Web RA Installation Guide

ASCERTIA LTD

MAY 2021

Document Version- 2.2

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

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 Web RA.

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.
- 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

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
Server System	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012
Hard Disk Space	• 200 GB (Minimum)
Memory	• 16 GB (Minimum) • 24 GB (If the number of concurrent users is higher) • 32 GB (If the database is also on the same server as the Web RA)
Processor	• A modern multi-core CPU such as Xeon E3-XXXX or E5-XXXX series is recommended
Processor Type	• x64
HSM (Optional)	• 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
IIS	- IIS 10
IIS Rewrite Module	- v2.1
.Net Framework	- .Net Framework 4.6.1 or above - .Net Core 3.1
.Net Core SDK	- Dotnet-sdk-3.1.101
.Net Core Runtime & Hosting Bundle	- Dotnet-sdk-3.1.101
Database Server	- Microsoft SQL Server 2019 - Microsoft SQL Server 2017 - Microsoft SQL Server 2016 - Microsoft SQL Server 2014
Database Management Studio	- 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)**	The following browsers are supported: - Chrome 40+ - Firefox 35+ - Edge 14+ - IE 11 (Not supported by Microsoft anymore) - Safari 8+ - Opera 26+
ADSS Server	Web RA is using 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 follow 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 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. 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 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.

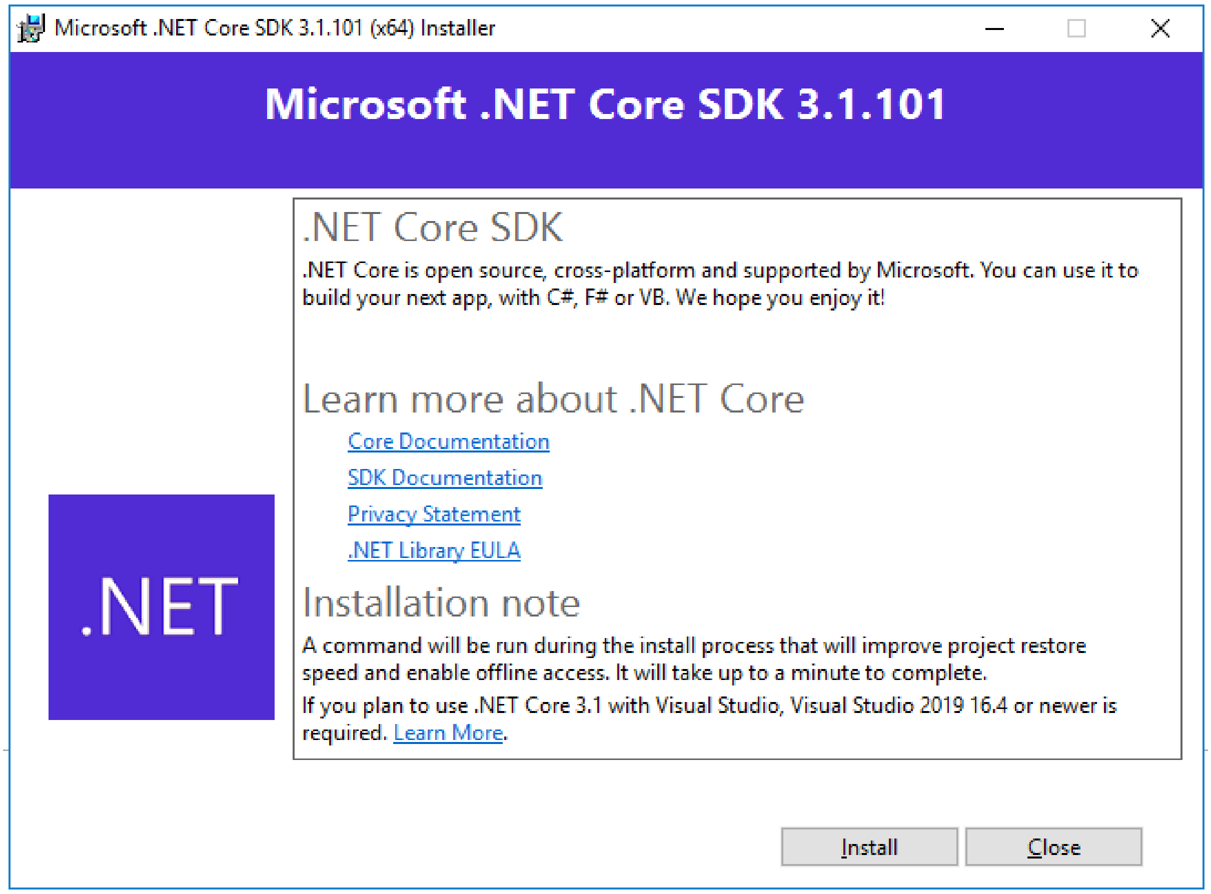
2.3 Microsoft .Net Core SDK

Web RA has been developed on the latest framework and technologies of Microsoft which are not shipped by default with Windows operating system. To run the Web RA application on an IIS and windows operating system, install Microsoft .Net Core SDK v3.1.101 from the following link.

- Download .Net Core 3.1 SDK

While downloading the setup, please ensure that the version is correct, as you need to download the same version in which your application has been developed.

Once the setup is downloaded, execute it in administrator mode i.e. Run as Administrator and the installation will begin:



Microsoft .NET Core SDK 3.1.101 (x64) Installer

Microsoft .NET Core SDK 3.1.101

.NET Core SDK

.NET Core is open source, cross-platform and supported by Microsoft. You can use it to build your next app, with C#, F# or VB. We hope you enjoy it!

Learn more about .NET Core

Core Documentation

SDK Documentation

Privacy Statement

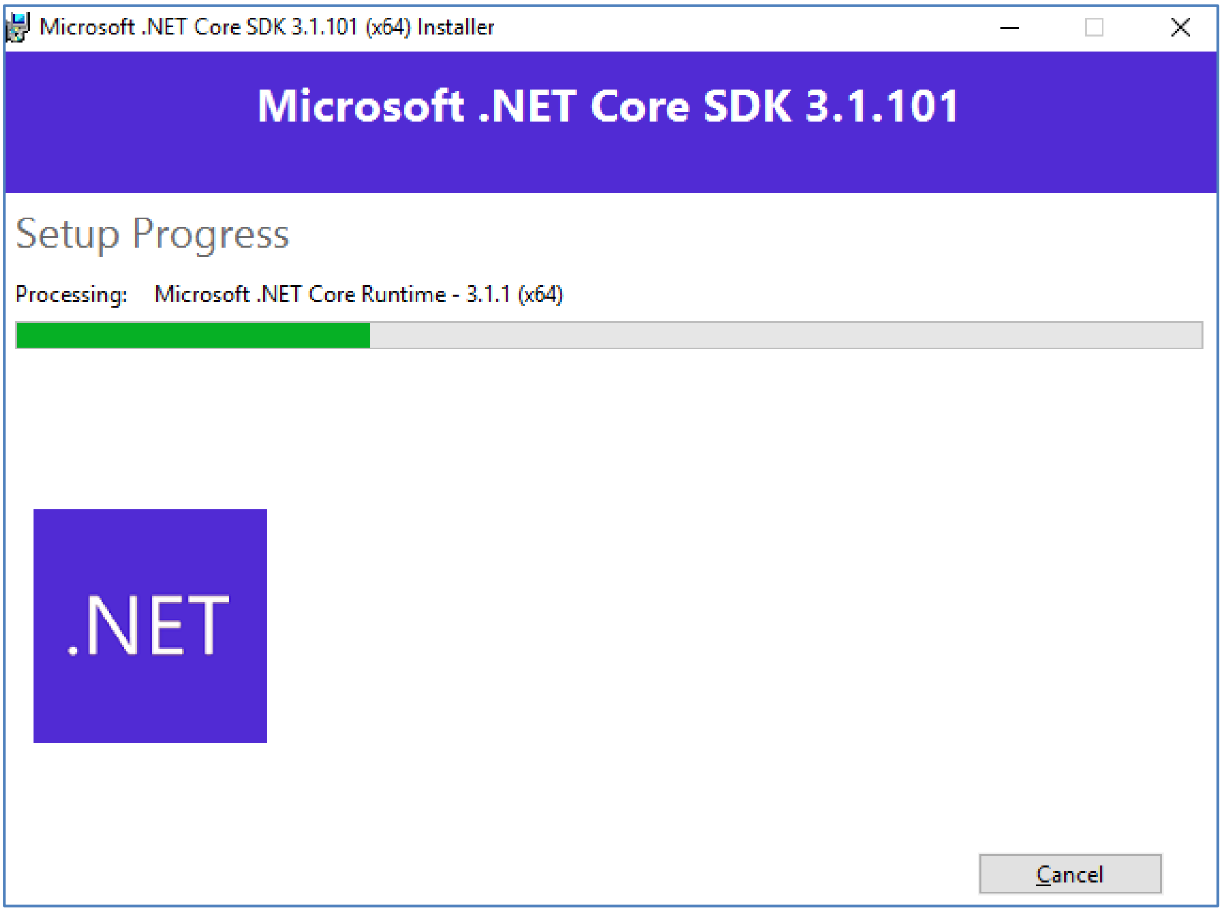
.NET Library EULA

Installation note

A command will be run during the install process that will improve project restore speed and enable offline access. It will take up to a minute to complete.

If you plan to use .NET Core 3.1 with Visual Studio, Visual Studio 2019 16.4 or newer is required. Learn More.

Click **Install** to start the installation.



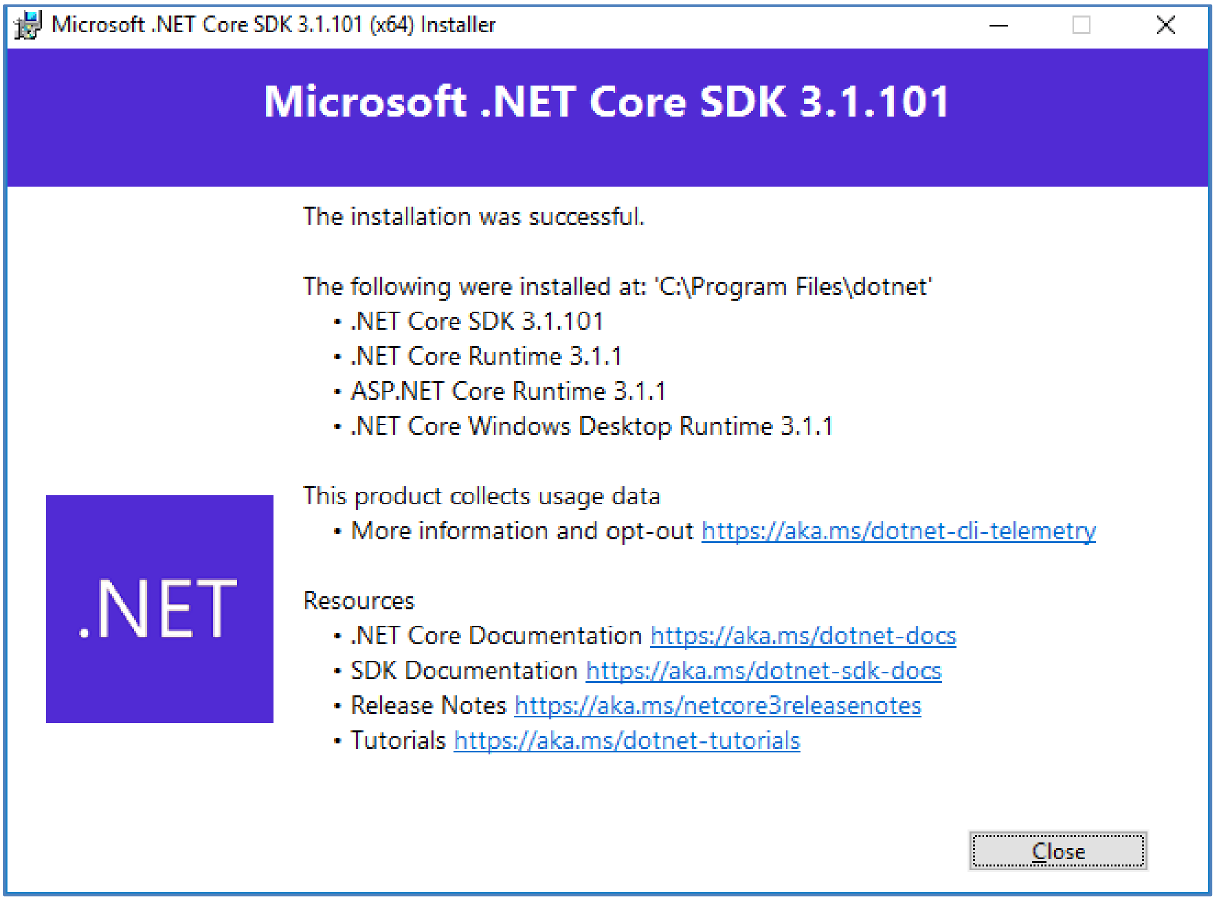
Microsoft .NET Core SDK 3.1.101 (x64) Installer

Microsoft .NET Core SDK 3.1.101

Setup Progress

Processing: Microsoft .NET Core Runtime - 3.1.1 (x64)

Let the installation complete on its own, it will take a few minutes to finish.



Microsoft .NET Core SDK 3.1.101

The installation was successful.

The following were installed at: 'C:\Program Files\dotnet'

- .NET Core SDK 3.1.101
- .NET Core Runtime 3.1.1
- ASP.NET Core Runtime 3.1.1
- .NET Core Windows Desktop Runtime 3.1.1

This product collects usage data

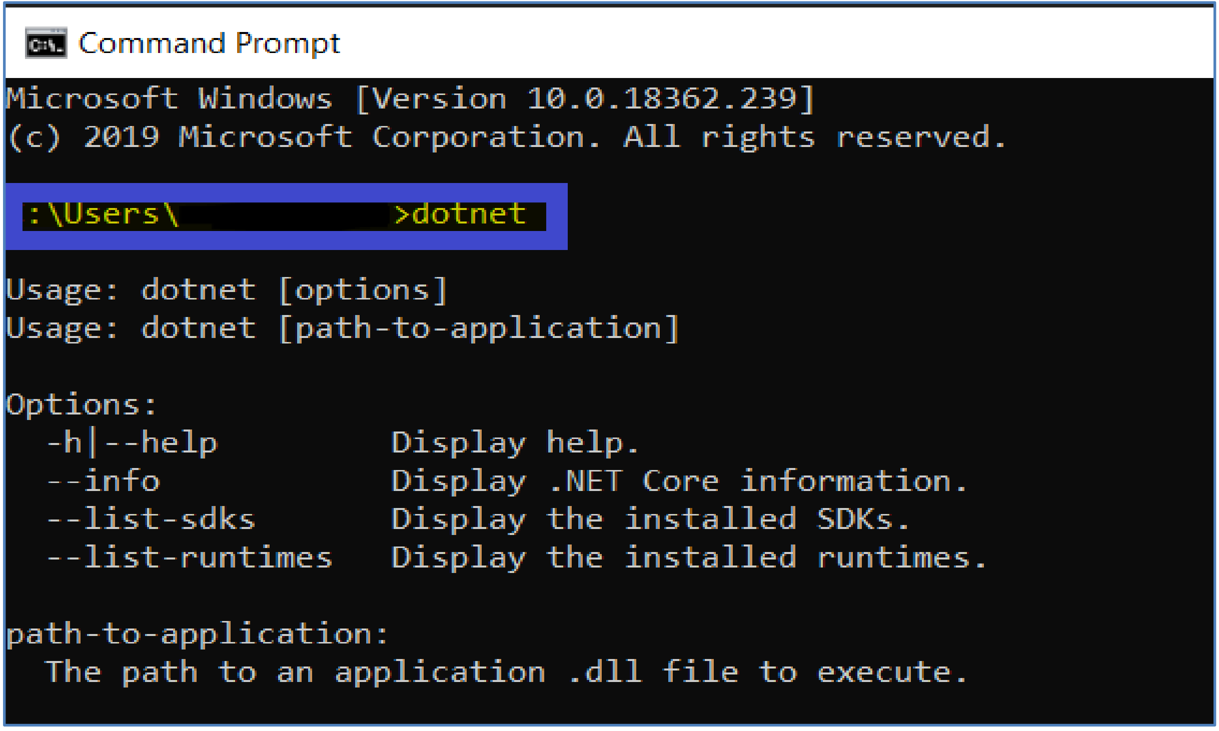
- More information and opt-out https://aka.ms/dotnet-cli-telemetry

Resources

- .NET Core Documentation https://aka.ms/dotnet-docs
- SDK Documentation https://aka.ms/dotnet-sdk-docs
- Release Notes https://aka.ms/netcore3releasenotes
- Tutorials https://aka.ms/dotnet-tutorials

Press **Close** when a successful installation is done.

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



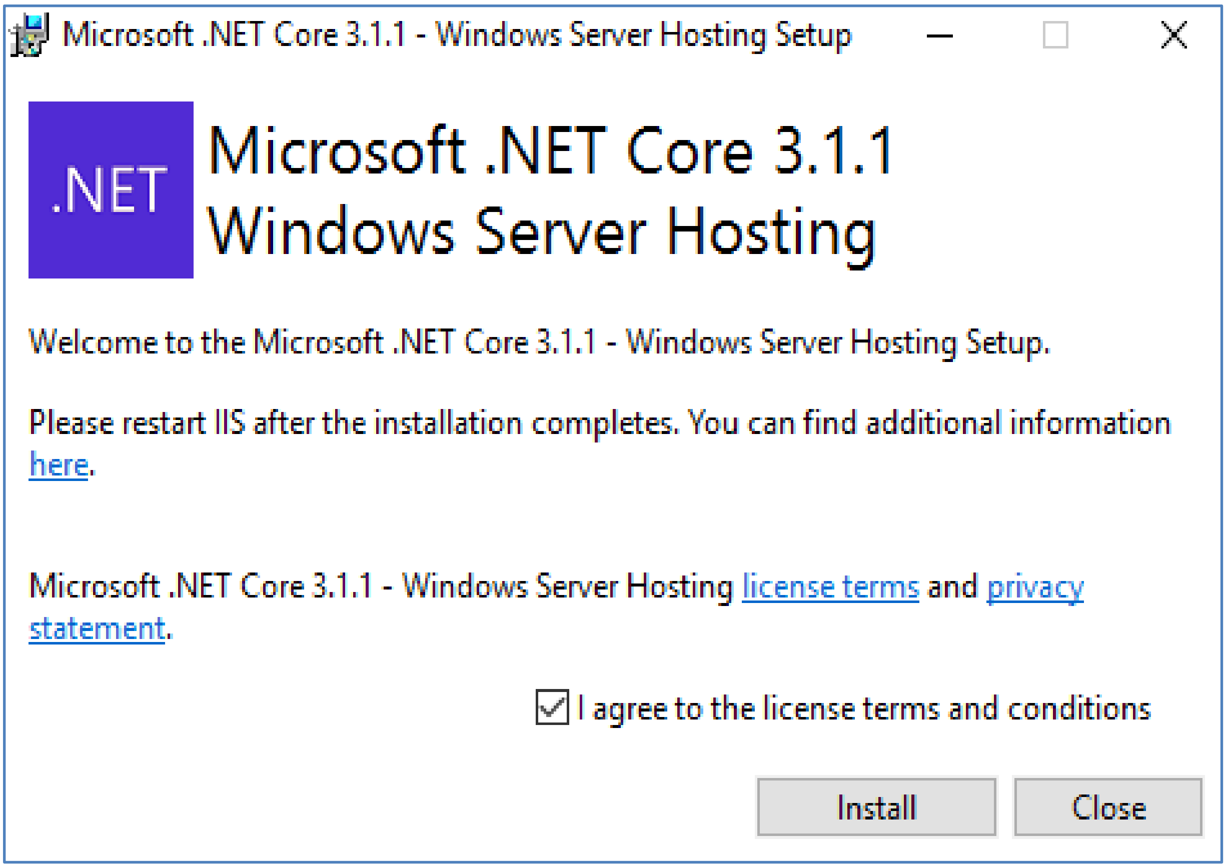
```
Microsoft Windows [Version 10.0.18362.239]
(c) 2019 Microsoft Corporation. All rights reserved.

:\Users\[redacted]>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.
```

2.4 Microsoft .Net Core 3.1.1 Runtime & Hosting Bundle

Download the Microsoft .Net Core 3.1.1 runtime and hosting bundle from the following link:

- **Microsoft .Net Core 3.1.1 Runtime & Hosting Bundle**

Once downloaded execute the installer by executing dotnet-hosting-3.1.1-win.exe



Microsoft .NET Core 3.1.1 - Windows Server Hosting Setup

Microsoft .NET Core 3.1.1 Windows Server Hosting

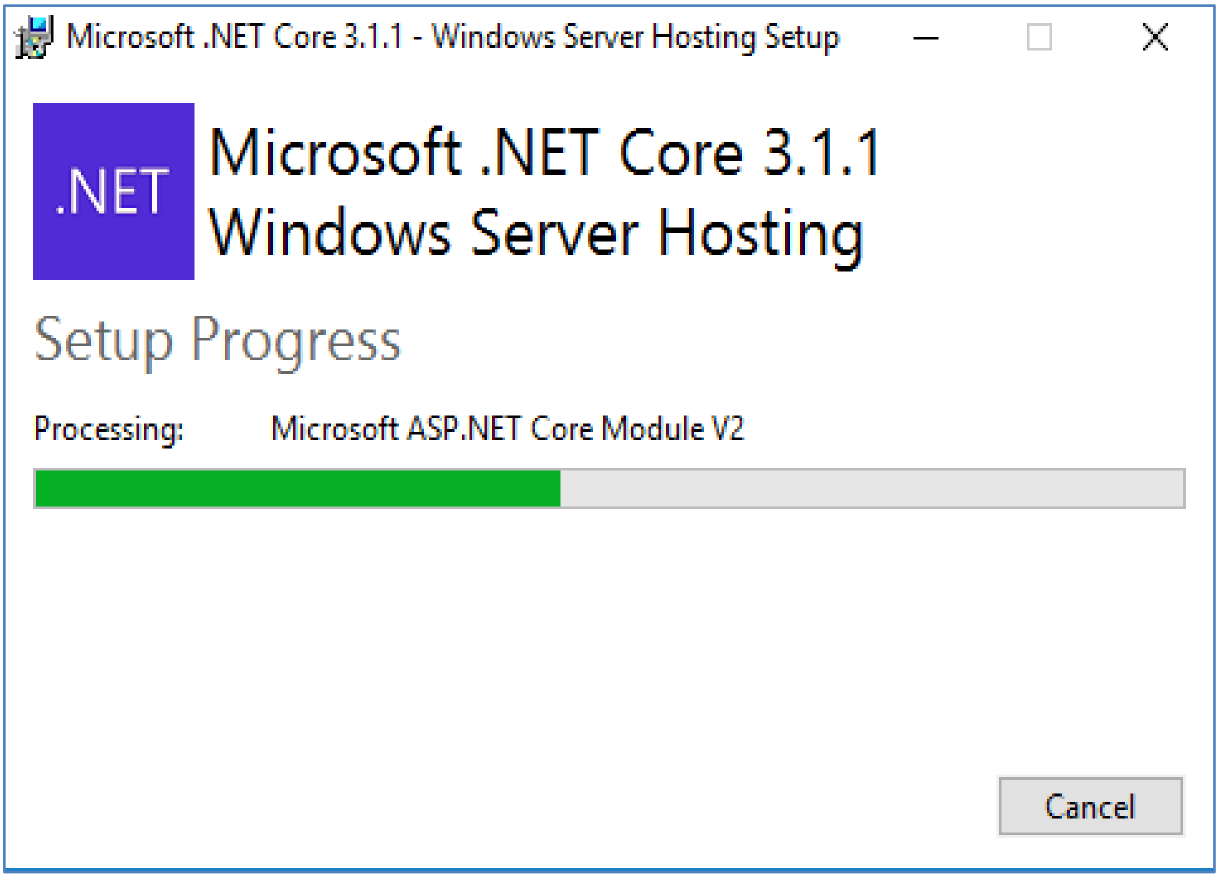
Welcome to the Microsoft .NET Core 3.1.1 - Windows Server Hosting Setup.

Please restart IIS after the installation completes. You can find additional information here.

Microsoft .NET Core 3.1.1 - Windows Server Hosting license terms and privacy statement.

☑ I agree to the license terms and conditions

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



Microsoft .NET Core 3.1.1 - Windows Server Hosting Setup

Microsoft .NET Core 3.1.1
Windows Server Hosting

Setup Progress

Processing: Microsoft ASP.NET Core Module V2

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

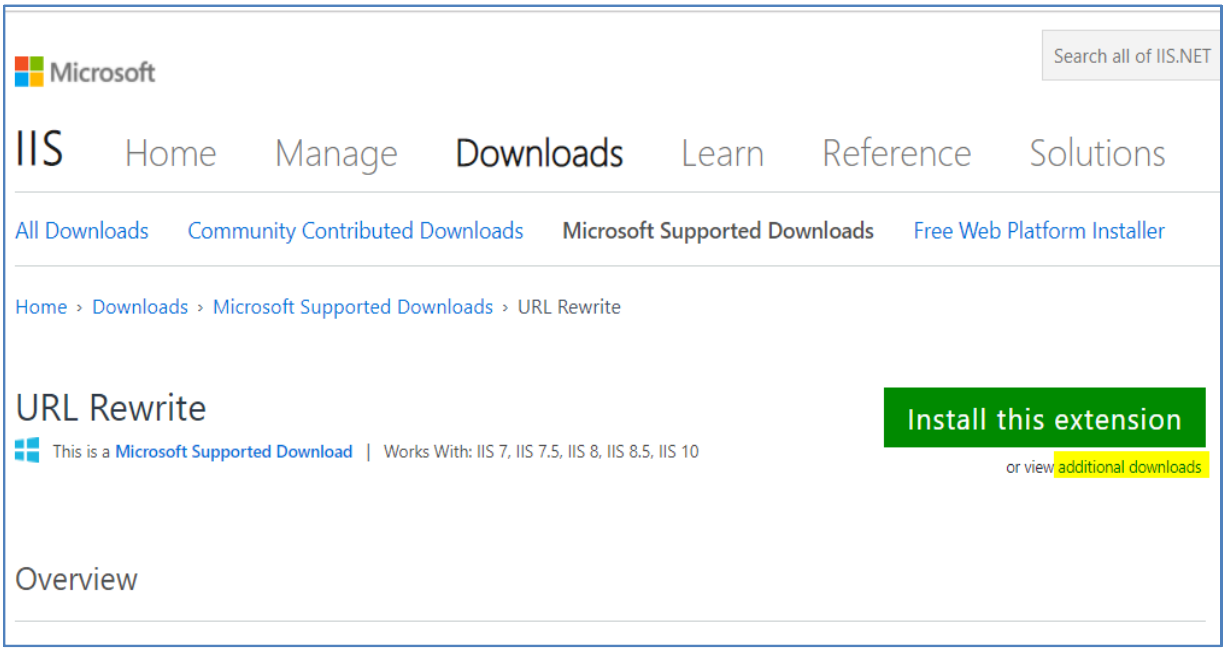
At this point, system is required to **restart** to apply these changes effectively.

2.5 Microsoft IIS URL Rewrite Module 2.1

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

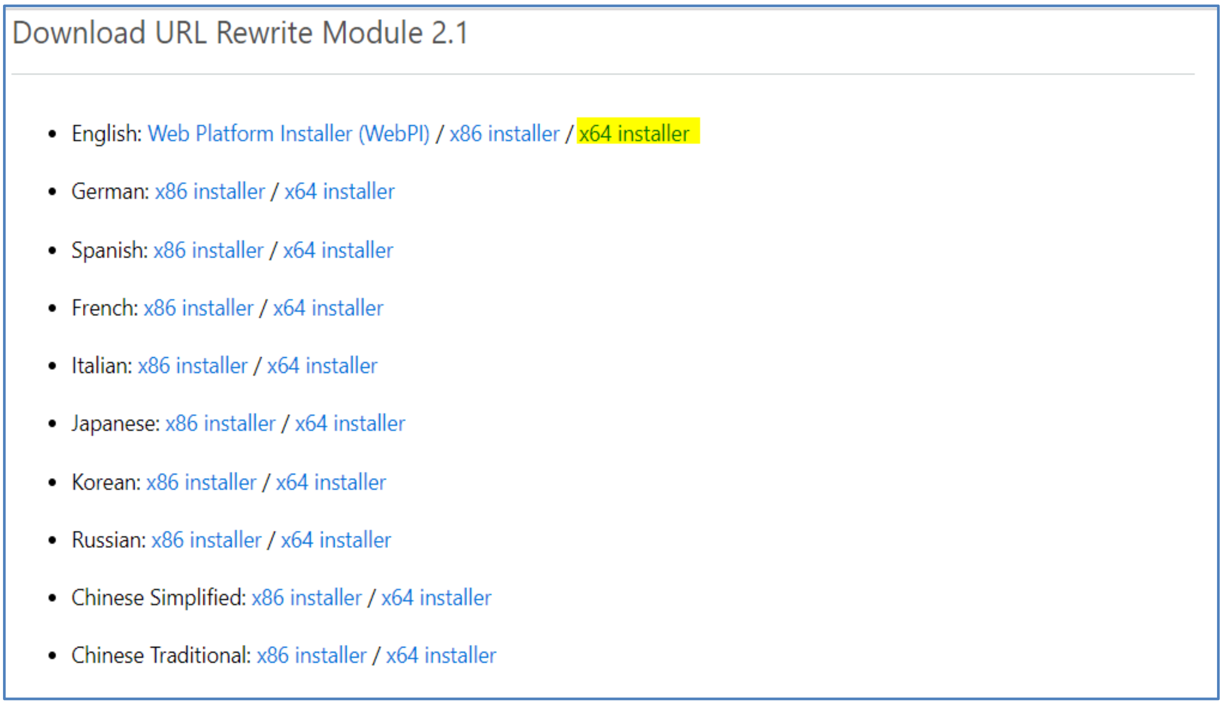
- Microsoft IIS URL Rewrite Module 2.1

Navigating to this URL will present with the following screen:



Microsoft
Search all of IIS.NET
IIS Home Manage Downloads Learn Reference Solutions
All Downloads Community Contributed Downloads Microsoft Supported Downloads Free Web Platform Installer
Home › Downloads › Microsoft Supported Downloads › URL Rewrite
URL Rewrite
This is a Microsoft Supported Download | Works With: IIS 7, IIS 7.5, IIS 8, IIS 8.5, IIS 10
Install this extension
or view additional downloads
Overview

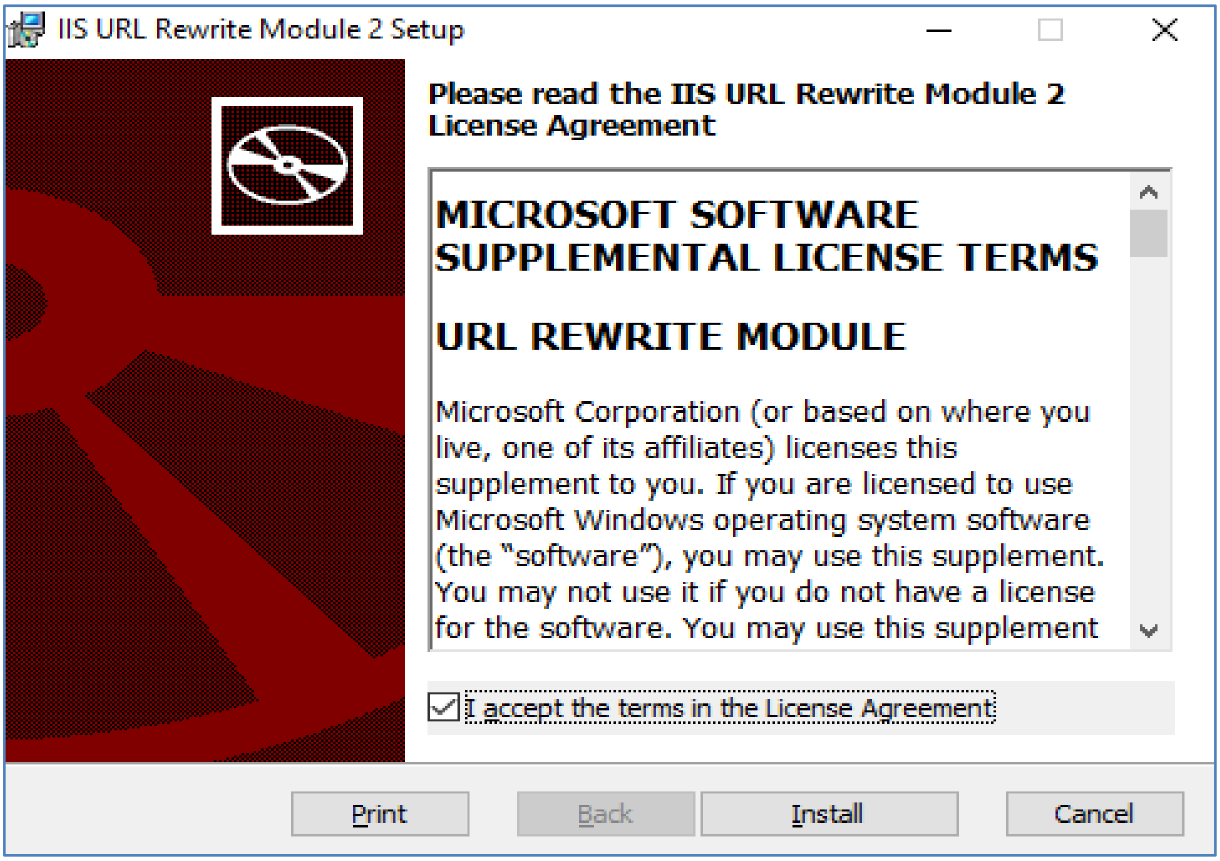
Clicking on the green **Install this extension** will install the extension on the current machine. For offline installers click **Additional Downloads** which will bring you down to the list of the installers



Download URL Rewrite Module 2.1

- English: Web Platform Installer (WebPI) / x86 installer / x64 installer
- German: x86 installer / x64 installer
- Spanish: x86 installer / x64 installer
- French: x86 installer / x64 installer
- Italian: x86 installer / x64 installer
- Japanese: x86 installer / x64 installer
- Korean: x86 installer / x64 installer
- Russian: x86 installer / x64 installer
- Chinese Simplified: x86 installer / x64 installer
- Chinese Traditional: x86 installer / x64 installer

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



Please read the IIS URL Rewrite Module 2 License Agreement

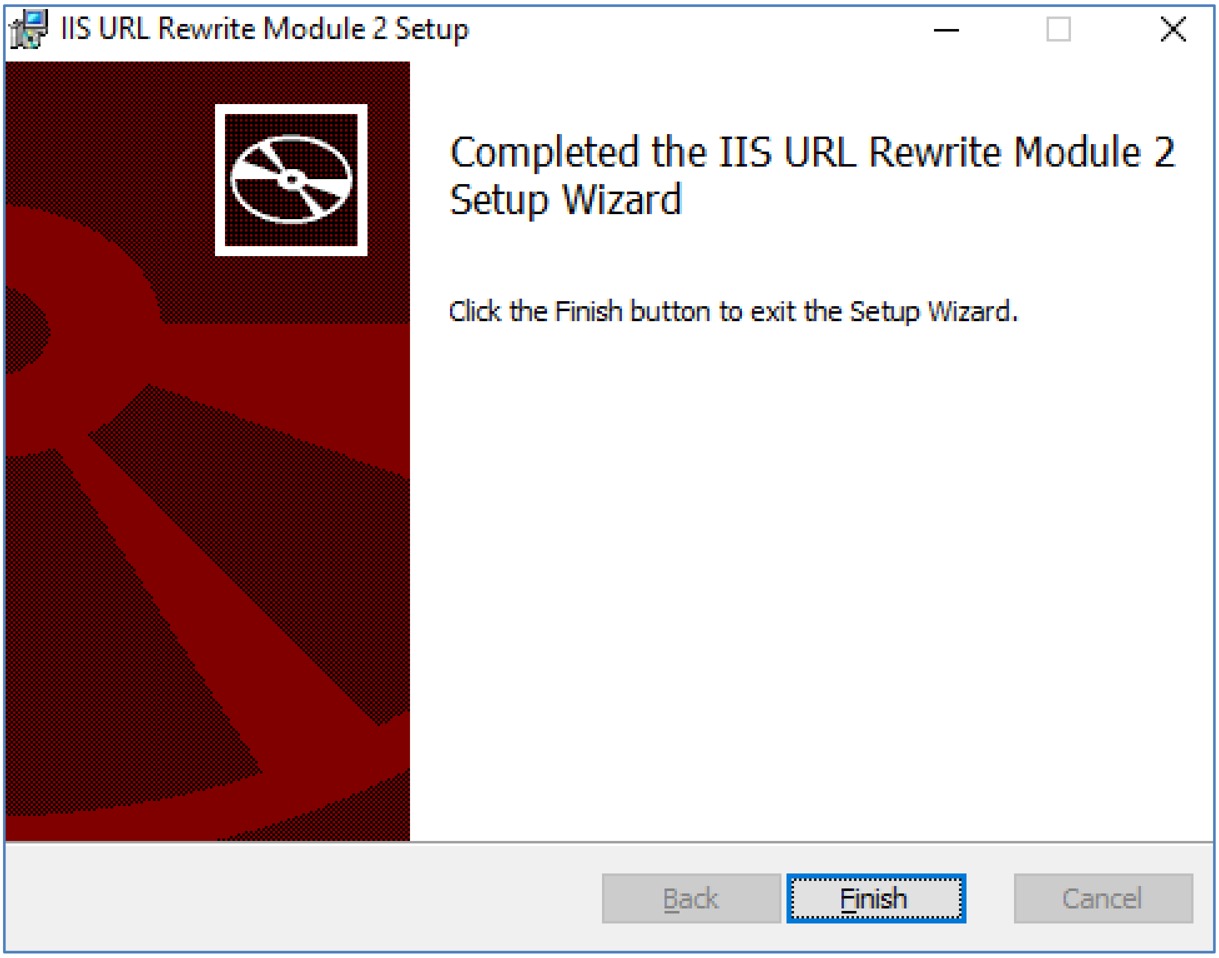
MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

URL REWRITE MODULE

Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows operating system software (the "software"), you may use this supplement. You may not use it if you do not have a license for the software. You may use this supplement

☑ I accept the terms in the License Agreement

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



IIS URL Rewrite Module 2 Setup

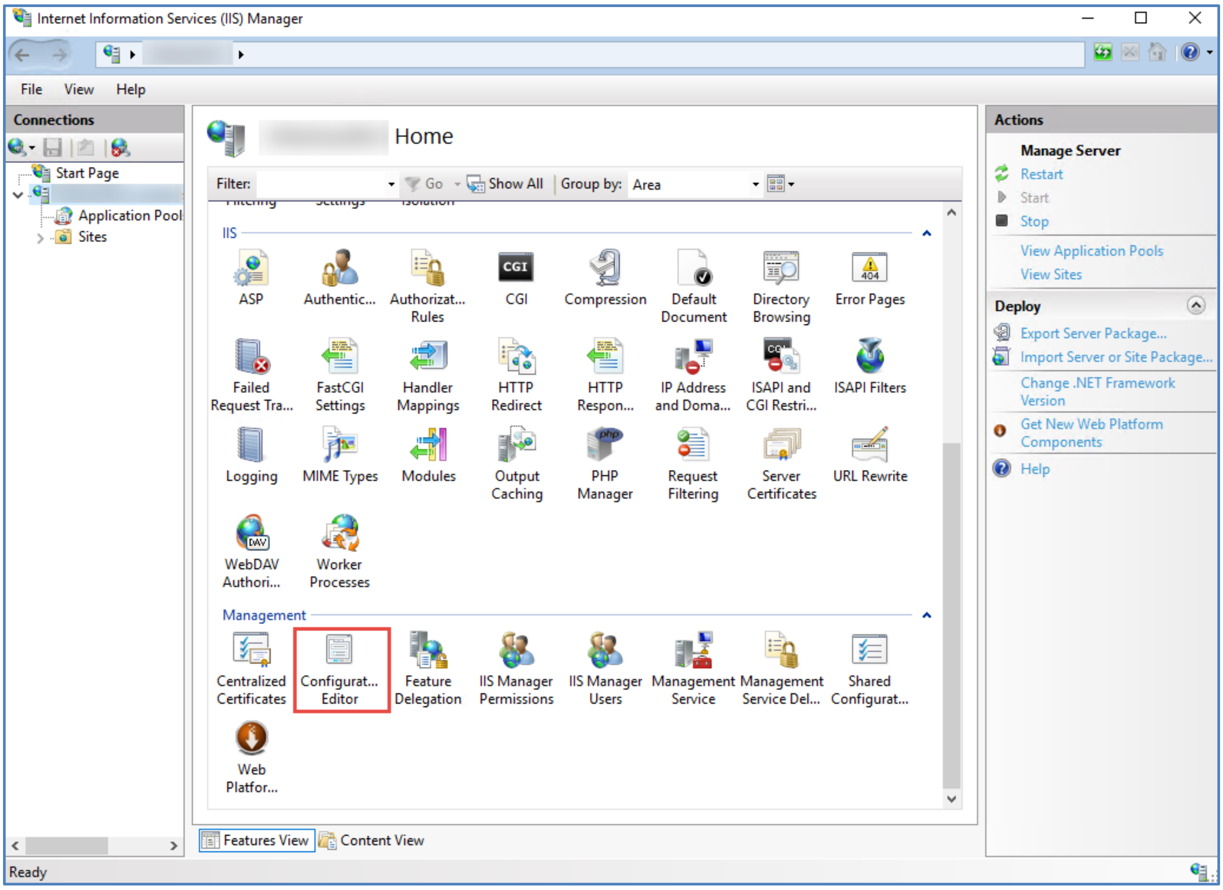
Completed the IIS URL Rewrite Module 2 Setup Wizard

Click the Finish button to exit the Setup Wizard.

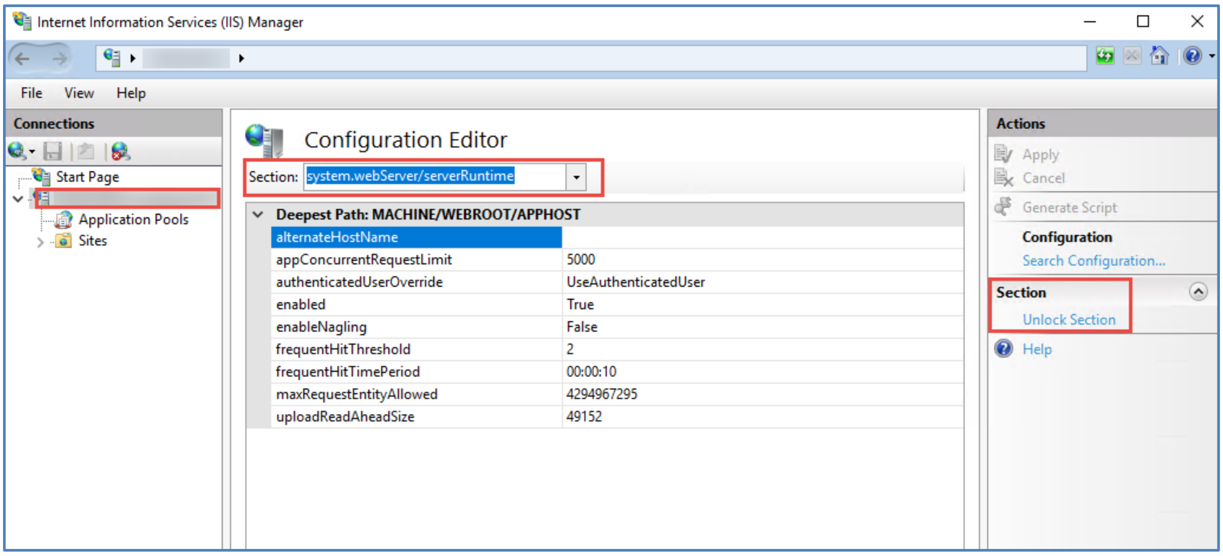
Click **Finish** once the installation is complete

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.



Section: system.webServer/serverRuntime

Deepest Path: MACHINE/WEBROOT/APPHOST

alternateHostName	
appConcurrentRequestLimit	5000
authenticatedUserOverride	UseAuthenticatedUser
enabled	True
enableNagling	False
frequentHitThreshold	2
frequentHitTimePeriod	00:00:10
maxRequestEntityAllowed	4294967295
uploadReadAheadSize	49152

We are done with the installation of prerequisites.

2.7 SMTP Server

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 Web RA
- Email to Address for alerts and warnings sent by Web RA
- Email Subject for alerts and warnings sent by Web RA

If there is no alternative it is possible to still use 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

Both 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

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

- **Web RA Admin**
  Administration application that allows to manage the system wide configurations, service plans, user accounts and access controls etc.
- **Web RA Desktop Web**
  Web RA Web is used to manage certificates for creation, renewal and revocation.
- **Web RA API (Restful Web Services)**
  REST architecture API support that is used to integrate 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.
- **Web RA Device**

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

4 Web RA Installation

4.1 Fresh Installation of Web RA

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

Prerequisites must be installed on the Web RA machine. If these are not installed, 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 Web RA.

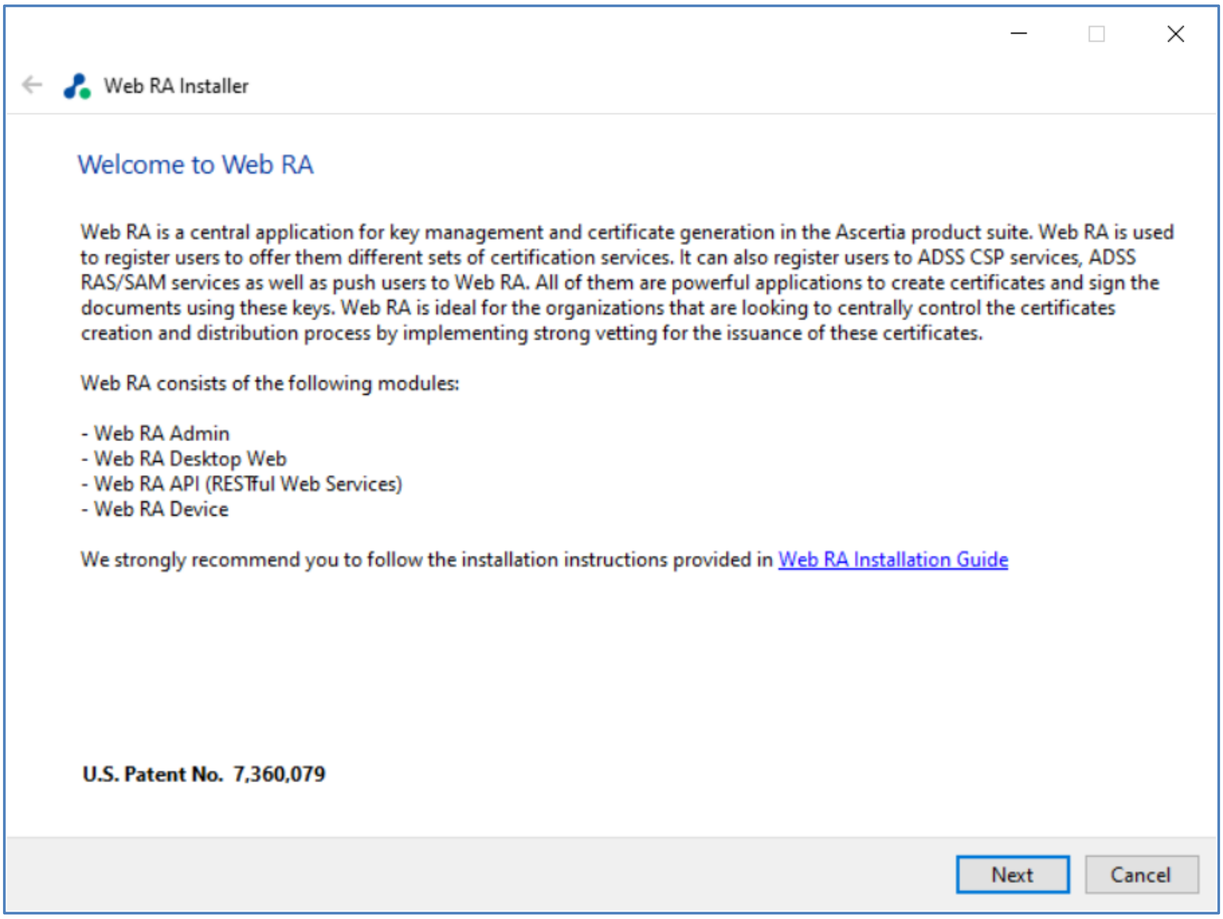
The Web RA package MUST be unzipped on to a disk that has sufficient space – a minimum of **100GB** is recommended. This is because the product is installed and runs from where the installation package is extracted to. Hence please choose a suitable location and naming structure. If you extract the installer on Desktop then 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 Web RA installation. The installer must be run from a user account with the Windows Administrator privileges.

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:



Welcome to Web RA

Web RA is a central application for key management and certificate generation in the Ascertia product suite. Web RA is used to register users to offer them different sets of certification services. It can also register users to ADSS CSP services, ADSS RAS/SAM services as well as push users to Web RA. All of them are powerful applications to create certificates and sign the documents using these keys. Web RA is ideal for the organizations that are looking to centrally control the certificates creation and distribution process by implementing strong vetting for the issuance of these certificates.

Web RA consists of the following modules:

- Web RA Admin
- Web RA Desktop Web
- Web RA API (RESTful Web Services)
- Web RA Device

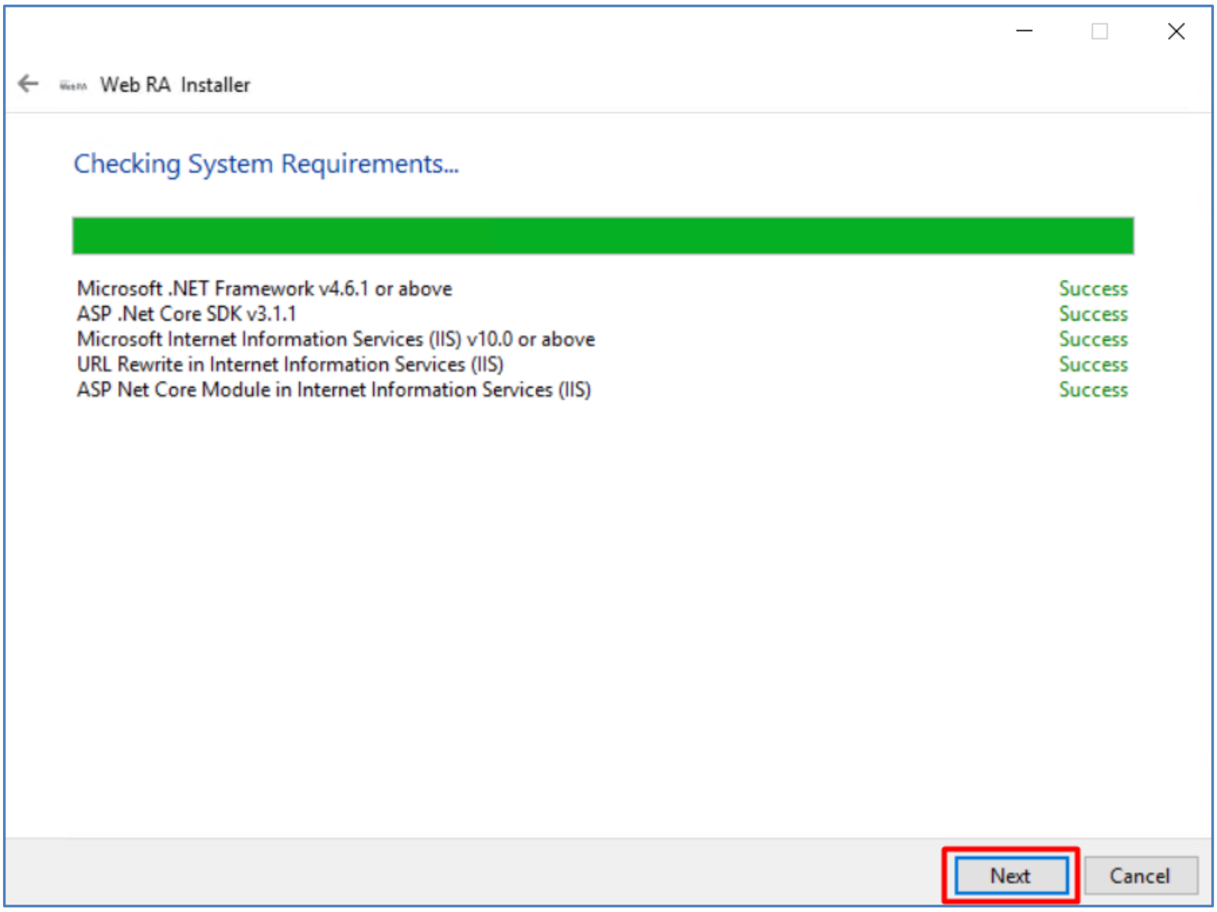
We strongly recommend you to follow the installation instructions provided in Web RA Installation Guide

U.S. Patent No. 7,360,079

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 Web RA system dependencies is not found, or not functioning, then this will be reported on the screen.

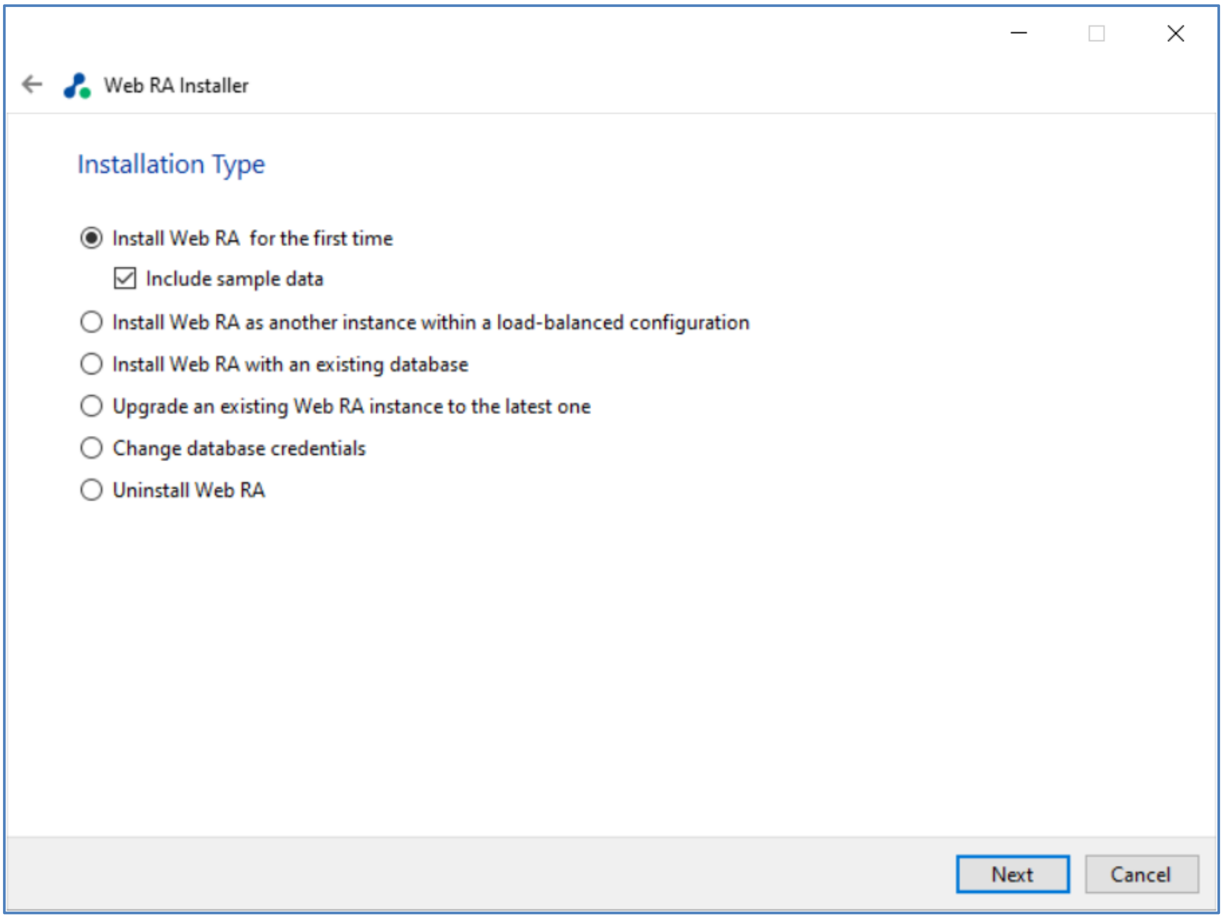
Note you can only proceed with the installation once all issues related to system dependencies are resolved as shown here:



Checking System Requirements...

Microsoft .NET Framework v4.6.1 or above Success
ASP .Net Core SDK v3.1.1 Success
Microsoft Internet Information Services (IIS) v10.0 or above Success
URL Rewrite in Internet Information Services (IIS) Success
ASP Net Core Module in Internet Information Services (IIS) Success

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



Web RA Installer

Installation Type

● Install Web RA for the first time

☑ Include sample data

○ Install Web RA as another instance within a load-balanced configuration

○ Install Web RA with an existing database

○ Upgrade an existing Web RA instance to the latest one

○ Change database credentials

○ Uninstall Web RA

If you are installing 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 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 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 Web RA against an existing 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 Web RA installation. Select the last option **Uninstall Web RA** if you wish to uninstall Web RA from the system.

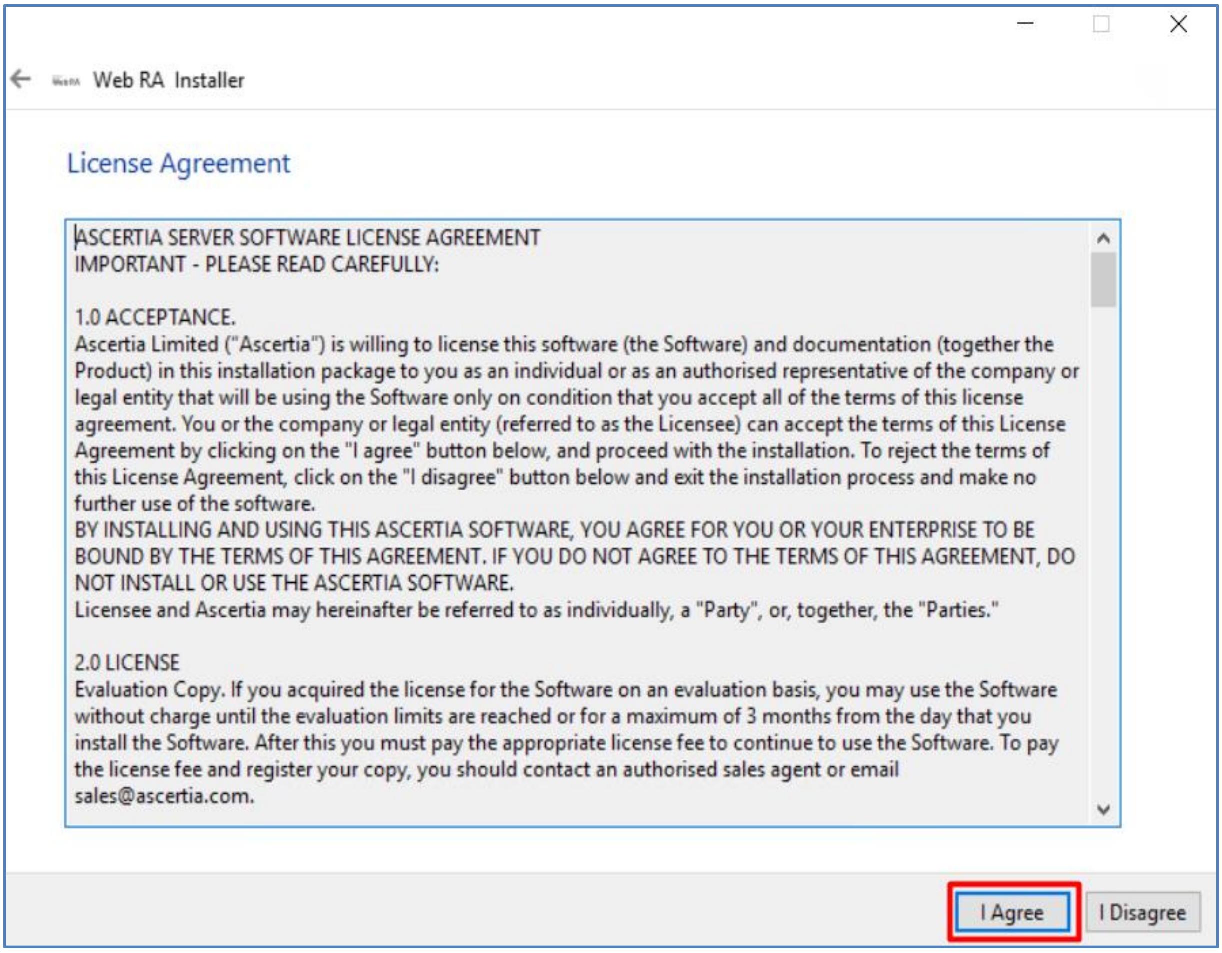
Select the option **Install Web RA for the first time.**

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:



ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:

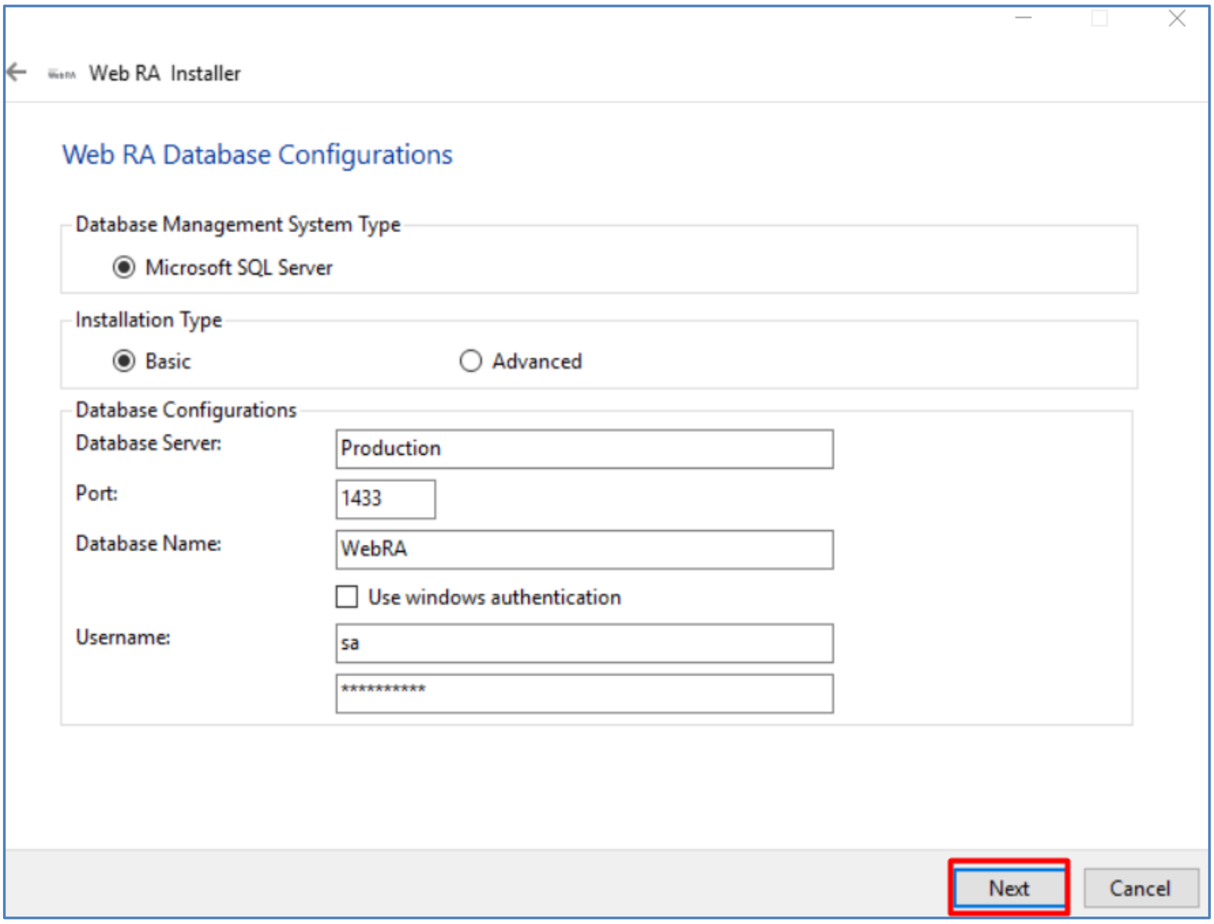
1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition that you accept all of the terms of this license agreement. You or the company or legal entity (referred to as the Licensee) can accept the terms of this License Agreement by clicking on the "I agree" button below, and proceed with the installation. To reject the terms of this License Agreement, click on the "I disagree" button below and exit the installation process and make no further use of the software.
BY INSTALLING AND USING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE ASCERTIA SOFTWARE.
Licensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Parties."

2.0 LICENSE
Evaluation Copy. If you acquired the license for the Software on an evaluation basis, you may use the Software without charge until the evaluation limits are reached or for a maximum of 3 months from the day that you install the Software. After this you must pay the appropriate license fee to continue to use the Software. To pay the license fee and register your copy, you should contact an authorised sales agent or email sales@ascertia.com.

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:



Web RA Installer

Web RA Database Configurations

Database Management System Type

● Microsoft SQL Server

Installation Type

● Basic ○ Advanced

Database Configurations

Database Server: Production

Port: 1433

Database Name: WebRA

□ Use windows authentication

Username: sa

****

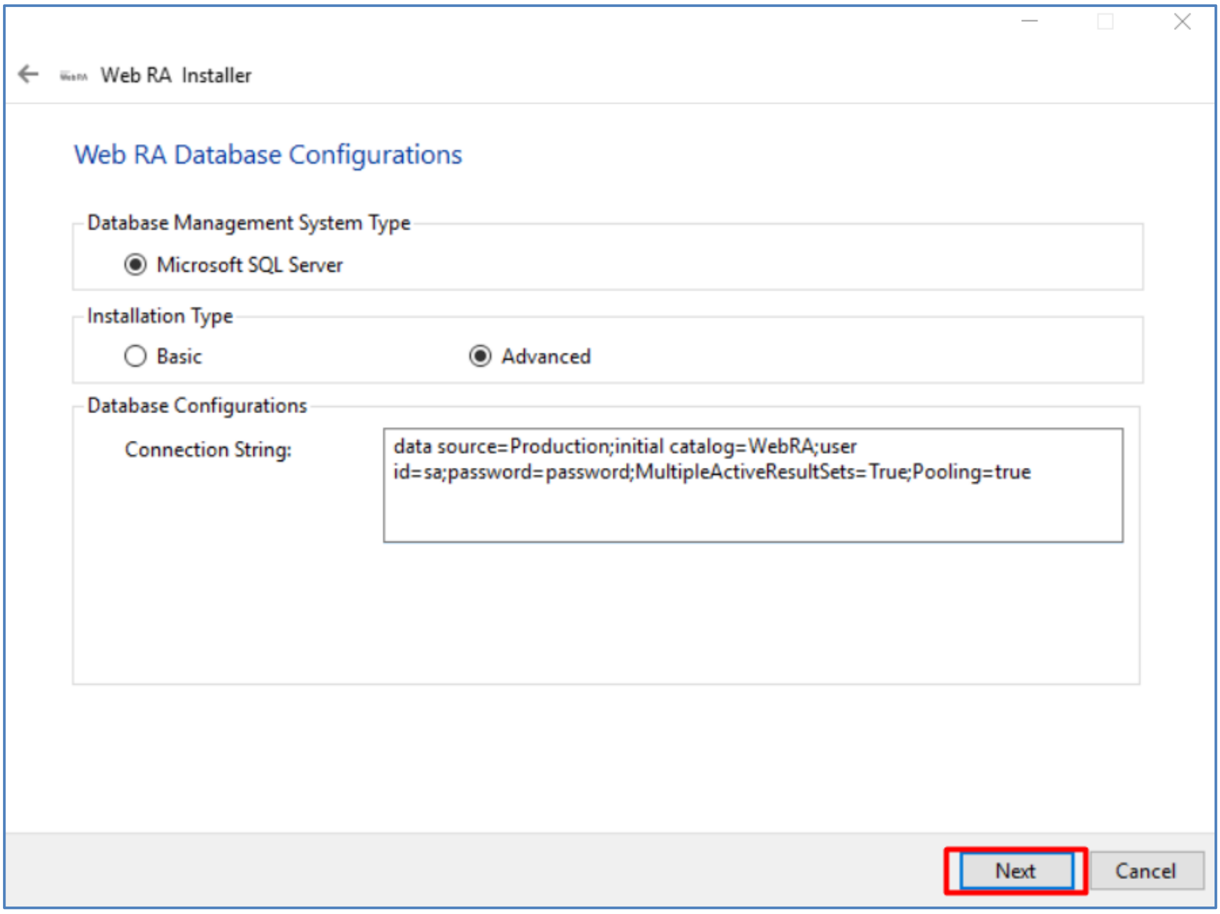
Furthermore, you can either choose to do a basic installation or use an advanced one. If this is a basic installation, then use the first option **Basic** and provide the appropriate Web RA database credentials. The information displayed above is an example and you should configure the relevant settings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



Web RA Database Configurations

Database Management System Type

● Microsoft SQL Server

Installation Type

○ Basic ● Advanced

Database Configurations

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

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.

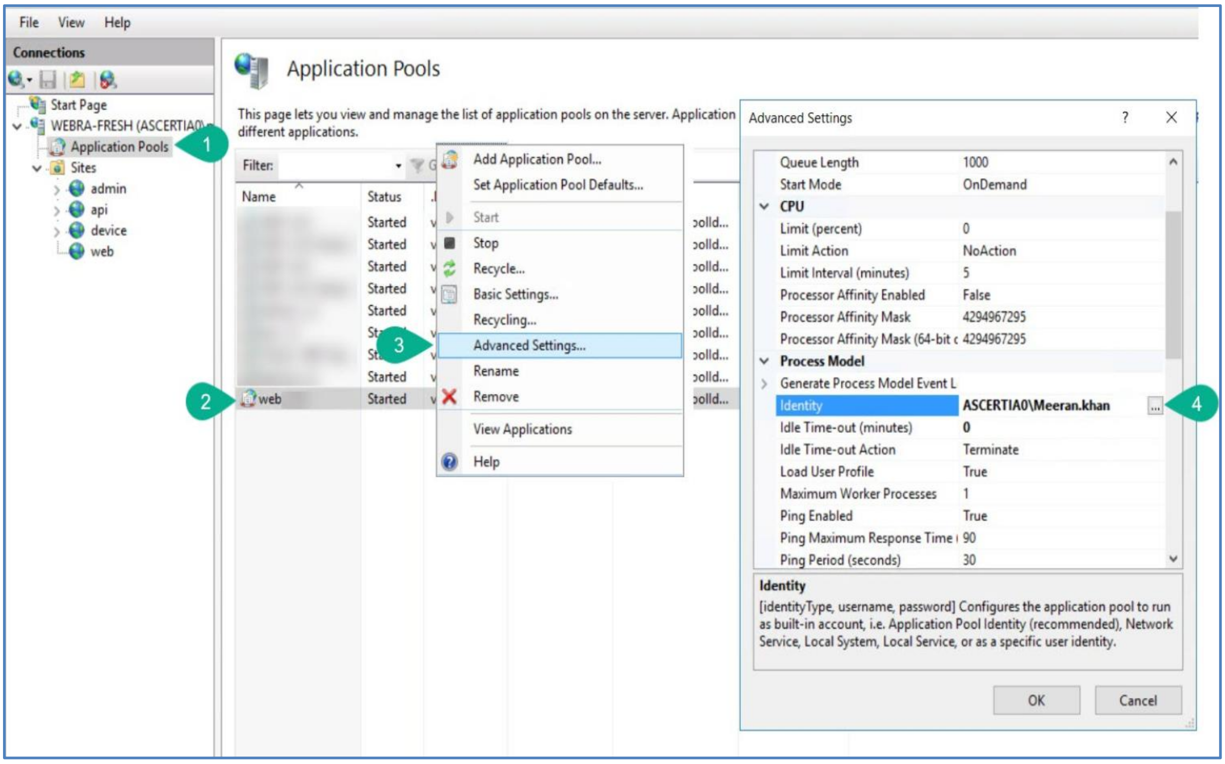
The following table details the configuration options:

Item	**Description**
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 Web RA under a different Windows user, then you need to change it manually. As shown in the following Screen:



Application Pools

This page lets you view and manage the list of application pools on the server. Application ... different applications.

Filter:

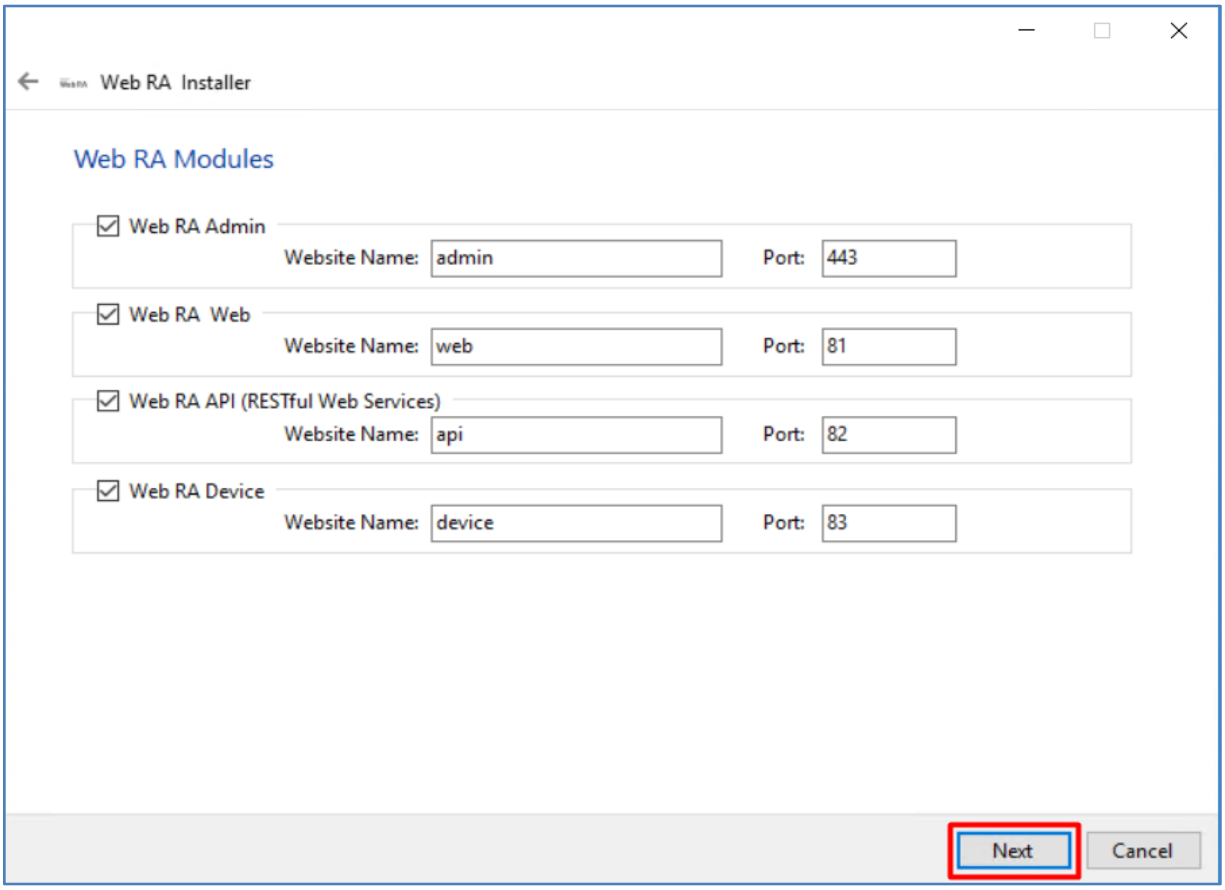
Name	Status
	Started
	Started
	Started
	Started
	Started
	St...
	St...
	Started
web	Started

Advanced Settings

Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	ASCERTIA0\Meeran.khan
Idle Time-out (minutes)	0
Idle Time-out Action	Terminate
Load User Profile	True
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (	90
Ping Period (seconds)	30

Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

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



Web RA Modules

☑ 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

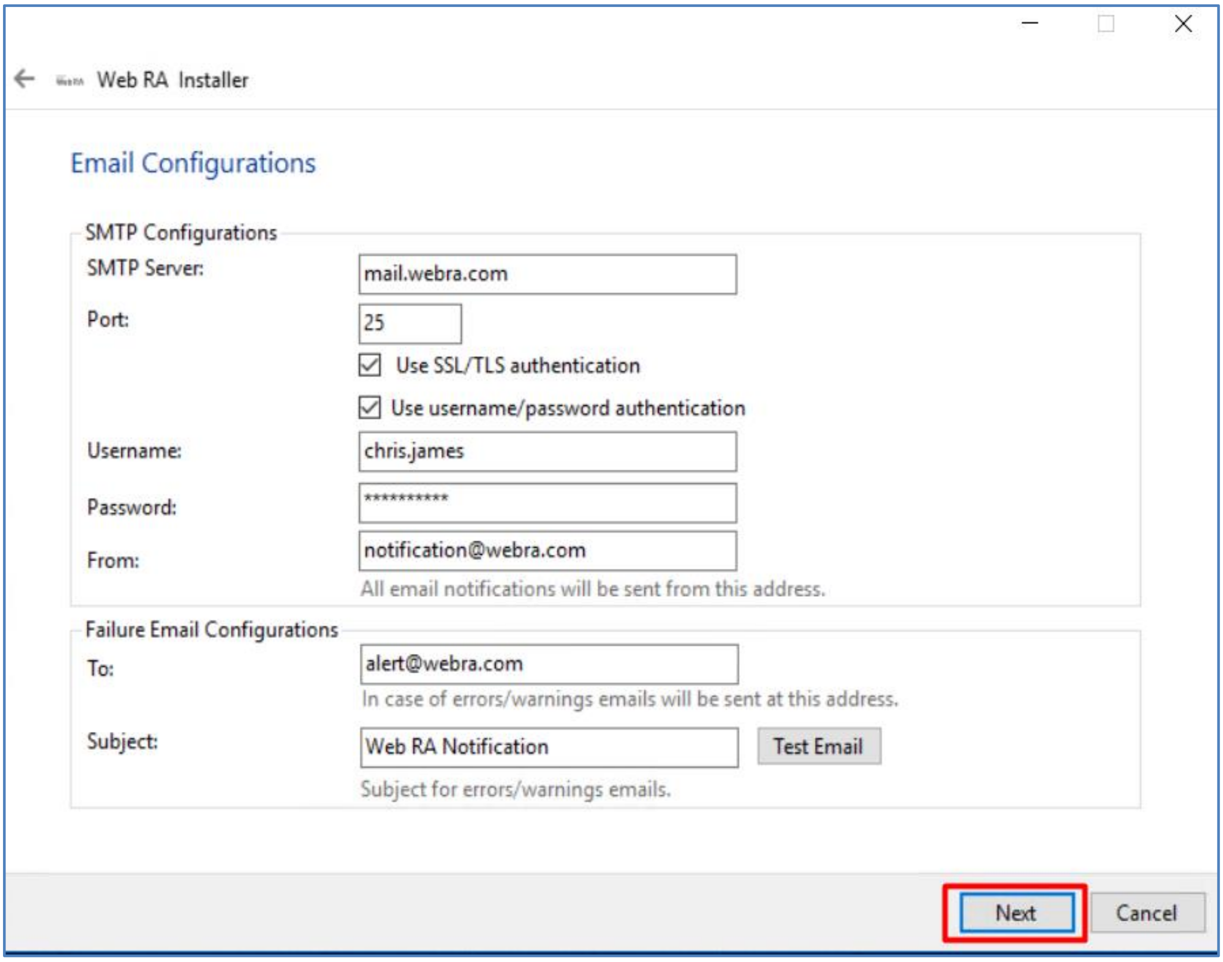
Select the appropriate modules to install the required features. For each selected application, provide the web application name and port. A typical in-house installation of Web RA should only include Admin, Desktop Web, and the API and lastly, the device will be added.

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
Web RA Admin	Web RA Admin is used by the administrators to manage the system wide configurations, service plans, user accounts and access control etc.
Web RA Web	Web RA Web is used to manage certificates for creation, renewal and revocation.
Web RA API	**REST API** is used to integrate Web RA functionality within your own portal.
Web RA Device	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:



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

Subject for errors/warnings emails.

Configure the SMTP Server and email settings for your environment. 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.

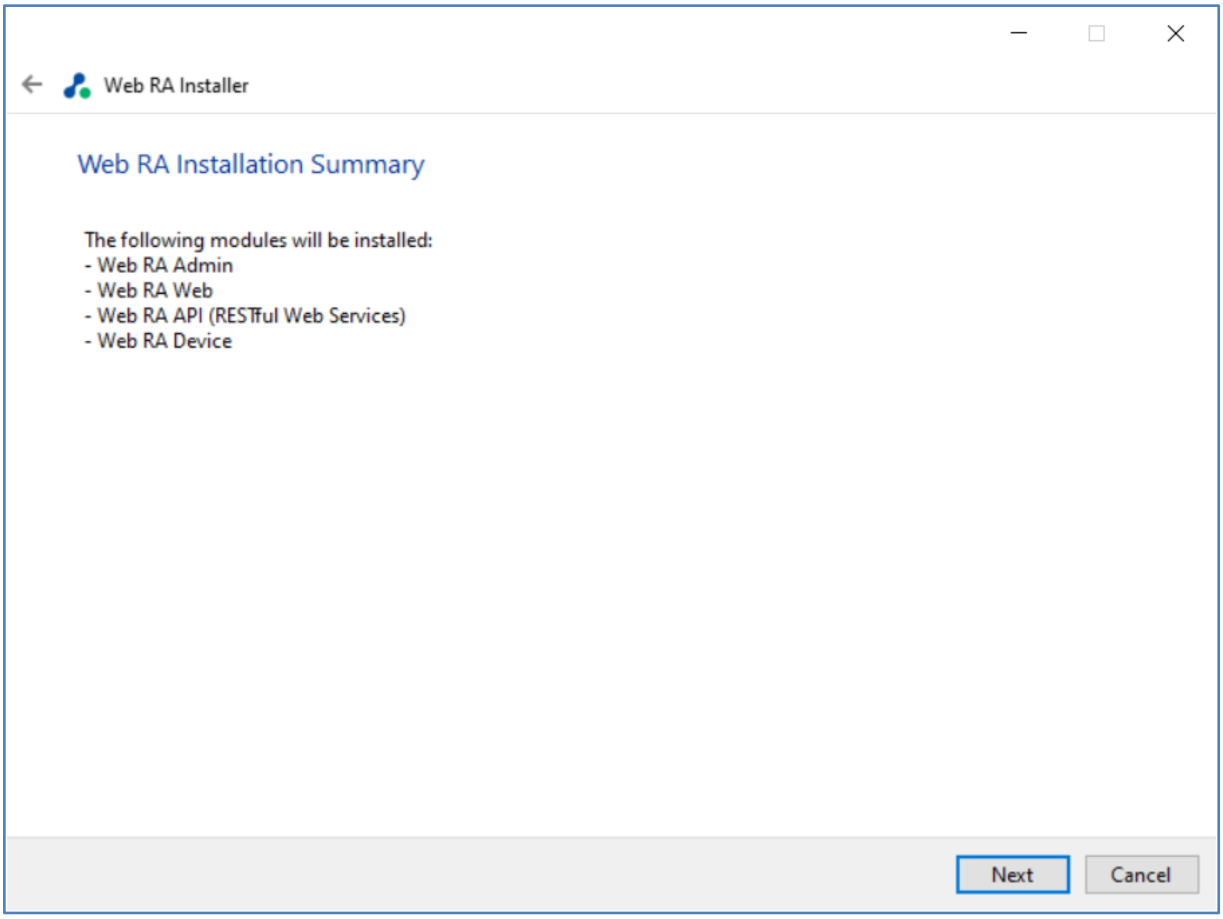
The configuration items are explained in the following table:

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 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 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. 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:



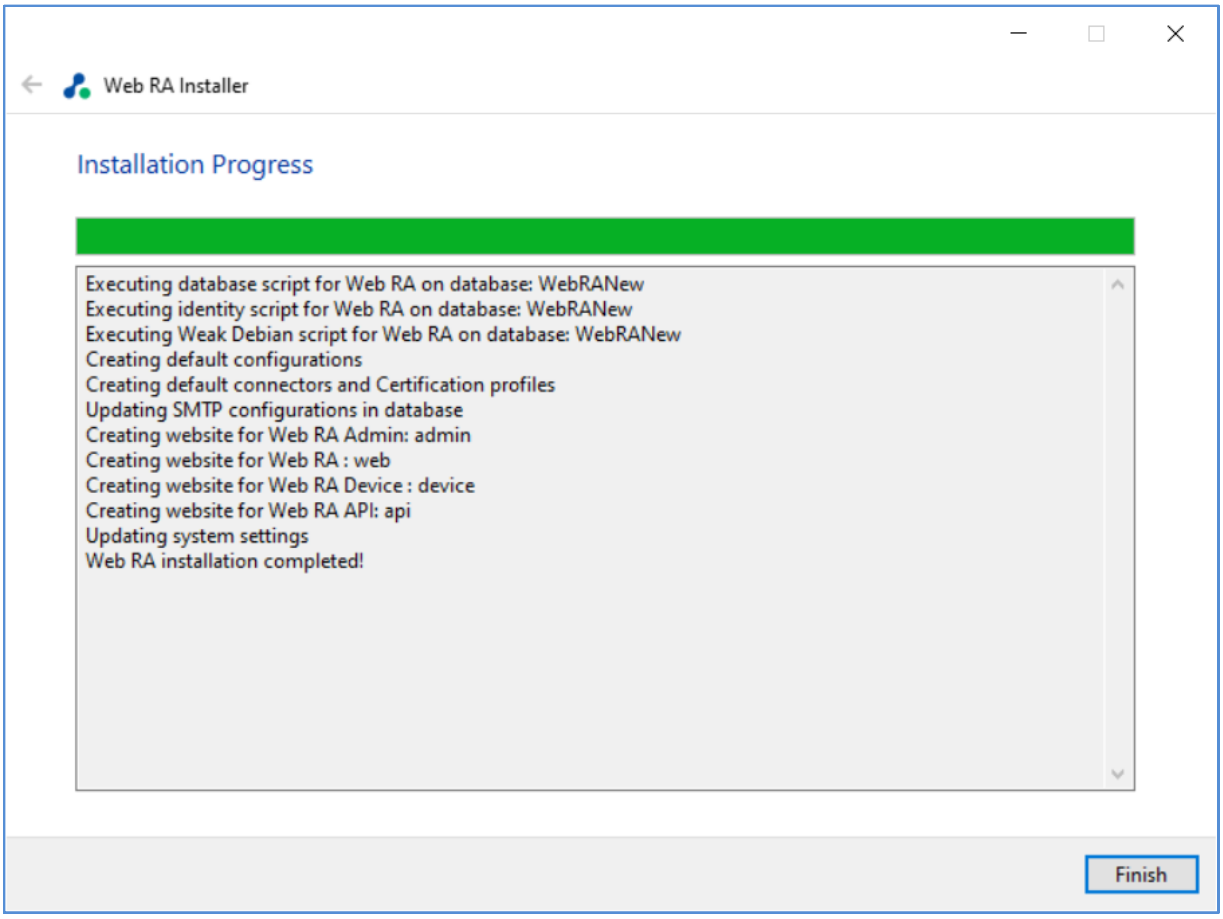
Web RA Installation Summary

The following modules will be installed:
- Web RA Admin
- Web RA Web
- Web RA API (RESTful Web Services)
- Web RA Device

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.



Executing database script for Web RA on database: WebRANew
Executing identity script for Web RA on database: WebRANew
Executing Weak Debian script for Web RA on database: WebRANew
Creating default configurations
Creating default connectors and Certification profiles
Updating SMTP configurations in database
Creating website for Web RA Admin: admin
Creating website for Web RA : web
Creating website for Web RA Device : device
Creating website for Web RA API: api
Updating system settings
Web RA installation completed!

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

4.1.1 Web RA URLs

See these URLs to access the Web RA web sites:

Service	URL Format	Example
Web RA Admin	https://<machine-name>:PORT	https://localhost:443
Web RA Desktop Web	https://<machine-name>:PORT	https://localhost:81
Web RA API	https://<machine-name>:PORT	https://localhost:82
Web RA Device	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 Web RA site:

1. Using standard IIS web server HTTP redirects. This means the basic installation is done with various 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 Web RA site can then be configured to permanently redirect to the secure version.
2. Once the deployment of 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 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.

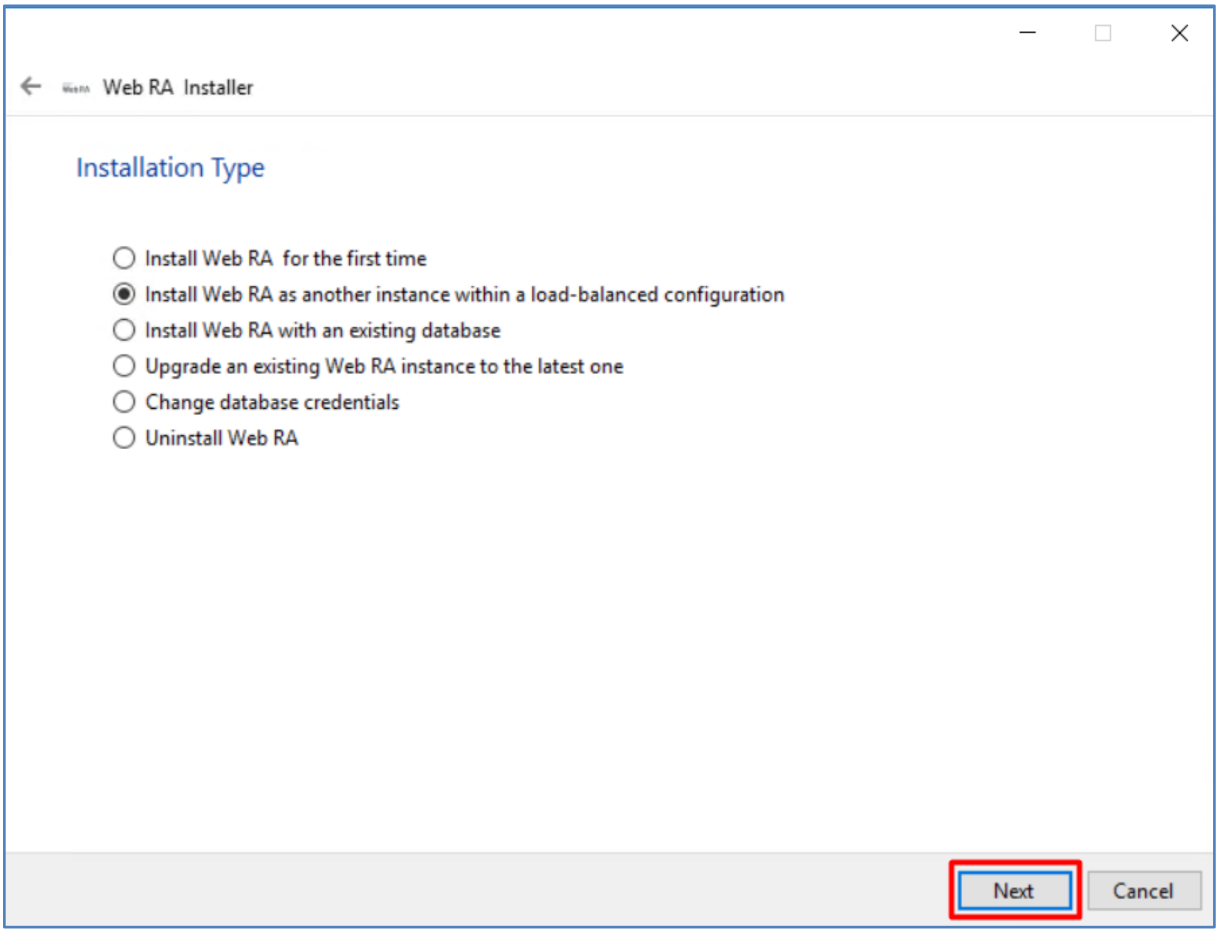
4.2 Installing Web RA with A Load-Balanced Configuration

Follow these instructions to install 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 Web RA as another instance within a load-balanced configuration**

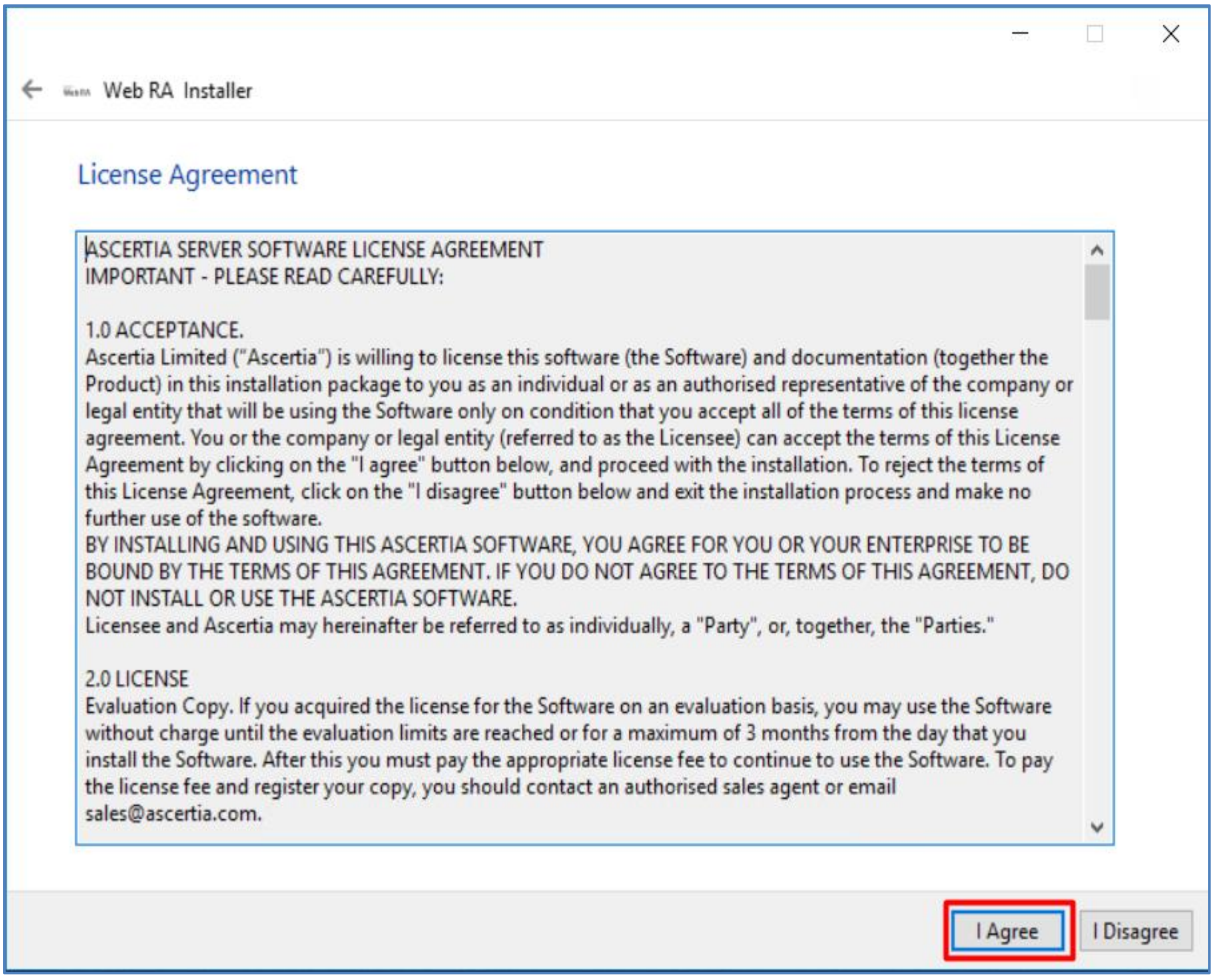


Web RA Installer

Installation Type

○ Install Web RA for the first time
● Install Web RA as another instance within a load-balanced configuration
○ Install Web RA with an existing database
○ Upgrade an existing Web RA instance to the latest one
○ Change database credentials
○ Uninstall Web RA

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



License Agreement

ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:

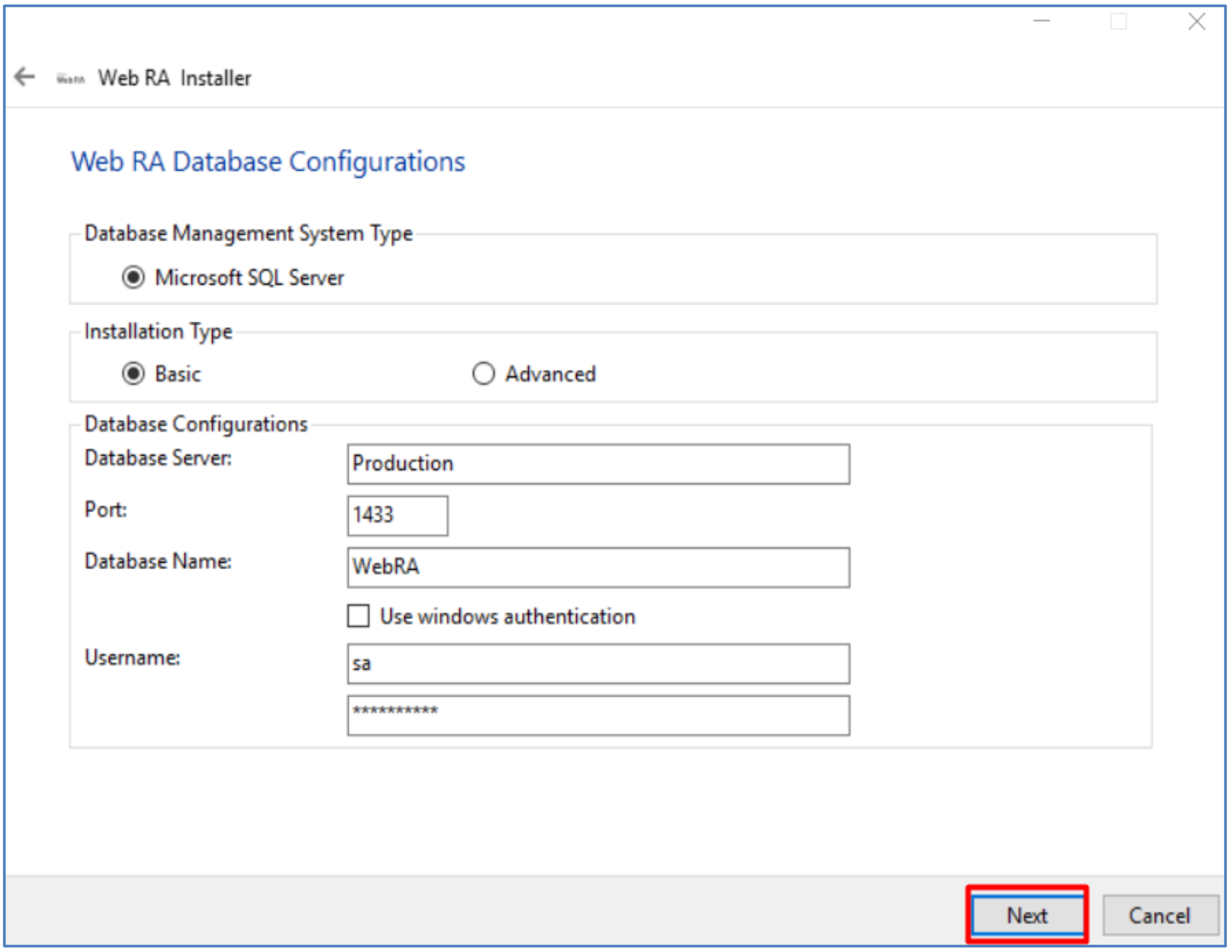
1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition that you accept all of the terms of this license agreement. You or the company or legal entity (referred to as the Licensee) can accept the terms of this License Agreement by clicking on the "I agree" button below, and proceed with the installation. To reject the terms of this License Agreement, click on the "I disagree" button below and exit the installation process and make no further use of the software.
BY INSTALLING AND USING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE ASCERTIA SOFTWARE.
Licensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Parties."

2.0 LICENSE
Evaluation Copy. If you acquired the license for the Software on an evaluation basis, you may use the Software without charge until the evaluation limits are reached or for a maximum of 3 months from the day that you install the Software. After this you must pay the appropriate license fee to continue to use the Software. To pay the license fee and register your copy, you should contact an authorised sales agent or email sales@ascertia.com.

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:



Web RA Installer

Web RA Database Configurations

Database Management System Type

● Microsoft SQL Server

Installation Type

● Basic ○ Advanced

Database Configurations

Database Server: Production

Port: 1433

Database Name: WebRA

□ Use windows authentication

Username: sa

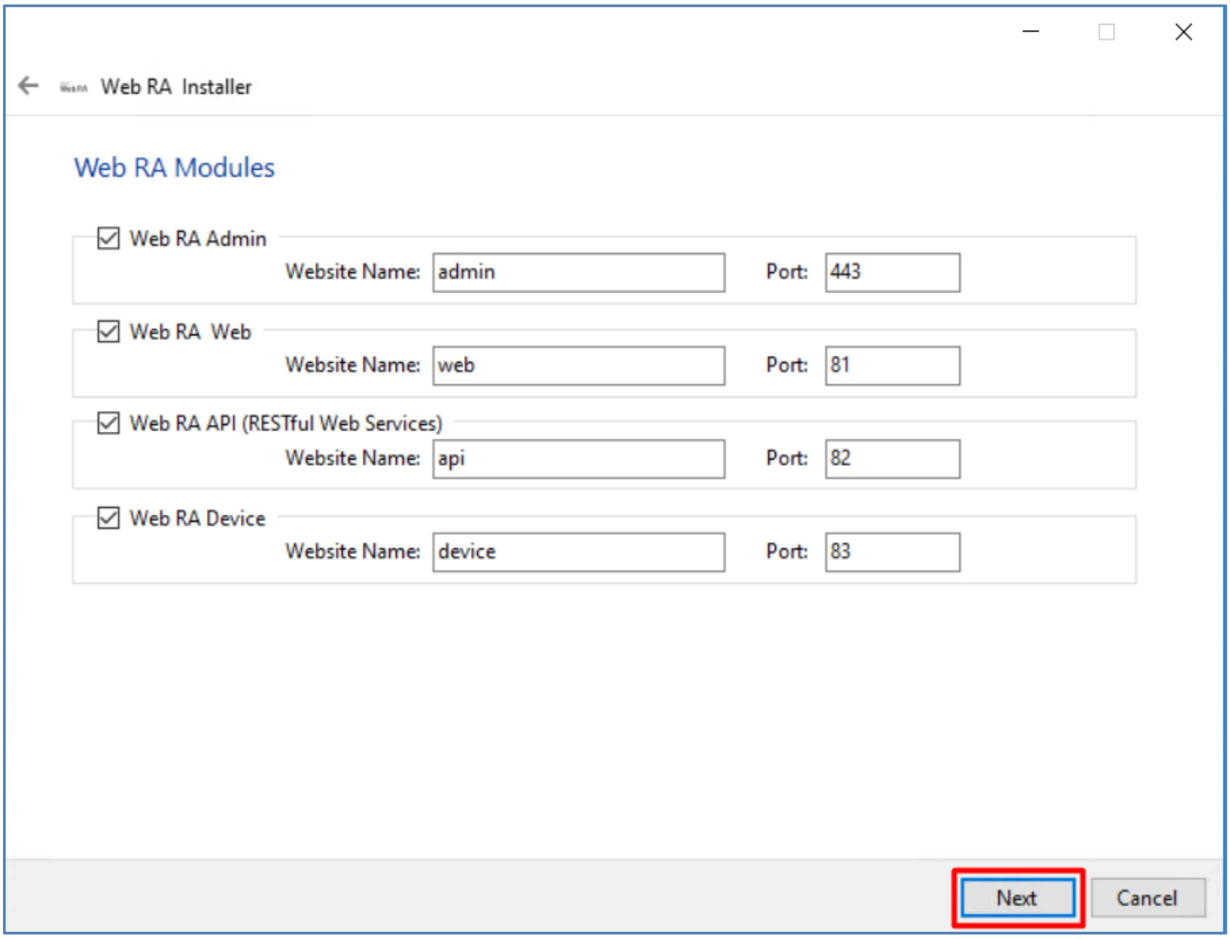
****

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

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

If the current Web RA database schema is older than the version required by the installer, and you click ***Next,*** *the installer will prompt you that 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.



Web RA Modules

☑ Web RA Admin
Website Name: admin
Port: 443

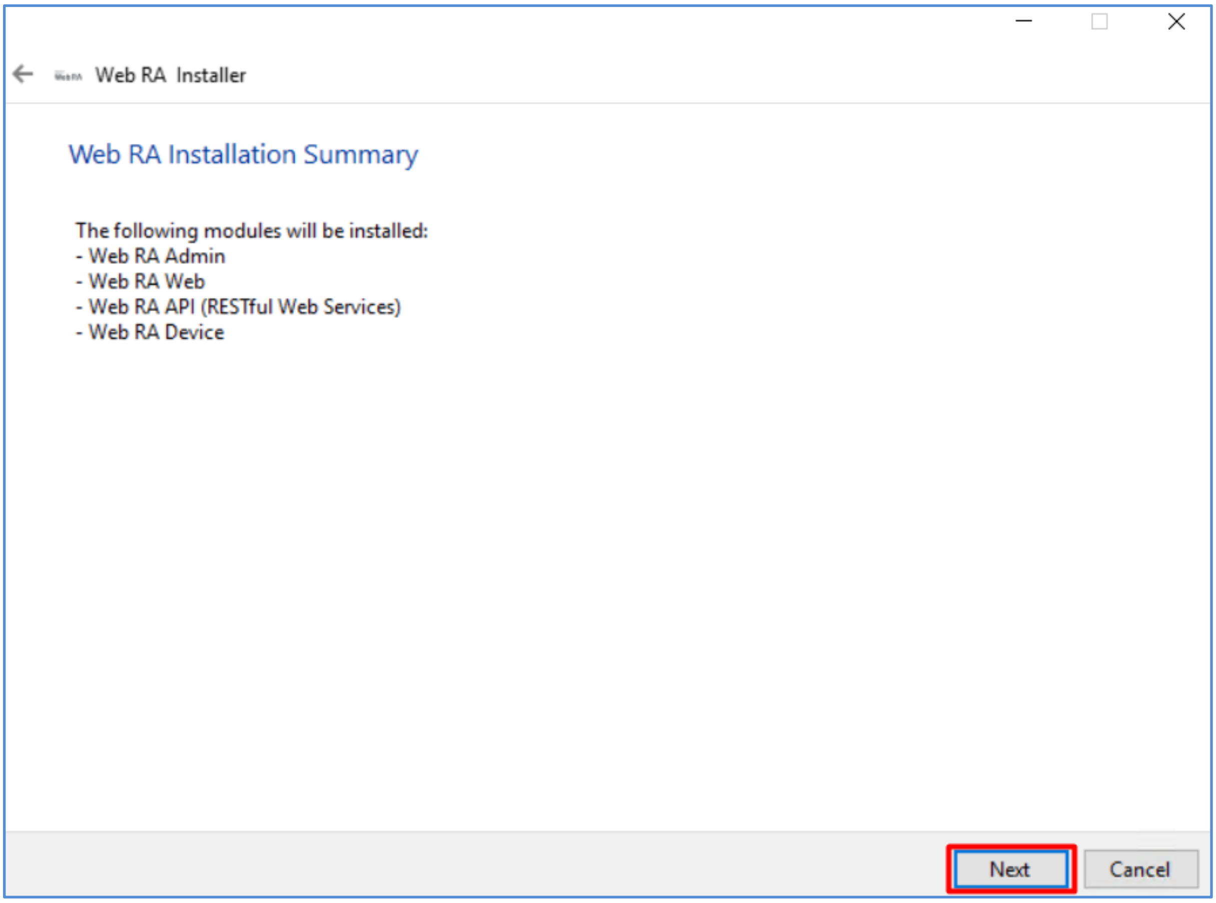
☑ Web RA Web
Website Name: web
Port: 81

☑ Web RA API (RESTful Web Services)
Website Name: api
Port: 82

☑ Web RA Device
Website Name: device
Port: 83

Select the appropriate modules to install the required features.

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

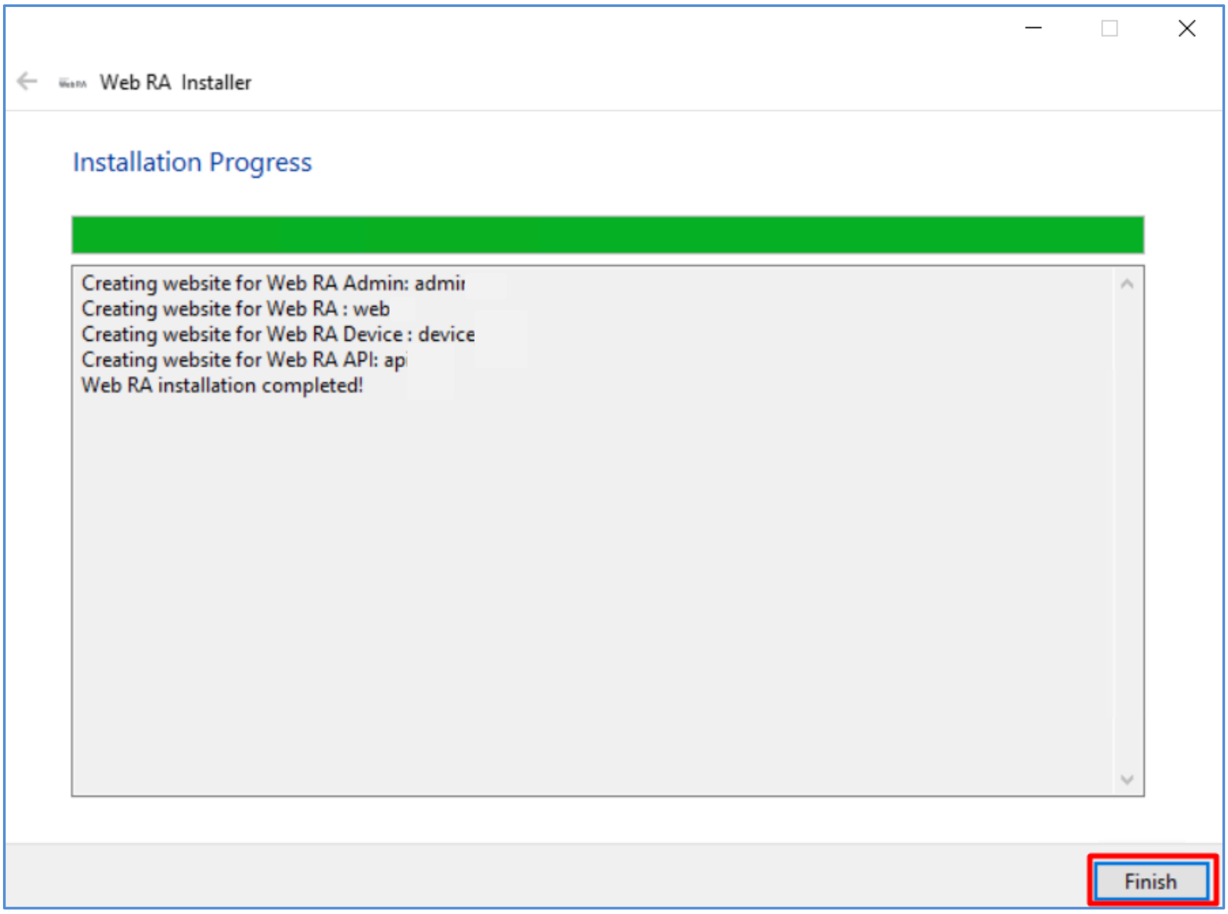


Web RA Installation Summary

The following modules will be installed:
- Web RA Admin
- Web RA Web
- Web RA API (RESTful Web Services)
- Web RA Device

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

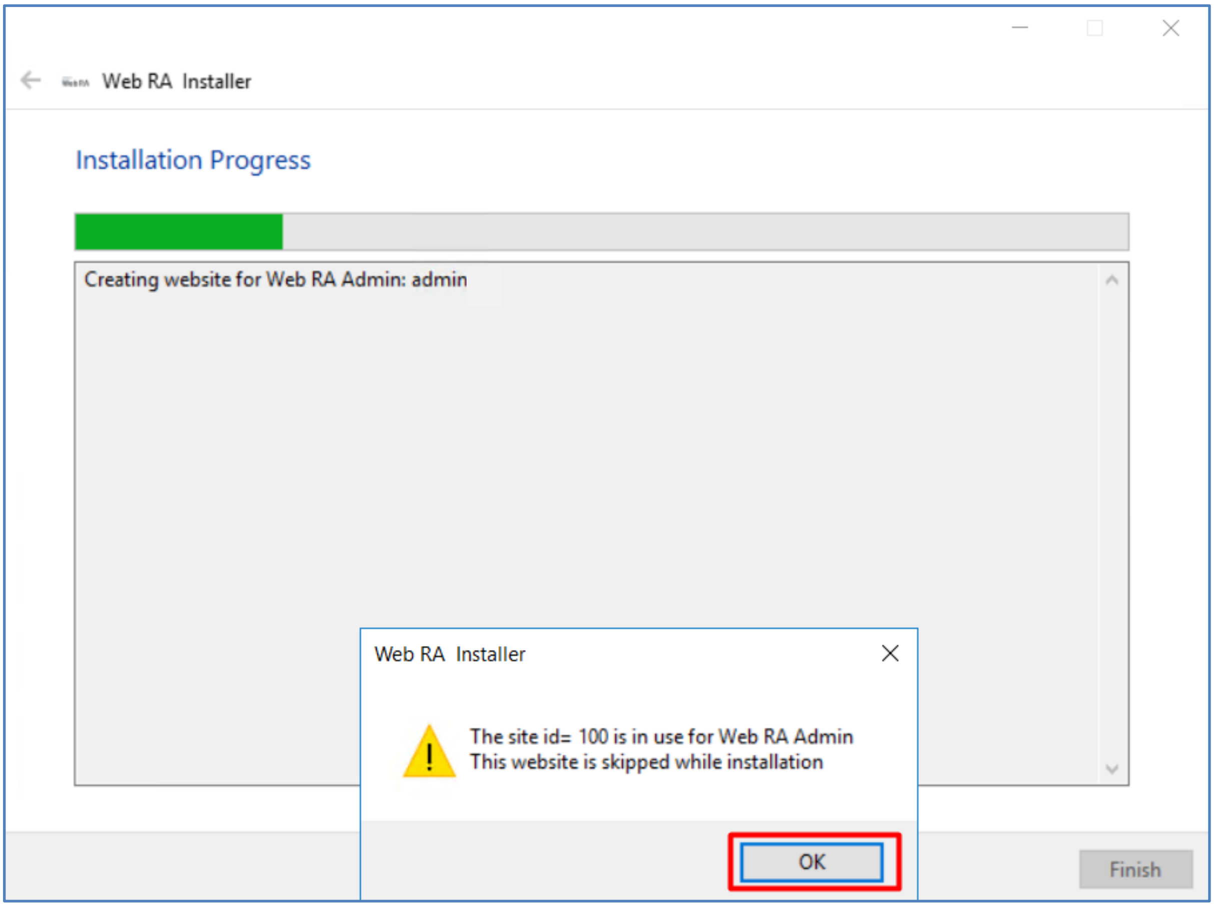
If you think any listed item is incorrect then use the **Back** button (arrow towards the top-left of the dialogue box) to correct your choices before proceeding ahead.



Creating website for Web RA Admin: admi
Creating website for Web RA : web
Creating website for Web RA Device : device
Creating website for Web RA API: ap
Web RA installation completed!

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

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



Web RA Installer

Installation Progress

Creating website for Web RA Admin: admin

Web RA Installer

The site id= 100 is in use for Web RA Admin
This website is skipped while installation

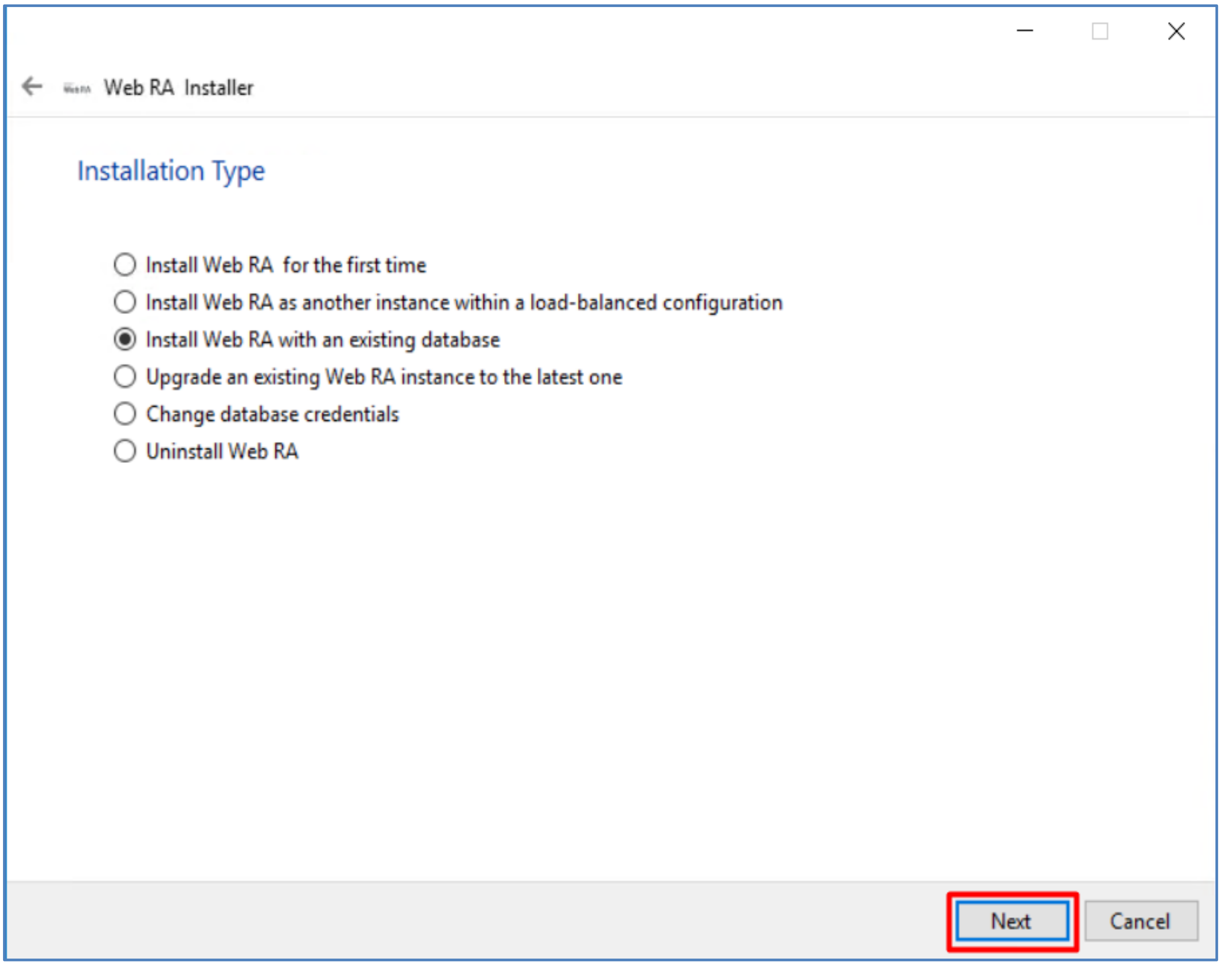
Click the **Finish** button to complete the installation process.

4.3 Installing Web RA with an Existing Database

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

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:

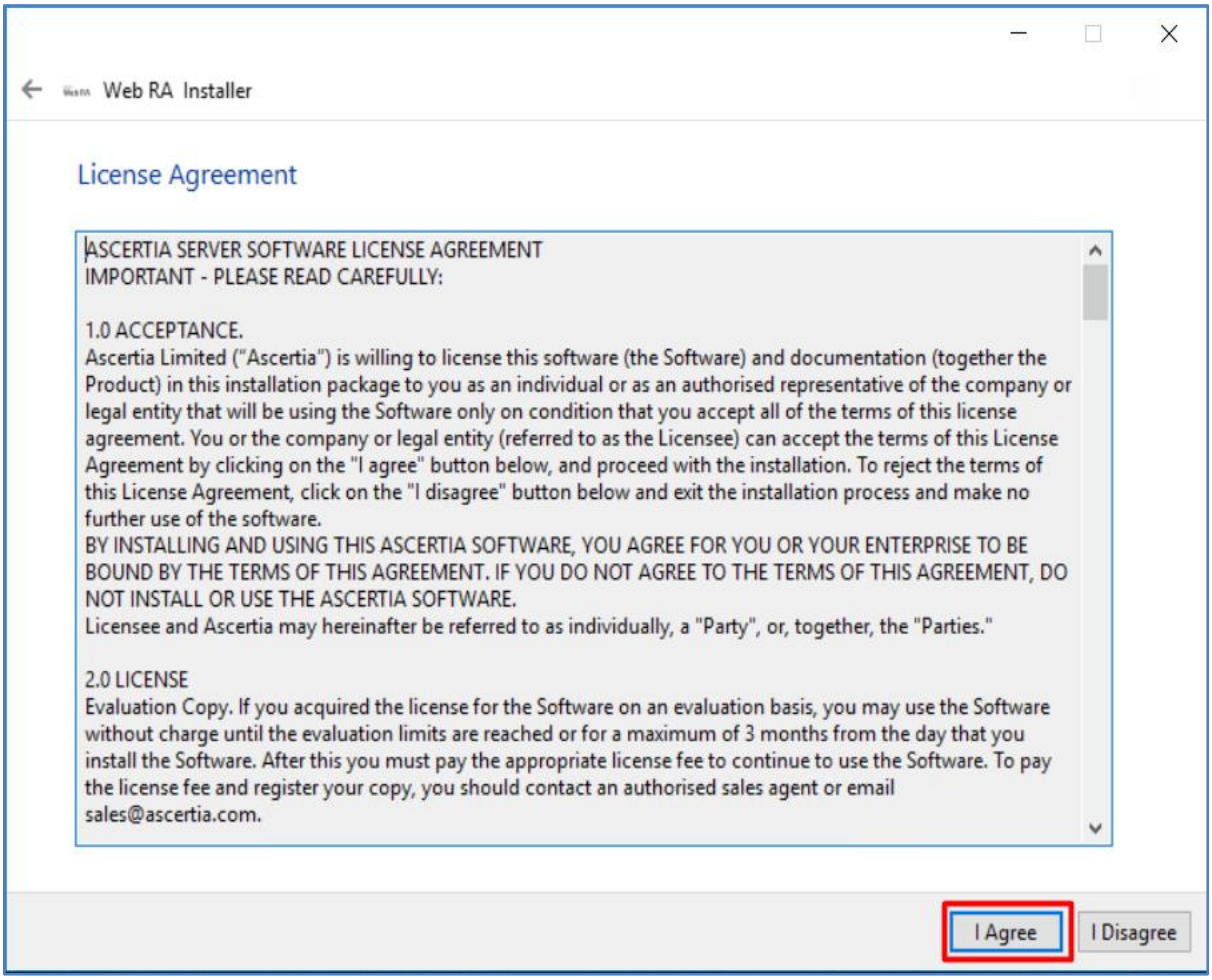
Select the option **Install Web RA within existing database**



Installation Type

○ Install Web RA for the first time
○ Install Web RA as another instance within a load-balanced configuration
● Install Web RA with an existing database
○ Upgrade an existing Web RA instance to the latest one
○ Change database credentials
○ Uninstall Web RA

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



ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:

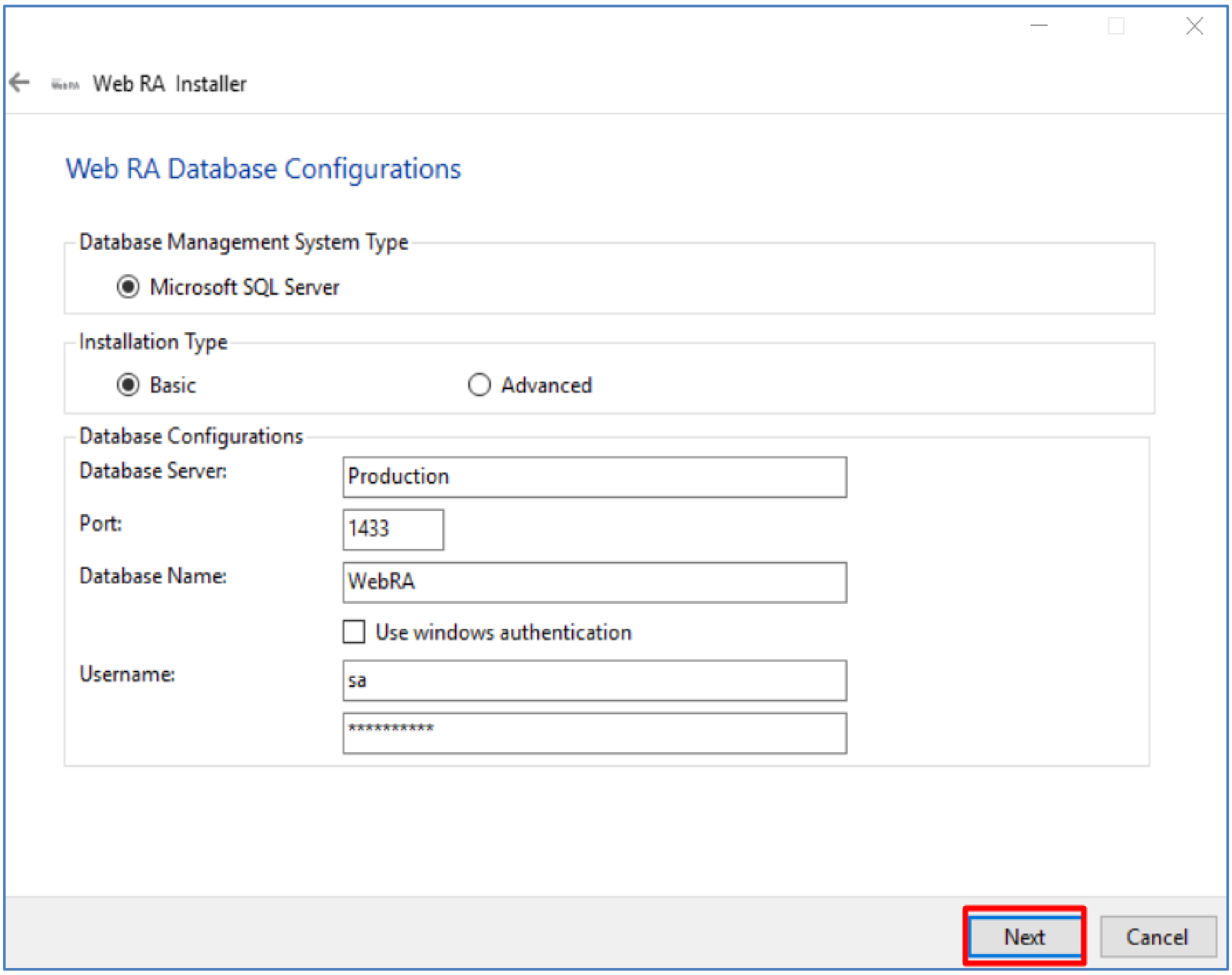
1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition that you accept all of the terms of this license agreement. You or the company or legal entity (referred to as the Licensee) can accept the terms of this License Agreement by clicking on the "I agree" button below, and proceed with the installation. To reject the terms of this License Agreement, click on the "I disagree" button below and exit the installation process and make no further use of the software.
BY INSTALLING AND USING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE ASCERTIA SOFTWARE.
Licensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Parties."

2.0 LICENSE
Evaluation Copy. If you acquired the license for the Software on an evaluation basis, you may use the Software without charge until the evaluation limits are reached or for a maximum of 3 months from the day that you install the Software. After this you must pay the appropriate license fee to continue to use the Software. To pay the license fee and register your copy, you should contact an authorised sales agent or email sales@ascertia.com.

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:



Web RA Database Configurations

Database Management System Type

● Microsoft SQL Server

Installation Type

● Basic ○ Advanced

Database Configurations

Database Server: Production

Port: 1433

Database Name: WebRA

□ Use windows authentication

Username: sa

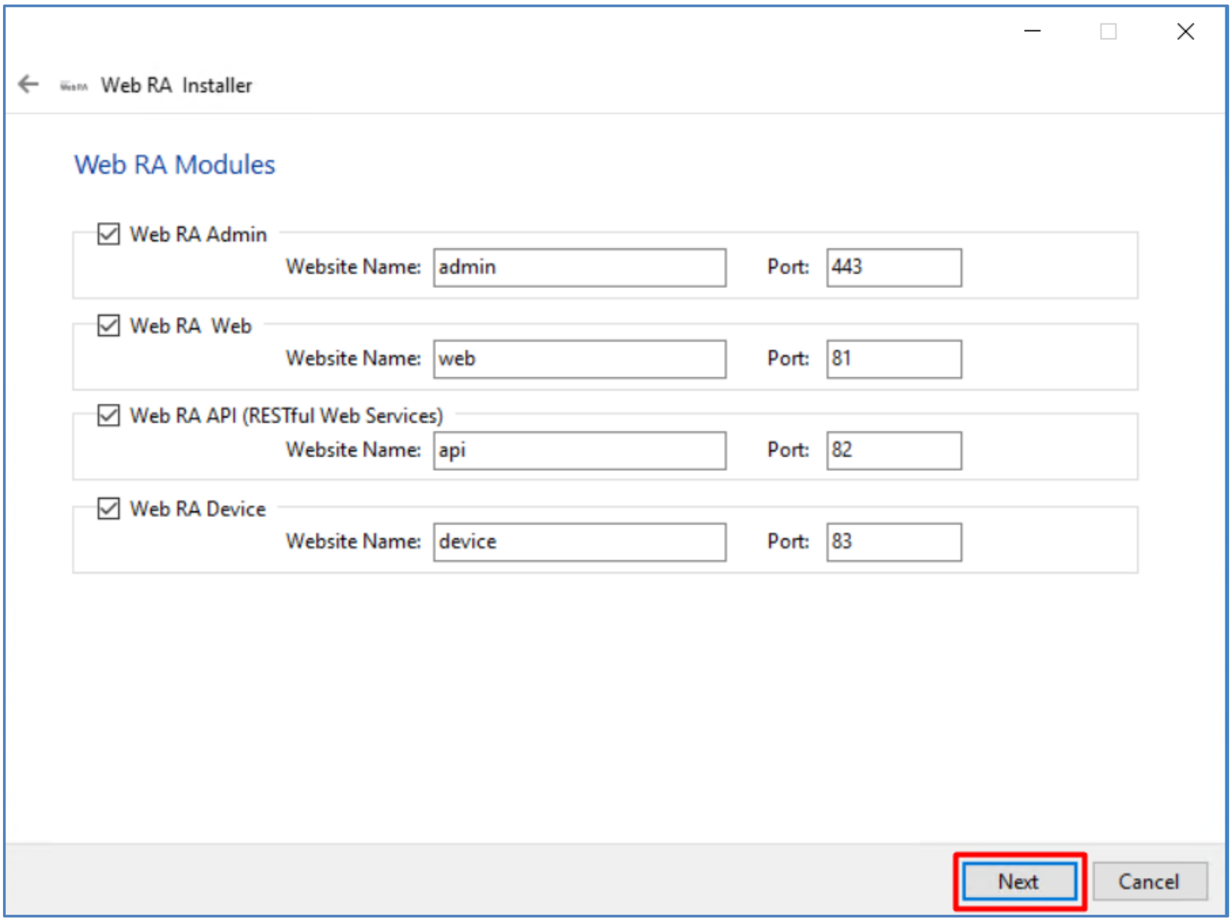
****

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

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

*If the current Web RA database schema is older than the version required by the installer, and you click **Next,** the installer will prompt you that 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.



Web RA Modules

☑ Web RA Admin

Website Name: admin Port: 443

☑ Web RA Web

Website Name: web Port: 81

☑ Web RA API (RESTful Web Services)

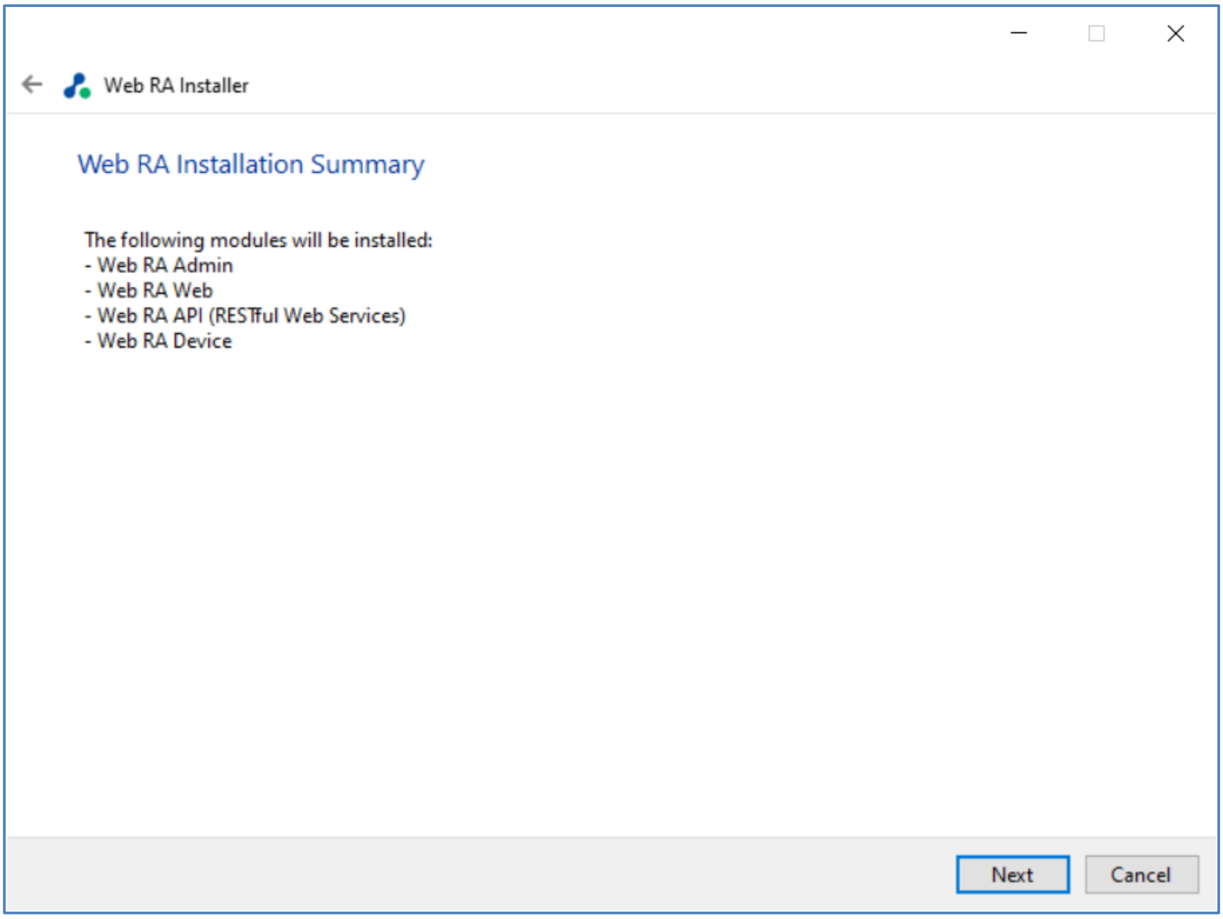
Website Name: api Port: 82

☑ Web RA Device

Website Name: device Port: 83

Select the appropriate modules to install the required features.

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



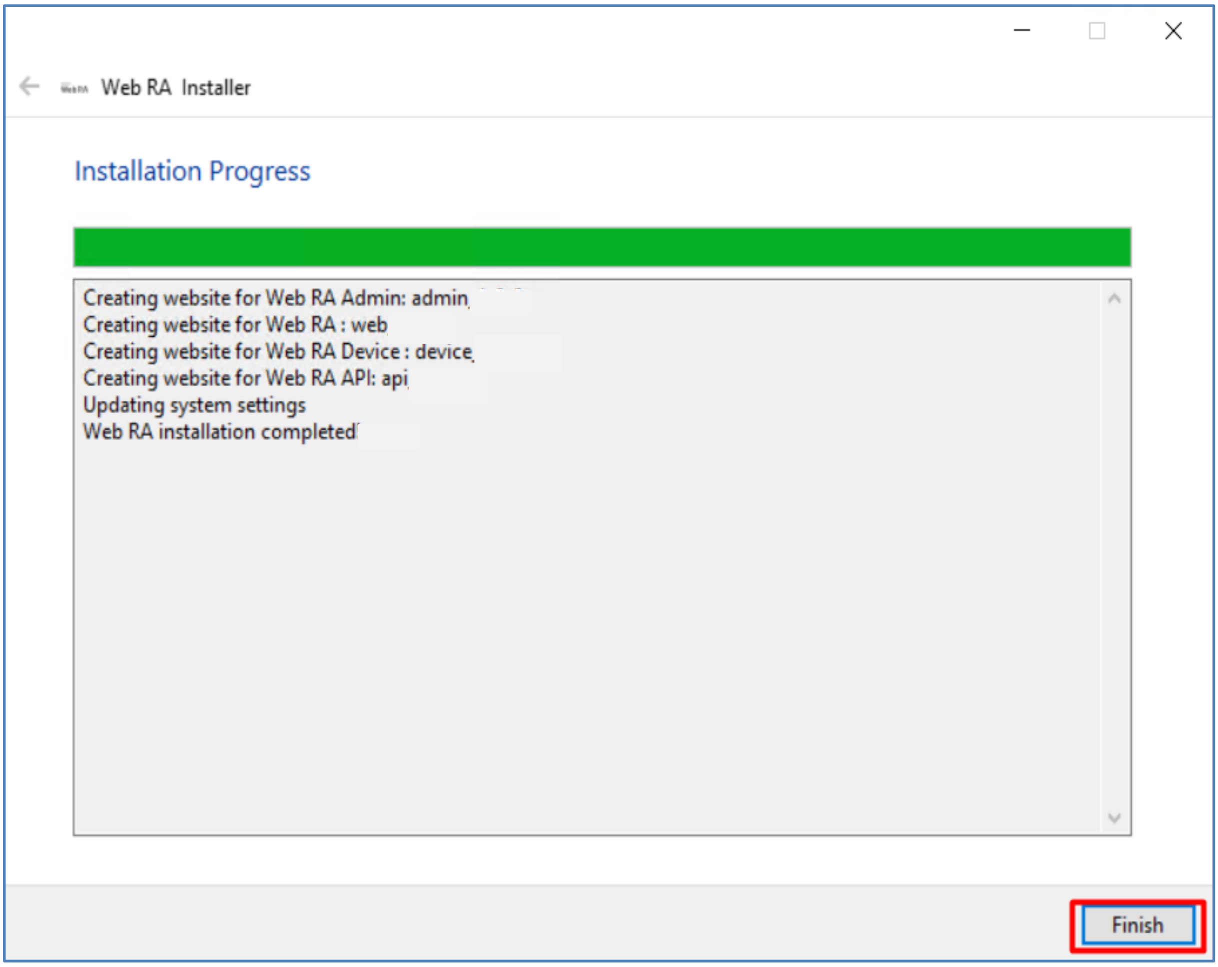
Web RA Installation Summary

The following modules will be installed:
- Web RA Admin
- Web RA Web
- Web RA API (RESTful Web Services)
- Web RA Device

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.



```
Creating website for Web RA Admin: admin
Creating website for Web RA : web
Creating website for Web RA Device : device
Creating website for Web RA API: api
Updating system settings
Web RA installation completed
```

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

4.4 Upgrading Web RA

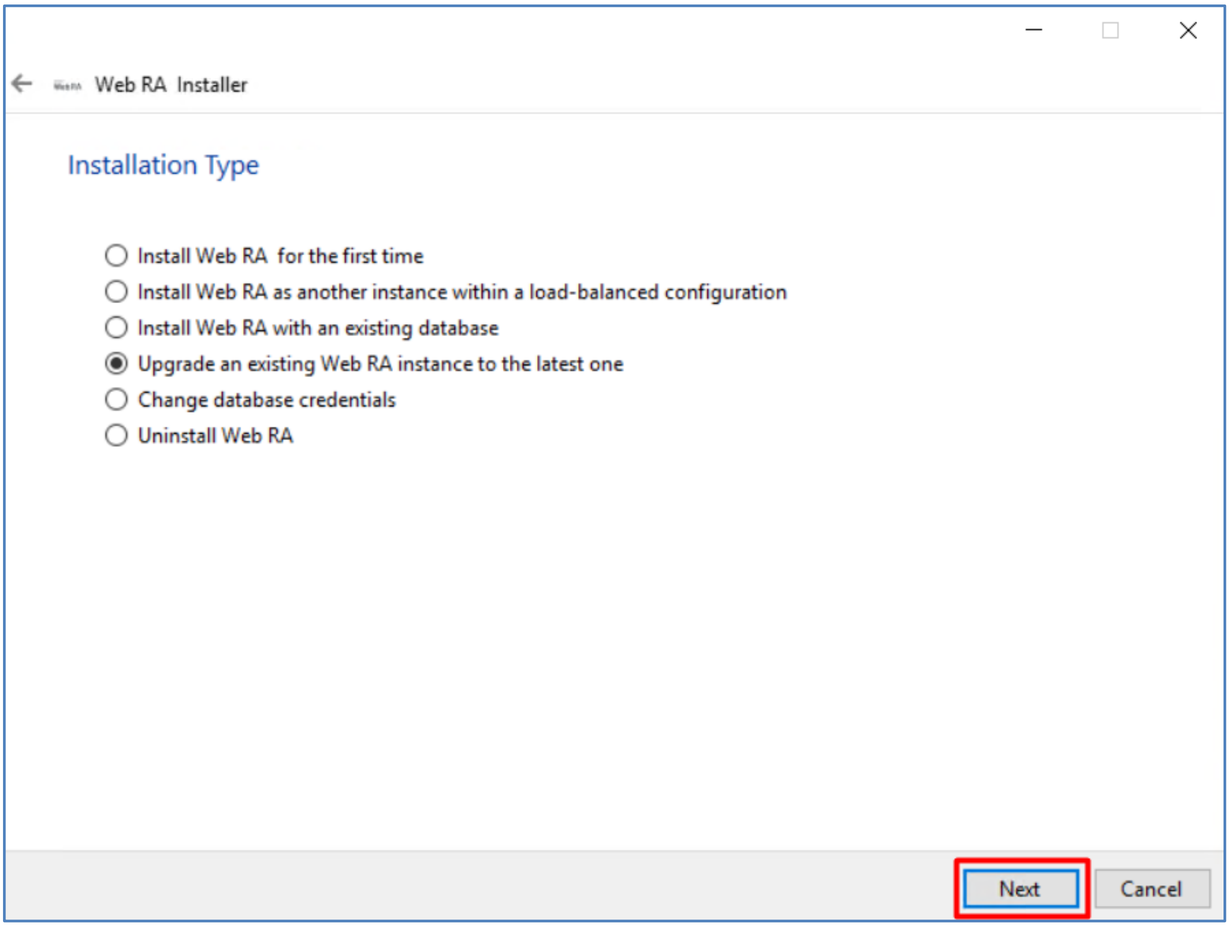
The upgrade process for Web RA is quick and easy. The existing data files, database schema and database entries are automatically upgraded during the process.

4.4.1 Upgrade Procedure

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

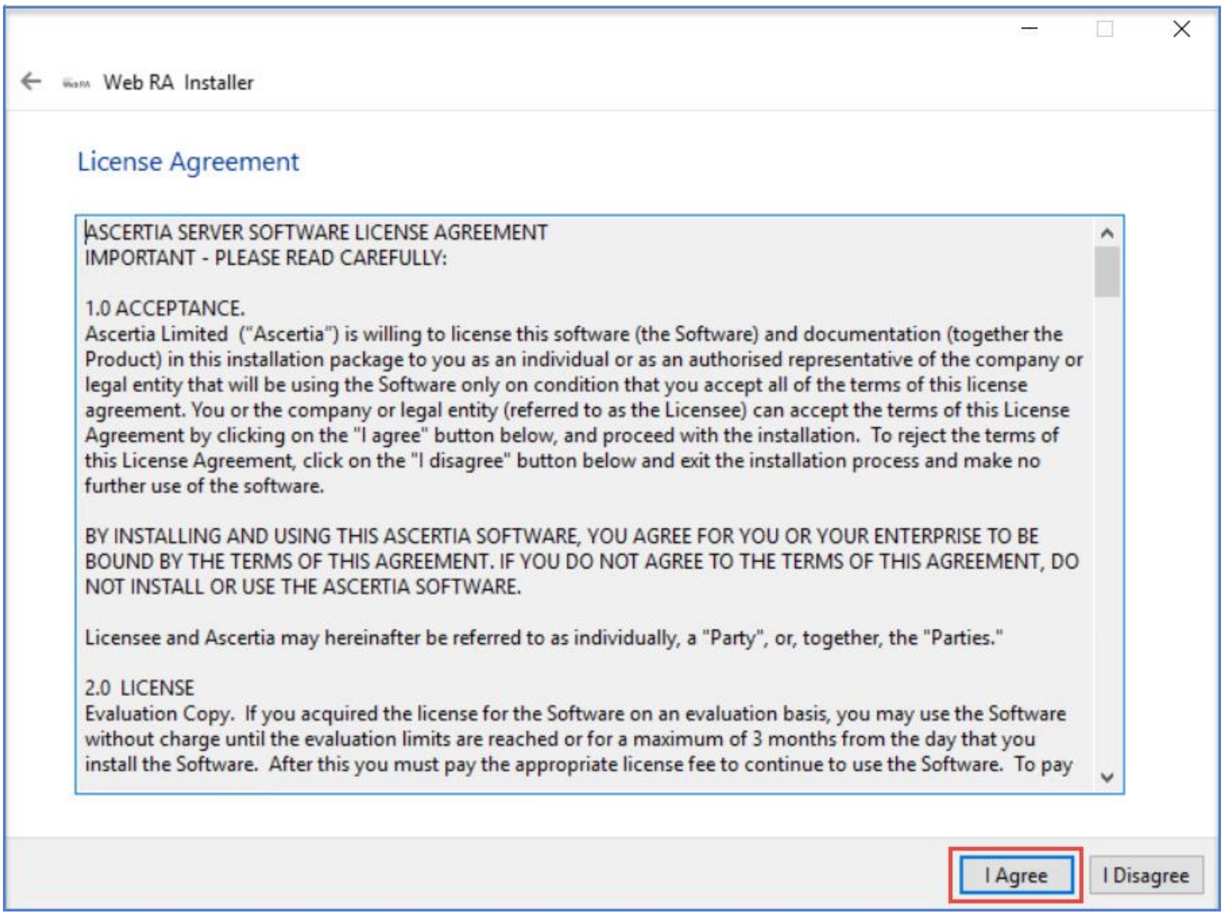
Select the option **Upgrade an existing Web RA instance to latest one**



Installation Type

○ Install Web RA for the first time
○ Install Web RA as another instance within a load-balanced configuration
○ Install Web RA with an existing database
● Upgrade an existing Web RA instance to the latest one
○ Change database credentials
○ Uninstall Web RA

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



ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:

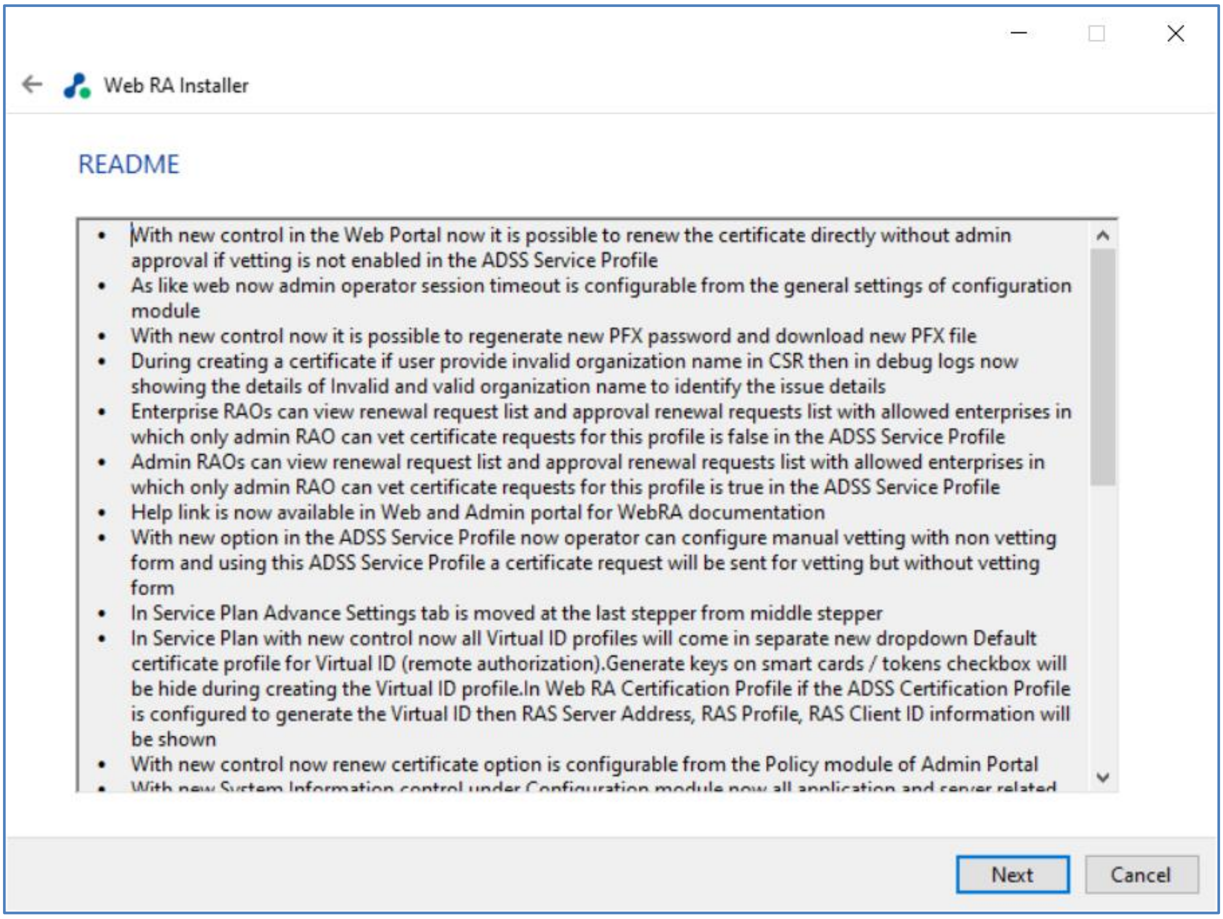
1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition that you accept all of the terms of this license agreement. You or the company or legal entity (referred to as the Licensee) can accept the terms of this License Agreement by clicking on the "I agree" button below, and proceed with the installation. To reject the terms of this License Agreement, click on the "I disagree" button below and exit the installation process and make no further use of the software.

BY INSTALLING AND USING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE ASCERTIA SOFTWARE.

Licensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Parties."

2.0 LICENSE
Evaluation Copy. If you acquired the license for the Software on an evaluation basis, you may use the Software without charge until the evaluation limits are reached or for a maximum of 3 months from the day that you install the Software. After this you must pay the appropriate license fee to continue to use the Software. To pay

Click the **I Agree** button to proceed

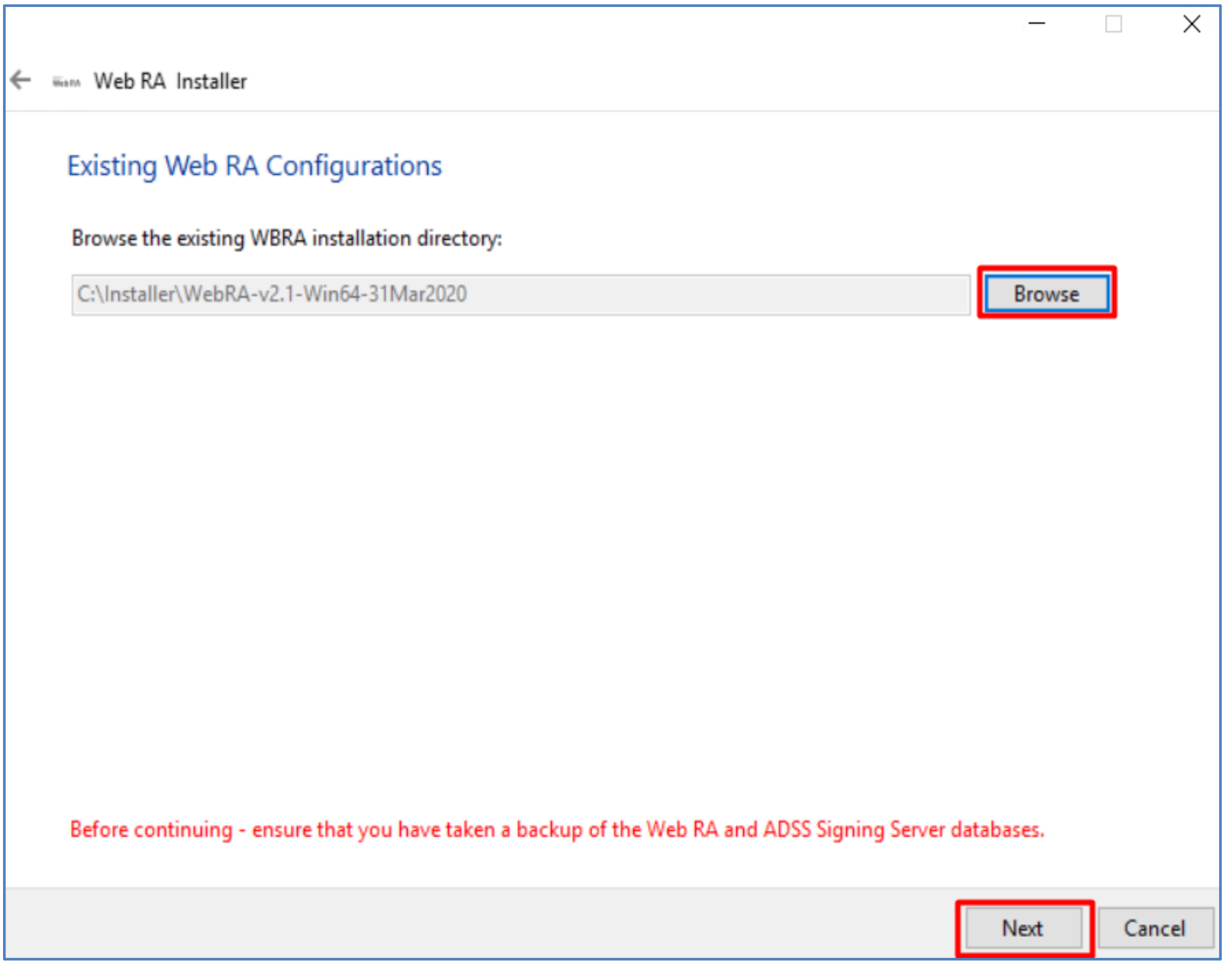


README

- With new control in the Web Portal now it is possible to renew the certificate directly without admin approval if vetting is not enabled in the ADSS Service Profile
- As like web now admin operator session timeout is configurable from the general settings of configuration module
- With new control now it is possible to regenerate new PFX password and download new PFX file
- During creating a certificate if user provide invalid organization name in CSR then in debug logs now showing the details of Invalid and valid organization name to identify the issue details
- Enterprise RAOs can view renewal request list and approval renewal requests list with allowed enterprises in which only admin RAO can vet certificate requests for this profile is false in the ADSS Service Profile
- Admin RAOs can view renewal request list and approval renewal requests list with allowed enterprises in which only admin RAO can vet certificate requests for this profile is true in the ADSS Service Profile
- Help link is now available in Web and Admin portal for WebRA documentation
- With new option in the ADSS Service Profile now operator can configure manual vetting with non vetting form and using this ADSS Service Profile a certificate request will be sent for vetting but without vetting form
- In Service Plan Advance Settings tab is moved at the last stepper from middle stepper
- In Service Plan with new control now all Virtual ID profiles will come in separate new dropdown Default certificate profile for Virtual ID (remote authorization).Generate keys on smart cards / tokens checkbox will be hide during creating the Virtual ID profile.In Web RA Certification Profile if the ADSS Certification Profile is configured to generate the Virtual ID then RAS Server Address, RAS Profile, RAS Client ID information will be shown
- With new control now renew certificate option is configurable from the Policy module of Admin Portal
- With new System Information control under Configuration module now all application and server related

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

Click Next to proceed



Existing Web RA Configurations

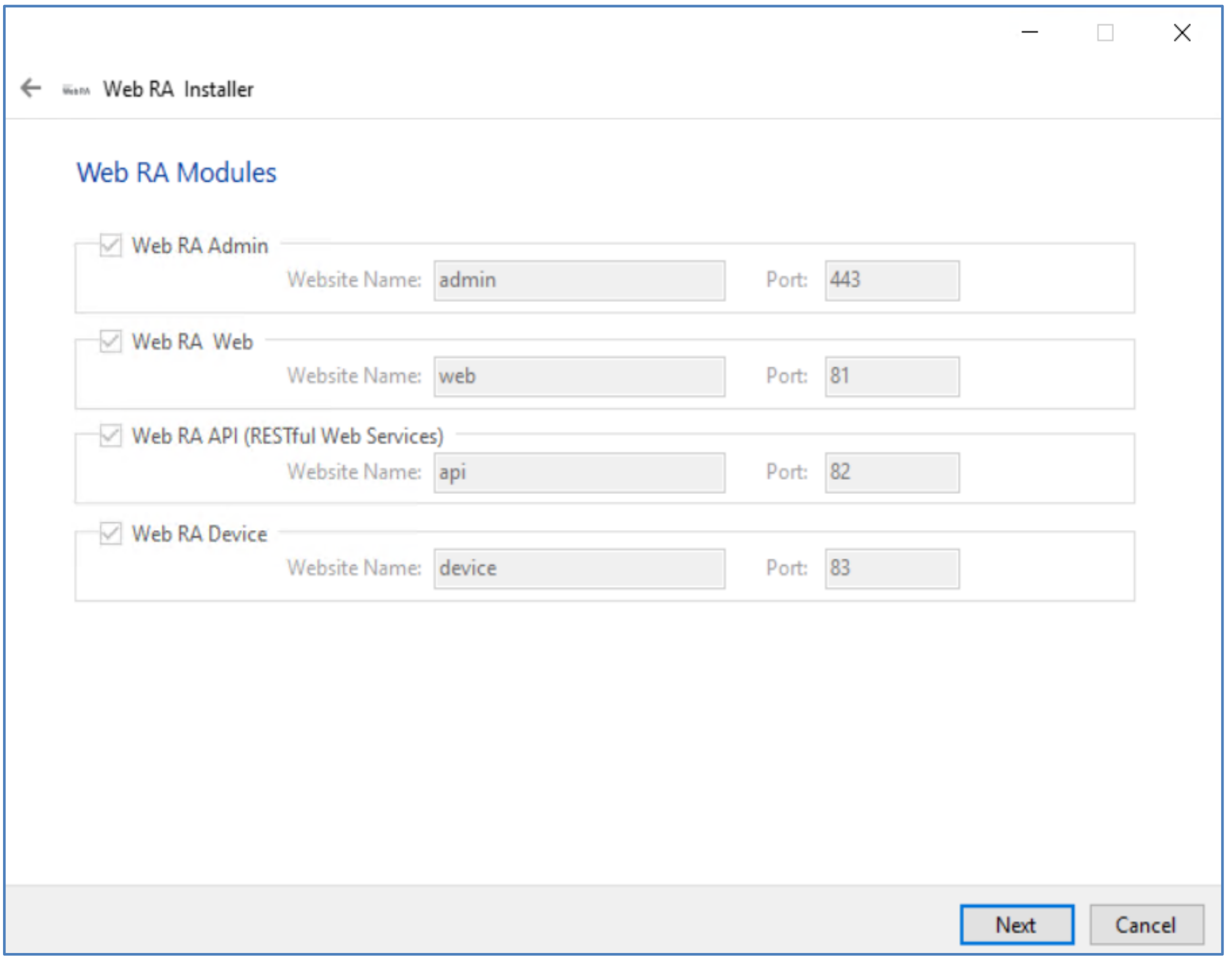
Browse the existing WBRA installation directory:

C:\Installer\WebRA-v2.1-Win64-31Mar2020

Before continuing - ensure that you have taken a backup of the Web RA and ADSS Signing Server databases.

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

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


Web RA Installer

Web RA Modules

☑ Web RA Admin
Website Name: admin
Port: 443

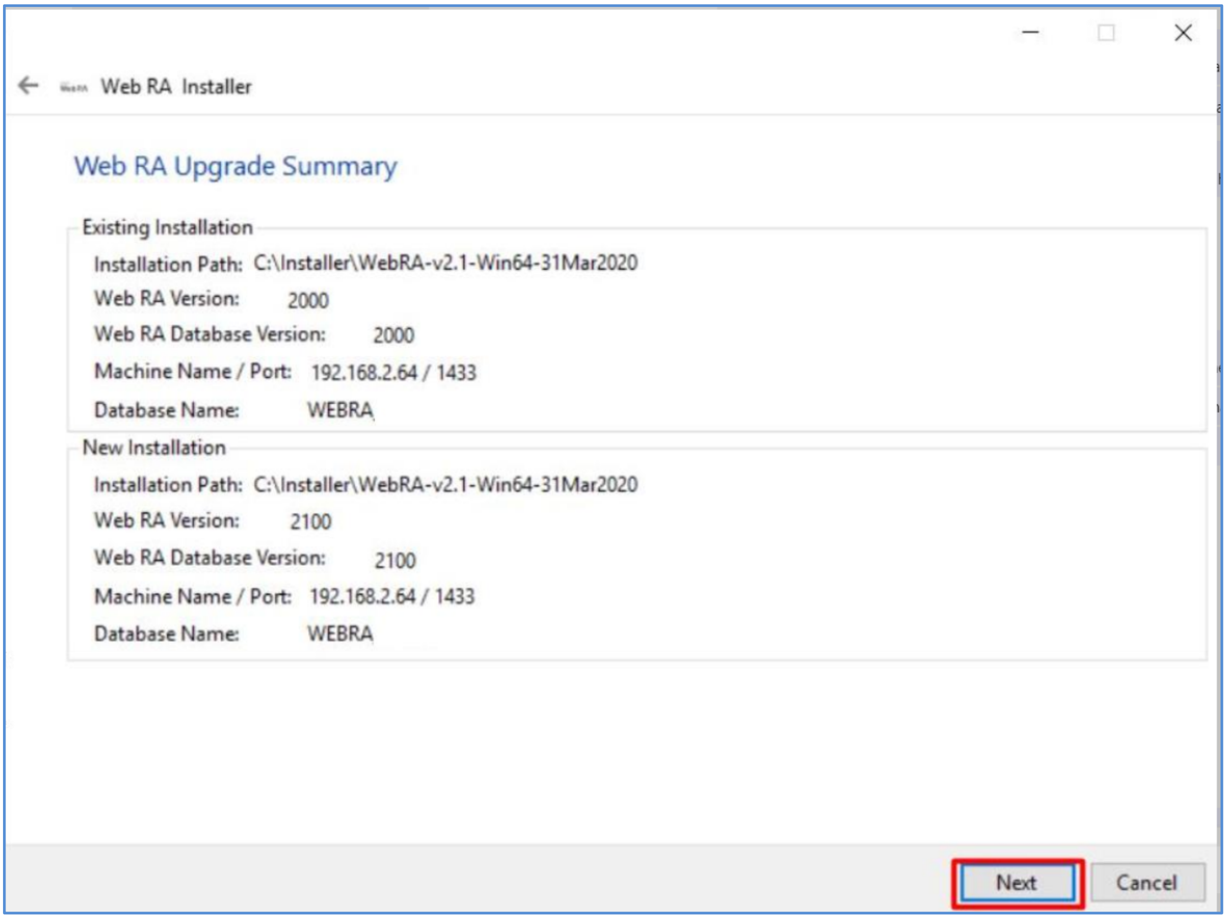
☑ Web RA Web
Website Name: web
Port: 81

☑ Web RA API (RESTful Web Services)
Website Name: api
Port: 82

☑ Web RA Device
Website Name: device
Port: 83

This screen shows a list of all Web RA modules. Components that are already installed are displayed but **greyed** out, while any 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:



Web RA Upgrade Summary

Existing Installation

Installation Path: C:\Installer\WebRA-v2.1-Win64-31Mar2020

Web RA Version: 2000

Web RA Database Version: 2000

Machine Name / Port: 192.168.2.64 / 1433

Database Name: WEBRA

New Installation

Installation Path: C:\Installer\WebRA-v2.1-Win64-31Mar2020

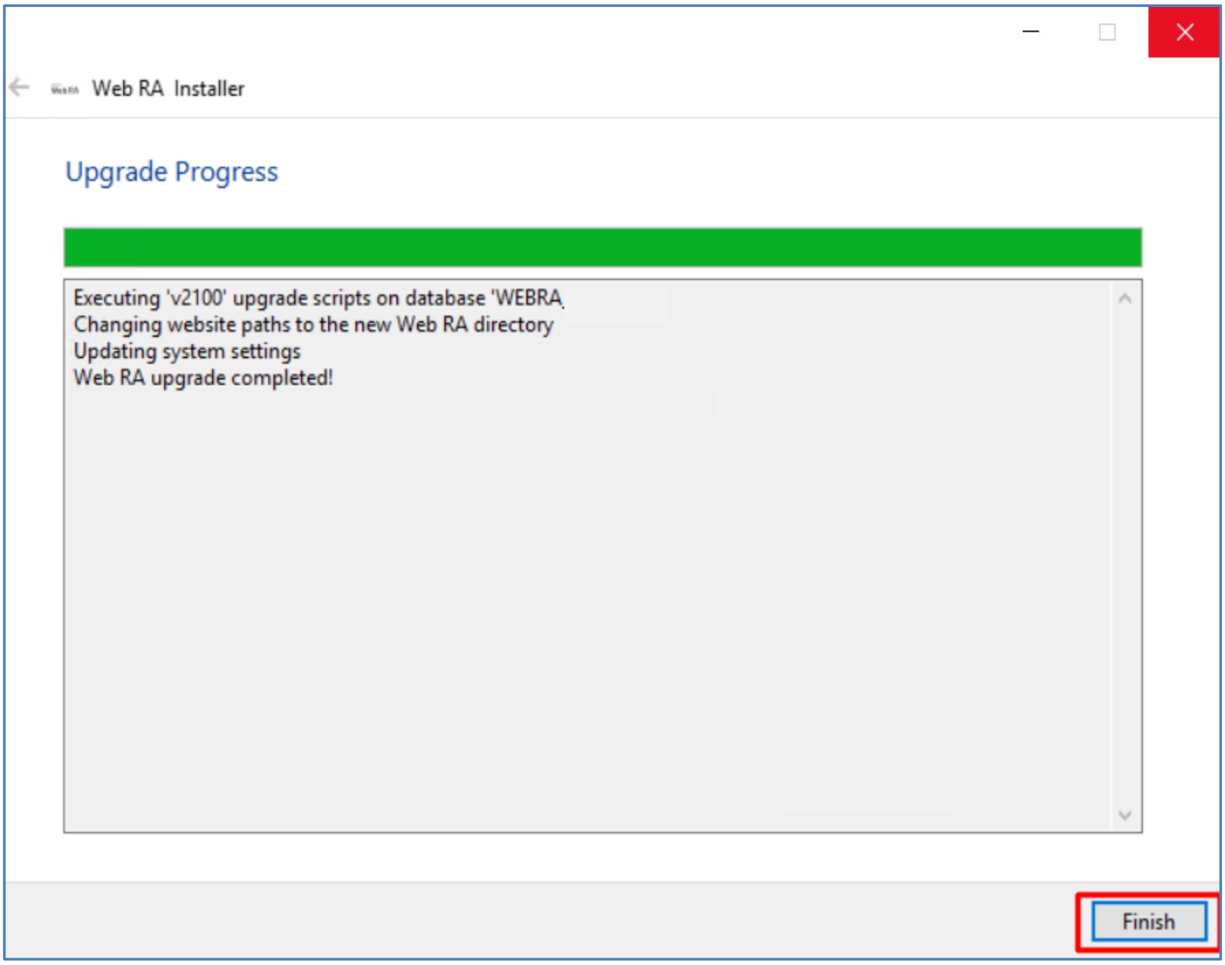
Web RA Version: 2100

Web RA Database Version: 2100

Machine Name / Port: 192.168.2.64 / 1433

Database Name: WEBRA

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



```
Executing 'v2100' upgrade scripts on database 'WEBRA
Changing website paths to the new Web RA directory
Updating system settings
Web RA upgrade completed!
```

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

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

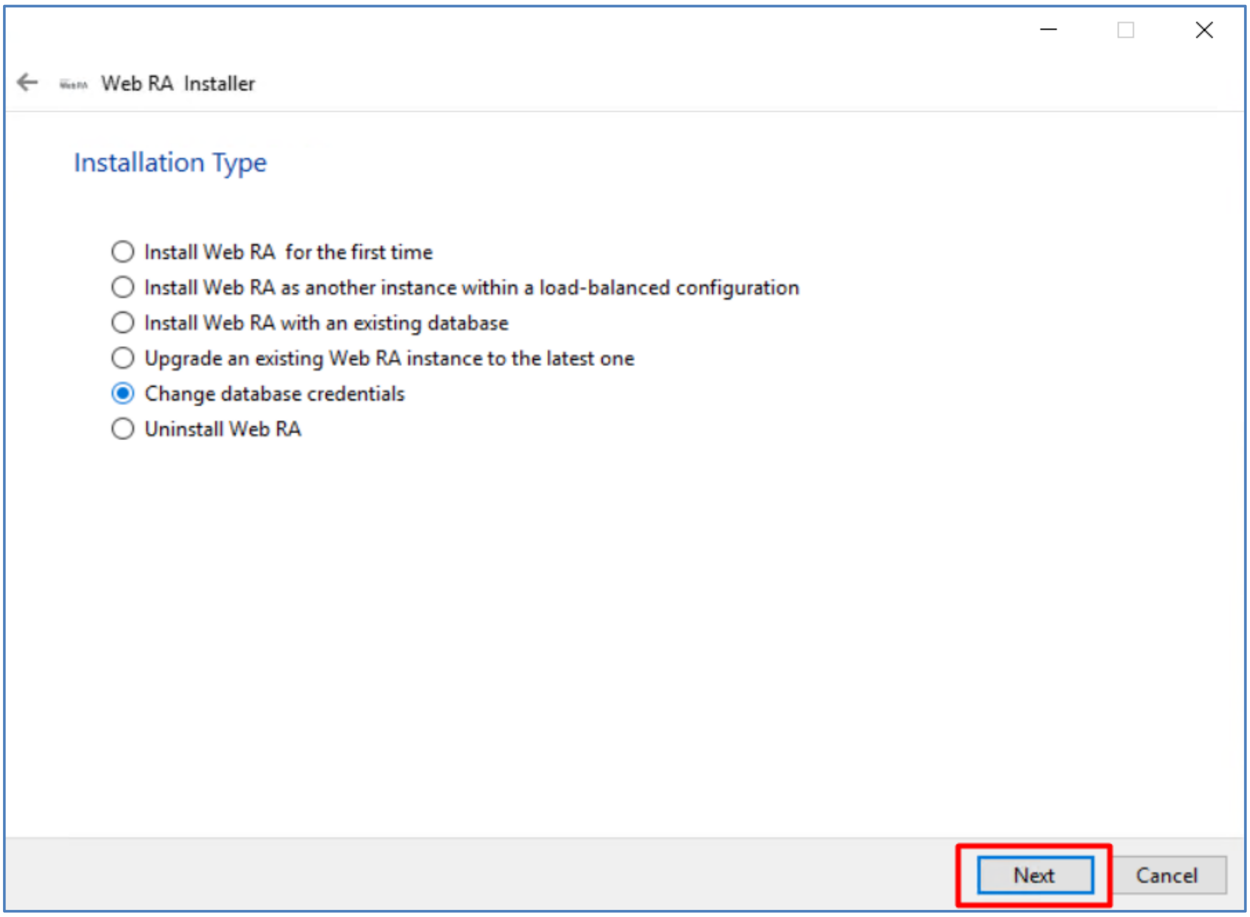
4.5 Changing Database Credentials for an Existing Installation

Database credentials stored by 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 Web RA installation for the signing operations to continue.

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:

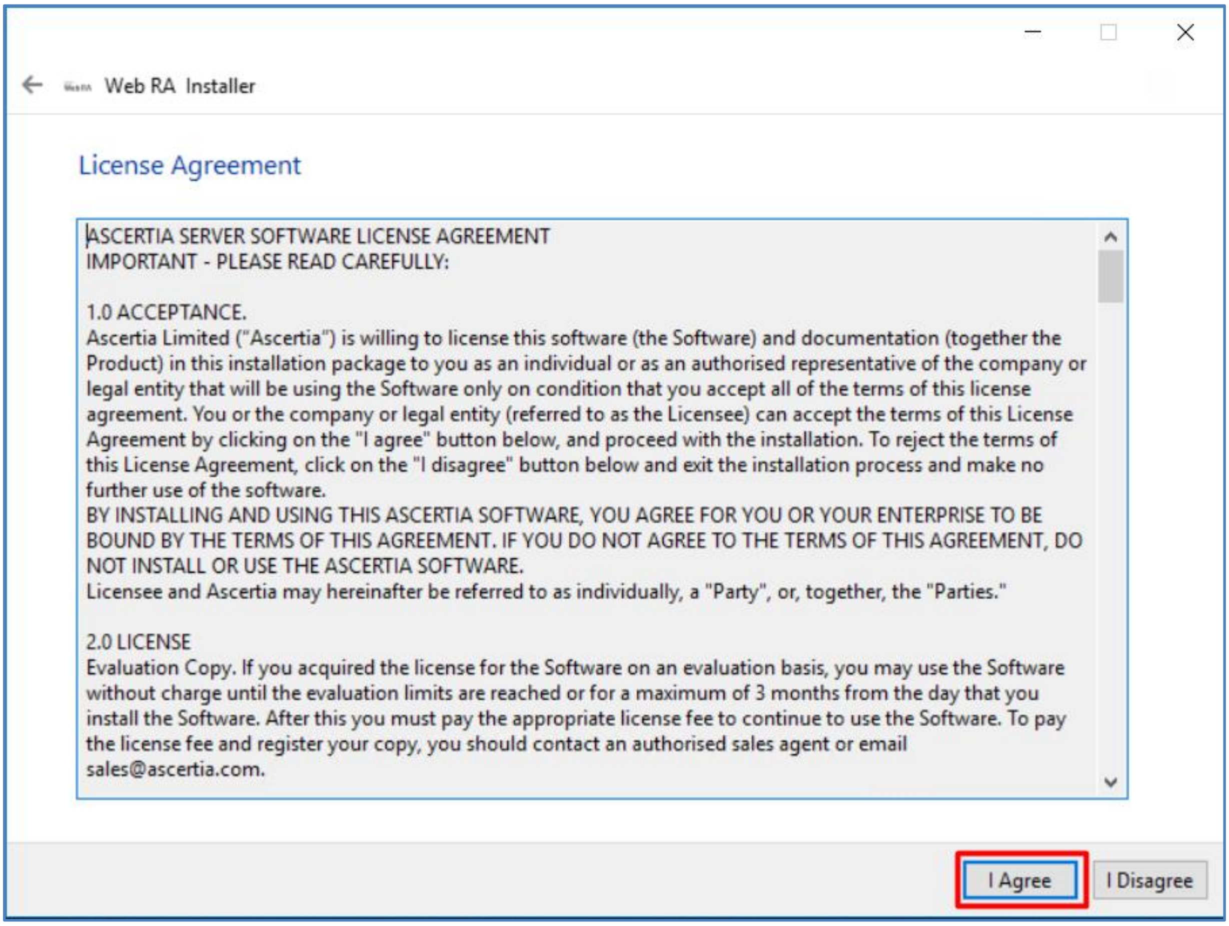


Web RA Installer

Installation Type

○ Install Web RA for the first time
○ Install Web RA as another instance within a load-balanced configuration
○ Install Web RA with an existing database
○ Upgrade an existing Web RA instance to the latest one
● Change database credentials
○ Uninstall Web RA

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



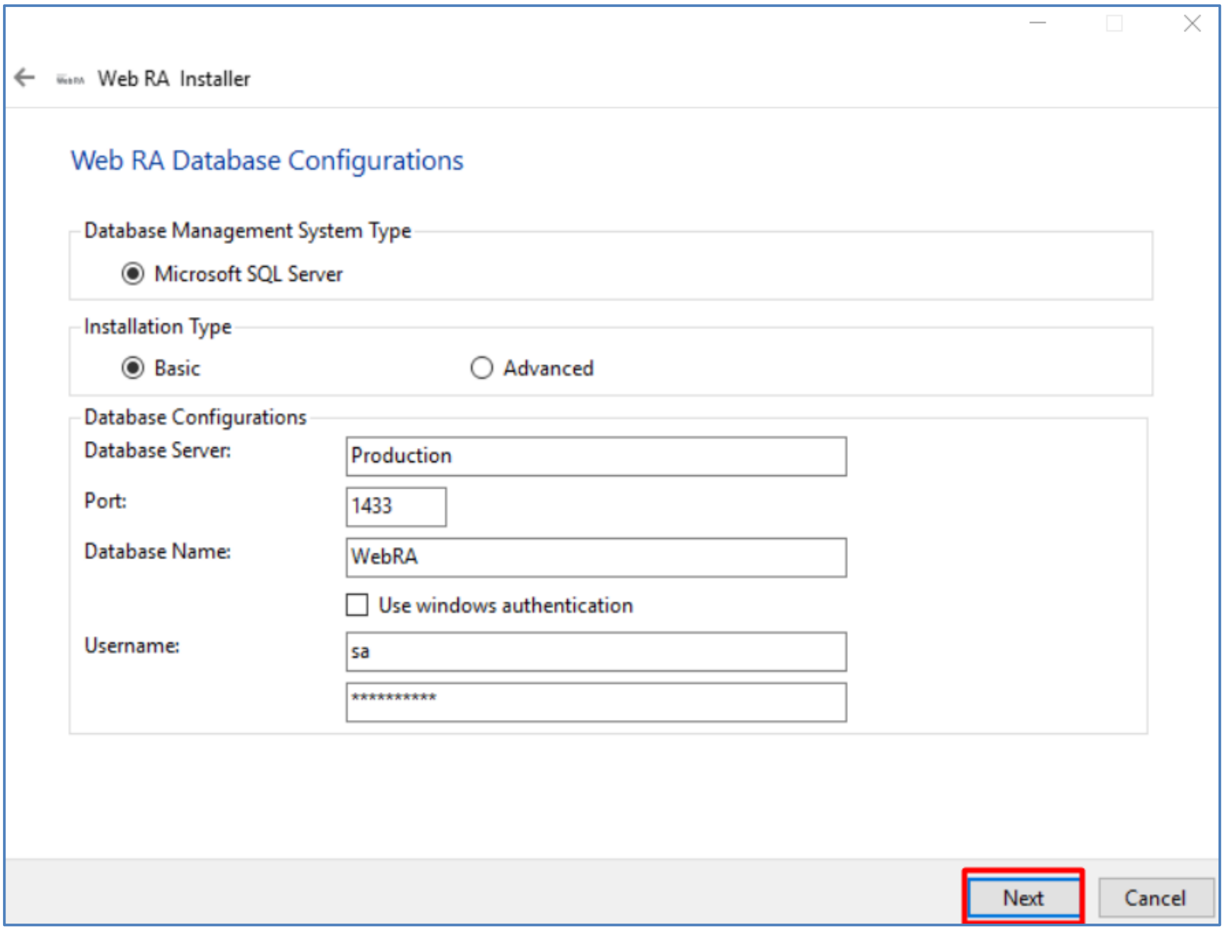
ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:

1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition that you accept all of the terms of this license agreement. You or the company or legal entity (referred to as the Licensee) can accept the terms of this License Agreement by clicking on the "I agree" button below, and proceed with the installation. To reject the terms of this License Agreement, click on the "I disagree" button below and exit the installation process and make no further use of the software.
BY INSTALLING AND USING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE ASCERTIA SOFTWARE.
Licensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Parties."

2.0 LICENSE
Evaluation Copy. If you acquired the license for the Software on an evaluation basis, you may use the Software without charge until the evaluation limits are reached or for a maximum of 3 months from the day that you install the Software. After this you must pay the appropriate license fee to continue to use the Software. To pay the license fee and register your copy, you should contact an authorised sales agent or email sales@ascertia.com.

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

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



Web RA Database Configurations

Database Management System Type

● Microsoft SQL Server

Installation Type

● Basic ○ Advanced

Database Configurations

Database Server: Production

Port: 1433

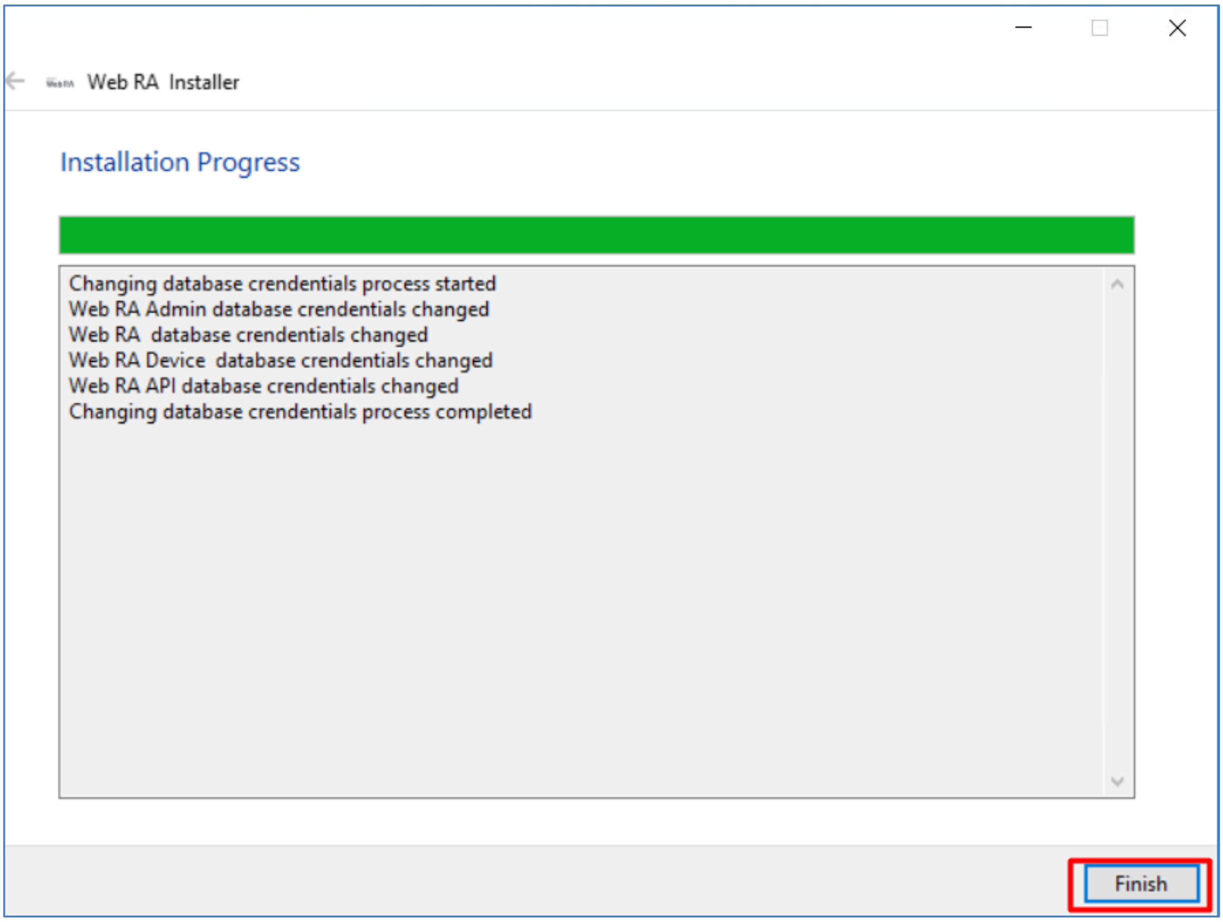
Database Name: WebRA

□ Use windows authentication

Username: sa

****

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



```
Changing database crendentials process started
Web RA Admin database crendentials changed
Web RA  database crendentials changed
Web RA Device  database crendentials changed
Web RA API database crendentials changed
Changing database crendentials process completed
```

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

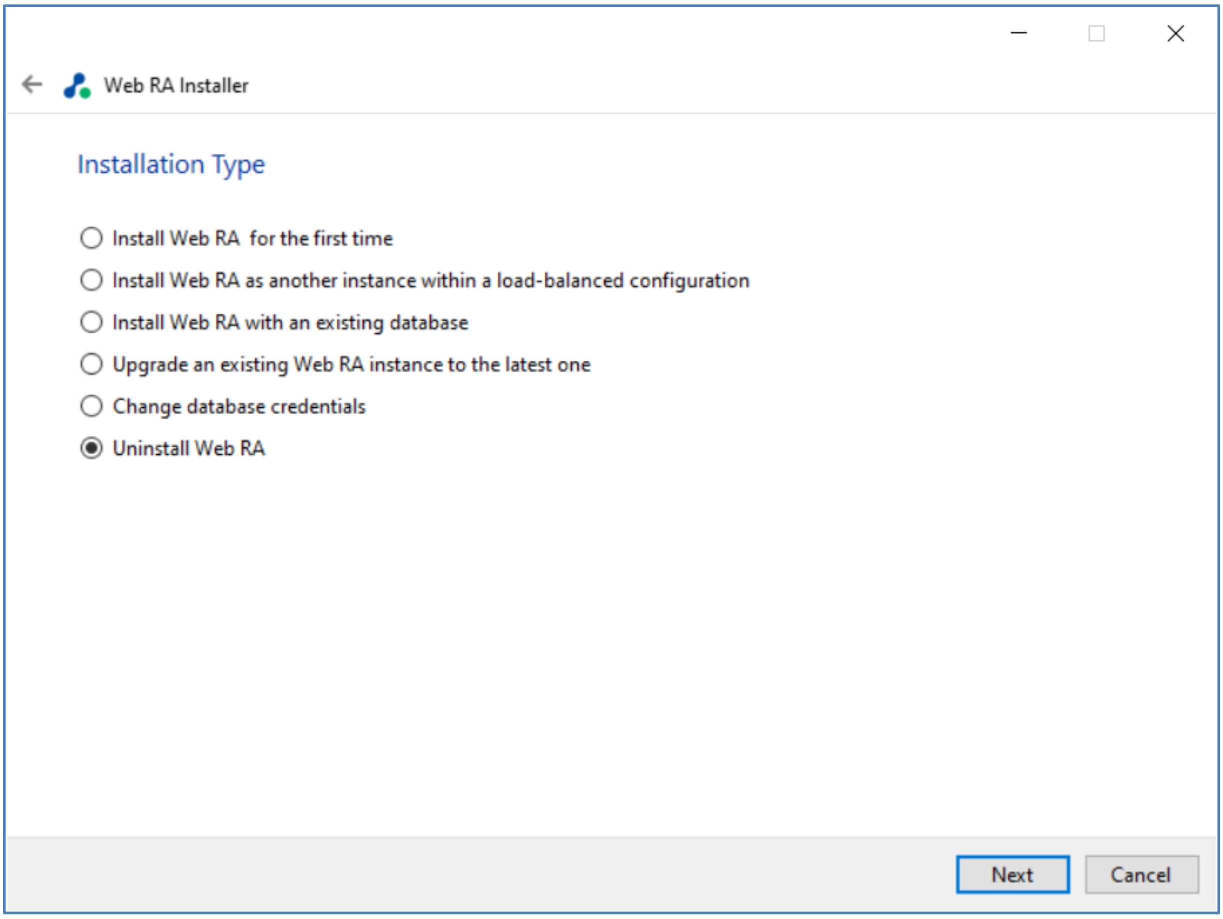
5 Web RA Uninstallation

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

For this:

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

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



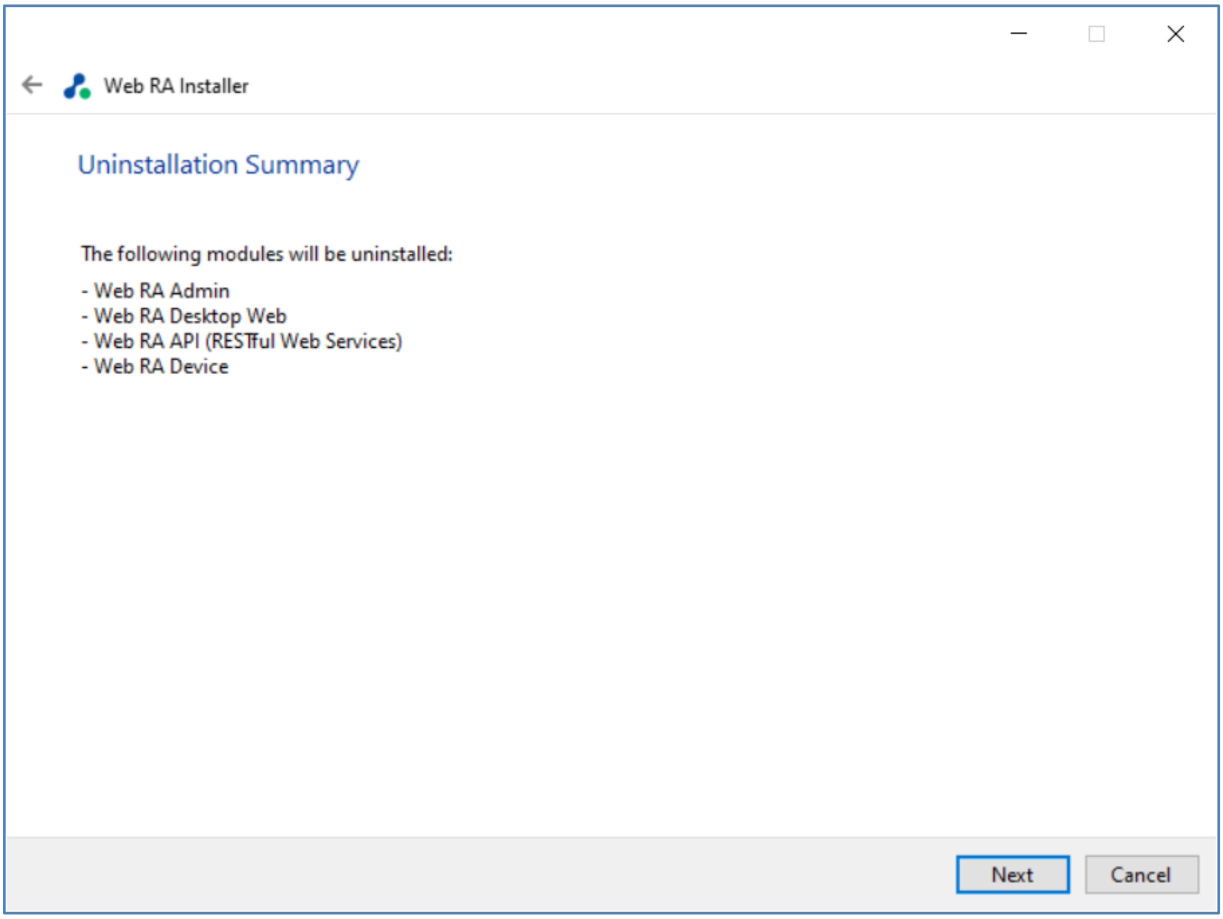
Installation Type

○ Install Web RA for the first time
○ Install Web RA as another instance within a load-balanced configuration
○ Install Web RA with an existing database
○ Upgrade an existing Web RA instance to the latest one
○ Change database credentials
● Uninstall Web RA

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

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

The following screen is shown:

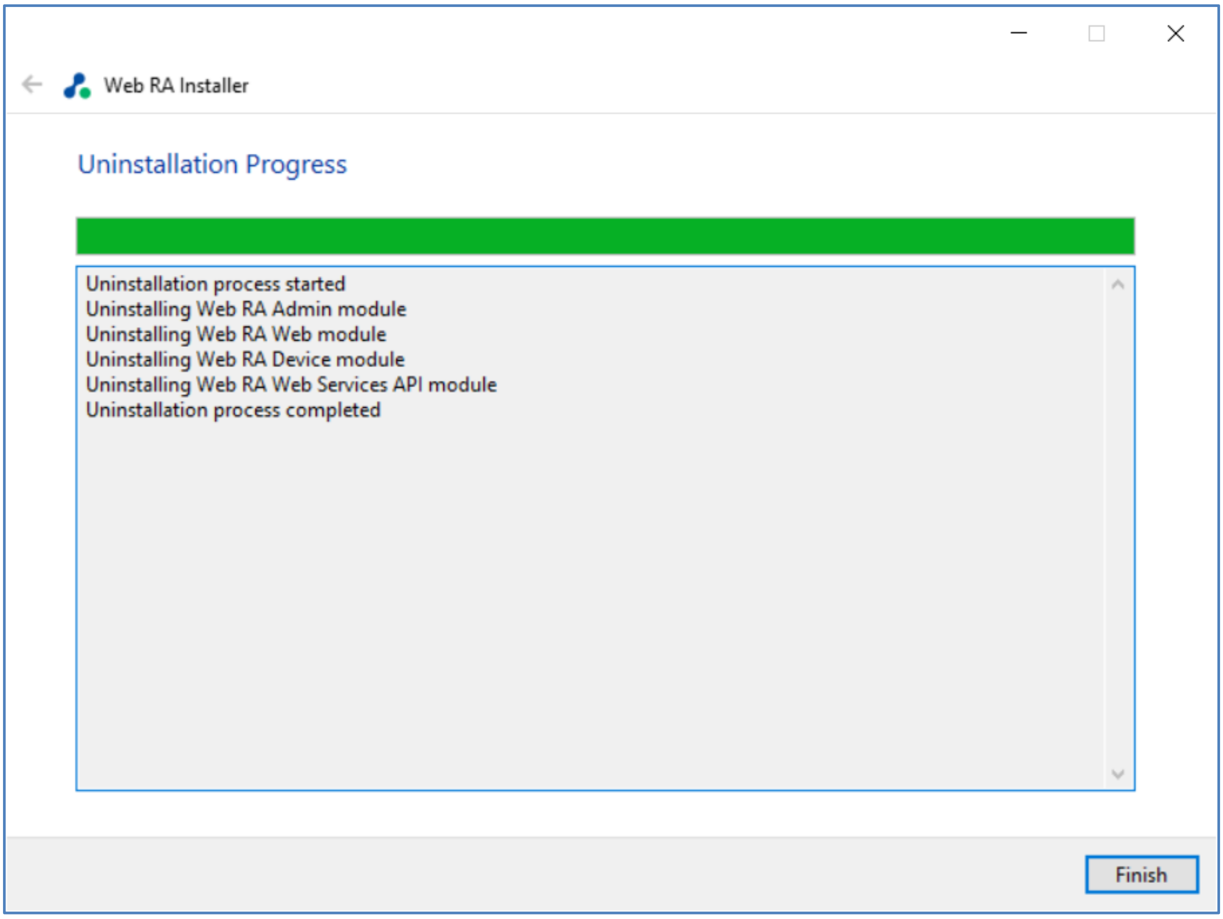


Uninstallation Summary

The following modules will be uninstalled:

- Web RA Admin
- Web RA Desktop Web
- Web RA API (RESTful Web Services)
- Web RA Device

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



Uninstallation process started
Uninstalling Web RA Admin module
Uninstalling Web RA Web module
Uninstalling Web RA Device module
Uninstalling Web RA Web Services API module
Uninstallation process completed

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 Web RA Admin module is installed on Windows 2012 R2, then the HTTP 403.16 error code may occur when you access the 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**

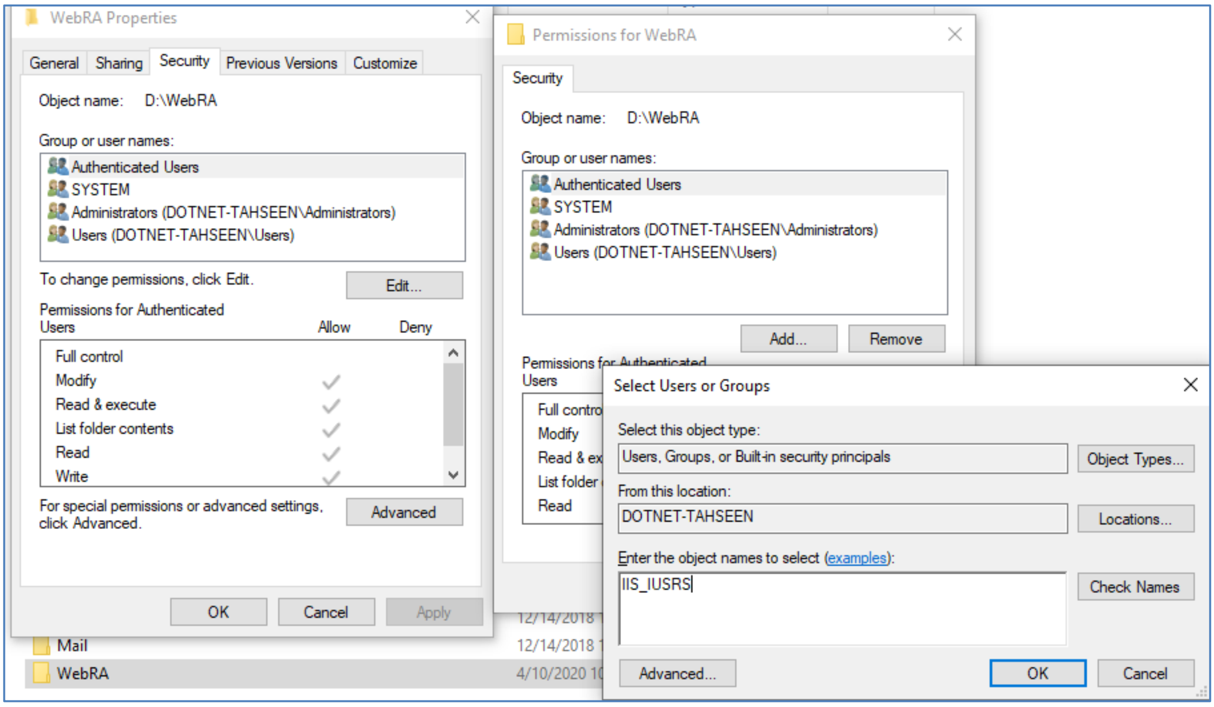
d. Edit the field and set **Value Data: 2**

- 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



WebRA Properties

General | Sharing | Security | Previous Versions | Customize

Object name: D:\WebRA

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (DOTNET-TAHSEEN\Administrators)
- Users (DOTNET-TAHSEEN\Users)

To change permissions, click Edit. Edit...

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply

Permissions for WebRA

Security

Object name: D:\WebRA

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (DOTNET-TAHSEEN\Administrators)
- Users (DOTNET-TAHSEEN\Users)

Add... Remove

Select Users or Groups

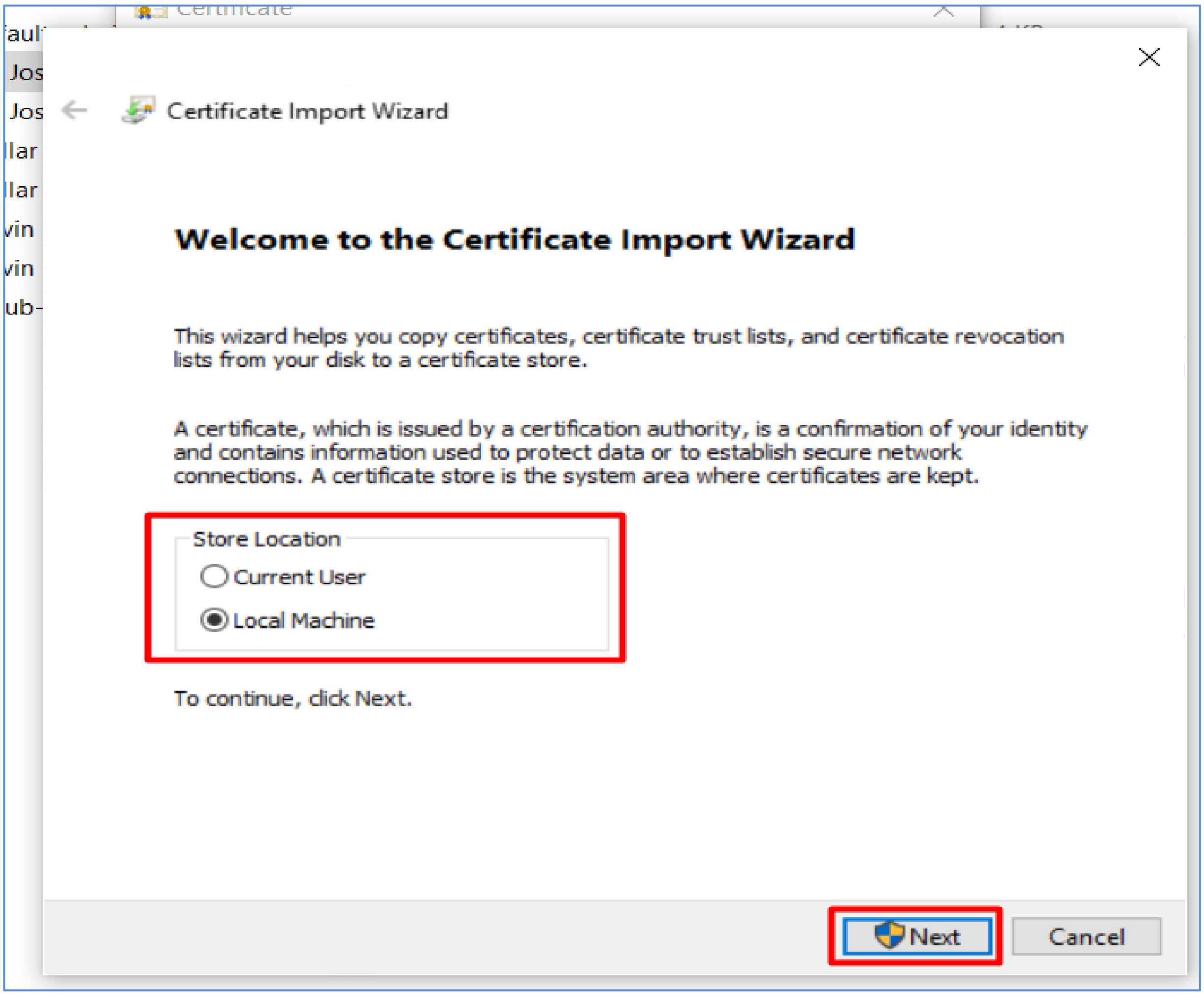
Select this object type:
Users, Groups, or Built-in security principals | Object Types...

From this location:
DOTNET-TAHSEEN | Locations...

Enter the object names to select (examples):
IIS_IUSRS | Check Names

Advanced... OK Cancel

- 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.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

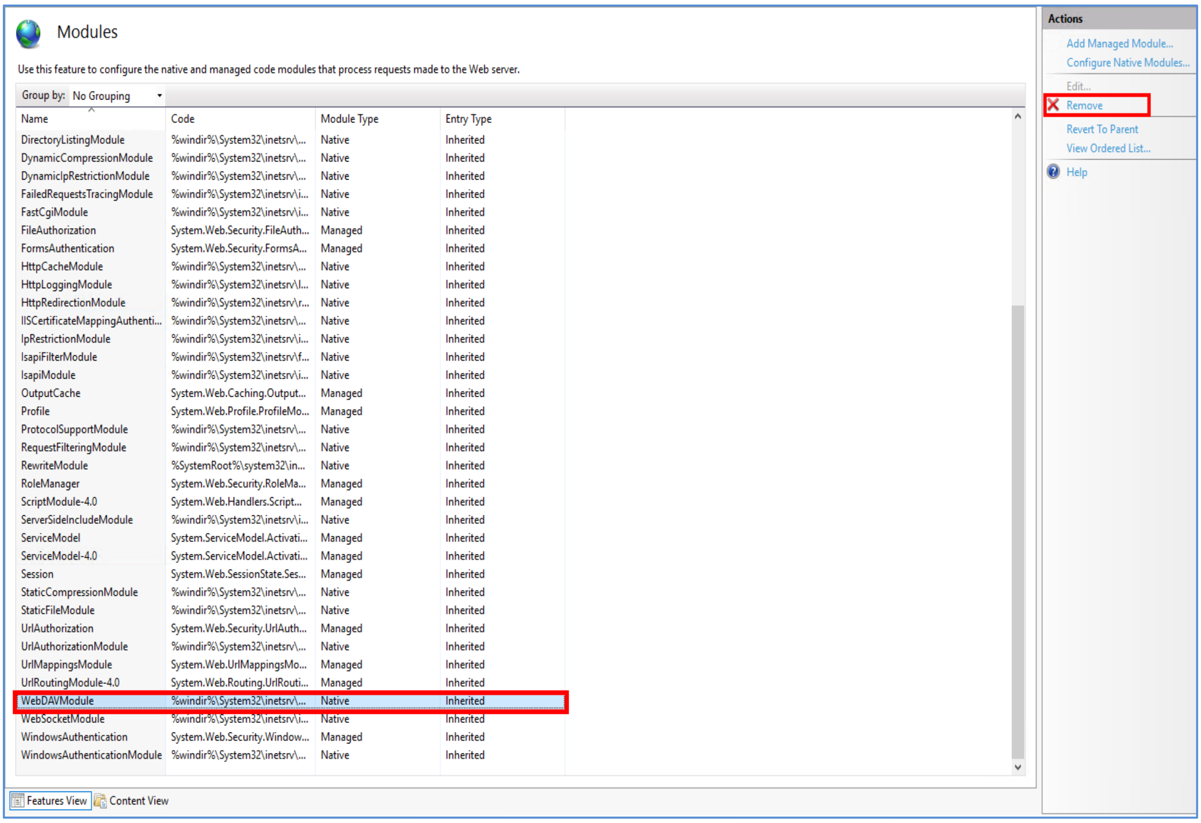
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

Next Cancel

- 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.



Modules

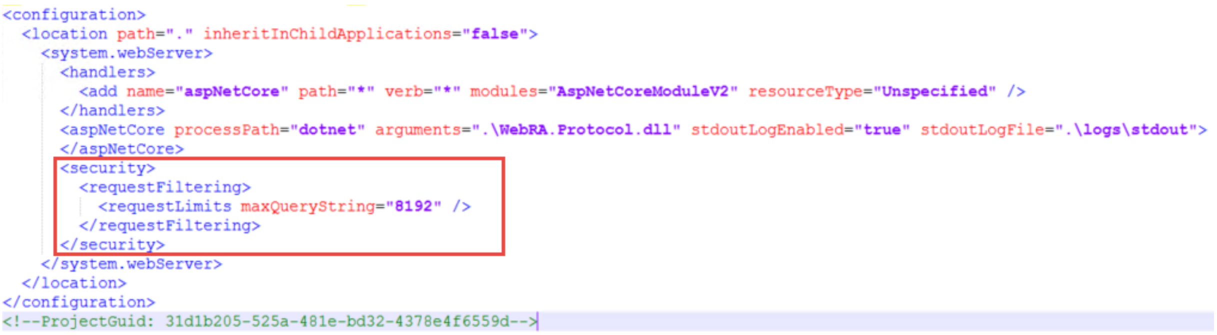
Use this feature to configure the native and managed code modules that process requests made to the Web server.

Group by: No Grouping

Name	Code	Module Type	Entry Type
DirectoryListingModule	%windir%\System32\inetsrv\...	Native	Inherited
DynamicCompressionModule	%windir%\System32\inetsrv\...	Native	Inherited
DynamicIpRestrictionModule	%windir%\System32\inetsrv\...	Native	Inherited
FailedRequestsTracingModule	%windir%\System32\inetsrv\i...	Native	Inherited
FastCgiModule	%windir%\System32\inetsrv\i...	Native	Inherited
FileAuthorization	System.Web.Security.FileAuth...	Managed	Inherited
FormsAuthentication	System.Web.Security.FormsA...	Managed	Inherited
HttpCacheModule	%windir%\System32\inetsrv\...	Native	Inherited
HttpLoggingModule	%windir%\System32\inetsrv\l...	Native	Inherited
HttpRedirectionModule	%windir%\System32\inetsrv\r...	Native	Inherited
IISCertificateMappingAuthenti...	%windir%\System32\inetsrv\...	Native	Inherited
IpRestrictionModule	%windir%\System32\inetsrv\i...	Native	Inherited
IsapiFilterModule	%windir%\System32\inetsrv\f...	Native	Inherited
IsapiModule	%windir%\System32\inetsrv\i...	Native	Inherited
OutputCache	System.Web.Caching.Output...	Managed	Inherited
Profile	System.Web.Profile.ProfileMo...	Managed	Inherited
ProtocolSupportModule	%windir%\System32\inetsrv\...	Native	Inherited
RequestFilteringModule	%windir%\System32\inetsrv\...	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\inetsrv\i...	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\inetsrv\...	Native	Inherited
StaticFileModule	%windir%\System32\inetsrv\...	Native	Inherited
UrlAuthorization	System.Web.Security.UrlAuth...	Managed	Inherited
UrlAuthorizationModule	%windir%\System32\inetsrv\...	Native	Inherited
UrlMappingsModule	System.Web.UrlMappingsMo...	Managed	Inherited
UrlRoutingModule-4.0	System.Web.Routing.UrlRouti...	Managed	Inherited
WebDAVModule	%windir%\System32\inetsrv\...	Native	Inherited
WebSocketModule	%windir%\System32\inetsrv\i...	Native	Inherited
WindowsAuthentication	System.Web.Security.Window...	Managed	Inherited
WindowsAuthenticationModule	%windir%\System32\inetsrv\...	Native	Inherited

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

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



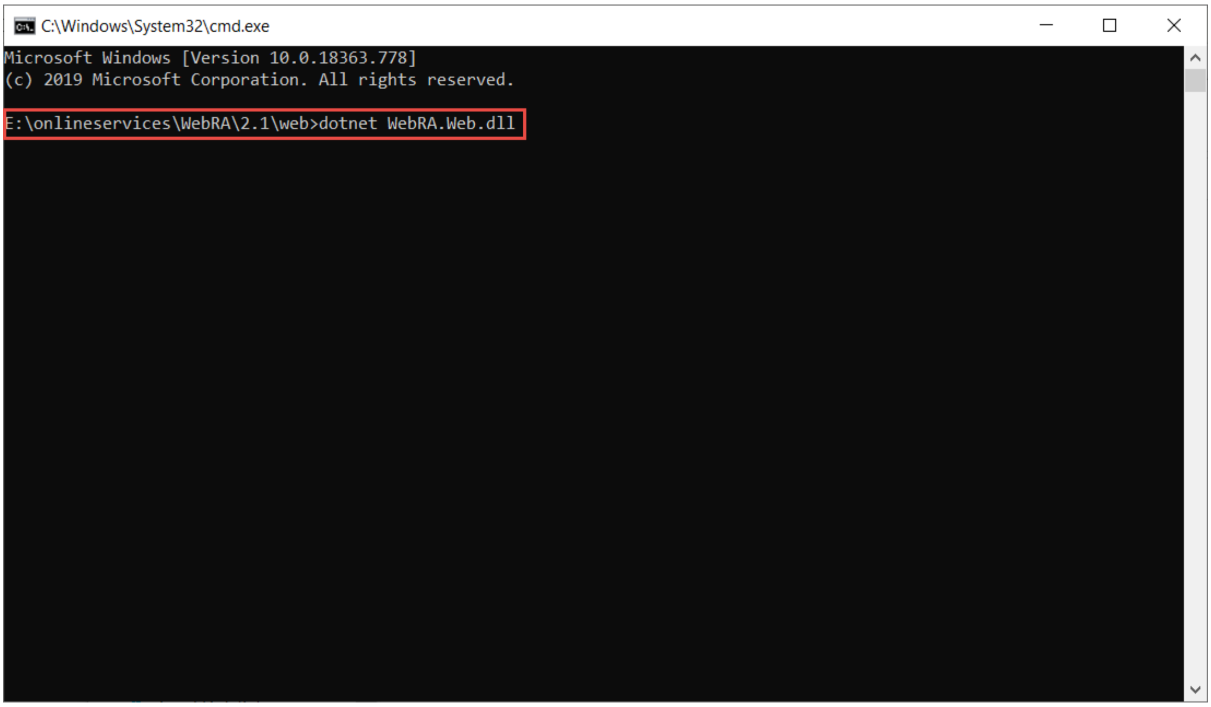
```
<configuration>
  <location path="." inheritInChildApplications="false">
    <system.webServer>
      <handlers>
        <add name="aspNetCore" path="*" verb="*" modules="AspNetCoreModuleV2" resourceType="Unspecified" />
      </handlers>
      <aspNetCore processPath="dotnet" arguments=".\WebRA.Protocol.dll" stdoutLogEnabled="true" stdoutLogFile=".\logs\stdout">
      </aspNetCore>
      <security>
        <requestFiltering>
          <requestLimits maxQueryString="8192" />
        </requestFiltering>
      </security>
    </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

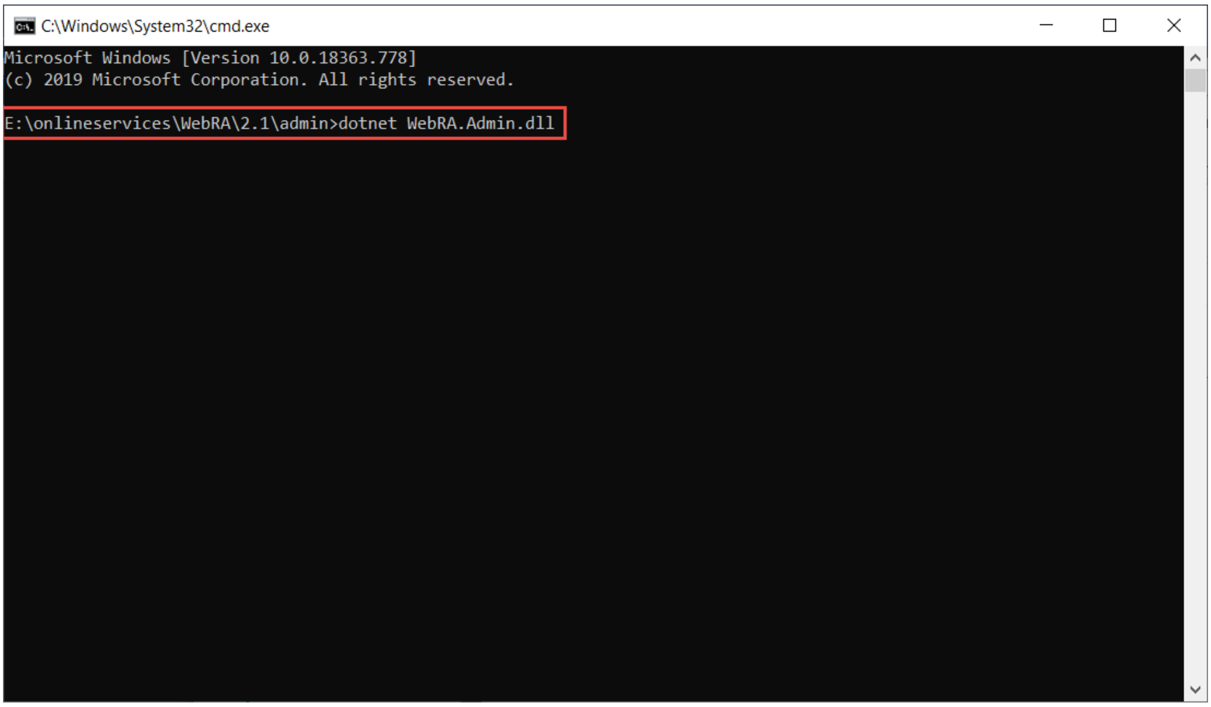
- Update URL value in Expect-CT header in "**web.config**" for web and admin modules according to your deployment URL.
  e.g.
  <add name="Expect-CT" value="max-age=0, report-uri='https://adminra.signinghub.com'" />

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



```
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:



```
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

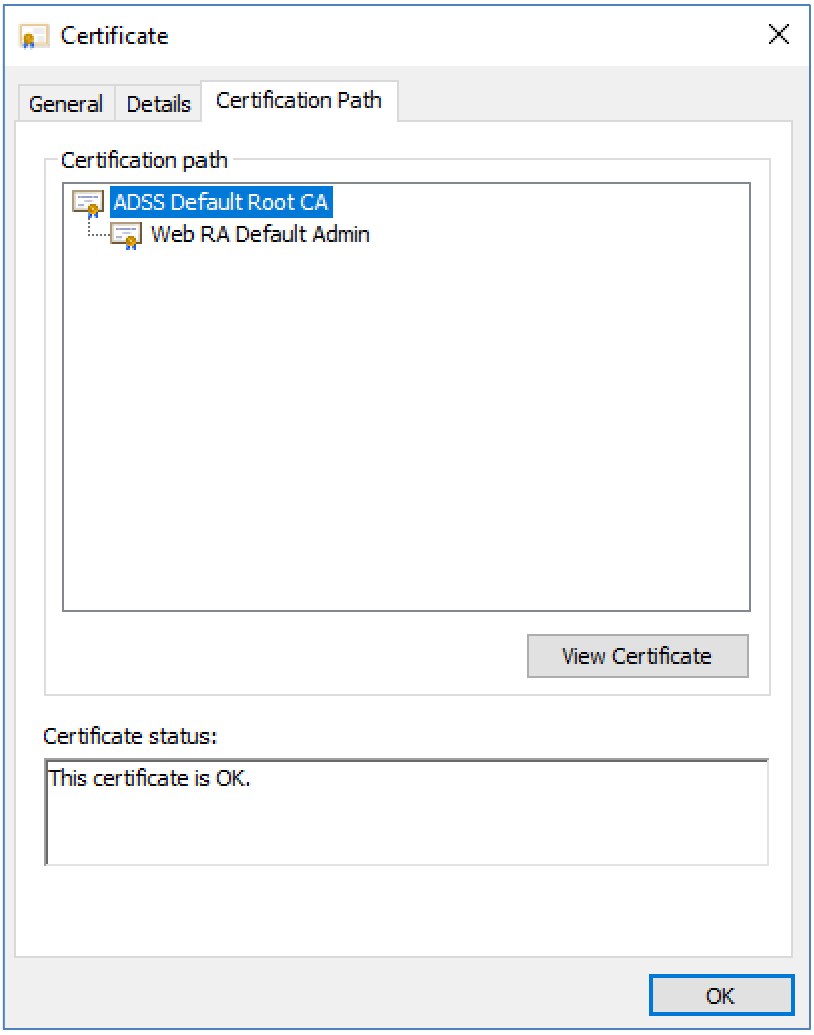
Web RA is a web application that is hosted in IIS. It is recommended to secure the communication between the server and browsers by using SSL over HTTPS. It is also recommended to use an SSL certificate issued by a well-known certificate authority (CA) e.g., Comodo, Symantec, Digicert etc.

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

6.2.1 Exporting Root and Intermediate Certificates

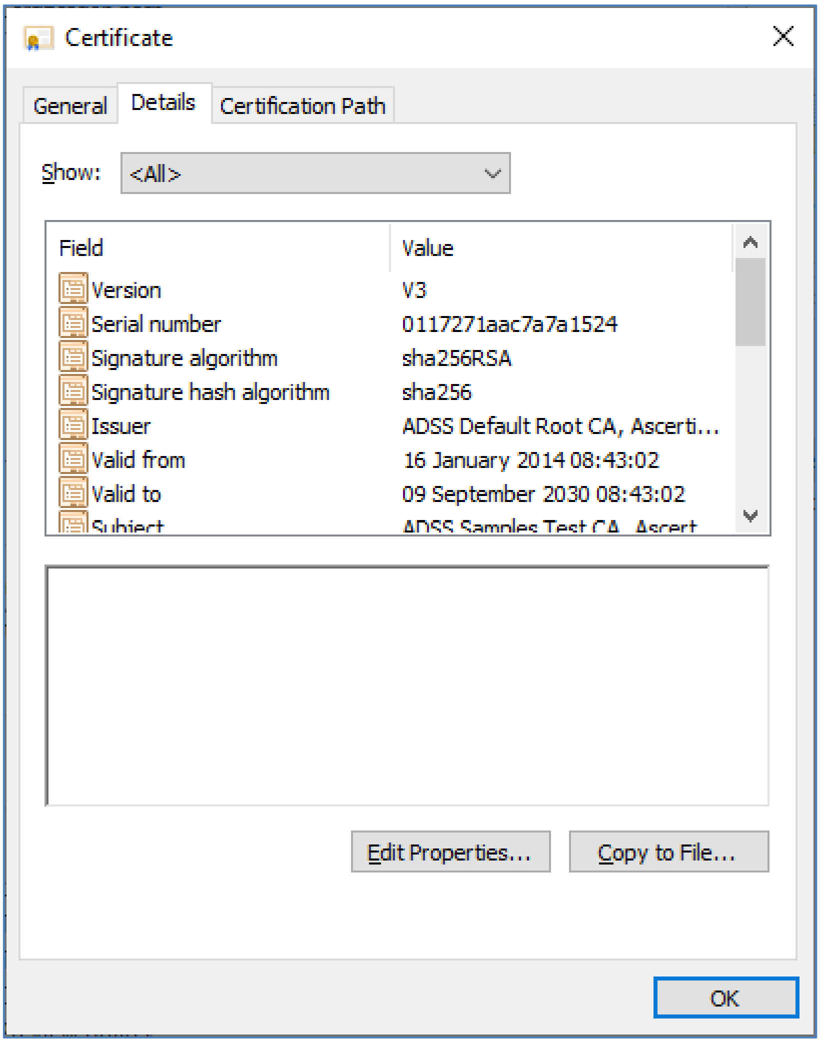
In the [installation_dir]/setup/certs directory there are two files with the name ***web-ra-default-admin.cer*** and ***web-ra-default-admin.pfx***. TLS certificate is installed, but root certificates are not validated by the machine. To validate it, root certificate needs to be imported in the certificate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

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



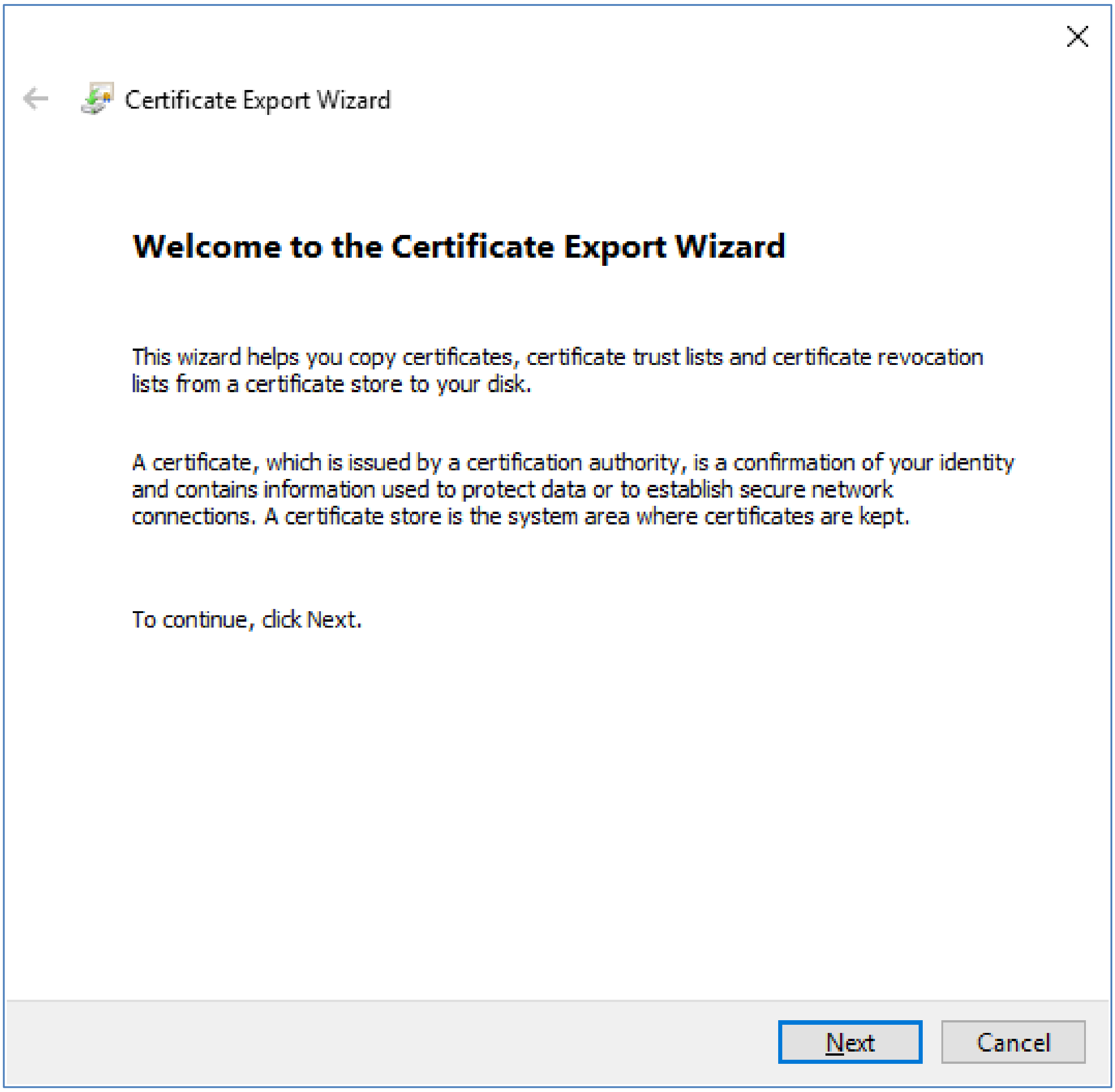
This certificate is OK.

Select the **Certification Path** tab from the top. Default 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.



Field	Value
Version	V3
Serial number	0117271aac7a7a1524
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADSS Default Root CA, Ascerti...
Valid from	16 January 2014 08:43:02
Valid to	09 September 2030 08:43:02
Subject	ADSS Samples Test CA, Ascert

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



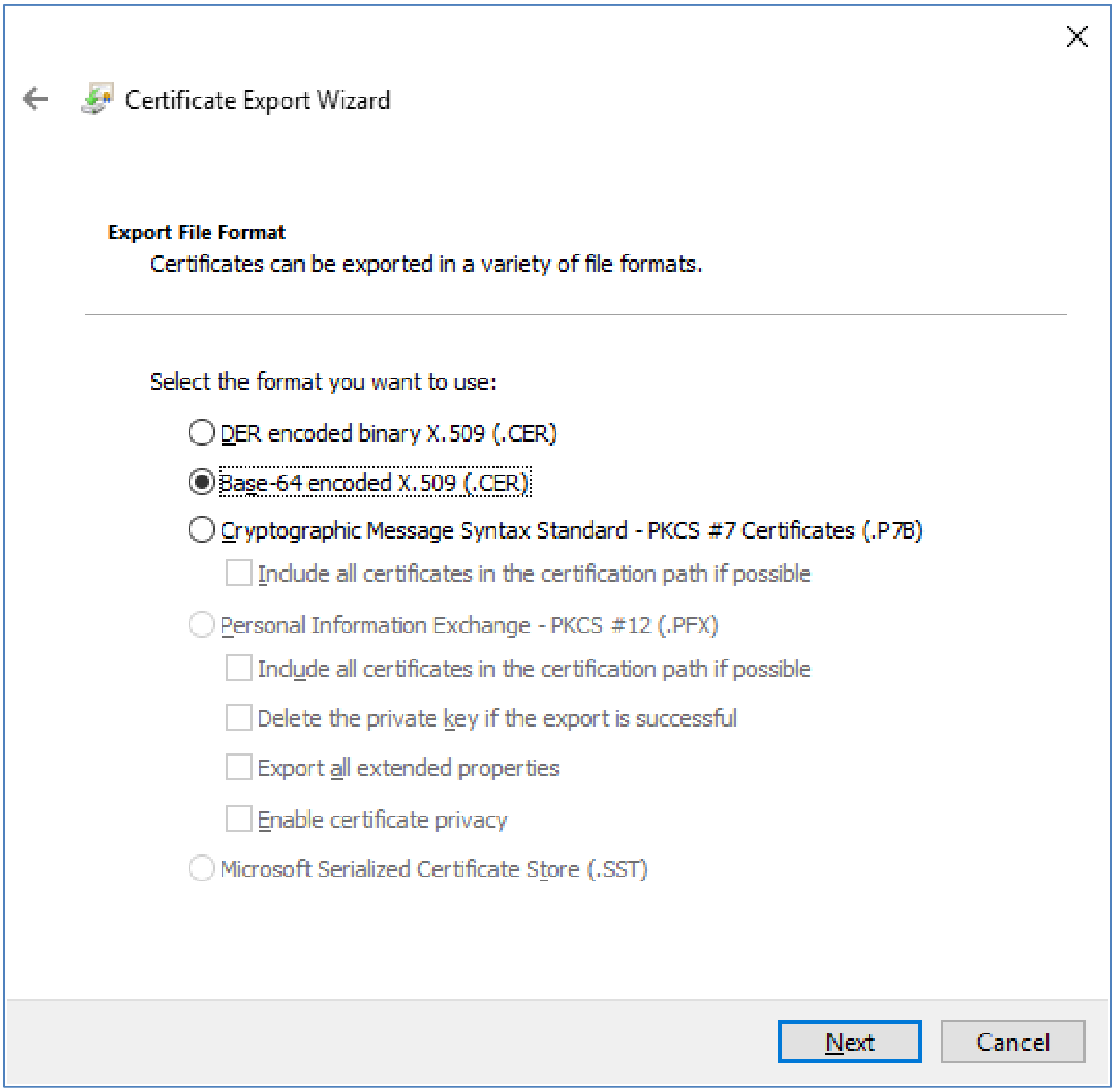
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Click **Next**



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

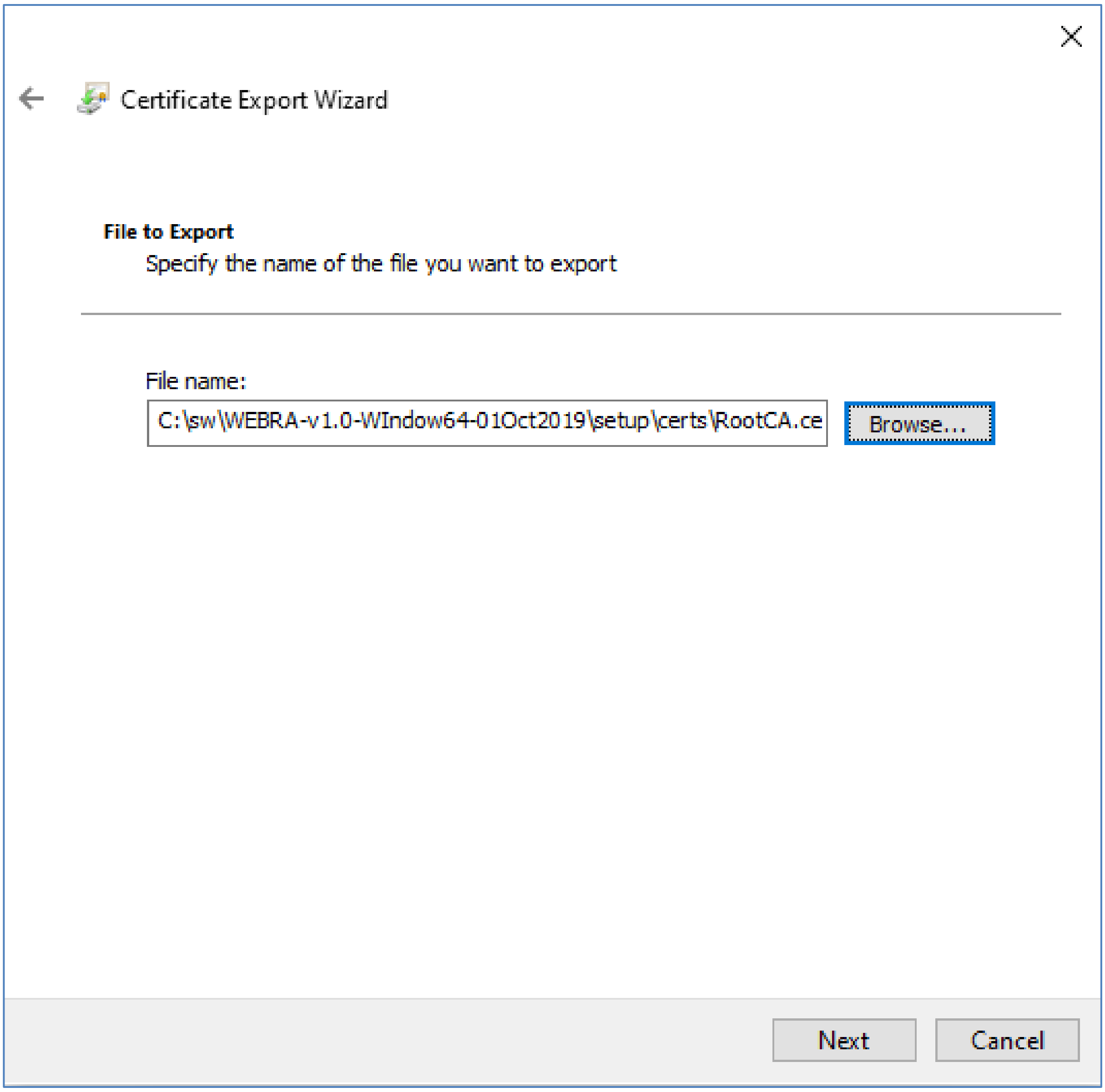
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

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



Certificate Export Wizard

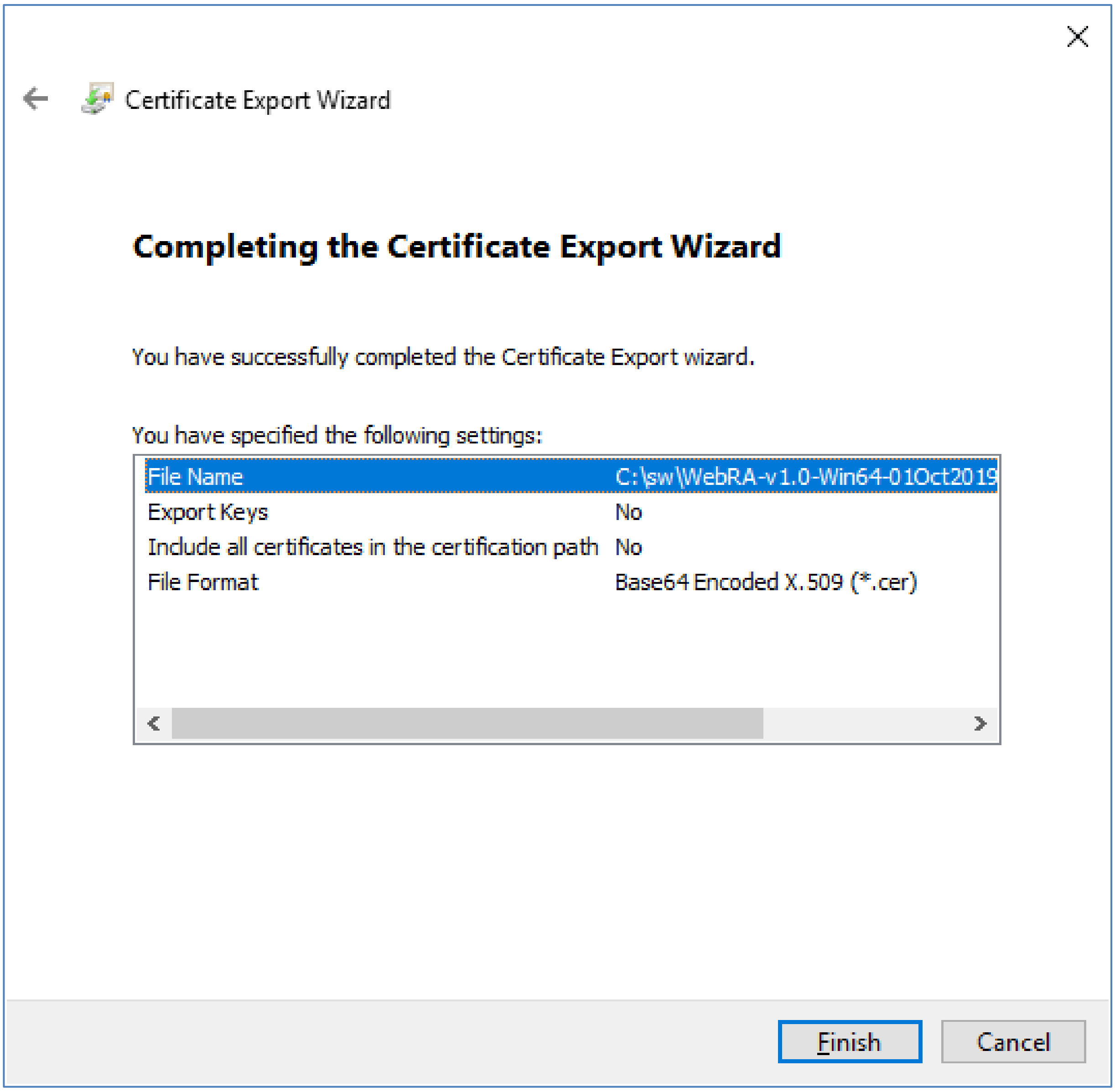
File to Export

Specify the name of the file you want to export

File name:

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

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



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

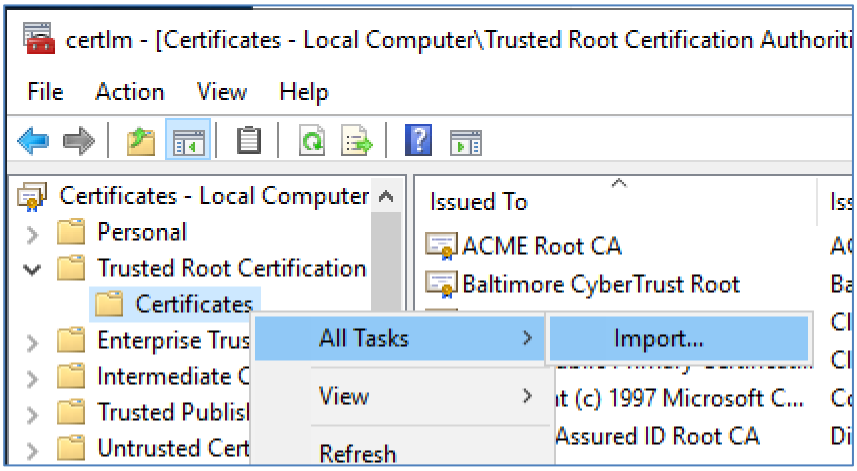
You have specified the following settings:

File Name	C:\sw\WebRA-v1.0-Win64-01Oct2019
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

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

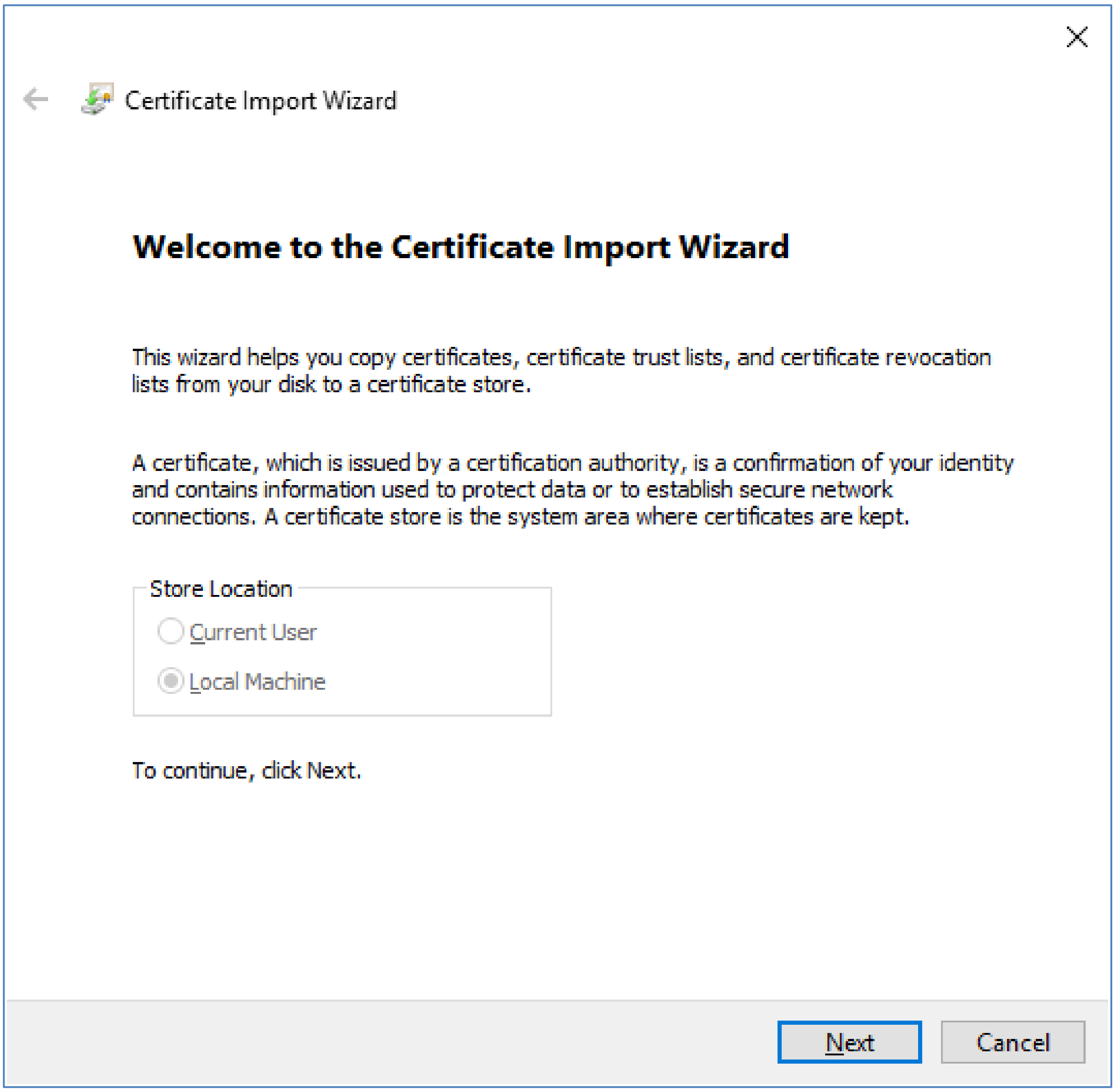
6.3 Importing Root and Intermediate Certificates

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.



certlm - [Certificates - Local Computer\Trusted Root Certification Authoriti
File Action View Help
Certificates - Local Computer
Personal
Trusted Root Certification
Certificates
Enterprise Trus
Intermediate C
Trusted Publisl
Untrusted Cert
All Tasks
View
Refresh
Import...
Issued To
Iss
ACME Root CA
Baltimore CyberTrust Root
it (c) 1997 Microsoft C...
Assured ID Root CA

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



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

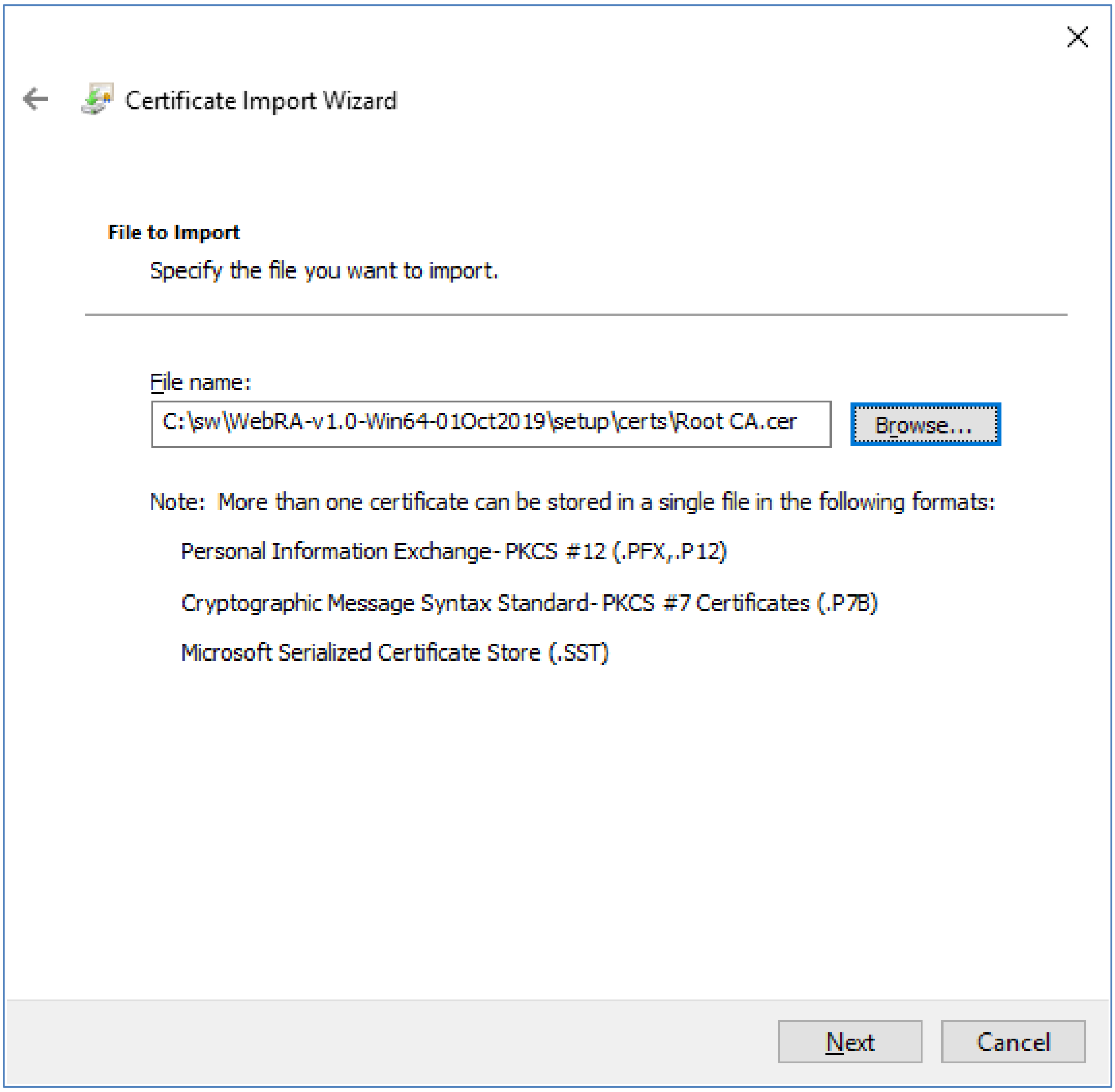
Store Location

○ Current User

● Local Machine

To continue, click Next.

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



File to Import

Specify the file you want to import.

File name:

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

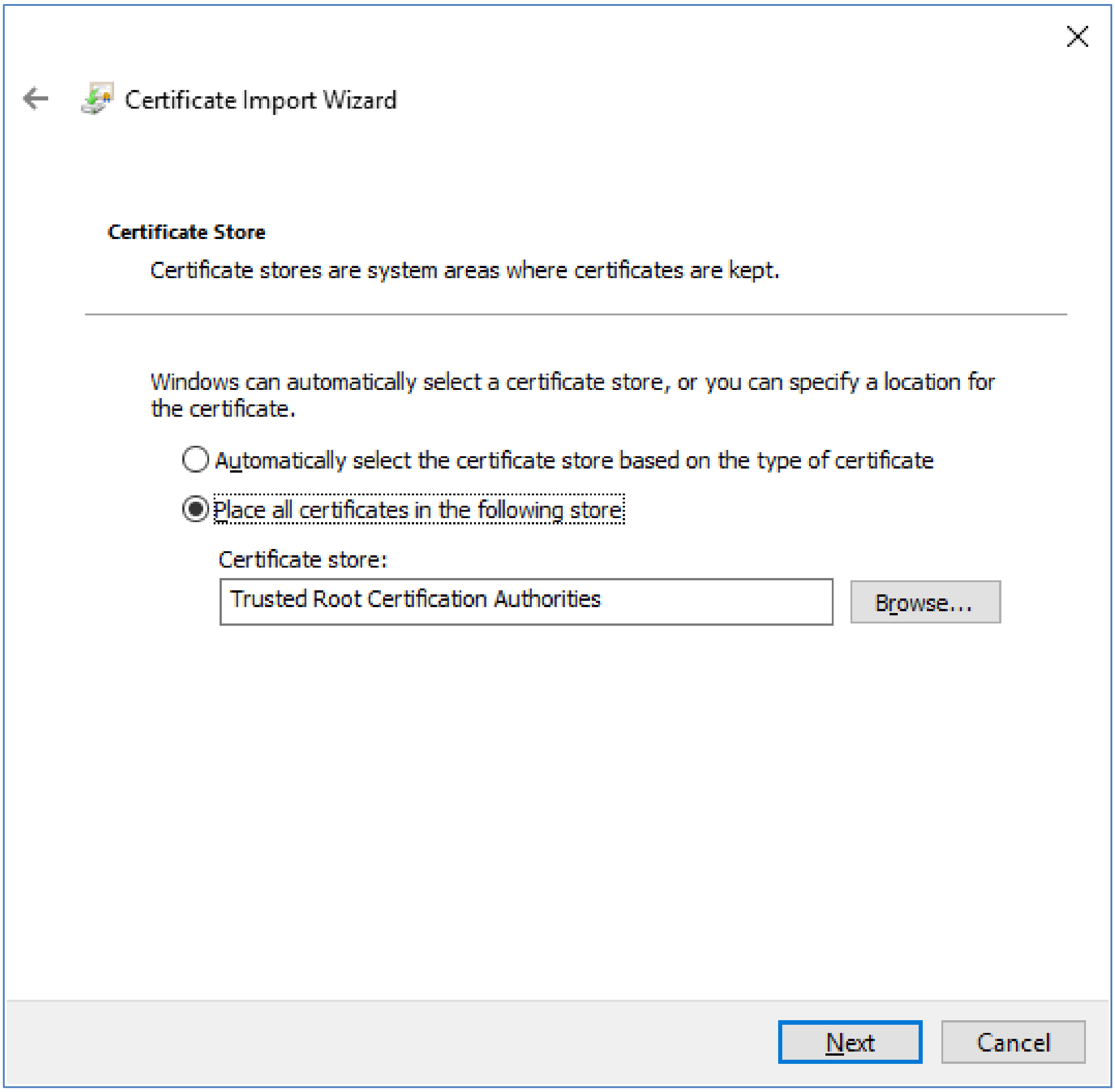
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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



Certificate Store

Certificate stores are system areas where certificates are kept.

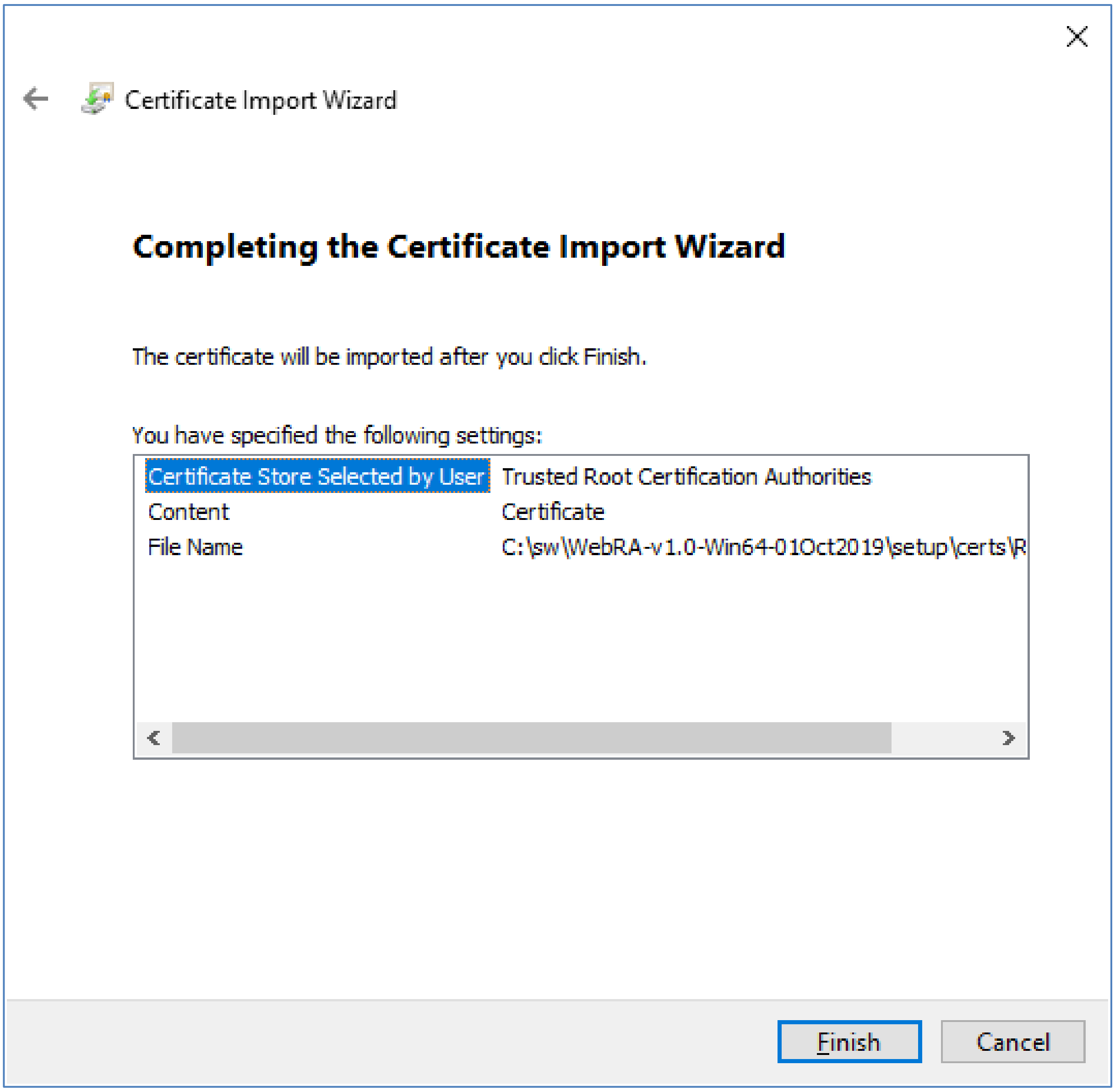
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Click **Next** to proceed.



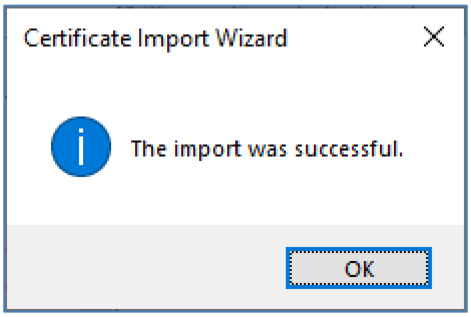
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\sw\WebRA-v1.0-Win64-01Oct2019\setup\certs\R

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



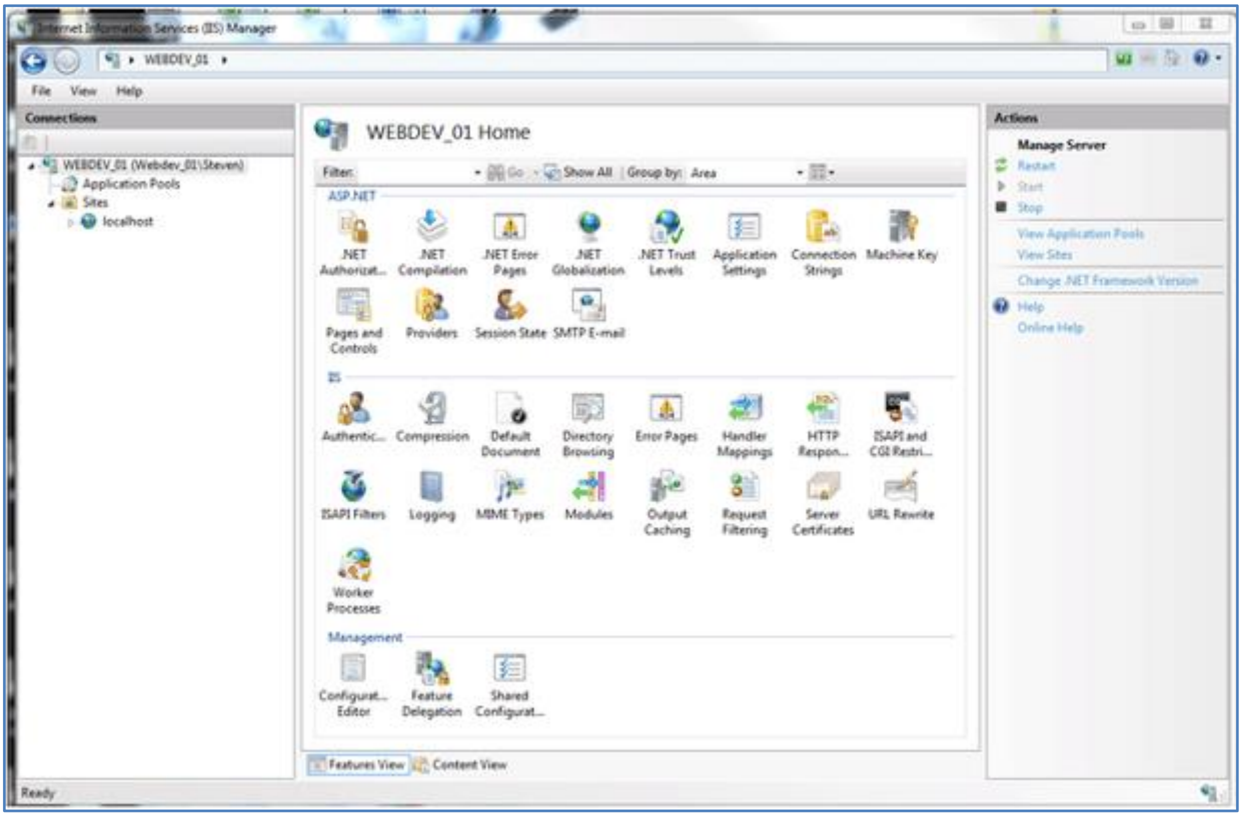
The import was successful.

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

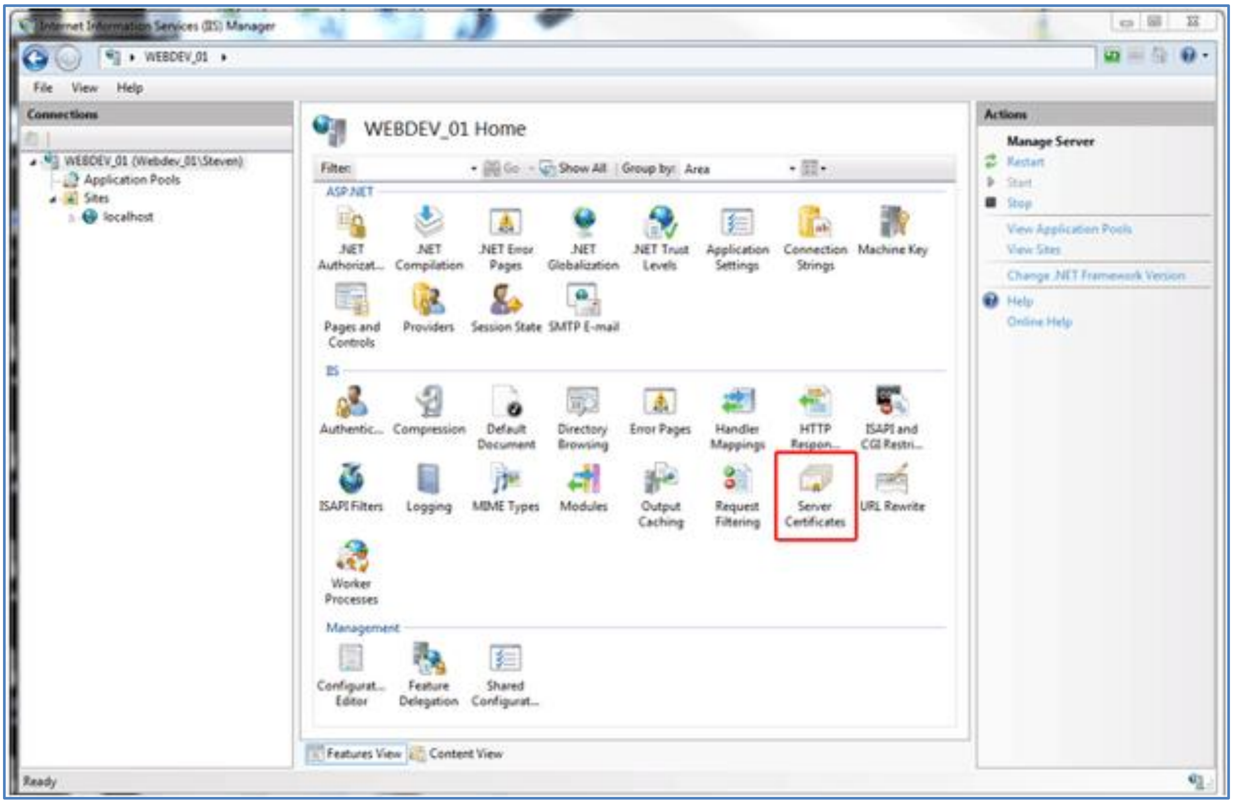
If you want to deploy the application for testing purpose you may want to use a self-signed certificate for proof of concept.

6.4 Generate a Self -Signed Certificate

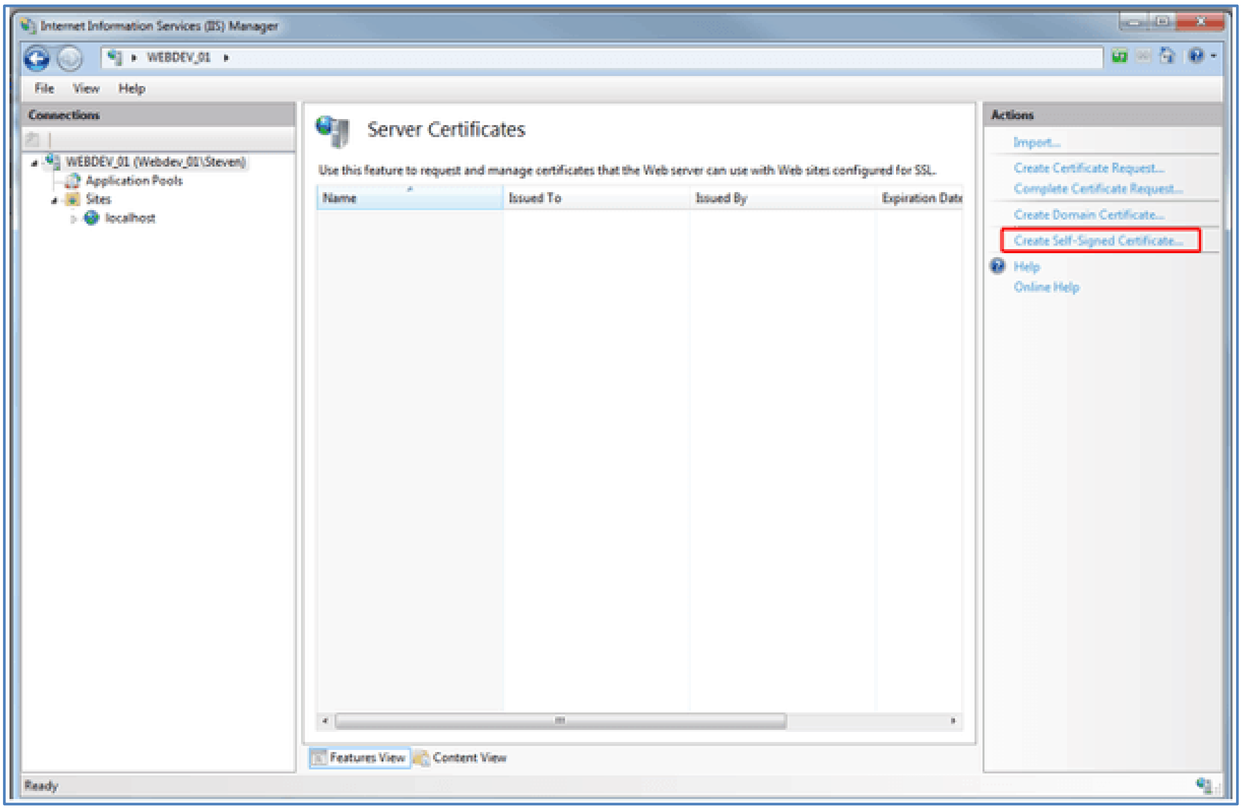
For testing purpose or a proof of concepts, mostly a self-signed certificate will be needed. It is easy to create a self-signed certificate with IIS. Launch the IIS



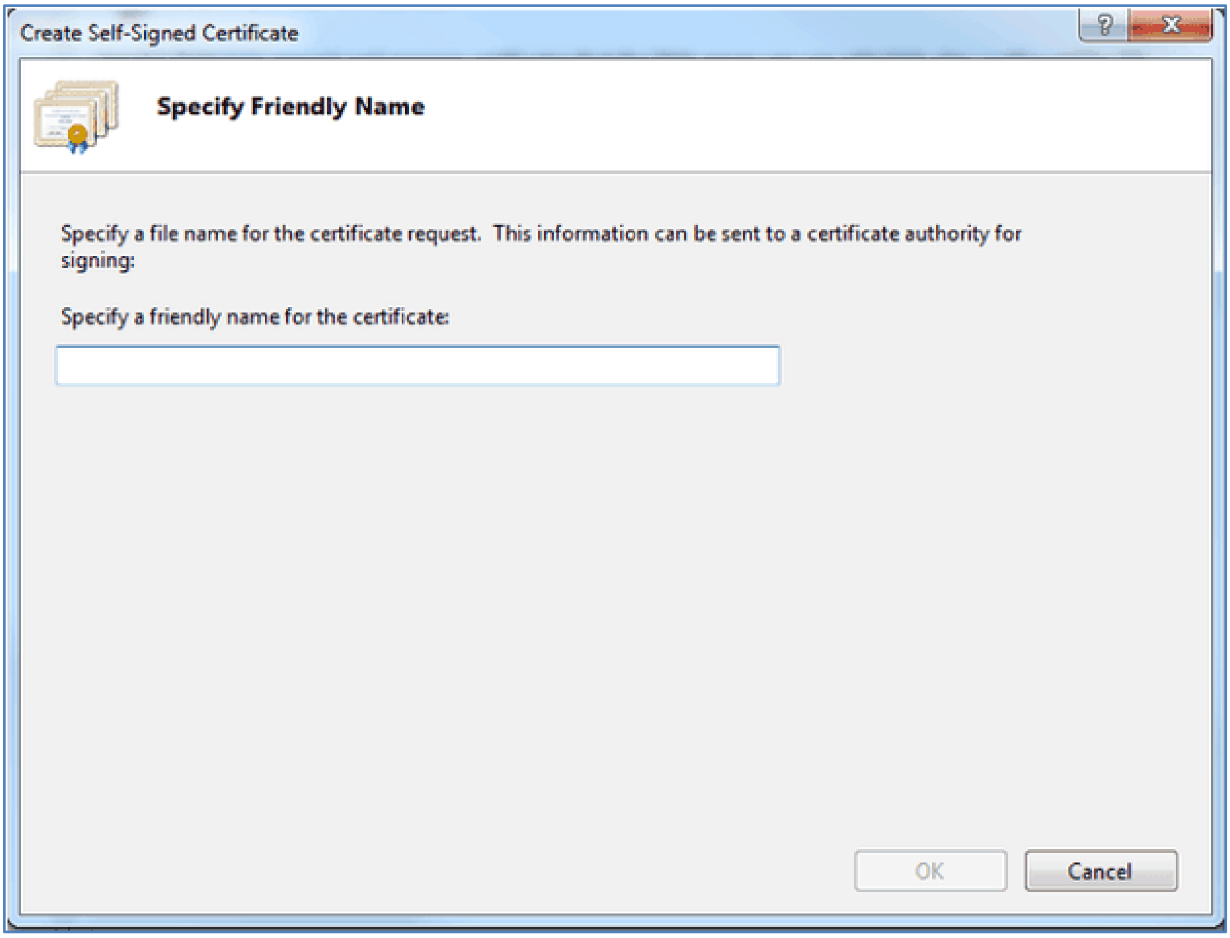
Click the **server name** from the left menu of **connections**



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


Internet Information Services (IIS) Manager
WEBDEV_01
File View Help
Connections
WEBDEV_01 (Webdev_01\Steven)
Application Pools
Sites
localhost
Server Certificates
Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.
Name
Issued To
Issued By
Expiration Date
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help
Ready

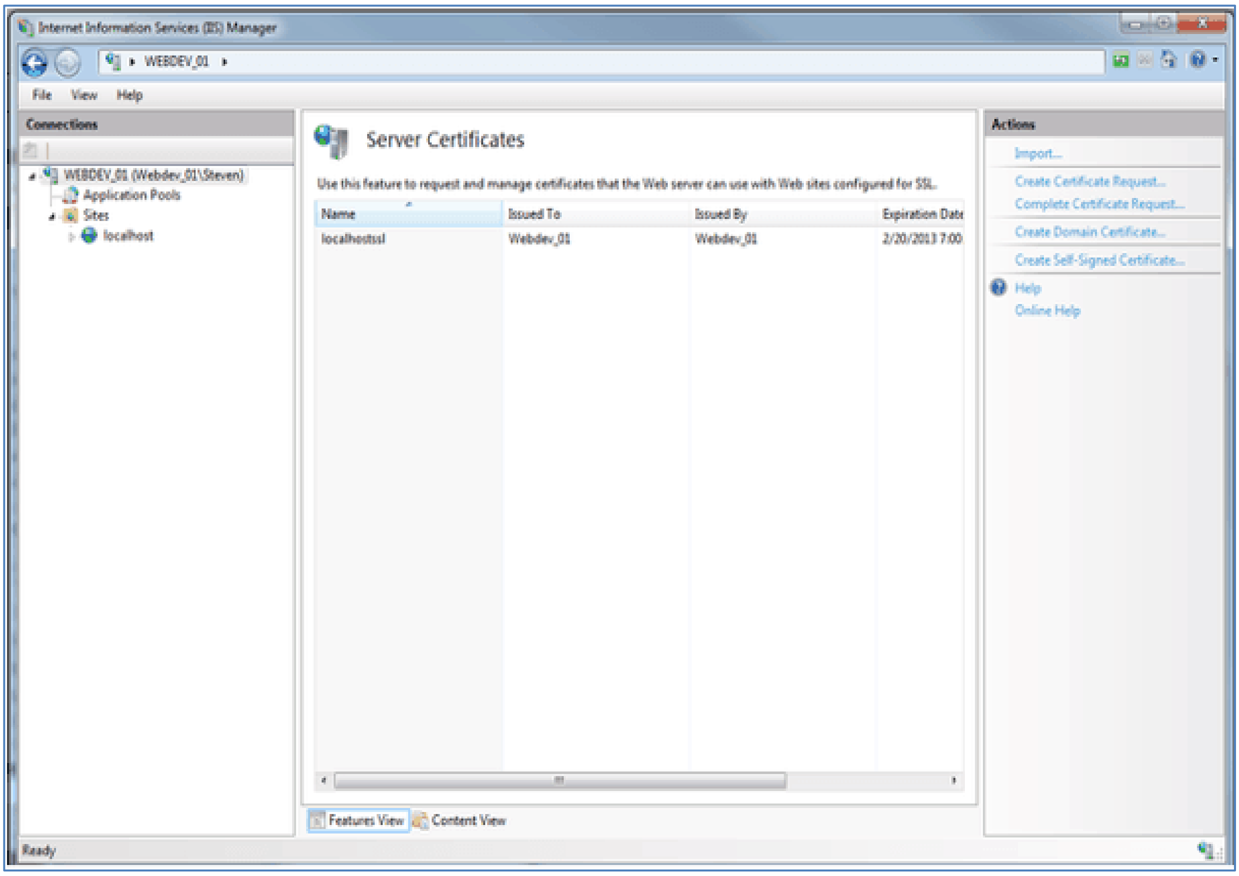
Click **Create Self-Signed Certificate**... under the right **Actions** column



Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

Provide a meaningful name and press **OK**


Internet Information Services (IIS) Manager
WEBDEV_01
File
View
Help
Connections
WEBDEV_01 (Webdev_01\Steven)
Application Pools
Sites
localhost
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help
Features View
Content View
Ready

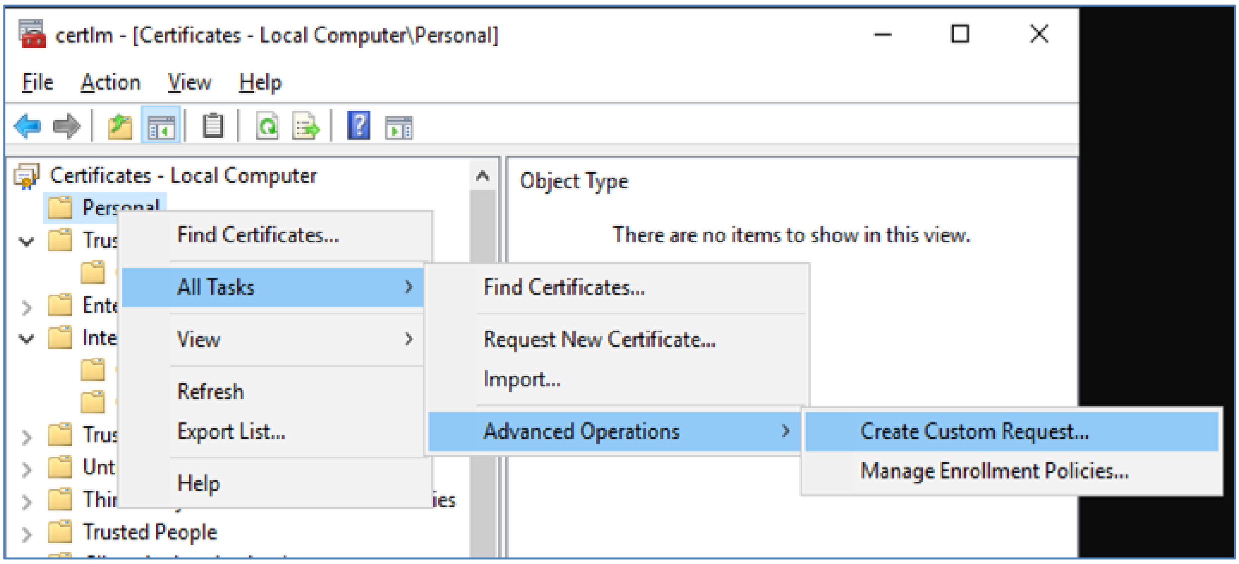
Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date
localhostssl	Webdev_01	Webdev_01	2/20/2013 7:00

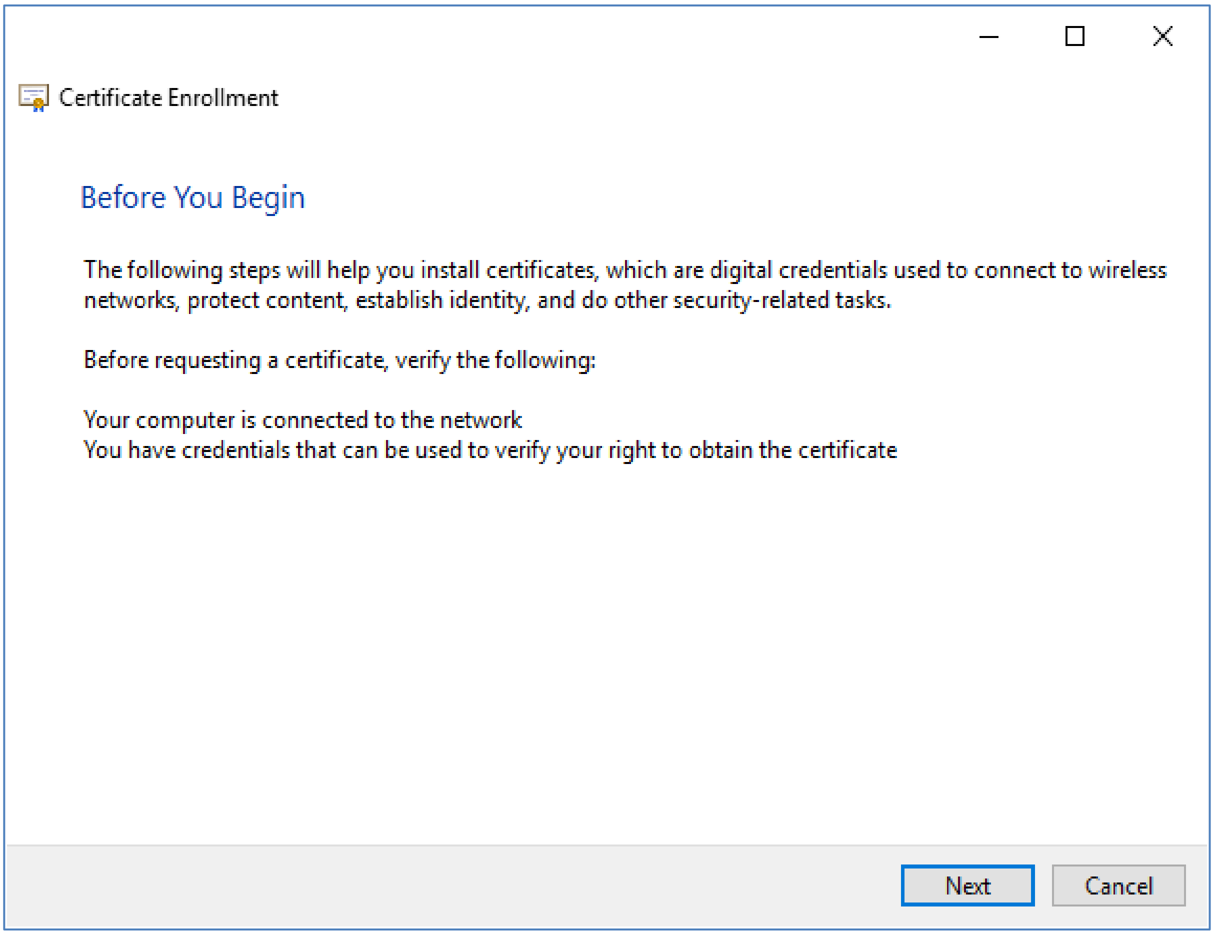
Now you have an SSL certificate that is self-signed and has a validity of 1 year. You can select this certificate for creation of HTTPS binding for test and proof of concepts purposes.

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.



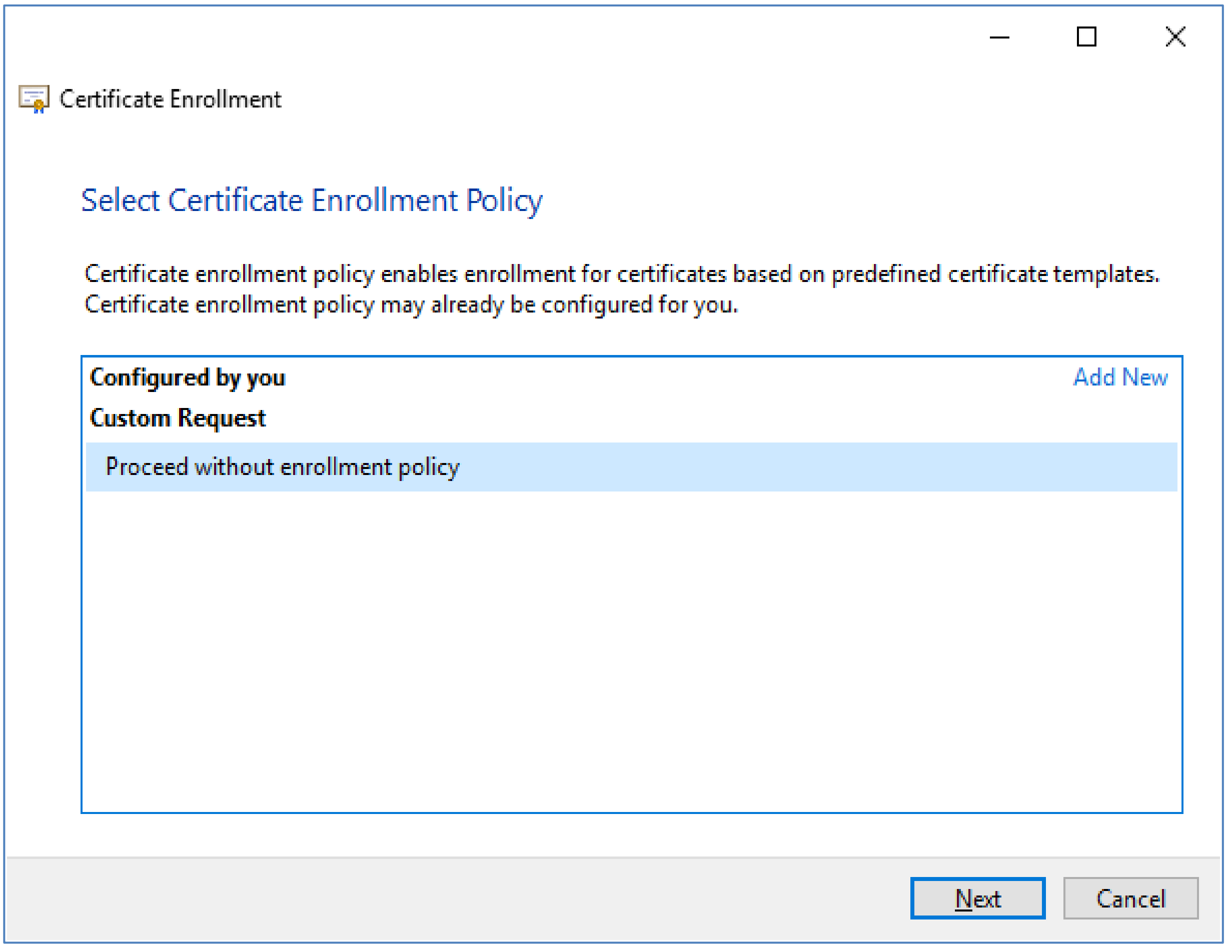
Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

Press **Next** to proceed.



Select Certificate Enrollment Policy

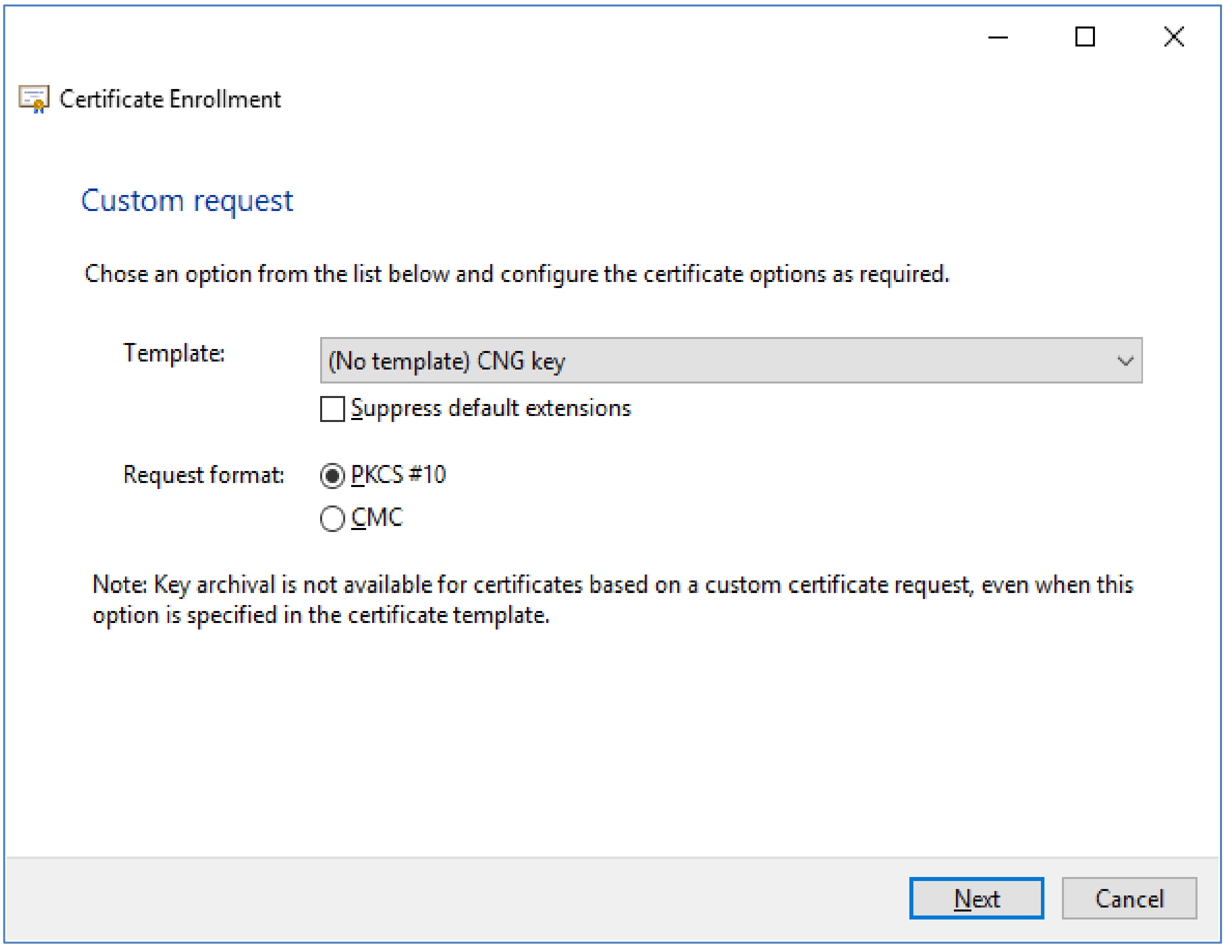
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you

Custom Request

Proceed without enrollment policy

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



Certificate Enrollment

Custom request

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

Template: (No template) CNG key

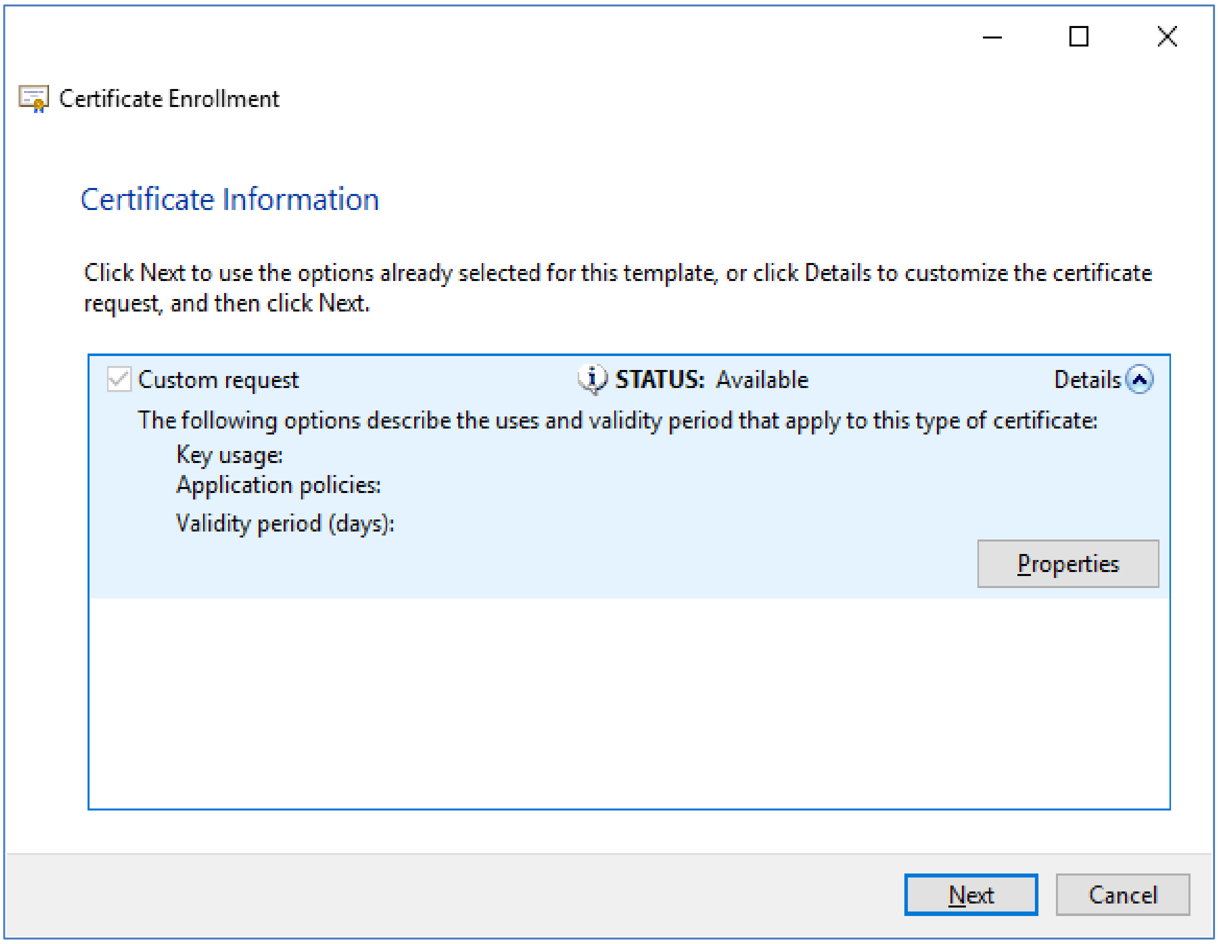
□ Suppress default extensions

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.

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



Certificate Enrollment

Certificate Information

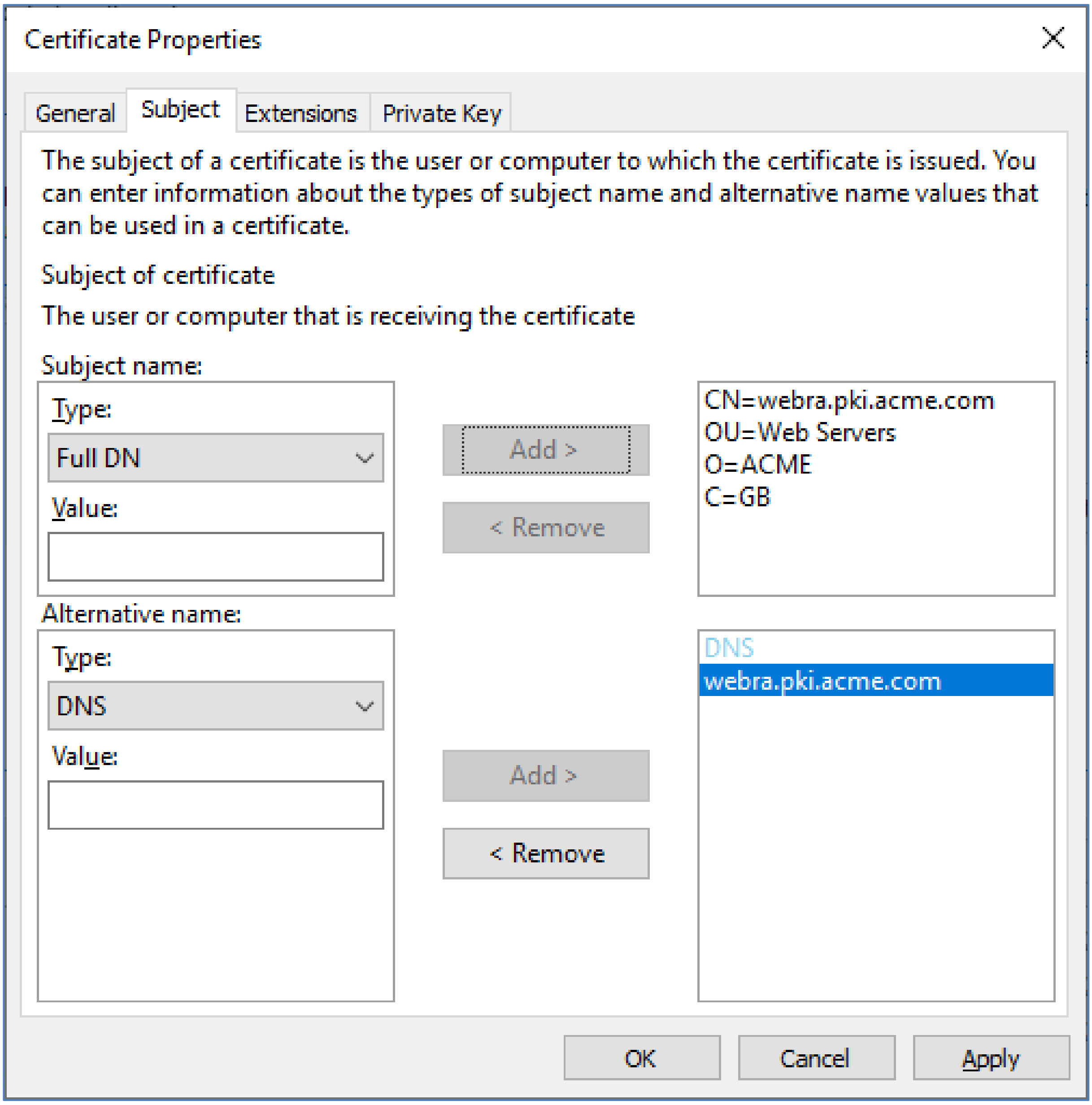
Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☑ 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):

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



Certificate 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

Value:

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

Alternative name:

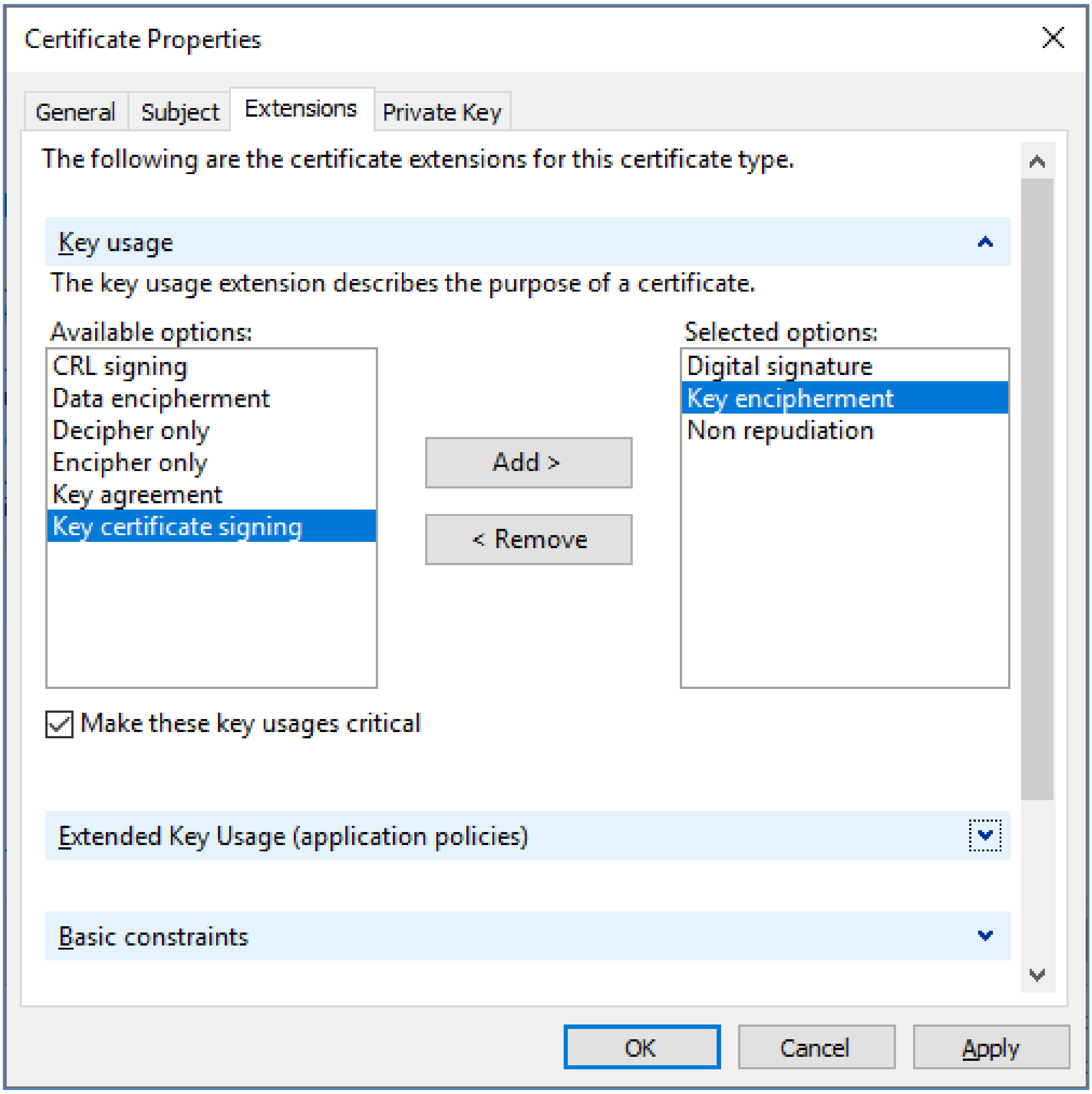
Type: DNS

Value:

DNS
webra.pki.acme.com

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.



Certificate Properties

General | Subject | Extensions | Private Key

The following are the certificate extensions for this certificate type.

Key usage

The key usage extension describes the purpose of a certificate.

Available options:

- CRL signing
- Data encipherment
- Decipher only
- Encipher only
- Key agreement
- Key certificate signing

Selected options:

- Digital signature
- Key encipherment
- Non repudiation

☑ Make these key usages critical

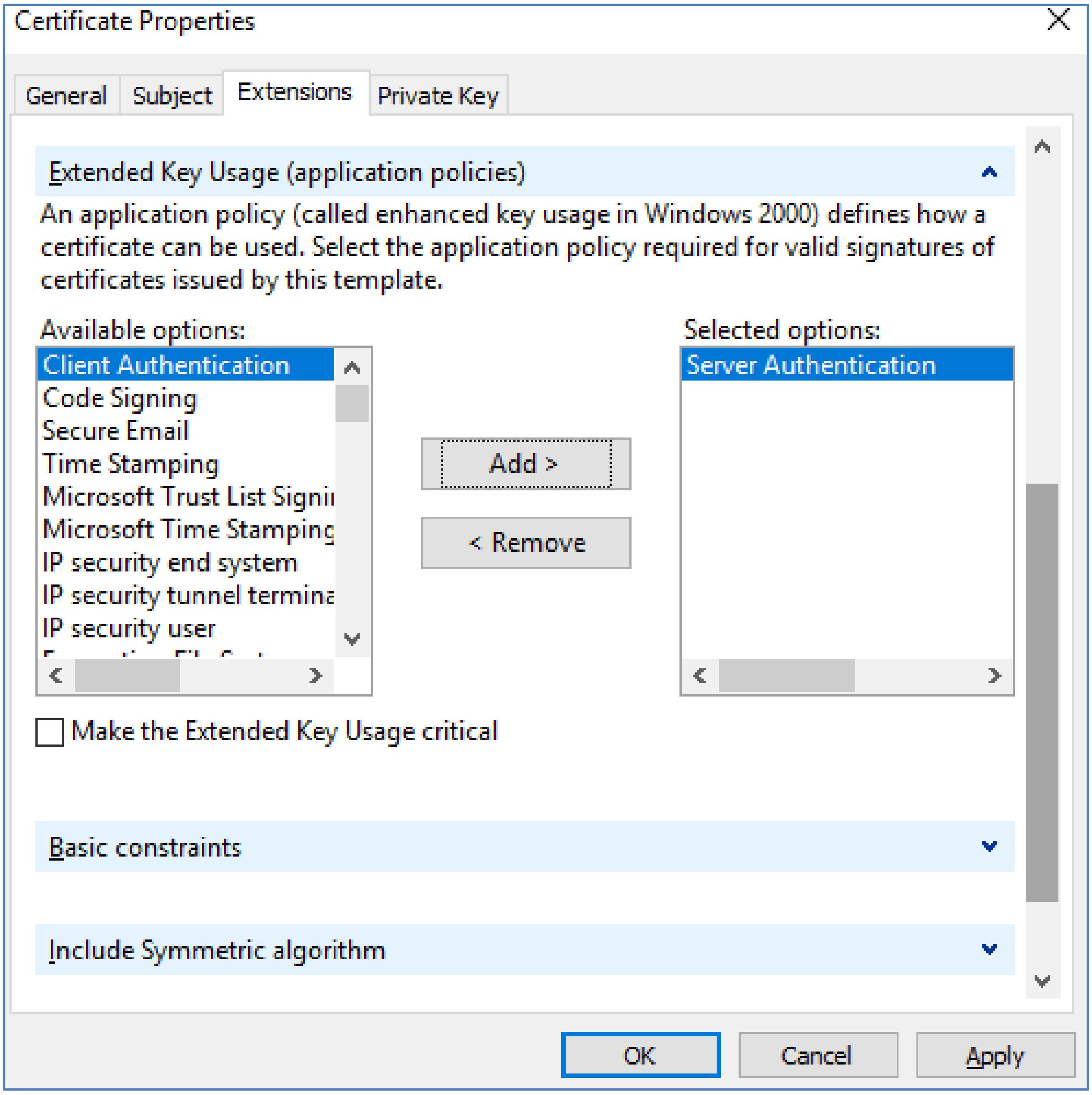
Extended Key Usage (application policies)

Basic constraints

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.



Extended Key Usage (application policies)

An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Available options:

- Client Authentication
- Code Signing
- Secure Email
- Time Stamping
- Microsoft Trust List Signi
- Microsoft Time Stamping
- IP security end system
- IP security tunnel termina
- IP security user

Selected options:

- Server Authentication

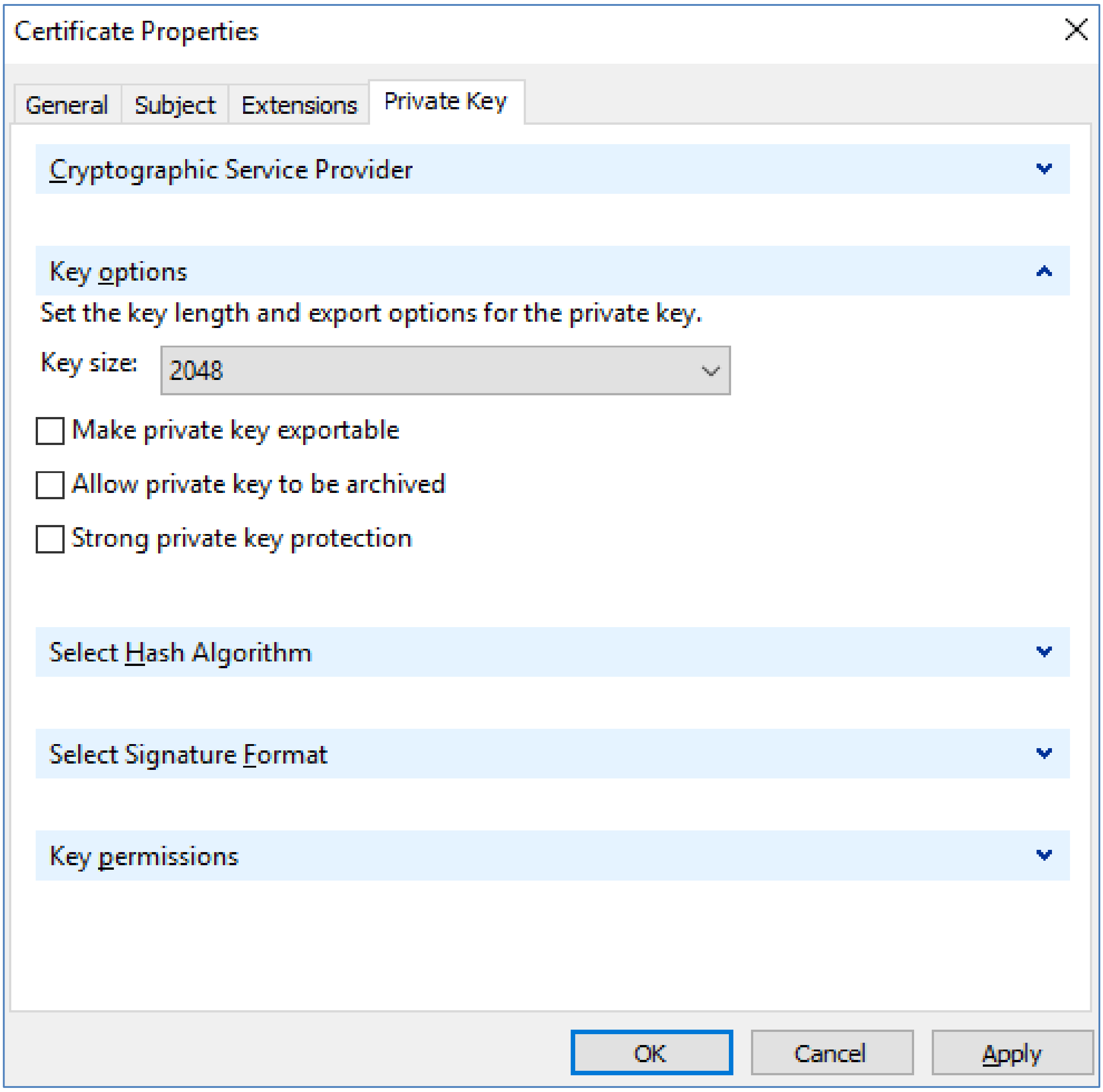
□ Make the Extended Key Usage critical

Basic constraints

Include Symmetric algorithm

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

- Server Authentication



Certificate Properties

Key options

Set the key length and export options for the private key.

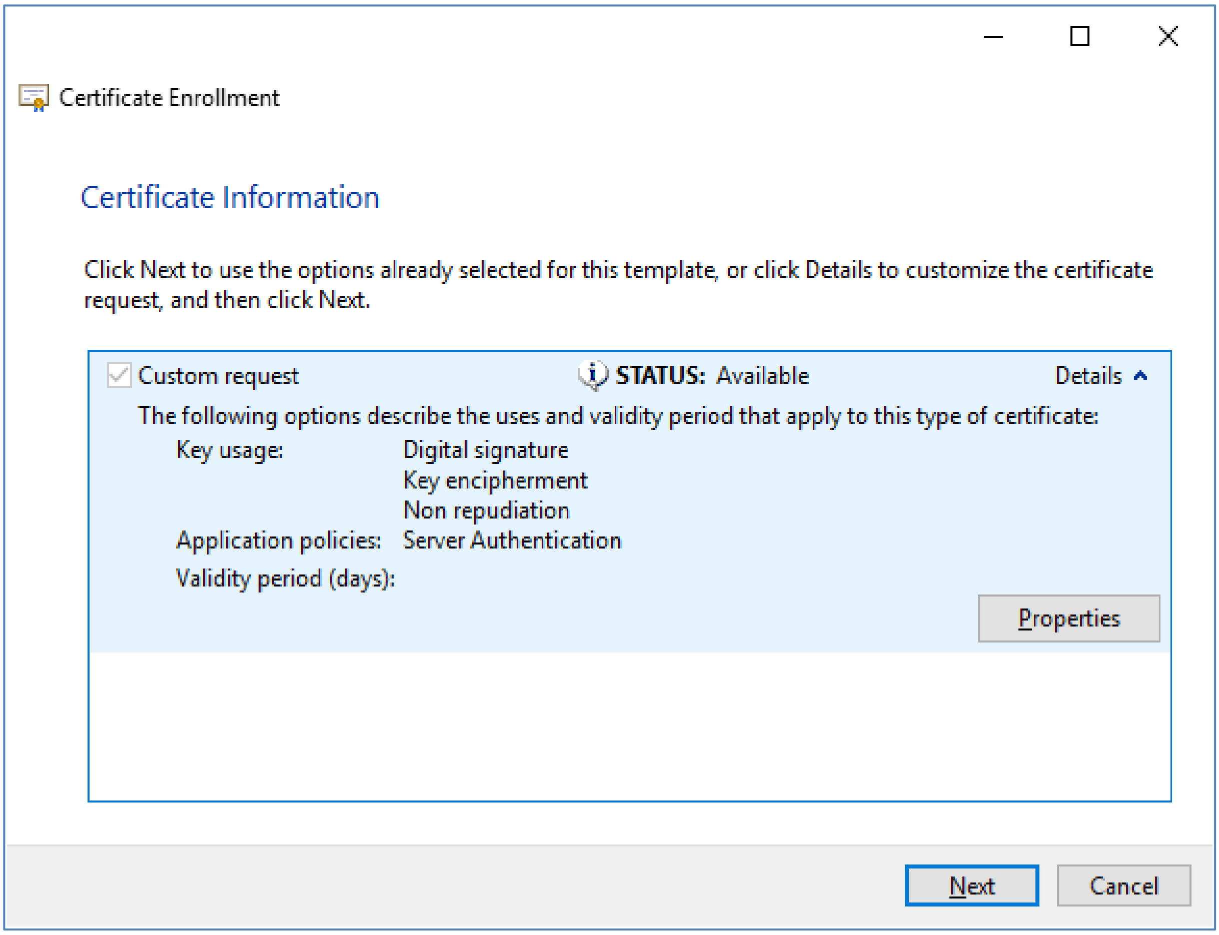
Key size: 2048

☐ Make private key exportable

☐ Allow private key to be archived

☐ Strong private key protection

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



Certificate Information

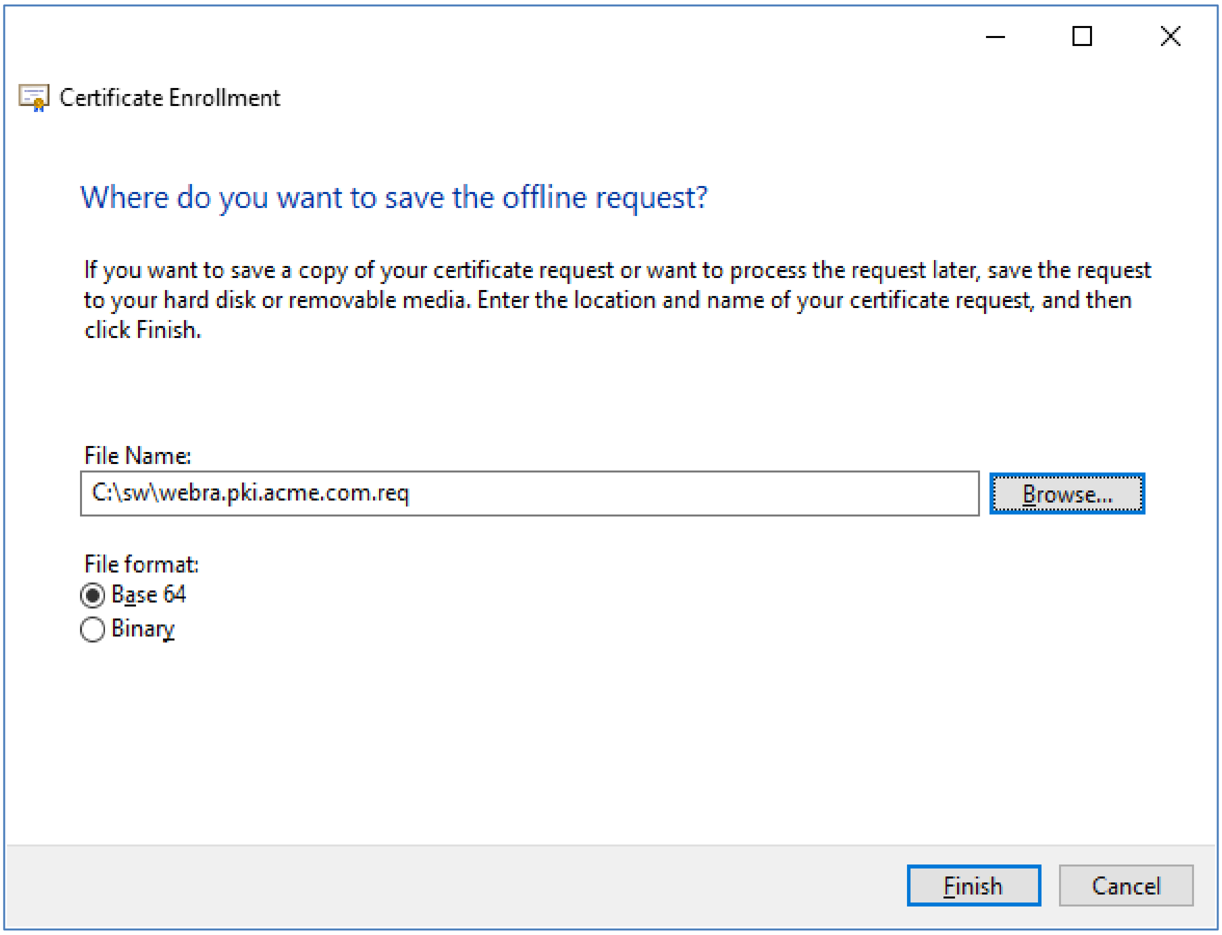
Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☑ 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):	

Press **Next** to proceed.



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

File format:
● Base 64
○ Binary

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 ***