

ADSS Web RA Server 2.9

Installation

Guide

ASCERTIA LTD

December 2023

Document Version- 1.0.0

© 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 In	troduction	3
1.1	Scope	3
1.2	Intended Readership	3
1.3	Technical Support	3
1.4	Glossary	4
2 S	ystem Requirements	5
2.1	Hardware Prerequisites	5
2.2	Software Prerequisites	
2.3	Application Development feature in IIS	7
2.4	Microsoft .Net Core 7.0.0. Runtime & Hosting Bundle	8
2.5	Microsoft IIS URL Rewrite Module 2.1	
2.6	Unlock system.webServer/serverRuntime section in IIS	12
2.7	SMTP Server	13
2.8	Database	13
0 I	stallation Modules	11
3 In	stallation modules	
-	DSS Web RA Installation	
-		15
4 A	DSS Web RA Installation Fresh Installation of ADSS Web RA	15 15
4 A 4.1	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration	15 15 26
4 A 4.1 4.2.	DSS Web RA Installation Fresh Installation of ADSS Web RA	15 15 26 34
4 A 4.1 4.2. 4.2.	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration Installing ADSS Web RA with an Existing Database	15 26 34 42
4 A 4.1 4.2. 4.2. 4.3. 4.4.	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration Installing ADSS Web RA with an Existing Database Upgrading ADSS Web RA	15 26 34 42 46
 4 A 4.1 4.2. 4.2. 4.3. 4.4. 5. A 	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration Installing ADSS Web RA with an Existing Database Upgrading ADSS Web RA Changing Database Credentials for an Existing Installation	15 26 34 42 46 48
 4 A 4.1 4.2. 4.2. 4.3. 4.4. 5. A 	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration Installing ADSS Web RA with an Existing Database Upgrading ADSS Web RA Changing Database Credentials for an Existing Installation DSS Web RA Uninstallation	15 26 34 42 46 48 50
 4 A 4.1 4.2. 4.3. 4.4. 5. A 6. A 	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration Installing ADSS Web RA with an Existing Database Upgrading ADSS Web RA Changing Database Credentials for an Existing Installation DSS Web RA Uninstallation Troubleshooting	15 26 34 42 46 46 48 50
 4 A 4.1 4.2. 4.2. 4.3. 4.4. 5. A 6. A 	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration Installing ADSS Web RA with an Existing Database Upgrading ADSS Web RA Changing Database Credentials for an Existing Installation DSS Web RA Uninstallation	15 26 34 42 46 48 50 50 52
 4 A 4.1 4.2. 4.3. 4.4. 5. A 6.1. 6.2. 	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration Installing ADSS Web RA with an Existing Database Upgrading ADSS Web RA Changing Database Credentials for an Existing Installation DSS Web RA Uninstallation ppendix Troubleshooting Configurations used for Simple Certificate Enrollment Protocol (SCEP)	15 26 34 42 46 48 50 50 53
 4 A 4.1 4.2. 4.2. 4.3. 4.4. 5. A 6.1. 6.2. 6.3. 	DSS Web RA Installation Fresh Installation of ADSS Web RA Installing ADSS Web RA with A Load-Balanced Configuration Installing ADSS Web RA with an Existing Database Upgrading ADSS Web RA Changing Database Credentials for an Existing Installation DSS Web RA Uninstallation ppendix Troubleshooting Configurations used for Simple Certificate Enrollment Protocol (SCEP) . SSL Certificates	15 26 34 42 46 48 50 50 52 53 56

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 <u>Ascertia Ticketing System</u> or email address: <u>support@ascertia.com</u>

Ascertia provides formal support agreements with all product sales. Contact <u>sales@ascertia.com</u> 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	ents 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: <u>https://manuals.ascertia.com/WebRA-v2.9/ADSS-WebRA-Server-Platform-Support.pdf</u>		
Microsoft IIS	IIS 10Application Development feature in IIS		
IIS Rewrite Module	• v2.1		
.Net Framework	.Net Framework 4.8. or above		
.Net Core Runtime & Hosting Bundle	ASP.NET Core Runtime 7.0.0 or above		

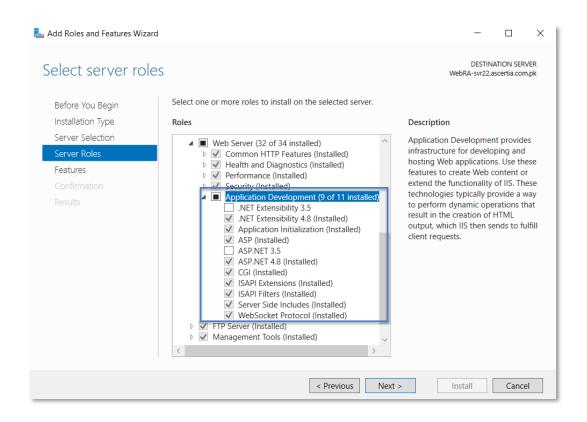
Database Server	 Follow this link to view details about Database Server: <u>https://manuals.ascertia.com/WebRA-v2.9/ADSS-WebRA-Server-Platform-Support.pdf</u> Follow this link to view details about Web Browsers:
(for end-users and administrators)	https://manuals.ascertia.com/WebRA-v2.9/ADSS-WebRA-Server- Platform-Support.pdf
ADSS Server	 ADSS Web RA uses ADSS Server under the hood to create and manage certificates for the end user as a CA. ADSS Server can be installed on a separate machine or on the same machine for testing and proof of concept. It is recommended to keep the ADSS installation on a separate machine for a production environment. For further requirements related to the installation of ADSS Server, please refer to the installation guide of ADSS Server. ADSS Server 6.6 or above
DMZ Proxy Systems	 A DMZ proxy server is recommended to provide enhanced security for ADSS Web RA. Supported web servers are: Windows Server + IIS, Apache or IBM HTTP Server Linux + Apache or IBM HTTP Server It is recommended to use a reasonable CPU, 4 GB RAM (Minimum), 2000 MB Disk Space for the web server machine. ADSS Web RA and ADSS Server support network proxies to allow authenticated access to external services. Certificate generation with local smartcards or USB tokens requires ADSS Server Go>Sign Service.

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

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

2.3 Application Development feature in IIS

Enable the following features in IIS on the deployment machine:





2.4 Microsoft .Net Core 7.0.14. Runtime & Hosting Bundle

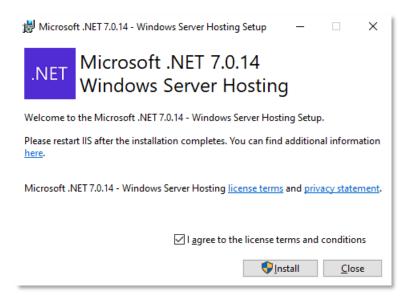
2.4.1 Download the latest version of Microsoft .Net Core i.e. Microsoft .Net Core 7.0.14. Runtime and Hosting Bundle from the following link:

Microsoft .Net Core 7.0.14. Runtime & Hosting Bundle

2.4.2 Download the Hosting Bundle installer.

	0.14 Security patch () Latest release date November	14, 2023				
Build app	s - SDK ()		Run apps	- Runtime 🛈		
SDK 7.	0.404		ASP.NE	T Core Runtime 7.0	.14	
OS	Installers	Binaries			run existing web/server applicati	
Linux	Package manager instructions	Arm32 Arm32 Alpine Arm64 Arm64 Alpine x64 x64 Alpine	Windows, we recommend installing the Hosting Bundle, which includes the .NET Runtime and IIS support.			the .NET
macOS	<u>Arm64 x64</u>	<u>Arm64 x64</u>	115 runtim 17.0.2329	ie support (ASP.NET Core Modi 5.14	ule v2)	
Windows	Arm64 x64 x86 winget instructions	<u>Arm64 x64 x86</u>	OS	Installers	Binaries	
All	dotnet-install scripts		Linux	Package manager instructions	Arm32 Arm32 Alpine Arm Arm64 Alpine x64 x64 Alp	
	dio support lio 2022 (v17.7)		macOS <u>Arm64 x64</u>			
	lio 2022 (v17.7)		Windows	Hosting Bundle x64 x86	<u>Arm64 x64 x86</u>	
Included i Visual Stud				winget instructions		
			The .NET [release in	cludes the .NET Runtime; you	.14 run existing Windows desktop ap don't need to install it separate	ly.
Language C# 12.0	support		OS Windows	Arm64 x64 x86 wings	at instructions	Binaries
F# 6.0			WITCOWS	ALLI04 X04 X00 WILLS		
Visual Basi	c 16.9		.NET R	untime 7.0.14		
SDK 7.	0.311				nents needed to run a console ap Runtime or .NET Desktop Runtime	
OS	Installers	Binaries				
Linux	Package manager instructions	Arm32 Arm32 Alpine Arm64 Arm64 Alpine x64 x64 Alpine	OS Linux	Installers Package manager instructions	Binaries Arm32 Arm32 Alpine Arm64	1
macOS	<u>Arm64 x64</u>	Arm64 x64			Arm64 Alpine x64 x64 Alpine	
Windows	Arm64 x64 x86 winget instructions	<u>Arm64 x64 x86</u>	macOS Windows	Arm64 x64 Arm64 x64 x86	Arm64 x64 Arm64 x64 x86	
All	dotnet-install scripts			winget instructions	/ /	
Viewal Stor	dio support		All	dotnet-install scripts		
	lio 2022 (v17 6)					

2.4.1. Once downloaded, execute the installer by executing dotnet-hosting-7.0.14-win.exe





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

👹 Microsoft .NET 7.0.14 - Windows Server Hosting Setup 🦳 —	
.NET Microsoft .NET 7.0.14 Windows Server Hosting	
Setup Progress	
Processing: Microsoft .NET Runtime - 7.0.14 (x86)	
	<u>C</u> ancel
₿ Microsoft .NET 7.0.14 - Windows Server Hosting Setup —	□ ×
.NET Microsoft .NET 7.0.14 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 [Versi (c) 2018 Microsoft Corpo	on 10.0.17763.4252] ration. All rights reserved.		^
C:\Users\ >d	lotnet		
Usage: dotnet [options] Usage: dotnet [path-to-a	pplication]		
info Disp list-sdks Disp list-runtimes Disp path-to-application:	lay help. lay .NET information. lay the installed SDKs. lay the installed runtimes. tion .dll file to execute.		
C:\Users [\]			Ĵ

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

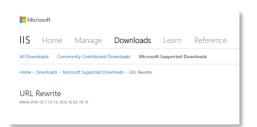


2.5 Microsoft IIS URL Rewrite Module 2.1

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

Microsoft IIS URL Rewrite Module 2.1

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



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

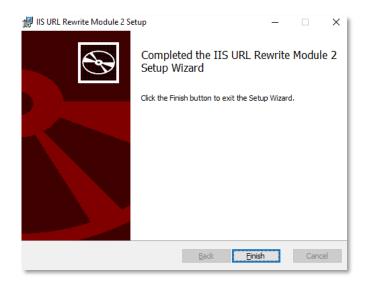
Down	load URL Rewrite Module 2.1
• E	nglish: x86 installer / x64 installer
• G	erman: x86 installer / x64 installer
• S	panish: x86 installer / x64 installer
• Fi	rench: x86 installer / x64 installer
• It	alian: x86 installer / x64 installer
• Ja	apanese: x86 installer / x64 installer
• K	orean: x86 installer / x64 installer
• R	ussian: x86 installer / x64 installer
• c	hinese Simplified: x86 installer / x64 installer
• c	hinese 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.





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

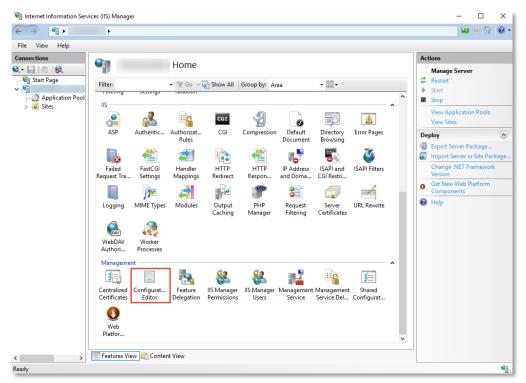


2.5.6. Click **Finish** once the installation process is complete.



2.6 Unlock system.webServer/serverRuntime section in IIS

- 2.6.1. Launch the IIS Manager
- 2.6.2. Select Server from left panel
- **2.6.3.** Open **Configuration Editor** from right pane under the Management section.



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

> ••••	•		🔤 🖂 🙆		
File View Help					
onnections	Configuration Editor		Actions		
🔍 - 🗔 🖄 😣 📲 Configuration Editor		E Apply			
📲 Start Page	Section: system.webServer/serverRuntim	e 👻	Cancel		
1		TABBLOCT	Generate Script		
Application Pools	Deepest Path: MACHINE/WEBROOT/APPHOST alternateHostName				
> - 🗃 Sites	appConcurrentReguestLimit	5000	Configuration Search Configuration		
	authenticatedUserOverride	UseAuthenticatedUser			
	enabled	True	Section		
	enableNagling	False	Unlock Section		
	frequentHitThreshold	2	Help		
	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

4.1 Fresh Installation of ADSS Web RA

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

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

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



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

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

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

The following welcome screen is shown:

•	🐍 Web RA Installer
	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
	Next Can

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:

	-		×
← 🔏 Web RA Installer			
Checking System Requirements			
Microsoft .NET Framework v4.8 or above		Success	
ASP .Net Core v7.0.0 or above Microsoft Internet Information Services (IIS) v10.0 or above		Success Success	
URL Rewrite in Internet Information Services (IIS) ASP .Net Core Module in Internet Information Services (IIS) runtime support		Success Success	
E	Next	Can	cel

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

- 🔥 Web RA Installer		-		×
Installation Type				
Install Web RA for the first time				
✓ Include sample data				
Install Web RA as another instance within a load-balanced confi	guration			
Install Web RA with an existing database				
O Upgrade an existing Web RA instance to the latest one				
O Change database credentials				
O Uninstall Web RA				
		Next	Ca	ncel

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

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



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

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

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

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

4.1.6 Click the Next button to show the License Agreement.

License Agreemen	it	
ASCERTIA SERVER SOFT	TWARE LICENSE AGREEMENT READ CAREFULLY:	^
1.0 ACCEPTANCE.		
Product) in this installa legal entity that will be agreement. You or the Agreement by clicking	ertia") is willing to license this software (the Software) and documentation (together tion package to you as an individual or as an authorised representative of the comp- using the Software only on condition that you accept all of the terms of this license company or legal entity (referred to as the Licensee) can accept the terms of this Lic on the "1 agree" button below, and proceed with the installation. To reject the terms (dick on the "1 disagree" button below and exit the installation process and make n vare.	any or ense s of
BOUND BY THE TERMS	SING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISE TO B 5 OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMEN THE ASCERTIA SOFTWARE.	
Licensee and Ascertia n	nay hereinafter be referred to as individually, a "Party", or, together, the "Parties."	
2.0 LICENSE		
without charge until th	u acquired the license for the Software on an evaluation basis, you may use the Softw e evaluation limits are reached or for a maximum of 3 months from the day that you ther this you must pay the appropriate license fee to continue to use the Software. To	1

4.1.3. Click the I Agree button to proceed.

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

Web RA Database	Configurations		
Database Managemer	nt System Type		
Microsoft SQL	Server		
Installation Type			
Basic	Advanced		
Database Configuration	ons		
Database Server:	Production-Server]	
Port:	1433		
Database Name:	WebRA]	
	Use windows authentication		
Username:	sa]	
Password:	****]	
	L		

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



0

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

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

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

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

- 🔏 Web RA Installer		
Web RA Database Con	figurations	
– Database Management Syst	em Type	
Microsoft SQL Serve	r	
Installation Type		
⊖ Basic	Advanced	
Database Configurations		
Connection String:	data source= Production-Server;initial catalog= WebR4;user id=sa;password=password;MultipleActiveResultSets=True;Pooling=true	
	Next	Cano



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

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

The following table entails details of the Advanced Installation type:

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

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

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

onnections	Applicatio	n Pools				
		nd manage the list of applicati	on pools on the serv	er. Application pools a	re associated with worker processes, con	tain one or more applications, and pro-
Application Pools	Filter:	• 🐨 Go 🕞 🖓 Show All	Group by: No Grou	uping •	Advanced Settings	? >
 	Name	Status JAET CLR V Started v4.0 Started	Managed Pipel Integrated Classic Integrated Integrated Integrated	ApplicationPoold ApplicationPoold ApplicationPoold ApplicationPoold ApplicationPoold ApplicationPoold ApplicationPoold ApplicationPoold	Enable 32-Bit Applications Managed Pipeline Mode Name Curve Length Start Mode Curve Length Start Mode Curve Length Limit Action Limit Action Limit Action Limit Action Limit Action Limit Action Mark (64-bit c Constant Pice Generation Identity Ide Time-out Action Identity Identity Pipe, username, password]	ascertia0\webra.qa 4 20 Terminate

4.1.8 Click the Next button to select specific modules:

	_		×
← 🔏 Web RA Installer			
Web RA Modules			
Fully Qualified Domain Name: webra.ascertia.com.pk			
 Fully qualified domain name will be set for the all instances in system settings. It will not update t setting for existing instances. 	he syster	n	
☑ Web RA Admin			
Website Name: admin Port: 443			
Web RA Web			
Website Name: web Port: 81			
☑ Web RA API (RESTful Web Services)			
Website Name: api Port: 82			
	Next	Car	ncel

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

v	/eb 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):	ssidevice	Port:	86]	

4.1.10Select **Windows Enrolment**. For each selected application, provide the web application name and port. Then click **Next**.

		-		×
← 🔏 Web RA Installer				
Windows Enrolment Modules				
Vindows 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) windowsSsICesService	Port:	92		
		lext	Can	rel
		TEAL	Can	

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

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

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



4.1.11Click the Next button to configure the SMTP Server and Email Settings.

Email Configurati	ons		
- 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 Configu	rations		
To:	support@ascertia.com		
	In case of errors/warnings emails will be sent at this addr	ess.	
Subject:	Web RA Notification Test Email		
	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.

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

ltem	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.				
То	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.

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

	_		×
← 🔧 Web RA Installer			
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			
	Next	Car	ncel

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.

1			
Installation Progress			
			L
Executing database script for Web RA on database: WebRA-Database		^	1
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			L
Creating windows integrated CEP service site : windowsIntegratedCepServi	ce		
Creating windows integrated windows CES service site : windowsIntegrated			L
Creating UserName/Password windows CEP service site : windowsIntegrate			L
Creating UserName/Password windows CES service site : windowsIntegrate	dCesService		
Creating SSL windows CEP service site : windowsIntegratedCepService			L
Creating SSL windows CES service site : windowsSsICesService			L
Updating system settings			Ŀ
Web RA installation completed!		~	L

4.1.13Click **Finish** to complete the installation process.



4.1.14ADSS Web RA URLs

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

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

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-defaultadmin.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. .



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.

- 🔏 Web RA Installer	-		×
Installation Type			
Install Web RA for the first time			
Install Web RA as another instance within a load-balanced configuration			
Install Web RA with an existing database			
O Upgrade an existing Web RA instance to the latest one			
Change database credentials			
O Uninstall Web RA			
	Vext	Car	ncel
	WCA'L		reel

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 (tog		
Product) in this installation package to you as an individual or as an authorised representative of the		r
legal entity that will be using the Software only on condition that you accept all of the terms of this li- agreement. You or the company or legal entity (referred to as the Licensee) can accept the terms of th		
Agreement by clicking on the "I agree" button below, and proceed with the installation. To reject the		
this License Agreement, click on the "I disagree" button below and exit the installation process and m	ake 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 AGREE		>
NOT INSTALL OR USE THE ASCERTIA SOFTWARE.		
Licensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Partie	s."	
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 th		
install the Software. After this you must pay the appropriate license fee to continue to use the Software	re. To pay	2 23



- 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**.

Veb RA Database	Configurations		
Database Managemer	it System Type		
Microsoft SQL	Server		
Installation Type			
Basic	Advanced		
Database Configuratio	ns		
Database Server:	Production-Server		
Port:	1433		
Database Name:	WebRA		
	Use windows authentication		
Username:	sa		
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.

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



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



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

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

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

🔶 🤧 Web RA Installer		×
Web RA Database Cont	ïgurations	
 Database Management Syste Microsoft SQL Server 		
Installation Type	Advanced Advanced	
Database Configurations Connection String:	data source= Production-Server;initial catalog= WebRA;user id=sa;password=password;MultipleActiveResultSets=True;Pooling=true	
	Next Ca	ncel

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:

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

4.2.7 Click the Next button to select Web RA Modules.

	-		×
← 💑 Web RA Installer			
Web RA Modules			
Fully Qualified Domain Name: webra.ascertia.com.pk			
In the set of the set of the set of the set for the all instances in system settings. It will not update setting for existing instances.	the syste	m	
☑ Web RA Admin			
Website Name: admin Port: 443			
☑ Web RA Web			
Website Name: web Port: 81			
☑ Web RA API (RESTful Web Services)			
Website Name: api Port: 82			
	Next	Car	ncel



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

 Web RA Installer eb 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			
			N	lext	Can	cel

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

indows 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)	windowsSsICepService	Port:	91	_
Certificat Enrolement Service (CES)	windowsSsICesService	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.



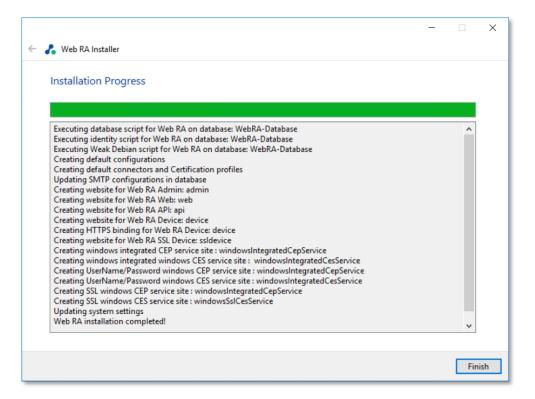
The following table explains the **Windows Enrolment** section.

ltem	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 Installer			
Mich DA Installation Common			
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			
И	lext	Cano	el

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



4.2.11 Click Finish to complete the installation process.

4.2.12ADSS 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</machine-name>	https://localhost:443
ADSS Web RA Desktop Web	https:// <machine-name>:PORT</machine-name>	https://localhost:81
ADSS Web RA API	https:// <machine-name>:PORT</machine-name>	https://localhost:82
ADSS Web RA Device	https:// <machine-name>:PORT</machine-name>	http://localhost:83 https://localhost:84
ADSS Web RA SSL Device	https:// <machine-name>:PORT</machine-name>	https://localhost:85 https://localhost:86
ADSS Web RA Windows Integrated CEP Service	https:// <machine-name>:PORT</machine-name>	https://localhost:87
ADSS Web RA Windows Integrated CES Service	https:// <machine-name>:PORT</machine-name>	https://localhost:88
ADSS Web RA Windows SSL CEP Service	https:// <machine-name>:PORT</machine-name>	https://localhost:89
ADSS Web RA Windows SSL CES Service	https:// <machine-name>:PORT</machine-name>	https://localhost:90



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



4.3 Installing ADSS Web RA with an Existing Database

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

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

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

4	_		×
Web RA Installer			
Installation Type			
O Install Web RA for the first time			
O Install Web RA as another instance within a load-balanced configuration			
Install Web RA with an existing database			
O Upgrade an existing Web RA instance to the latest one			
Change database credentials			
🔿 Uninstall Web RA			
	Next	Can	cel

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

icense Agreement	
ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT	^
MPORTANT - PLEASE READ CAREFULLY:	
1.0 ACCEPTANCE.	
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (top Product) in this installation package to you as an individual or as an authorised representative of the egal entity that will be using the Software only on condition that you accept all of the terms of this li agreement. You or the company or legal entity (referred to as the Licensee) can accept the terms of t Agreement by clicking on the "I agree" button below, and proceed with the installation. To reject the his License Agreement, click on the "I disagree" button below and exit the installation process and n further use of the software.	company or icense this License e terms of
	C TO DE
BY INSTALLING AND USING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISI BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGRE NOT INSTALL OR USE THE ASCERTIA SOFTWARE.	
icensee and Ascertia may hereinafter be referred to as individually, a "Party", or, together, the "Partic	es."
2.0 LICENSE	
Evaluation Copy. If you acquired the license for the Software on an evaluation basis, you may use the without charge until the evaluation limits are reached or for a maximum of 3 months from the day the install the Software. After this you must pay the appropriate license fee to continue to use the Software.	hat you

- **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:

Database Managemen	t System Type	
Microsoft SQL		
Installation Type		
Basic	○ Advanced	
Database Configuratio	ns	
Database Server:	Production-Server	
Port:	1433	
Database Name:	WebRA	
	Use windows authentication	
Username:	sa	
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.

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



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



The following table explains the Database Configurations.

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

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

Database Management Syste	figurations em Type	
Microsoft SQL Serve	r	
Installation Type		
○ Basic	Advanced	
Database Configurations		
Connection String:	data source= Production-Server;initial catalog= WebRA;user id=sa;password=password;MultipleActiveResultSets=True;Pooling=true	

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

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

The following	table explains	the Advanced	Database	Configurations.
into rono ming	Cable explaine		Dutubuoo	ooningarationo.

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

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

/eb RA Modules					
Fully Qualified Dom	nain Name:	webra.ascertia.com.pk			
Fully qualified de setting for existin		be set for the all instances in sys	tem settings	. It will not update	the system
Web RA Admin					
	Website Name:	admin	Port:	443	
Web RA Web					
	Website Name:	web	Port:	81	
🗹 Web RA API (RE	STful Web Service	s)			
	Website Name:	api	Port:	82	

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 Device		
HTTP (Install SCEP) Website Name:	device	Port: 84
HTTPS (Install CMP, ACME, EST)		
Website Name (CMP, ACM	E, EST): device	Port: 85
Client Authentication (Install EST)		
Website Name (EST):	ssldevice	Port: 86

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

indows Enrolment Modules				
Vindows 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)	windowsSsICepService	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. The names will appear as websites under IIS.



The following table explains the Windows Enrolment Modules.

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

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

				-		×
🔶 者 Web RA Installer						
Web RA Installation S	ummary					
The following modules will - Web RA Admin	be installed:					
- Web RA Web						
 Web RA API (RESTful Web Web RA Device 	Services)					
- Web RA SSL Device - Web RA Windows Enrolm	ent Services					
			N	ext	Can	cel

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.

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 We Device: ssldevice		
Creating windows integrated CEP service site : windowsIntegratedCepService		
Creating windows integrated windows CES service site : windowsIntegratedCesSer		
Creating UserName/Password windows CEP service site : windowsIntegratedCepSe		
Creating UserName/Password windows CES service site : windowsIntegratedCesSer	rvice	
Creating SSL windows CEP service site : windowsIntegratedCepService		
Creating SSL windows CES service site : windowsSslCesService		
Updating system settings Web RA installation completed!		
Web KA installation completed:		~

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

4.3.11ADSS 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</machine-name>	https://localhost:443
ADSS Web RA Desktop Web	https:// <machine-name>:PORT</machine-name>	https://localhost:81
ADSS Web RA API	https:// <machine-name>:PORT</machine-name>	https://localhost:82
ADSS Web RA Device	https:// <machine-name>:PORT</machine-name>	http://localhost:83 https://localhost:84
ADSS Web RA SSL Device	https:// <machine-name>:PORT</machine-name>	https://localhost:85 https://localhost:86
ADSS Web RA Windows Integrated CEP Service	https:// <machine-name>:PORT</machine-name>	https://localhost:87
ADSS Web RA Windows Integrated CES Service	https:// <machine-name>:PORT</machine-name>	https://localhost:88
ADSS Web RA Windows SSL CEP Service	https:// <machine-name>:PORT</machine-name>	https://localhost:89
ADSS Web RA Windows SSL CES Service	https:// <machine-name>:PORT</machine-name>	https://localhost:90

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



4.4 Upgrading ADSS Web RA

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

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

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

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

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

	-		×
🔶 🔏 Web RA Installer			
Installation Type			
O Install Web RA for the first time			
O Install Web RA as another instance within a load-balanced configuration			
O Install Web RA with an existing database			
Opgrade an existing Web RA instance to the latest one			
Change database credentials			
O Uninstall Web RA			
_			
L	Next	Car	ncel

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

license Agreement	
ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT	^
IMPORTANT - PLEASE READ CAREFULLY:	
1.0 ACCEPTANCE.	
Asceria Limited ("Ascertia") is willing to license this software (the Software) and documentation (toge Product) in this installation package to you as an individual or as an authorised representative of the co legal entity that will be using the Software only on condition that you accept all of the terms of this lice agreement. You or the company or legal entity (referred to as the Licensee) can accept the terms of this A greement by clicking on the "I agree" button below, and proceed with the installation. To reject the t this License Agreement, click on the "I disagree" button below and exit the installation process and mal further use of the software.	ompany or ense s License erms of
BY INSTALLING AND USING THIS ASCERTIA SOFTWARE, YOU AGREE FOR YOU OR YOUR ENTERPRISE T BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEN 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 S without charge until the evaluation limits are reached or for a maximum of 3 months from the day that install the Software. After this you must pay the appropriate license fee to continue to use the Software	t you



4.4.4. Click the I Agree button to proceed

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

Web RA Installer	
Existing Web RA Configurations	
Browse the existing Web RA installation directory:	
C:\WebRA-Deployment\WebRA_AGCE\WebRA-v2.8-Win64-12Jun2023	Browse
Before continuing - ensure that you have taken a backup of the ADSS Web RA	

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

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

						-		×
←	💦 Web RA Installer							
	Web RA Modules							
	Web RA Admin Website Name: admin Port: 444							
	Web RA Web	Vebsite Name: web	Por	t: 81				
	Web RA API (RES	ul Web Services) Vebsite Name: api	Por	t: 83				
					N	ext	Car	icel



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

Web RA Device					
- ₩ HTTP (Install SCI		device	Port:	84	
HTTPS (Install C	MP, ACME, EST)				
Website	Name (CMP, ACME, EST):	device	Port	85	
Client Authentic	ation (Install EST)				
Website	Name (EST):	ssIdevice	Port:	86	

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

indows Enrolment Modules			
Vindows 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)	windowsSsICepService	Port:	91
Certificat Enrolement Service (CES)	windowsSslCesService	Port:	92

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



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

Web RA Upgrade Summary		
Existing Installation		
Installation Path: C:\Installer\WebRA-v2.1-Win64-31Mar2020		
Web RA Version: 2000		
Web RA Database Version: 2000		
Machine Name / Port: 192.168.2.64 / 1433		
Database Name: WEBRA		
New Installation		
Installation Path: C:\Installer\WebRA-v2.1-Win64-31Mar2020		
Web RA Version: 2100		
Web RA Database Version: 2100		
Machine Name / Port: 192.168.2.64 / 1433		
Database Name: WEBRA		

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

Upgrade Progress	
Changing website paths to the new Web RA directory	<u>^</u>
Updating system settings	
Web RA upgrade completed!	
	~

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

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



4.5 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)

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

	-		×
🔶 🔏 Web RA Installer			
Installation Type			
○ Install Web RA for the first time			
Install Web RA as another instance within a load-balanced configuration			
O Install Web RA with an existing database			
O Upgrade an existing Web RA instance to the latest one			
O Change database credentials			
O Uninstall Web RA			
	Next	Can	cel

4.5.2. Click the Next button to show the License Agreement.



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

				_		×
←	🐍 Web RA Installer					
	Web RA Database Co	nfigurations				
	Database Management Sys	stem Type				
	Microsoft SQL Service	er				
	Installation Type					
	Basic	Advanced				
	Database Configurations					
	Database Server:	Production-Server				
	Port:	1433				
	Database Name:	WebRA				
		Use windows authentication				
	Username:	sa				
	Password:	******				
			Ne	st	Car	cel

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

Install	ation Progress	
	-	
C I		
	ng database credentials process started A Admin database credentials changed	
	A Web database credentials changed	
	A API database credentials changed A Device database credentials changed	
Web RA	A SSL Device database credentials changed	
	A Windows Integrated CEP service database credentials changed A Windows Integrated CES service database credentials changed	
Web R/	Windows UserName/Password CEP service database credentials changed	
	A Windows UserName/Password CES service database credentials changed A Windows SSL CES service database credentials changed	
Web R/	Windows SSL CES service database credentials changed	
Changi	ng database credentials process completed	
		\sim

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



5 ADSS Web RA Uninstallation

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

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

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

🗧 者 Web RA Installer	_		×
Installation Type			
○ Install Web RA for the first time			
Install Web RA as another instance within a load-balanced configuration			
O Install Web RA with an existing database			
O Upgrade an existing Web RA instance to the latest one			
Change database credentials			
Uninstall Web RA			
	Next	Can	cel

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

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

		-		×
← ,	🐍 Web RA Installer			
	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			
	Γ	Next	Can	cel



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

Uninstallation Progress	
Uninstallation process started Uninstalling Web RA Admin module	^
Uninstalling Web RA Web module Uninstalling Web RA Web Services API module Uninstalling Web RA Device module	
Uninstalling Web RA SSL Device module Uninstallation process completed	т
	~

5.5. 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.



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 ×	Permissions for WebRA X	
General Sharing Security Previous Versions Customize	Security	
Object name: D:\WebRA Group or user names:	Object name: D:\WebRA Group or user names:	
総 SYSTEM 総 Administrators (DOTNET-TAHSEEN\Administrators) 総 Users (DOTNET-TAHSEEN\Users)	Authenticated Users SYSTEM Administrators (DOTNET-TAHSEEN Vadministrators) Set (DOTNET-TAHSEEN Vaers)	
To change permissions, click Edit. Edit Permissions for Authenticated Users Allow Deny	Add Remove	
Full control Modify Read & execute List folder contents	Permissions for Authentinstand Users Select Users or Groups Full contro Modify Select this object type:	>
Read V Write V	Read & ex Users, Groups, or Built-in security principals	Object Types
For special permissions or advanced settings, Advanced click Advanced.	Read DOTNET-TAHSEEN	Locations
OK Cancel Apply	Enter the object names to select (<u>examples</u>): IIS_IUSRS	Check Names
Mail WebRA	12/14/2018 4/10/2020 10 Advanced OI	< Cancel



• 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.

	Certificate	
aul Jos		×
Jos ←	🐓 Certificate Import Wizard	- 1
llar		- 1
llar		- 1
vin vin	Welcome to the Certificate Import Wizard	- 1
ub-		- 1
	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	- 1
	O Current User	- 1
	Local Machine	
	To continue, dick Next.	- 1
		- 1
		- 1
		- 1
	Cance	

• 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.

A					Actions
Modules					Add Managed Module
Use this feature to configure the n	ation and managed code module	that process requests made	to the Web server		Configure Native Modules
	and and managed code module	s one process requests mass	to the may perior.		Edit
Group by: No Grouping .					X Remove
Name	Code	Module Type	Entry Type	^	Revert To Parent
DirectoryListingModule	%windir%\System32\inetsrv\	Native	Inherited		View Ordered List
DynamicCompressionModule	%windir%\System32\inetsrv\	Native	Inherited		
DynamiclpRestrictionModule	%windir%\System32\inetsrv\	Native	Inherited		😢 Help
FailedRequestsTracingModule	%windir%\System32\inetsrv\i	Native	Inherited		
FastCgiModule	%windir%\System32\inetsr\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		
ISCertificateMappingAuthenti	%windir%\System32\inetsrv\	Native	Inherited		
IpRestrictionModule	%windir%\System32\inetsr/\i	Native	Inherited		
IsapiFilterModule	%windir%\System32\inetsrv/d	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		
UnAuthorizationModule	%windir%\System32\inetsrv\	Native	Inherited		
UrlMappingsModule	System.Web.UrlMappingsMo	Managed	Inherited		
UrlRoutingModule-4.0	System.Web.Routing.UrlRouti	Managed	Inherited		
WebDAVModule	%windir%\System32\inetsr/\	Native	Inherited		
WebSocketModule	%windir%\System32\inetsrv\i		Inherited		
WindowsAuthentication	System.Web.Security.Window	Managed	Inherited		
WindowsAuthenticationModule	%windir%\System32\inetsrv\	Native	Inherited		
Features View 💦 Content View	v.				
terre and the second se					

</system. </location>



6.2 Configurations used for Simple Certificate Enrollment Protocol (SCEP)

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

<	security>
	<requestfiltering></requestfiltering>
	<requestlimits maxquerystring="8192"></requestlimits>
	<pre>configuration> <location inheritinchildapplications="false" path="."> <aystem.webserver> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <handlers> <hand< td=""></hand<></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></handlers></aystem.webserver></location></pre>

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

</configuration> <!--ProjectGuid: 31d1b205-525a-481e-bd32-4378e4f6559d-->

- "[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, reporturi='https://adminra.signinghub.com'" />

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

C:\Windows\System32\cmd.exe	-	×
Microsoft Windows [Version 10.0.18363.778] (c) 2019 Microsoft Corporation. All rights reserved.		^
E:\onlineservices\WebRA\2.1\web>dotnet WebRA.Web.dll		
		\sim

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



C\Windows\System32\cmd.exe	 	×
Microsoft Windows [Version 10.0.18363.778] (c) 2019 Microsoft Corporation. All rights reserved.		^
:\onlineservices\WebRA\2.1\admin>dotnet WebRA.Admin.dll		

6.3 SSL Certificates

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

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

6.3.1 Exporting Root and Intermediate Certificates

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

💽 Certificate	×
General Details Certification Path	
Certification path	
Certificate status:	View Certificate
This certificate is OK.	
	OK

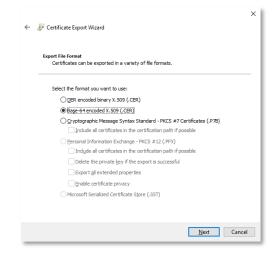
6.3.4 Select the Certification Path tab from the top. The default ADSS Web RA TLS certificate has one root certificate. Select the root certificate and click the View Certificate button. A new window will appear showing general details of the intermediate certificate.

🔲 Certificate			×
General Details	Certification F	Path	
Show: <all></all>		\checkmark	
Field		Value	^
Version	er	V3 0117271aac7a7a1524	
Signature a	algorithm	sha256RSA	
Signature ł	ash algorithm	sha256	
Issuer		ADSS Default Root CA, Asce	erti
Valid from		16 January 2014 08:43:02	
Valid to		09 September 2030 08:43:0	b.d.
Subject		ADSS Samples Test CA Asr	ert T
		Edit Properties Copy to	
		L	ОК

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

← <i>∰</i> Certificate Export Wizard	×
Welcome to the Certificate Export Wizard	
This witard 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, dick Next.	
<u>N</u> ext Cance	1

6.3.6 Click Next.



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

×	← 😺 Certificate Export Wizard
	File to Export Specify the name of the file you want to export
	File name:
	C: \$W/WEBKA-Y1WINDOWO+JICC2012/\$Ectip (Set 5 KoorCA.CE
	Next
	C:\sw\WEBRA-v1.0-\WIndow64-01Oct2019\setup\certs\RootCA.ce

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

← 🛿 ← 🖉 Certificate Export Wizard	>	<
Completing the Certificate Ex	port Wizard	
You have successfully completed the Certificate	e Export wizard.	
You have specified the following settings:		- 1
File Name	C:\sw\WebRA-v1.0-Win64-01Oct2019	- 1
Export Keys	No	- 1
Include all certificates in the certification path	No	- 1
File Format	Base64 Encoded X.509 (*.cer)	- 1
		- 1
		- 1
<	>	- 1
		- 1
		- 1
		- 1
		- 1
		- 1
		- 1
	<u>F</u> inish Cancel	

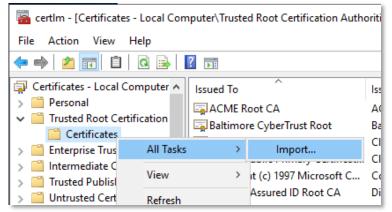
6.3.9 Click Finish to complete the root certificate export process.



6.4 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.

- 6.4.1 Launch certim.msc from the command prompt.
- 6.4.2 Expand the Trusted Root Certification Authorities folder from the left panel and right-click on Certificates. Now select All Tasks and then Import...



6.4.3 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 <u> <u> <u> </u> <u></u></u></u>	
	To continue, dick Next.	
	<u>N</u> ext Cance	I

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

← 🛿 🐉 Certificate Import Wizard	X
File to Import Specify the file you want to import.	
Eile 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 formate Personal Information Exchange- PKCS #12 (.PFX,.P12)	5:
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)	
Next	Cancel

6.4.5 Click Next to proceed.

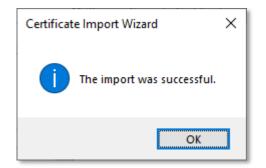
	icate Store					
C	ertificate st	ores are system a	areas where certi	ficates are kept.		
v t	Vindows car he certificat	automatically sel	ect a certificate s	tore, or you car	specif	y a location for
	◯ A <u>u</u> tom	atically select the	certificate store	based on the ty	pe of ce	ertificate
	Place a	all certificates in th	ne following store			
	Certif	cate store:				
	Trus	ted Root Certifica	tion Authorities			Browse

 ~ 1

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

÷	F Certificate Import Wizard		
	Completing the Certific	ate Import Wizard	
	The certificate will be imported after y	rou dick Finish.	
	You have specified the following setting	ngs:	
	Certificate Store Selected by User	Trusted Root Certification Authorities Certificate	
		C: \sw\WebRA-v1.0-Win64-01Oct2019\setup\certs\R	
	<	>	
		<u>F</u> inish Cancel	

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



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



6.5 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.

6.5.1 Launch the IIS Manager.

ile View Help		
Interctions	WEBDEV_01 Home Fitter:	Actions Manage Server Peters Seat Stop View Application Peols View Stes Change NET Framework Version Peology NET Framework Version Change NET Framework Version
	5 Authentic- Compression Defusit Authentic- Compression Defusit SAME Types Modules Output SAME Types Modules Output Example Authentice Caching Results Sample Authentice Sample	

6.5.2 Click the Server Name from the Server Connections.

Solution Solution		1 III III III III III III III III III I
Connections	WEBDEV_01 Home Image: State S	Actions Manage Server Restant Stat Stop View Application Pools View Stat Change AET Framework Version Pholp Online Help
	Image: SAVE Filters Logging MME Types Modules Worker Filtering Server URL Rewrite Worker Worker Processes Magagement Modules Water Server URL Rewrite Imagement Imagement <td></td>	
ady	Configurat Editor Delegation Configurat	



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

] Internet Information Services (IIS) Manager					- D ×
🚱 💿 📲 🖌 WEBDEV_01 🔸					🖬 🗟 😧 •
File View Help					
	Server Cel Use this feature to reque Name		he Web server can use with Web s Issued By	ites configured for SSL. Expiration Date	Actions Import Create Certificate Request Complete Certificate Request Create Self-Signed Certificate Create Self-Signed Certificate Online Help
	*				
	Features View 🍋 Con	tent View			
ady					

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

Create Self-Signed Certificate	8 X
Specify Friendly Name	
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:	
OK	Cancel



6.5.5 Provide a meaningful name and press OK.

S Internet Information Services (IIS) Manager					
() () () () () () () () () () () () () (🖬 🛯 🔂 🔞 •
File View Help					
File View Help Connections	Server Cer Use this feature to request Name locathestssl		e Web server can use with Web sit Browd By Webdec_01	tes configured for SSL. Expiration Date 2/20/20337.00	Actions Import Create Certificate Request Consiste Certificate Create Self-Signed Certificate Online Help
1	e			,	
	Features View 💦 Cont	ient View			
Ready					9 .:

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.



6.6 Generate a CSR for an SSL Certificate

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

6.6.1 Launch certim.msc from the command prompt.

👼 ce	rtlm - [C	ertificates - Local Computer\l	Personal	1			-		×	
<u>F</u> ile	<u>File Action View Help</u>									
<₽ ⇒) 🖄 [🖬 🗎 🗟 📑 🚺								
	rtificates Persona	- Local Computer	^	Object Type						
~ 🚞	Trus	Find Certificates		There are no i	items to	o sho	w in this	view.		
> 🗎	Ente	All Tasks	F	ind Certificates						
✓ 📋	Inte	View >	R	Request New Certificate						
		Refresh	h	mport						
> 🖺	Trus	Export List	A	Advanced Operations	>		Create	Custom	Request	
> 🖺	Unt Thir	Help	ies				Manag	je Enrollr	ment Policies	
>	Trusted	People	les l							

6.6.2 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.

	-		×
🛱 Certificate Enrollment			
Before You Begin			
The following steps will help you install certificates, which are digital credentials use networks, protect content, establish identity, and do other security-related tasks.	d to conne	ct to wire	eless
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			
C	Next	Can	cel

6.6.3 Press Next to proceed.

		-		×
📮 Ce	ertificate Enrollment			
	Select Certificate Enrollment Policy			
	Certificate enrollment policy enables enrollment for certificates based on predefined Certificate enrollment policy may already be configured for you.	certificate	templates	
	Configured by you		Add Net	N
	Custom Request			
	Proceed without enrollment policy			
		<u>N</u> ext	Cance	ł

6.6.4 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:	<u> <u> </u> </u>			
	<u>○ <u>c</u>mc</u>			
	not available for certificates based on a custom certificate request the certificate template.	, even wl	hen this	
	N	lext	Canc	el

6.6.5 Accept the default values and press Next without changing anything

ertificate Information			
lick Next to use the options already se equest, and then click Next.	elected for this template, or click Details to o	customize ti	he certificat
Custom request	③ STATUS: Available		Details 🕢
2 · ·	e uses and validity period that apply to this	s type of cer	tificate:
Key usage: Application policies:			
Validity period (days):			
Validity period (days):		E	properties
Validity period (days):		E	<u>P</u> roperties
Validity period (days):		E	<u>P</u> roperties
Validity period (days):		E	<u>P</u> roperties
Validity period (days):		E	2roperties

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

Certificate Properties		×
General Subject Extensions	Private Key	
		nich the certificate is issued. You and alternative name values that
Subject of certificate		
The user or computer that is re	eceiving the certificate	
Subject name:	_	
<u>T</u> ype:		CN=webra.pki.acme.com OU=Web Servers
Full DN \sim	Add >	O=ACME
<u>V</u> alue:	< Remove	C=GB
	< Remove	
Alternative name:	1	
Туре:		DNS
DNS ~		webra.pki.acme.com
Val <u>u</u> e:	Add >	
	Add >	
	< Remove	
	ОК	Cancel <u>A</u> pply



6.6.7 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	\times
General Subject Extensions Private Key	
The following are the certificate extensions for this certificate type.	^
Key usage The key usage extension describes the purpose of a certificate.	
Available options: Selected options: CRL signing Data encipherment Decipher only Add > Key agreement Add > Vertificate signing < Remove	
Extended Key Usage (application policies)]
Basic constraints	v
OK Cancel Ap	ply

- **6.6.8** Select the Extensions tab from the top. Select the Key usage option from the drop down extensions. Now from the Available options, choose the following:
- Digital signature
- Key encipherment
- Non repudiation

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

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

ertificate Properties		~
General Subject Extensions Private Key		
Extended Key Usage (application policies) An application policy (called enhanced key usage in certificates issued by this template. Available options: Client Authentication Code Signing Secure Email Time Stamping Microsoft Trus List Signin Microsoft True List Signin Microsoft True List Signin P security tunnel terminz		^
IP security user	< >>	
Make the Extended Key Usage critical		
Basic constraints	~	
Include Symmetric algorithm	*	~
	OK Cancel Apply	у



6.6.10 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.

Certificate Properties	×
General Subject Extensions Private Key	
<u>C</u> ryptographic Service Provider	*
Key <u>options</u>	^
Set the key length and export options for the private key.	
Key size: 2048 V	
Make private key exportable	
Allow private key to be archived	
Strong private key protection	
Select <u>H</u> ash Algorithm	*
Select Signature <u>F</u> ormat	*
Key germissions	~
OK Cancel	Apply

6.6.11 Press Next to proceed.

		-		×
Certificate Enrollment				
Certificate Information				
Click Next to use the options a request, and then click Next.	Iready selected for this template, or click Details to cus	tomize th	e certifica	ıte
Custom request	③ STATUS: Available		Details	^
Key usage:	scrübe the uses and validity period that apply to this typ Digital signature Key encipherment Non repudation Server Authentication :		ificate: roperties	
		<u>N</u> ext	Can	cel

6.6.12Browse 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.

	-		\times
📮 Certificate Enrollment			
Where do you want to save the offline request?			
If you want to save a copy of your certificate request or want to process the request to your hard disk or removable media. Enter the location and name of your certifici click Finish.			
File Name:			
C:\sw\webra.pki.acme.com.req	B	rowse	
File format: ●Bgse 64 ○ Binary			
	<u>E</u> inish	Can	cel

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

*** End of Document ***