ADSS Web RA Server 2.9.7

Installation

Guide

ASCERTIA LTD

JUNE 2025

Document Version- 1.0.3

© Ascertia Limited. All rights reserved.

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

Table of Contents

1 Introduction

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

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

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

1.1 Scope

This manual describes how to install ADSS Web RA Server.

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

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

1.2 Intended Readership

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

1.3 Technical Support

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

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

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

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

1.4 Glossary

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

2 System Requirements

System Requirements includes hardware and software requirements both.

2.1 Hardware Prerequisites

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

2.2 Software Prerequisites

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

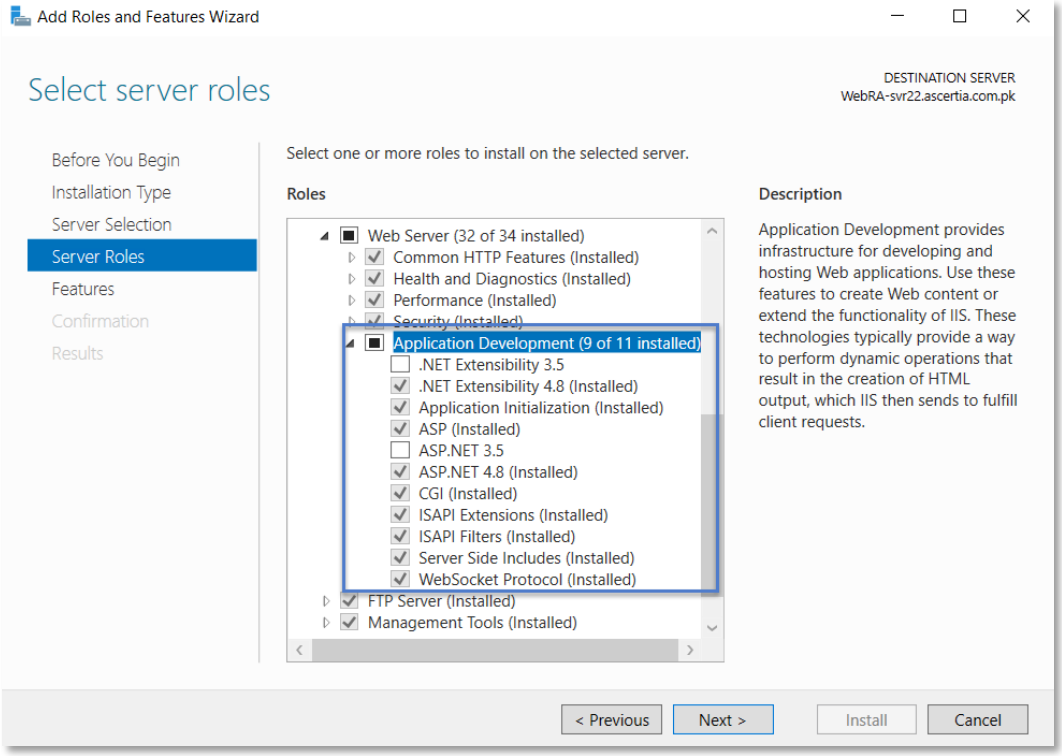
Database Server	- Follow this link to view details about Database Server: https://manuals.ascertia.com/WebRA/ADSS-WebRA-Server-Platform-Support.pdf
Web Brower **(for end-users and administrators)**	- Follow this link to view details about Web Browsers: https://manuals.ascertia.com/WebRA/ADSS-WebRA-Server-Platform-Support.pdf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

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

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

2.3 Application Development feature in IIS

Enable the following features in IIS on the deployment machine:



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WebRA-svr22.ascertia.com.pk

Select one or more roles to install on the selected server.

Roles

- ■ Web Server (32 of 34 installed)
  - ☑ Common HTTP Features (Installed)
  - ☑ Health and Diagnostics (Installed)
  - ☑ Performance (Installed)
  - ☑ Security (Installed)
  - ■ Application Development (9 of 11 installed)
    - □ .NET Extensibility 3.5
    - ☑ .NET Extensibility 4.8 (Installed)
    - ☑ Application Initialization (Installed)
    - ☑ ASP (Installed)
    - □ ASP.NET 3.5
    - ☑ ASP.NET 4.8 (Installed)
    - ☑ CGI (Installed)
    - ☑ ISAPI Extensions (Installed)
    - ☑ ISAPI Filters (Installed)
    - ☑ Server Side Includes (Installed)
    - ☑ WebSocket Protocol (Installed)
  - ☑ FTP Server (Installed)
  - ☑ Management Tools (Installed)

Description

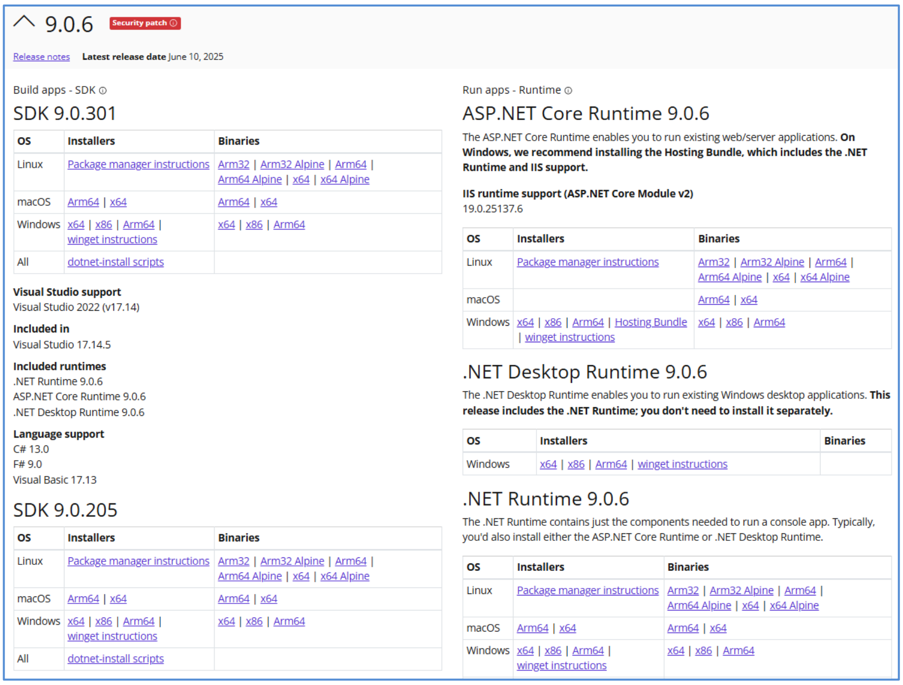
Application Development provides infrastructure for developing and hosting Web applications. Use these features to create Web content or extend the functionality of IIS. These technologies typically provide a way to perform dynamic operations that result in the creation of HTML output, which IIS then sends to fulfill client requests.

2.4 Microsoft .Net Core 9.0.6. Runtime & Hosting Bundle

2.4.1 Download the latest version of Microsoft .Net Core i.e. Microsoft .Net Core 9.0.6. Runtime and Hosting Bundle from the following link:

Microsoft .Net Core 9.0. Runtime & Hosting Bundle

2.4.2 Download the Hosting Bundle installer.



9.0.6 Security patch

Release notes **Latest release date** June 10, 2025

Build apps - SDK

SDK 9.0.301

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

Visual Studio support
Visual Studio 2022 (v17.14)

Included in
Visual Studio 17.14.5

Included runtimes
.NET Runtime 9.0.6
ASP.NET Core Runtime 9.0.6
.NET Desktop Runtime 9.0.6

Language support
C# 13.0
F# 9.0
Visual Basic 17.13

SDK 9.0.205

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

Run apps - Runtime

ASP.NET Core Runtime 9.0.6

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

IIS runtime support (ASP.NET Core Module v2)
19.0.25137.6

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

.NET Desktop Runtime 9.0.6

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

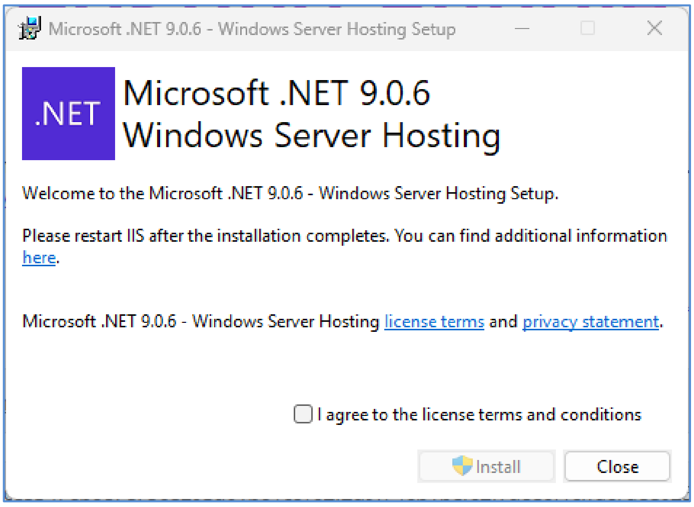
OS	Installers	Binaries
Windows	x64 | x86 | Arm64 | winget instructions	

.NET Runtime 9.0.6

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

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

2.4.1. Once downloaded, execute the installer by executing **dotnet-hosting-9.0.6-win.exe**



Microsoft .NET 9.0.6 - Windows Server Hosting Setup

Microsoft .NET 9.0.6
Windows Server Hosting

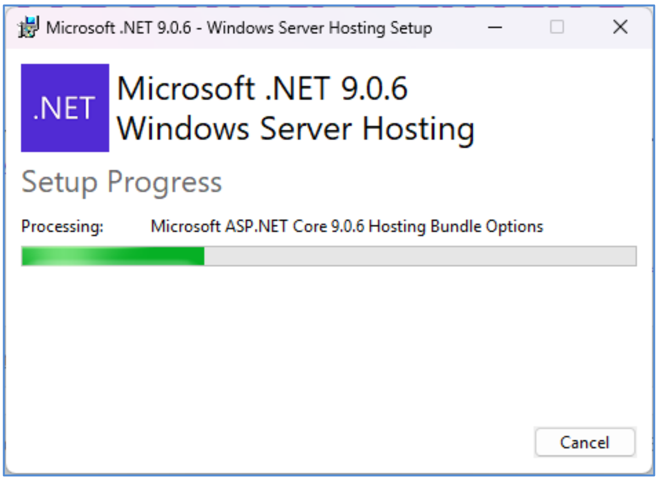
Welcome to the Microsoft .NET 9.0.6 - Windows Server Hosting Setup.

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

Microsoft .NET 9.0.6 - Windows Server Hosting license terms and privacy statement.

☐ I agree to the license terms and conditions

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

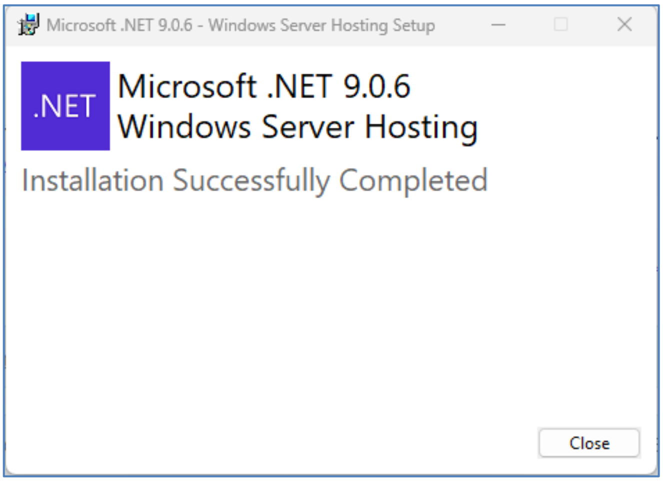


Microsoft .NET 9.0.6 - Windows Server Hosting Setup

Microsoft .NET 9.0.6
Windows Server Hosting

Setup Progress

Processing: Microsoft ASP.NET Core 9.0.6 Hosting Bundle Options



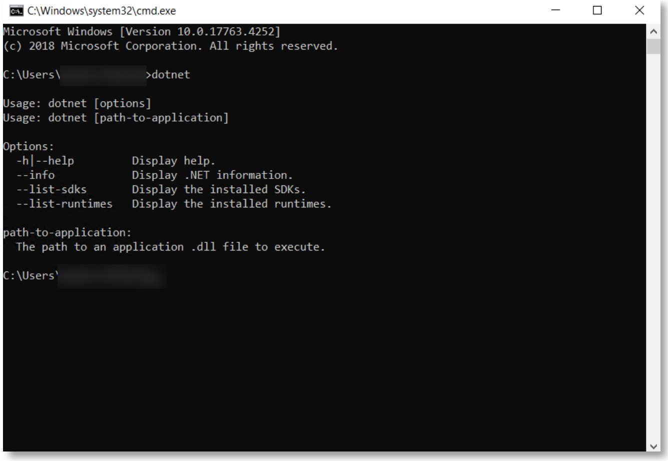
Microsoft .NET 9.0.6 - Windows Server Hosting Setup

Microsoft .NET 9.0.6
Windows Server Hosting

Installation Successfully Completed

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

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



C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.4252]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>dotnet

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

Options:
  -h|--help         Display help.
  --info            Display .NET 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.

C:\Users\[redacted]
```

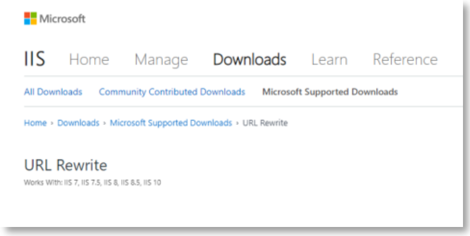
2.4.5. Now, restart your machine to apply these changes effectively.

2.5 Microsoft IIS URL Rewrite Module 2.1

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

Microsoft IIS URL Rewrite Module 2.1

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

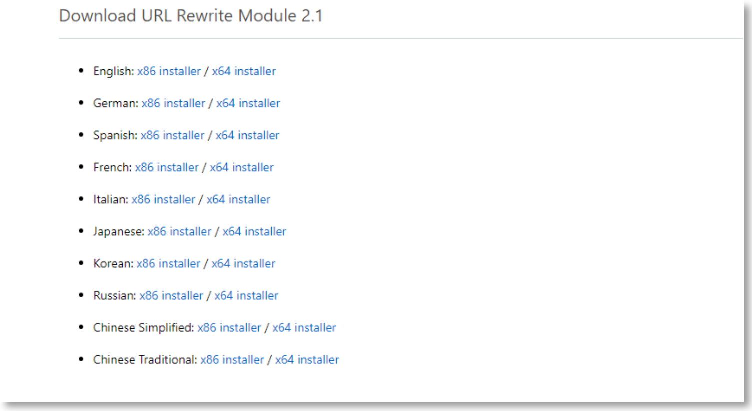


Microsoft
IIS
Home
Manage
Downloads
Learn
Reference
All Downloads
Community Contributed Downloads
Microsoft Supported Downloads
Home › Downloads › Microsoft Supported Downloads › URL Rewrite

URL Rewrite

Works With: IIS 7, IIS 7.5, IIS 8, IIS 8.5, IIS 10

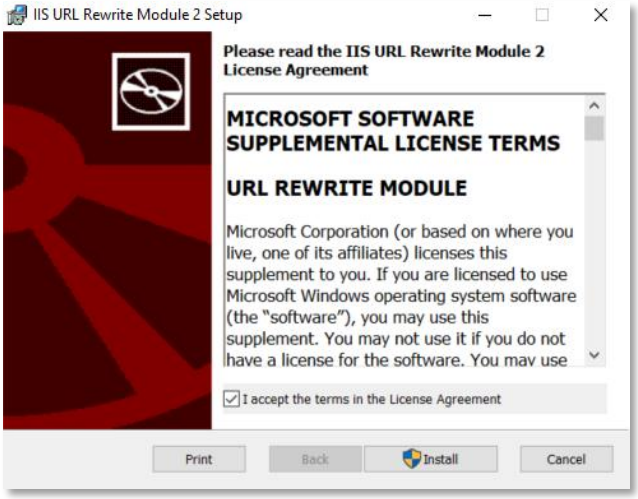
2.5.3. Scroll down to find a list of links available for download.



Download URL Rewrite Module 2.1

- English: 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

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



Please read the IIS URL Rewrite Module 2 License Agreement

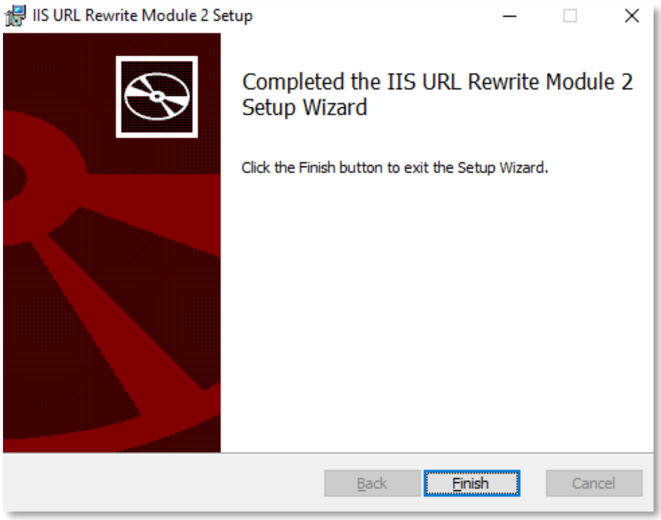
MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

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 mav use

☑ I accept the terms in the License Agreement

2.5.5. 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.

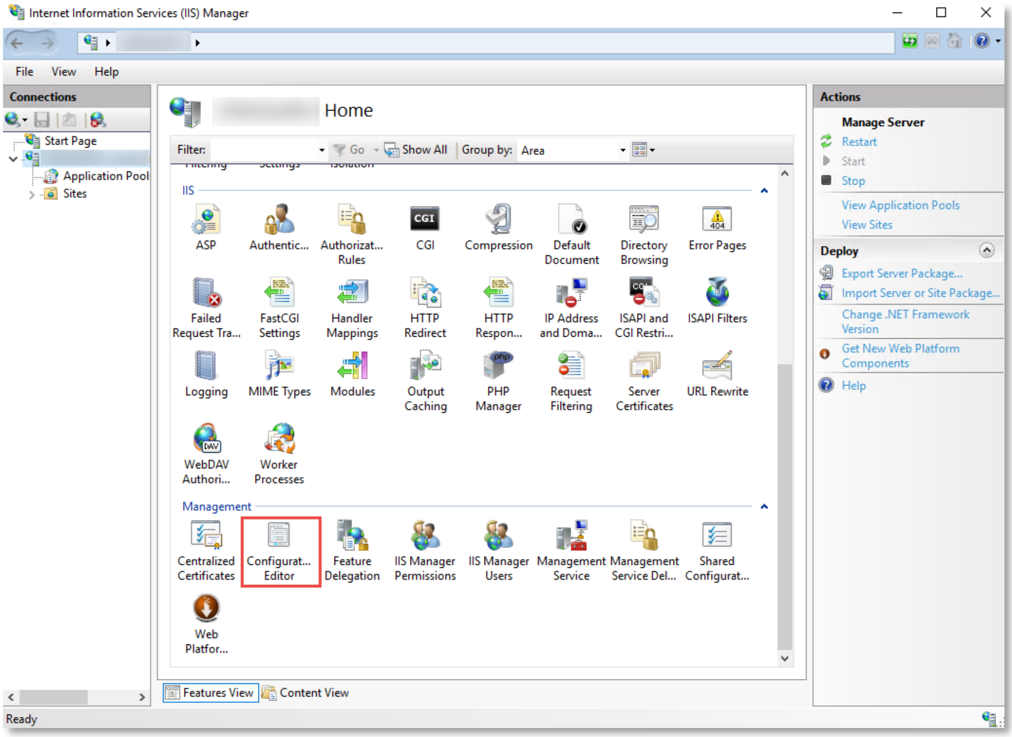
2.5.6. Click **Finish** once the installation process is complete.

2.6 Unlock system.webServer/serverRuntime section in IIS

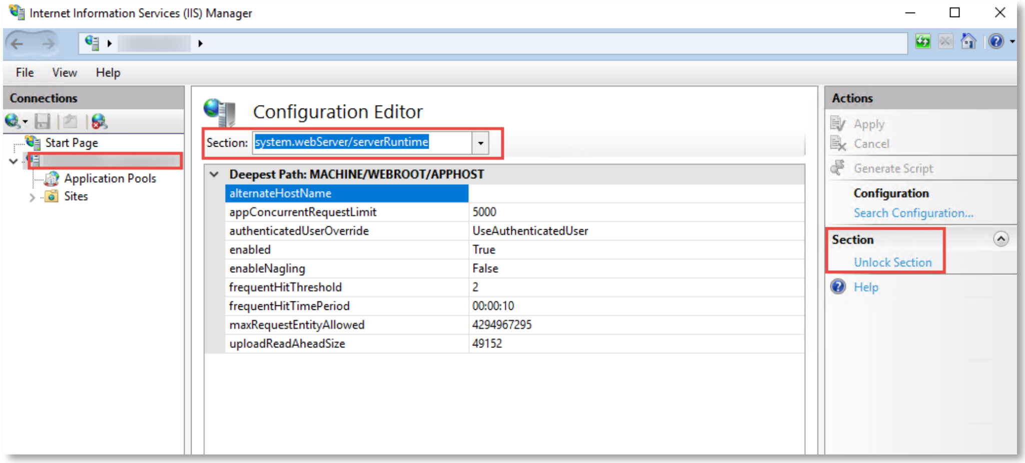
2.6.1. Launch the **IIS Manager**

2.6.2. Select **Server** from left panel

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



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



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

The installation process for prerequisites is complete.

2.7 SMTP Server

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

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

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

2.8 Database

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

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

3 Installation Modules

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

- **ADSS Web RA Admin**

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

- **ADSS Web RA Desktop Web**

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

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

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

- **ADSS Web RA Device**

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

- **ADSS Web RA SSL Device**

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

- **Windows Enrolment**

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

4 ADSS Web RA Installation on Windows Server

4.1 Fresh Installation of ADSS Web RA

Before starting the ADSS Web RA installation process, ensure that the following requirements are met:

- All prerequisites are installed on the ADSS Web RA machine. Without these, ADSS Web RA will not open or display any pages when accessed.
- An empty database is required if you are installing this version with PostgreSQL as fresh installation.

Once all the required prerequisites are installed and the database is prepared, you can start installing ADSS Web RA.

The ADSS Web RA package must be unzipped onto a disk that has sufficient space – a minimum of **100GB** is recommended. This is because the product is installed and runs from the location where the installation package is extracted.

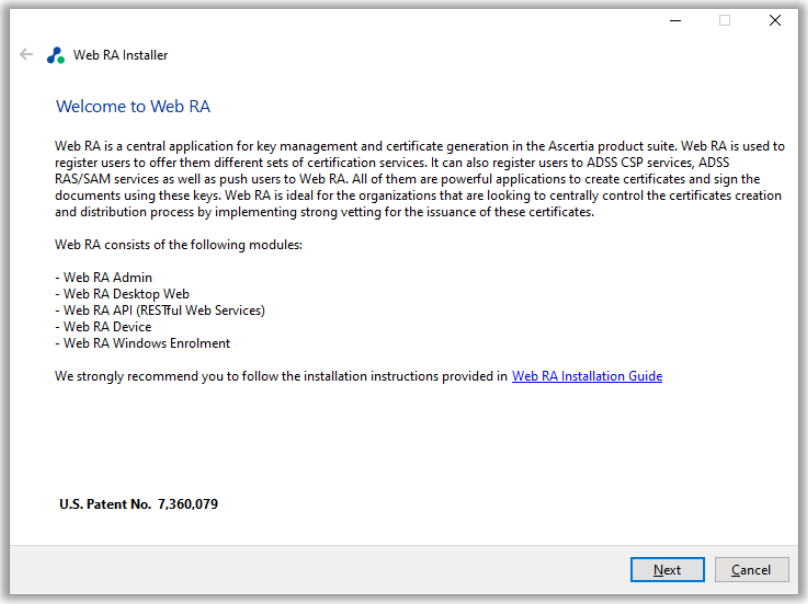
Moreover, if you extract the installer on the Desktop, it will not work. Therefore, choose a proper drive or folder to extract it.

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

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

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

The following welcome screen is shown:



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
- Web RA Windows Enrolment

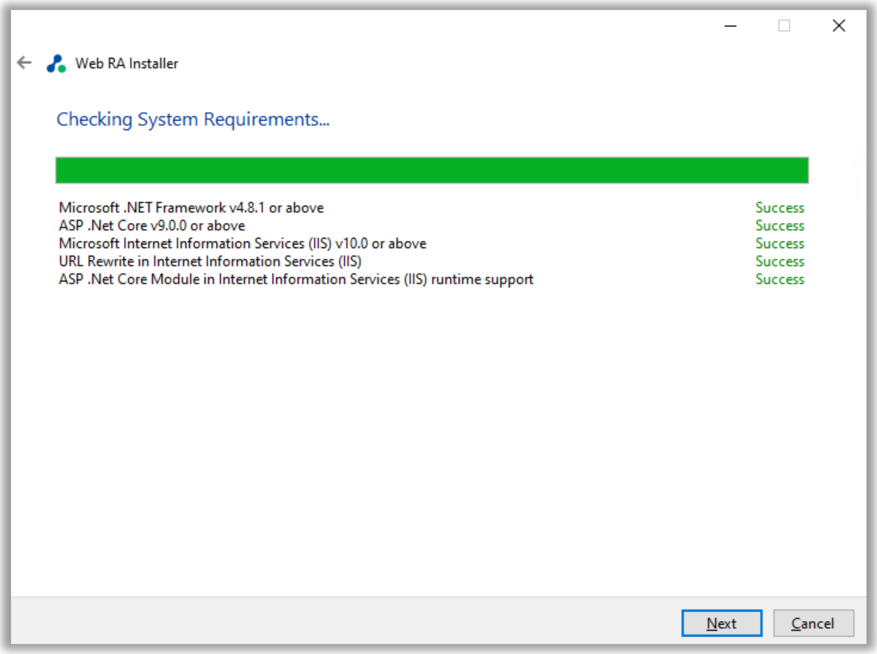
We strongly recommend you to follow the installation instructions provided in Web RA Installation Guide

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

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

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

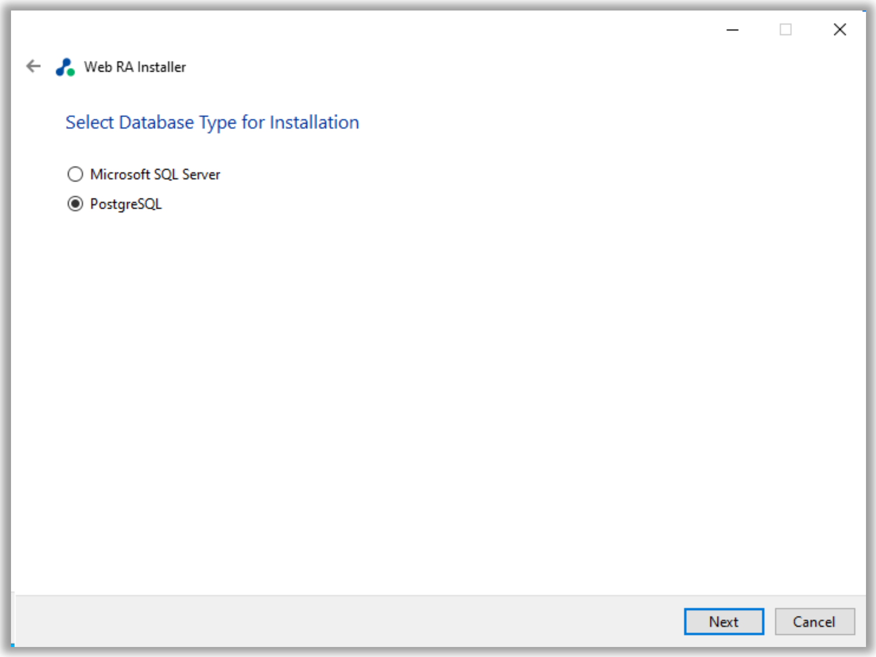
You can only proceed with the installation process once all issues related to system dependencies are resolved as shown below:



Checking System Requirements...

Microsoft .NET Framework v4.8.1 or above	Success
ASP .Net Core v9.0.0 or above	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) runtime support	Success

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

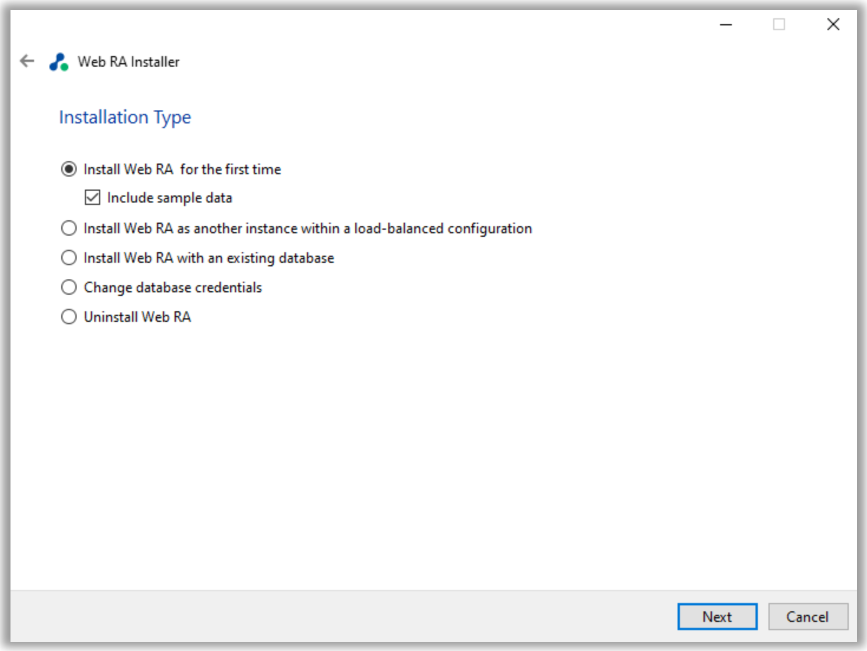


Select Database Type for Installation

○ Microsoft SQL Server

● PostgreSQL

4.1.5 Select the "PostgreSQL" radio button and click "Next".



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

○ Change database credentials

○ Uninstall Web RA

If you are installing ADSS Web RA for the first time or you wish to deploy a fresh installation with a new PostgreSQL database, then select "**Install Web RA for the first time**". If you want to install Web RA with sample data, enable the **'Include sample data"** checkbox.

The "**Install Web RA as another instance within a load-balanced configuration**" option will install the ADSS Web RA instance in a load-balanced mode.

The "**Install Web RA with an existing database"** option will install ADSS Web RA against an existing ADSS Web RA database. For example, this option can be used to recover a system from a database back-up.

The "**Change database credentials"** option is used if the database password, user, database name and/or server is changed, and it needs to be updated in ADSS Web RA installation.

Select the last option **Uninstall Web RA** if you wish to uninstall ADSS Web RA from the system.

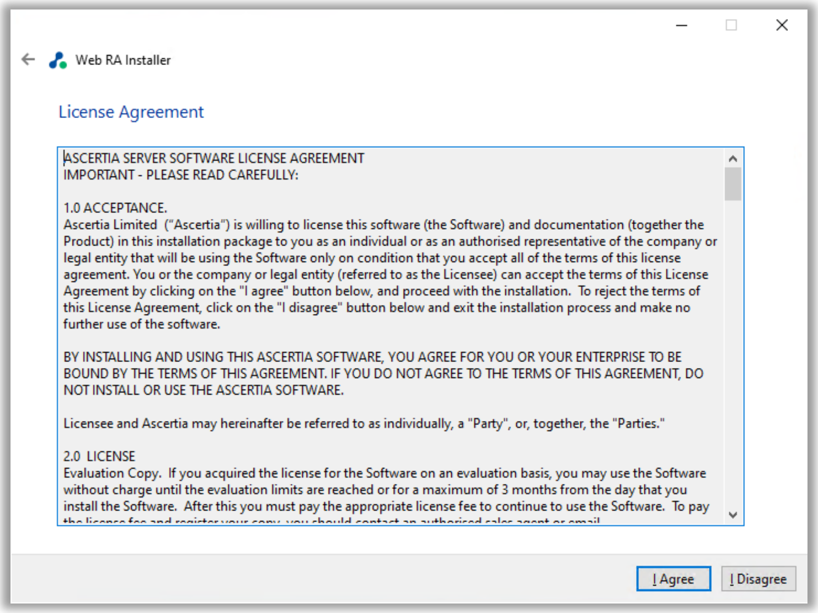
4.1.6 To install Web RA for the very first time, select the option **"Install Web RA for the first time"**.

You can include sample data in application during fresh installation. Sample data includes following data:

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

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

4.1.7 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.

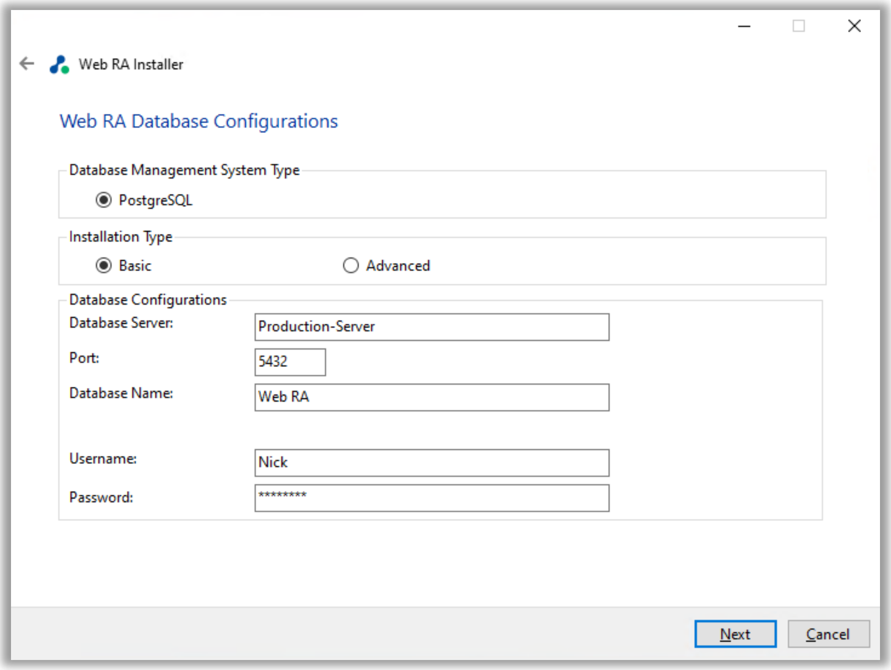
Licensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Parties."

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

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

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

The following screen for **Database Configurations** will be displayed.



Web RA Database Configurations

Database Management System Type
● PostgreSQL

Installation Type
● Basic ○ Advanced

Database Configurations
Database Server: Production-Server
Port: 5432
Database Name: Web RA
Username: Nick
Password: ********

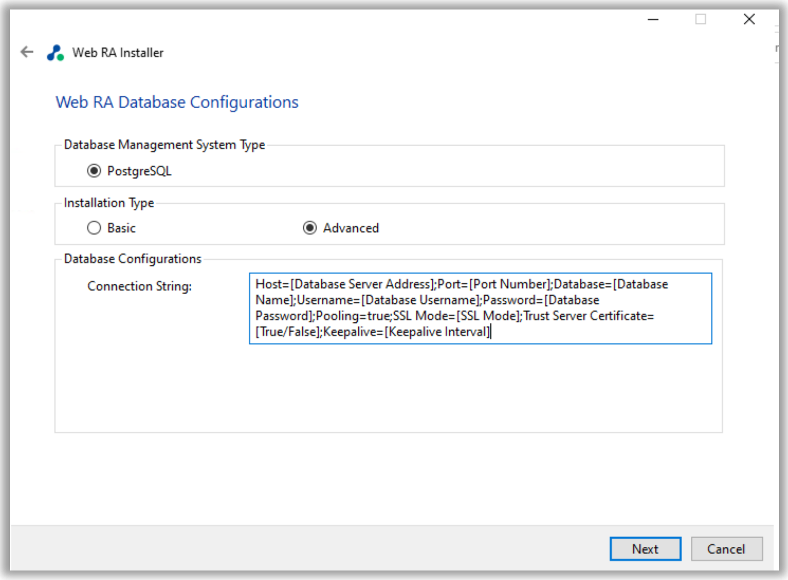
You can either choose to do a **"Basic"** installation or an **"Advanced"** one. If this is a basic installation, then use the first option "**Basic"** and provide the appropriate ADSS Web RA database credentials. The information displayed above is an example and you should configure the relevant settings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

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

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

Item	Description
Database Server / Host Name	Database server IP or DNS name.
Port	It is the database listening port. - For PostgreSQL Server the default port is **5432**.
Database Name	Name of the database instance. **Note:** This must exist prior to the installation.
Username	Name of the database user.
Password	Password credential of the database user.

If you select the **Advanced** option for database configurations, then the following screen will appear:



Web RA Database Configurations

Database Management System Type

● PostgreSQL

Installation Type

○ Basic ● Advanced

Database Configurations

Connection String: Host=[Database Server Address];Port=[Port Number];Database=[Database Name];Username=[Database Username];Password=[Database Password];Pooling=true;SSL Mode=[SSL Mode];Trust Server Certificate=[True/False];Keepalive=[Keepalive Interval]

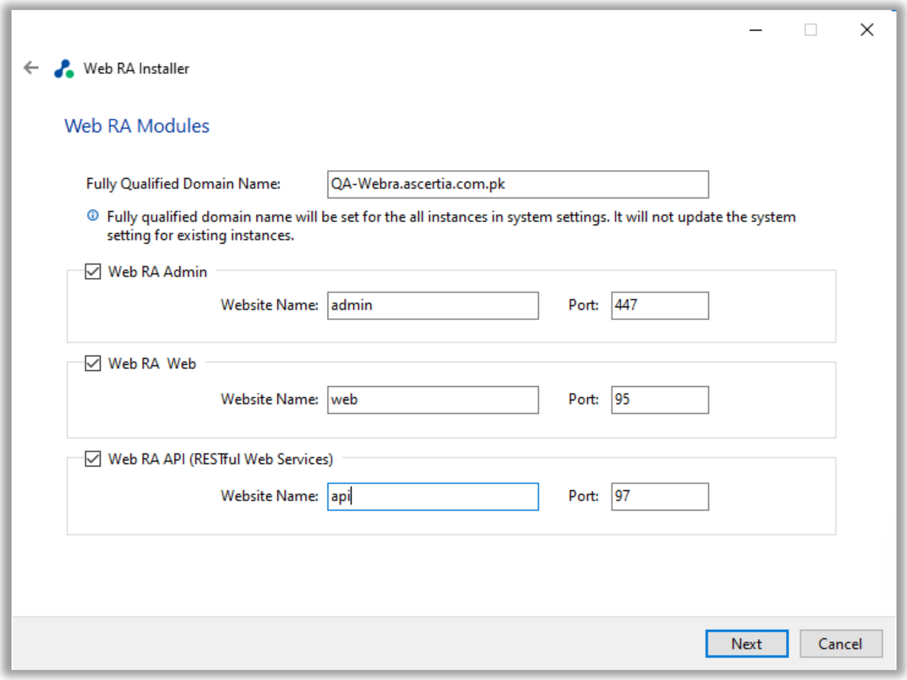
Note: The information displayed above is an example and you should configure the relevant settings for your own environment.

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

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

Item	Description
ADSS Web RA Connection String	The following is the sample connection string for PostgreSQL Server: - RAEntities": "Host=**[Database Server Address]**;Port**=[Port Number]**;Database=**[Database Name];**Username**=[Database Username]**;Password=**[Database Password]**;Pooling=true;SSL Mode=**[SSL Mode]**;Trust Server Certificate=[True/False];Keepalive=[Keepalive Interval]"

4.1.9 After completing the database configurations, click the Next button to select specific modules.



Web RA Installer

Web RA Modules

Fully Qualified Domain Name: QA-Webra.ascertia.com.pk

Fully qualified domain name will be set for the all instances in system settings. It will not update the system setting for existing instances.

☑ Web RA Admin
Website Name: admin Port: 447

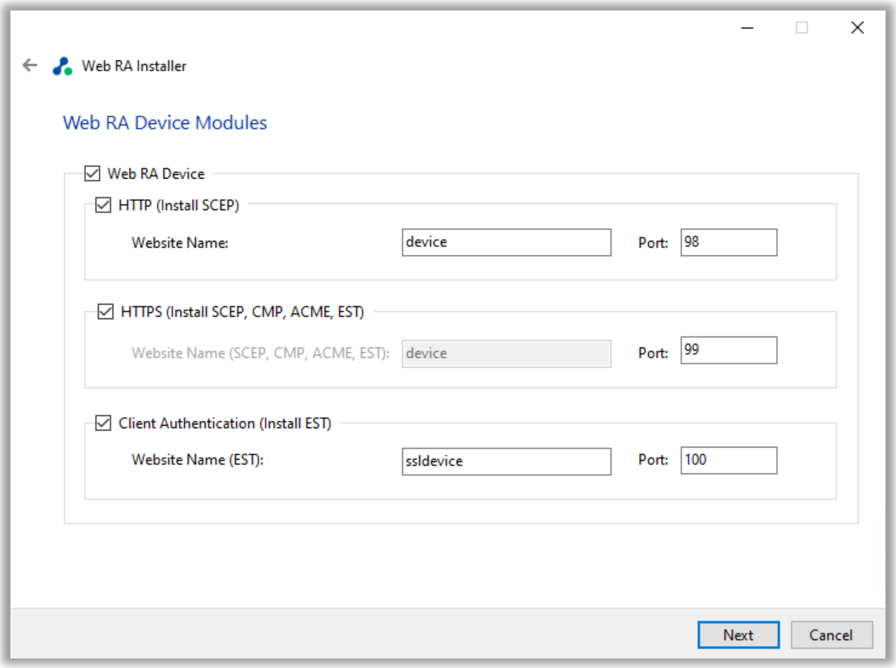
☑ Web RA Web
Website Name: web Port: 95

☑ Web RA API (RESTful Web Services)
Website Name: api Port: 97

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

After entering the information, click 'Next' to proceed.

4.1.11 Select the 'Web RA Device Modules", then click "Next' to continue.



Web RA Installer

Web RA Device Modules

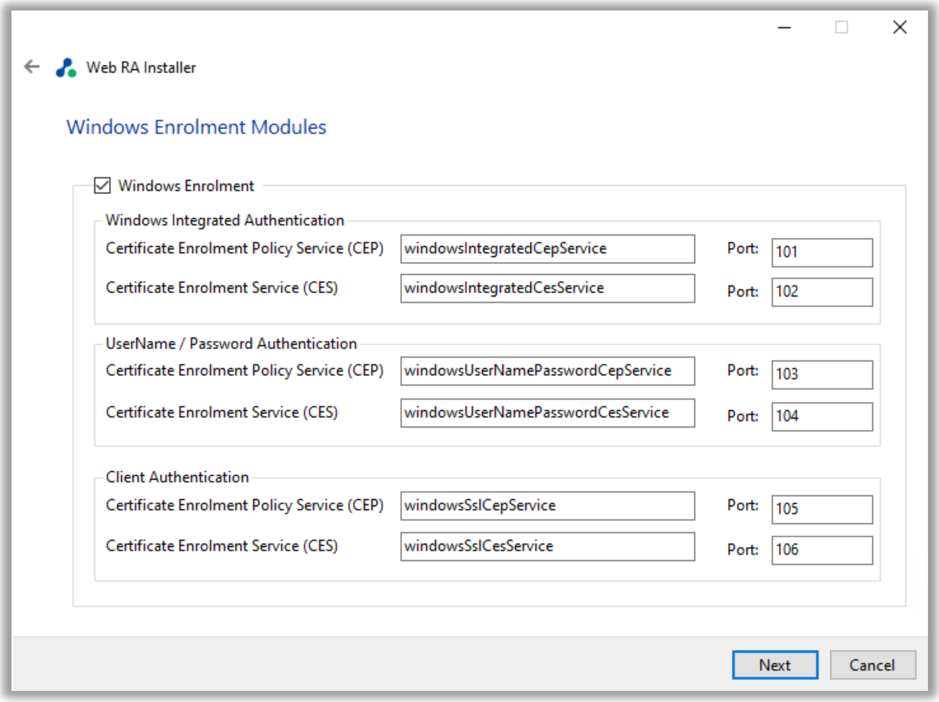
☑ Web RA Device

☑ HTTP (Install SCEP)
Website Name: device Port: 98

☑ HTTPS (Install SCEP, CMP, ACME, EST)
Website Name (SCEP, CMP, ACME, EST): device Port: 99

☑ Client Authentication (Install EST)
Website Name (EST): ssldevice Port: 100

4.1.12 The next step is to select “Windows Enrolment Modules”. For each selected application, provide the web application name and port, then click Next.



Web RA Installer

Windows Enrolment Modules

☑ Windows Enrolment

Windows Integrated Authentication

Certificate Enrolment Policy Service (CEP): windowsIntegratedCepService Port: 101

Certificate Enrolment Service (CES): windowsIntegratedCesService Port: 102

UserName / Password Authentication

Certificate Enrolment Policy Service (CEP): windowsUserNamePasswordCepService Port: 103

Certificate Enrolment Service (CES): windowsUserNamePasswordCesService Port: 104

Client Authentication

Certificate Enrolment Policy Service (CEP): windowsSslCepService Port: 105

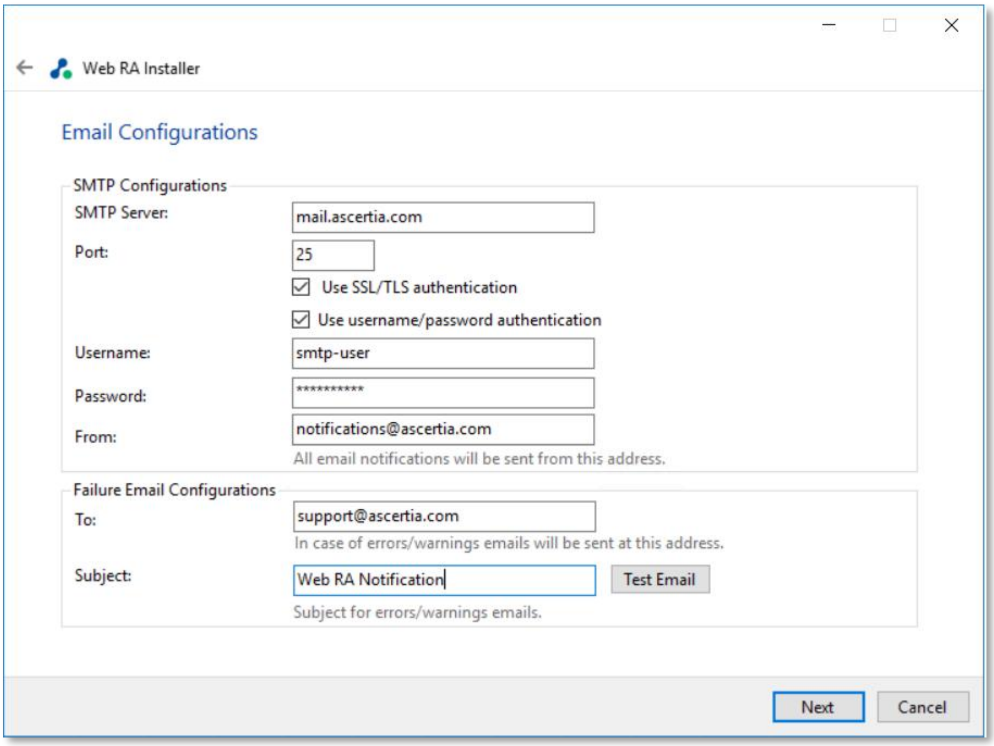
Certificate Enrolment Service (CES): windowsSslCesService Port: 106

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

The following table explains the details of the module options:

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

4.1.13 Click “Next” button to configure the “SMTP Server and Email” settings.



Email Configurations

SMTP Configurations

SMTP Server: mail.ascertia.com

Port: 25

☑ Use SSL/TLS authentication

☑ Use username/password authentication

Username: smtp-user

Password: **********

From: notifications@ascertia.com

All email notifications will be sent from this address.

Failure Email Configurations

To: support@ascertia.com

In case of errors/warnings emails will be sent at this address.

Subject: Web RA Notification

Subject for errors/warnings emails.

Configure SMTP Server and email settings for your environment. ADSS Web RA must have access to a suitable SMTP Server without which users will not be able to receive registration emails that are required to complete the user registration process. Moreover, you will not receive the system generated email notifications either. Although the latter will not prevent functionality, but it is not a recommended approach. The information displayed above is an example and you should setup configurations for your own environment.

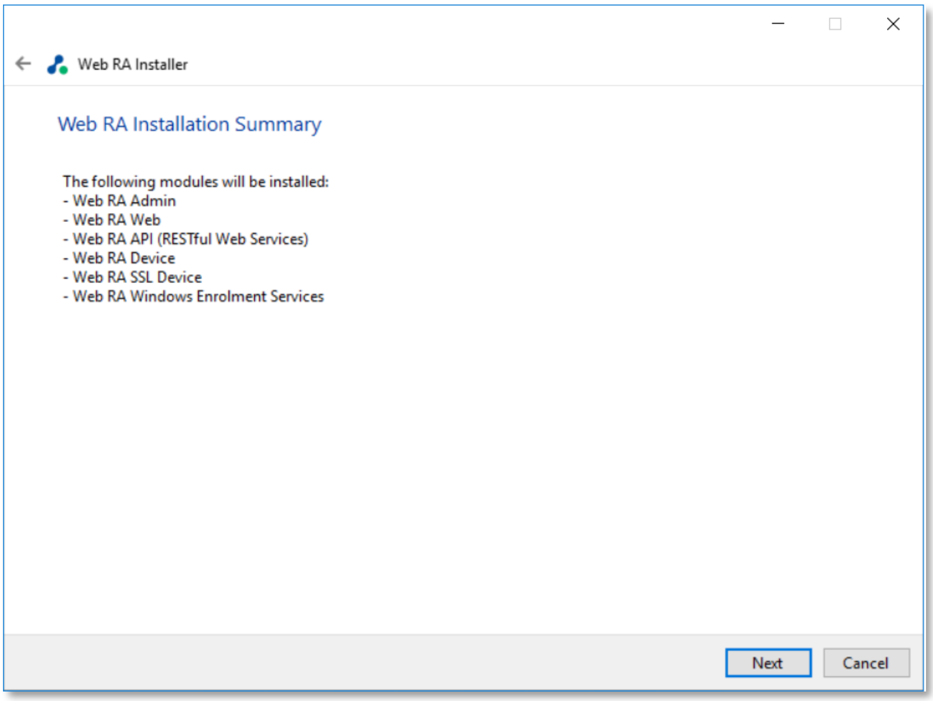
The configuration items are explained in the following table:

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

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

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

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



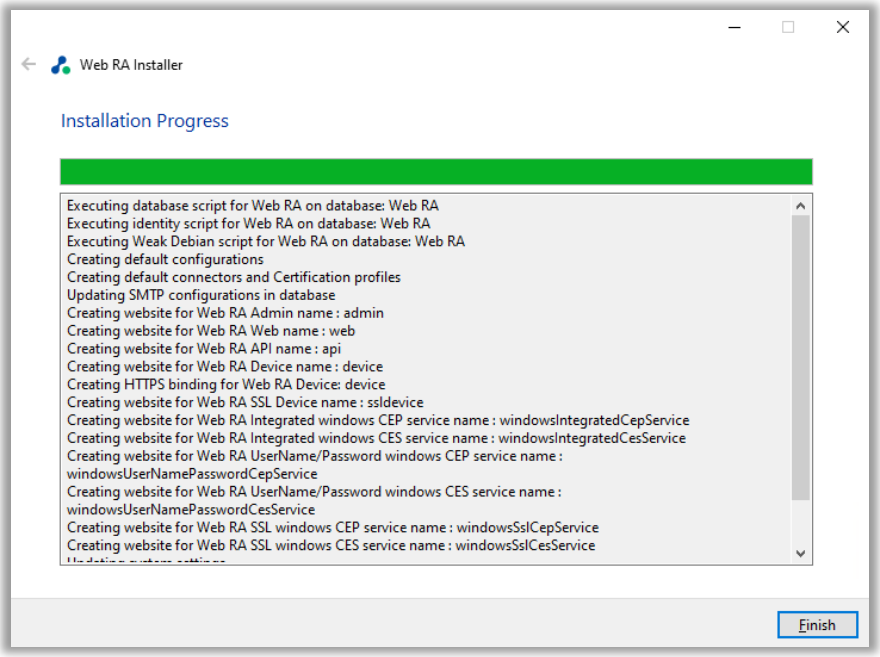
Web RA Installation Summary

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

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

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

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



Installation Progress

```
Executing database script for Web RA on database: Web RA
Executing identity script for Web RA on database: Web RA
Executing Weak Debian script for Web RA on database: Web RA
Creating default configurations
Creating default connectors and Certification profiles
Updating SMTP configurations in database
Creating website for Web RA Admin name : admin
Creating website for Web RA Web name : web
Creating website for Web RA API name : api
Creating website for Web RA Device name : device
Creating HTTPS binding for Web RA Device: device
Creating website for Web RA SSL Device name : ssldevice
Creating website for Web RA Integrated windows CEP service name : windowsIntegratedCepService
Creating website for Web RA Integrated windows CES service name : windowsIntegratedCesService
Creating website for Web RA UserName/Password windows CEP service name :
windowsUserNamePasswordCepService
Creating website for Web RA UserName/Password windows CES service name :
windowsUserNamePasswordCesService
Creating website for Web RA SSL windows CEP service name : windowsSslCepService
Creating website for Web RA SSL windows CES service name : windowsSslCesService
Updating system settings
```

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

4.1.16 ADSS Web RA URLs

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

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

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

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

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

- Using standard IIS web server HTTP redirects. This means the basic installation is done with various ADSS Web RA sites, where each site has their respective default port/binding but no host name. You can then add new sites for each web site and bind this to the desired external public facing host name and secure port, likely to be 443. Each site can be configured in such a fashion. Each default ADSS Web RA site can then be configured to permanently redirect to the secure version.
- Once the deployment of ADSS Web RA is completed, the bindings of each site can be changed to use a secure (443) port. The new binding will include the appropriate public facing host name.

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

The second option is recommended.

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

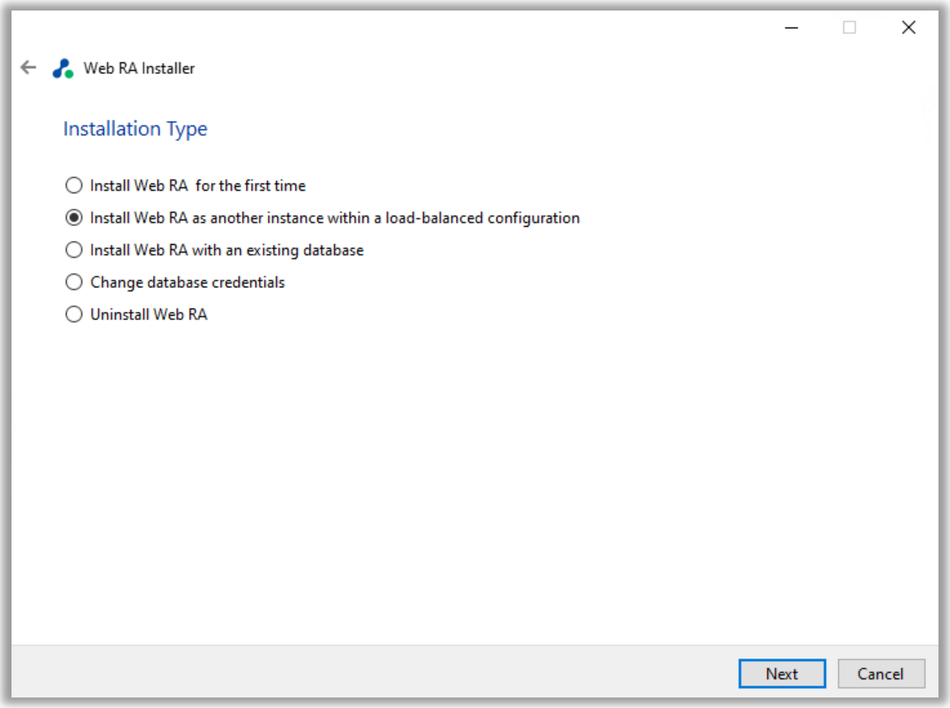
4.2 Installing ADSS Web RA with A Load-Balanced Configuration

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

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

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

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



Installation Type

○ Install Web RA for the first time

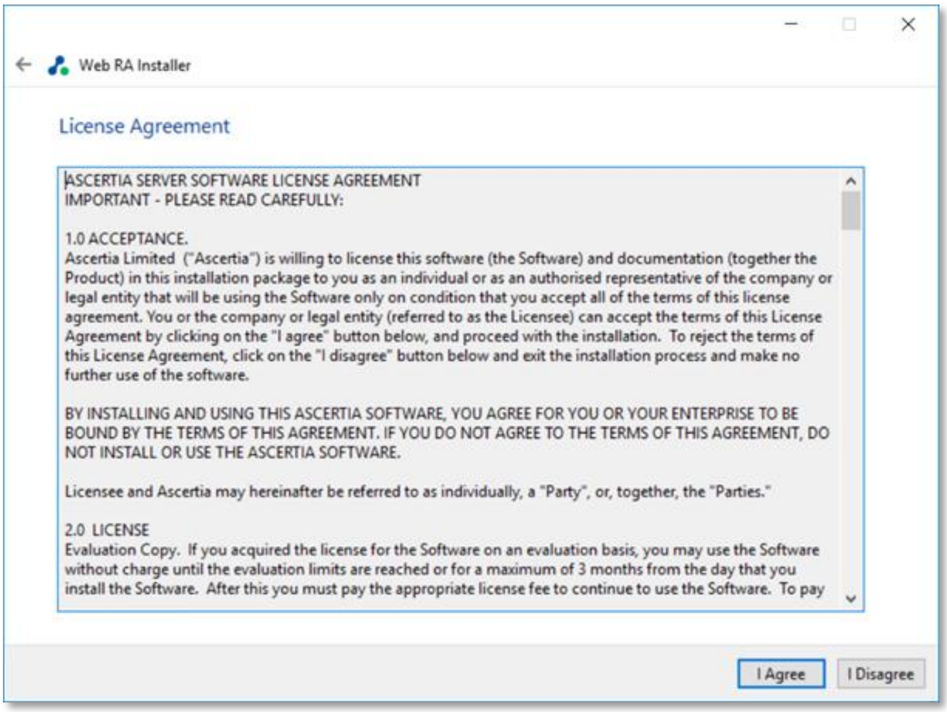
● Install Web RA as another instance within a load-balanced configuration

○ Install Web RA with an existing database

○ Change database credentials

○ Uninstall Web RA

4.2.3 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.

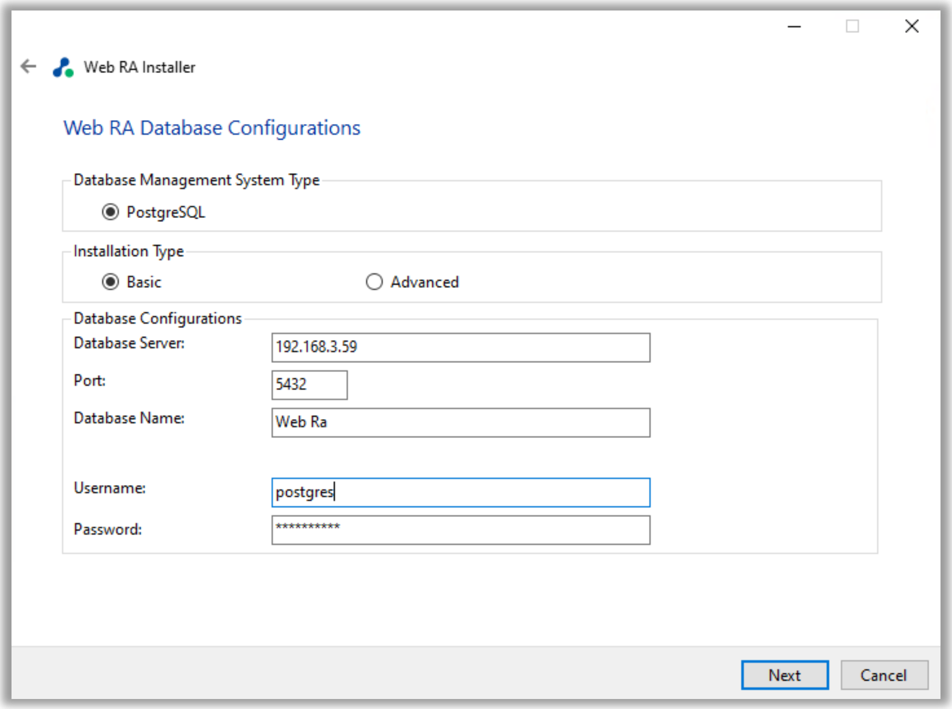
Licensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Parties."

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

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

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

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



Web RA Database Configurations

Database Management System Type

● PostgreSQL

Installation Type

● Basic ○ Advanced

Database Configurations

Database Server: 192.168.3.59

Port: 5432

Database Name: Web Ra

Username: postgres

Password: **********

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

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

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

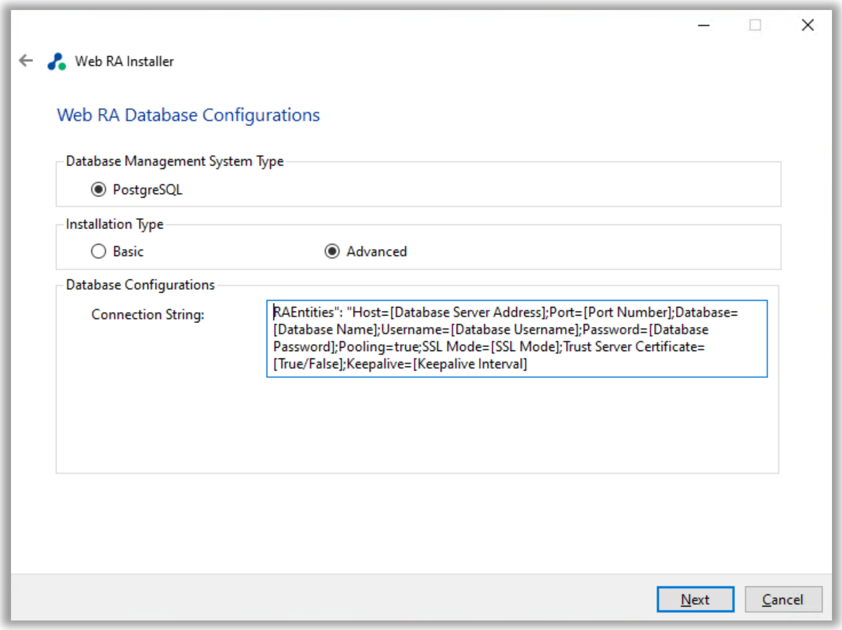
You can either choose to do a basic installation or use an advanced one. If this is a basic installation, then use the first option **Basic** and provide the appropriate ADSS Web RA database credentials. The information displayed above is an example and you should configure the relevant settings for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

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

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

Item	Description
Database Server / Host Name	Database server IP or DNS name.
Port	Database listening port. - For PostgreSQL Server the default port is 5432**.**
Database Name	Name of the database instance. **Note:** This must exist prior to the installation.
Username	Name of the database user. **Note:** This must exist prior to the installation.
Password	Password credential of the database user. **Note:** This must exist prior to the installation.

If you choose the “**Advanced”** option**,** the following screen is displayed:



Web RA Database Configurations

Database Management System Type

● PostgreSQL

Installation Type

○ Basic ● Advanced

Database Configurations

Connection String: RAEntities": "Host=[Database Server Address];Port=[Port Number];Database=[Database Name];Username=[Database Username];Password=[Database Password];Pooling=true;SSL Mode=[SSL Mode];Trust Server Certificate=[True/False];Keepalive=[Keepalive Interval]

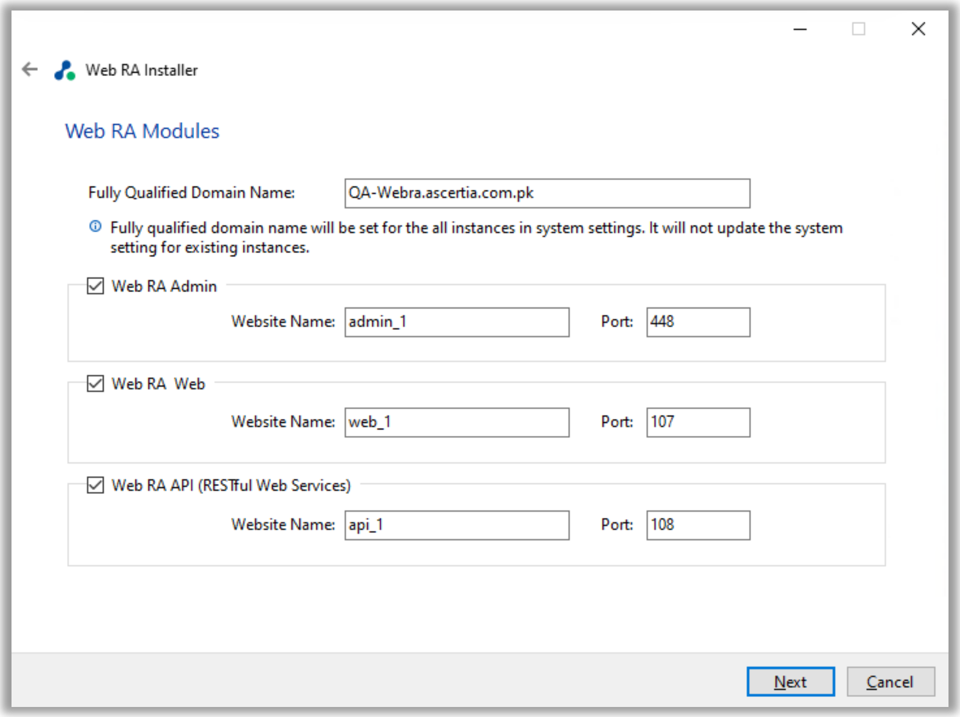
The information displayed above is an example and you should configure the relevant settings for your own environment.

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

The following table entails details of the configuration options:

Item	Description
ADSS Web RA Connection String	The following is the sample connection string for PostgreSQL Server: • RAEntities": Host=**[Database Server Address]**;Port**=[Port Number]**;Database=**[Database Name];**Username**=[Database Username]**;Password=**[Database Password]**;Pooling=true;SSL Mode=**[SSL Mode]**;Trust Server Certificate=[True/False];Keepalive=[Keepalive Interval]

4.2.7 Click the **Next** button to select the specific **Web RA Modules**. Add the modules that you want to install in load balancing environment.



Web RA Installer

Web RA Modules

Fully Qualified Domain Name: QA-Webra.ascertia.com.pk

Fully qualified domain name will be set for the all instances in system settings. It will not update the system setting for existing instances.

☑ Web RA Admin

Website Name: admin_1 Port: 448

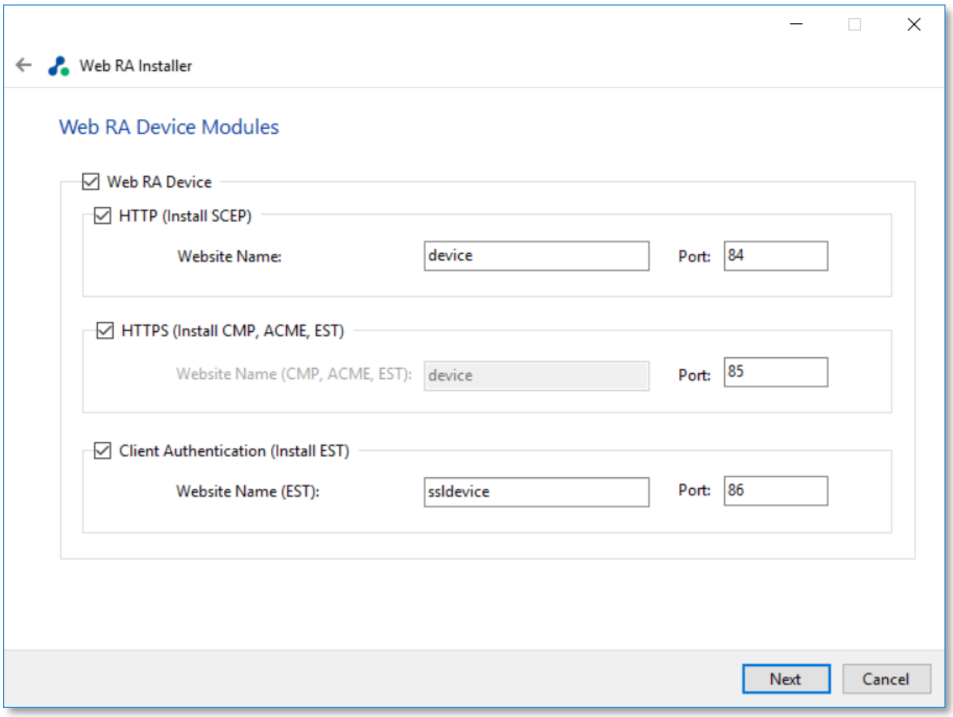
☑ Web RA Web

Website Name: web_1 Port: 107

☑ Web RA API (RESTful Web Services)

Website Name: api_1 Port: 108

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



Web RA Installer

Web RA Device Modules

☑ Web RA Device

☑ HTTP (Install SCEP)

Website Name: device Port: 84

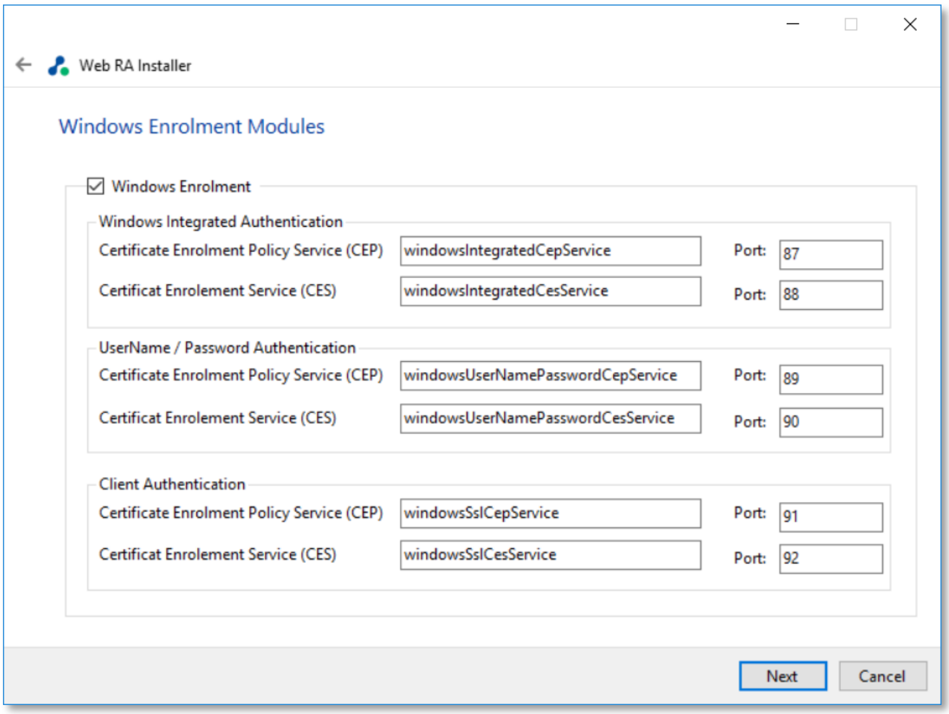
☑ HTTPS (Install CMP, ACME, EST)

Website Name (CMP, ACME, EST): device Port: 85

☑ Client Authentication (Install EST)

Website Name (EST): ssldevice Port: 86

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



Windows Enrolment Modules

☑ Windows Enrolment

Windows Integrated Authentication

Certificate Enrolment Policy Service (CEP) windowsIntegratedCepService Port: 87

Certificat Enrolement Service (CES) windowsIntegratedCesService Port: 88

UserName / Password Authentication

Certificate Enrolment Policy Service (CEP) windowsUserNamePasswordCepService Port: 89

Certificat Enrolement Service (CES) windowsUserNamePasswordCesService Port: 90

Client Authentication

Certificate Enrolment Policy Service (CEP) windowsSslCepService Port: 91

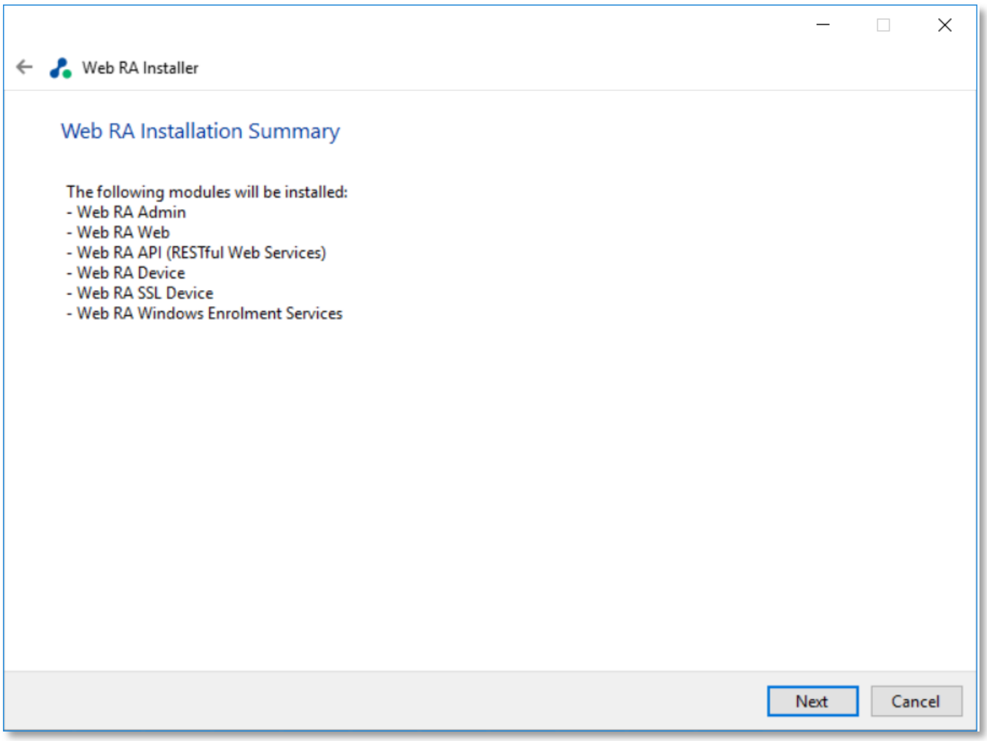
Certificat Enrolement Service (CES) windowsSslCesService Port: 92

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

The following table explains the details of the modules:

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

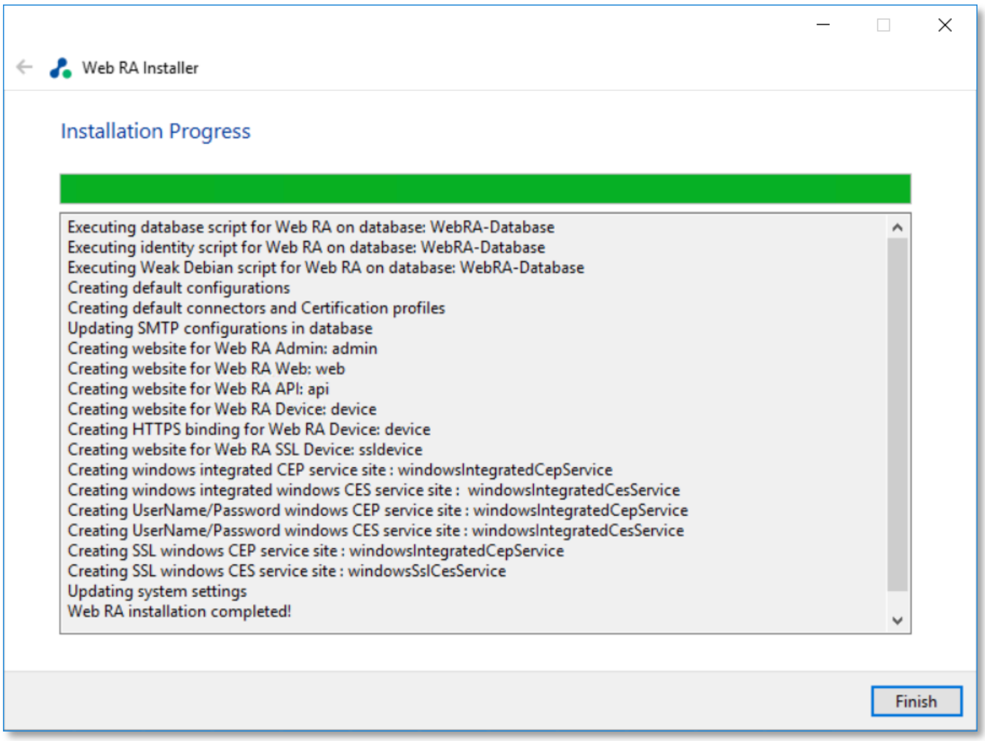
4.2.10 Click the **Next** button to show the **Installation Summary** and complete the installation.



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
- Web RA SSL Device
- Web RA Windows Enrolment Services

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 present at the top-left corner of the installer dialogue box) to correct your choices before proceeding.



Installation Progress

```
Executing database script for Web RA on database: WebRA-Database
Executing identity script for Web RA on database: WebRA-Database
Executing Weak Debian script for Web RA on database: WebRA-Database
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: web
Creating website for Web RA API: api
Creating website for Web RA Device: device
Creating HTTPS binding for Web RA Device: device
Creating website for Web RA SSL Device: ssldevice
Creating windows integrated CEP service site : windowsIntegratedCepService
Creating windows integrated windows CES service site :  windowsIntegratedCesService
Creating UserName/Password windows CEP service site : windowsIntegratedCepService
Creating UserName/Password windows CES service site : windowsIntegratedCesService
Creating SSL windows CEP service site : windowsIntegratedCepService
Creating SSL windows CES service site : windowsSslCesService
Updating system settings
Web RA installation completed!
```

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

4.2.12 ADSS Web RA URLs

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

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

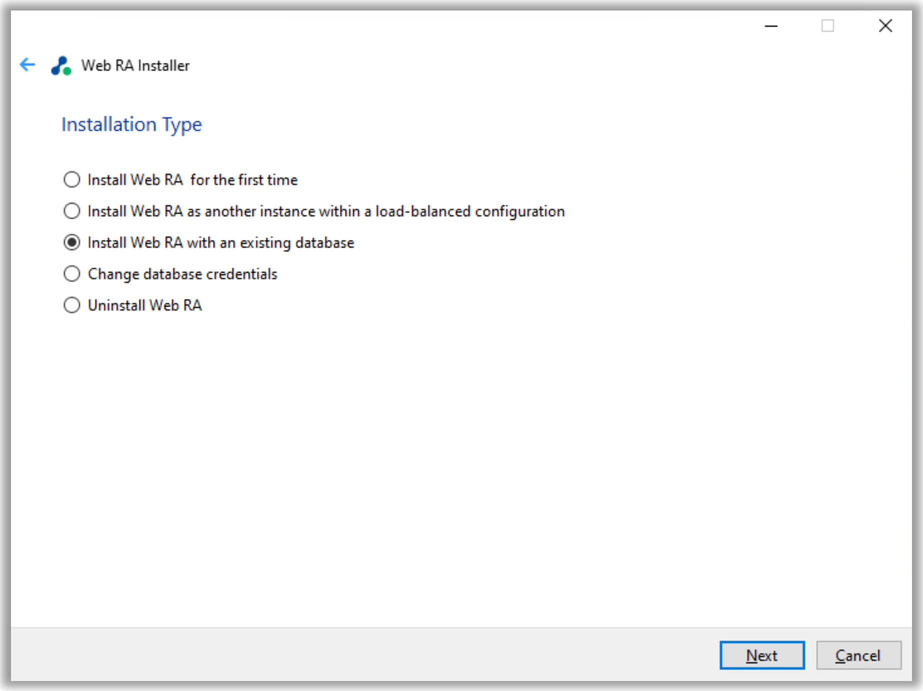
The site IDs of deployed IIS websites should be the same across all the instances in a load balanced environment to run Web RA application properly. Therefore, to ensure a successful load-balanced installation, you should check that the required site IDs on the primary instance are also available on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

4.3 Installing ADSS Web RA with an Existing Database

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

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

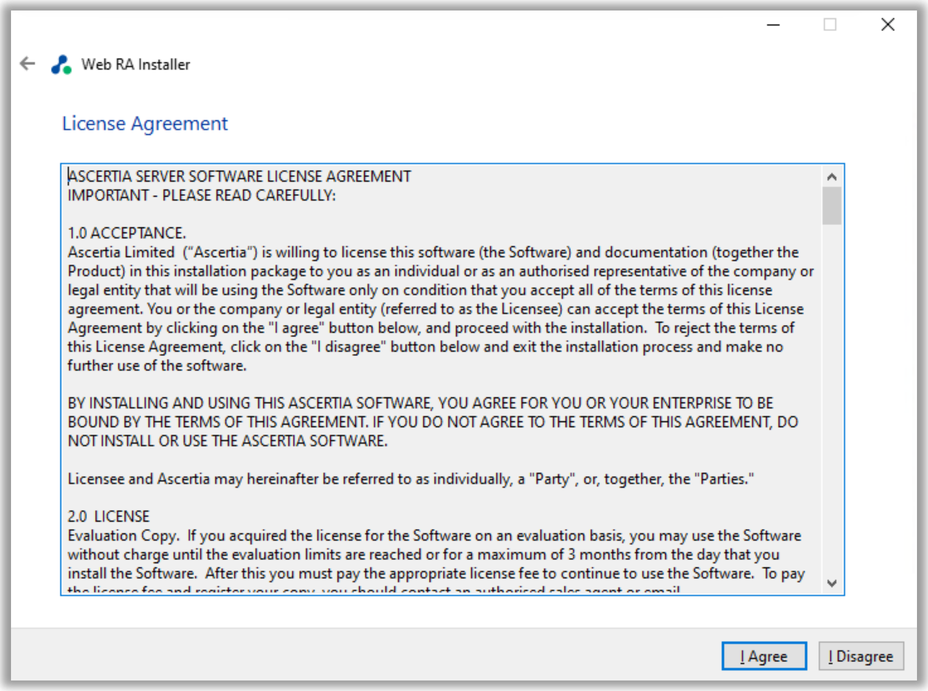
4.3.2 Select the option **Install ADSS Web RA within an existing database**.



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
○ Change database credentials
○ Uninstall Web RA

4.3.3 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.

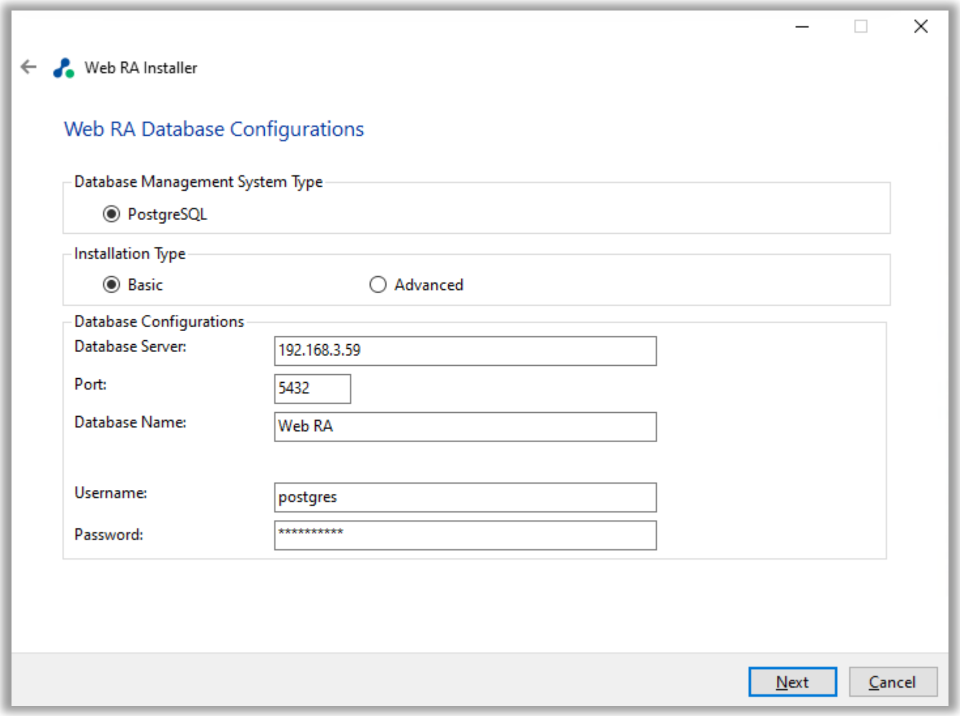
BY INSTALLING AND USING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE ASCERTIA SOFTWARE.

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 licence fee and register your copy, you should contact an authorised sales agent or email

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

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



Web RA Installer

Web RA Database Configurations

Database Management System Type

● PostgreSQL

Installation Type

● Basic ○ Advanced

Database Configurations

Database Server: 192.168.3.59

Port: 5432

Database Name: Web RA

Username: postgres

Password: **********

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

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

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

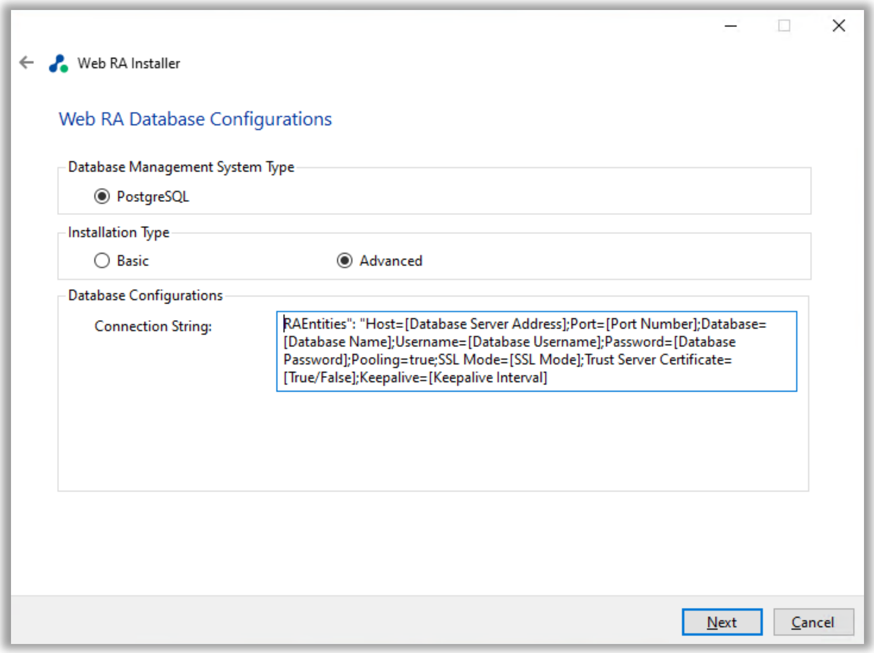
You can either choose to do a basic installation or use an advanced one. If you want to perform a basic installation, then use the first option **Basic** and provide the appropriate ADSS Web RA database credentials. The information displayed above is an example and you should configure the relevant settings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

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

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

Item	Description
Database Server / Host Name	Database server IP or DNS name.
Port	It is the database listening port. - For PostgreSQL Server the default port is 5432**.**
Database Name	Name of the database instance. **Note:** This must exist prior to the installation.
Username	Name of the database user. **Note:** This must exist prior to the installation.
Password	Password credential of the database user. **Note:** This must exist prior to the installation.

Alternatively, if you choose the second "**Advanced"** option, then the following screen is displayed:



Web RA Installer

Web RA Database Configurations

Database Management System Type

● PostgreSQL

Installation Type

○ Basic ● Advanced

Database Configurations

Connection String: RAEntities": "Host=[Database Server Address];Port=[Port Number];Database=[Database Name];Username=[Database Username];Password=[Database Password];Pooling=true;SSL Mode=[SSL Mode];Trust Server Certificate=[True/False];Keepalive=[Keepalive Interval]

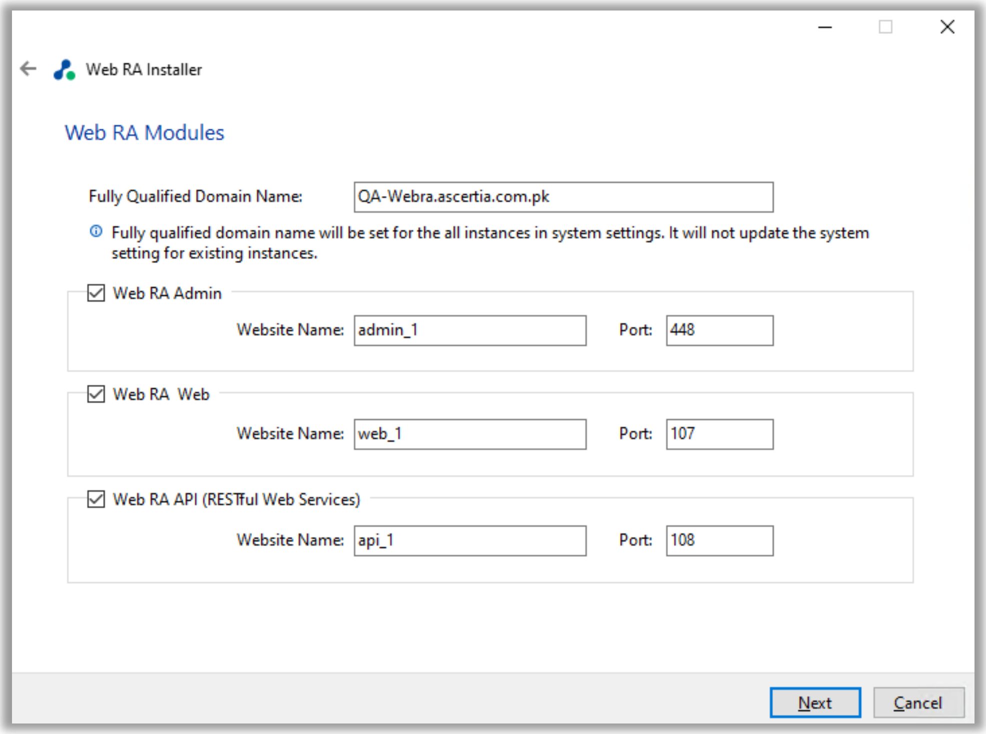
The information displayed above is an example and you should configure the relevant settings for your own environment.

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

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

Item	Description
ADSS Web RA Connection String	The following is the sample connection string for PostgreSQL Server: • "RAEntities": "Host=[Database Server Address];Port=[Port Number];Database=[Database Name];Username=[Database Username];Password=[Database Password];Pooling=true;SSL Mode=[SSL Mode];Trust Server Certificate=[True/False];Keepalive=[Keepalive Interval]"

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



Web RA Installer

Web RA Modules

Fully Qualified Domain Name: QA-Webra.ascertia.com.pk

ⓘ Fully qualified domain name will be set for the all instances in system settings. It will not update the system setting for existing instances.

☑ Web RA Admin

Website Name: admin_1 Port: 448

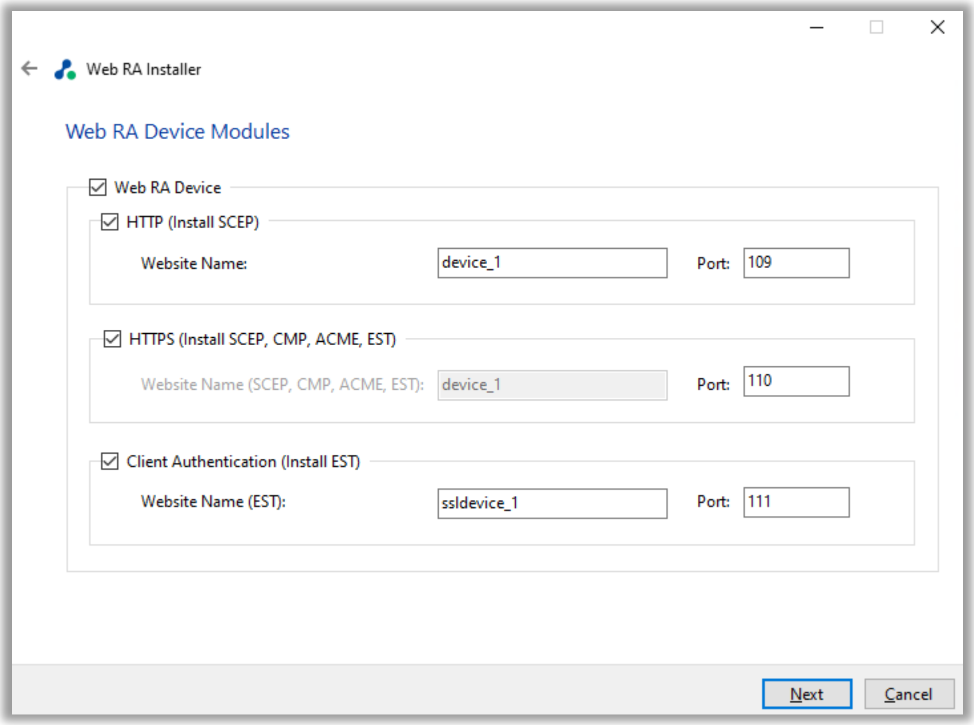
☑ Web RA Web

Website Name: web_1 Port: 107

☑ Web RA API (RESTful Web Services)

Website Name: api_1 Port: 108

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



Web RA Installer

Web RA Device Modules

☑ Web RA Device

☑ HTTP (Install SCEP)

Website Name: device_1 Port: 109

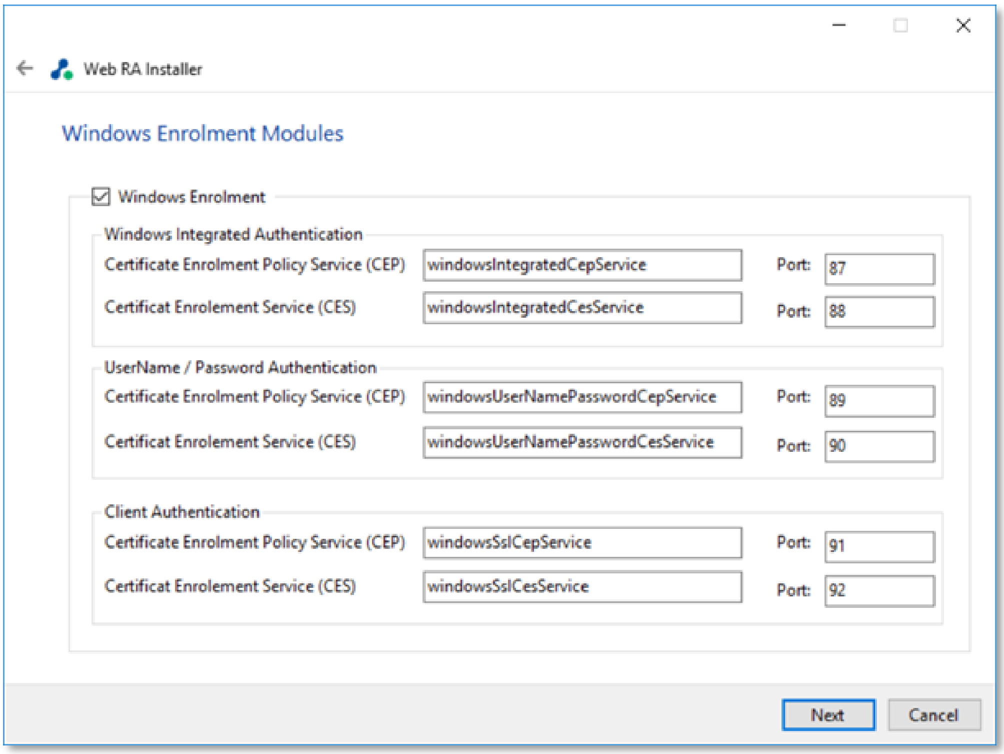
☑ HTTPS (Install SCEP, CMP, ACME, EST)

Website Name (SCEP, CMP, ACME, EST): device_1 Port: 110

☑ Client Authentication (Install EST)

Website Name (EST): ssldevice_1 Port: 111

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



Web RA Installer

Windows Enrolment Modules

☑ Windows Enrolment

Windows Integrated Authentication

Certificate Enrolment Policy Service (CEP)	windowsIntegratedCepService	Port:	87
Certificat Enrolement Service (CES)	windowsIntegratedCesService	Port:	88

UserName / Password Authentication

Certificate Enrolment Policy Service (CEP)	windowsUserNamePasswordCepService	Port:	89
Certificat Enrolement Service (CES)	windowsUserNamePasswordCesService	Port:	90

Client Authentication

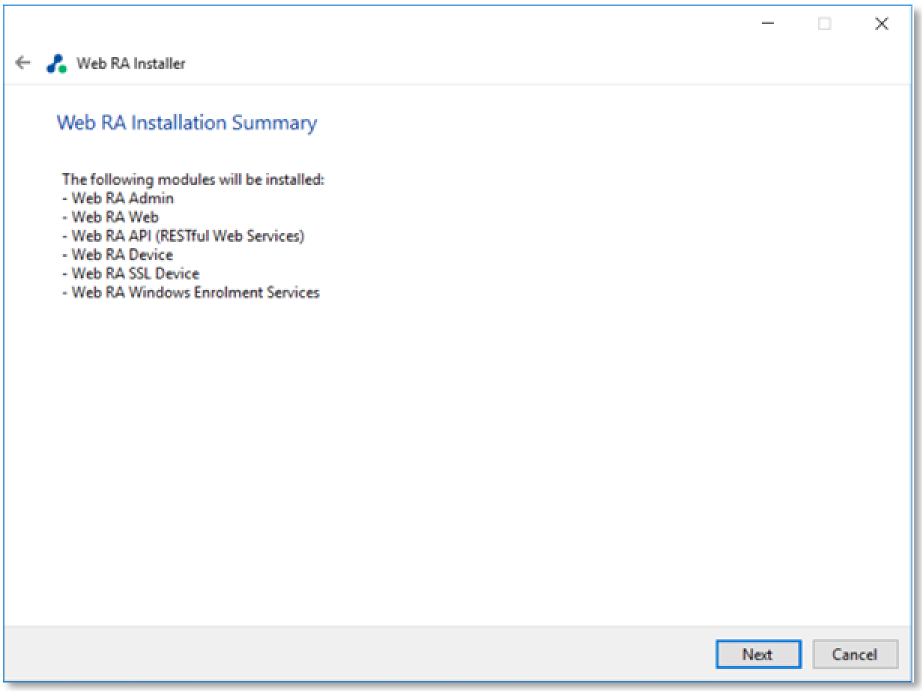
Certificate Enrolment Policy Service (CEP)	windowsSslCepService	Port:	91
Certificat Enrolement Service (CES)	windowsSslCesService	Port:	92

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

The following table explains the details of modules options:

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

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

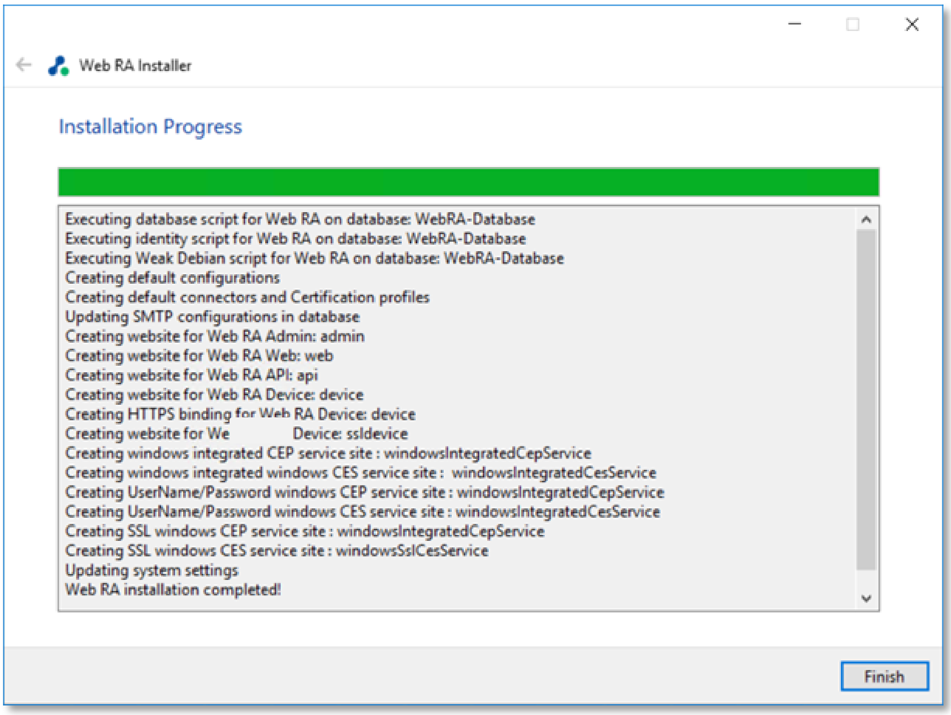


The following modules will be installed:
- Web RA Admin
- Web RA Web
- Web RA API (RESTful Web Services)
- Web RA Device
- Web RA SSL Device
- Web RA Windows Enrolment Services

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

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

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



```
Executing database script for Web RA on database: WebRA-Database
Executing identity script for Web RA on database: WebRA-Database
Executing Weak Debian script for Web RA on database: WebRA-Database
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: web
Creating website for Web RA API: api
Creating website for Web RA Device: device
Creating HTTPS binding for Web RA Device: device
Creating website for We           Device: ssldevice
Creating windows integrated CEP service site : windowsIntegratedCepService
Creating windows integrated windows CES service site :  windowsIntegratedCesService
Creating UserName/Password windows CEP service site : windowsIntegratedCepService
Creating UserName/Password windows CES service site : windowsIntegratedCesService
Creating SSL windows CEP service site : windowsIntegratedCepService
Creating SSL windows CES service site : windowsSslCesService
Updating system settings
Web RA installation completed!
```

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

4.3.11 ADSS Web RA URLs

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

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

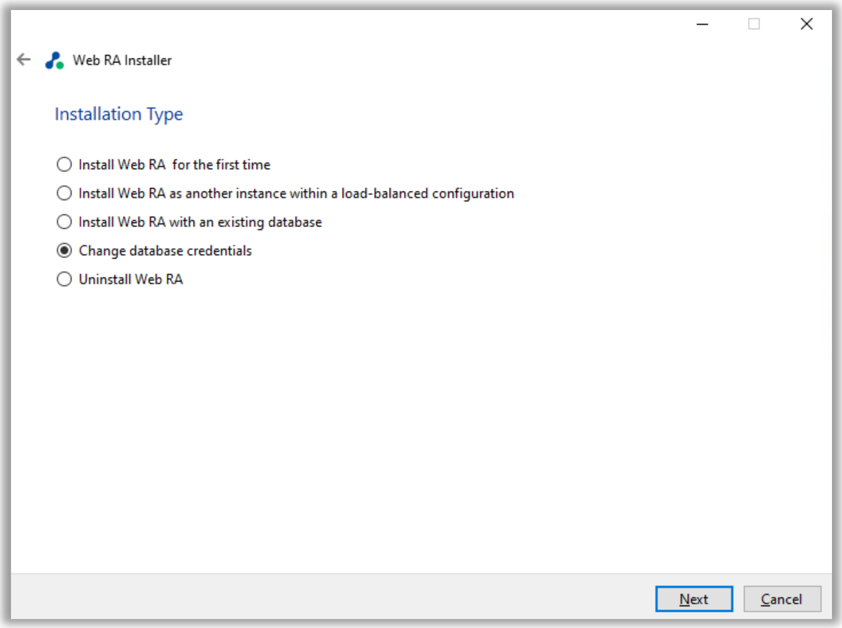
4.4 Changing Database Credentials for an Existing Installation

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

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

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

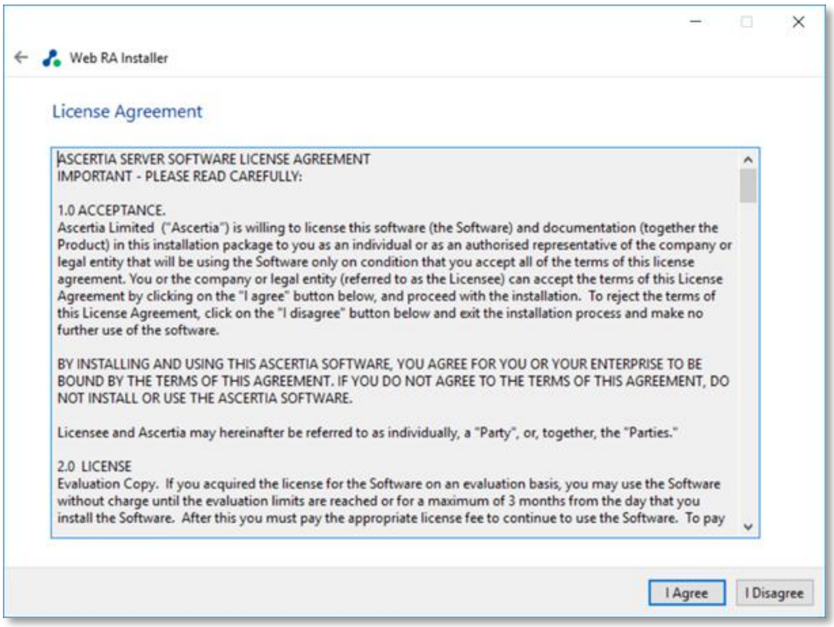
4.6.1. Follow the installation wizard, and select the **"Change database credentials"** option, when the **Installation Type** screen is shown:



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
● Change database credentials
○ Uninstall Web RA

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



License Agreement

ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:

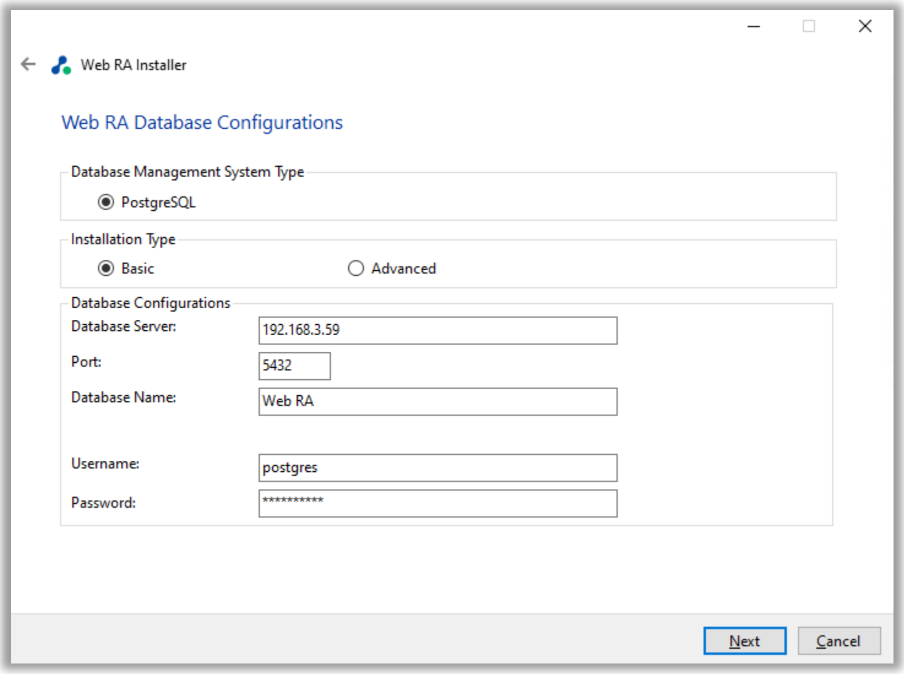
1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition 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

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



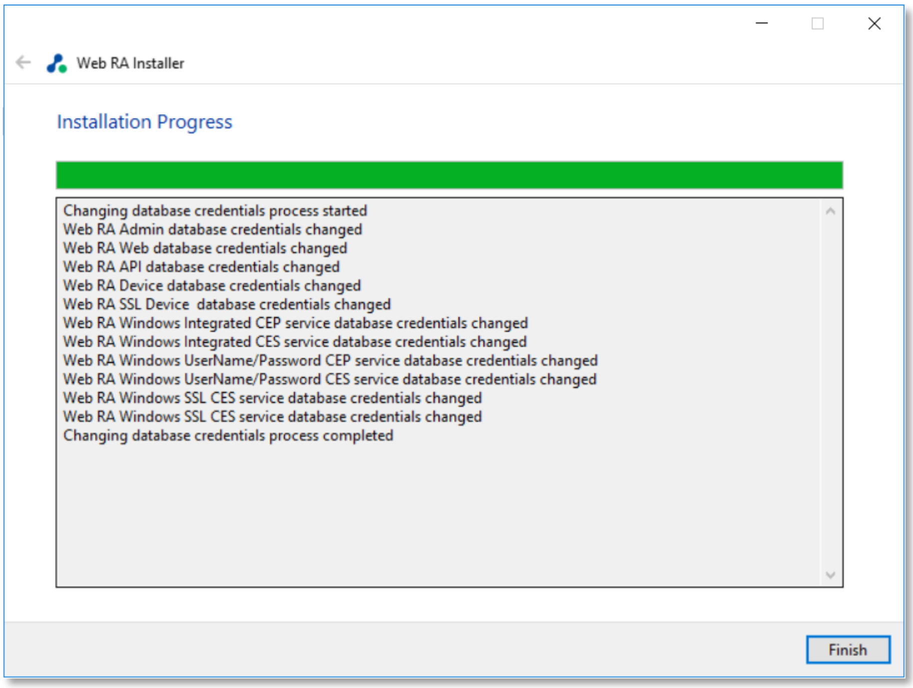
Web RA Database Configurations

Database Management System Type
● PostgreSQL

Installation Type
● Basic ○ Advanced

Database Configurations
Database Server: 192.168.3.59
Port: 5432
Database Name: Web RA
Username: postgres
Password: **********

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



Installation Progress

```
Changing database credentials process started
Web RA Admin database credentials changed
Web RA Web database credentials changed
Web RA API database credentials changed
Web RA Device database credentials changed
Web RA SSL Device  database credentials changed
Web RA Windows Integrated CEP service database credentials changed
Web RA Windows Integrated CES service database credentials changed
Web RA Windows UserName/Password CEP service database credentials changed
Web RA Windows UserName/Password CES service database credentials changed
Web RA Windows SSL CES service database credentials changed
Web RA Windows SSL CES service database credentials changed
Changing database credentials process completed
```

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

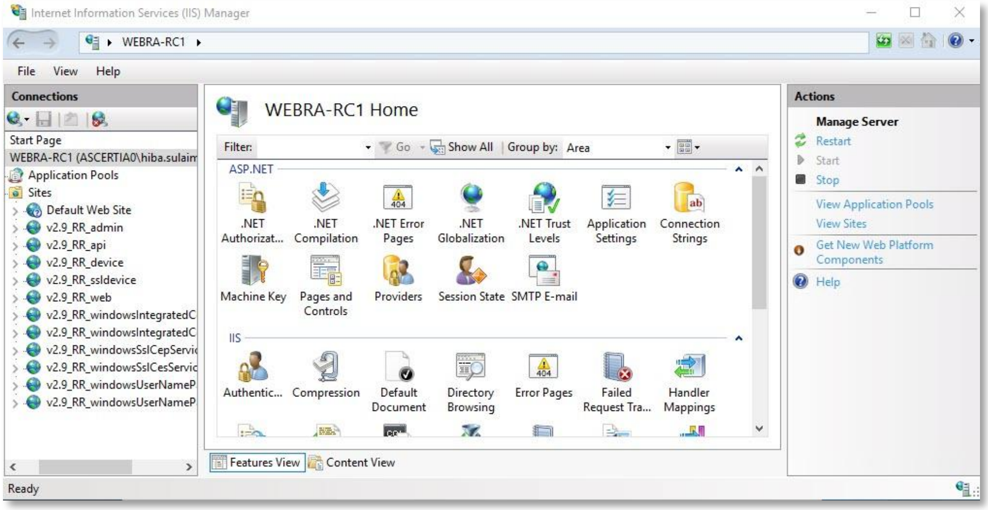
4.5 Regular Release Installation

***Note:** If you are upgrading from v2.9 to v2.9.7, ensure that your v2.9 deployment is functioning properly by accessing it in a browser.*

Note: The ‘Regular Release” installation type will only be available if ADSS Web RA was previously installed with Microsoft SQL Server database. This option is not available for PostgreSQL database, as it will be freshly supported starting from v2.9.7.

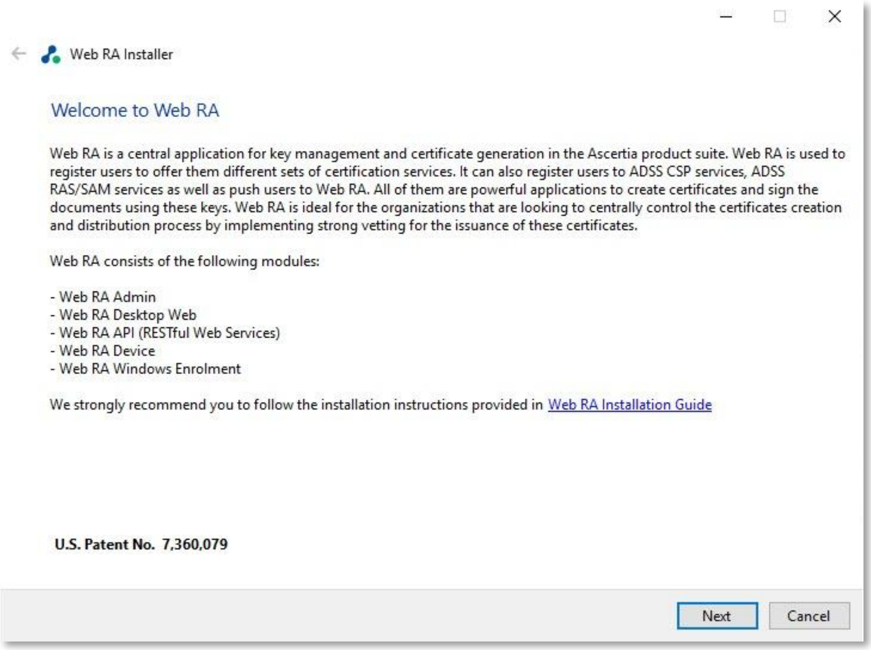
Follow the instructions below to install ADSS Web RA's regular release. Before starting the installation make sure that you have taken a backup of the Web RA database and have stopped the IIS Server.

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



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

The Welcome screen will appear:



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.

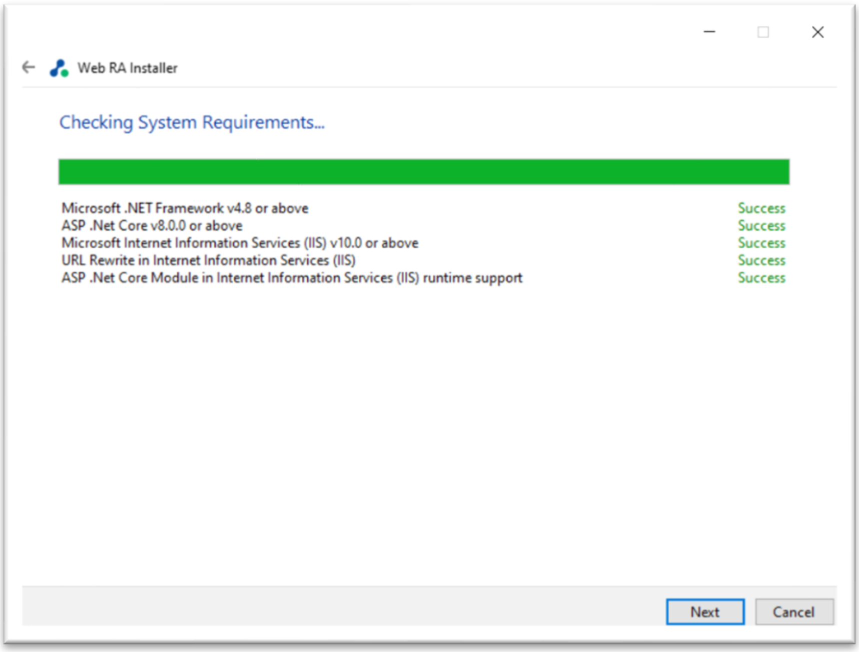
Web RA consists of the following modules:

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

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

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

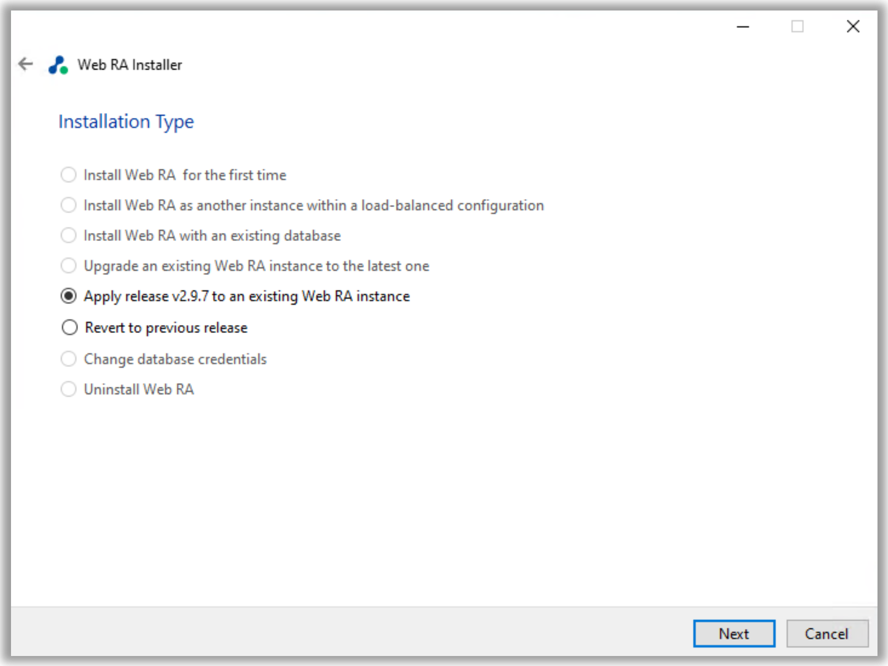
4.5.2 Click the Next button to continue. The system requirements screen will appear next to validate if all the required prerequisites are installed.



Checking System Requirements...

Microsoft .NET Framework v4.8 or above	Success
ASP .Net Core v8.0.0 or above	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) runtime support	Success

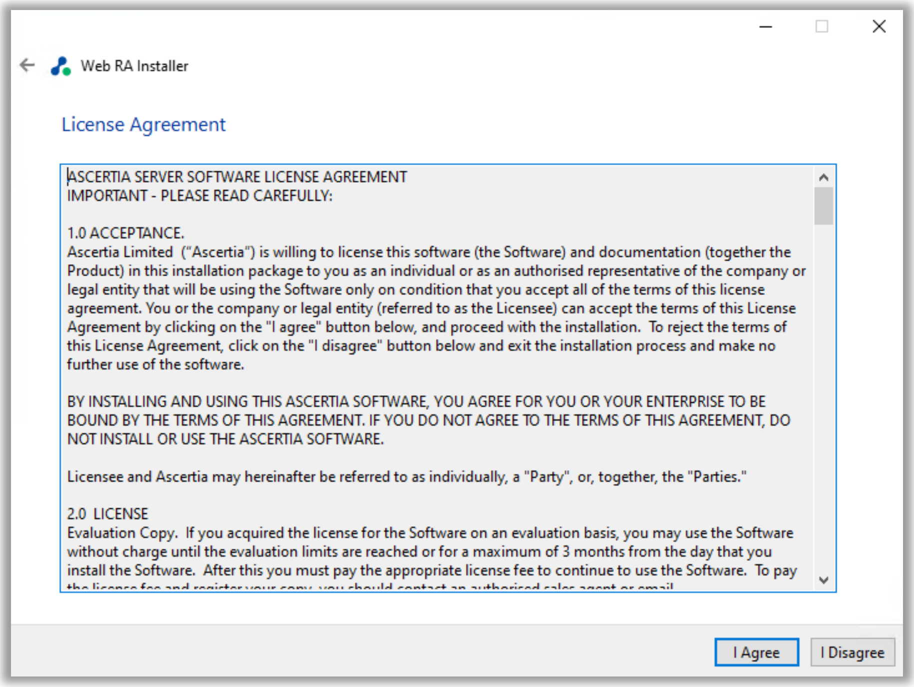
4.5.3 Click the Next button to show the Installation Type.



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
● Apply release v2.9.7 to an existing Web RA instance
○ Revert to previous release
○ Change database credentials
○ Uninstall Web RA

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



License Agreement

ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:

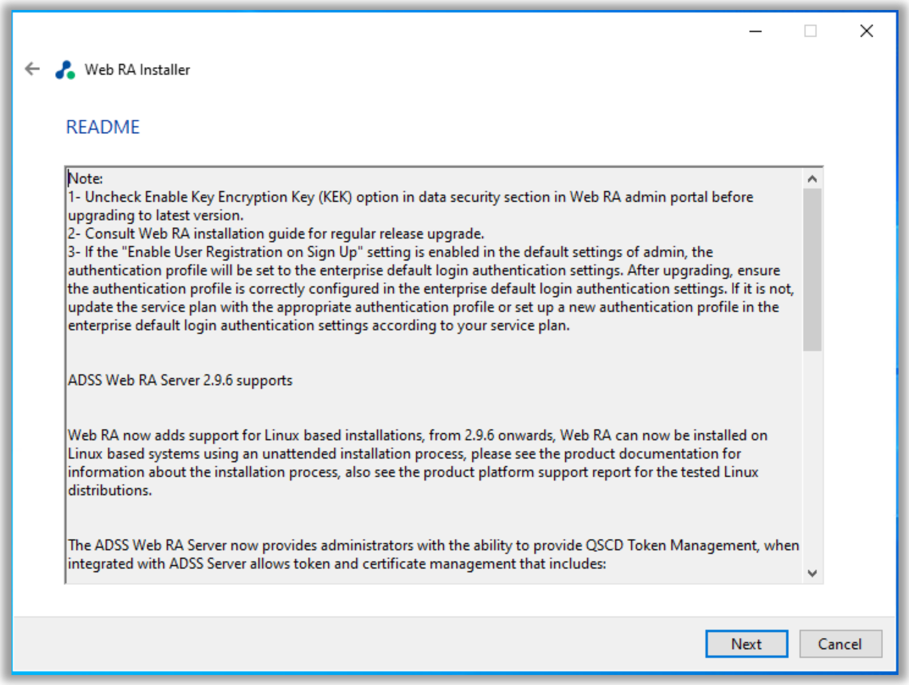
1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition 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

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



README

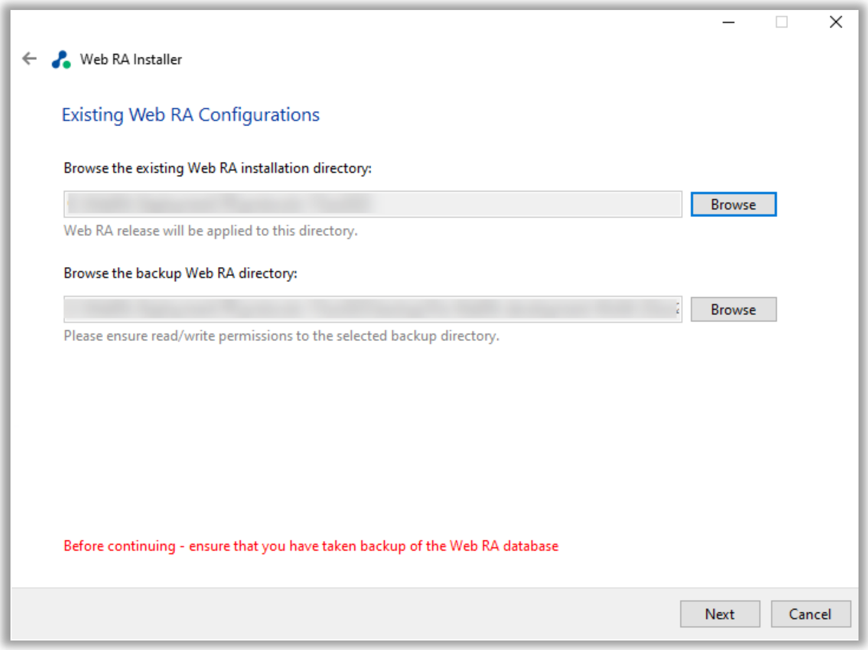
Note:
1- Uncheck Enable Key Encryption Key (KEK) option in data security section in Web RA admin portal before upgrading to latest version.
2- Consult Web RA installation guide for regular release upgrade.
3- If the "Enable User Registration on Sign Up" setting is enabled in the default settings of admin, the authentication profile will be set to the enterprise default login authentication settings. After upgrading, ensure the authentication profile is correctly configured in the enterprise default login authentication settings. If it is not, update the service plan with the appropriate authentication profile or set up a new authentication profile in the enterprise default login authentication settings according to your service plan.

ADSS Web RA Server 2.9.6 supports

Web RA now adds support for Linux based installations, from 2.9.6 onwards, Web RA can now be installed on Linux based systems using an unattended installation process, please see the product documentation for information about the installation process, also see the product platform support report for the tested Linux distributions.

The ADSS Web RA Server now provides administrators with the ability to provide QSCD Token Management, when integrated with ADSS Server allows token and certificate management that includes:

4.5.6 Click the Next button to provide the existing Web RA directory addresses.



Web RA Installer

Existing Web RA Configurations

Browse the existing Web RA installation directory:

[redacted]

Web RA release will be applied to this directory.

Browse the backup Web RA directory:

[redacted]

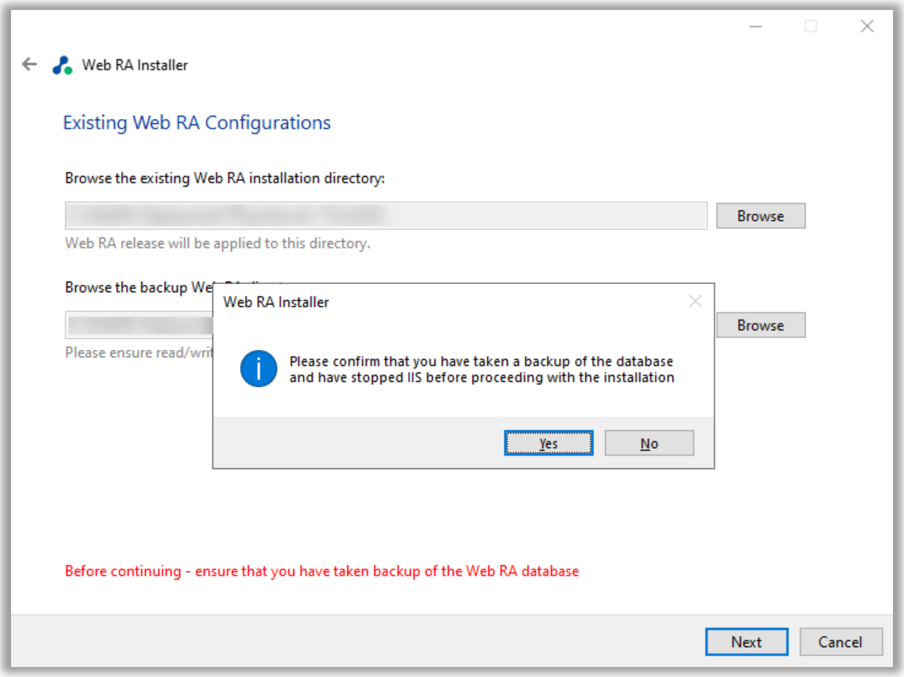
Please ensure read/write permissions to the selected backup directory.

Before continuing - ensure that you have taken backup of the Web RA database

Click the Browse button against the existing Web RA installation directory. Then click the Browse button against the backup Web RA directory, to browse to the addresses for the respective directories.

By default, when the existing Web RA installation directory address is selected, the installer will automatically create a backup Web RA folder and select it as backup directory. However, if the user wants to change the backup directory, they can click "Browse" and manually select the backup directory.

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



Web RA Installer

Existing Web RA Configurations

Browse the existing Web RA installation directory:

[redacted]

Web RA release will be applied to this directory.

Browse the backup We

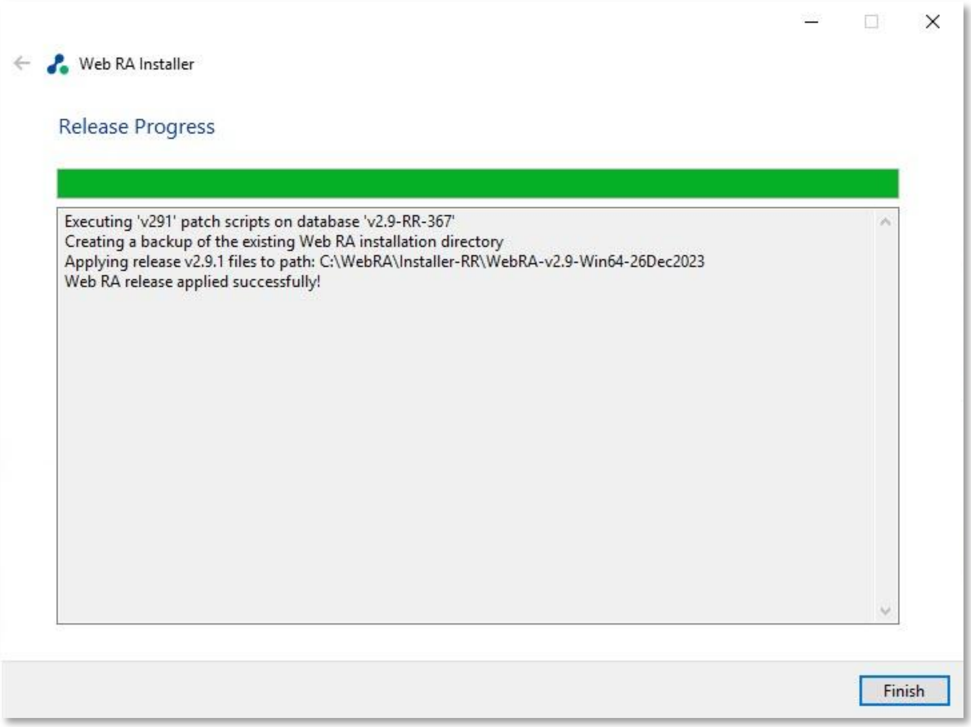
Please ensure read/wri

Web RA Installer

Please confirm that you have taken a backup of the database and have stopped IIS before proceeding with the installation

Before continuing - ensure that you have taken backup of the Web RA database

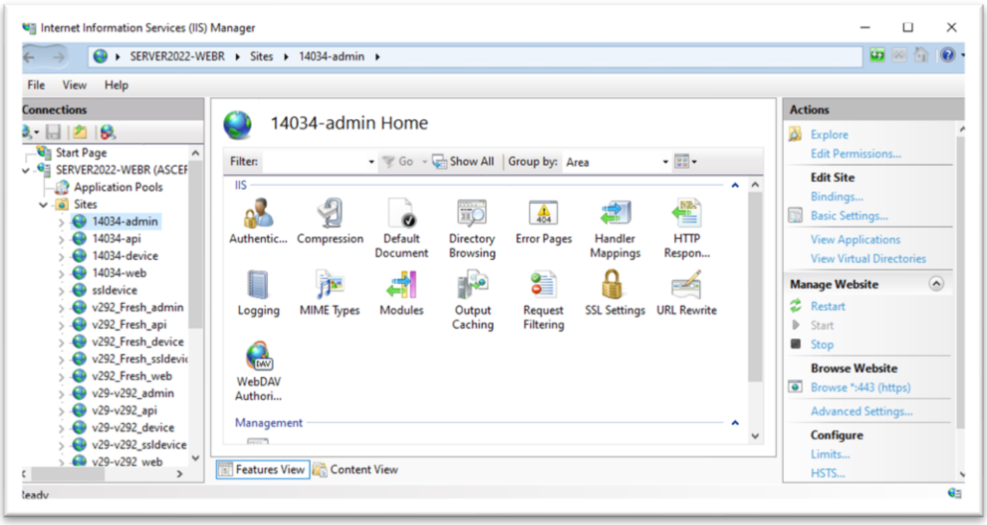
4.5.7 Click the Finish button to complete the installation process.



```
Executing 'v291' patch scripts on database 'v2.9-RR-367'
Creating a backup of the existing Web RA installation directory
Applying release v2.9.1 files to path: C:\WebRA\Installer-RR\WebRA-v2.9-Win64-26Dec2023
Web RA release applied successfully!
```

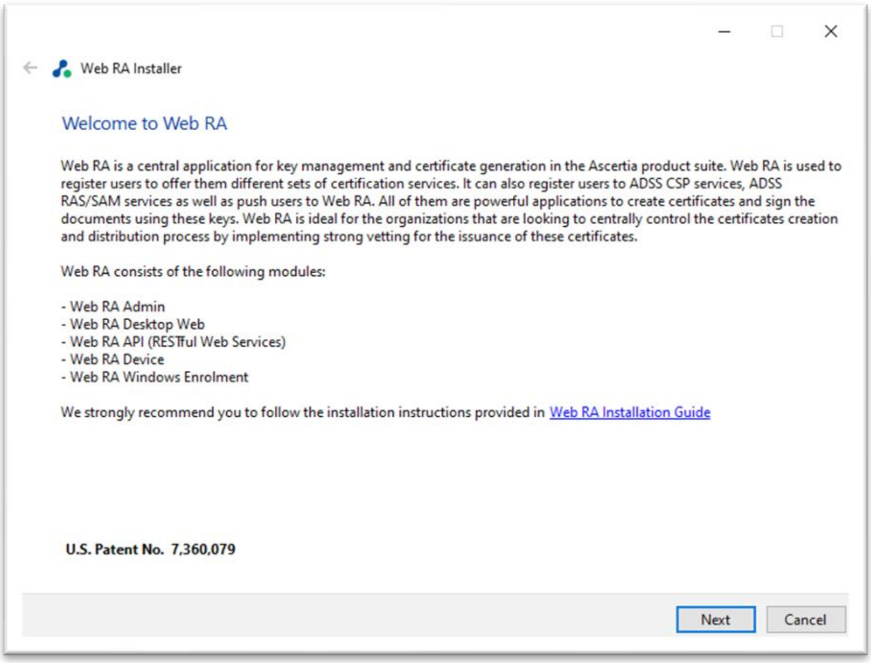
4.6 Uninstalling Regular Release

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



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

The Welcome screen will appear:



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.

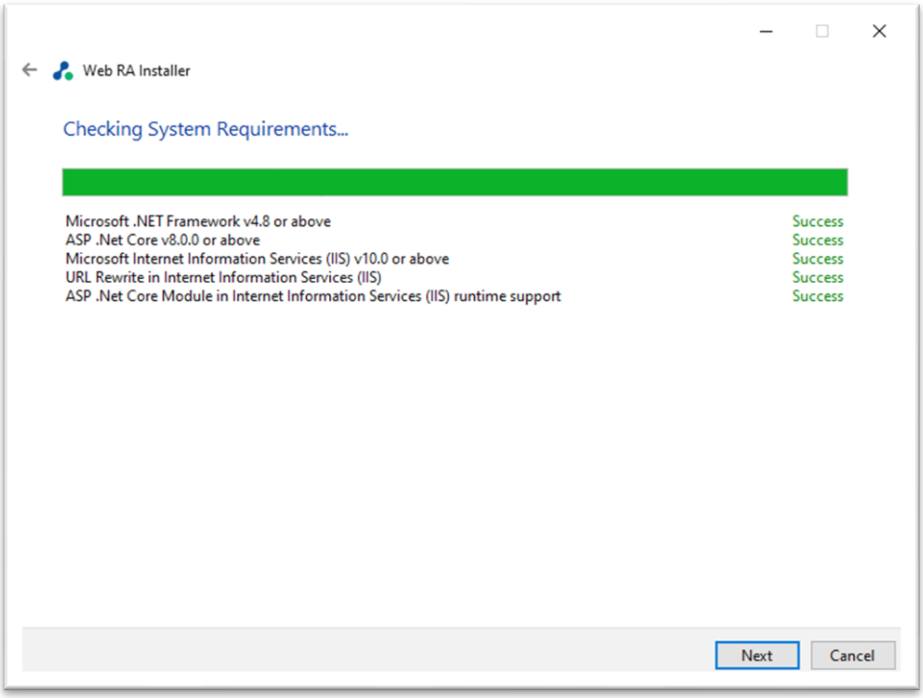
Web RA consists of the following modules:

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

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

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

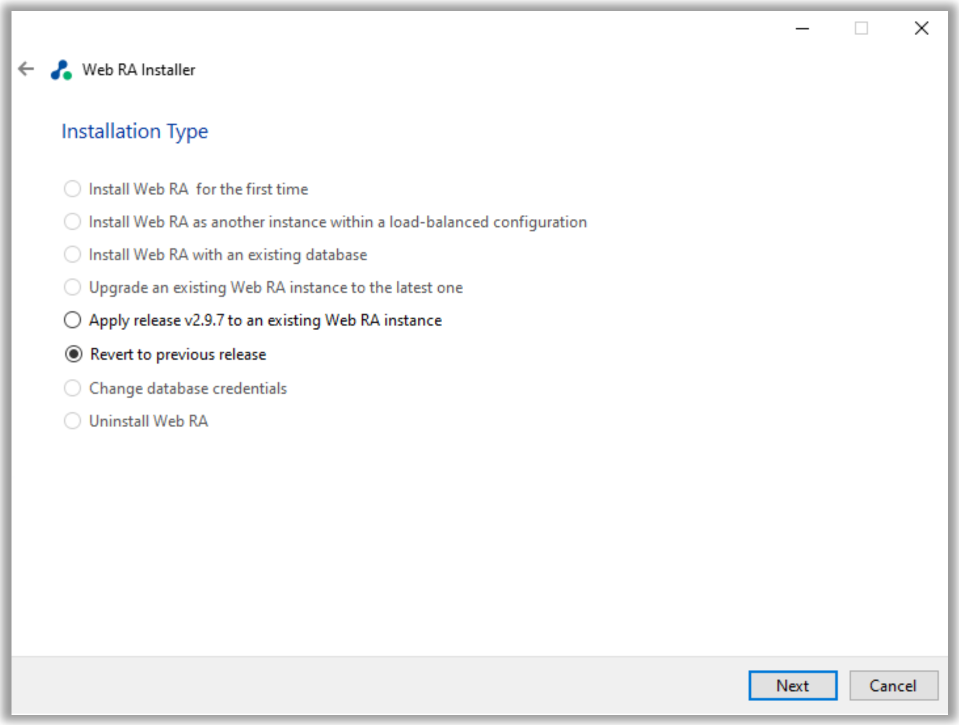
4.6.2 Click the Next button to continue. The system requirements screen will appear next to validate if all the required prerequisites are installed.



Checking System Requirements...

Microsoft .NET Framework v4.8 or above	Success
ASP .Net Core v8.0.0 or above	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) runtime support	Success

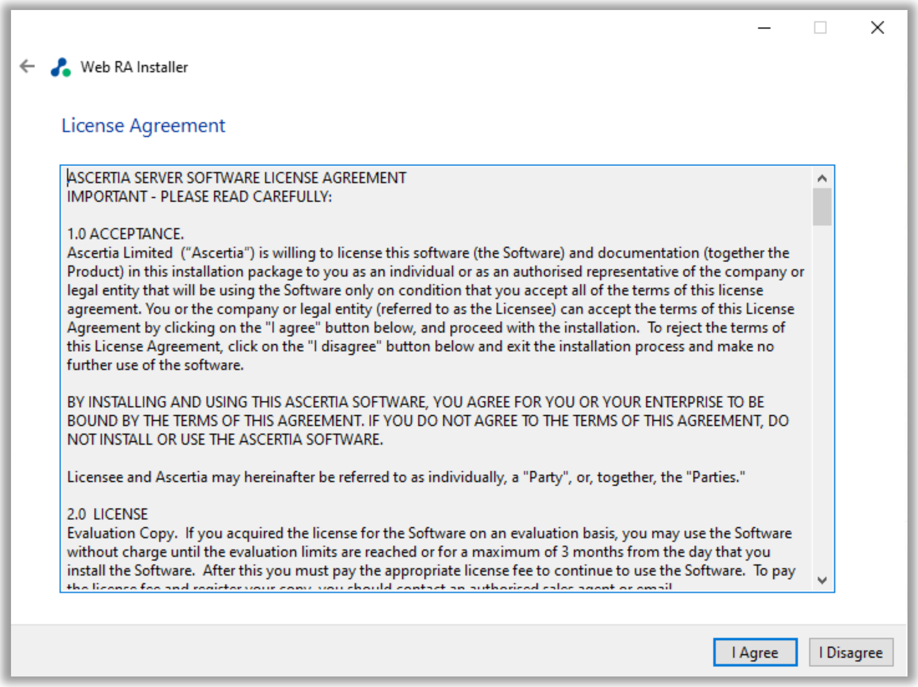
4.6.3 Click the Next button to select the “Revert to previous release” option.



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
○ Apply release v2.9.7 to an existing Web RA instance
● Revert to previous release
○ Change database credentials
○ Uninstall Web RA

4.6.4 The, click ‘Next’ button to view and accept the License Agreement.



License Agreement

ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:

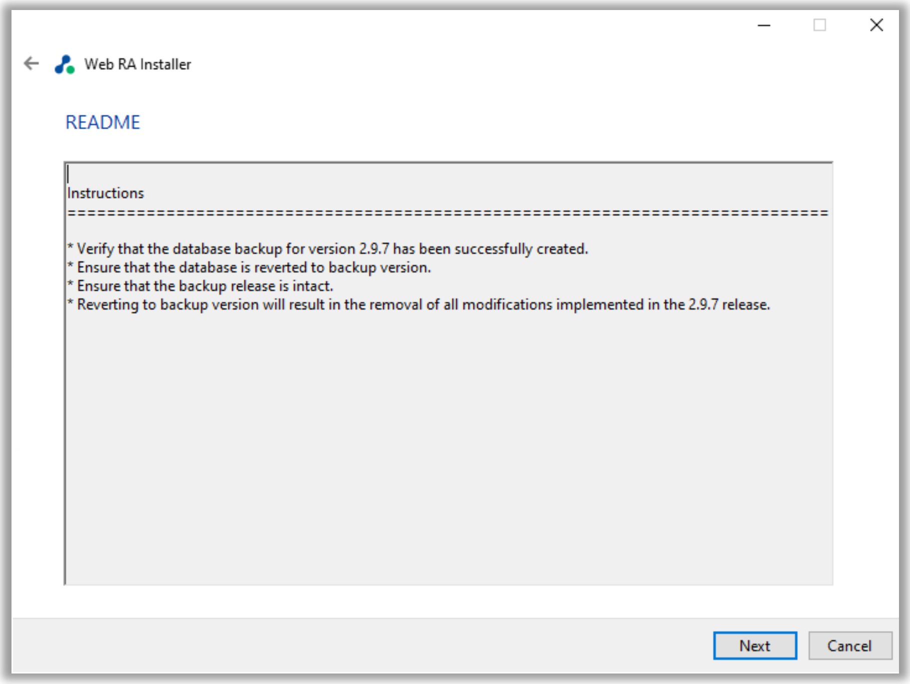
1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition 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

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

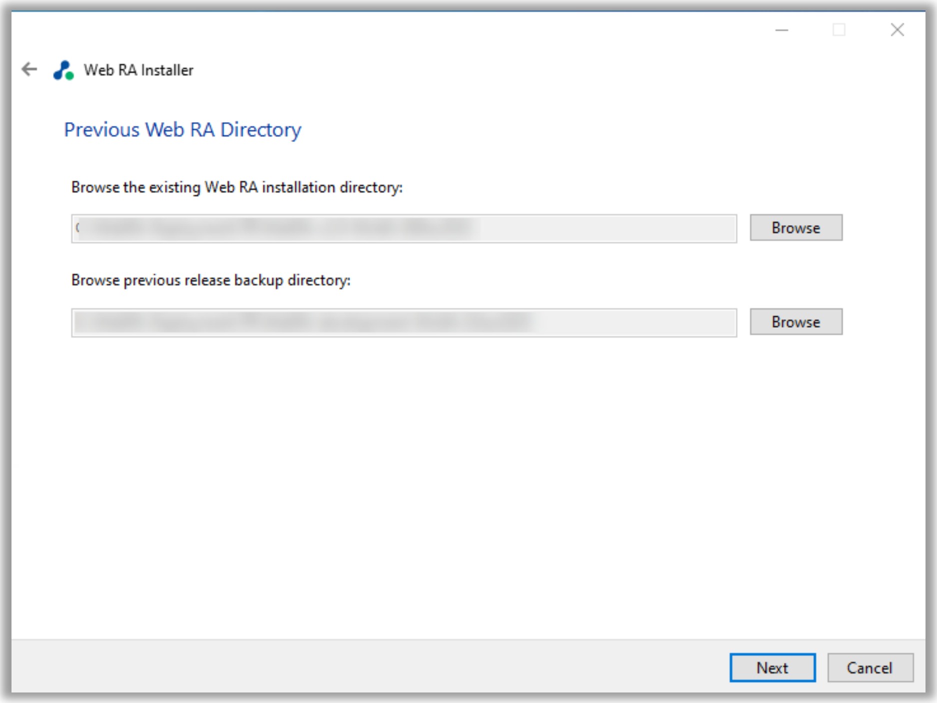


README

```
Instructions
================================================================================

* Verify that the database backup for version 2.9.7 has been successfully created.
* Ensure that the database is reverted to backup version.
* Ensure that the backup release is intact.
* Reverting to backup version will result in the removal of all modifications implemented in the 2.9.7 release.
```

4.6.6 Click the Next button to provide:

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

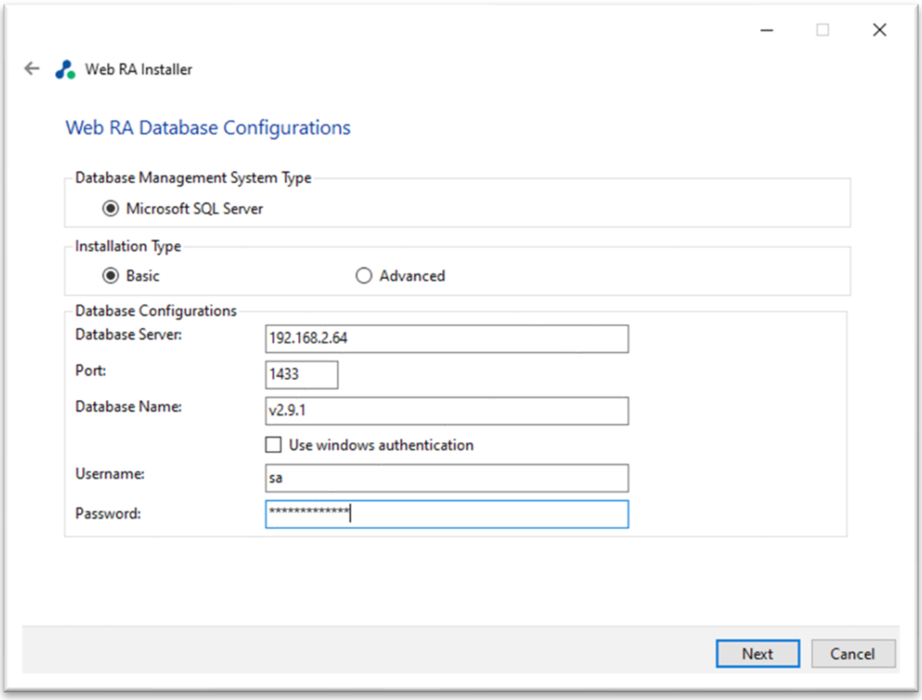


Previous Web RA Directory

Browse the existing Web RA installation directory: [redacted]

Browse previous release backup directory: [redacted]

4.6.7 Click next to view database details:



Web RA Database Configurations

Database Management System Type

● Microsoft SQL Server

Installation Type

● Basic ○ Advanced

Database Configurations

Database Server: 192.168.2.64

Port: 1433

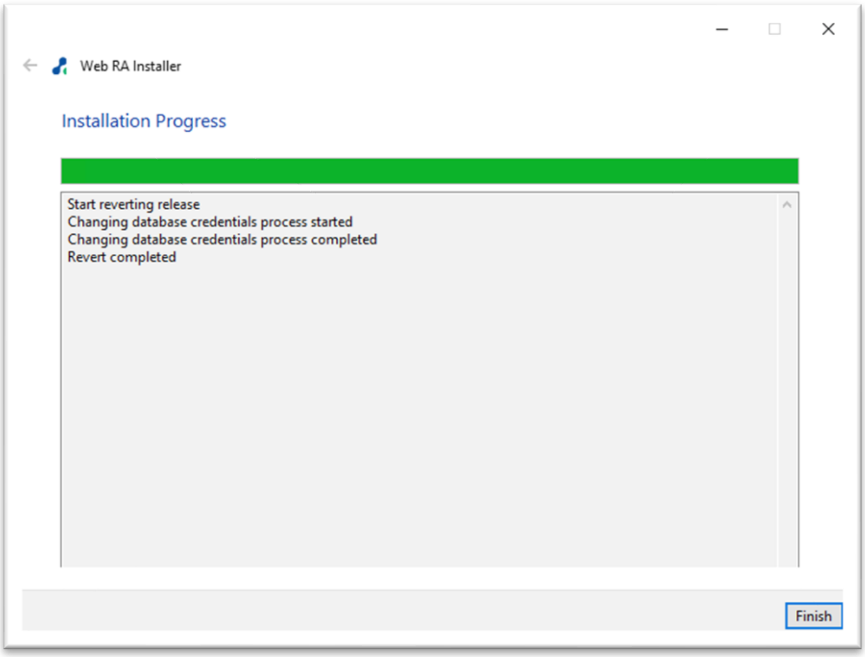
Database Name: v2.9.1

□ Use windows authentication

Username: sa

Password: *************

4.6.8 Click the Finish button to complete the installation process.



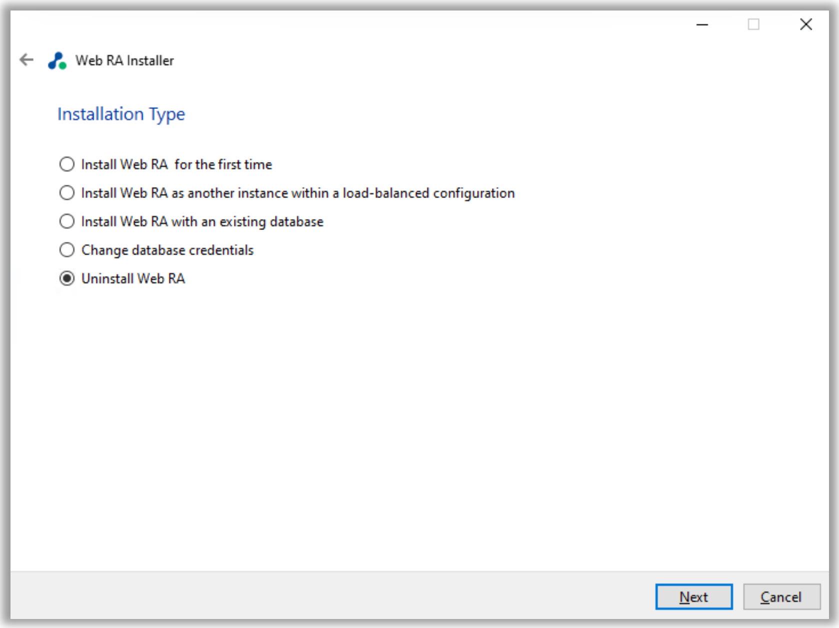
```
Start reverting release
Changing database credentials process started
Changing database credentials process completed
Revert completed
```

4.7 ADSS Web RA Uninstallation

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

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

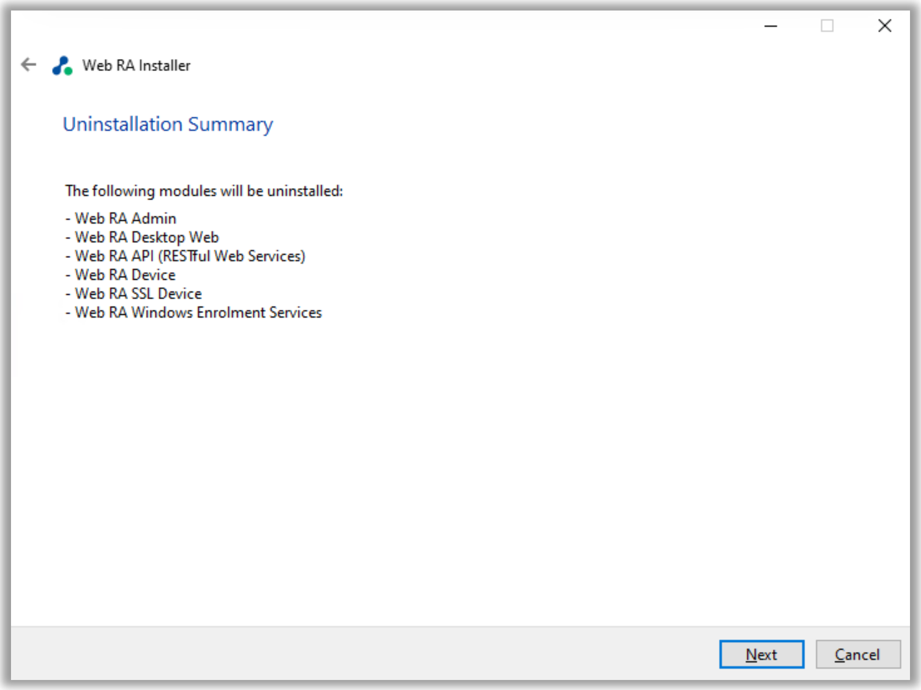
4.7.2 Follow the installation wizard until the Installation Type screen is shown.



○ 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
○ Change database credentials
● Uninstall Web RA

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

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

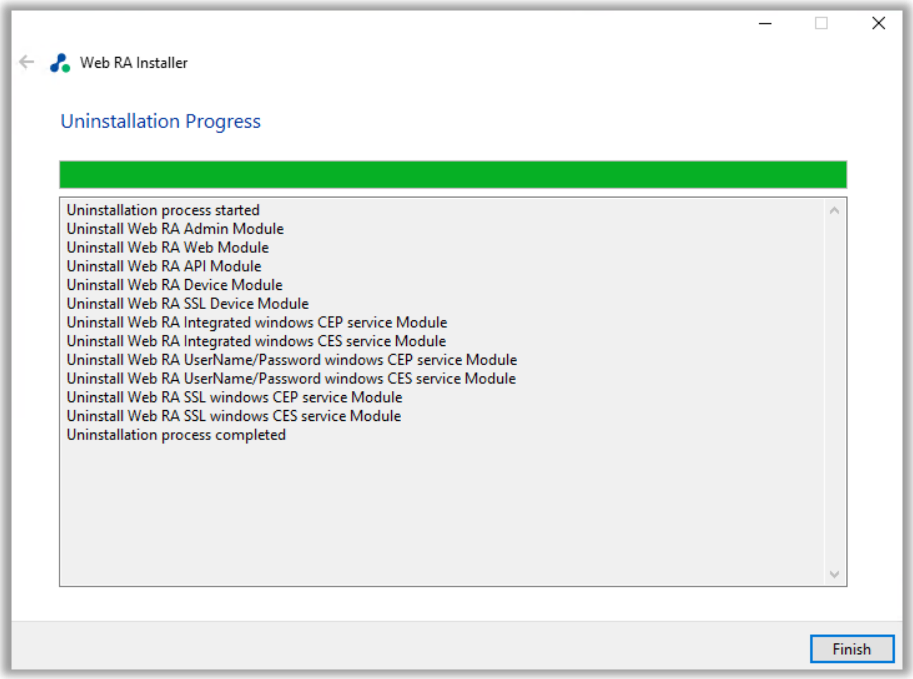


Uninstallation Summary

The following modules will be uninstalled:

- Web RA Admin
- Web RA Desktop Web
- Web RA API (RESTful Web Services)
- Web RA Device
- Web RA SSL Device
- Web RA Windows Enrolment Services

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



Uninstallation Progress

```
Uninstallation process started
Uninstall Web RA Admin Module
Uninstall Web RA Web Module
Uninstall Web RA API Module
Uninstall Web RA Device Module
Uninstall Web RA SSL Device Module
Uninstall Web RA Integrated windows CEP service Module
Uninstall Web RA Integrated windows CES service Module
Uninstall Web RA UserName/Password windows CEP service Module
Uninstall Web RA UserName/Password windows CES service Module
Uninstall Web RA SSL windows CEP service Module
Uninstall Web RA SSL windows CES service Module
Uninstallation process completed
```

4.7.5 Click the Finish button to complete the process.

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

5 ADSS Web RA Installation on Linux System

5.1 Prerequisites for Linux Installation

5.1.1 Install and Setup .Net Runtime 9

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

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

Installation

In your terminal, run the following command:

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

Verify Installation by running the following command:

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

5.1.2 Install and Setup Nginx

Source: nginx: Linux packages

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

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

- **Installing Nginx on AlmaLinux 9.**

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

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

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

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

- Configure Firewall.

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

- Accessing Nginx Web Interface

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

5.1.3 Install CIFS Utilities

The “cifs-utils” package is required for mounting shared folders using the CIFS (Common Internet File System) protocol. During installation, the absence of this package may cause interruptions or mounting errors.

To install "cifs-utils", run the following command:

```
sudo apt install cifs-utils
```

Ensure this package is installed on the Linux system before proceeding with the Web RA installation.

5.1.4 Java JRE Installation [Required for Certificate Signing Request (CSR) Verification]

Need to install the Java JRE latest version on Linux machine for CSR policy verifications during certificate creation.

The Java Runtime Environment (JRE) is required to support CSR policy checks when creating certificates through Web RA. Ensure OpenJDK 17 JRE is installed and properly configured on your Linux machine.

On Ubuntu:

1. Update your package list:

```
sudo apt update
```

2. Install OpenJDK 17 JRE:

```
sudo apt install openjdk-17-jre
```

3. Verify installation:

```
java -version
```

- Expected output should look like this:

```
openjdk version "17.0.x" ...
```

- Optional (if full JDK is needed):

```
sudo apt install openjdk-17-jdk
```

On AlmaLinux:

1. Update your package list:

```
sudo dnf update -y
```

2. Install OpenJDK 17 JRE:

```
sudo dnf install java-17-openjdk -y
```

3. Verify installation:

```
java -version
```

- Expected output should look like this:

```
openjdk version "17.0.x" ...
```

- Optional (if multiple Java versions are installed):

```
sudo alternatives --config java
```

You will be prompted to select the default version.

5.2 Pre-Installation Steps

5.2.1 Access the Root Directory

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

5.2.2 Locate the `/var` Folder

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

5.2.3 Check for the `www` Folder

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

If the www folder is not present:

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

5.2.4 Place the Installation Package

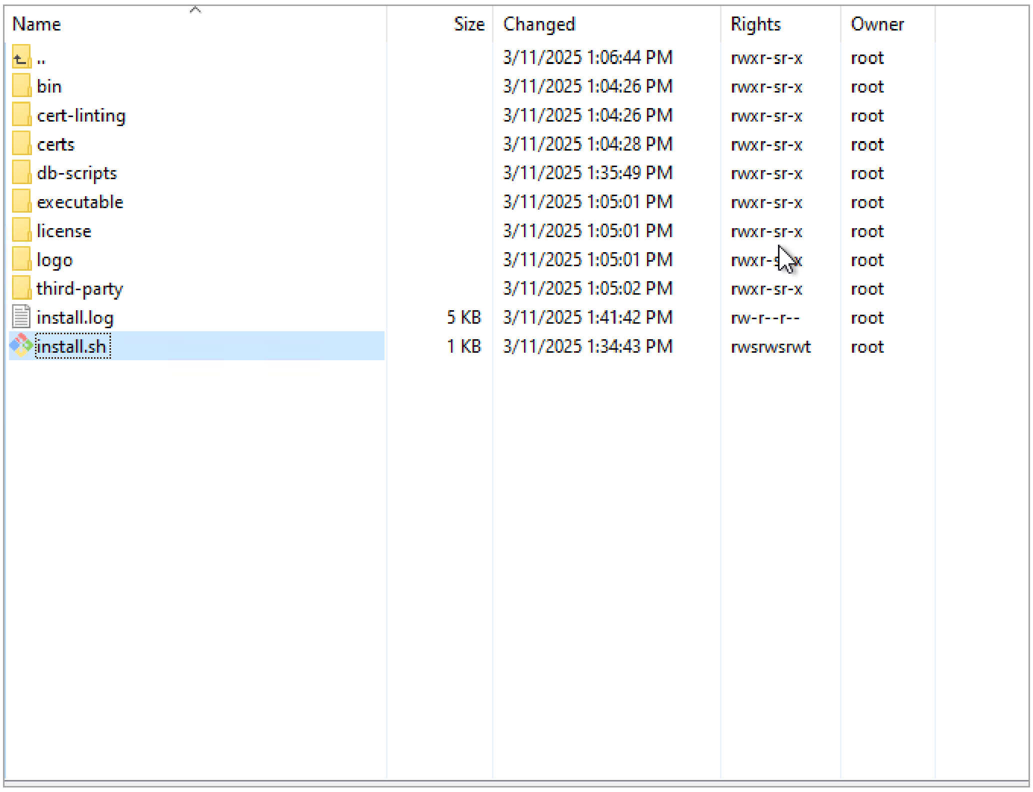
- Copy the extracted WebRA installation package into the /var/www/ directory.

5.2.5 Access the Installation Folder

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

5.2.6 Set Execution Permissions for the Installation Script

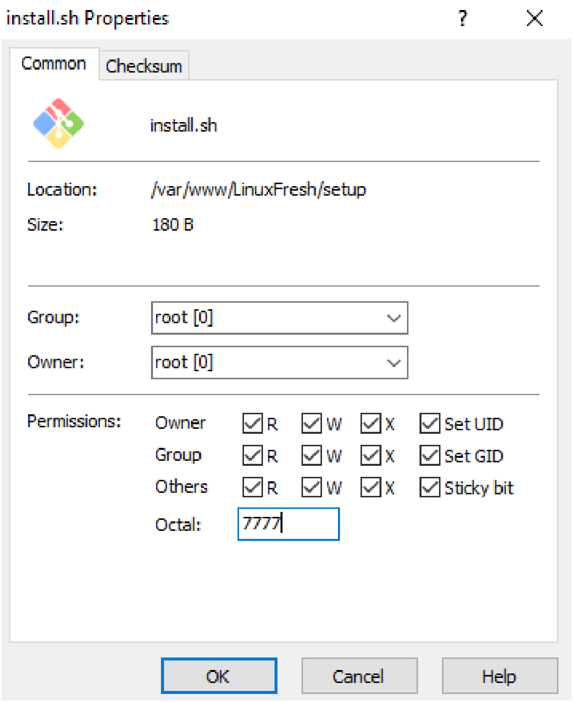
Before starting the installation, the install.sh file must have execution permissions enabled.



Name	Size	Changed	Rights	Owner
..		3/11/2025 1:06:44 PM	rwxr-sr-x	root
bin		3/11/2025 1:04:26 PM	rwxr-sr-x	root
cert-linting		3/11/2025 1:04:26 PM	rwxr-sr-x	root
certs		3/11/2025 1:04:28 PM	rwxr-sr-x	root
db-scripts		3/11/2025 1:35:49 PM	rwxr-sr-x	root
executable		3/11/2025 1:05:01 PM	rwxr-sr-x	root
license		3/11/2025 1:05:01 PM	rwxr-sr-x	root
logo		3/11/2025 1:05:01 PM	rwxr-sr-x	root
third-party		3/11/2025 1:05:02 PM	rwxr-sr-x	root
install.log	5 KB	3/11/2025 1:41:42 PM	rw-r--r--	root
install.sh	1 KB	3/11/2025 1:34:43 PM	rwsrwsrwt	root

To grant execution permissions:

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



install.sh Properties

install.sh

Location: /var/www/LinuxFresh/setup

Size: 180 B

Group: root [0]

Owner: root [0]

Permissions:

Owner	☑ R	☑ W	☑ X	☑ Set UID
Group	☑ R	☑ W	☑ X	☑ Set GID
Others	☑ R	☑ W	☑ X	☑ Sticky bit

Octal: 7777

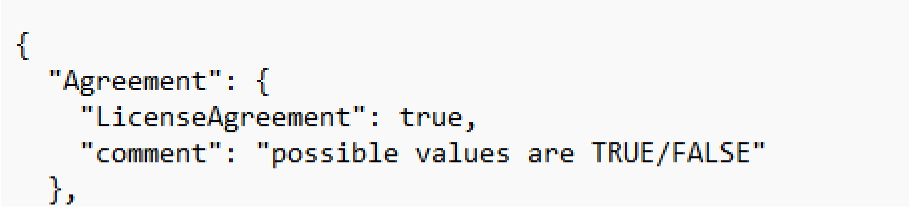
5.3 Configuring Installation Parameters in install.json file

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

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

5.3.1 Set Agreement Parameter

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



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

5.3.2 Installation Modes

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

Possible values:

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

1. Database and SMTP configuration details will not appear in the "install.json" file after the installation of Web RA is complete on the Linux machine.

2. If you are installing a regular release update, make sure to use the same site names and port numbers that were used during the original installation.

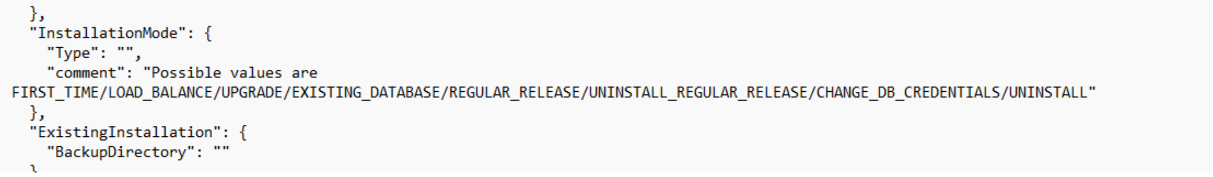
Note:

If you want to install Web RA with a PostgreSQL database, you must perform a fresh installation. The following installation modes are supported when using PostgreSQL:

- FIRST_TIME
- LOAD_BALANCE
- EXISTING_DATABASE
- CHANGE_DB_CREDENTIALS
- UNINSTALL

If you already have Web RA installed with an MSSQL database, the supported modes are:

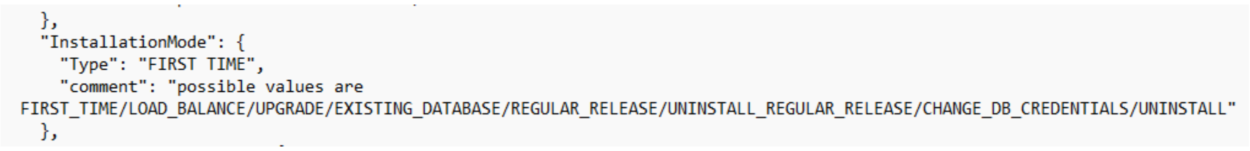
- REGULAR_RELEASE
- UNINSTALL_REGULAR_RELEASE



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

5.3.2.1 First Time Installation

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



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

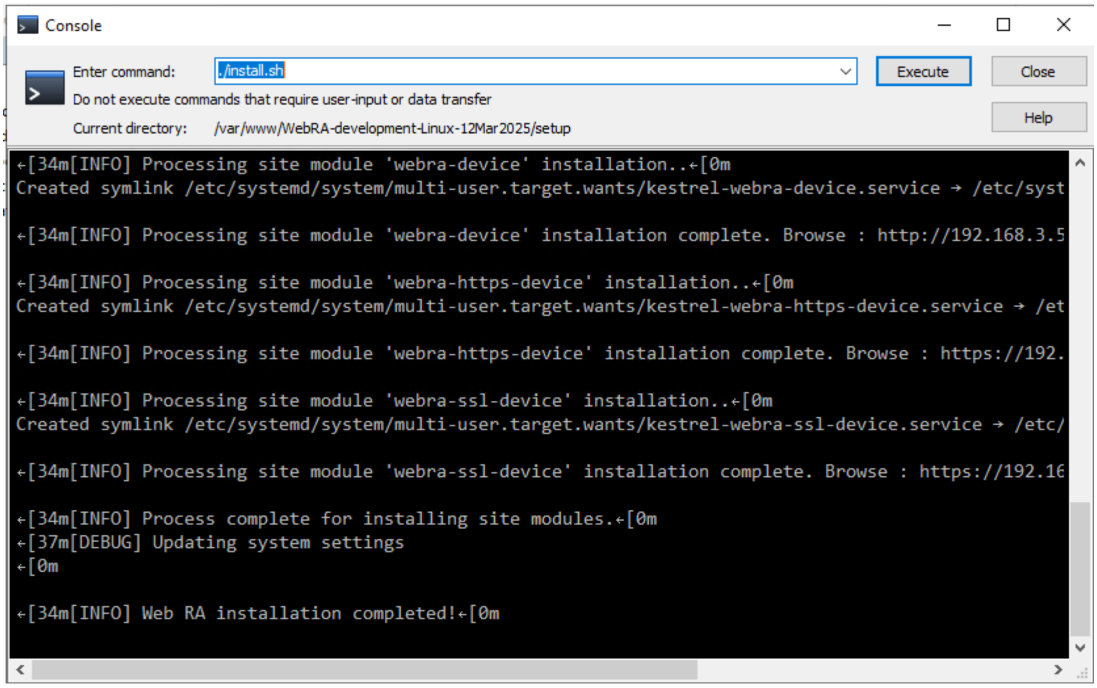
After setting the Type, save the file and close it. Then navigate to **the /var/www/LinuxFresh/setup/** folder and run the install.sh script.

***Note:** Before executing /install.sh, run the following commands:*

```
dos2unix install.sh

cat -A install.sh
```

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

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



Console
Enter command:
./install.sh
Execute
Close
Do not execute commands that require user-input or data transfer
Help
Current directory:
/var/www/WebRA-development-Linux-12Mar2025/setup

```
←[34m[INFO] Processing site module 'webra-device' installation..←[0m
Created symlink /etc/systemd/system/multi-user.target.wants/kestrel-webra-device.service → /etc/syst

←[34m[INFO] Processing site module 'webra-device' installation complete. Browse : http://192.168.3.5

←[34m[INFO] Processing site module 'webra-https-device' installation..←[0m
Created symlink /etc/systemd/system/multi-user.target.wants/kestrel-webra-https-device.service → /et

←[34m[INFO] Processing site module 'webra-https-device' installation complete. Browse : https://192.

←[34m[INFO] Processing site module 'webra-ssl-device' installation..←[0m
Created symlink /etc/systemd/system/multi-user.target.wants/kestrel-webra-ssl-device.service → /etc/

←[34m[INFO] Processing site module 'webra-ssl-device' installation complete. Browse : https://192.16

←[34m[INFO] Process complete for installing site modules.←[0m
←[37m[DEBUG] Updating system settings
←[0m

←[34m[INFO] Web RA installation completed!←[0m
```

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

5.3.2.2 Installing in Load Balanced Mode

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

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

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

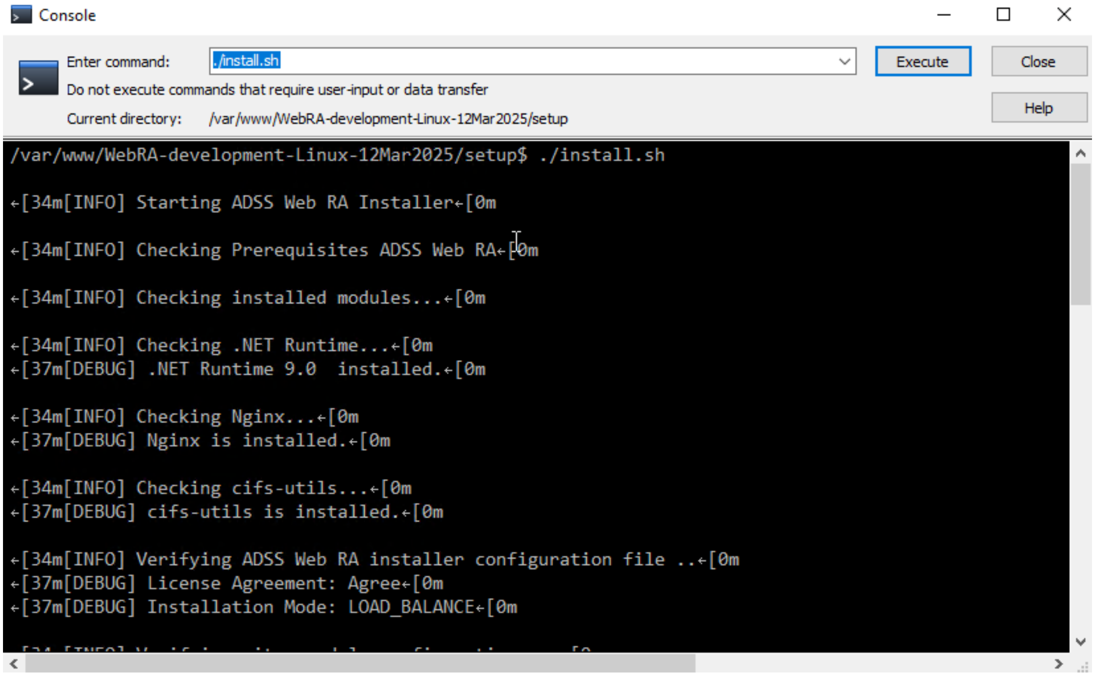
Note: *Before executing /install.sh, run the following commands:*

```
dos2unix install.sh
```

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

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

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



Enter command: ./install.sh

Do not execute commands that require user-input or data transfer

Current directory: /var/www/WebRA-development-Linux-12Mar2025/setup

```
/var/www/WebRA-development-Linux-12Mar2025/setup$ ./install.sh

←[34m[INFO] Starting ADSS Web RA Installer←[0m

←[34m[INFO] Checking Prerequisites ADSS Web RA←[0m

←[34m[INFO] Checking installed modules...←[0m

←[34m[INFO] Checking .NET Runtime...←[0m
←[37m[DEBUG] .NET Runtime 9.0  installed.←[0m

←[34m[INFO] Checking Nginx...←[0m
←[37m[DEBUG] Nginx is installed.←[0m

←[34m[INFO] Checking cifs-utils...←[0m
←[37m[DEBUG] cifs-utils is installed.←[0m

←[34m[INFO] Verifying ADSS Web RA installer configuration file ..←[0m
←[37m[DEBUG] License Agreement: Agree←[0m
←[37m[DEBUG] Installation Mode: LOAD_BALANCE←[0m
```

5.3.2.3 Installing Web RA with an Existing Database

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

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

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

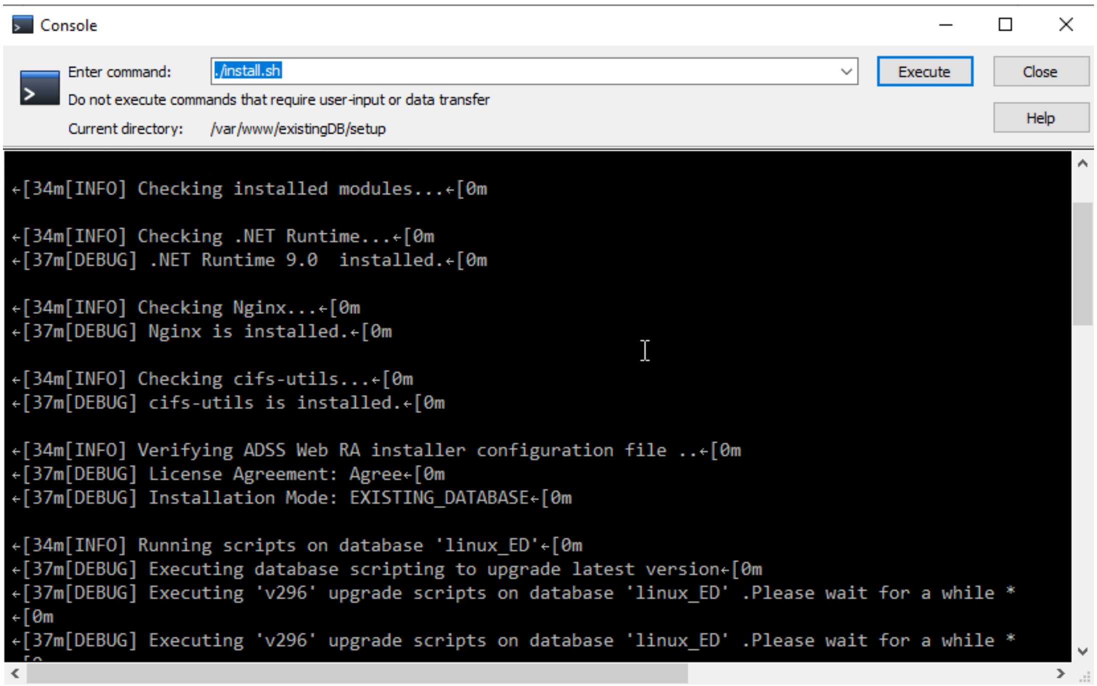
Note: *Before executing /install.sh, run the following commands:*

```
dos2unix install.sh
```

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

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

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



Enter command: ./install.sh

Do not execute commands that require user-input or data transfer

Current directory: /var/www/existingDB/setup

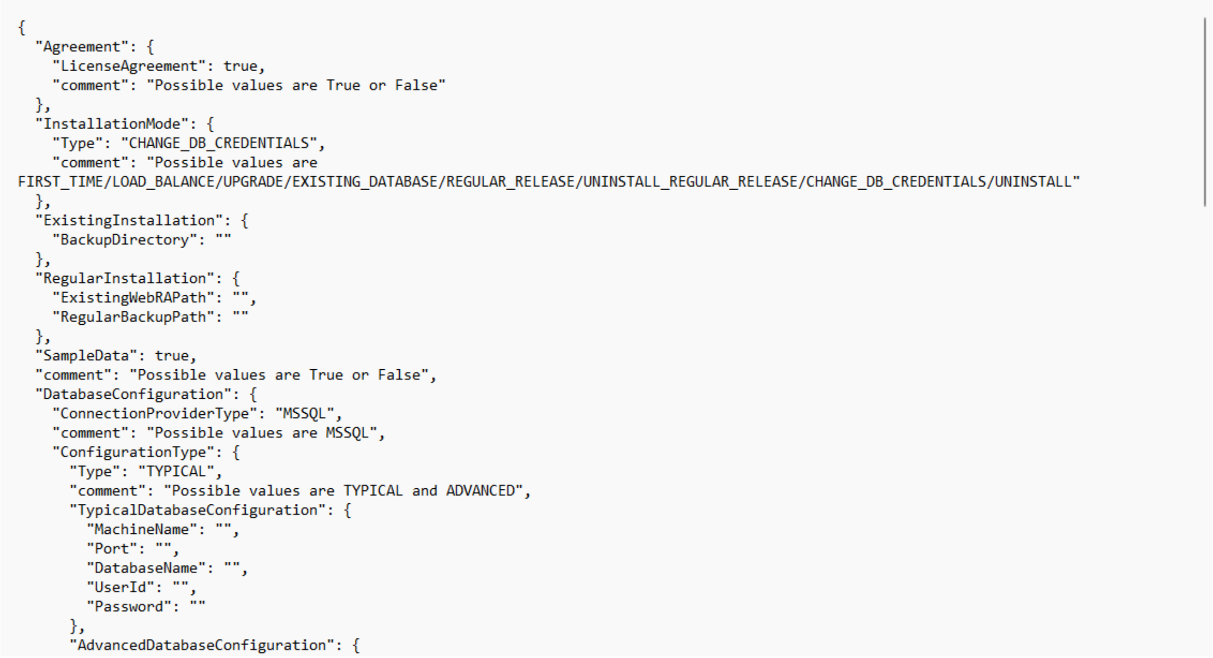
```
←[34m[INFO] Checking installed modules...←[0m

←[34m[INFO] Checking .NET Runtime...←[0m
←[37m[DEBUG] .NET Runtime 9.0  installed.←[0m

←[34m[INFO] Checking Nginx...←[0m
←[37m[DEBUG] Nginx is installed.←[0m

←[34m[INFO] Checking cifs-utils...←[0m
←[37m[DEBUG] cifs-utils is installed.←[0m

←[34m[INFO] Verifying ADSS Web RA installer configuration file ..←[0m
←[37m[DEBUG] License Agreement: Agree←[0m
←[37m[DEBUG] Installation Mode: EXISTING_DATABASE←[0m

←[34m[INFO] Running scripts on database 'linux_ED'←[0m
←[37m[DEBUG] Executing database scripting to upgrade latest version←[0m
←[37m[DEBUG] Executing 'v296' upgrade scripts on database 'linux_ED' .Please wait for a while *
←[0m
←[37m[DEBUG] Executing 'v296' upgrade scripts on database 'linux_ED' .Please wait for a while *
```

5.3.2.4 Changing Database Credentials in Web RA

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

- ConnectionProviderType
- MachineName
- Port
- Authentication
- UserId
- Password

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



```
{
  "Agreement": {
    "LicenseAgreement": true,
    "comment": "Possible values are True or False"
  },
  "InstallationMode": {
    "Type": "CHANGE_DB_CREDENTIALS",
    "comment": "Possible values are
FIRST_TIME/LOAD_BALANCE/UPGRADE/EXISTING_DATABASE/REGULAR_RELEASE/UNINSTALL_REGULAR_RELEASE/CHANGE_DB_CREDENTIALS/UNINSTALL"
  },
  "ExistingInstallation": {
    "BackupDirectory": ""
  },
  "RegularInstallation": {
    "ExistingWebRAPath": "",
    "RegularBackupPath": ""
  },
  "SampleData": true,
  "comment": "Possible values are True or False",
  "DatabaseConfiguration": {
    "ConnectionProviderType": "MSSQL",
    "comment": "Possible values are MSSQL",
    "ConfigurationType": {
      "Type": "TYPICAL",
      "comment": "Possible values are TYPICAL and ADVANCED",
      "TypicalDatabaseConfiguration": {
        "MachineName": "",
        "Port": "",
        "DatabaseName": "",
        "UserId": "",
        "Password": ""
      },
      "AdvancedDatabaseConfiguration": {
```

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

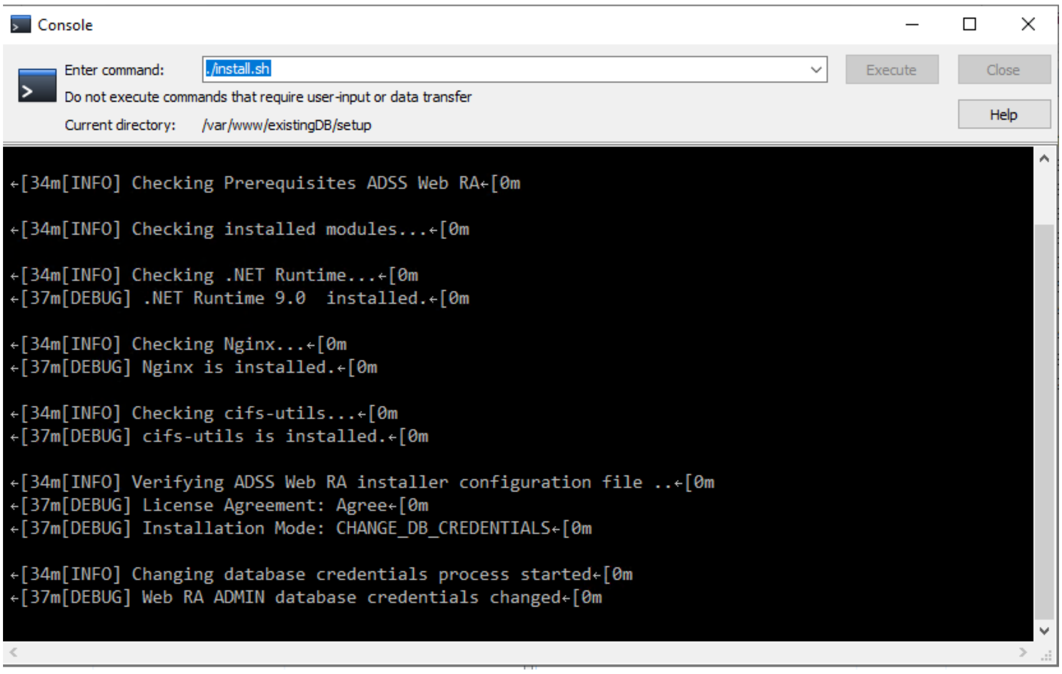
Note: *Before executing /install.sh, run the following commands:*

```
dos2unix install.sh
```

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

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

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



Enter command: ./install.sh

Do not execute commands that require user-input or data transfer

Current directory: /var/www/existingDB/setup

```
←[34m[INFO] Checking Prerequisites ADSS Web RA←[0m

←[34m[INFO] Checking installed modules...←[0m

←[34m[INFO] Checking .NET Runtime...←[0m
←[37m[DEBUG] .NET Runtime 9.0  installed.←[0m

←[34m[INFO] Checking Nginx...←[0m
←[37m[DEBUG] Nginx is installed.←[0m

←[34m[INFO] Checking cifs-utils...←[0m
←[37m[DEBUG] cifs-utils is installed.←[0m

←[34m[INFO] Verifying ADSS Web RA installer configuration file ..←[0m
←[37m[DEBUG] License Agreement: Agree←[0m
←[37m[DEBUG] Installation Mode: CHANGE_DB_CREDENTIALS←[0m

←[34m[INFO] Changing database credentials process started←[0m
←[37m[DEBUG] Web RA ADMIN database credentials changed←[0m
```

5.3.3 Existing Installation Parameter

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

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

5.3.4 Regular Installation Parameter

- **ExistingWebRAPath**: Specifies the file path where the currently installed Web RA instance is located. **For example:** existing installation directory/.
- **RegularBackupPath**: Directory where a backup of the current Web RA instance will be stored before installation. **For example:** existing directory/backup directory/.

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

5.3.5 Sample Data

- If set to **True**, the installation will include sample data to help with testing and initial configuration. The following items will be included in the sample data:
    - Default ADSS Connector
    - Default SMTP Connector
    - Default ADSS Service Profile
    - Default Subscriber Agreement
    - Default Vetting Form
    - Default Service Plan
    - Default Authentication Profile
- If set to **False**, the installation will proceed without adding sample data and you will have to create everything by scratch.

5.3.5.1 Database Configuration

- **ConnectionProviderType**:

Defines the type of database server that Web RA will connect to.

- **Possible values:**
    - **MSSQL** — Use Microsoft SQL Server as the database.
    - **PGSQL** — Use PostgreSQL as the database.
- **ConfigurationType**:

Specifies how the database connection will be configured during installation.

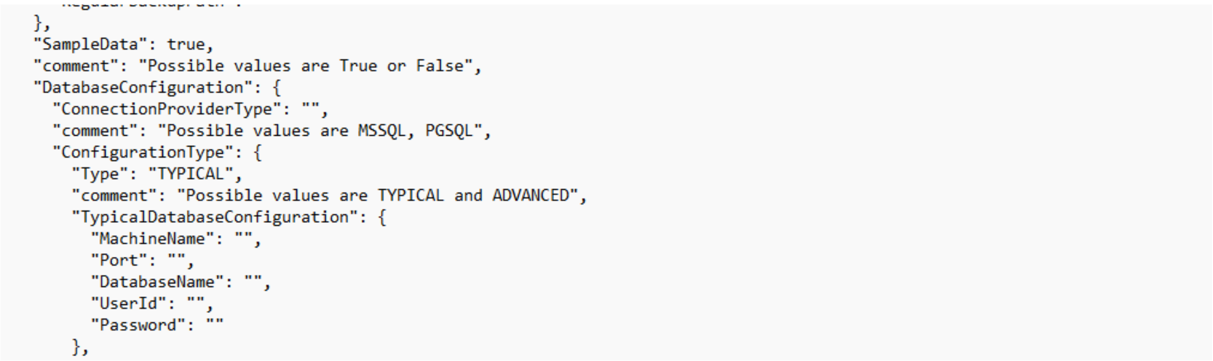
- **Possible values:**
    - **TYPICAL** — Uses default, commonly required settings with minimal manual input.
    - **ADVANCED** — Allows manual editing of the full database connection string or additional custom settings.

Note: *You must choose either **Typical** or **Advanced** configuration. Both cannot be used at the same time.*

5.3.5.1.1 Typical Database Configuration

When you choose TYPICAL as the configuration type, you need to provide the following details:

Machine Name	The hostname or IP address of the database server that will host the Web RA database
Port	The port number used for connecting to the database. • For Microsoft SQL Server the default port is 1433 • For PostgreSQL Server the default port is 5432
Database Name	The name of the database to be created or used by Web RA
UserId	The database username that Web RA will use to authenticate and connect to the database.
Password	The password for database authentication.



```
  },
  "SampleData": true,
  "comment": "Possible values are True or False",
  "DatabaseConfiguration": {
    "ConnectionProviderType": "",
    "comment": "Possible values are MSSQL, PGSQL",
    "ConfigurationType": {
      "Type": "TYPICAL",
      "comment": "Possible values are TYPICAL and ADVANCED",
      "TypicalDatabaseConfiguration": {
        "MachineName": "",
        "Port": "",
        "DatabaseName": "",
        "UserId": "",
        "Password": ""
      },
```

5.3.6 Advanced Database Configuration

This option allows you to provide a custom connection string for full control over how Web RA connects to your database. Use this if you need to define specific connection parameters beyond what the "Typical" configuration allows.

Supported database types:

- **MSSQL**
- **PGSQL**

Below are example connection strings for each supported database:

Example for MSSQL Authentication

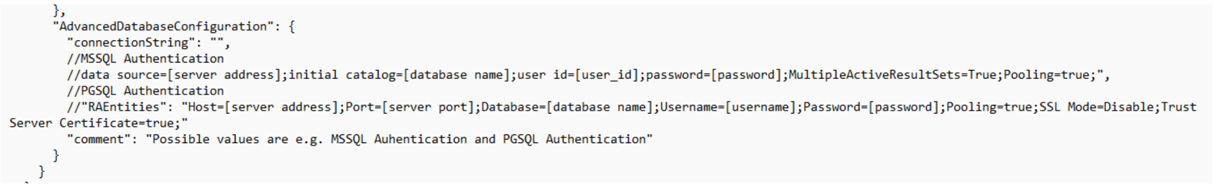
data source=[server address];initial catalog=[database name];user id=[user_id];password=[password];MultipleActiveResultSets=True;Pooling=true;

Example for PGSQL Authentication

Host=[server address];Port=[server port];Database=[database name];Username=[username];Password=[password];Pooling=true;SSL Mode=Disable;Trust Server Certificate=true;

Note:

Make sure to replace the placeholders (e.g., [server address], [database name], [username], [password]) with the actual details for your database server.



```
      },
      "AdvancedDatabaseConfiguration": {
        "connectionString": "",
        //MSSQL Authentication
        //data source=[server address];initial catalog=[database name];user id=[user_id];password=[password];MultipleActiveResultSets=True;Pooling=true;",
        //PGSQL Authentication
        //"RAEntities": "Host=[server address];Port=[server port];Database=[database name];Username=[username];Password=[password];Pooling=true;SSL Mode=Disable;Trust
Server Certificate=true;"
        "comment": "Possible values are e.g. MSSQL Auhentication and PGSQL Authentication"
      }
    }
```

5.3.7 Custom Installation Parameter

Defines the modules to be installed and their respective configurations.

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

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

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

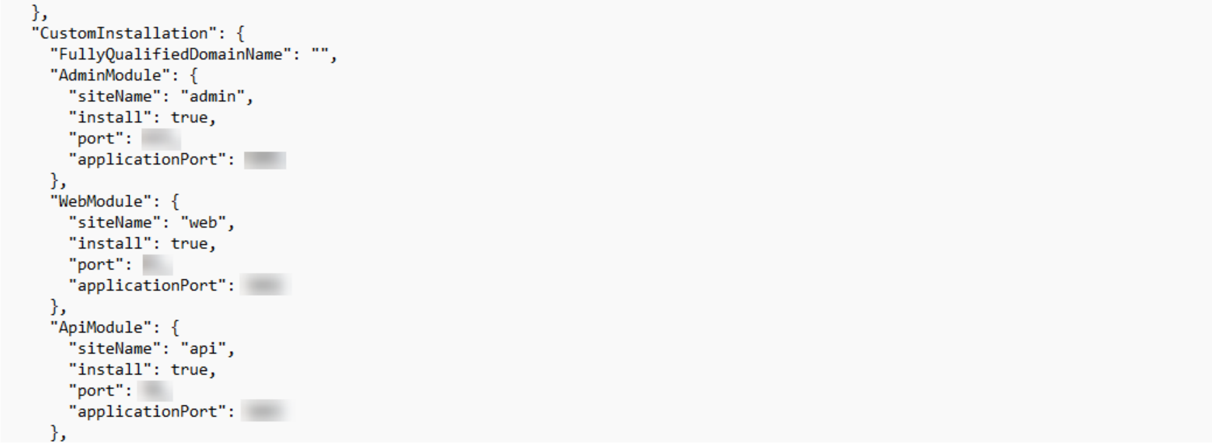
- **WebModule**:
  - Site name: web
  - Install: true
  - Port: “Port Number”
  - Application Port: “Port Number”

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

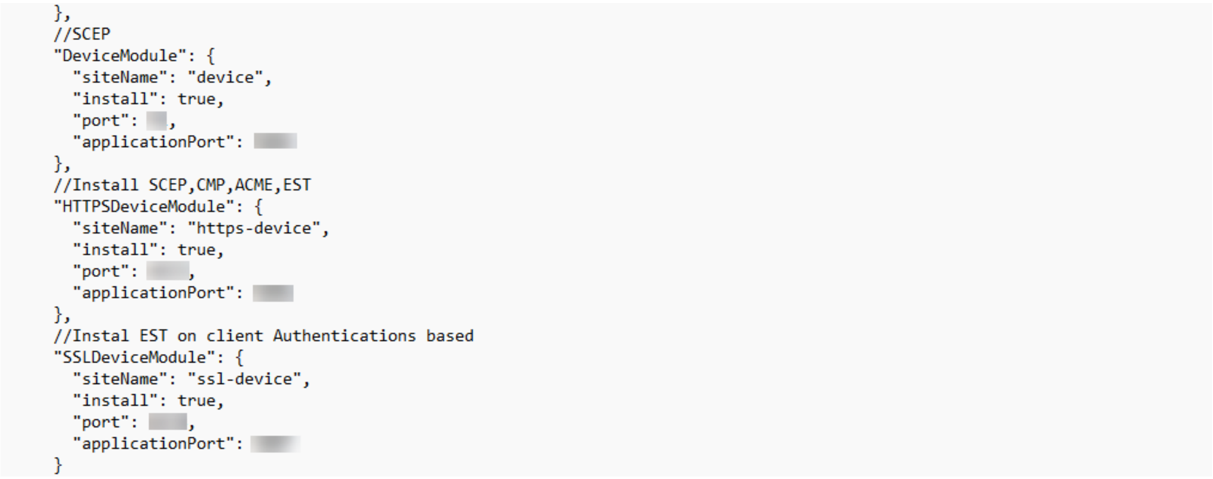
- **DeviceModule** (SCEP support):
  - Site name: device
  - Install: true
  - Port: “Port Number”
  - Application Port: “Port Number”

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

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



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



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

5.3.7.1 Port Usage Guidelines

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

Constraints

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

5.3.7.2 Allowing Ports on Ubuntu

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

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

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

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

To verify the firewall status:

```
sudo ufw status
```

5.3.7.3 Allowing Ports on AlmaLinux

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

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

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

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

After making changes, reload the firewall settings:

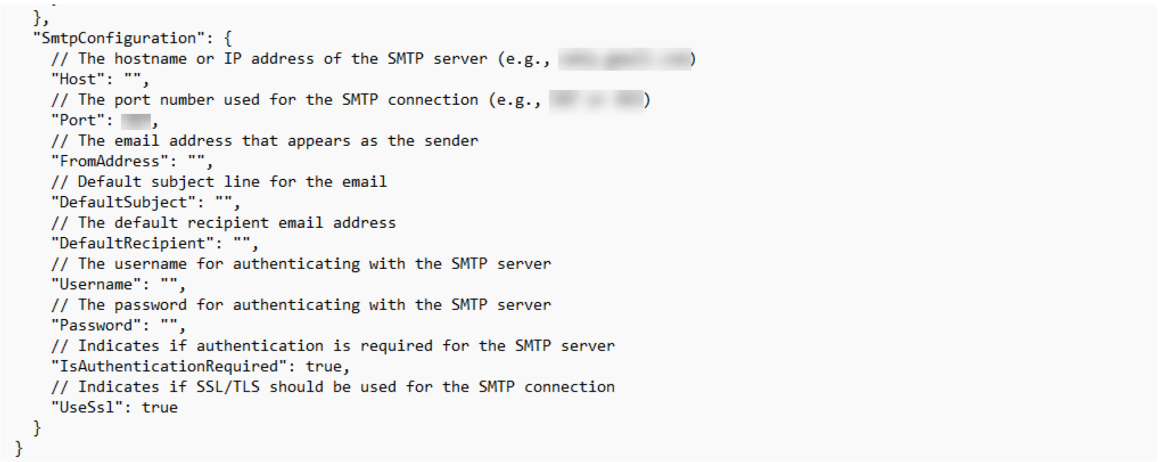
```
sudo firewall-cmd –reload
```

5.3.8 SMPT Configuration

Defines email settings for notifications:

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

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



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

After configuring all necessary parameters in the install.json file, launch the /install.sh file to install ADSS Web RA with the required set of configurations.

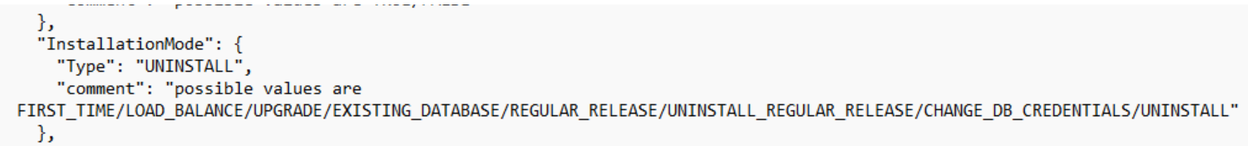
5.3.9 Uninstallation Process

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

Note: Always uninstall the deployed package before removing it to avoid configuration issues.

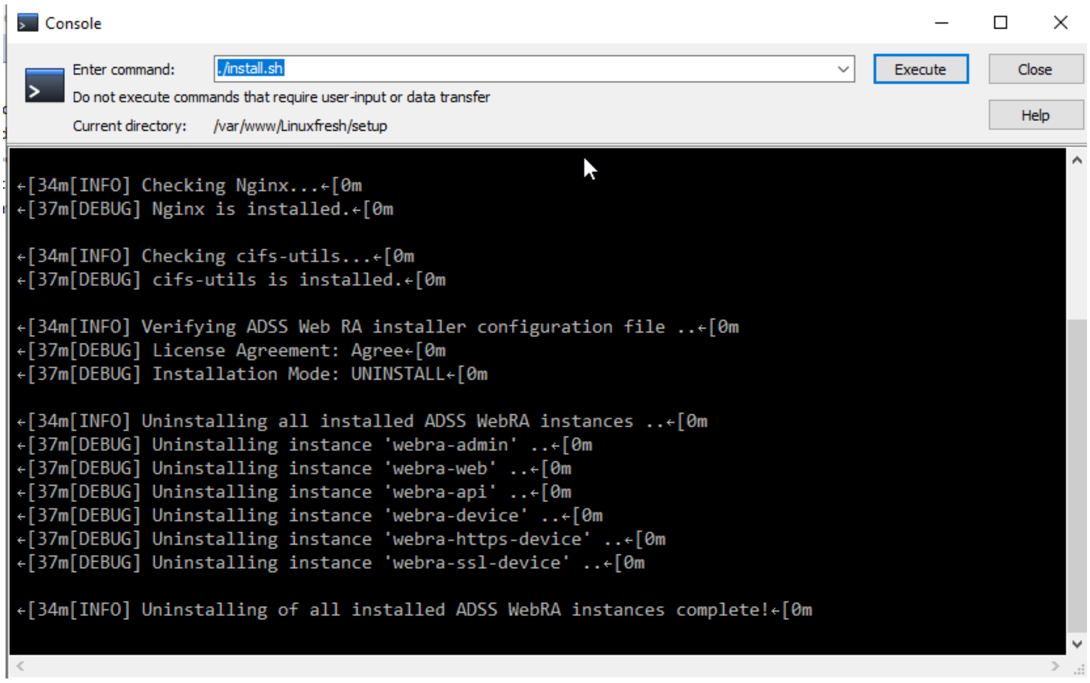
5.3.9.1 Uninstalling a Simple Installation

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



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

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



Enter command: ./install.sh

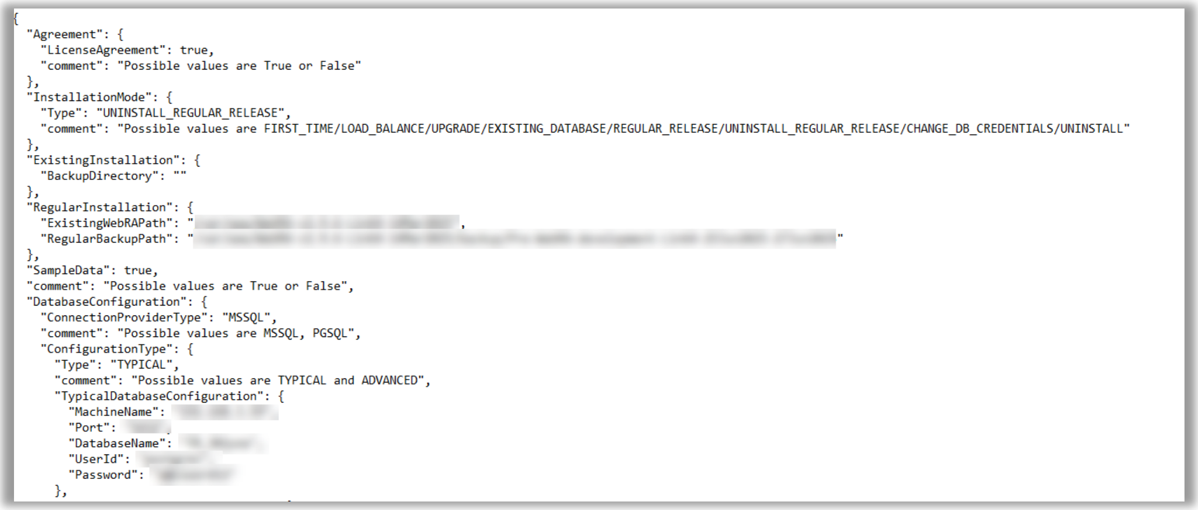
Do not execute commands that require user-input or data transfer

Current directory: /var/www/Linuxfresh/setup

```
←[34m[INFO] Checking Nginx...←[0m
←[37m[DEBUG] Nginx is installed.←[0m

←[34m[INFO] Checking cifs-utils...←[0m
←[37m[DEBUG] cifs-utils is installed.←[0m

←[34m[INFO] Verifying ADSS Web RA installer configuration file ..←[0m
←[37m[DEBUG] License Agreement: Agree←[0m
←[37m[DEBUG] Installation Mode: UNINSTALL←[0m

←[34m[INFO] Uninstalling all installed ADSS WebRA instances ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-admin' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-web' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-api' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-device' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-https-device' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-ssl-device' ..←[0m

←[34m[INFO] Uninstalling of all installed ADSS WebRA instances complete!←[0m
```

5.3.9.2 Uninstalling a Regular Release

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



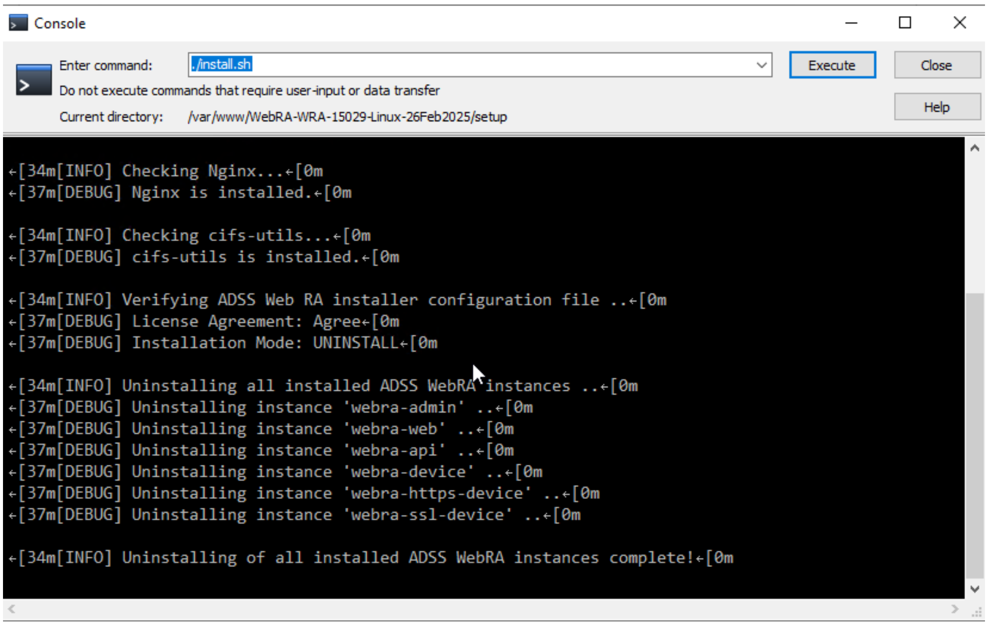
```
{
  "Agreement": {
    "LicenseAgreement": true,
    "comment": "Possible values are True or False"
  },
  "InstallationMode": {
    "Type": "UNINSTALL_REGULAR_RELEASE",
    "comment": "Possible values are FIRST_TIME/LOAD_BALANCE/UPGRADE/EXISTING_DATABASE/REGULAR_RELEASE/UNINSTALL_REGULAR_RELEASE/CHANGE_DB_CREDENTIALS/UNINSTALL"
  },
  "ExistingInstallation": {
    "BackupDirectory": ""
  },
  "RegularInstallation": {
    "ExistingWebRAPath": "[redacted],
    "RegularBackupPath": "[redacted]"
  },
  "SampleData": true,
  "comment": "Possible values are True or False",
  "DatabaseConfiguration": {
    "ConnectionProviderType": "MSSQL",
    "comment": "Possible values are MSSQL, PGSQL",
    "ConfigurationType": {
      "Type": "TYPICAL",
      "comment": "Possible values are TYPICAL and ADVANCED",
      "TypicalDatabaseConfiguration": {
        "MachineName": [redacted]
        "Port": [redacted]
        "DatabaseName": [redacted]
        "UserId": [redacted]
        "Password": [redacted]
      },
```

You must also provide the following two parameters for the uninstallation process to complete successfully:

ExistingWebRAPath - This is the location where your current Web RA is installed. The system needs this path to find and remove the regular release. **For example:** existing installation directory/.

RegularBackupPath - This is where a backup of the current Web RA will be saved before the uninstallation starts. It helps you restore things in case something goes wrong. **For example:** existing directory/backup directory/backup folder.

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



Enter command: ./install.sh

Do not execute commands that require user-input or data transfer

Current directory: /var/www/WebRA-WRA-15029-Linux-26Feb2025/setup

```
←[34m[INFO] Checking Nginx...←[0m
←[37m[DEBUG] Nginx is installed.←[0m

←[34m[INFO] Checking cifs-utils...←[0m
←[37m[DEBUG] cifs-utils is installed.←[0m

←[34m[INFO] Verifying ADSS Web RA installer configuration file ..←[0m
←[37m[DEBUG] License Agreement: Agree←[0m
←[37m[DEBUG] Installation Mode: UNINSTALL←[0m

←[34m[INFO] Uninstalling all installed ADSS WebRA instances ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-admin' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-web' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-api' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-device' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-https-device' ..←[0m
←[37m[DEBUG] Uninstalling instance 'webra-ssl-device' ..←[0m

←[34m[INFO] Uninstalling of all installed ADSS WebRA instances complete!←[0m
```

6 Appendix

6.1 Troubleshooting

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

Follow these instructions to solve this issue:

a. Open registry and add the key:

KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\ SCHANNEL

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

c. Set **Value Name: ClientAuthTrustMode**

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

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

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

a. Open IIS Management Console.

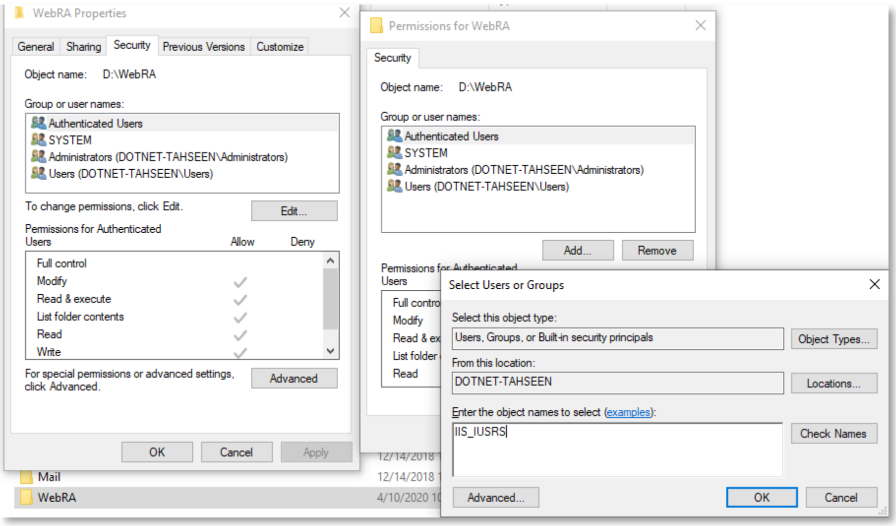
b. Go to Application Pools.

c. Select a site and click Advanced Setting.

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

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

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



WebRA Properties

Object name: D:\WebRA

Group or user names:
Authenticated Users
SYSTEM
Administrators (DOTNET-TAHSEEN\Administrators)
Users (DOTNET-TAHSEEN\Users)

To change permissions, click 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.

Permissions for WebRA

Object name: D:\WebRA

Group or user names:
Authenticated Users
SYSTEM
Administrators (DOTNET-TAHSEEN\Administrators)
Users (DOTNET-TAHSEEN\Users)

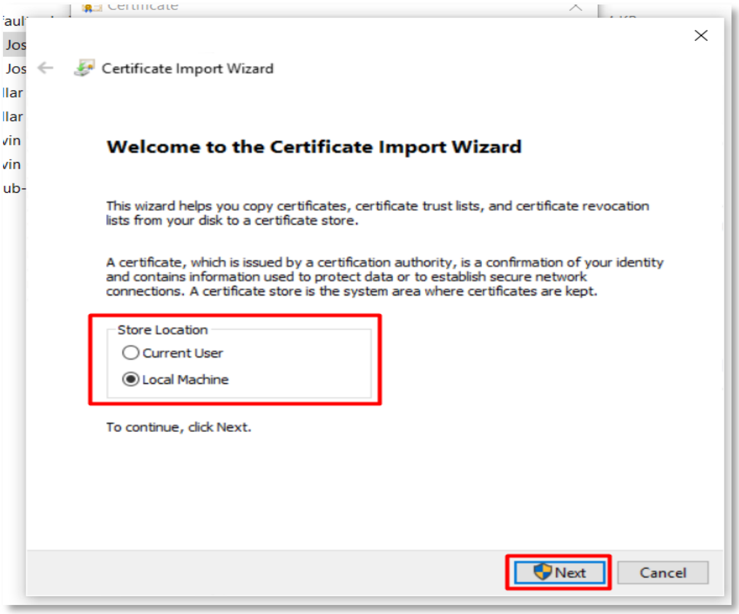
Select Users or Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: DOTNET-TAHSEEN

Enter the object names to select (examples): IIS_IUSRS

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



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.

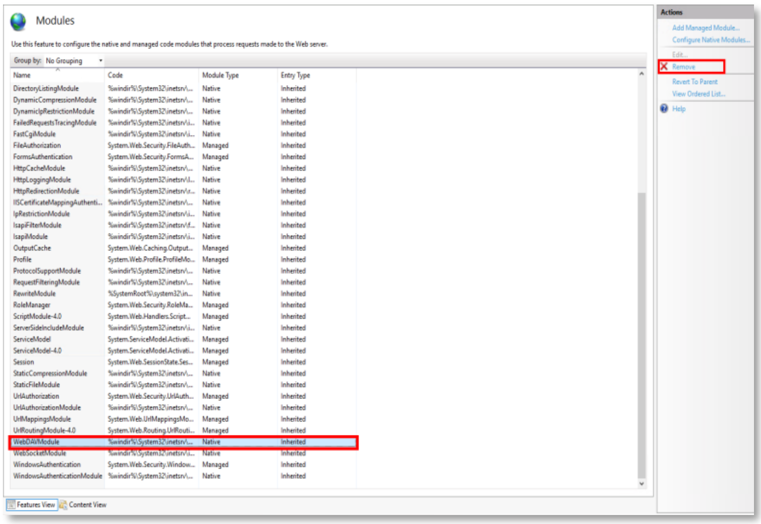
Store Location

○ Current User

● Local Machine

To continue, click Next.

- 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

6.2 Troubleshooting for Linux

- ### Deployment Stops Unexpectedly

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

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

   ```
   sudo setenforce 0
   ```

   This forces the security module to be turned off.

2. Test the ngnix configuration by running the following command:

   ```
   sudo nginx -t
   ```

   This command tests your ngnix configuration without actually starting or restarting the server.

   - It checks for syntax errors in your ngnix configuration files.
   - Validates file paths (e.g., certs, keys, includes).
   - Ensures ngnix won't crash when restarted.
   - It is a safe way to debug before restarting a live server.

3. Restart the nginx service to ensure proper functionality:

   ```
   systemctl restart nginx
   ```

- ### A Specific Web RA Service is Not Running

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

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

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

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

Issue:

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

Solution:

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

- **Nginx is Inactive or Not Running**

If Nginx is inactive, Web RA will not be accessible in the browser. Check the service status and restart it if necessary.

Symptom:

Active: inactive (dead)

Solution:

1. Test the ngnix configuration by running the following command:

```
sudo nginx -t
```

This command tests your ngnix configuration without actually starting or restarting the server.

- It checks for syntax errors in your ngnix configuration files.
- Validates file paths (e.g., certs, keys, includes).
- Ensures ngnix won't crash when restarted.
- It is a safe way to debug before restarting a live server.

2. Then, restart the nginx service using the following command:

```
sudo systemctl start nginx
```

- **413 Request Entity Too Large – API or File Upload Failure**

In case of executing APIs with large datasets or files, if the following error appears, apply the configuration and commands below to resolve it:

Error:

"413 Request Entity Too Large"

This error occurs when a client (such as a browser or an API request) tries to upload data exceeding the allowed size limit configured in nginx.

Resolution: Increase the client_max_body_size limit in nginx.

1. Open the nginx Configuration File

Edit your main nginx configuration file (`/etc/nginx/nginx.conf`) or the specific site configuration in `/etc/nginx/sites-available/your-site.conf`:

```
sudo nano /etc/nginx/nginx.conf
```

2. Increase "client_max_body_size"

Add or modify this directive inside the http, server, or location block:

```
    http {
        client_max_body_size 100M;
}
```

3. Test the Configuration

```
nginx -t
```

4. Reload nginx to apply changes

```
sudo systemctl reload nginx
```

- ## License Upload Error on AlmaLinux Due to SHA-1 Restriction

If you encounter an error while uploading the application license on an AlmaLinux machine, you need to enable the SHA-1 algorithm. Once enabled, the license upload will work successfully.

How to Enable SHA-1 Algorithm on CentOS Stream 9 / AlmaLinux 9 / RockyLinux 9:

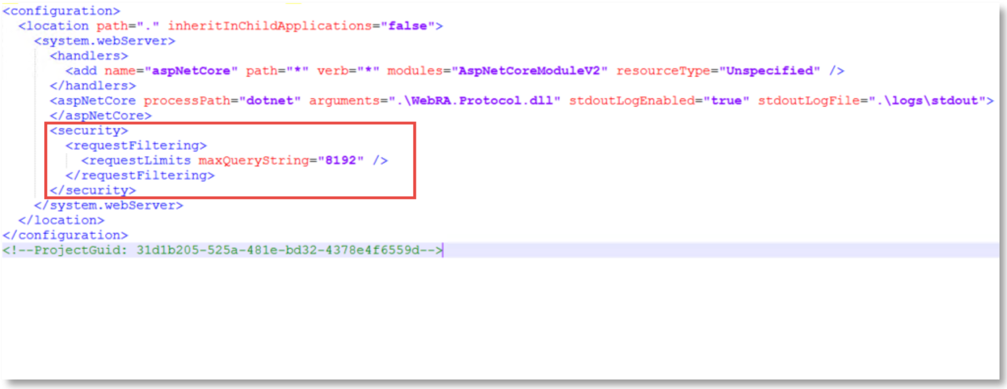
To fix this, you need to enable the SHA-1 algorithm in your modern OS, for example in EL9 / CentOS 9. To enable it, run the following command:

```
update-crypto-policies --set DEFAULT:SHA1
```

6.3 Configurations used for Simple Certificate Enrollment Protocol (SCEP)

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

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

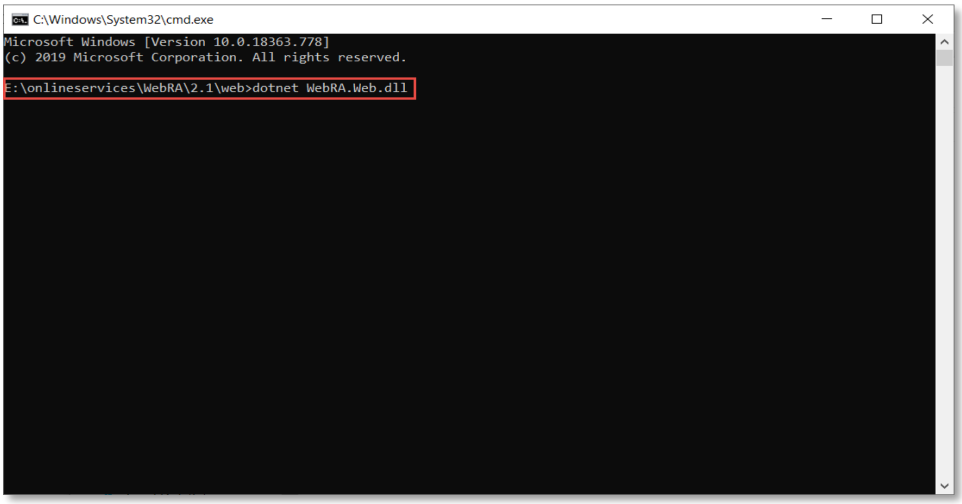


```
<configuration>
  <location path="." inheritInChildApplications="false">
    <system.webServer>
      <handlers>
        <add name="aspNetCore" path="*" verb="*" modules="AspNetCoreModuleV2" resourceType="Unspecified" />
      </handlers>
      <aspNetCore processPath="dotnet" arguments=".\WebRA.Protocol.dll"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

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

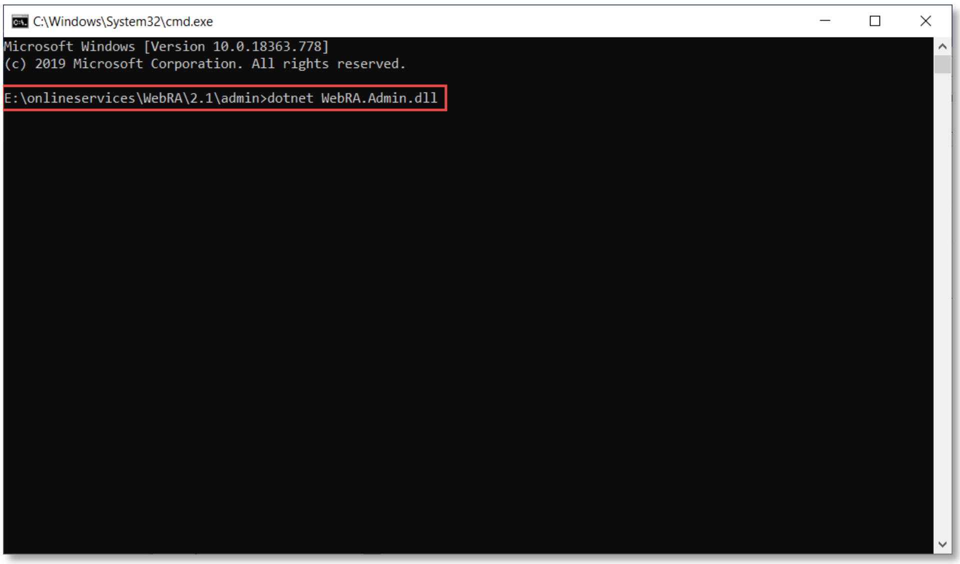
- “[Server URL]/scep” e.g “https://beta.web.ra.signinghub.com/scep
- Update URL value in Expect-CT header in “**web.config**” for web and admin modules according to your deployment URL. e.g. **<add name="Expect-CT" value="max-age=0, report-uri='https://adminra.signinghub.com'" />**

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



```
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
```

6.4 SSL Certificates

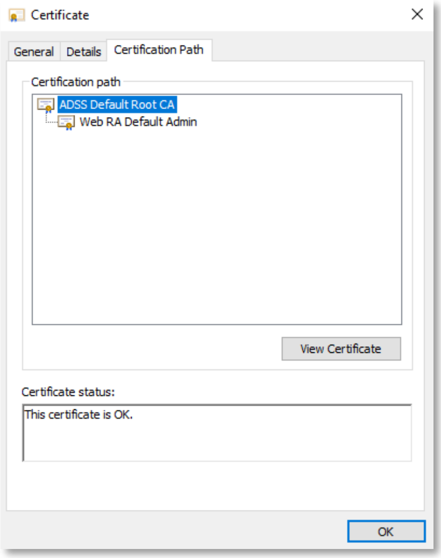
ADSS Web RA is a web application that is hosted in IIS. It is recommended to secure the communication between the server and browsers by using SSL over HTTPS. It is also recommended to use an SSL certificate issued by a well-known certificate authority (CA) e.g., Comodo, Symantec, Digicert, etc.

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

6.4.1 Exporting Root and Intermediate Certificates

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

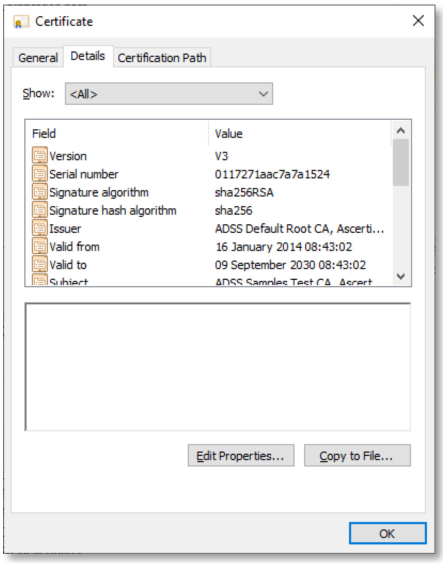
6.4.3 Double click the web-ra-default-admin.cer file



Certificate status:

This certificate is OK.

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

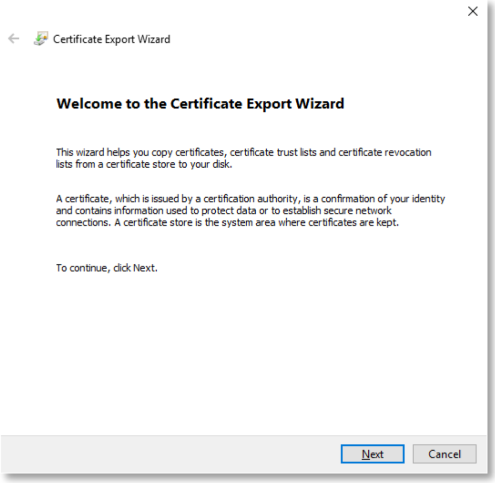


Certificate

Show: <All>

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...

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



Certificate Export Wizard

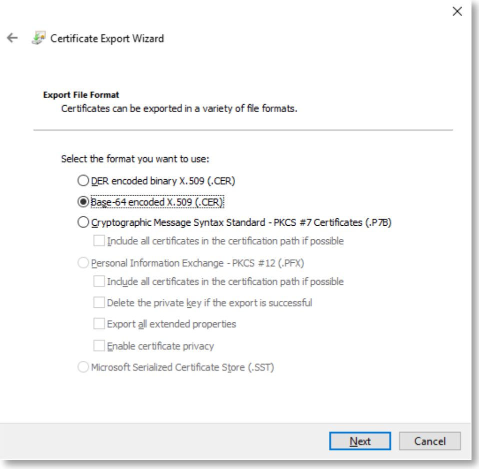
Welcome to the Certificate Export Wizard

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.

6.4.6 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

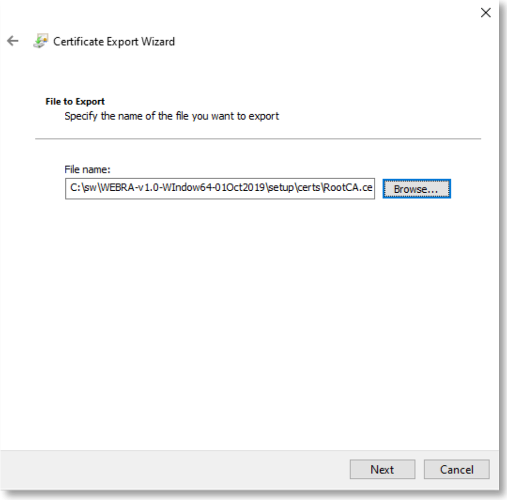
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

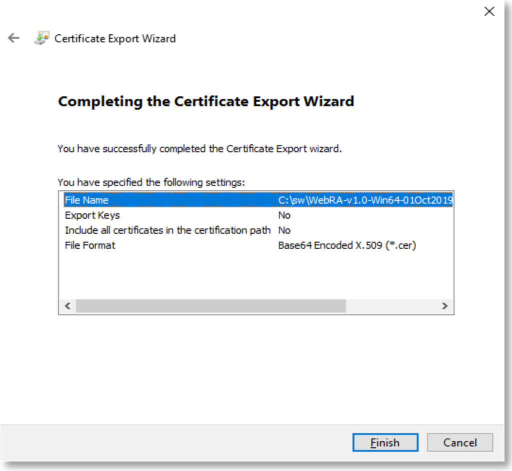
6.4.7 Select the Base-64 encoded X.509 (.CER) option and click Next



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

6.4.8 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)

6.4.9 Click Finish to complete the root certificate export process.

6.5 SSL Configuration for Linux

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

6.5.1 Navigate to the nginx configuration directory:

The configuration for the SSL device module is stored in the **sites-available** directory.

Open the file with a text editor:

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

6.5.2 Locate the SSL Configuration Block:

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

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

6.5.3 Update the Certificate Paths:

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

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

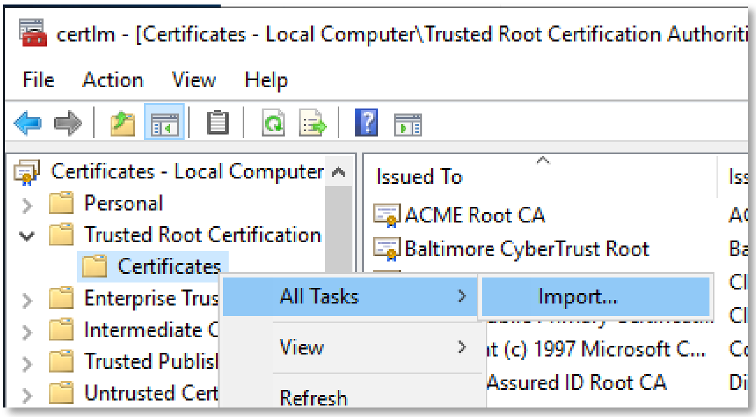
After updating the paths, save and exit the file**.** Once the configuration is updated, restart Nginx to load the new certificate. By following these steps, the WebRA module will be properly configured to use the provided SSL certificates.

6.6 Importing Root and Intermediate Certificates

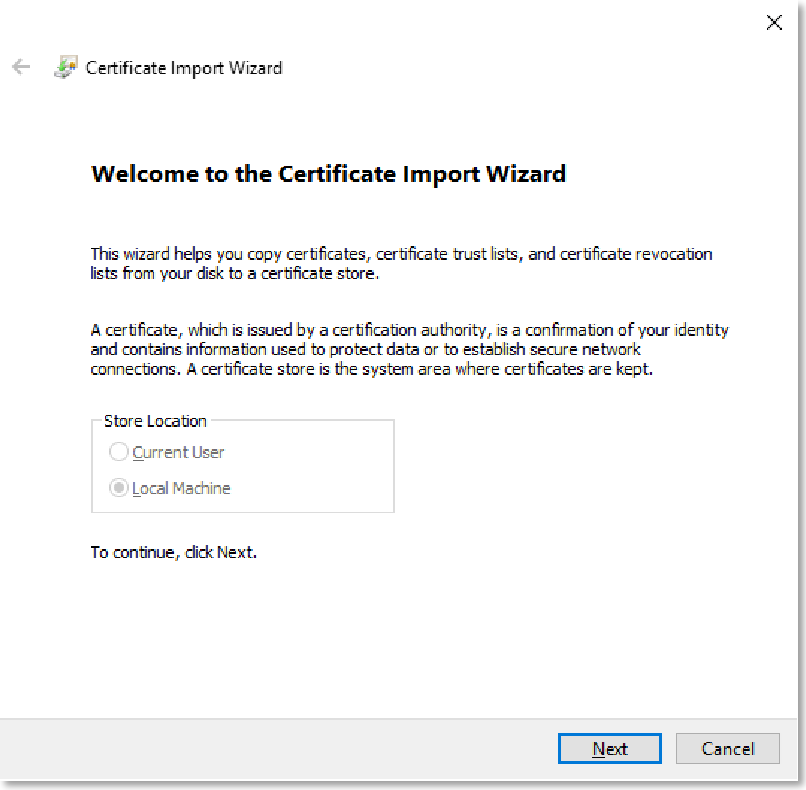
Now that we have the intermediate and root certificates exported and saved in a local file, we can import it to the certificate store.

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

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


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
Issued To
Iss
ACME Root CA
Baltimore CyberTrust Root
All Tasks
Import...
View
Refresh
it (c) 1997 Microsoft C...
Assured ID Root CA

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



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.

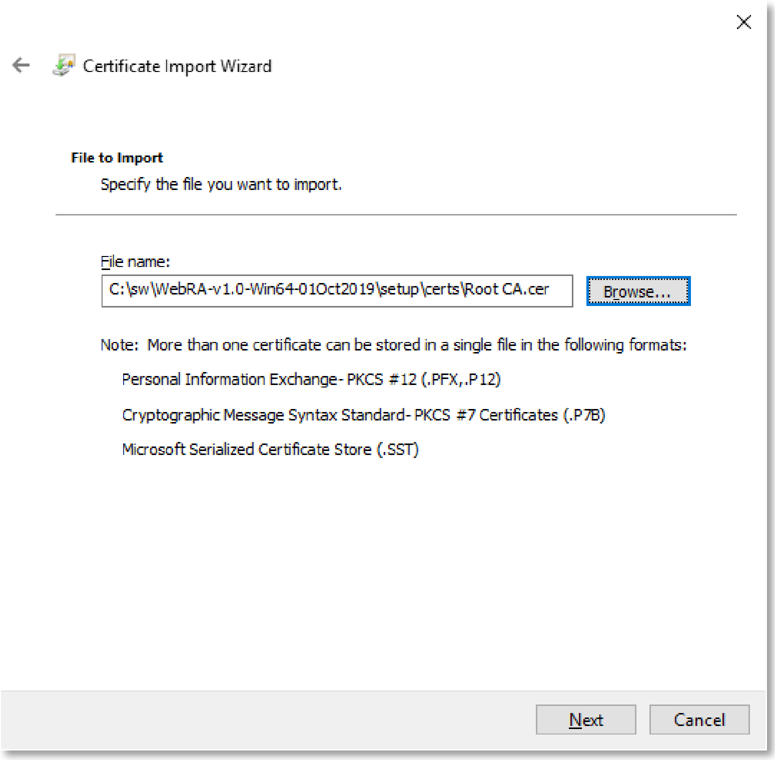
Store Location

○ Current User

● Local Machine

To continue, click Next.

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



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

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

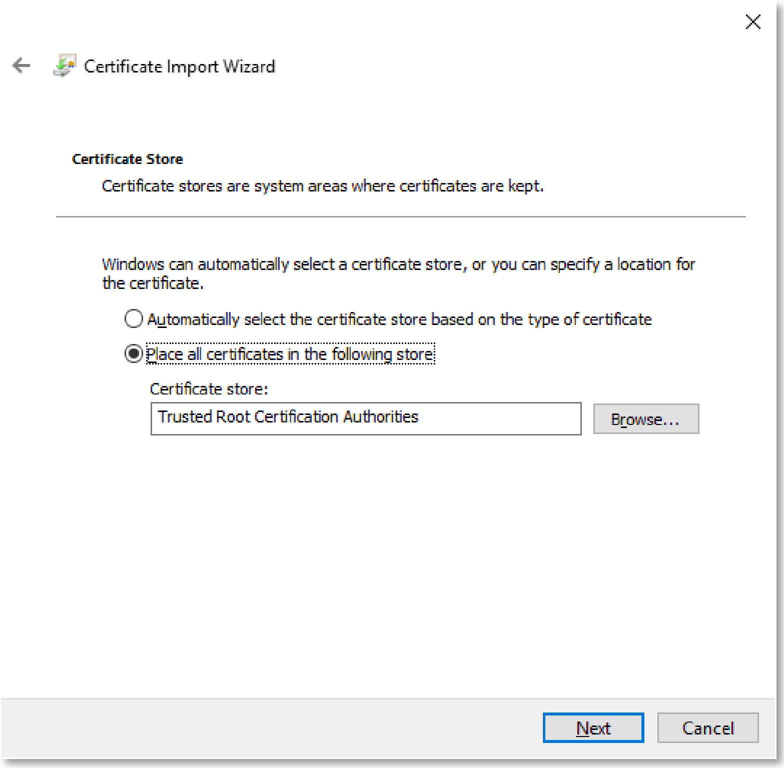
Note: More than one certificate can be stored in a single file in the following formats:

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

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

Microsoft Serialized Certificate Store (.SST)

6.6.5 Click **Next** to proceed.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

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

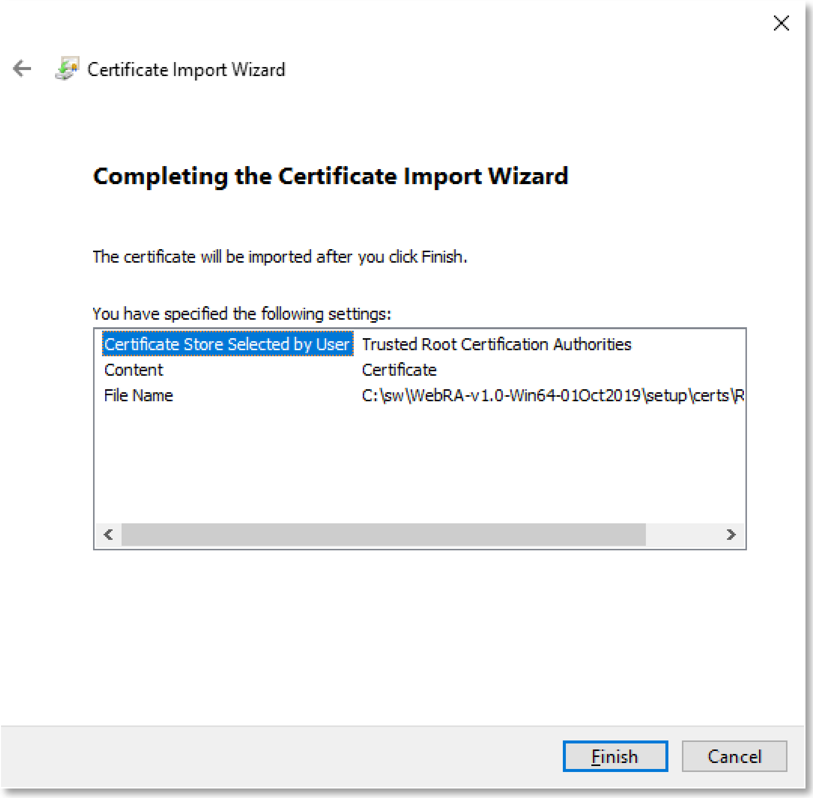
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

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



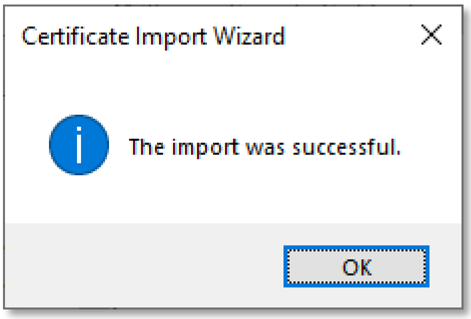
Completing the Certificate Import Wizard

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

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



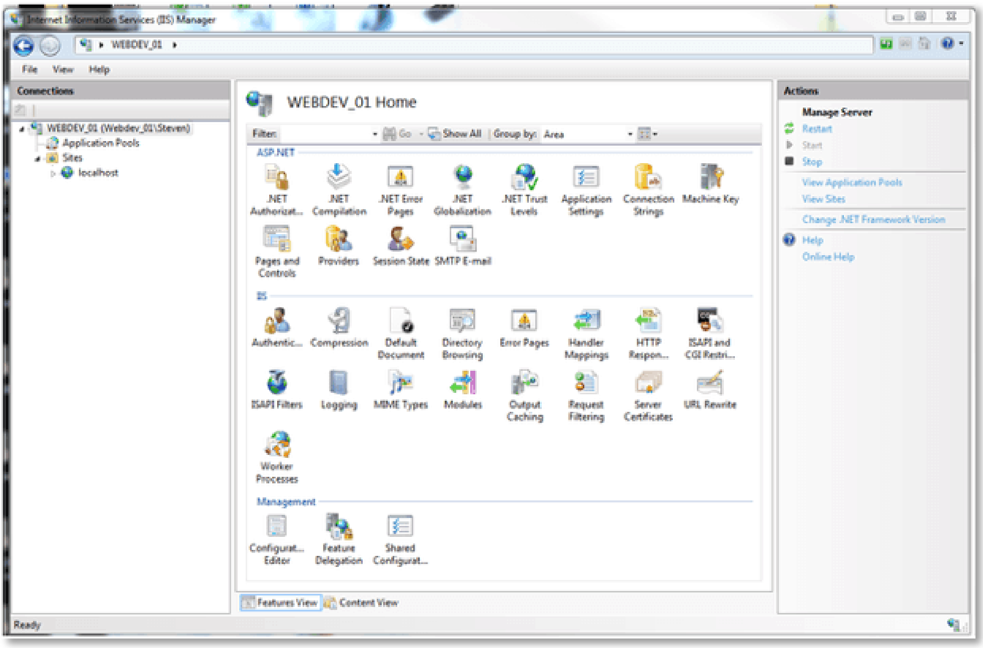
The import was successful.

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

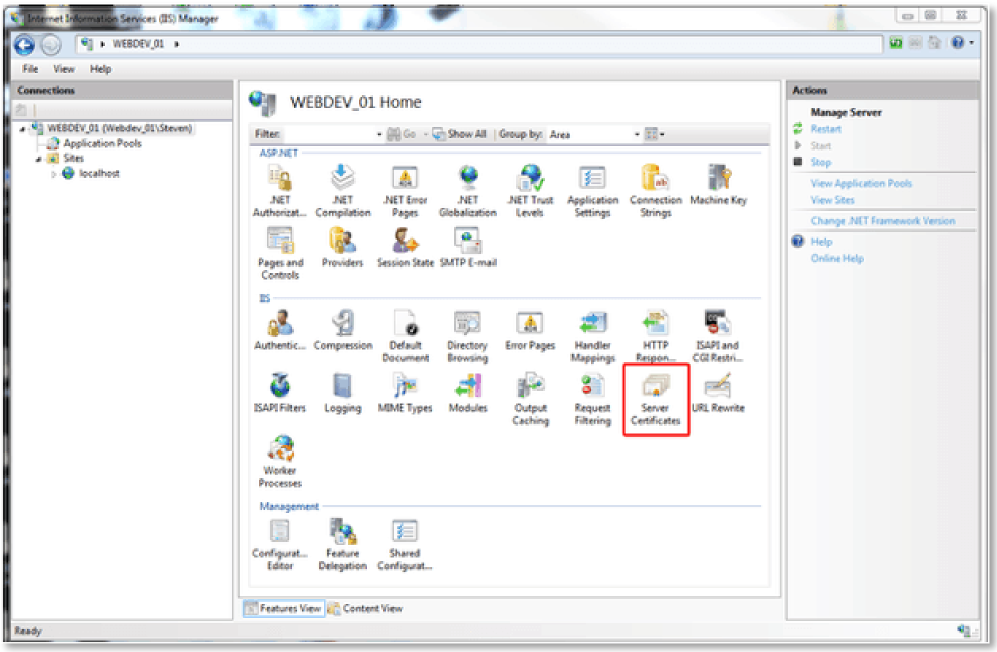
6.7 Generate a Self -Signed Certificate

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

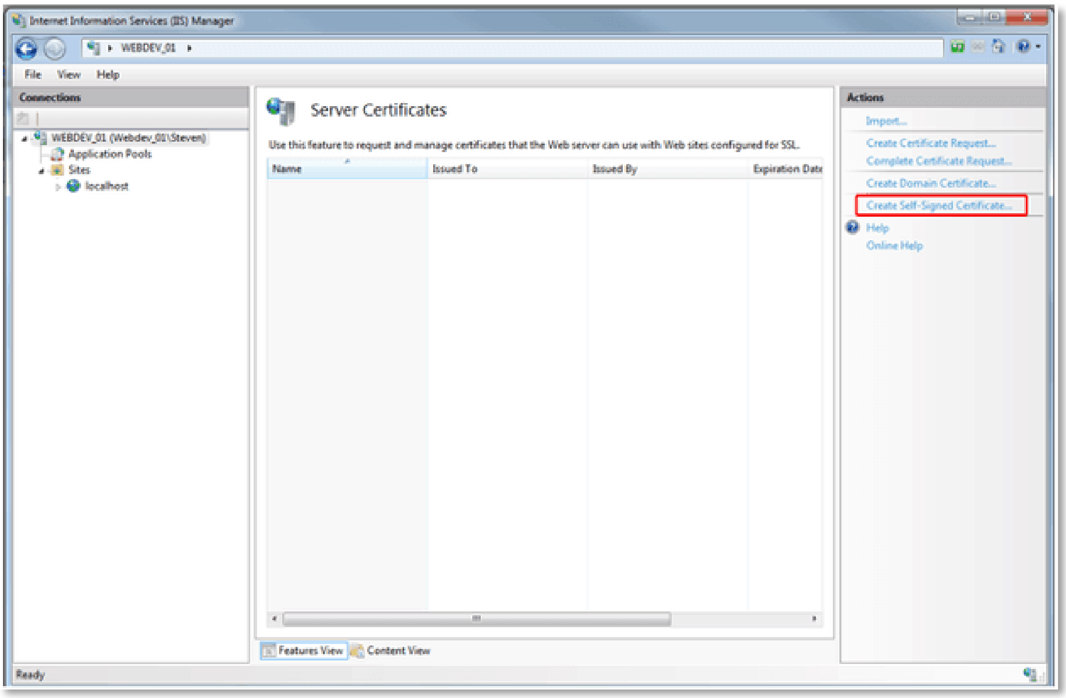
6.7.1 Launch the **IIS Manager**.



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

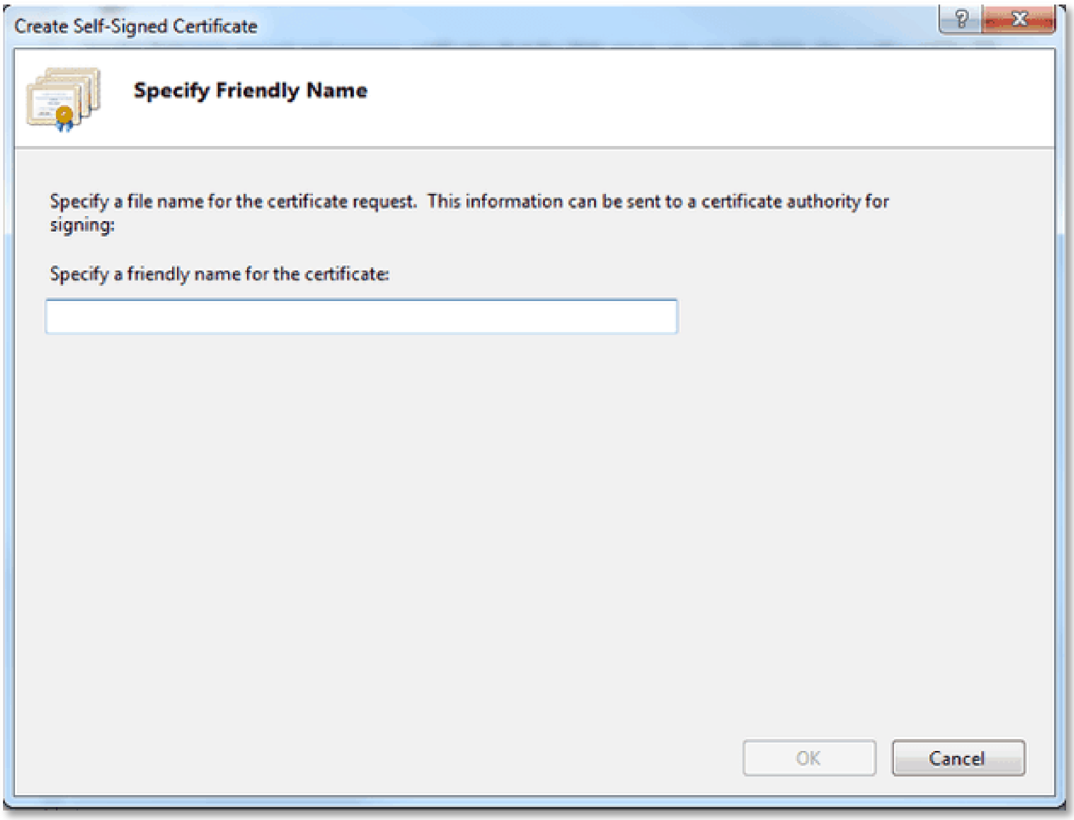


6.7.3 Double-click on **Server Certificates** from the IIS section in the middle panel.


Internet Information Services (IIS) Manager
WEBDEV_01
File
View
Help
Connections
WEBDEV_01 (Webdev_01\Steven)
Application Pools
Sites
localhost
Server Certificates
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

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

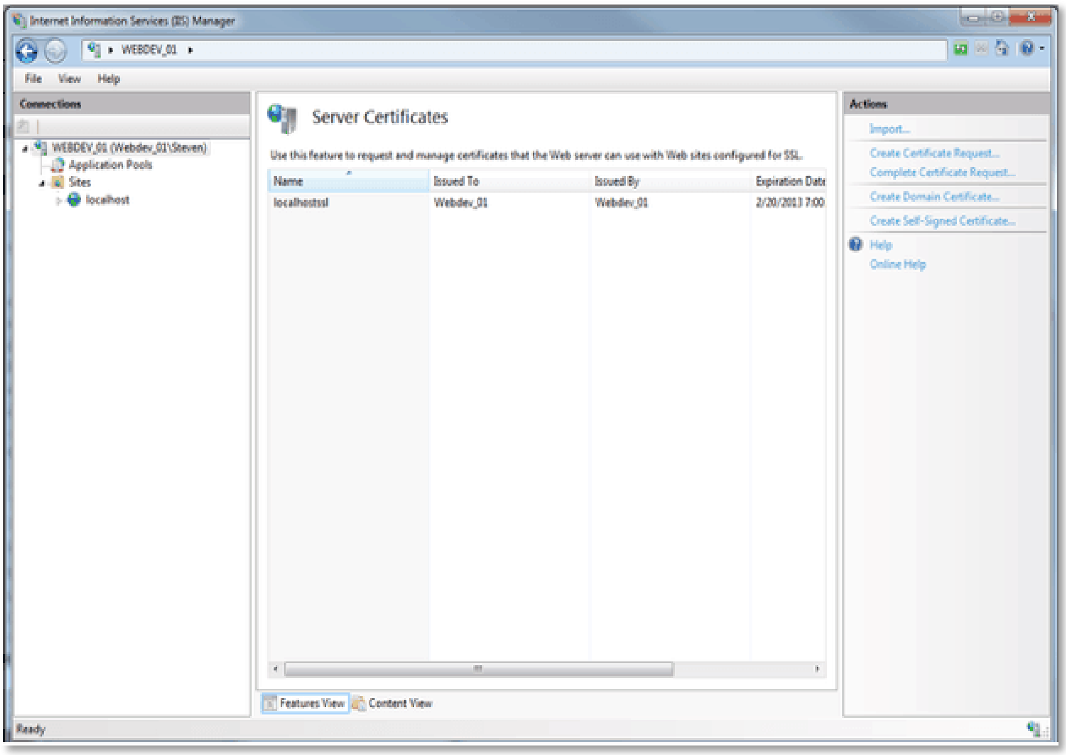
6.7.4 Click **Create Self-Signed Certificate**... under the right Actions column.



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:

6.7.5 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.

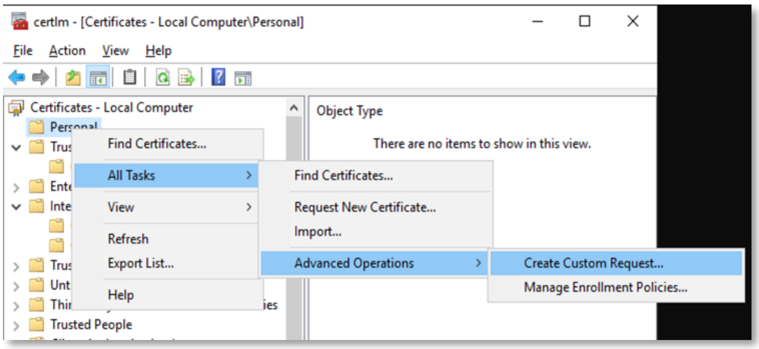
Name	Issued To	Issued By	Expiration Date
localhostssl	Webdev_01	Webdev_01	2/20/2013 7:00

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

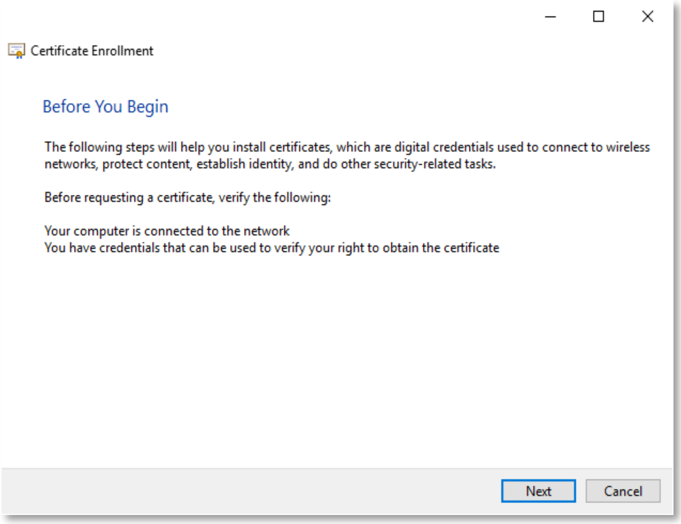
6.8 Generate a CSR for an SSL Certificate

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

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



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



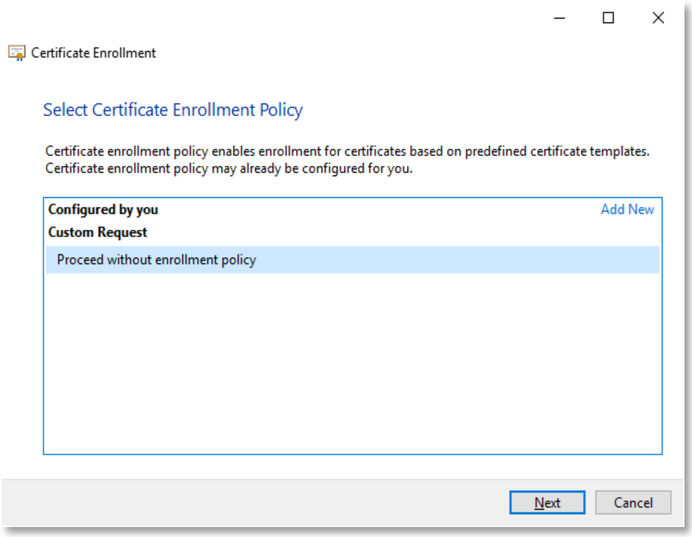
Before You Begin

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

6.8.3 Press **Next** to proceed.



Certificate Enrollment

Select Certificate Enrollment Policy

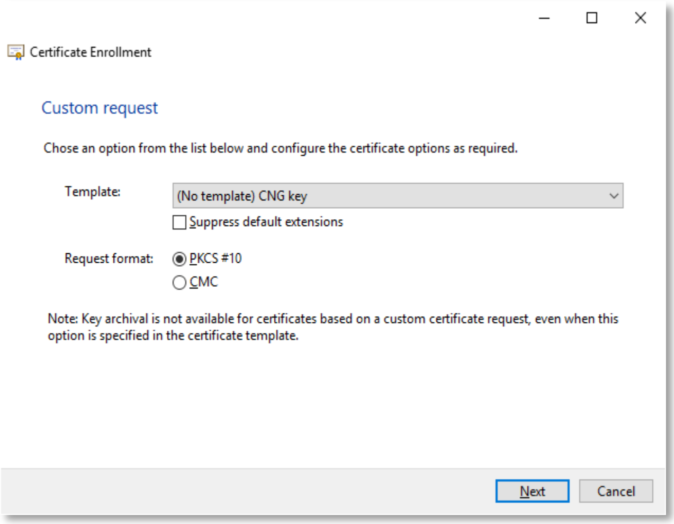
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you Add New

Custom Request

Proceed without enrollment policy

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



Certificate Enrollment

Custom request

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

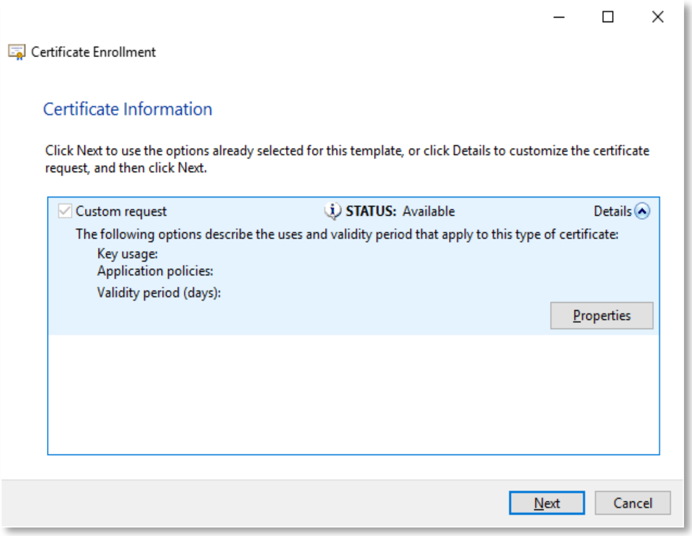
Template: (No template) CNG key

□ 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.

6.8.5 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

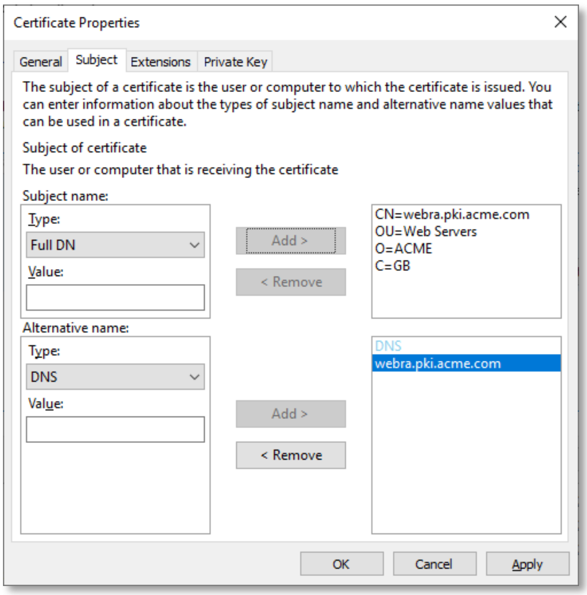
The following options describe the uses and validity period that apply to this type of certificate:

Key usage:

Application policies:

Validity period (days):

6.8.6 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:

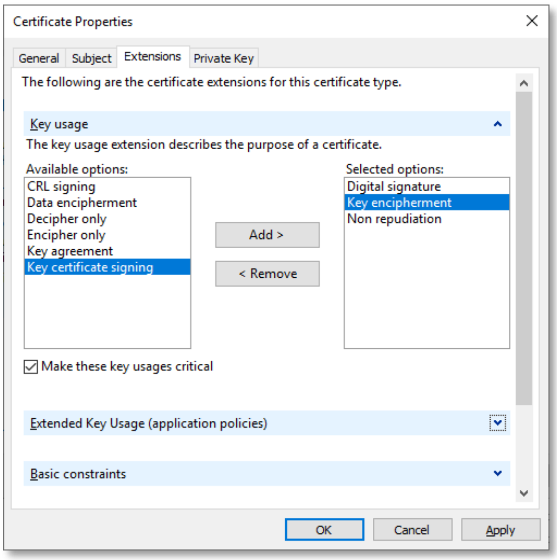
Type: DNS

Value:

DNS
webra.pki.acme.com

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

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



Certificate Properties

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)

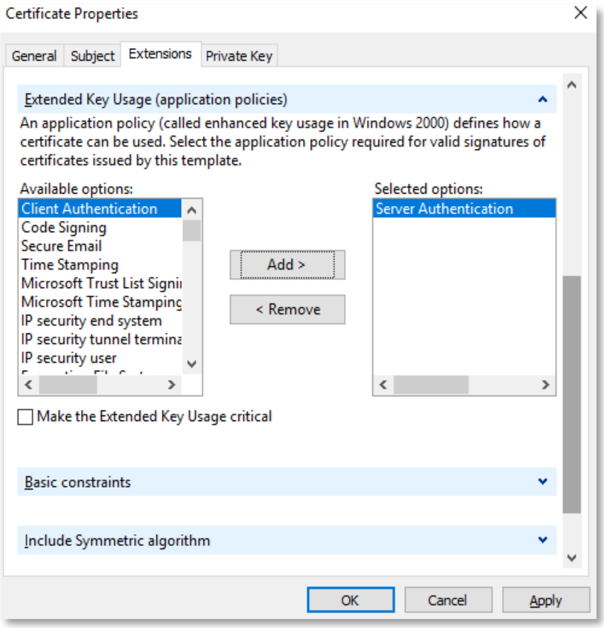
Basic constraints

6.8.8 Select the Extensions tab from the top. Select the Key usage option from the dropdown extensions. Now from the Available options, choose the following:

- Digital signature
- Key encipherment
- Non-repudiation

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

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



Extended Key Usage (application policies)

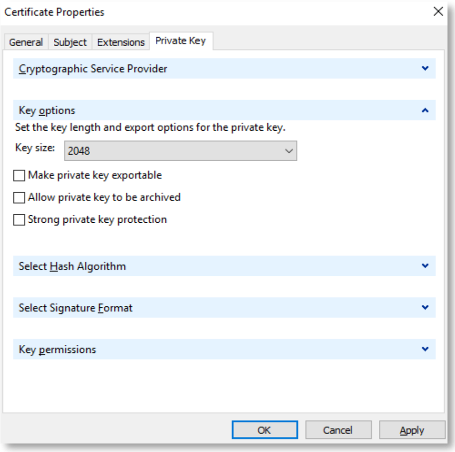
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Available options:
Client Authentication
Code Signing
Secure Email
Time Stamping
Microsoft Trust List Signii
Microsoft Time Stamping
IP security end system
IP security tunnel termina
IP security user

Selected options:
Server Authentication

□ Make the Extended Key Usage critical

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



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

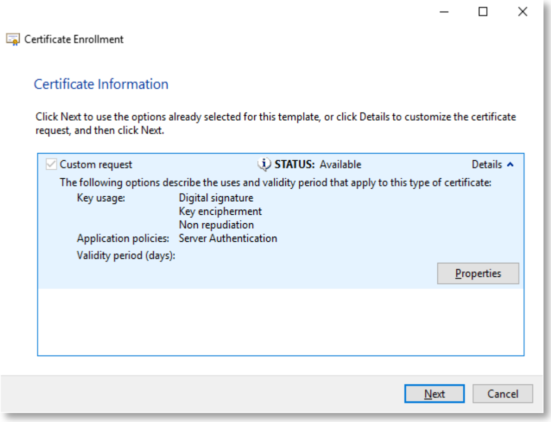
Key size: 2048

□ Make private key exportable

□ Allow private key to be archived

□ Strong private key protection

6.8.11 Press Next to proceed.



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

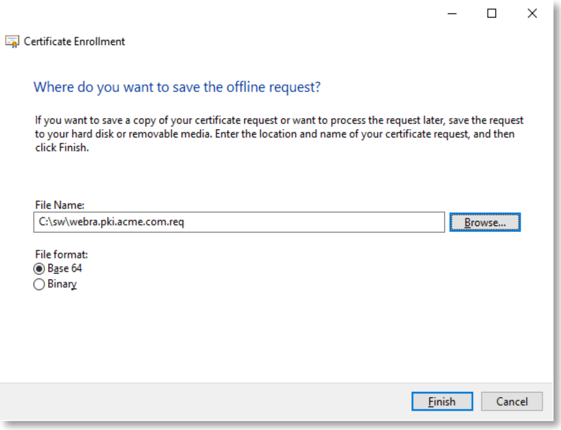
The following options describe the uses and validity period that apply to this type of certificate:

Key usage: Digital signature
Key encipherment
Non repudiation

Application policies: Server Authentication

Validity period (days):

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



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

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

*** End of Document ***