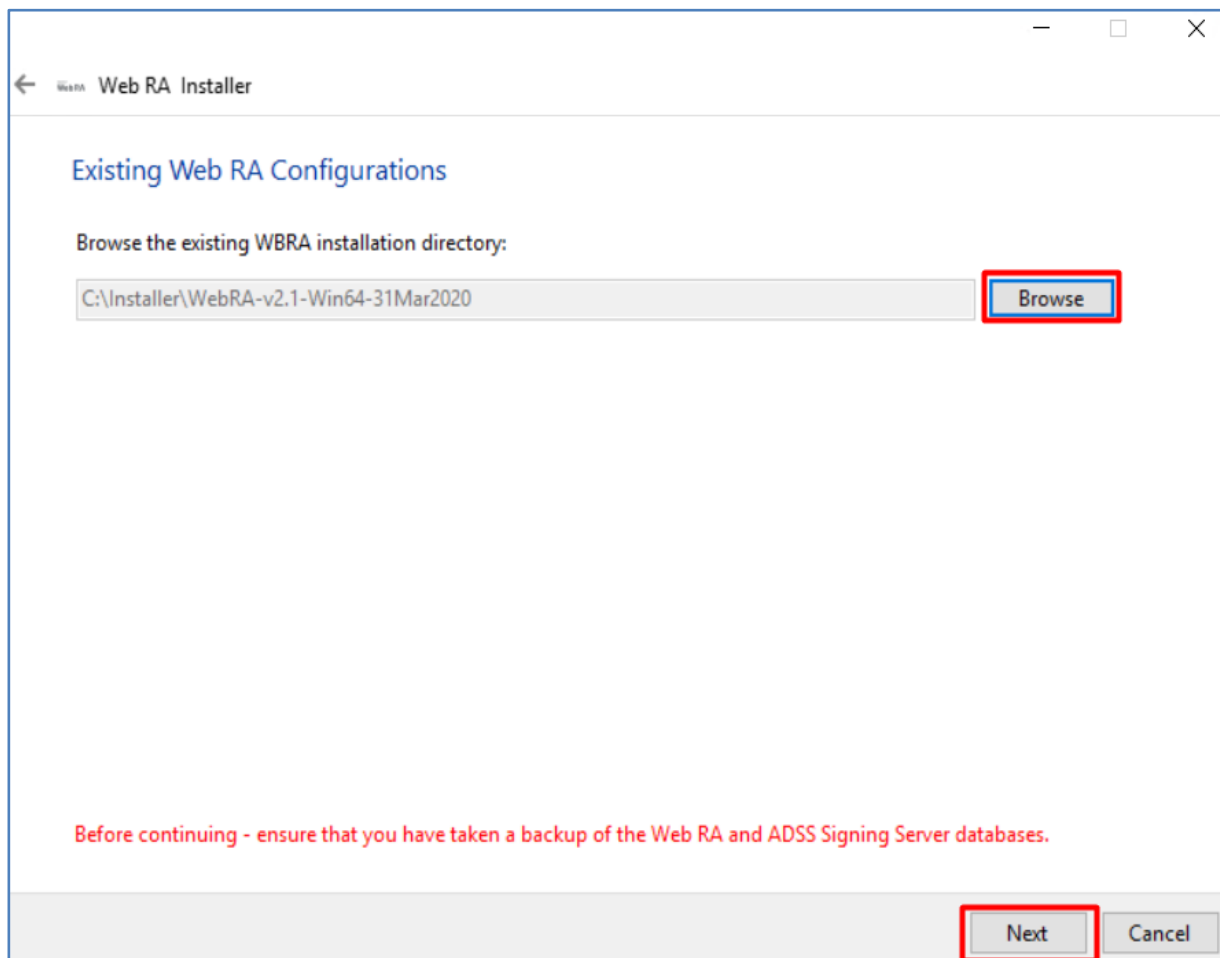


Click the **I Agree** button to proceed



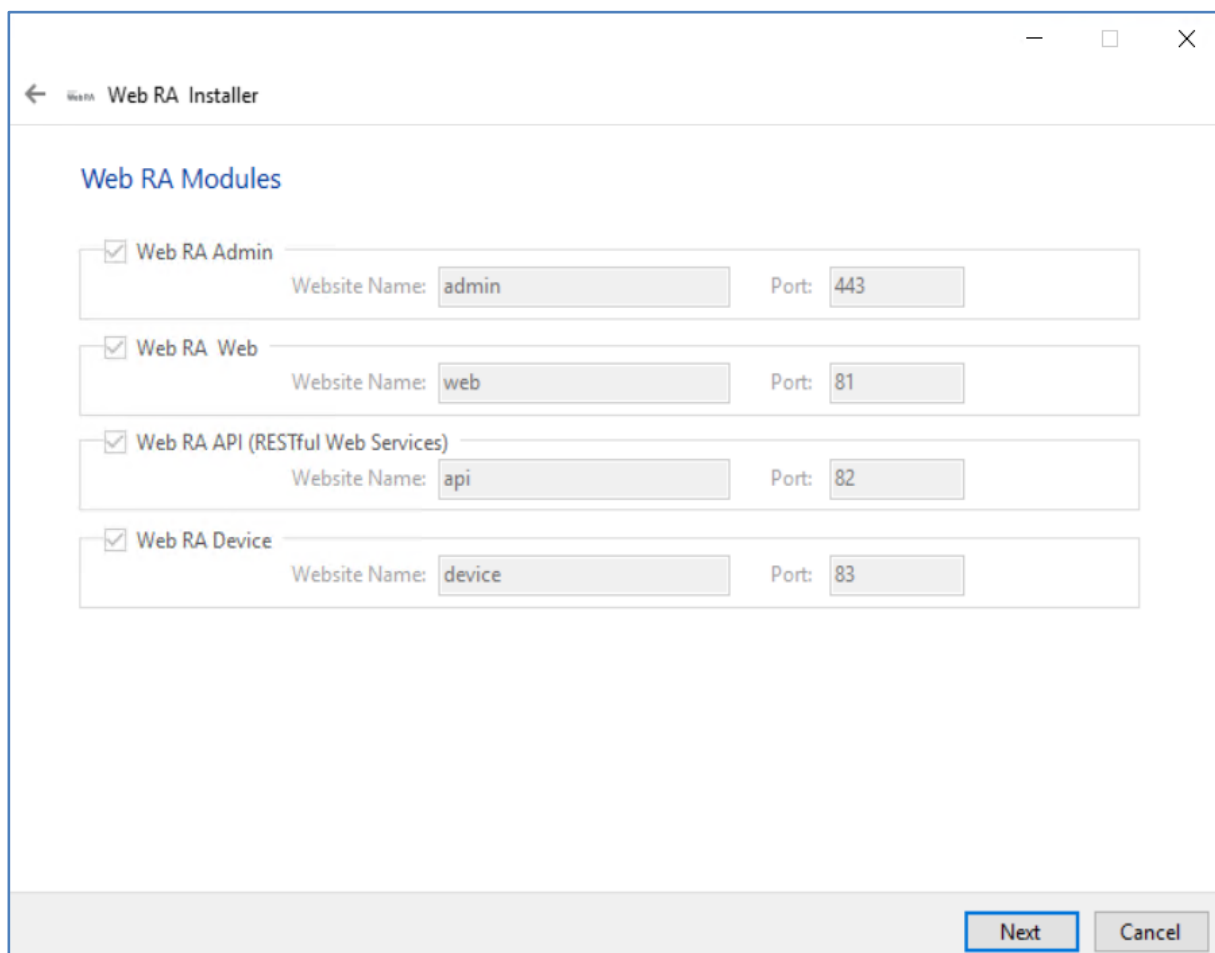
Readme file screen will be open. This includes all features of current version.

Click Next to proceed



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

Click the **Next** button to select specific modules:

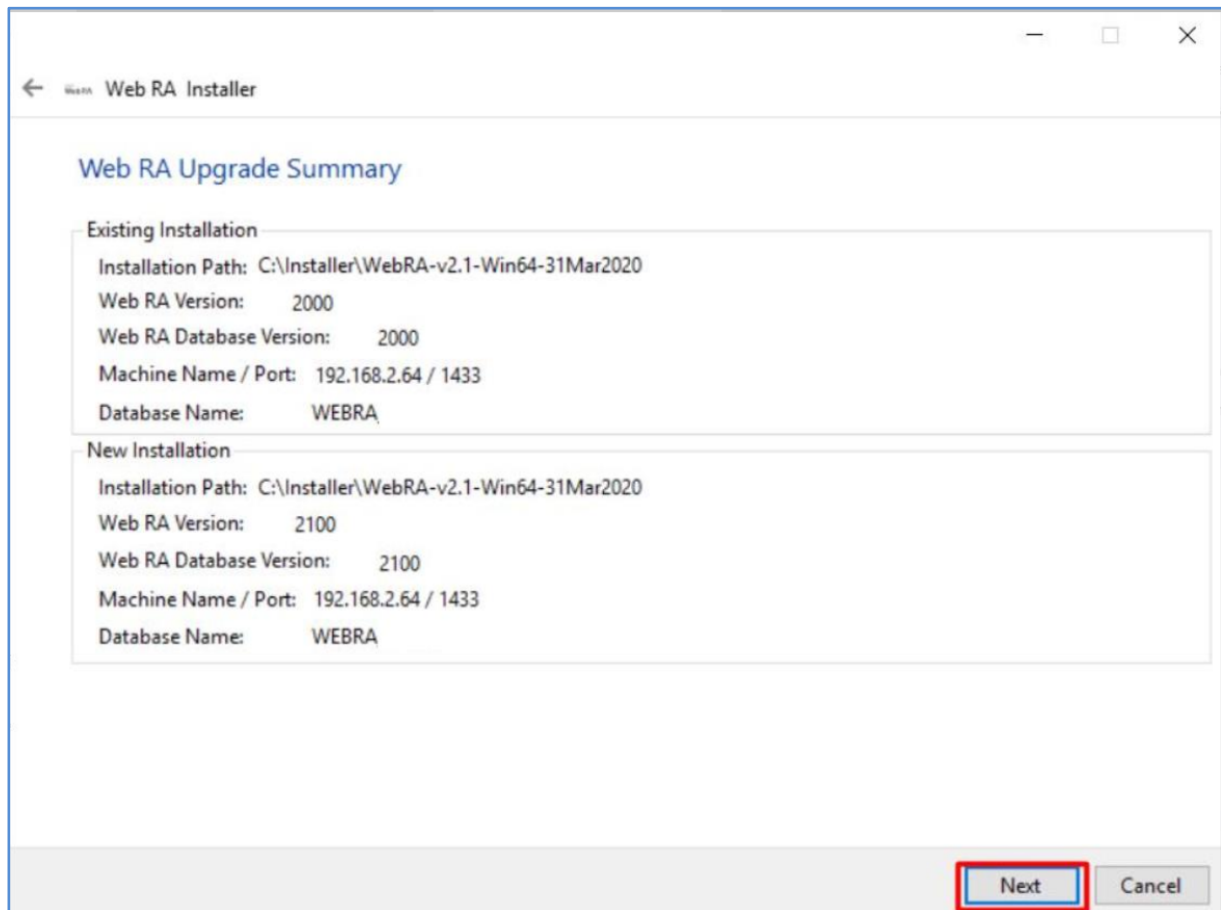


The image shows a screenshot of the 'Web RA Installer' window. The title bar includes a back arrow, the text 'Web RA Installer', and standard window controls. The main content area is titled 'Web RA Modules' and lists four modules, each with a checked checkbox, a 'Website Name' field, and a 'Port' field. The modules are: 'Web RA Admin' (Website Name: admin, Port: 443), 'Web RA Web' (Website Name: web, Port: 81), 'Web RA API (RESTful Web Services)' (Website Name: api, Port: 82), and 'Web RA Device' (Website Name: device, Port: 83). At the bottom right, there are 'Next' and 'Cancel' buttons.

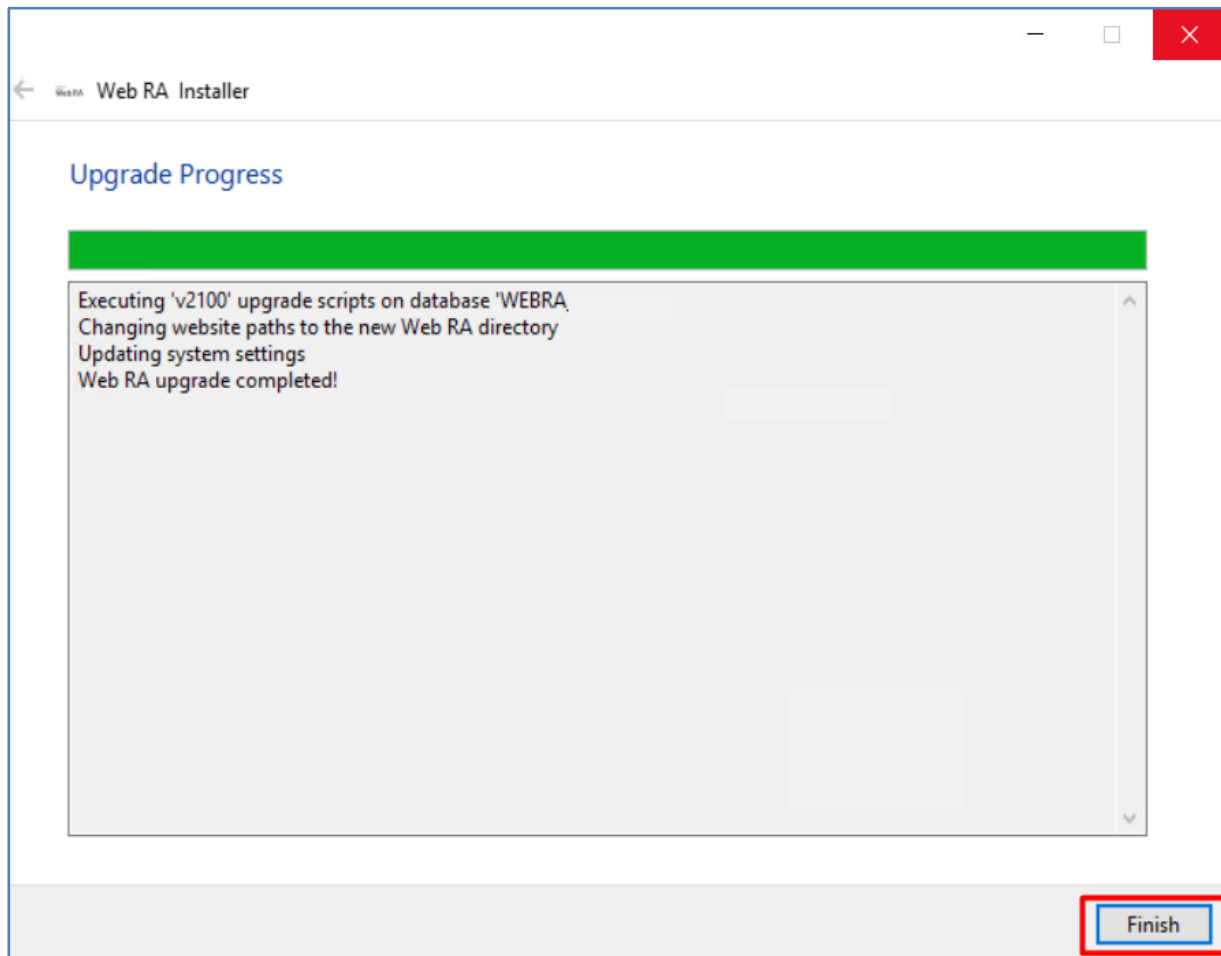
Module	Website Name	Port
<input checked="" type="checkbox"/> Web RA Admin	admin	443
<input checked="" type="checkbox"/> Web RA Web	web	81
<input checked="" type="checkbox"/> Web RA API (RESTful Web Services)	api	82
<input checked="" type="checkbox"/> Web RA Device	device	83

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.

Click the **Next** button to see the upgrade summary:



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



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

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

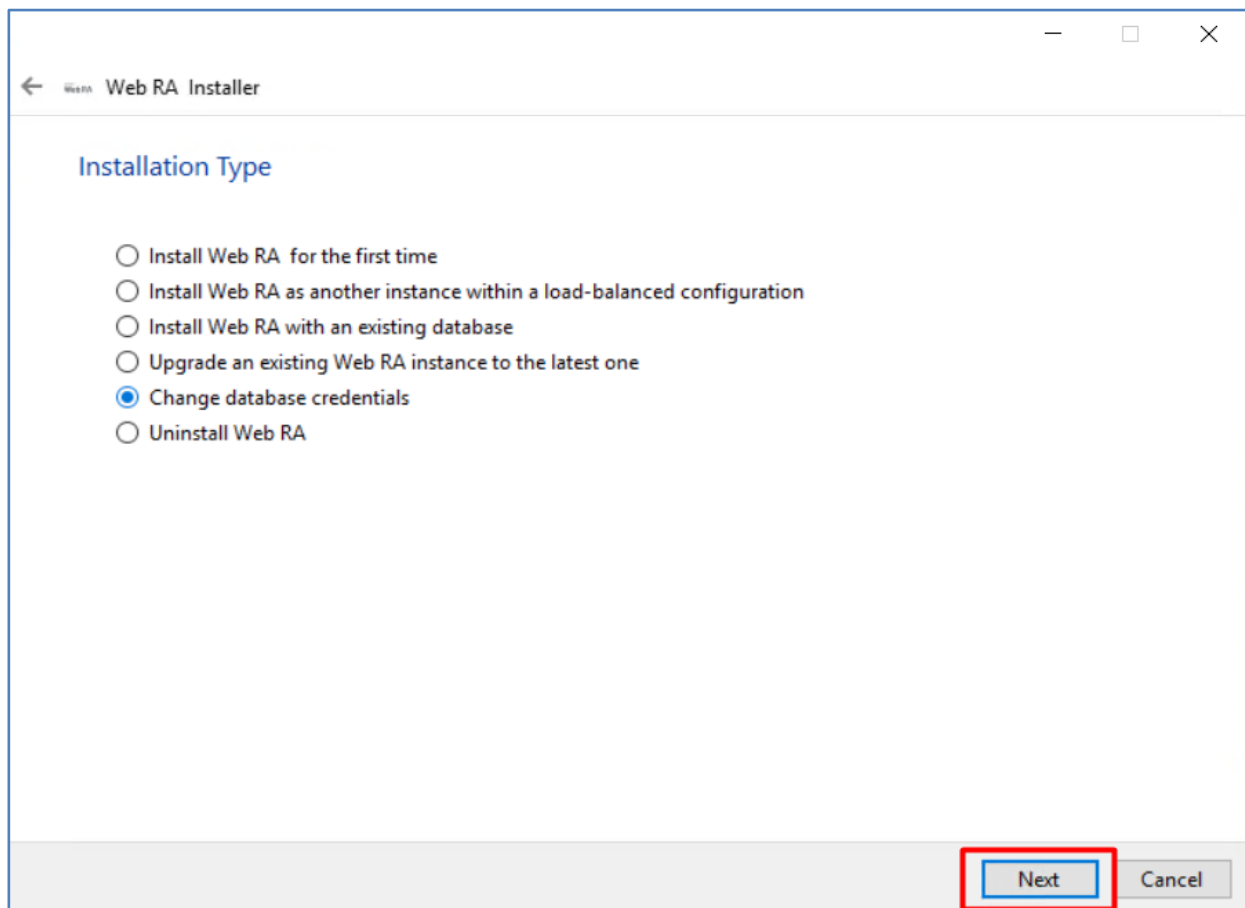
4.5 Changing Database Credentials for an Existing Installation

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.

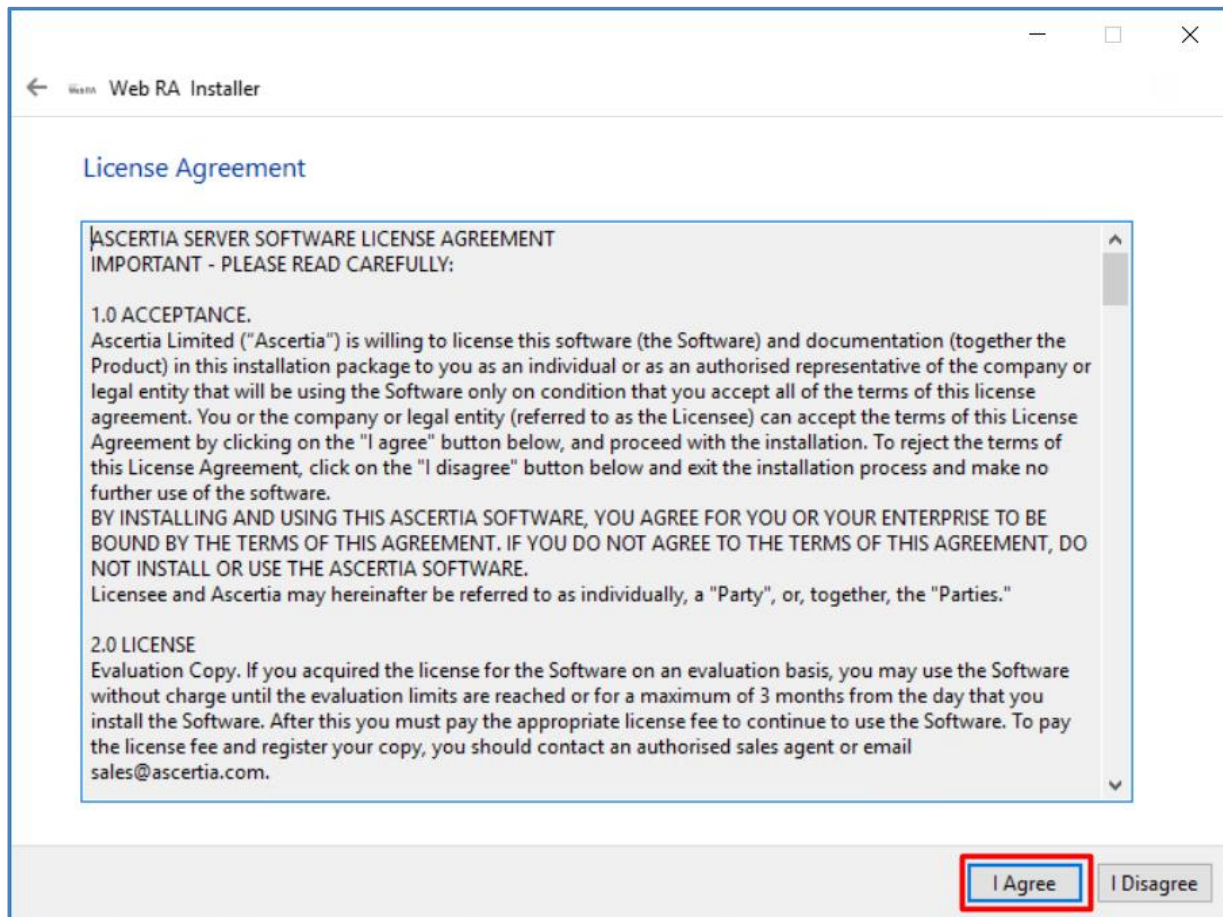
ADSS Web RA provides an option through the installer to update the following types of database related information:

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

Follow the installation wizard, and select the “**Change database credentials**” option, when the **Installation Type** screen is shown:

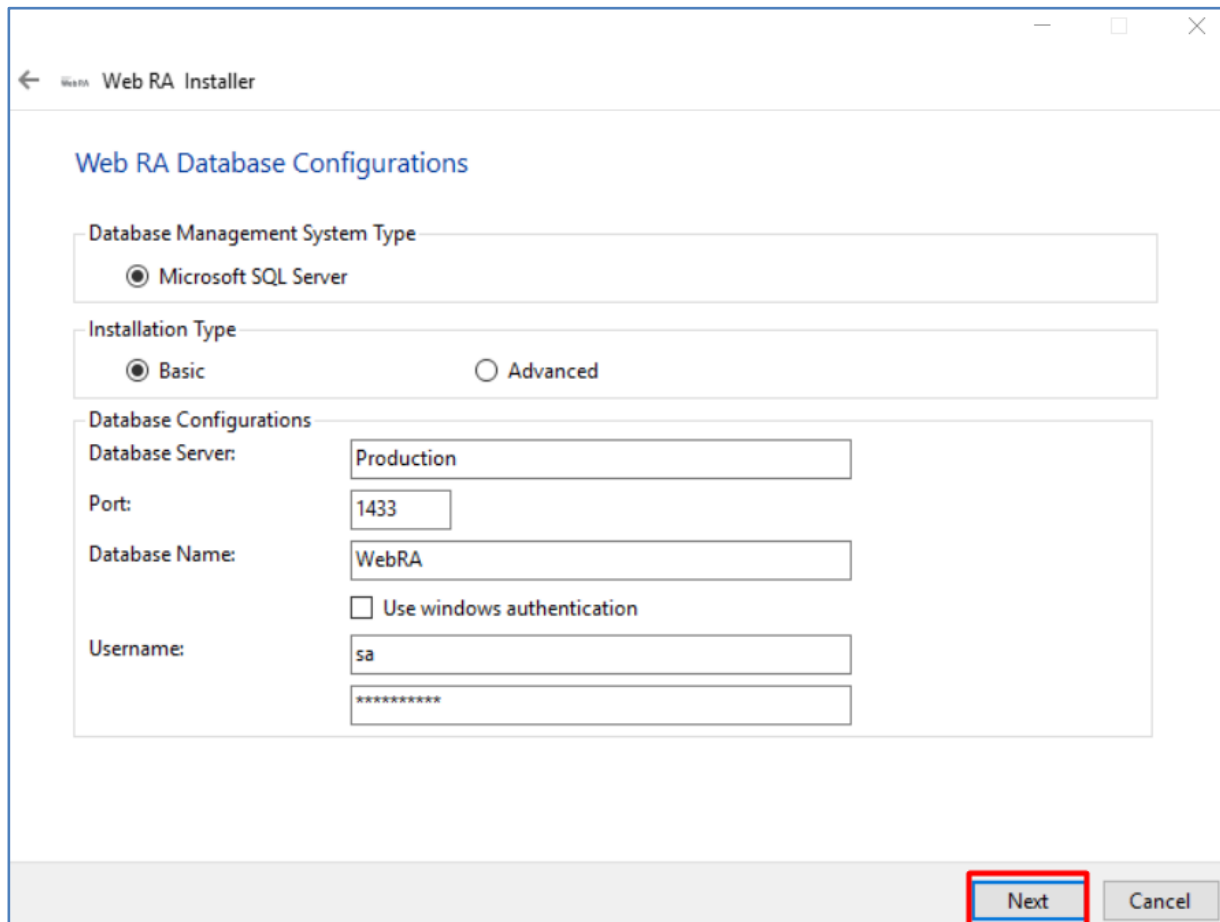


Click the **Next** button to show the License Agreement:



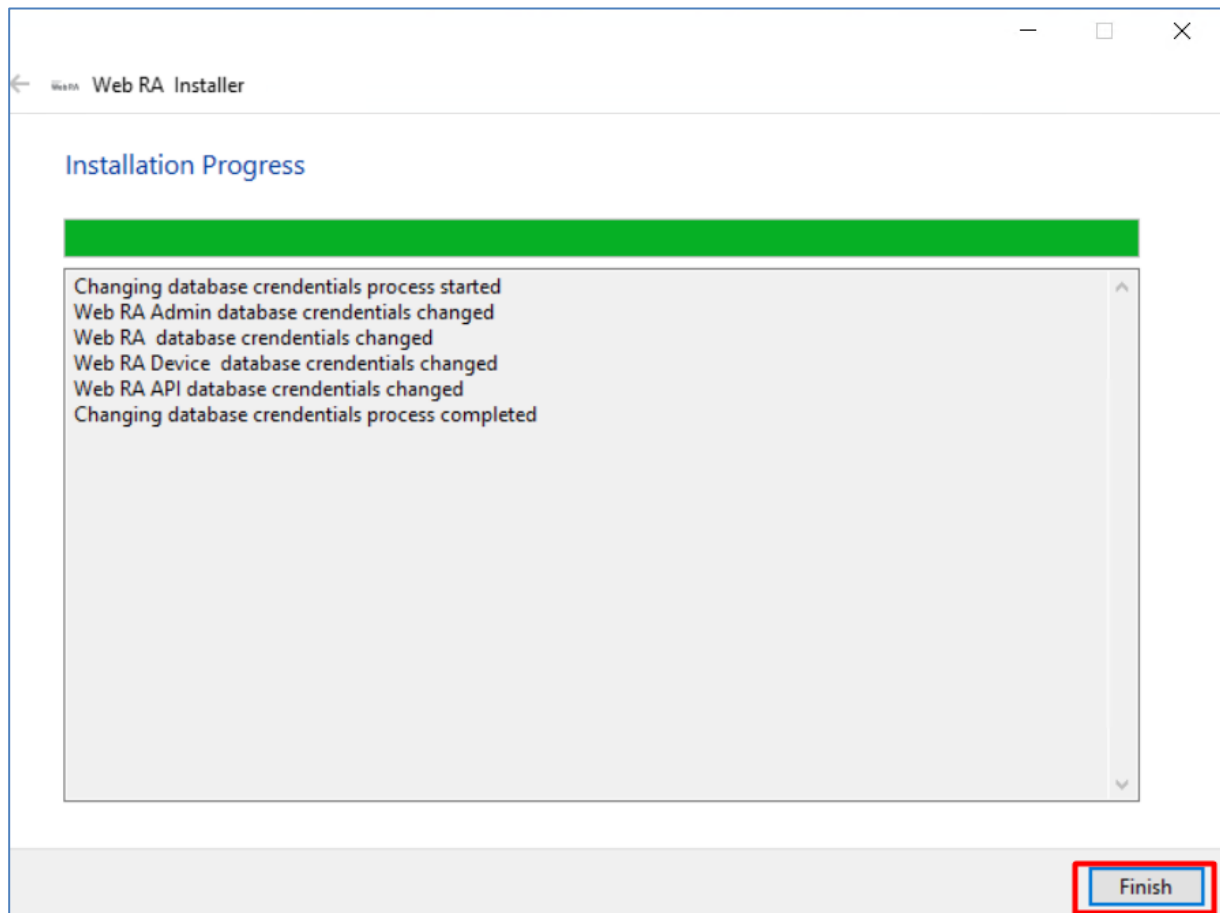
Click the **I Agree** button to proceed.

The following screen to prompt for database details will be displayed:



The image shows a screenshot of the 'Web RA Database Configurations' window in the 'Web RA Installer'. The window has a title bar with a back arrow, 'Web RA', and 'Web RA Installer'. The main content area is titled 'Web RA Database Configurations' and contains three sections: 'Database Management System Type' with a radio button for 'Microsoft SQL Server'; 'Installation Type' with radio buttons for 'Basic' (selected) and 'Advanced'; and 'Database Configurations' which includes fields for 'Database Server' (Production), 'Port' (1433), 'Database Name' (WebRA), a checkbox for 'Use windows authentication' (unchecked), 'Username' (sa), and a password field (masked with asterisks). At the bottom right, there are 'Next' and 'Cancel' buttons, with the 'Next' button highlighted by a red rectangle.

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



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

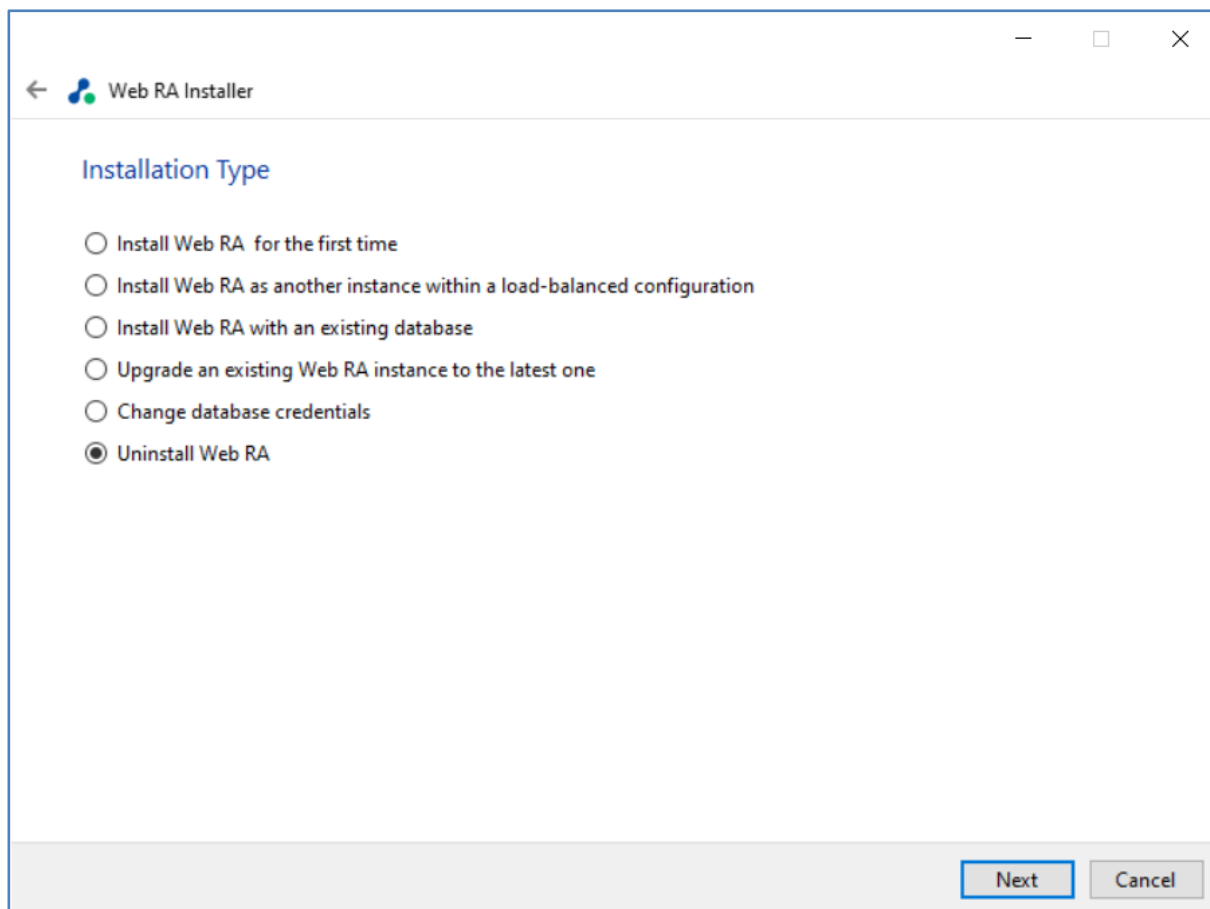
5 ADSS Web RA Uninstallation

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.

For this:

Right click the **[ADSS Web RA Directory]/setup/install.bat** file and choose **Run as administrator**.

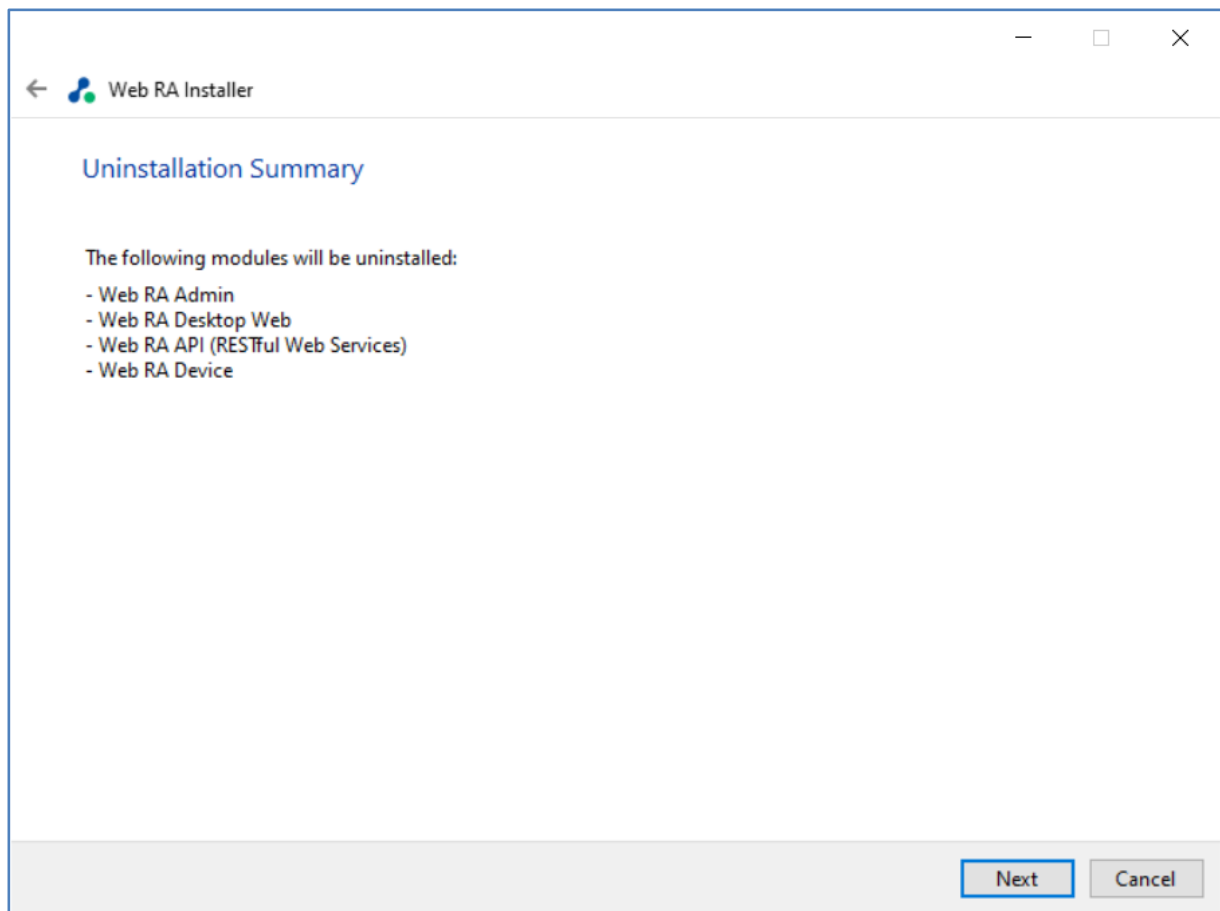
Follow the installation wizard until the **Installation Type** screen is shown:



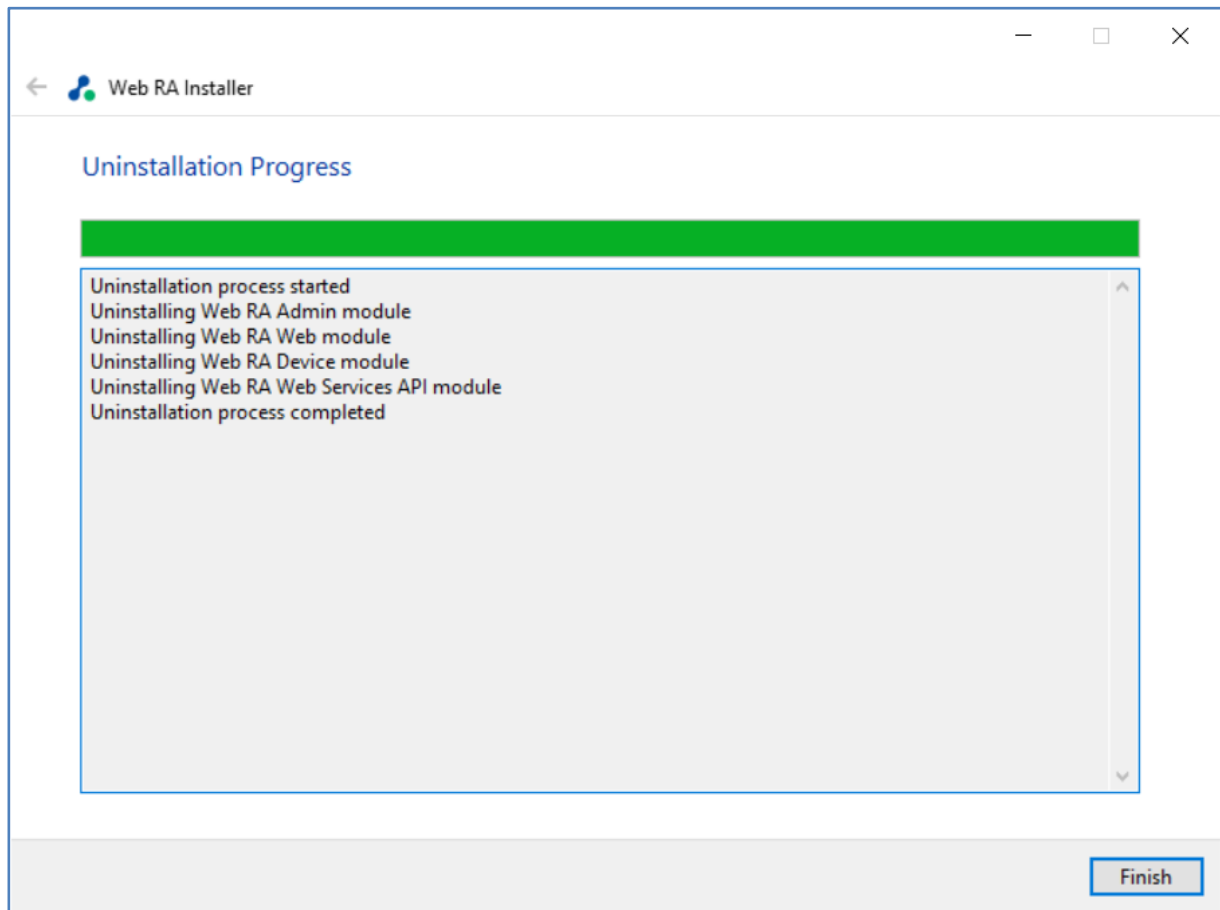
Select **"Uninstall ADSS Web RA"** to remove all websites from IIS mapped and this directory.

Click the **Next** button to proceed further.

The following screen is shown:



Click the **Next** button to proceed with the uninstall process.



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

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

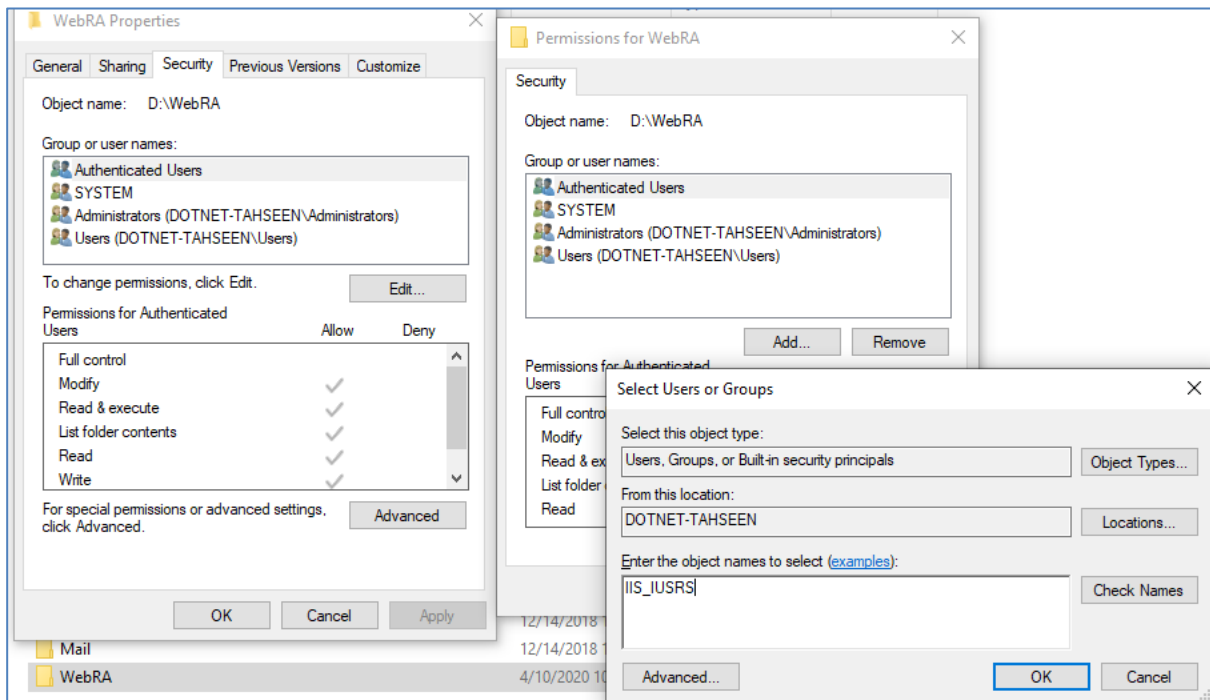
6 Appendix

6.1 Troubleshooting

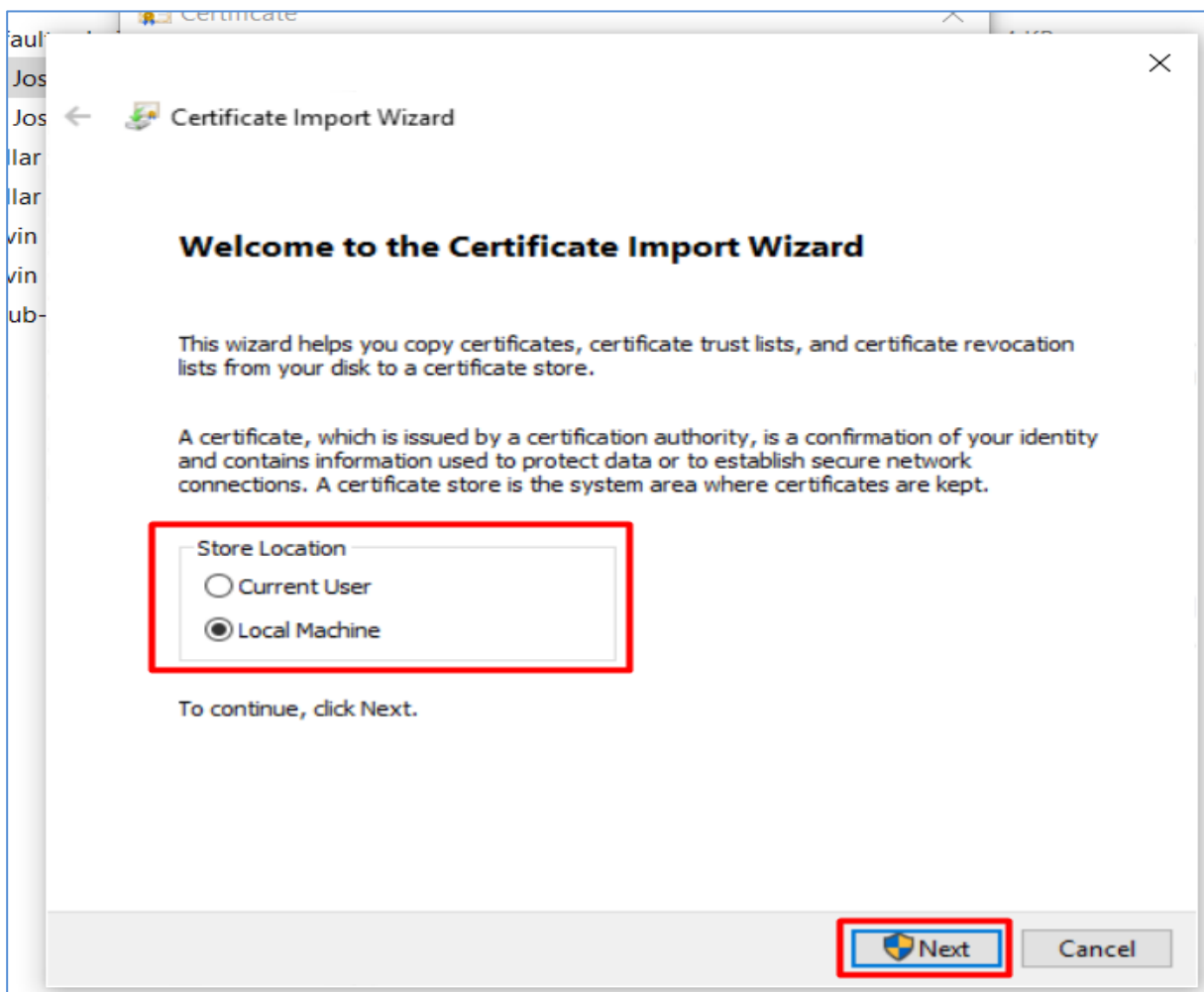
1. If ADSS Web RA Admin module is installed on Windows 2012 R2, then the HTTP 403.16 error code may occur when you access the ADSS Web RA Admin console from web browser.

Follow these instructions to solve this issue:

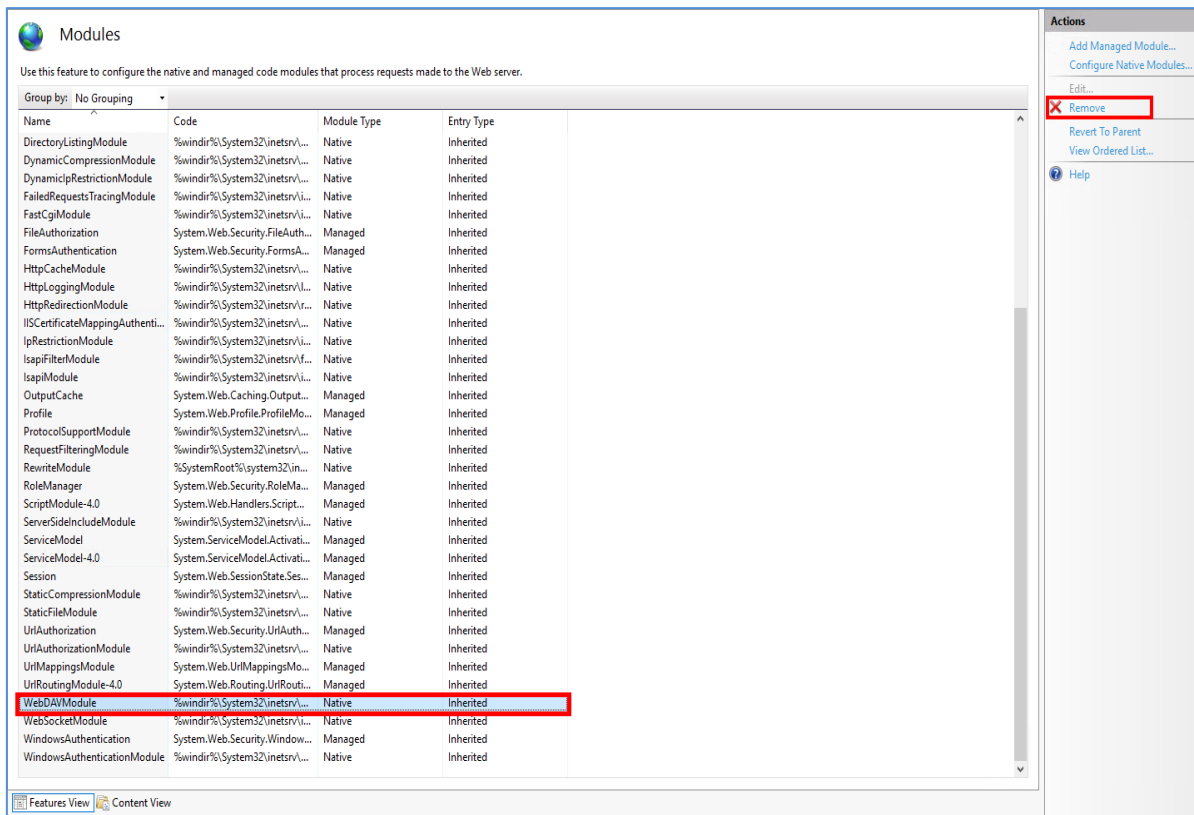
- a. Open registry and add the key:
KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
 - b. Create a new key with **Value Type: REG_DWORD (32-bit)**
 - c. Set **Value Name: ClientAuthTrustMode**
 - d. Edit the field and set **Value Data: 2**
 - If you are interested to know more details about it, browse the Microsoft KB link:
<https://support.microsoft.com/en-us/kb/2464556>.
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**.
 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 import to IIS so, connection between server and application could establish 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.



Use this feature to configure the native and managed code modules that process requests made to the Web server.

Name	Code	Module Type	Entry Type
DirectoryListingModule	%windir%\System32\inetrv...	Native	Inherited
DynamicCompressionModule	%windir%\System32\inetrv...	Native	Inherited
DynamicIpRestrictionModule	%windir%\System32\inetrv...	Native	Inherited
FailedRequestsTracingModule	%windir%\System32\inetrv...	Native	Inherited
FastCgiModule	%windir%\System32\inetrv...	Native	Inherited
FileAuthorization	System.Web.Security.FileAuth...	Managed	Inherited
FormsAuthentication	System.Web.Security.FormsA...	Managed	Inherited
HttpCacheModule	%windir%\System32\inetrv...	Native	Inherited
HttpLoggingModule	%windir%\System32\inetrv...	Native	Inherited
HttpRedirectionModule	%windir%\System32\inetrv...	Native	Inherited
IISCertificateMappingAuthenti...	%windir%\System32\inetrv...	Native	Inherited
IpRestrictionModule	%windir%\System32\inetrv...	Native	Inherited
IsapiFilterModule	%windir%\System32\inetrv...	Native	Inherited
IsapiModule	%windir%\System32\inetrv...	Native	Inherited
OutputCache	System.Web.Caching.Output...	Managed	Inherited
Profile	System.Web.Profile.ProfileMo...	Managed	Inherited
ProtocolSupportModule	%windir%\System32\inetrv...	Native	Inherited
RequestFilteringModule	%windir%\System32\inetrv...	Native	Inherited
RewriteModule	%SystemRoot%\system32\in...	Native	Inherited
RoleManager	System.Web.Security.RoleMa...	Managed	Inherited
ScriptModule-4.0	System.Web.Handlers.Script...	Managed	Inherited
ServerSideIncludeModule	%windir%\System32\inetrv...	Native	Inherited
ServiceModel	System.ServiceModel.Activati...	Managed	Inherited
ServiceModel-4.0	System.ServiceModel.Activati...	Managed	Inherited
Session	System.Web.SessionState.Ses...	Managed	Inherited
StaticCompressionModule	%windir%\System32\inetrv...	Native	Inherited
StaticFileModule	%windir%\System32\inetrv...	Native	Inherited
UrlAuthorization	System.Web.Security.UrlAuth...	Managed	Inherited
UrlAuthorizationModule	%windir%\System32\inetrv...	Native	Inherited
UrlMappingsModule	System.Web.UrlMappingsMo...	Managed	Inherited
UrlRoutingModule-4.0	System.Web.Routing.UrlRout...	Managed	Inherited
WebDAVModule	%windir%\System32\inetrv...	Native	Inherited
WebSocketModule	%windir%\System32\inetrv...	Native	Inherited
WindowsAuthentication	System.Web.Security.Window...	Managed	Inherited
WindowsAuthenticationModule	%windir%\System32\inetrv...	Native	Inherited

Actions

- Add Managed Module...
- Configure Native Modules...
- Edit...
- Remove**
- Revert To Parent
- View Ordered List...
- Help

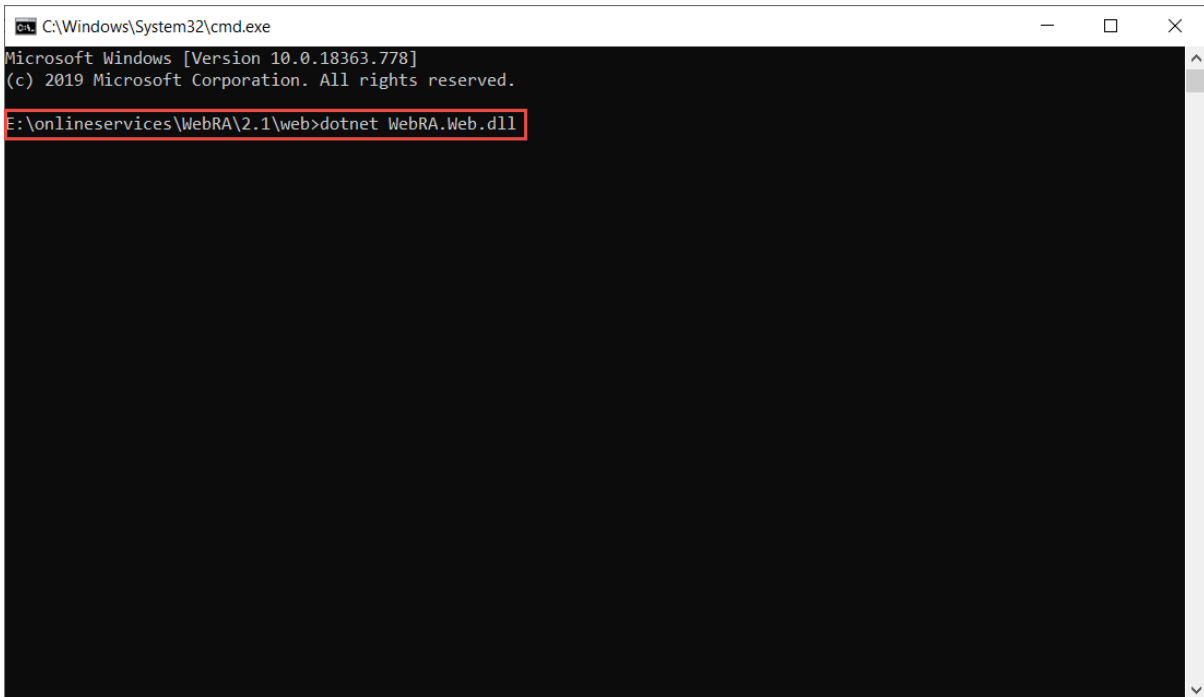
- Configurations used for Simple Certificate Enrollment Protocol (SCEP)
 - Make sure that following tag is added in “web.config” of web module:

```
<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>
        </aspNetCore>
      </aspNetCore>
    </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'" />

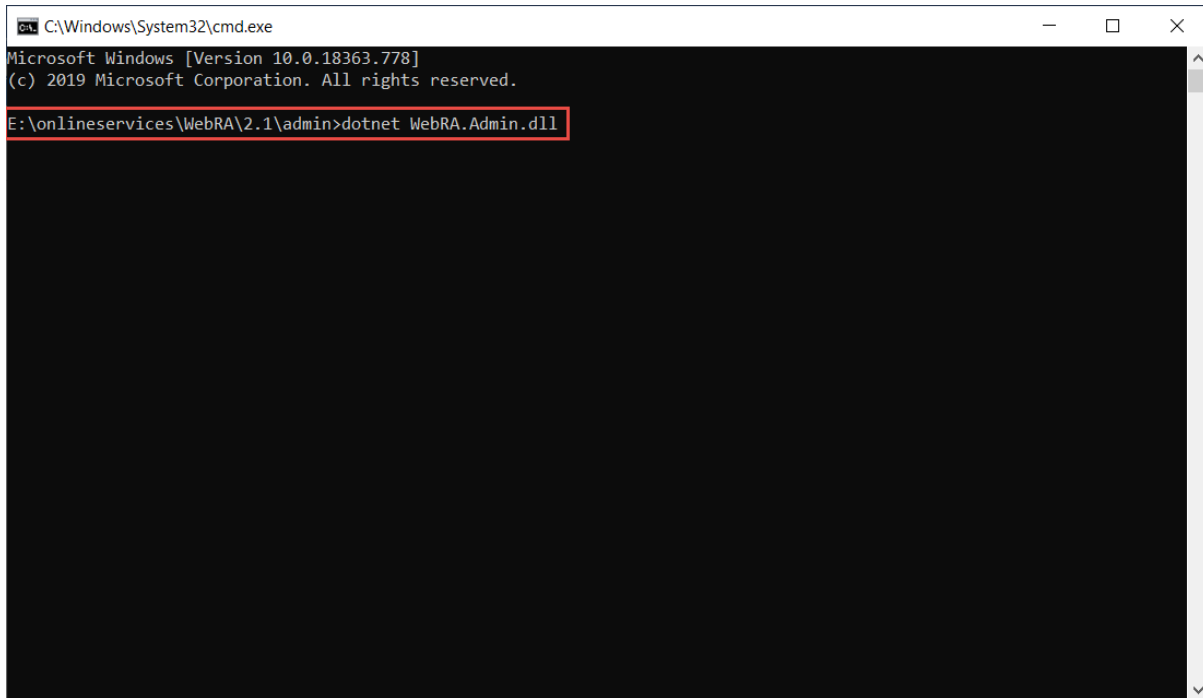
To test if the code is working properly for web, run command line in [installation-dir]/web and type following command:



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

E:\onlineservices\WebRA\2.1\web>dotnet WebRA.Web.dll
```

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



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

E:\onlineservices\WebRA\2.1\admin>dotnet WebRA.Admin.dll
```

6.2 SSL Certificates

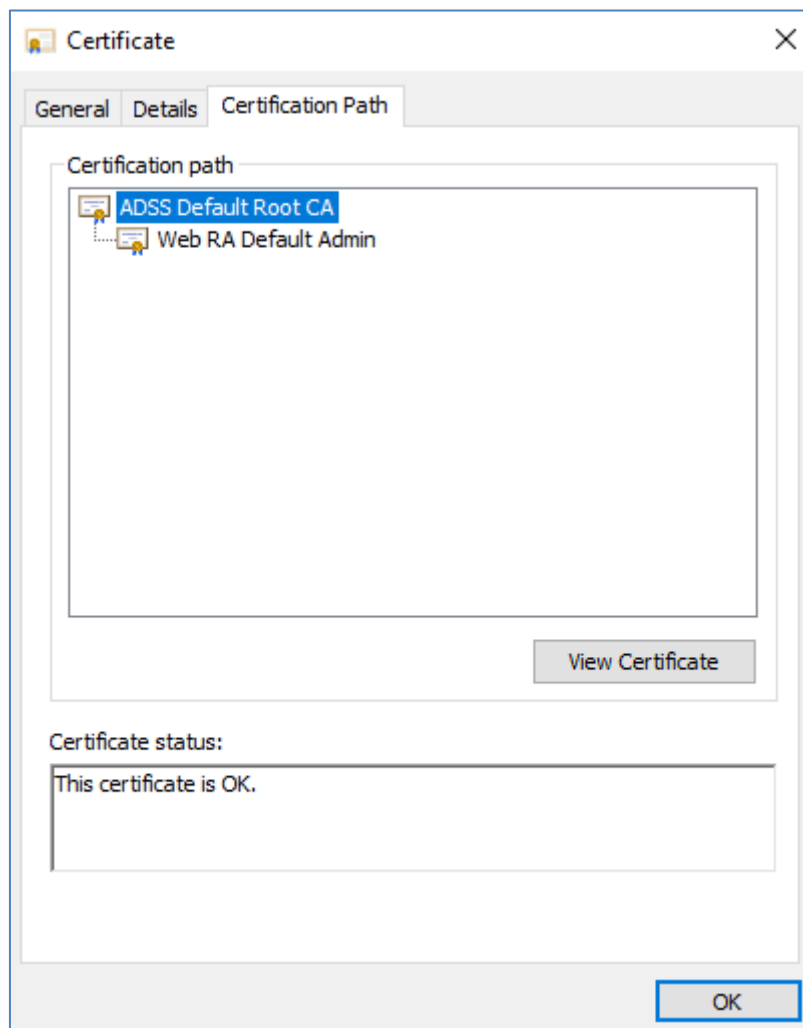
ADSS Web RA is a web application that is hosted in IIS. It is recommended to secure the communication between the server and browsers by using SSL over HTTPS. It is also recommended to use an SSL certificate issued by a well-known certificate authority (CA) e.g., Comodo, Symantec, Digicert etc.

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

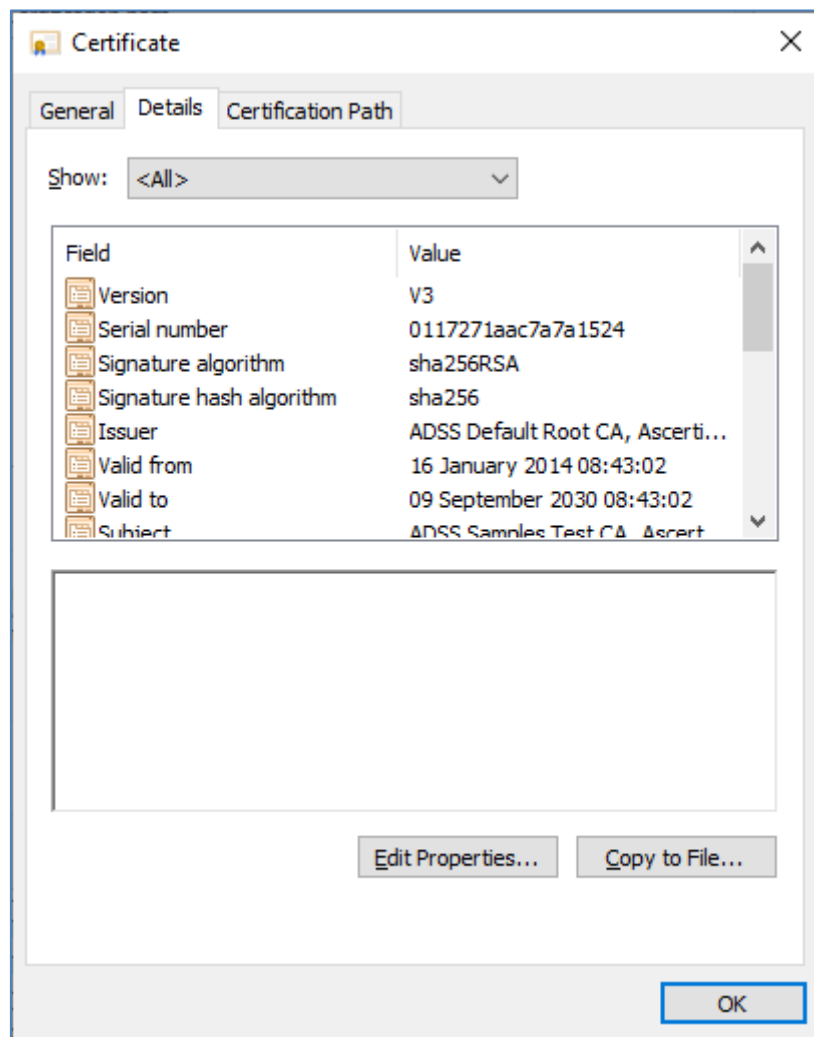
6.2.1 Exporting Root and Intermediate Certificates

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.

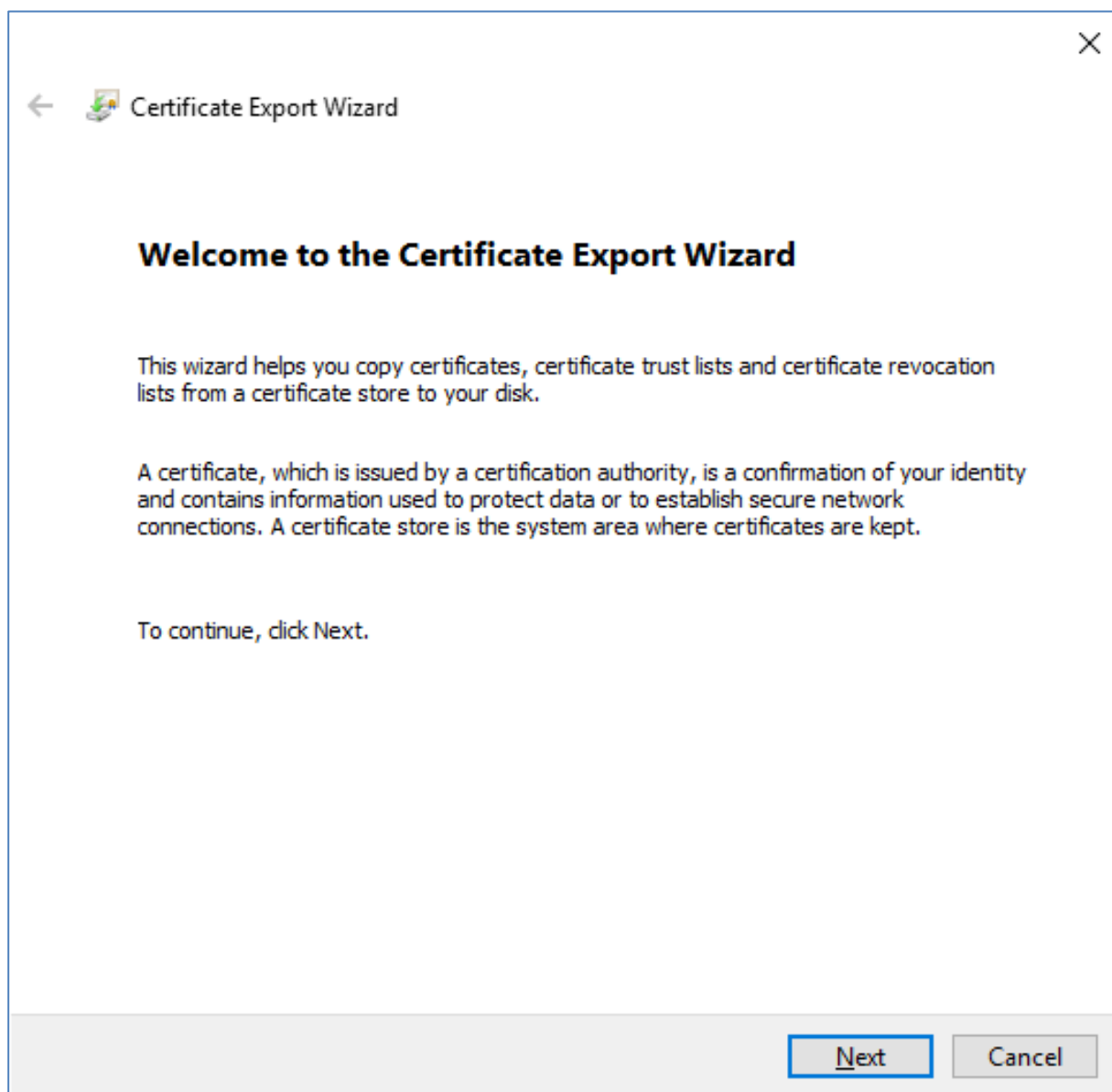
Double click the **web-ra-default-admin.cer** file



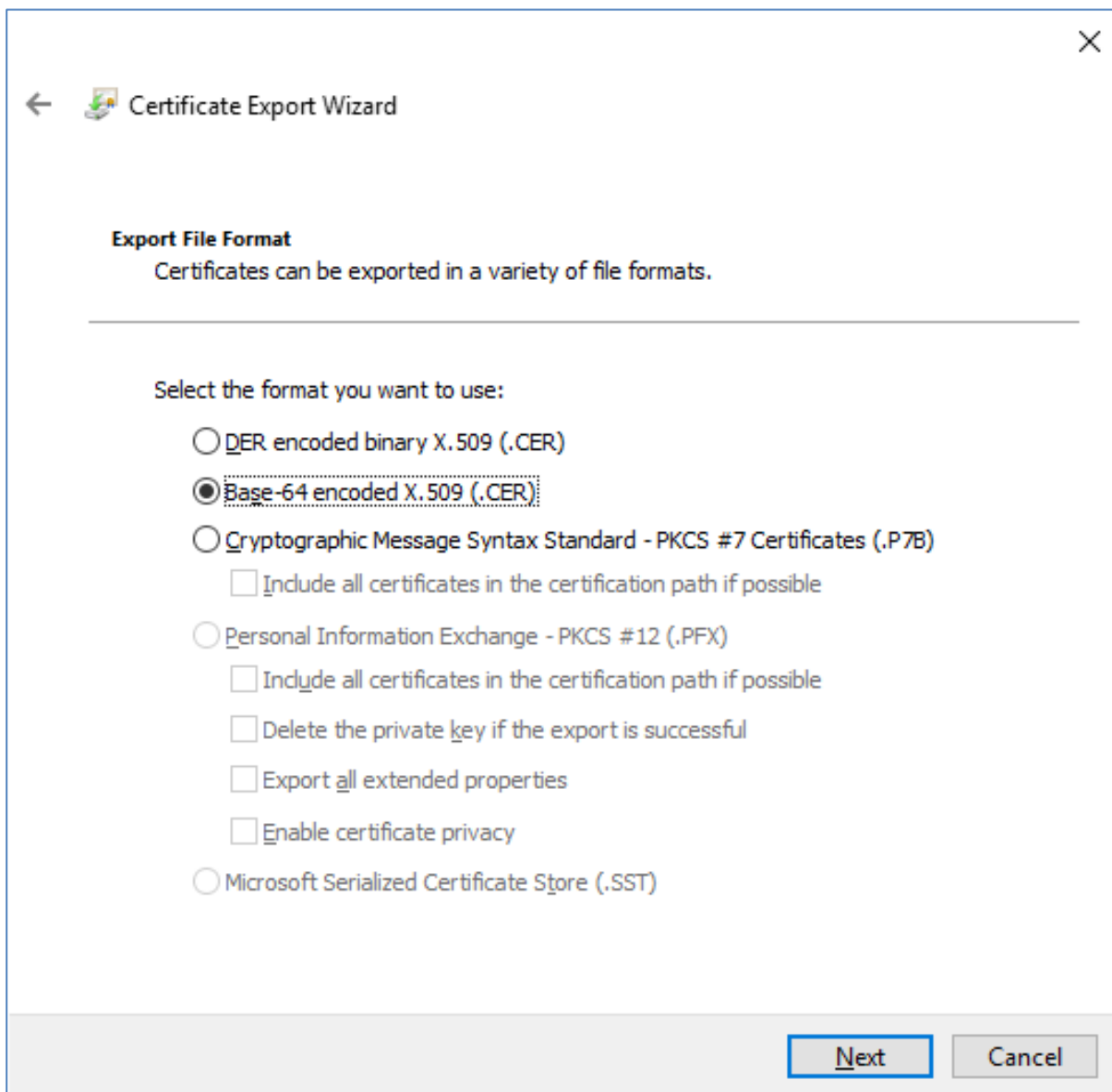
Select the **Certification Path** tab from the top. Default ADSS Web RA TLS certificate has one root certificate. Select the root certificate and click the **View Certificate** button. A new window will appear showing the general details of the intermediate certificate.



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



Click **Next**



The image shows a 'Certificate Export Wizard' dialog box. At the top, there is a back arrow and a folder icon. Below this, the title 'Certificate Export Wizard' is displayed. The main section is titled 'Export File Format' and contains the text 'Certificates can be exported in a variety of file formats.' Below this, a horizontal line separates the header from the options. The text 'Select the format you want to use:' is followed by five radio button options: 'DER encoded binary X.509 (.CER)', 'Base-64 encoded X.509 (.CER)' (which is selected), 'Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)', 'Personal Information Exchange - PKCS #12 (.PFX)', and 'Microsoft Serialized Certificate Store (.SST)'. Under the 'Cryptographic Message Syntax Standard' and 'Personal Information Exchange' options, there are three checkboxes each: 'Include all certificates in the certification path if possible', 'Delete the private key if the export is successful', and 'Export all extended properties'. Under the 'Personal Information Exchange' option, there is also a checkbox for 'Enable certificate privacy'. At the bottom right, there are 'Next' and 'Cancel' buttons.

← Certificate Export Wizard

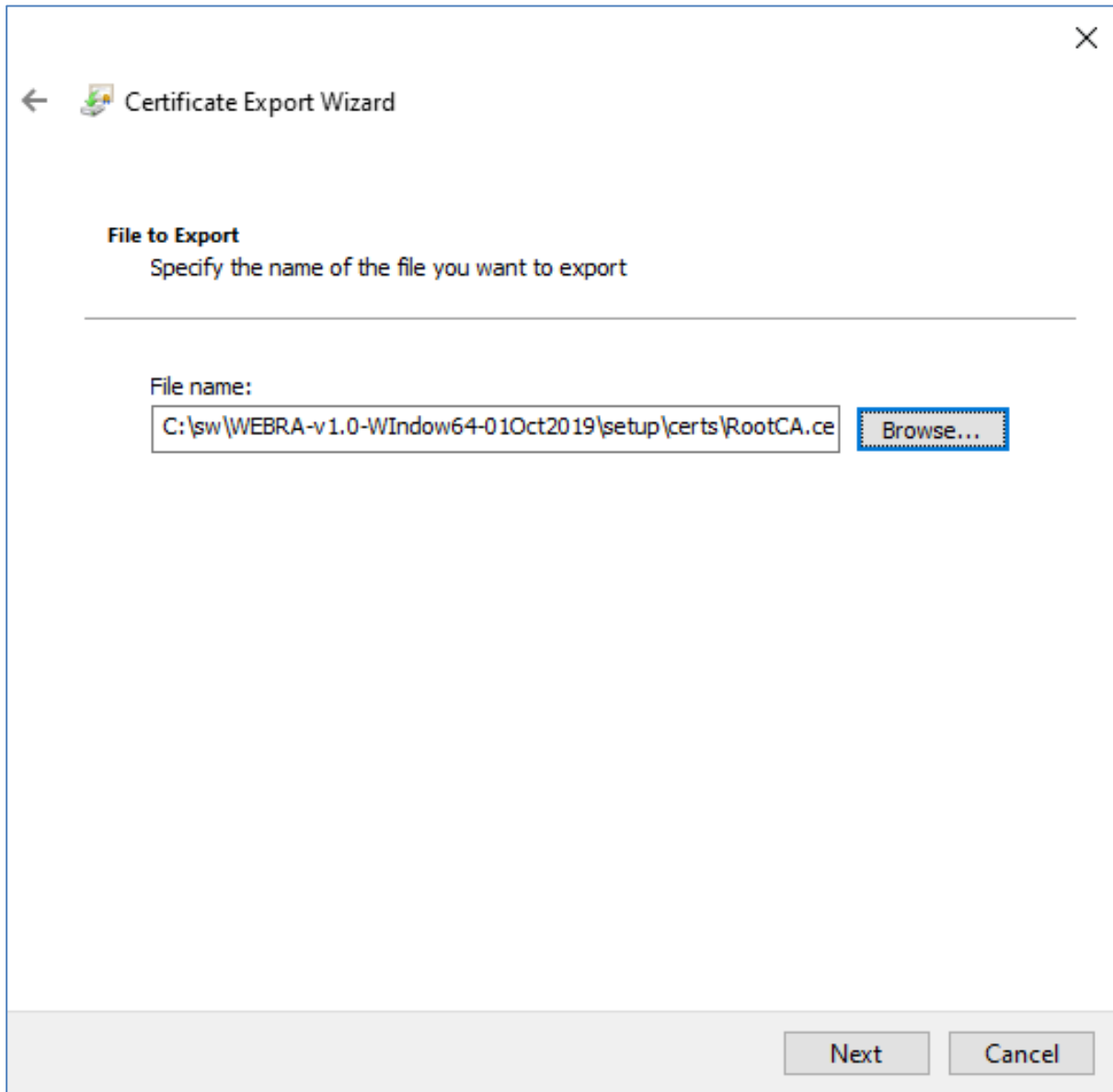
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ☐ DER encoded binary X.509 (.CER)
- ☒ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - ☐ Include all certificates in the certification path if possible
- ☐ Personal Information Exchange - PKCS #12 (.PFX)
 - ☐ Include all certificates in the certification path if possible
 - ☐ Delete the private key if the export is successful
 - ☐ Export all extended properties
 - ☐ Enable certificate privacy
- ☐ Microsoft Serialized Certificate Store (.SST)

Next Cancel

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



The image shows a 'Certificate Export Wizard' dialog box. At the top, there is a back arrow and a folder icon next to the title 'Certificate Export Wizard'. Below this, the section 'File to Export' is followed by the instruction 'Specify the name of the file you want to export'. A horizontal line separates this from the 'File name:' label. Below the label is a text box containing the path 'C:\sw\WEBRA-v1.0-WIndow64-01Oct2019\setup\certs\RootCA.ce'. To the right of the text box is a 'Browse...' button. At the bottom right of the dialog are 'Next' and 'Cancel' buttons.

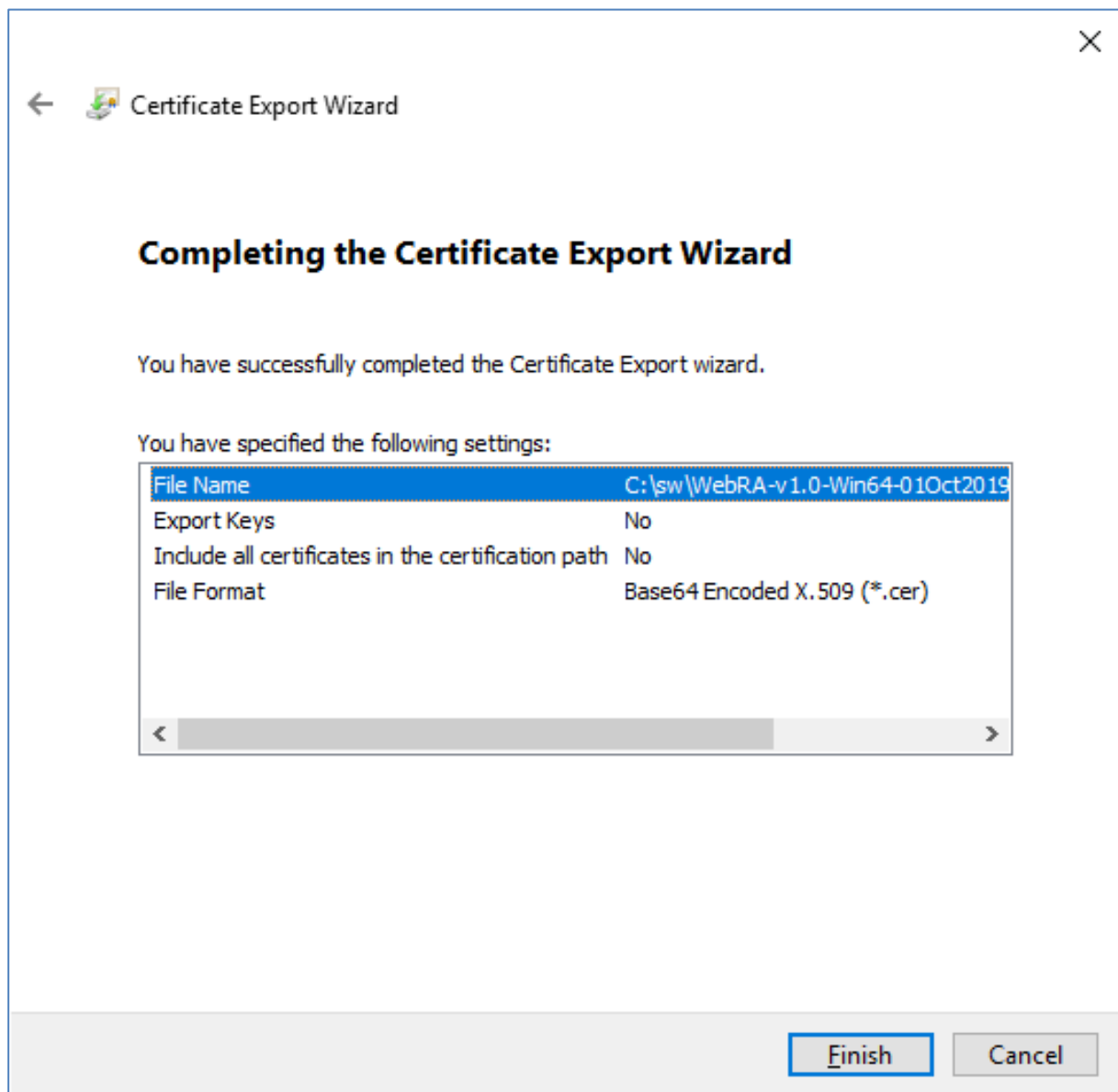
← Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:
C:\sw\WEBRA-v1.0-WIndow64-01Oct2019\setup\certs\RootCA.ce Browse...

Next Cancel

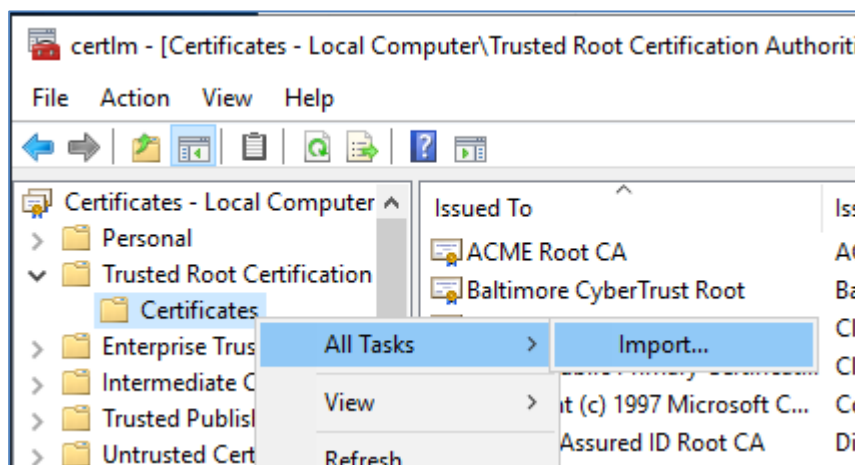
Choose a path where you want to save the certificate file for the intermediate certificate, and click **Next**.



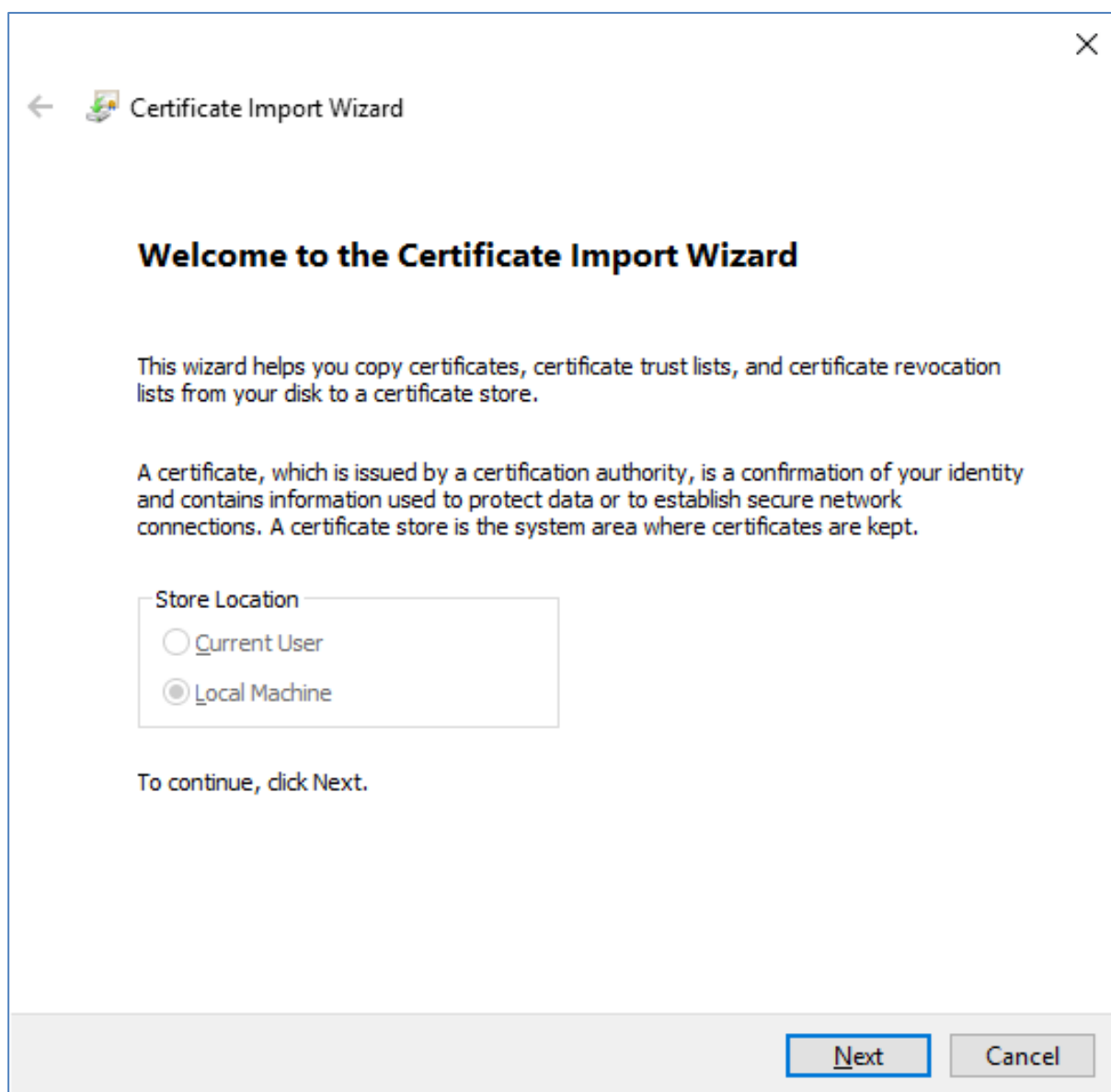
Click **Finish** to complete the export process for the root certificate.

6.3 Importing Root and Intermediate Certificates

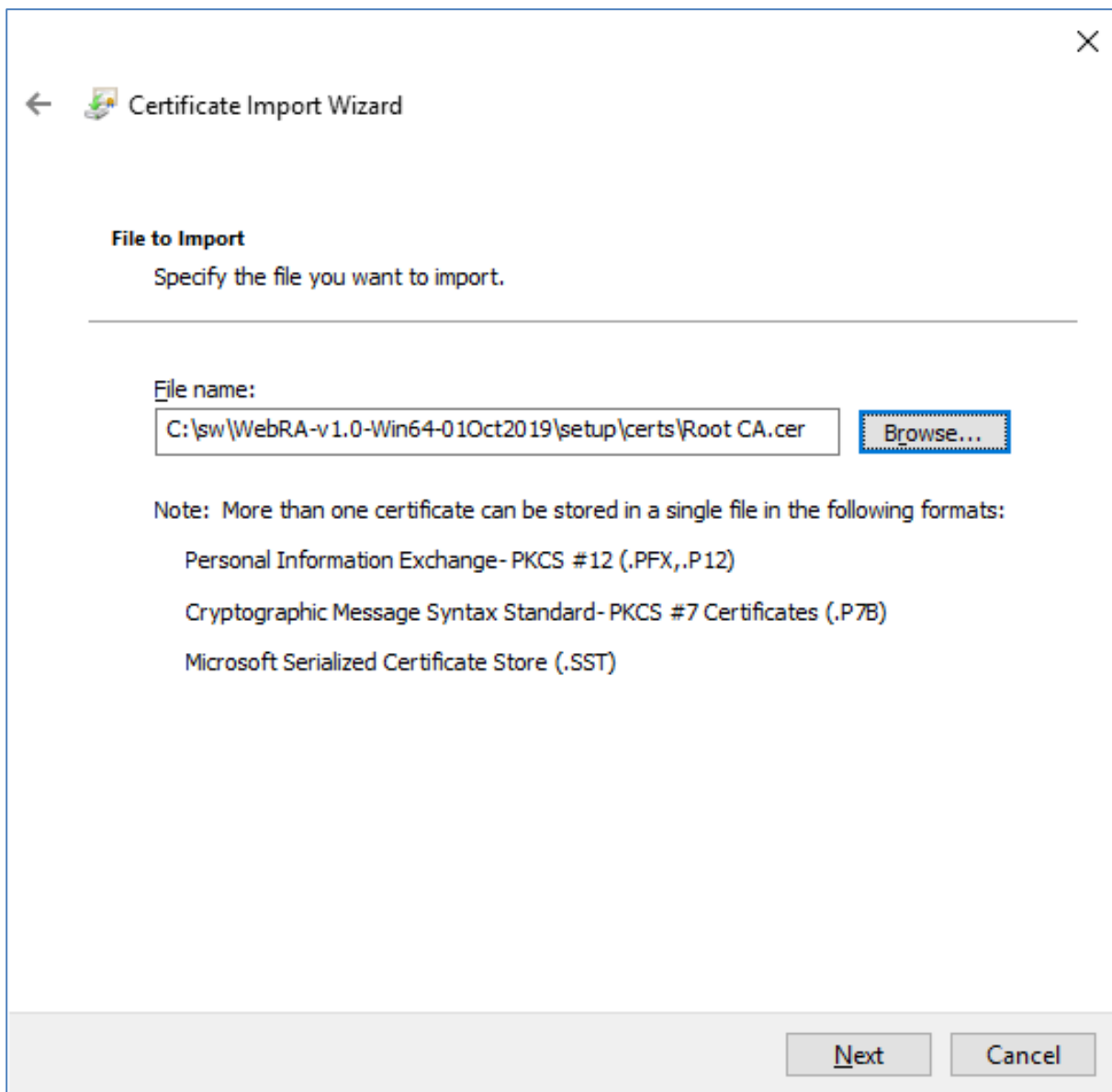
Now that we have the intermediate and root certificates exported and saved in a local file, we can import it to the certificate store. Launch **certlm.msc** from the command prompt.



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



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



The image shows a 'Certificate Import Wizard' dialog box. At the top, there is a back arrow and a 'Certificate Import Wizard' title bar with a close button. Below the title bar, the text 'File to Import' is followed by 'Specify the file you want to import.' A horizontal line separates this from the input section. The input section has a label 'File name:' followed by a text box containing the path 'C:\sw\WebRA-v1.0-Win64-01Oct2019\setup\certs\Root CA.cer' and a 'Browse...' button. Below this, a 'Note' states: 'More than one certificate can be stored in a single file in the following formats:'. This is followed by three bullet points: 'Personal Information Exchange- PKCS #12 (.PFX,.P12)', 'Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)', and 'Microsoft Serialized Certificate Store (.SST)'. At the bottom right, there are 'Next' and 'Cancel' buttons.

← Certificate Import Wizard

File to Import
Specify the file you want to import.

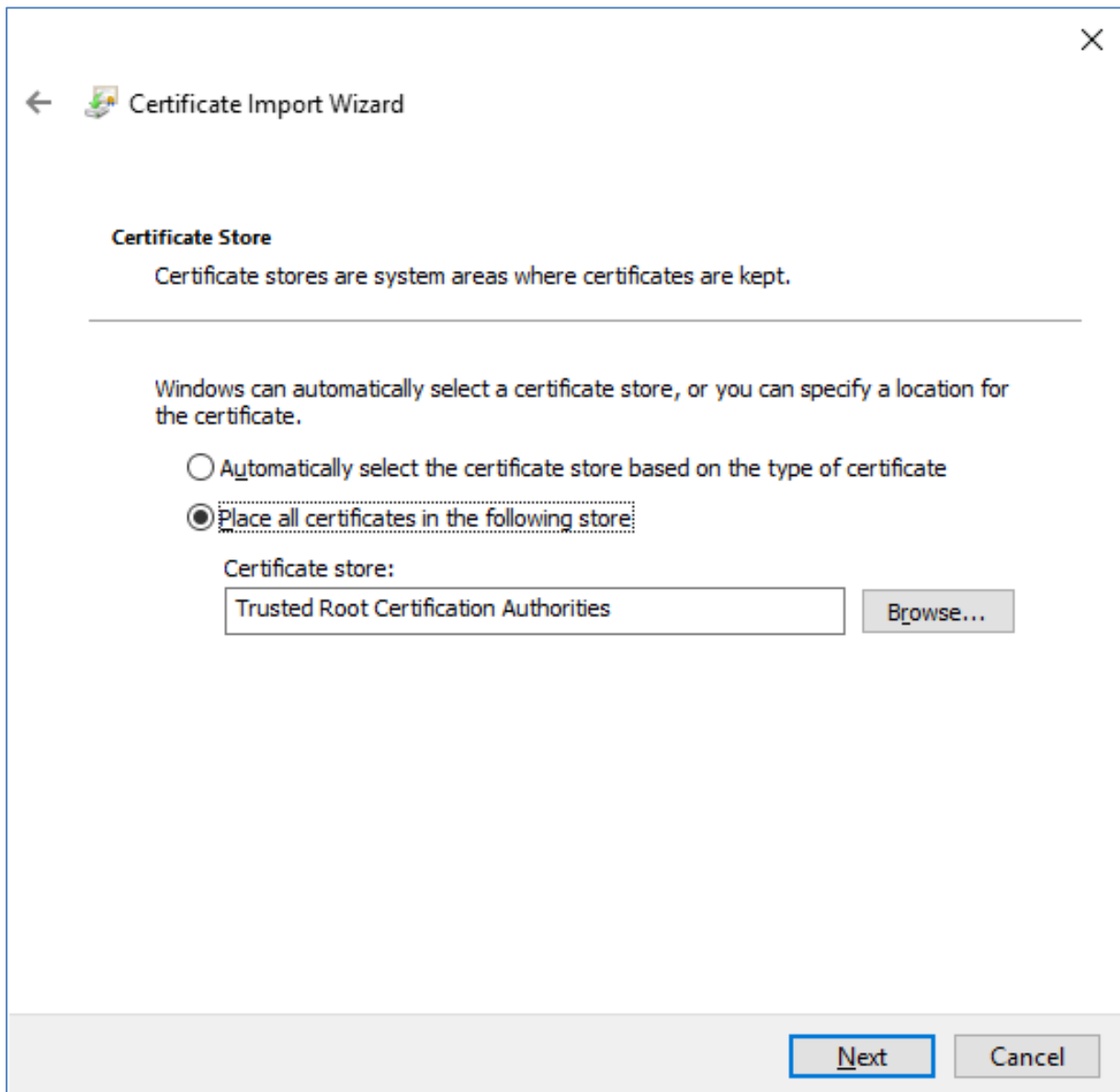
File name:
C:\sw\WebRA-v1.0-Win64-01Oct2019\setup\certs\Root CA.cer Browse...

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Next Cancel

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



The image shows a Windows 'Certificate Import Wizard' dialog box. At the top, there is a back arrow and the title 'Certificate Import Wizard'. Below this, the section 'Certificate Store' is highlighted. A descriptive text states: 'Certificate stores are system areas where certificates are kept.' A horizontal line separates this from the next section. The next section explains: 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is unselected) and 'Place all certificates in the following store:' (which is selected). Below the selected option, there is a text box labeled 'Certificate store:' containing the text 'Trusted Root Certification Authorities'. To the right of this text box is a 'Browse...' button. At the bottom right of the dialog, there are two buttons: 'Next' (which is highlighted with a blue border) and 'Cancel'.

← Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store:

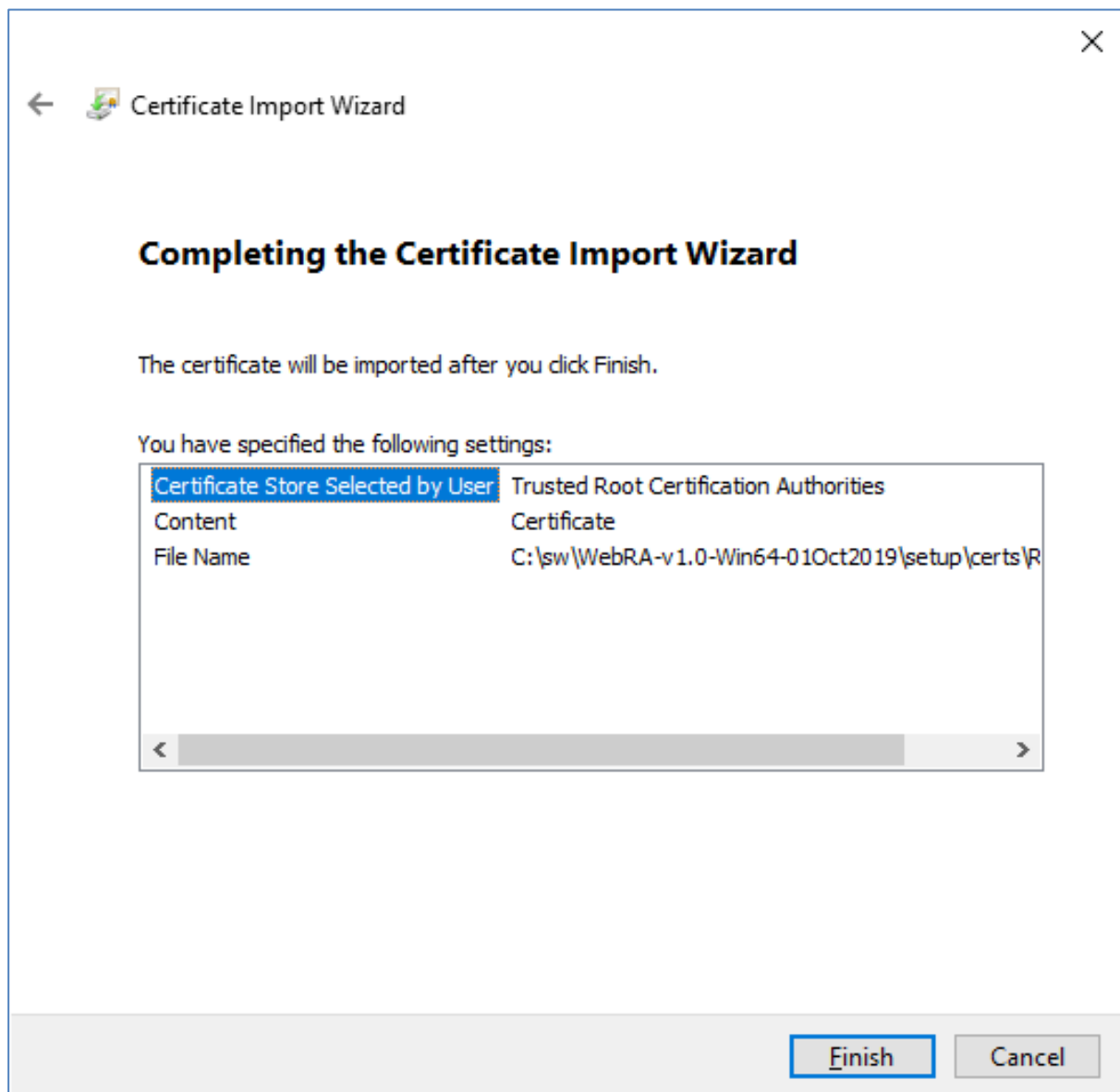
Certificate store:

Trusted Root Certification Authorities

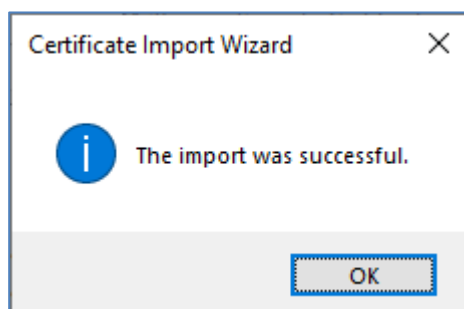
Browse...

Next Cancel

Click **Next** to proceed.



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

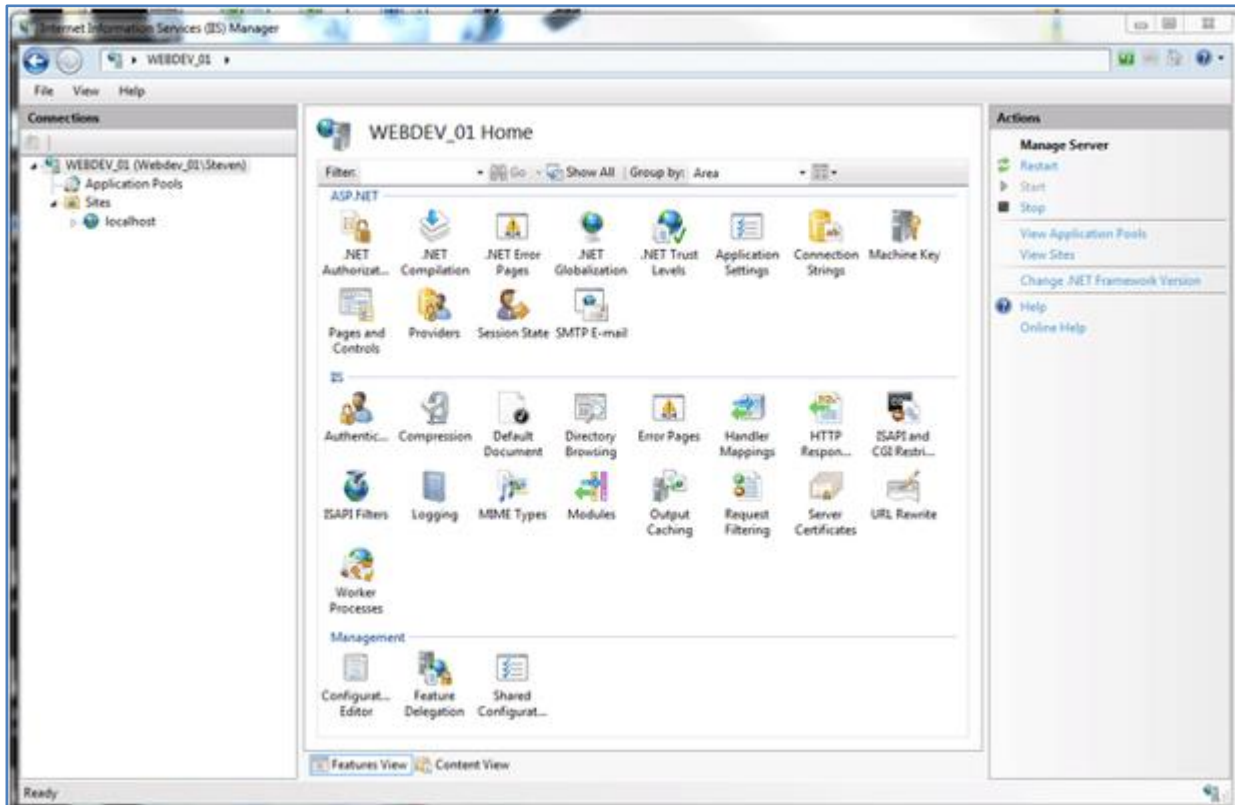


A prompt will appear informing about the successful import of the certificate.

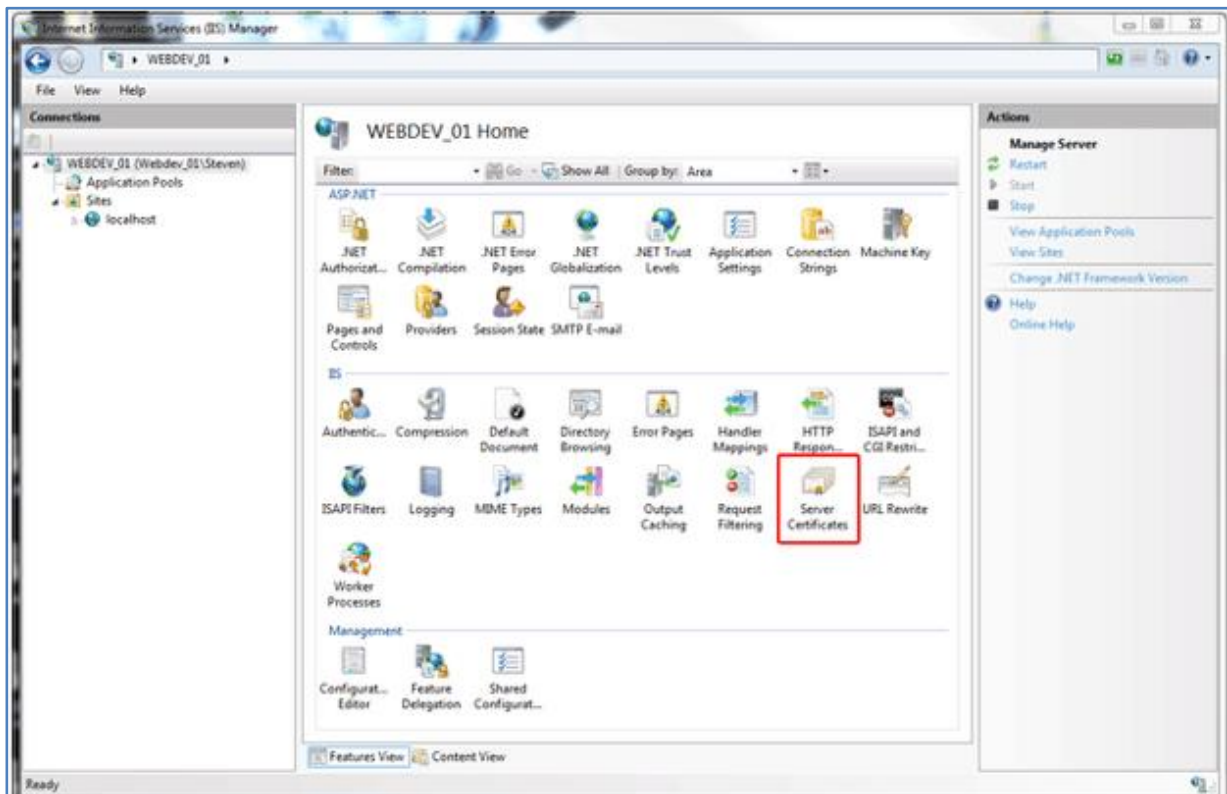
If you want to deploy the application for testing purpose you may want to use a self-signed certificate for proof of concept.

6.4 Generate a Self -Signed Certificate

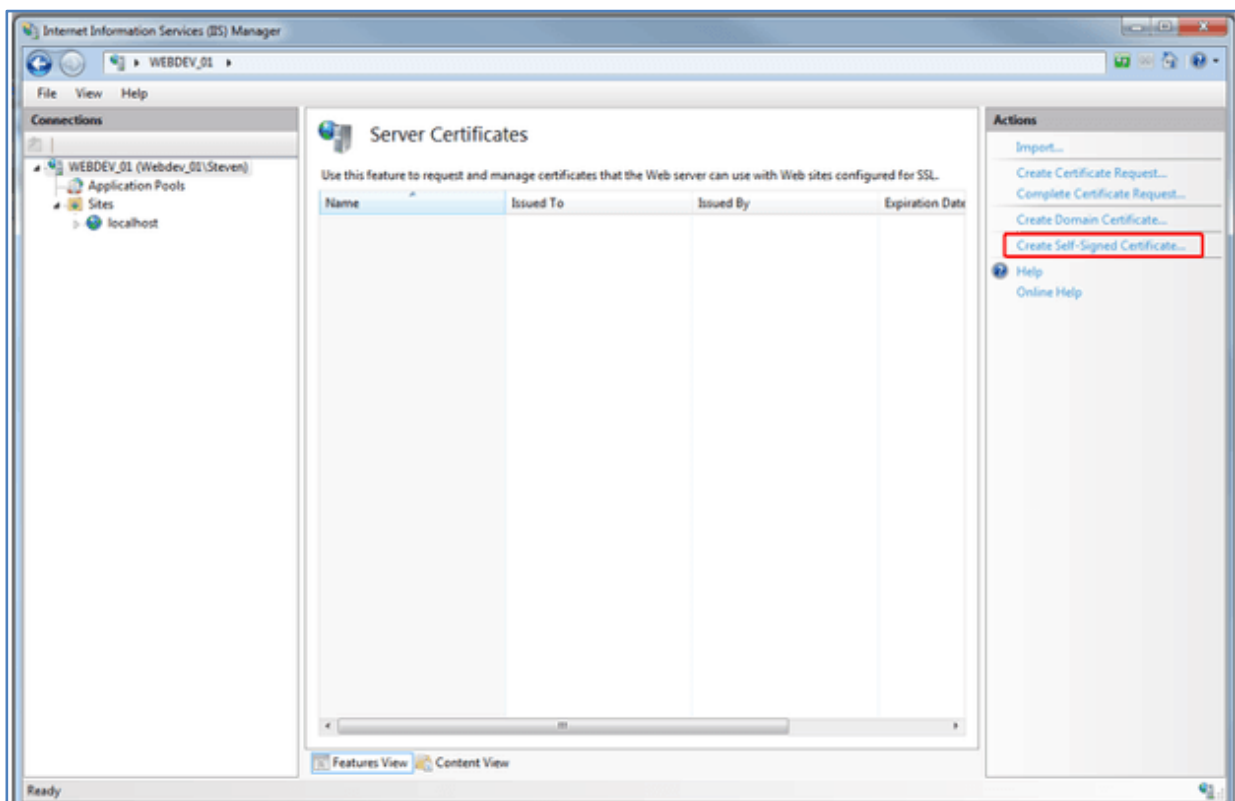
For testing purpose or a proof of concepts, mostly a self-signed certificate will be needed. It is easy to create a self-signed certificate with IIS. Launch the IIS



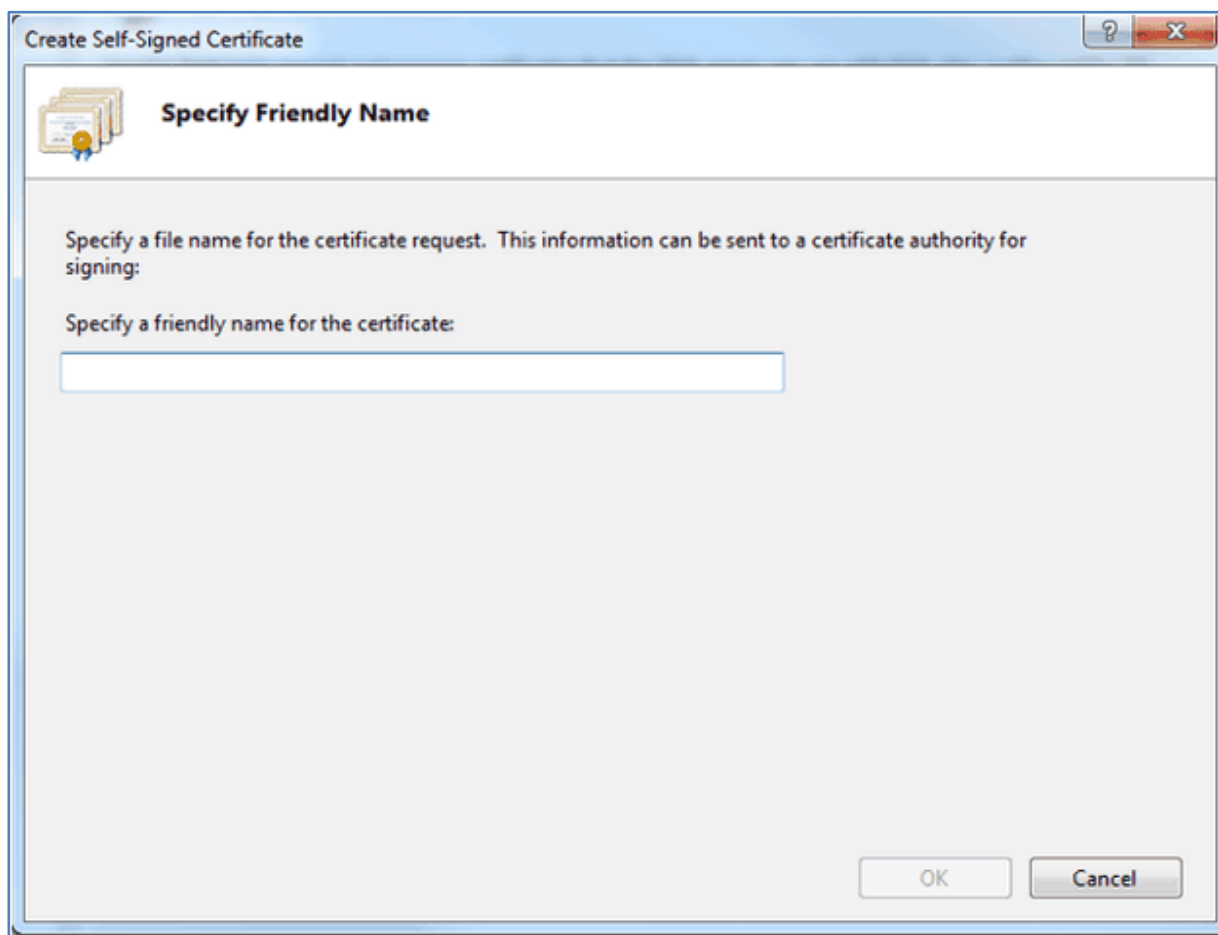
Click the **server name** from the left menu of **connections**



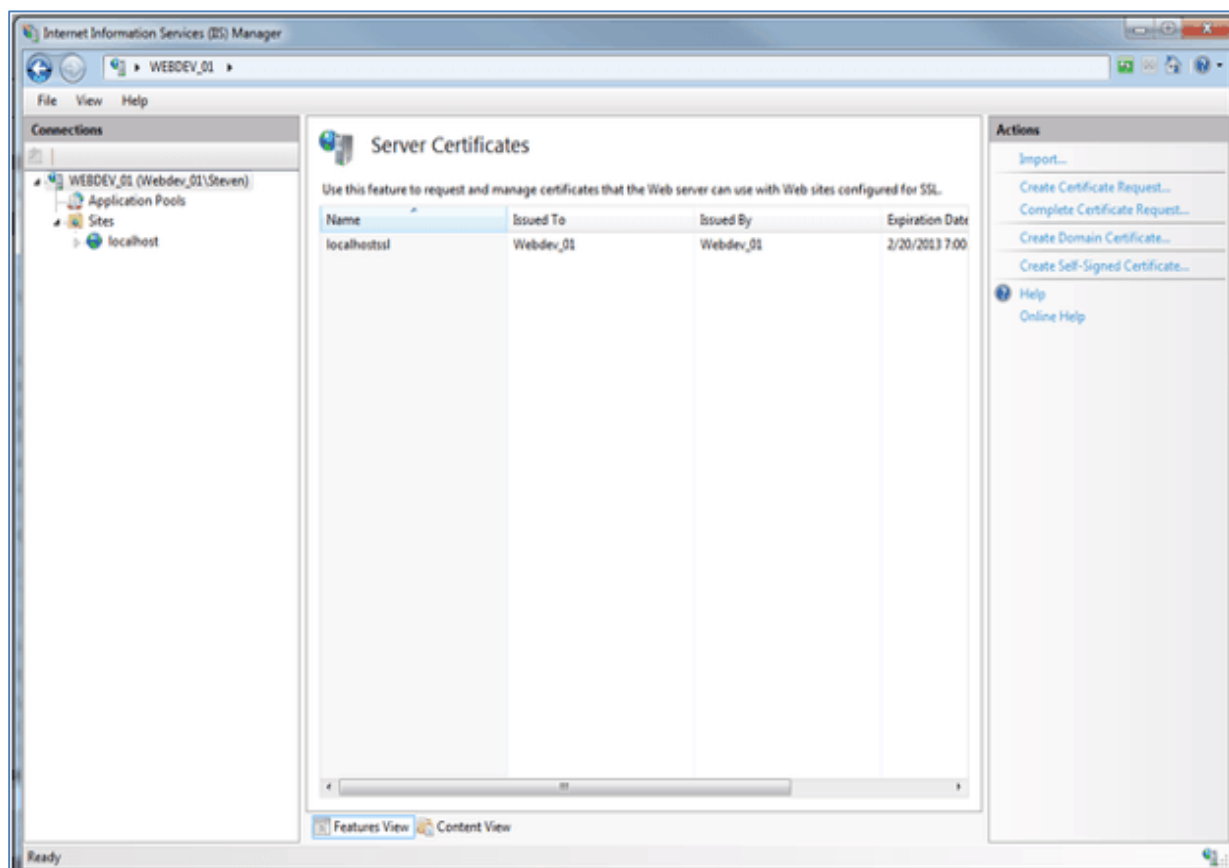
Double click **Server Certificates** from the IIS section in the middle panel.



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



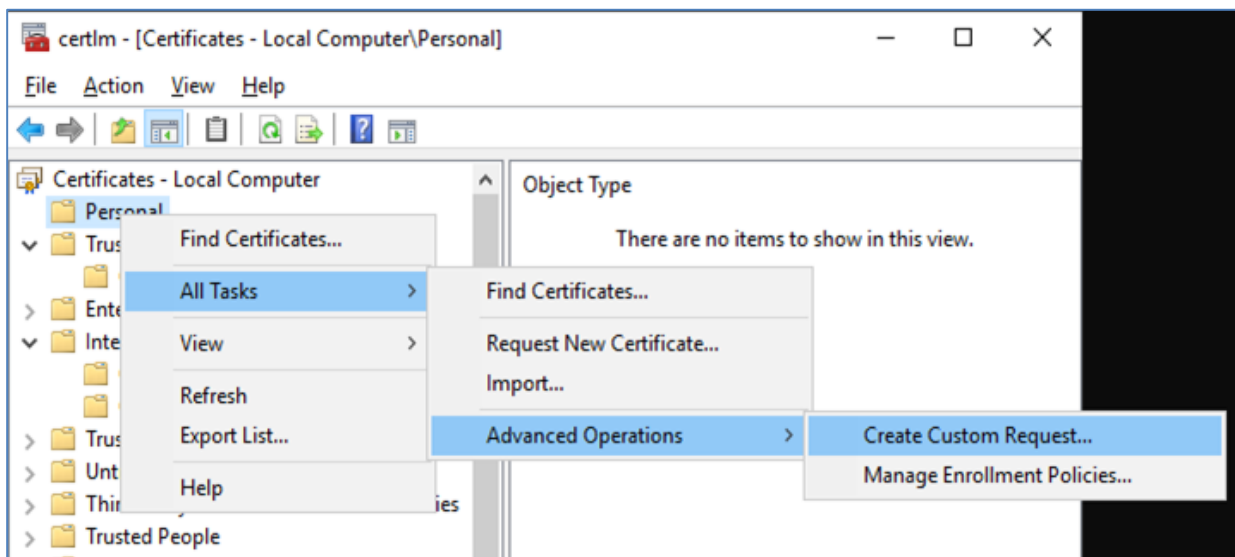
Provide a meaningful name and press **OK**



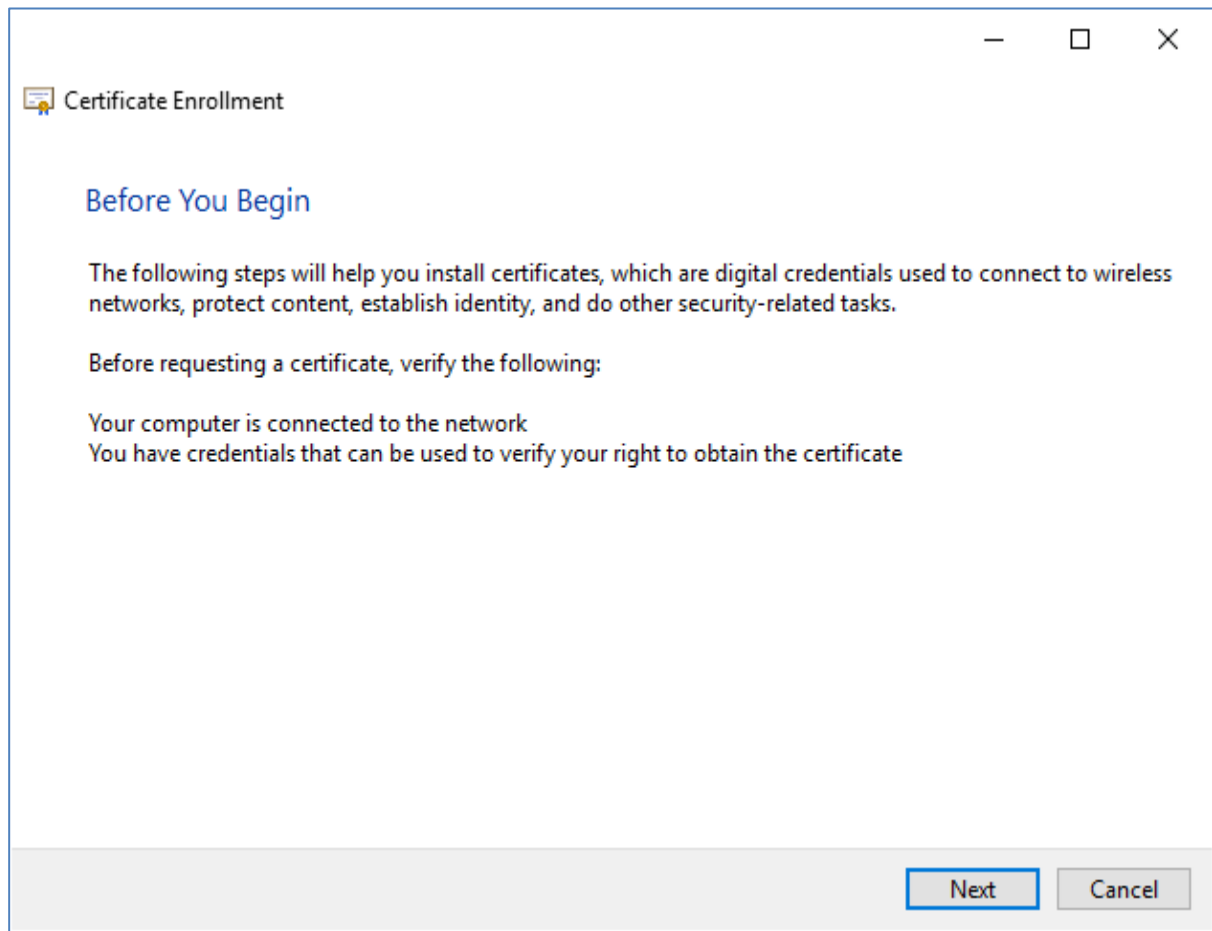
Now you have an SSL certificate that is self-signed and has a validity of 1 year. You can select this certificate for creation of HTTPS binding for test and proof of concepts purposes.

6.5 Generate a CSR for an SSL Certificate

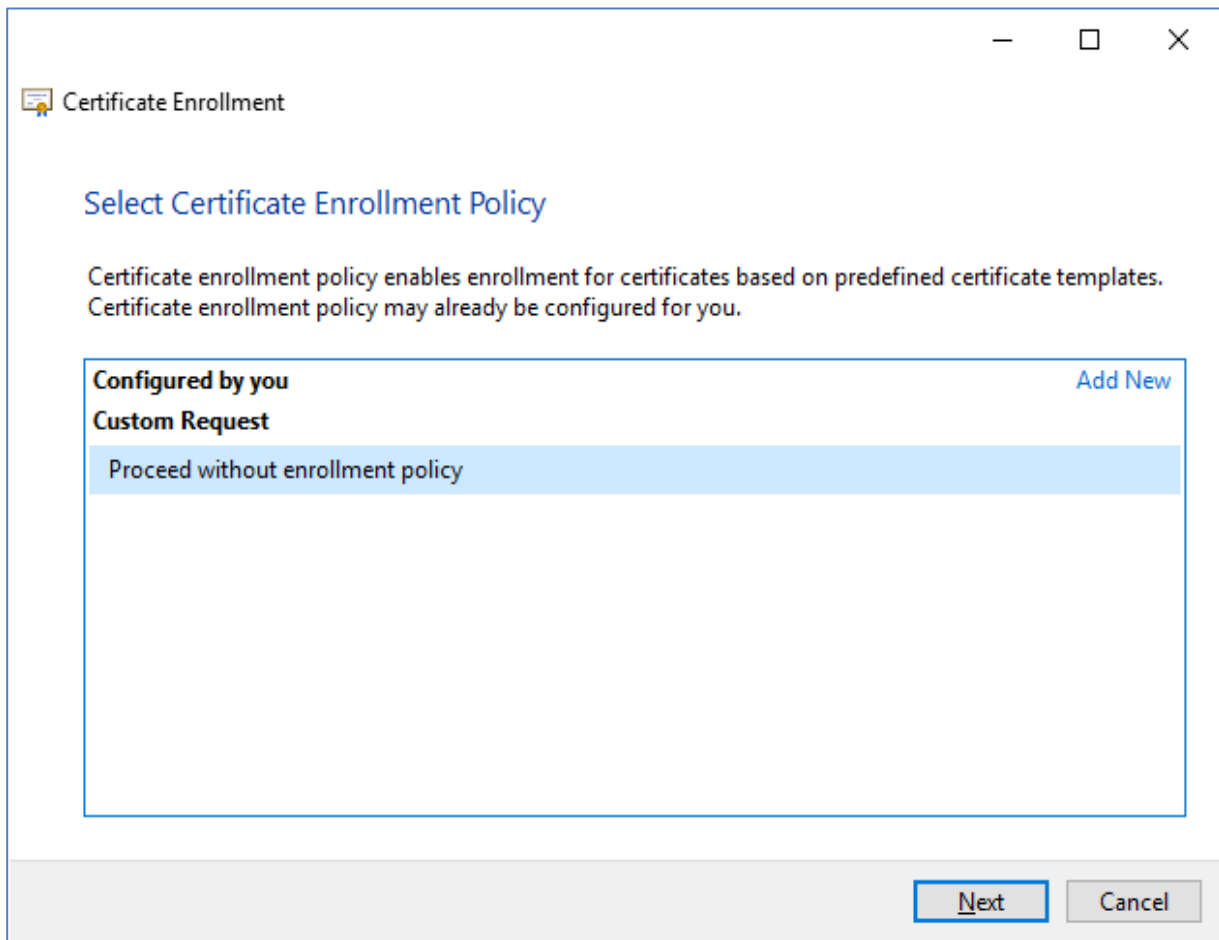
To generate a self-signed SSL certificate from IIS, launch **certlm.msc** from the command prompt.



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



Press **Next** to proceed.



The image shows a Windows-style window titled "Certificate Enrollment". It has a title bar with minimize, maximize, and close buttons. The main content area has a heading "Select Certificate Enrollment Policy" in blue. Below the heading is a paragraph: "Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you." Below this is a box titled "Configured by you" with an "Add New" link in the top right corner. Inside this box, under the sub-heading "Custom Request", there is a single list item "Proceed without enrollment policy" which is highlighted with a light blue background. At the bottom right of the window are two buttons: "Next" (highlighted with a blue border) and "Cancel".

Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

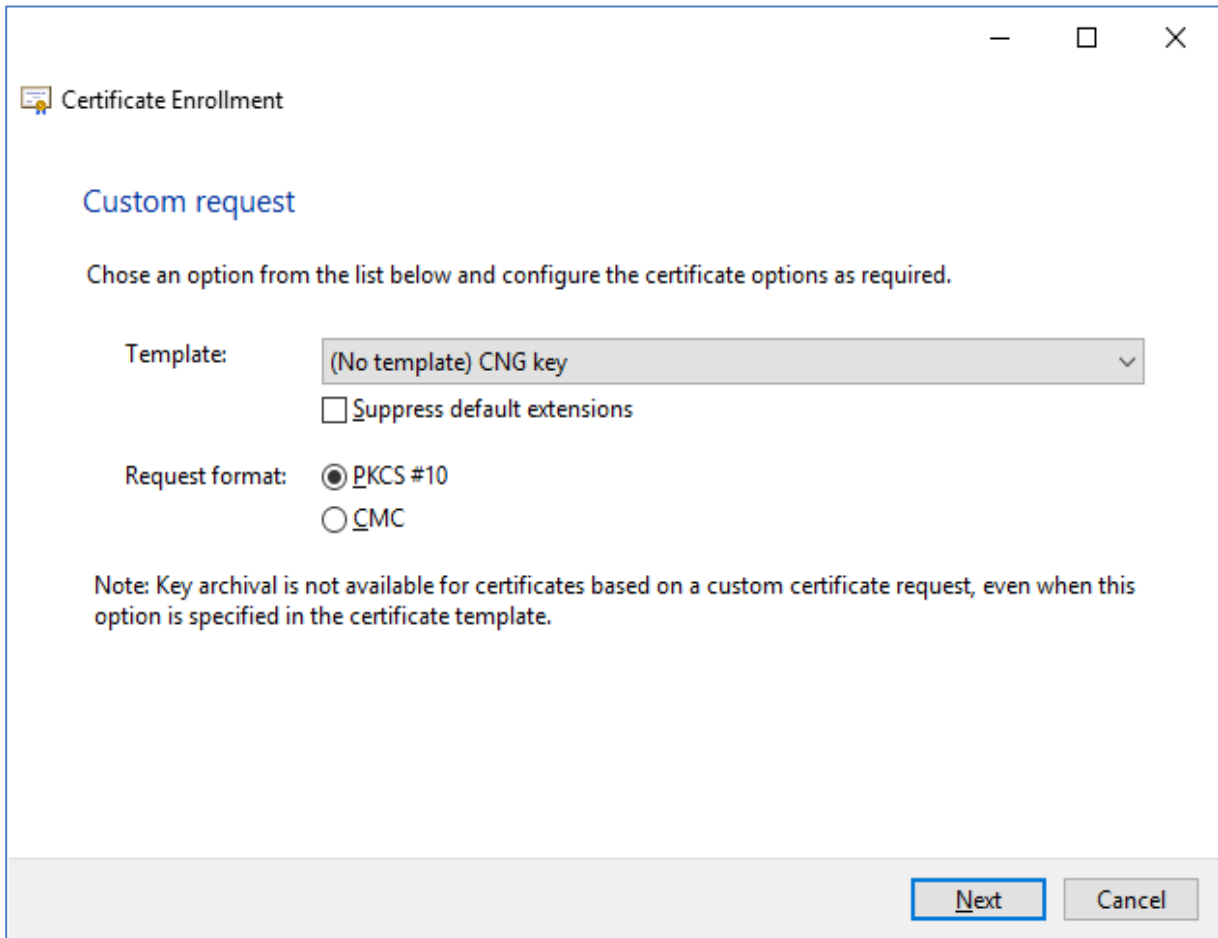
Configured by you [Add New](#)

Custom Request

- Proceed without enrollment policy

Next **Cancel**

Select **Proceed without enrollment policy** and press **Next**.



The image shows a 'Certificate Enrollment' dialog box with a title bar containing standard Windows window controls. The main content area is titled 'Custom request' in blue. Below this, a message states: 'Chose an option from the list below and configure the certificate options as required.' There are two configuration sections. The first, 'Template:', features a dropdown menu currently showing '(No template) CNG key' and a checkbox labeled 'Suppress default extensions' which is unchecked. The second, 'Request format:', has two radio button options: 'PKCS #10' (which is selected) and 'CMC'. A note at the bottom of the main area reads: 'Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.' At the bottom right of the dialog, there are two buttons: 'Next' and 'Cancel'.

Certificate Enrollment

Custom request

Chose an option from the list below and configure the certificate options as required.

Template: (No template) CNG key

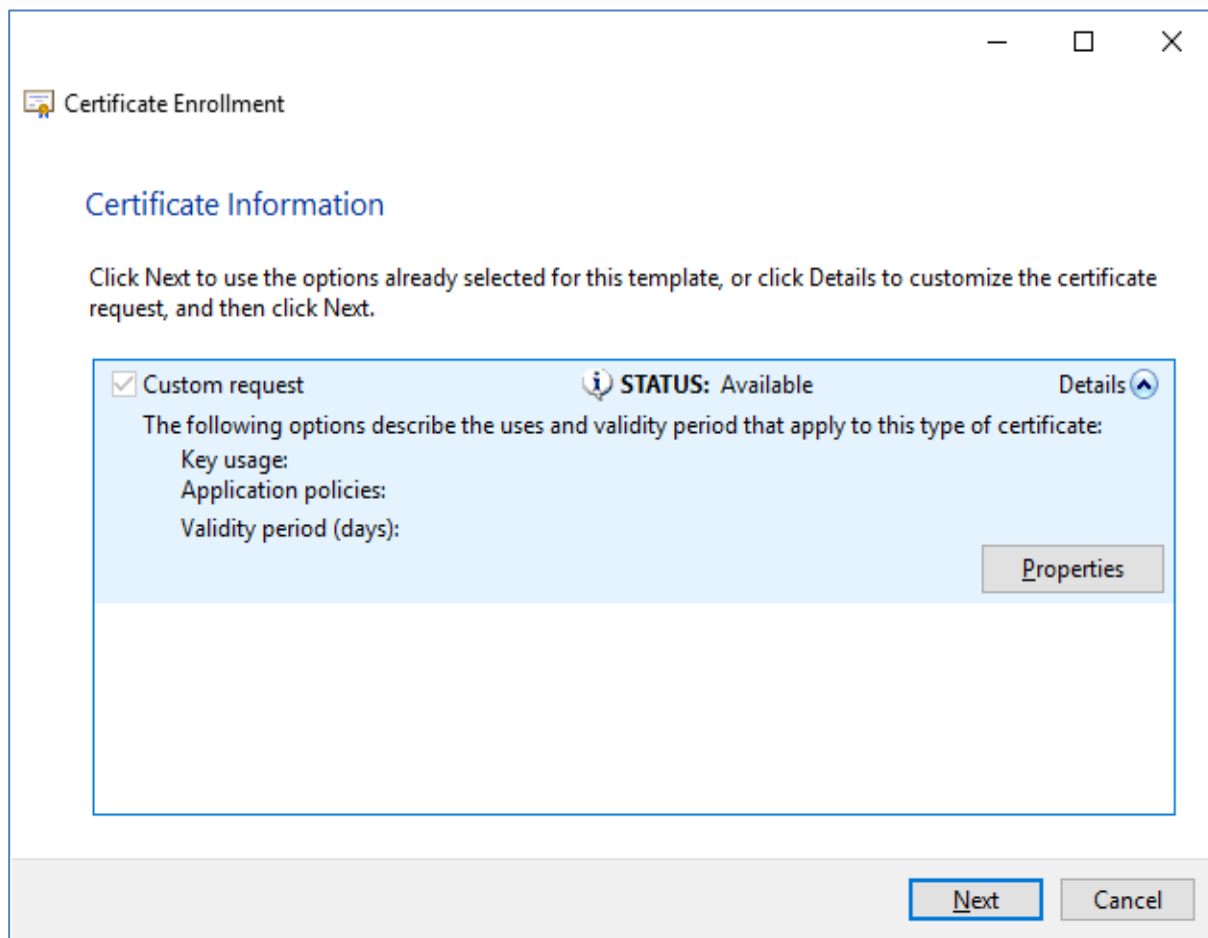
☐ Suppress default extensions

Request format: ☒ PKCS #10
☐ CMC

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Next Cancel

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



The image shows a 'Certificate Enrollment' window. At the top, there's a title bar with standard window controls. Below the title bar, the window is titled 'Certificate Enrollment'. Underneath, there's a section header 'Certificate Information'. A paragraph of text instructs the user: 'Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.' Below this text is a light blue bordered box. Inside this box, on the left, is a checked checkbox labeled 'Custom request'. To its right, there's a status indicator 'STATUS: Available' with an information icon. Further right is a 'Details' link with an upward arrow. Below these, the text says 'The following options describe the uses and validity period that apply to this type of certificate:' followed by three lines: 'Key usage:', 'Application policies:', and 'Validity period (days):'. A 'Properties' button is located on the right side of this light blue box. At the bottom of the window, outside the light blue box, are two buttons: 'Next' and 'Cancel'.

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☒ Custom request STATUS: Available Details

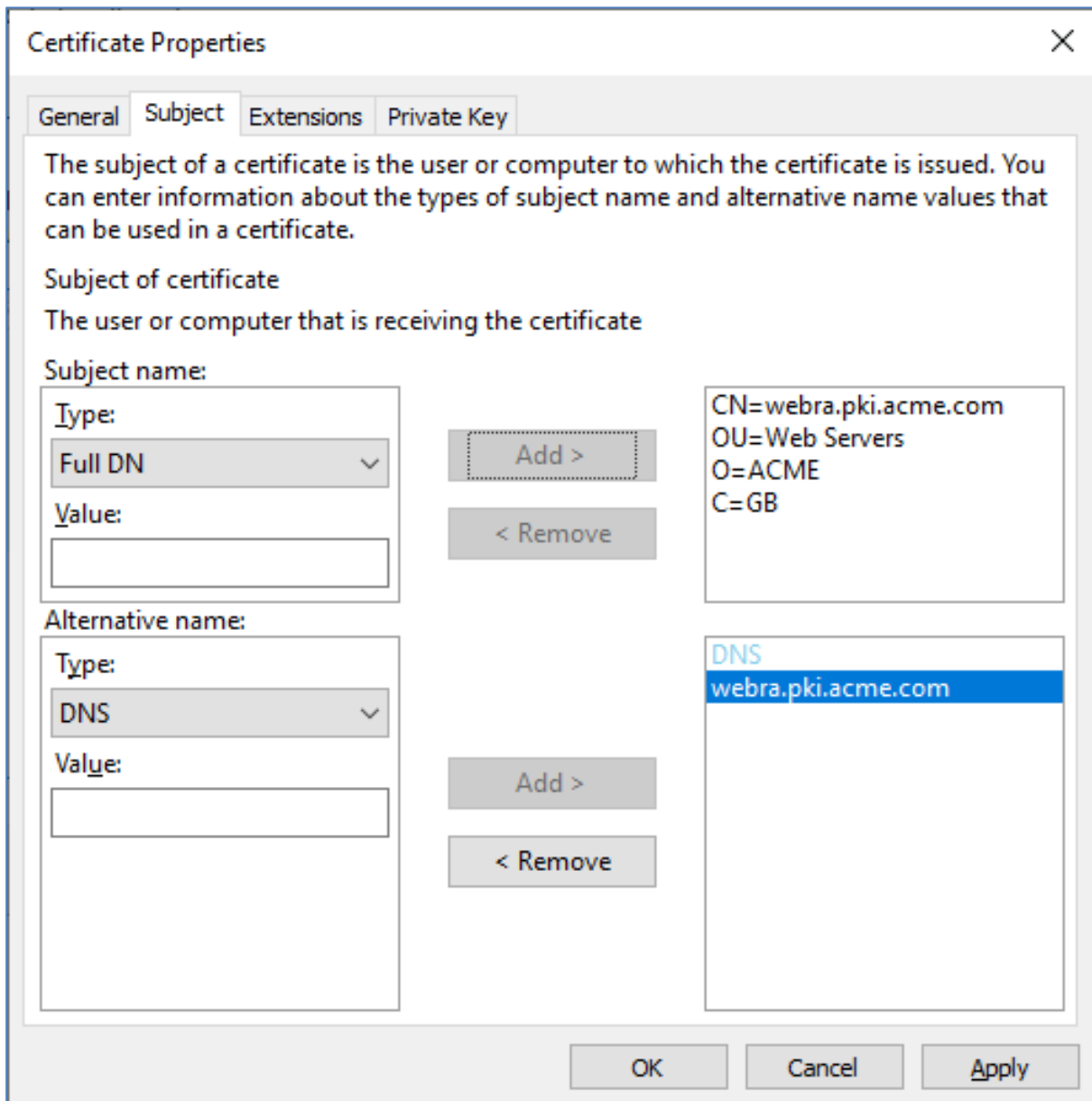
The following options describe the uses and validity period that apply to this type of certificate:

Key usage:
Application policies:
Validity period (days):

Properties

Next Cancel

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



The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type:
Full DN

Add >

< Remove

Value:

CN=webra.pki.acme.com
OU=Web Servers
O=ACME
C=GB

Alternative name:

Type:
DNS

Add >

< Remove

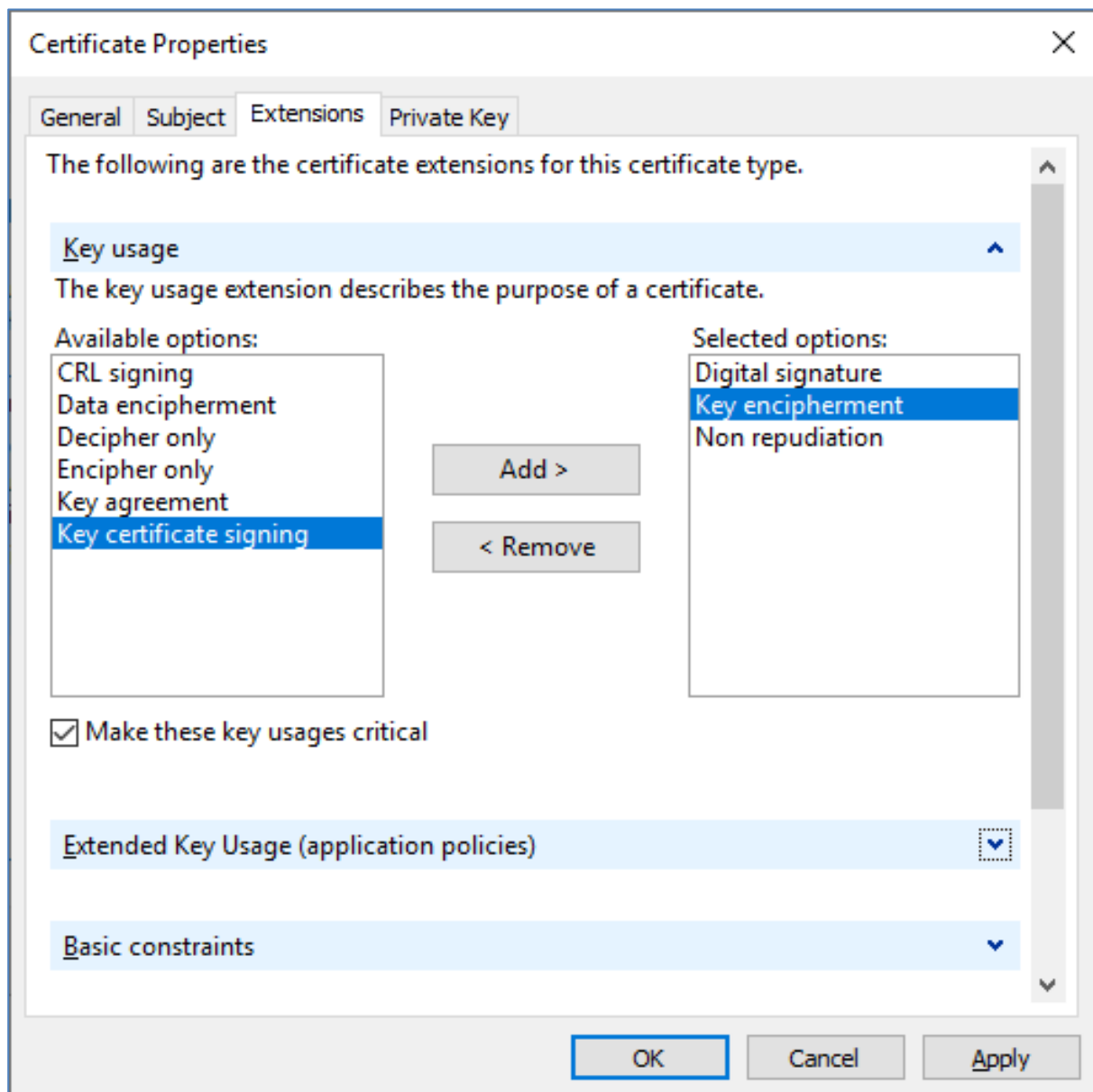
Value:

DNS
webra.pki.acme.com

OK Cancel Apply

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**.

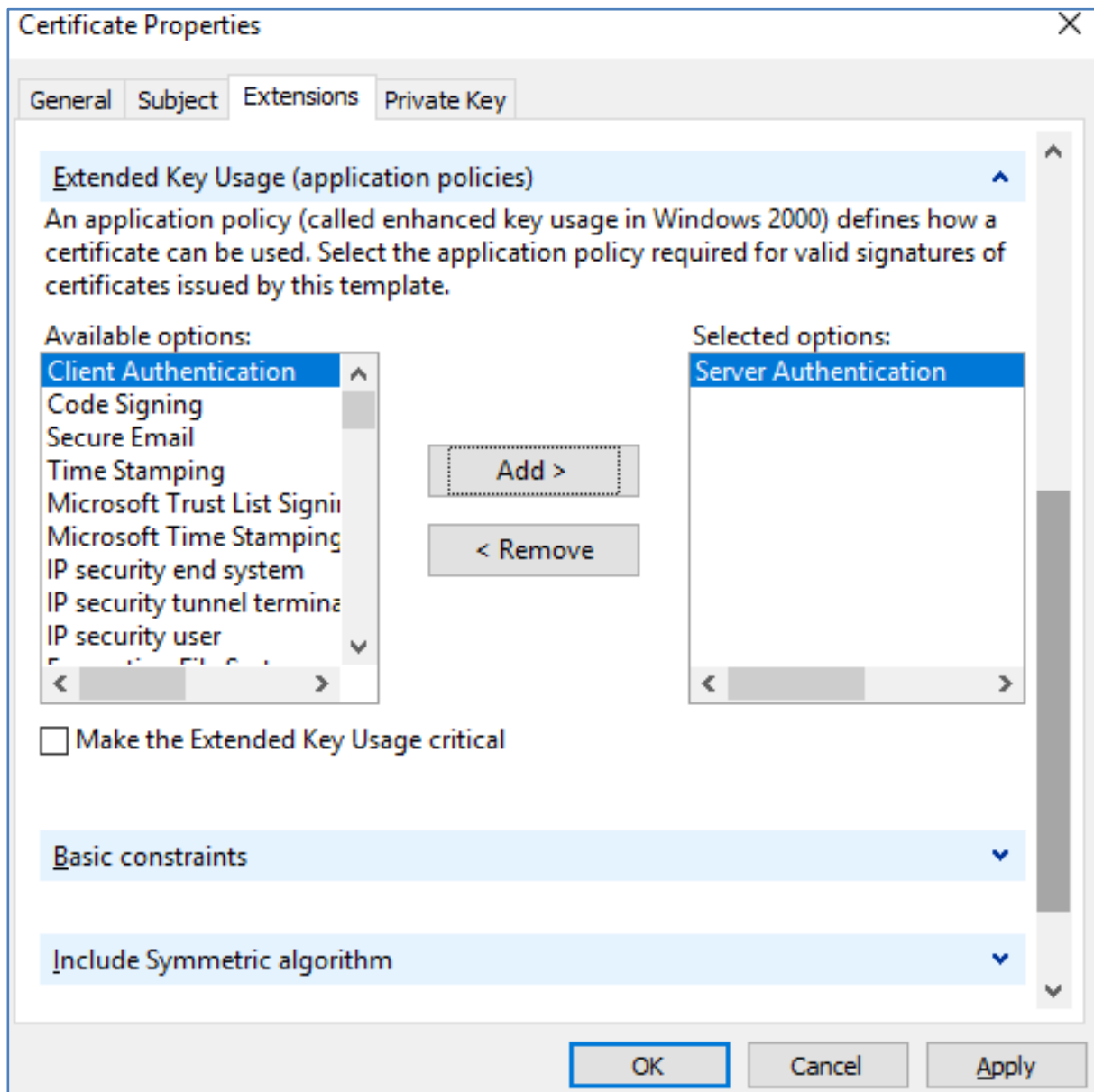
Note, these values are the sample values for the certificate and can be replaced with the realistic data.



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:

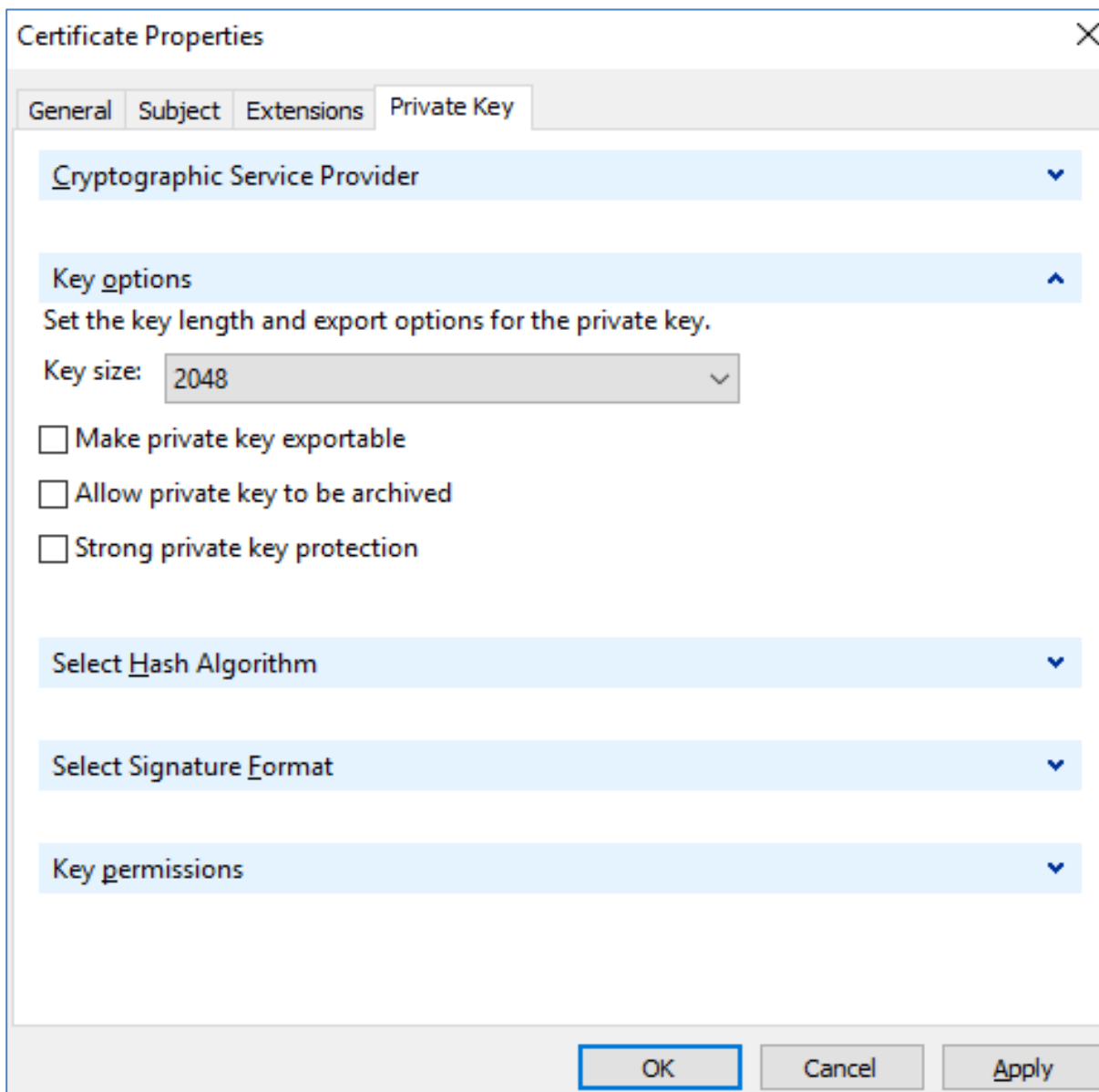
- Digital signature
- Key encipherment
- Non repudiation

Make sure the check box against **Make these key usages critical** is checked.



Now select the **Extended Key Usage (application policies)** from the drop down, and select the following from the available options:

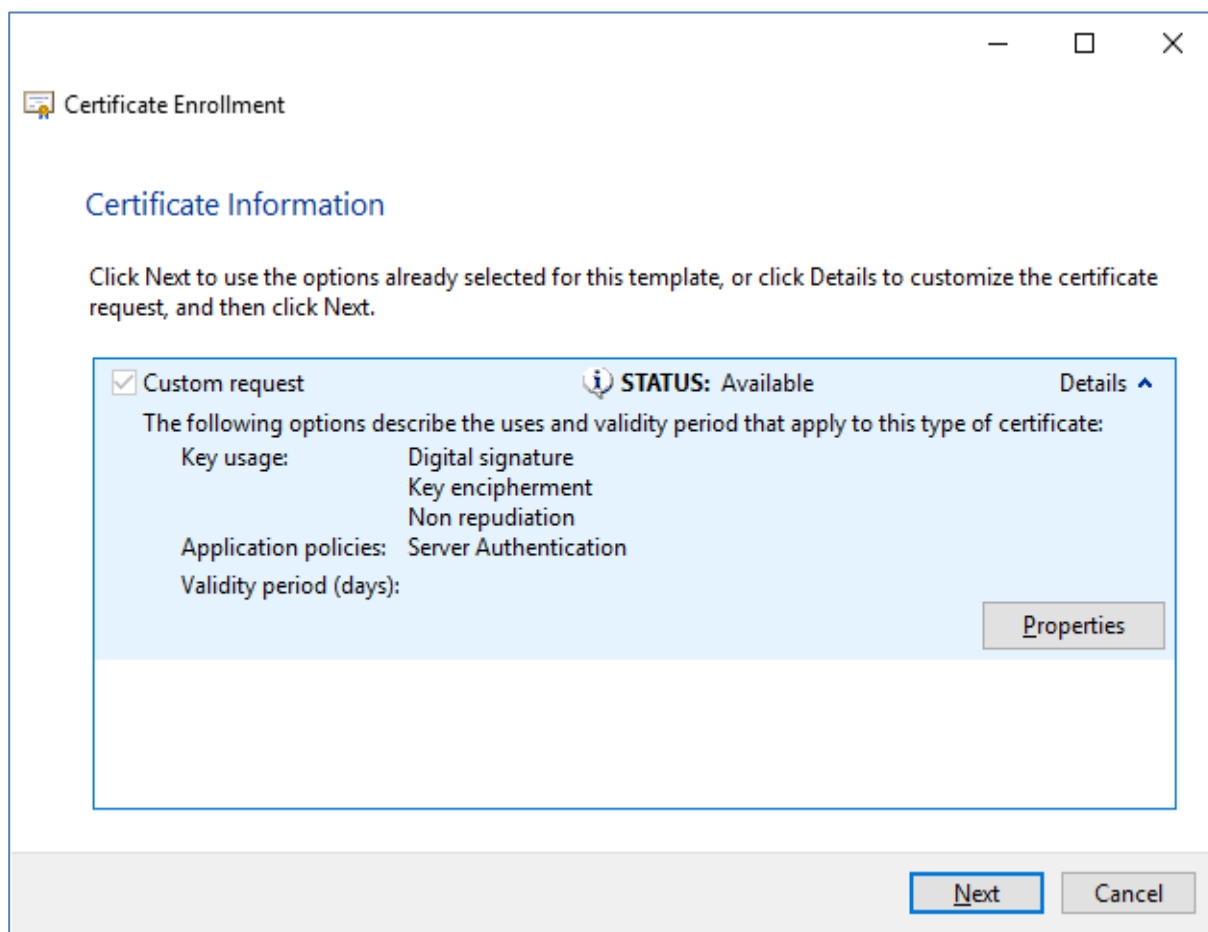
- Server Authentication



The image shows a 'Certificate Properties' dialog box with the 'Private Key' tab selected. The dialog has a title bar with a close button (X). Below the title bar are four tabs: 'General', 'Subject', 'Extensions', and 'Private Key'. The 'Private Key' tab is active and contains the following elements:

- A dropdown menu labeled 'Cryptographic Service Provider' with a downward arrow.
- A section titled 'Key options' with an upward arrow. Below this title is the text 'Set the key length and export options for the private key.' and a 'Key size:' dropdown menu set to '2048'.
- Three unchecked checkboxes:
 - ☐ Make private key exportable
 - ☐ Allow private key to be archived
 - ☐ Strong private key protection
- A dropdown menu labeled 'Select Hash Algorithm' with a downward arrow.
- A dropdown menu labeled 'Select Signature Format' with a downward arrow.
- A dropdown menu labeled 'Key permissions' with a downward arrow.
- At the bottom right are three buttons: 'OK' (highlighted with a blue border), 'Cancel', and 'Apply'.

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**. You will be back to the certificate enrollment screen



The image shows a 'Certificate Enrollment' window. At the top, there's a title bar with standard window controls. Below the title bar, the window is titled 'Certificate Enrollment'. Underneath, there's a section 'Certificate Information'. A text block instructs the user to click 'Next' to use pre-selected options or 'Details' to customize. A large light blue box contains a checked 'Custom request' option, a status indicator 'STATUS: Available', and a 'Details' link with an upward arrow. Inside this box, a list of certificate options is shown: 'Key usage' with 'Digital signature', 'Key encipherment', and 'Non repudiation'; 'Application policies' with 'Server Authentication'; and 'Validity period (days)'. A 'Properties' button is located at the bottom right of this light blue box. At the bottom of the window, there are 'Next' and 'Cancel' buttons. The 'Next' button is highlighted with a blue border.

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☒ Custom request STATUS: Available Details ^

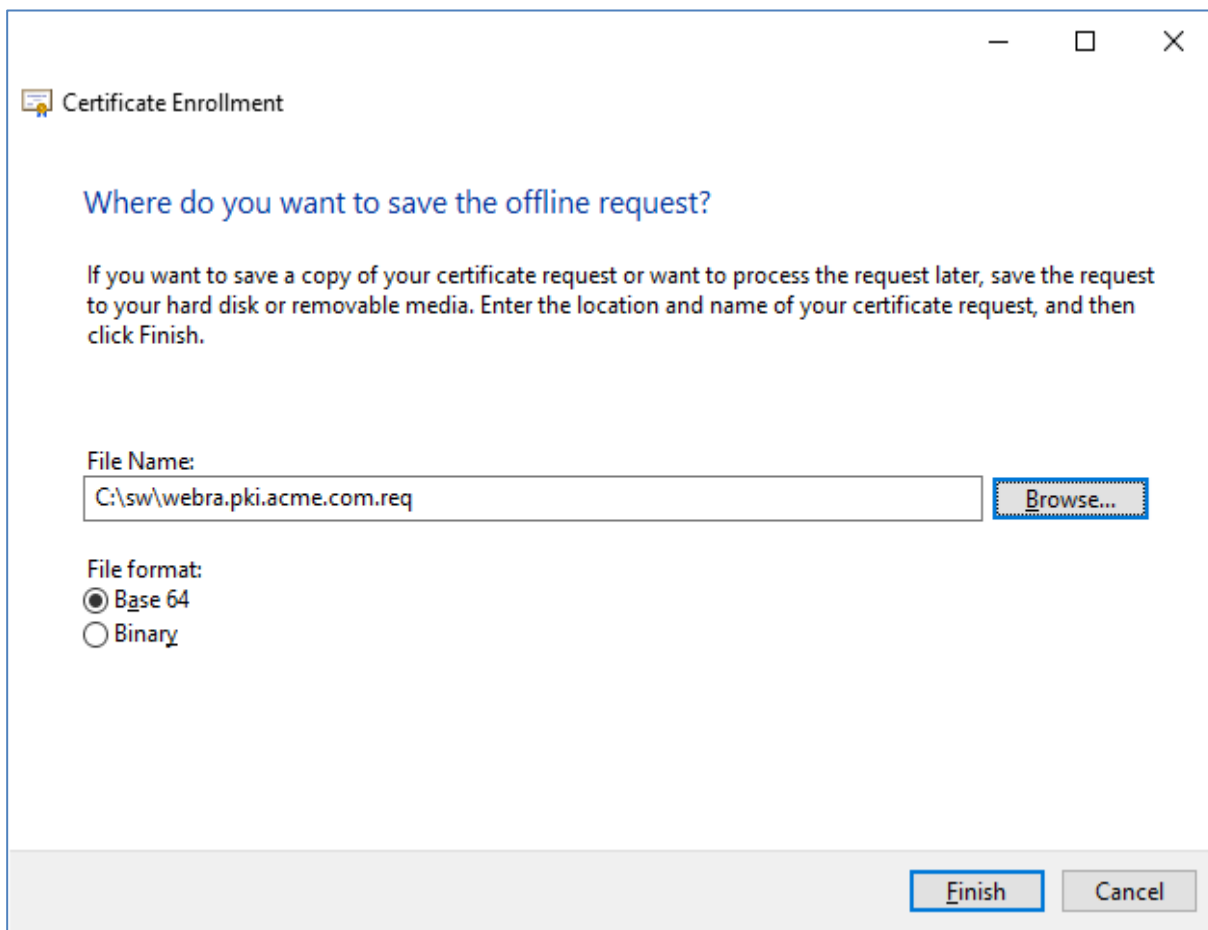
The following options describe the uses and validity period that apply to this type of certificate:

Key usage:	Digital signature
	Key encipherment
	Non repudiation
Application policies:	Server Authentication
Validity period (days):	

Properties

Next Cancel

Press **Next** to proceed.



The image shows a Windows-style dialog box titled "Certificate Enrollment". It has a standard title bar with minimize, maximize, and close buttons. The main content area has a blue heading "Where do you want to save the offline request?". Below this is a paragraph of instructions: "If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish." There is a "File Name:" label followed by a text input field containing "C:\sw\webra.pki.acme.com.req" and a "Browse..." button. Below this is a "File format:" label with two radio button options: "Base 64" (which is selected) and "Binary". At the bottom right, there are "Finish" and "Cancel" buttons.

Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:
C:\sw\webra.pki.acme.com.req Browse...

File format:
☒ Base 64
☐ Binary

Finish Cancel

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 ***