

ADSS Web RA Server

Windows Enrolment

Deployment Guide

ASCERTIA LTD

AUGUST 2023

DOCUMENT VERSION- 1.0.4

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



Docume	Document Revisions				
Version	Date	Author	Action	Notes	
1.0.0	1 Jul 23	MH	Created	Initial draft	
1.0.1	3 Jul 23	MH	Created	Added custom enrolment group for computer certificates	
1.0.2	6 Jul 23	HS	Updated	Reformatting and proof-reading document	
1.0.3	13 July 23	HS	Updated	Reformatting and proof-reading document	
1.0.4	21 Aug 20	МН	Updated	Remove redundant steps and correct typos.	

CONTENTS

1 li	ntroduction	4
1.1	Scope	4
1.2	Intended Readership	4
1.3	Conventions	4
1.4	Technical Support	4
2 V	Vindows Certificate Enrolment	5
3 C	eployment Pre-Requisites	7
3.1	ADSS Server Pre-Requisites	7
3.2	ADSS Web RA Server Pre-Requisites	9
4 C	Configure Active Directory	. 10
4.1	Create a Windows service account	. 10
4.2	Create Windows Groups	. 12
4.3	Active Directory Schema Requirements	. 13
4.4	Adding Windows certificate templates to Active Directory	. 14
5 li	nstalling ADSS Web RA Server	. 25
5.1	ADSS Web RA Installation	. 25
5.2	Import CA certificates into Microsoft Group Policy	. 27
5.3	Configure IIS for Web RA Server	. 31
6 A	DSS Web RA Server Configuration	. 45
6.1	ADSS Web RA Admin Portal	. 45
7 A	ctive Directory Configuration	. 62
7.1	Create an enrolment service in Active Directory	. 62
7.2	Configure Certificate Enrolment	. 65



1 Introduction

This manual is intended for ADSS Web RA Server administrators responsible for installation and configurations of the Windows Certificate Enrolment. It describes an end-to-end flow, right from installation, to configurations and certificate issuance. It is assumed that the reader has a basic knowledge of digital signatures, certificates and information security.

1.1 Scope

This manual describes how to install and configure Ascertia ADSS Server and Microsoft Active Directory and Windows Servers and Clients to enable manual and automated certificate issuance of digital certificates.

1.2 Intended Readership

This manual is intended for use by Ascertia staff and customers who will be installing and configuring ADSS Server and ADSS Web RA Server to issue certificates within a Microsoft Active Directory Environment. It is assumed that the reader has a basic knowledge of standard Windows commands.

1.3 Conventions

The following typographical conventions are used in this guide to help locate and identify information:

- Bold text identifies menu names, menu options, items that can be clicked on the screen, file names, folder names, and keyboard keys.
- Courier New font identifies code and text that appears on the command line.
- Bold Courier New identifies commands that are required to be typed in.

1.4 Technical Support

If Technical Support is required, Ascertia has a dedicated support team. Ascertia Support can be reached/accessed in the following ways:

Website	https://www.ascertia.com
Email	support@ascertia.com
Knowledge Base	https://www.ascertia.com/products/knowledge-base/adss-server/
FAQs	https://ascertia.force.com/partners/login

In addition to the free support services detailed above, Ascertia provides formal support agreements with all product sales. Please contact <u>sales@ascertia.com</u> for more details.

When sending support queries to Ascertia Support team send ADSS Trust Monitor logs. Use the Ascertia's trace log export utility to collect logs for last two days or from the date, the problem arose. It will help the support team to diagnose the issue faster. Follow the instructions on how to run the trace log export utility.

2 Windows Certificate Enrolment

ADSS Web RA Server provides an implementation of the Microsoft WSTEP Windows Enrolment protocol for automating x.509 certificate issuance for public key infrastructure (PKI) clients. These include web servers, endpoint devices and user identities, and anywhere PKI certificates are used, as well as the associated certificates from a trusted Certificate Authority (CA). Windows Enrolment uses certificate enrolment policy to enrol identity certificates based on authentication scheme in deployment URLs. The following workflow explains how Windows enrolment works. (Typical Scenario)



Client connects to the CEP web service over HTTPS.

The Windows Client \ Windows Server computer is configured to enrol for certificates against ADSS Web RA CEP server. When CEP server is configured in the environment, the client will connect to the CEP server via port 443 (HTTPS), and connect to the Certificate Enrolment Policy (CEP) web service.

Administrators can configure via group policy to identify which CEP server to use. The configurations for CEP web service are further explained in this document.

CEP web service queries LDAP.

The CEP service will send an LDAP query to a domain controller to get the following:

- Queries for a list of *pKICertificateTemplate* objects (Certificate Templates) within the forest.
- Queries for a list of *pKIEnrollmentService* objects (Enterprise CA's) within the forest.
- Queries for a list of *msPKI-Enterprise-Oid* objects within the forest.

Once all the objects are collected and sent back to the client computer, it determines the types of certificates for which it can enrol and which enterprise CAs can issue those certificates. There is a new attribute in the CA's "*pKIEnrollmentService* object" that indicates the URLs for the CES servers in the environment to the client computer. The attribute name is *msPKI-Enrollment-Servers*. The attribute is a multi-valued string so there can be multiple URL's defined if you need to support different authentication methods.



Client connects to ADSS Web RA CES Web Service over HTTPS.

The client then connects to the Certificate Enrolment (CES) web Service that answers for the Certification Authority that is configured to issue the certificate. The actual CES URL is defined in *the msPKI-Enrollment-Servers* attribute on the *pKIEnrollmentService* object for that CA.

Web RA CES Web service requests a certificate

The ADSS Web RA CES web service requests a certificate from ADSS Server and then provides the certificate back to the client.



3 Deployment Pre-Requisites

The installation of ADSS Web RA Server Windows Enrolment requires the following prerequisites to be met.

Installation of:

- SMTP Server
- Microsoft Active Directory
- Microsoft Active Directory Clients (Windows 10, 11 or Server 2019, 2022 Domain Members)
- Windows Server 2019 Domain Member for Web RA Server to be hosted
- ADSS Server installed with Root and Issuing CA pre-configured

3.1 ADSS Server Pre-Requisites

Before installing the ADSS Web RA Server Windows enrolment feature, ADSS Server must be installed and configured. A Root and Issuing Certification Authority need to be created prior to installing the ADSS Web RA Server. The Issuing CA operator will need to create certification profiles required to issue certificates to Windows users, service accounts and domain computers.

When issuing certificates from ADSS Server using Windows Certificate Templates, it is important to note that the ADSS Server Certificate Template controls the certificate extensions, lifetime, and subject distinguished name, the Microsoft Certificate Template will control which Cryptographic Service Provider or Key Service Provider is used to generate the private key, and if the private key is exportable.

ADSS Server requires the following to be set in the certificate templates:

Subject Alternative Naming

Computer and User certificates can optionally contain the following attributes.

- Computer Certificates
 - o DNS Name
 - User Certificates
 - Email Address
 - User Principal Name

If you wish to issue certificates with any of the above subject alternative names, then they must be enabled in the ADSS Server Certificate Template, within the required certificate template, ensure that the following is enabled to add the required subject alternative name entries:

Note: Subject Alternative Names can contain multiple entries, it is common to see Email Address and User Principal Name in user certificates.

subject alternative name value	ADSS Server profile certificate extension
	Subject Alternative Name
DNS Name	dNSName



	 Subject Alternative Name rfc822Name otherName iPAddress dNSName directoryName uniformResourceIdentifier ediPartyName registeredID
Email Address	rfc822Name ✓ Subject Alternative Name ✓ rfc822Name otherName → iPAddress dNSName → directoryName uniformResourceIdentifier → ediPartyName registeredID
User Principal Name	OtherName Subject Alternative Name rfc822Name otherName iPAddress dNSName directoryName uniformResourceIdentifier ediPartyName registeredID

Subject Distinguished Name Handling

When ADSS Web RA Server sends a request to ADSS Server, the Certificate Enrolment Web Service queries Microsoft Active Directory to acquire information about the user or the computer requesting a certificate, in order to ensure that ADSS Server issues a certificate with the correct Subject Distinguished Name, you must ensure that the following is set within the ADSS Server Certification Profile:

Set the Subject Distinguished Name to \$REQUEST and mark this as Overridable

Certificate Details		
Crypto Profile*:	Software 🗸	
Key Algorithm:	RSA 🗸	Overrideable
Key Length:	2048 🗸	Overrideable
Subject Distinguished Name*:	\$REQUEST	Overrideable
	Match the pattern with subject DN in request	
Validity Period*:	12 Months 🗸	Overrideable
	Note:- The certificate template default expiry time is used if this values is set to zero.	
Valid From:	Time of Issuance	
	O Future Time	

Custom Extension Handling

Certificate templates must contain the following OID as a custom extension, note this does not need to be marked as critical, both represent Microsoft certificate extensions related to Microsoft Certificate Template and Certificate Types:

- 1.3.6.1.4.1.311.20.2
- 1.3.6.1.4.1.311.21.7

Custom Extensions	
Custom Extensions	
Extension OID*:	Critical
	Add
List of Extensions: 1 3 6 1 4 1 311	21.7(Non-Oritical)
1.3.6.1.4.1.311	20.2(Non-Critical)
	*
	Remove



To serve the purpose of this document, we will configure ADSS Web RA Server to issue certificate templates in Microsoft Active Directory that map to ADSS Server Certificate Profiles\Templates that are listed below:

- Computer Certificates
 - With Digital Signature Key Usage
 - Client \ Server TLS Extended Key Usage
- User Certificates
 - With Digital Signature Key Usage
 - Client TLS Extended Key Usage

3.2 ADSS Web RA Server Pre-Requisites

Before configuring the ADSS Web RA Server Windows enrolment feature, the following prerequisites are necessary:

- Install Windows Authentication IIS Security Feature.
- External connectors for:
 - o ADSS Server
 - o SMTP Server
 - Microsoft Active Directory
 - Authentication Profile for Microsoft Active Directory
 - Certification Profiles created at ADSS Server
- Create a service plan.
- Create an enterprise.
- Create a default role with Windows enrolment profile.
- Share certificate using the SDNs filter in the specific role.
- Import a license and allocate certificate quantities to the test enterprise.
- Ensure that all firewall ports are open that ADSS Web RA Services require.



4 Configure Active Directory

The following system and environment pre-requisites need to be fulfilled prior to the installation of the ADSS Web RA Server Windows Enrolment feature.

Domain Membership - If using Kerberos Authentication for Windows User and Machine enrolment, the server hosting ADSS Web RA Server must be a member of the Windows Domain where you plan to issue certificates.

4.1 Create a Windows service account

A Windows user account is required for the ADSS Web RA Server application pools to run.

- 1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
- 2. Expand Start > Windows Administrative Tools > Active Directory Users and Computers.
- 3. Active Directory Users and Computers management console will be displayed.
- 4. From the left panel, expand the domain, right-click the Users container, click New > User.



5. The New Object – User will appear. Enter a First Name, Last Name, and User logon name, click Next. The following is an example:

New Object - User		×
Create in:	ascertiademo Jocal/Users	
<u>F</u> irst name:	WebRA Initials:	
Last name:	Service	
Full n <u>a</u> me:	WebRA Service	
<u>U</u> ser logon name:		
webra_svc	@ascertiademo.local ~	
User logon name (pre	<u>-W</u> indows 2000):	
ASCERTIADEMO	webra_svc	
	< Back Next > Cance	el

6. Enter and confirm a strong password, uncheck User must change password at next logon, and check User cannot change password and Password never expires, click Next.

New Object - User	×
Create in: ascertiademo.local/Users	\$
Password:	••••
Confirm password:	••••
User must change password at next logon	
User cannot change password	
Password never expires	
Account is disabled	
< Back	Next > Cancel

7. The summary dialog will appear, click Finish.

New Object - User	×
Create in: ascertiademo.local/Users	
When you click Finish, the following object will be created:	
Full name: WebRA Service	^
User logon name: webra_svc@ascertiademo.local	
The user cannot change the password. The password never expires.	
	~
< Back Finish	Cancel

8. You will be returned to the Active Directory User and Computers management console, right-click the new service account and select Properties.





9. The Service Account User Properties dialog will display, enter their email address in the E-mail field, and click OK.

ebRA Servi	ce Prope	ties			?	>
		Console	Root\Acti	ve Directory Us	ers and	Con
Organizatio	n Me	ember Of	Dial-in	Environment	Sess	ions
Remote control		Remote Desktop Services Profile		COM+		
General	Address	Account	Profile	Telephones	Deleg	atior
8	WebRA S	èervice				
<u>First name:</u>		WebRA		Initials:		
Last name:		Service				
Display nam	ie:	WebRA Service				
Description						
Offi <u>c</u> e:						
Telephone	number:				<u>O</u> ther	
E- <u>m</u> ail:		webra_svc@	ascertiader	no.local		
Web page:					Othe <u>r</u>	

10. You will be returned to the Active Directory User and Computers management console, close the management console, the service account has been created successfully and is ready for use with Web RA.

4.2 Create Windows Groups

Windows Certificate auto-enrolment uses certificate templates that are stored in Active Directory. These templates instruct the Microsoft Certificate Services client where it should generate keys, the key length, if the private key should be exportable, etc.

During enrolment, clients download the certificate templates and check the Windows permissions on these templates to see if they have the permission to enrol or auto-enrol. Certificate template administrators set the enrol and auto-enrol permission when they create these templates. For this document a group will be created that will be used in the certificate templates to control enrolment.

- 1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
- 2. Expand Start > Windows Administrative Tools > Active Directory Users and Computers.
- 3. Active Directory Users and Computers management console will be displayed.
- 4. From the left panel, expand the domain, right-click the Users container, click New > Group



5. The New Object – Group dialog will display, enter ADSS Web RA Users in the Group name field, and click OK.

Create in: ascer	tiademo.local/Users	
Group name:		
ADSS Web RA UUsers		
Course and a state of the second	22).	
Group name (pre-Windows 20	00):	
ADSS Web RA UUSers		
Group scope	Group type	
O Domain local	Security	
Global	ODistribution	
OUniversal		
OUniversal		

6. You will be returned to Active Directory Users and Computers management console; the new group will have now appear on the right panel.



- 7. You have successfully created the Windows Certificate Enrolment Group.
- 8. Repeat this process for ADSS Web RA Computers.

4.3 Active Directory Schema Requirements

For Windows enrolment using ADSS Web RA Server, the Windows domain must have the 2016 Active Directory schema or later.

Check and verify the Active Directory schema version, open a PowerShell window and run the following command:



Example Output

Windows PowerShel Copyright (C) Mic	l rosoft Corporation. All rights reserved.
PS C:\Users\Admin	istrator> Get-ADObject (Get-ADRootDSE).schemaNamingContext - Version
FF	
DistinguishedName	: CN=Schema,CN=Configuration,DC=ascertialab,DC=local
Name ObjectClass	: Schema : dMD
ObjectGUID objectVorsion	: 984aee09-52f6-4e9a-8a5a-c948e113ebe8
objectVersion	: 88



4.4 Adding Windows certificate templates to Active Directory

The ADSS Web RA Server Windows enrolment service is Ascertia's implementation of the WSTEP protocol. The Ascertia WSTEP service will use Windows certificate templates when enrolling users, computers, or domain controllers with your Windows-native endpoints.

If Microsoft Active Directory Certificate Services is already installed in your Active Directory, the Certificate Templates feature is already installed and the certificate templates have already been published, you can skip this section. Otherwise, you must install the Certificate Templates feature using either Windows PowerShell or the Windows Server Manager graphical interface.

4.4.1 Adding the certificate templates feature using PowerShell

To add Certificate Templates using Windows PowerShell, complete the following procedure.

- 1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
- 2. Open an elevated PowerShell window. Expand Start > Windows PowerShell, then rightclick Windows PowerShell > Run as administrator.
- 3. Run the following command.

PS C:\Users\Administrator>Add-WindowsFeature RSAT-ADCS-Mgmt

Example Output



4. Run the following command to launch the Certificate Templates Console.

PS C:\Users\Administrator>C:\Windows\System32\certtmpl.msc

5. A Certificate Templates installation dialog will display, click Yes to install the new certificate templates.

Certificate Templates	\times
Windows has detected that new certificate templates should be installed. Do you want to install them?	
Yes No	



6. Click OK to the installation success message.



7. The Certificate Templates Console will appear.

Rertificate Templates Console				- 🗆 X
File Action View Help				
⇐ ➡ 📅 🍳 🗟 🗊				
Certificate Templates (ASC-DEN)	Template Display Name	Schema Version	^	Actions
	Administrator	1		Certificate Templates (ASC-DEMO-AD-01.ascertiademo.loc 🔺
	Authenticated Session	1		More Actions
	Basic EFS	1		
	CA Exchange	2		
	CEP Encryption	1		
	Code Signing	1		
	Computer	1		
	Cross Certification Authority	2		
	Directory Email Replication	2		
	Domain Controller	1		
	Domain Controller Authentication	2		

4.4.2 Adding the certificate templates feature using Server Manager

To add Certificate Templates using the Windows graphical interface, complete the following procedure.

- 1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
- 2. Launch Server Manager. Select Start > Server Manager.
- 3. The Server Manager Dashboard will be displayed.



4. Click Manage > Add Roles and Features.

5. The Add Roles and Features Wizard will launch, at the Before you begin dialog click Next.



6. At the "Installation Type" dialog click Next.

DESTI ASC-DEMO-AD-01.asc	IATION SEI Sertiademo.	RVER local
a nunning physical compu estures. e (VD) to create a virtual r	der or vir	tual
t	t > (rotali	t> Intall Care

7. At the "Server Selection" dialog click Next.





8. At the "Select Server Roles" dialog click Next.



 From the Select features dialog, expand Remote Server Administration Tools (4 of 43) > Role Administration (4 of 26) > Active Directory Certificate Services Tools and tick the check box to select Certificate Authority Management Tools, click Next.

Add Roles and Features Wizard		– 🗆 ×
Select features		DESTINATION SERVER ASC-DEMO-AD-01.ascertiademo.local
Before You Begin Installation Type Server Selection Server Foldes Features Confirmation Results	Select one or more features to install on the selected server: Fatures	Description Active Directory Certification Authority Management Tools Authority Management Tools Certificate Trephens, and Enterprise PKI snap-ins:
	< <u>Previous</u> <u>N</u> ext	> Install Cancel

10. At the "Confirm installation selections" dialog click Install.





11. Once the installation is complete, click Close.

Add Roles and Features Wizan	ł		-		×
Installation progr	ess	ASC-DEMO-A	DESTINA D-01.ascer	TION SERV	(ER cal
Before You Begin	View installation progress				
Installation Type	Feature installation				
Server Selection					
Server Roles	Installation succeeded on ASC-DEMO-AD-01.ascertiademo.loc	al.			
Features	Remote Server Administration Tools				
Confirmation	Role Administration Tools				
	You can close this wizard without interrupting running tasks.	/iew task pro	gress or a	open this	
	Export configuration settings	then look be	. comp.		
	< Previous Next >	Clo	se	Cance	1

12. Right-click Start, then click Run.

	Search	
	Run	
	Shut down or sign out	>
	Desktop	

13. In the Run dialog, type certtempl.msc, click OK.

💷 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
Open:	certtmpl.msc ~	
	This task will be created with administrative privileges.	
	OK Cancel <u>B</u> rowse	

14. A Certificate Templates installation dialog will display, click Yes to install the new certificate templates.

Certificate Templates	×
Windows has detected that new certificate templates should be installed. Do you want to install them?	
Yes No	

15. Click OK to the installation success message.



16. The Certificate Templates Console will be displayed.

Certificate Templates Console				– 🗆 X
File Action View Help				
🗢 🔿 📅 🖸 🖬 🖬				
Certificate Templates (ASC-DEM)	Template Display Name	Schema Version	^	Actions
	Administrator	1		Certificate Templates (ASC-DEMO-AD-01.ascertiademo.loc A
	Authenticated Session	1		More Actions
	Basic EFS	1		indications -
	R CA Exchange	2		
	CEP Encryption	1		
	R Code Signing	1		
	2 Computer	1		
	Cross Certification Authority	2		
	Directory Email Replication	2		
	Domain Controller	1		
	Domain Controller Authentication	2		

4.4.3 Creating Windows certificate templates for Web RA

The ADSS Web RA Server Windows Enrolment Service uses Windows certificate templates to enrol users, computers, service accounts, or domain controllers with Windows-native endpoints. Create the required Microsoft certificate templates using the Microsoft Certificate Templates management console. For example, users may require certificates with two key pairs (such as Digital Signature and Authentication) or one key pair (such as non-repudiation).

4.4.3.1 Create a new Windows Certificate Template

- 1. Log into an Active Directory domain controller as a member of the Domain Admins group.
- 2. Right-click Start, then click Run.



3. In the Run dialog, type certtmpl.msc, click OK.



4. The Certificate Templates Console will be displayed.

Certificate Templates Console				– 🗆 X
File Action View Help				
Certificate Templates (ASC-DEN)	Template Display Name	Schema Version	^	Actions
	Administrator	1		Certificate Templates (ASC-DEMO-AD-01.ascertiademo.loc A
	Real Authenticated Session	1		More Actions
	Resic EFS	1		
	🗟 CA Exchange	2		
	CEP Encryption	1		
	Real Code Signing	1		
	R Computer	1		
	Record Cross Certification Authority	2		
	Directory Email Replication	2		
	Domain Controller	1		
	Domain Controller Authentication	2		

5. From the list of available certificate templates, right-click the User template and select Duplicate Template.



- 6. The new duplicated template will appear. Set the following for the two templates we will create for this document:
 - a. ADSS TLS User
 - b. ADSS TLS Server

4.4.3.2 Create User Certificate Template

- 1. In the Compatibility tab make the following changes:
- a. Deselect the Show resulting changes check box.
- b. Set the Certification Authority drop down to Windows Server 2012 R2.
- c. Set the Certificate Recipient drop down to Windows 8.1 / Windows Server 2012 R2.



- 2. In the General tab, make the following changes:
 - a. Set the Template display name to ADSS TLS User.

oubject i	Vame	Ser	ver	Issuance R	equirements
Superse	ded Templa	ates	Exte	ensions	Security
ompatibility	General	Request	Handling	Cryptography	Key Attestation
Template di	solav name				
ADSS TLS	Userl	-			
Template na	me:				
ADSSTLSU	lser				
1.1.1.				Laurente de	
Validity perio	d:		<u>R</u> enewa	l period:	
Validity perio 1 yea	ıd: ars ∨	•	Renewa	l period: weeks ~	
<u>V</u> alidity perio 1 yea	ıd: ans ∨	r	<u>R</u> enewa 6	l period: weeks ~	
Validity perio	id: ars ∨	·	<u>R</u> enewa 6	l period: weeks v	
Validity perio	nd: ans ∽ entificate in	Active Di	Renewa 6	weeks v	wists in Active
Validity perio	id: ars v certificate in ot automatie tory	Active Di	Renewa 6 rectory oll if a dupl	I period: weeks ~	exists in Active
Validity perio	id: ars ~ certificate in ot automatio tory	Active Di	Renewa 6 rectory oll if a dupl	I period: weeks ~	exists in Active
Validity perio 1 yea ✓ Publish o Do no Direc	id: ars ~ certificate in ot automatio tory	Active Di	Renewa 6 rectory oll if a dupli	il period: weeks v	exists in Active
Validity perio 1 yea ✓ Publish c Do no Direc	id: ars ~ certificate in ot automation tory	Active Di cally reenn	Renewa 6 rectory oll if a dupl	Il period: weeks v	exists in Active
Validity perio 1 yea ✓ Publish c Do no Direc	id: ertificate in ot automatik tory	Active Di	Renewa 6	Il period: weeks V	exists in Active
<u>V</u> alidity perio 1 yez ✓ <u>P</u> ublish c □ <u>D</u> o no Direc	id: ars ~ ertificate in ot automatik tory	Active Di cally reenr	Renewa	Il period: weeks V	exists in Active
Validity perio 1 yea ✓ Publish o Do no Direc	id: ars ~ ertificate in ot automatik tory	Active Di cally reenr	Renewa	I period: weeks ~	exists in Active

3. In the Extensions tab, select Applications Policies and click Edit.

Properties of N	ew Temp	late			×
Subject Na	me	Ser	ver	Issuance F	Requirements
Compatibility (General	Request	Handling	Cryptography	Key Attestation
Supersede	d Templa	tes	Exte	insions	Security
To modify an e	extension,	select it,	and then c	lick Edit.	
Application Basic Con Certificate Issuance Key Usag	n Policies Istraints Template Policies e	Informati	ion		
Description of	Applicatio	n Policie:	8:		Edit
Encrypting Fil Secure Email Client Authent	e System tication				< >
	ОК		Cancel	Apply	Help

4. The Edit Application Policies Extensions dialog will display, highlight Encrypting File System, and click Remove. Repeat for Secure Email, and then click OK.

ropertie	s of New 1	femplate			×
Sub	ject Name	S	erver	Issuance Re	quirements
Compati Sur To more	Edit Appl An applica used.	ication Poli ation policy de	cies Extensio efines how a c	ertificate can be	× estation ity
Extens Ap Ba Ce Iss Ke	Application Client Au Encryptin Secure E	n policies: thentication ng File Syster imail	n		
Descrip Encryp Secure Client	□ Make t	Add	Edit	Remov	e ^
	C	ж	OK	Cance	Help

5. Select the Security tab, click Add.

ropenies of New Territ	olate		>
Subject Name	Server	Issuance	Requirements
Compatibility General	Request Hand	ling Cryptography	Key Attestation
Superseded Templa	tes	Extensions	Security
Group or user names:			
Authenticated Use	rs		
Administrator			
Section 2015 Admins (A	SCERTIADEM	O\Domain Admins)	
Somain Users (AS	CERTIADEMO	Domain Users)	
Enterprise Admins	(ASCERTIADE	MO\Enterprise Adm	ins)
		Add	Remove
		<u> </u>	
Permissions for Authent	icated Users	Allow	Deny
5.00 1.1			
Full Control			
Read			
Read Write			
Read Write Enroll			
Read Write Enroll Autoenroll			
Fuil Control Read Write Enroll Autoenroll			
Read Write Enroll Autoenroll			
Fuil Control Read Write Enroll Autoenroll			
Full Control Read Write Erroll Autoenroll	or advanced se	ttings, click	Adyanced
Full Control Read Write Enroll Autoenroll For special permissions Advanced.	or advanced so	ttings, click	Adyanced
Read Write Enroll Autoenroll For special permissions Advanced.	or advanced se	ttings, click	Adyanced
Fuil Control Read Write Enroll Autoenroll For special permissions Advanced.	or advanced se	ttings, click	Advanced
Read Write Erroll Autoenroll For special permissions Advanced.	or advanced se	ttings, click	Adyanced

6. The Select Users, Computers, Service Accounts, or Groups dialog will display, enter ADSS Web RA Users, this is the group created in step 4.2, click Check Names, click OK.

elect users, computers, service Accounts, or o	aroups	
Select this object type:		
Users, Groups, or Built-in security principals	Object Types.	
From this location:		
ascertiademo.local	Locations	
Enter the object names to select (<u>examples</u>):		
Enter the object names to select (<u>examples</u>): ADSS Web RA Users	Check Names	
Enter the object names to select (<u>examples</u>): ADSS Web RA Users	Check Names	,
Enter the object names to select (<u>examples</u>): <u>ADSS Web RA Users</u>]	Check Names	•

7. You will be returned to the properties of the new certificate template security tab, tick the check boxes for Enrol and Auto Enrol. This will allow users who are members of the ADSS Web RA Users group to enrol and auto enrol via Microsoft Group Policy, click OK.

Subject N	lame	Ser	ver	Issuance	Requirements
ompatibility	General	Request	Handling	Cryptography	Key Attesta
Supersec	ded Templa	ates	Exte	ensions	Security
<u>G</u> roup or use	r names:				
Authen	ticated Use	ers			
Adminis	trator	aam (ASC)		ADSC MA	PA Lloom)
RUSS I	Admins (A	SCERTIA		main Admins)	nA Users)
Somain Somain	Users (AS	CERTIAD	EMO\Don	nain Users)	
Senterpri	ise Admins	(ASCERT	IADEMO\	Enterprise Adm	ins)
				A <u>d</u> d	Remove
			[A <u>d</u> d	<u>R</u> emove
emissions	for ADSS V	Web RA U	sers	Add Allow	<u>R</u> emove Deny
ermissions f	for ADSS V	Web RA U	lsers	Add Allow	Remove Deny
ermissions Full Contro Read Write	for ADSS V	Web RA U	sers	Add Allow	Remove Deny
ermissions Full Contro Read Write Forcell	for ADSS \	Web RA U	lsers	Add	Remove Deny
ermissions f Full Contro Read Write Enroll Autoenroll	for ADSS V	Web RA U	sers	Add Allow	Remove Deny
ermissions f Full Contro Read Write Enroll Autoenroll	for ADSS V	Web RA U	lsers	Add Allow	Remove Deny
Permissions f Full Contro Read Write Enroll Autoenroll	for ADSS V	Web RA U	lsers	Add Allow	Remove Deny
Permissions f Full Contro Read Write Enroll Autoenroll	for ADSS V	Web RA U	lsers	Add	Remove
ermissions Full Contro Read Write Enroll Autoenroll	for ADSS V	Neb RA U	lsers	Add Allow	Remove Deny
ermissions : Full Contro Read Write Enroll Autoenroll	for ADSS V	Neb RA U	lsers	Add Allow	Remove Deny

8. You have successfully created the Windows certificate template for users. This process can be followed again to create other certificate templates with other key and extended key usages depending on use case requirements.

4.4.3.3 Create Device Certificate Template

1. From the list of available certificate templates, right-click the Computer template and select Duplicate Template.

V Template Display Name	Schema Version	Version	i.
Administrator	1	4.1	I
Authenticated Session	1	3.1	I
Residence EFS	1	3.1	I
🗷 CA Exchange	2	106.0	F
CEP Encryption	1	4.1	I
Code Signing	1	3.1	I
			_
Computer Computer	-	6.1	
Computer	Duplicate Templ	ate	1
Computer Const Certification Authority Directory Email Replication	Duplicate Templ	ate	C
Construction Authority Cross Certification Authority Cross Certification Authority Control Replication Controller	Duplicate Templ All Tasks	ate >	C
Computer Const Certification Authority Directory Email Replication Domain Controller Domain Controller	Duplicate Templ All Tasks Properties	ate >	C
Computer Computer Construct Certification Authority Directory Email Replication Domain Controller Domain Controller Authentication EFS Recovery Agent	Duplicate Templ All Tasks Properties Help	ate	C <
Computer Consolution Consolution Consolution Consolution Domain Controller Domain Controller Authentication Domain Controller Authentication EFS Recovery Agent Consolution Controllment Agent	Duplicate Templ All Tasks Properties Help	*-1	C

- 2. In the Compatibility tab, make the following changes:
 - a. Deselect the Show resulting changes check box.
 - b. Set the Certification Authority drop down to Windows Server 2012 R2.
 - c. Set the Certificate recipient drop down to Windows 8.1 / Windows Server 2012 R2.

roperties of	New Temp	plate			×
Subject N	lame	Ser	ver	Issuance R	equirements
Supersed	ded Templa	ates	Exte	ensions	Security
Compatibility	General	Request	Handling	Cryptography	Key Attestation
Compatibil Certificati	in Compati sulting char ty Settings o <u>n</u> Authority s Server 20	nges y 12 R2	igs.	 V 	ing system
Certificate Window	s <u>8.1 / Win</u> gs may not	prevent e	ver 2012 F	ating systems fro	n using this
[ОК		Cancel	Apply	Help

- 3. In the General tab name the following changes:
 - a. Set the Template display name to ADSS TLS Server.

Properties of	New Temp	olate			×
Subject N	lame	Ser	ver	Issuance R	equirements
Supersec	ded Templa	tes	Exte	insions	Security
Compatibility	General	Request	Handling	Cryptography	Key Attestation
Template dis	play name:				
ADSS TLS	Server				
Template na ADSSTLSS	me: erver				
Validity perio	d: ⊪s ∨]	Renewa 6	veeks v	
Publish c Do no Direct	ertificate in automatic ory	Active Di	rectory oll if a dupli	cate certificate e	exists in Active
[OK	(Cancel	Apply	Help



- 4. In the Extensions tab, select Applications Policies, ensure the following are listed in the description of Application Policies field:
 - a. Client Authentication.
 - b. Server Authentication.
- 5. Select the Security tab, click Add.

Subject Name Server Issuance Requirements Compatibility General Request Handling Cryptography Key Attestation Superseded Templates Extensions Security Group or user names: Auti-instrator Security Domain Adminis (ASCERTIADEMO\Domain Admins) Domain Computers (ASCERTIADEMO\Domain Computers) Enterprise Admins (ASCERTIADEMO\Domain Computers) Enterprise Admins (ASCERTIADEMO\Enterprise Admins) Valid Control	roperties of New Temp	plate			>
Compatibility General Request Handing Coptography Key Attestation Superseded Templates Extensions Security Group or user names: Authenticated Users Authenticated Users Domain Adminis (ASCERTIADEMO\Domain Admins) Domain Computers (ASCERTIADEMO\Domain Computers) Enterprise Admins (ASCERTIADEMO\Enterprise Admins) Add Remove Permissions for Authenticated Users Add Remove Permissions for Authenticated Users Add Remove Permissions for Authenticated Users For special permissions or advanced settings, click Advanced	Subject Name	Ser	ver	Issuance F	Requirements
Superseded Templates Extensions Security Group or user names: Image: Complete Security Image: Complete Security Image: Administrator Administrator Image: Complete Security Image: Complete Security Image: Complete Security Image: Complete Security Image: Complete Security Add Remove Image: Complete Security Add Remove Image: Complete Security Add Remove Permissions for Authenticated Users Allow Deny Full Control Image: Complete Security Image: Complete Security For special permissions or advanced settings, click Advanced	Compatibility General	Request	Handling	Cryptography	Key Attestation
Sroup or user names:	Superseded Templa	ites	Ext	ensions	Security
	Group or user names:				
Administrator Bomain Administrator Bomain Computers (ASCERTIADEMO\Domain Admins) Domain Computers (ASCERTIADEMO\Domain Computers) Demain Computers (ASCERTIADEMO\Enterprise Admins) Add Remove Add Remove Permissions for Authenticated Users Alow Deny Full Control Read Write Errol Accenrol For special permissions or advanced settings, click Advanced DK Cancel Remove	Authenticated Use	ns			
	Administrator				
	& Domain Admins (A	SCERTIA	DEMO\D	omain Admins)	
Erterprise Admins (ASCERTIADEMO\Enterprise Admins) Add Remove Add Remove Permissions for Authenticated Users Allow Deny Full Control Read Write Errol Actoenrol For special permissions or advanced settings, click Advanced OK cancel Berdy Etelo	Section 2018 Section 2018	s (ASCER	TIADEMO	\Domain Compu	ters)
Add Remove Pemissions for Authenticated Users Alow Deny Full Control Image: Control Image: Control Read Image: Control Image: Control Winte Image: Control Image: Control Erroll Image: Control Image: Control Autoennoll Image: Control Image: Control	Sector Admins	(ASCERT	IADEMO	Enterprise Admir	ns)
Add Remove Permissions for Authenticated Users Alow Deny Full Control					
Add Remove Pemissions for Authenticated Users Allow Deny Full Control					
Add Remove Pemissions for Authenticated Users Allow Deny Full Control Image: Control Image: Control Read Image: Control Image: Control Witte Image: Control Image: Control Erroll Image: Control Image: Control Autoenroll Image: Control Image: Control					
Pemissions for Authenticated Users Allow Deny Full Control Read Write Errol Actoenrol For special pemissions or advanced settings, click Advanced				Add	Remove
Full Control	Permissions for Authent	icated Us	ers	Allow	Deny
Read Winte W	Full Control				
Write Image: Control of the second settings, click For special permissions or advanced settings, click Advanced	Read				
Errol Autoenrol For special permissions or advanced settings, click Advanced	Write				
Autoenroll For special pemissions or advanced settings, click Advanced	Enrol				E I
For special permissions or advanced settings, click Advanced Advanced	Autoenroll				E I
For special permissions or advanced settings, click Advanced Advanced.					_
For special permissions or advanced settings, click Advanced Advanced.					
For special permissions or advanced settings, click Advanced Advanced	-				
OK Cannel Sonky Halo	For special permissions Advanced	or advanc	ed setting	IS, CIICK	Advanced
OK Cancel Broky Help	raranova.				
OK Cancel Apply Help					
OK Cancel Apply Help					
on cancel Apply Hep	OK		Cancel	Apply	Help

6. The Select Users, Computers, Service Accounts, or Groups dialog will display, enter ADSS Web RA Computers, this is the group created in step 4.2, click Check Names, click OK.

Select Users, Computers, Service Accounts, or Groups	×
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
ascertiademo local	Locations
Enter the object names to select (examples):	
ADSS Web RA Computers	Check Names
	_
Advanced OK	Cancel

 You will be returned to the properties of the new certificate template security tab, tick the check boxes for Enrol and Auto-Enrol. This will allow computers who are members of the ADSS Web RA Computers group to enrol and auto enrol via Microsoft Group Policy, click OK.

Subject I	Vame	Ser	ver	Issuance F	Requirements
mpatibility	General	Request	Handling	Cryptography	Key Attestatio
Superse	ded Templa	tes	Exte	ensions	Security
aroup or use	er names:				
State Authen	ticated Use	975			
Adminis	strator		ACCEDTU		Mak DA Care
ADSS R Domain	vveb RACC Admins (A	SCERTIA	DEMO\De	main Admins)	WED THA COM
Se Domain	Computer	s (ASCER	TIADEMO	Domain Compu	ters)
Senterpr	ise Admins	(ASCERT	IADEMO\	Enterprise Admir	15)
				Add	Remove
emissions	for ADSS V	Veb RA		Add	Remove
ermissions Computers	for ADSS V	Veb RA		Add Allow	Remove Deny
ermissions Computers Full Contr	for ADSS V	Veb RA		Add Allow	Remove Deny
ermissions Computers Full Contro Read	for ADSS V	Veb RA		Add Allow	Remove Deny
Permissions Computers Full Contre Read Write	for ADSS V	Veb RA		Add Allow	Remove Deny
Permissions Computers Full Contro Read Write Enroll	for ADSS V	Veb RA		Add Allow	Remove Deny
Permissions Computers Full Contre Read Write Enroll Autoenrol	for ADSS V ol	Veb RA		Add Allow	Remove Deny
Permissions Computers Full Contre Read Write Enroll Autoenrol	for ADSS V ol	Veb RA		Add Allow Q Q Q	Remove Deny
Permissions Computers Full Contre Read Write Enroll Autoenrol	for ADSS V ol	Veb RA	[Add Allow V V	Remove Deny
ermissions computers Full Contre Read Write Enroll Autoenrol	for ADSS V ol I	Veb RA	ed setting	Add Allow V S s, click	Remove Deny
Permissions Computers Full Contr Read Write Enroll Autoenrol or special p	for ADSS V ol I	Veb RA	ed setting	Add Allow 2 2 3, click	Remove Deny

8. You have successfully created the Windows certificate template for computers. This process can be followed again to create other certificate templates with other key and extended key usages depending on use case requirements.



5 Installing ADSS Web RA Server

ADSS Web RA Server should be installed by following the installation steps defined within the product installation guide.

- IIS + required features.
- .Net Windows Server Hosting 6.0.16.
- IIS URL Rewrite Module.

5.1 ADSS Web RA Installation

The Windows enrolment feature will only be available when the administrator installs the ADSS WEBRA Server with Windows enrolment from the installer. ADSS Web RA installer will include Windows enrolment module separately.

1. Extract the ADSS Web RA Server installation package to the following path

C:\ascertia\WebRA-v2.8-Win64-12Jun2023

- 2. Using Windows Explorer, navigate to C:\ascertia\WebRA-v2.8-Win64-12Jun2023\setup, double click install.bat
- 3. The Web RA installer will launch, at the Welcome dialog, click Next.

Welcom	ne to Web RA						
Web RA is to registe RAS/SAM documen creation a	s a central application r users to offer them I services as well as p its using these keys, and distribution proc	n for key managem different sets of cer bush users to Web R Web RA is ideal for t cess by implementin	ent and certificate rtification services A. All of them are the organizations og strong vetting f	generation in the Asc It can also register use powerful applications t that are looking to cen or the issuance of thes	ertia product suite. W ers to ADSS CSP servic to create certificates of trally control the cert e certificates.	eb RA is u es, ADSS ind sign th ficates	ised
Web RA c	onsists of the follow	ing modules:					
- Web RA - Web RA - Web RA - Web RA - Web RA	Admin Desktop Web API (RESTful Web Si Device Windows Enrolmen	ervices) t					
We strong	gly recommend you	to follow the install	ation instructions	provided in Web RA In	stallation Guide		
U.S. Pate	nt No. 7,360,079						
					Mark		

4. The Web RA Modules dialog will display, it is recommended to use Fully qualified domain name (FQDNs), enter the Web RA Servers FQDNs, click Next.

Fully Qualified Do	main Name:	WebRA-AS.ascertia.c	om.pk		
Fully qualified setting for exis	domain name will ting instances.	be set for the all instan	ices in system settings	. It will not u	update the system
Web RA Admi	n				
	Website Name:	admin	Port:	443	
Web RA Web					
	Website Name:	web	Port:	81	
Web RA API (R	ESTFul Web Service	s)			
	Website Name:	api	Port:	82	

5. The Windows Enrolment Modules dialog will display, tick the Windows Enrolment checkbox to install this feature, click Next.

ndows Enrolment Modules			
Windows Enrolment			
Windows Integrated Authentication			
Certificate Enrolment Policy Service (CEP)	windowsIntegratedCepService	Port:	96
Certificat Enrolement Service (CES)	windowsIntegratedCesService	Port:	97
UserName / Password Authentication			
Certificate Enrolment Policy Service (CEP)	windowsUserNamePasswordCepService	Port:	98
Certificat Enrolement Service (CES)	windowsUserNamePasswordCesService	Port:	99
Client Authentication			
Certificate Enrolment Policy Service (CEP)	windowsSsICepService	Port:	100
Certificat Enrolement Service (CES)	windowsSsICesService	Port:	101

The following fields describe items in the screenshot above.

Authentication Mechanism	Windows Enrolment Web Services	Description
Windows Integrated Authentication	Certificate Enrolment Policy Service (CEP)	Installer will deploy CEP service with Windows Integrated Authentication on this site and port.
	Certificate Enrolment Service (CES)	Installer will deploy CES service with Windows Integrated Authentication on this site and port.
UserName / Password Authentication	Certificate Enrolment Policy Service (CEP)	Installer will deploy CEP service with UserName/Password Authentication on this site and port.
	Certificate Enrolment Service (CES)	Installer will deploy CES service with UserName/Password Authentication on this site and port.
Client Authentication	Certificate Enrolment Policy Service (CEP)	Installer will deploy CEP service with Client Authentication on this site and port.
	Certificate Enrolment Service (CES)	Installer will deploy CES service with Client Authentication on this site and port.

Please refer to the ADSS Web RA installation guide for detailed steps for the installation process.



5.2 Import CA certificates into Microsoft Group Policy

Microsoft clients that are domain members who will rely on group policy configurations for certificate enrolment requires the Root CA and Issuing Certificates be added to a domain group policy and that certificate enrolment policy servers are added to enable clients to manually or automatically enrol.

ADSS Web RA Server leverages TLS Server certificates to secure access to enrolment and administration interfaces of the product, it is required that Web RA Server is a domain member and as a result will have the Root and Issuing CA certificates published to its certificates stores by group policy

For the following process, you will need to copy the Root and Issuing CA certificates to the domain controller.

- 1. Log in to the server hosting Active Directory as a member of the Domain Admins.
- 2. Click Start > Administrative Tools > Group Policy Management.
- 3. The Group Policy Management console is displayed. Expand Forest:domain_name > Domains > domain_name, right-click Default Domain Policy and select Edit.



- 4. The Group Policy Management Editor will display.
- 5. From the left panel, expand Computer Configuration > Policies > Windows Settings > Security Policies > Public Key Policies, right-click Trusted Root Certification Authorities, then click Import.



6. The Certificate Import Wizard will launch at the Welcome dialog, click Next.

~



🖉 Certificate Import Wizard	×
Welcome to the Certificate Im	port Wizard
This wizard helps you copy certificates, certifica lists from your disk to a certificate store.	te trust lists, and certificate revocation
A certificate, which is issued by a certification au and contains information used to protect data o connections. A certificate store is the system ar	uthority, is a confirmation of your identity r to establish secure network ea where certificates are kept.
Store Location	
O Current User	
Local Machine	
To continue, click Next.	
	Next Cancel

7. At the File to import dialog, browse the Root CA Certificate, click Next.



8. At the certificate store dialog, accept the defaults, click Next.

←	ᡒ Certificate Import Wizard	×
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	Automatically select the certificate store based on the type of certificate	
	Place all certificates in the following store	
	Certificate store:	
	Trusted Root Certification Authorities Browse	
	Next Canc	el

9. At the Completing the Certificate Import dialog, click Finish.

÷	ۍ 🧈	Certificate Import Wizard			×
		Completing the Certific	cate Import Wizard		
		The certificate will be imported after	you dick Finish.		
		You have specified the following sett	tings:		
		Certificate Store Selected by User	Trusted Root Certification Authoritie	s	
		Content	Certificate		
		File Name	C:\certs\RootCA.cer		
			Finis	sh Cance	I

10. Click OK to the success message.



11. You will be returned to the Group Policy Management Editor where the Root CA certificate will now display on the right panel.



12. Select Intermediate Certification Authorities from the left panel and repeat the same process for the Issuing CA certificate.



5.3 Configure IIS for Web RA Server

The Certificate Enrolment Policy Web Service and Certificate Enrolment Service are installed as an application in Microsoft Internet Information Services (IIS). Microsoft IIS requires a TLS certificate so that the Certificate Enrolment Policy Web Service can accept certificate enrolment requests over HTTPS.

The following section describes how to issue a TLS certificate for Microsoft IIS.

5.3.1 Creating a CSR for the Web server certificate

The Certificate Enrolment Policy Web Service and Certificate Enrolment Service are installed as applications with in an instance of Microsoft Internet Information Services (IIS). Microsoft IIS requires a TLS certificate so that the Certificate Enrolment Policy Web Service and Certificate Enrolment Service can process certificate enrolment requests over HTTPS.

The following procedure describes how to create a certificate-signing request (CSR) in Microsoft IIS for a certificate. A CSR contains information that the issuing CA will use to create the certificate.

Create a CSR for Microsoft IIS

- 1. Log into the server where Web RA will be installed as a domain administrator
- 2. Right-click Start > Run, type certlm.msc, click OK.



3. The Local Machine Certificate management console will display, right click Personal and select All Tasks > Advanced Operations > Create Custom Request.



4. The Certificate Enrolment wizard will launch, click Next.



5. The Select Certificate Enrolment Policy dialog will display, select "Proceed without enrolment policy" enrolment click Next.

	_		×
🙀 Certificate Enrollment			
Select Certificate Enrollment Policy			
Certificate enrollment policy enables enrollment for certificates based on predet Certificate enrollment policy may already be configured for you.	fined certificate	e template	s.
Configured by your administrator			
Active Directory Enrollment Policy			•
Configured by you		Add N	ew
Custom Request			
Proceed without enrollment policy			
	Next	Cano	el

6. The Custom request dialog will display, 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>PKCS #10</u>			
	O⊡mc			
Note: Key archival is option is specified in	not available for certificates based on a custom certificate request the certificate template.	. even wi	hen this	
	N	ext	Cano	:el

7. The Certificate information dialog will display, click the down arrow next to Details and click Properties.

		-		×
Certificate Enrollment				
Certificate Information				
Click Next to use the options alrea request, and then click Next.	dy selected for this template, or click Details to c	ustomize th	ne certifica	ite
Custom request	(j) STATUS: Available		Details	^
The following options descril Key usage: Application policies: Validity period (days):	be the uses and validity period that apply to this	type of cert	ificate: roperties	
	[Next	Can	cel

8. The Certificate Properties dialog will display, select the Subject Tab, in the Subject Name field, ensure that Full DN is selected for the Type drop down and enter the following in the Value field, click Add.



This is a sample value and should be updated to reflect the DNS name and certificate contents you require for your installation.

CN=asc-demo-wra-02.ascertiademo.local, OU=Services, O=Ascertia Lab, C=GB

9. In the Alternative Name field, select DNS from the type drop down and in the Value field, enter the following value, click Add.

asc-demo-wra-02.ascertiademo.local

This is a sample value and should be updated to reflect the DNS name and certificate
contents you require for your installation.

ertificat	te Propert	ies			:
General	Subject	Extensions	Private Key		
The sub can ent can be	oject of a ter inform used in a	certificate is ation about certificate.	the user or computer the types of subject na	to which the certificate is ime and alternative name	issued. You values that
Subject	of certifi	cate			
The use	er or com	puter that is	receiving the certificat	e	
Subject	name:		_		
Туре:				CN=asc-demo-w	ra-02.ascertia
Full D	N	~	, Add >	O=Ascertia Lab	
Value:			< Remove	C=GB	
Alterna	tive name	8		<	>
Type:				DNS	
DNS		· · · ·		asc-demo-wra-02	.ascertiadem
Value:			Add >		
			< Remove		
				<	>

10. Select the Private Key tab, click the drop down arrow for Key Options and set the key size to 2048, click OK.

Certificate Properties	×
General Subject Extensions Private Key	
Cryptographic Service Provider	~
Key options	^
Set the key length and export options for the private key.	
2048	
Make private key exportable	
Allow private key to be archived	
Strong private key protection	
Select Hash Algorithm	~
Select Signature Format	*
Key permissions	*
	_
OK Cancel A	pply

11. You will be returned to the Certificate Information dialog, click Next.

		-		\times
Certificate Enrollment				
Certificate Information				
Click Next to use the options alread request, and then click Next.	dy selected for this template, or click Details to c	ustomize th	ne certifica	te
Custom request	③ STATUS: Available		Details	^
The following options describ Key usage: Application policies: Validity period (days):	e the uses and validity period that apply to this	type of cert	ificate: roperties	
	[Next	Can	cel

12. The "Where do you want to save the offline request?" dialog will display, enter a disk location for where you want to save the request to and click Finish.

	-		×
🙀 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 requ to your hard disk or removable media. Enter the location and name of your cert click Finish.	uest later, save ificate request,	the reque and then	st
File Name: C:\certs\asc-demo-wra-02	В	rowse	
File format: ● Base 64 ○ Binary			
	Finish	Can	cel

13. The CSR is saved ready for processing.

5.3.2 Issuing the Web server certificate with ADSS Server

Copy the CSR to the server hosting ADSS Server and access the ADSS Server console as an operator with permissions to access the Issuing CA.

1. From the ADSS Server Console, navigate to CA Manager > Manual Certification and supply the following information, click Generate Certificate.



- Certificate Alias: asc-demo-wra-02-2023-2024.
- Import PKCS#10: browse to the CSR created from the Web RA Server.
- Select Use Local CA (ADSS Server inbuilt CA) radio button.
- Certificate Template: ACME TLS Server 1 Year (Set to your TLS Certificate Template Name).
- CA Certificate: ACME Issuing CA (Set to your Issuing CA Certificate).



ADSS Server - ADSS	Server (172.16.8.113)	L. 🕤
Search	CA Manager MANIJAL CERTIFICATION	01
Dashboard Management Reporting Key Manager Totst Manager CA Manager CA Manager Local CAs Letternal CAs	MANUAL CERTIFICATION Manual Certification Certificate Alias - sc-centro-rate 02-2023-2024 Impart NCUR10 - sc-centro-rate 02-2023-2024 Use Local CA (ADSS Server inbulk CA) Use Local CA (ADSS Server inbulk CA) Use Local CA (ADSS Server inbulk CA) Certificate Impalte - ACMENT SERver - 1 Year C A Certificate -	
Alerts Client Manager Global Settings Liternal Services User Manager User Manager Settem Lons		

- The ADSS Server CA will process and issue the certificate, the Certificate Generated Successfully dialog will display, select Download Certificate Chain and save the p7b file to disk.
- 3. Click Download Certificate and save the .cer file to disk.

MANUAL CERTIF	ICATION			×
✓ Certificate gene	rated successfully			
VIEW CERTIFICATE	DOWNLOAD CERTIFICATE CHAIN	DOWNLOAD CERTIFICATE	CLOSE	

4. Copy the .p7b and .cer files to the server hosting Web RA.

5.3.3 Installing the Web server certificates

- 1. Log into the server where Web RA will be installed as a domain administrator
- 2. Right-click Start > Run, type certIm.msc, click OK.

🖅 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
Open:	certIm.msd 🗸	5
	This task will be created with administrative privileges.	
	OK Cancel Browse]
	o H 🧲 📜 💷 🎙 🖂	

3. Expand Personal, right click Certificates select All Tasks > Import.



4. The Certificate Import Wizard will launch, at the welcome dialog, click Next.



5. The file to import dialog will display, browse to the certificate that was issued by ADSS Server, click Next.

	×
– 🛿 🐉 Certificate Import Wizard	
File to Import	
Specify the file you want to import.	
File name:	
C:\certs\asc-demo-wra-02 - 2023-2024 Certificate.cer Browse	
Note: More than one certificate can be stored in a single file in the following formats:	
Personal Information Exchange- PKCS #12 (.PFX, .P 12)	
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)	
Microsoft Serialized Certificate Store (.SST)	
Next Cano	el:

6. The Certificate store dialog will display, click Next.

Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
 Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: 	
Personal Browse	
Next Carro	PI
	Windows can automatically select a certificate store, or you can specify a location for the extificate. Automatically select the certificate store based on the type of certificate @ Ploca all certificate store: Certificate store: Personal Browse
7. The completing the certificate import wizard dialog will display, click Finish.



8. Click ok to the success message, the Web RA TLS Certificate has successfully imported.





5.3.4 Update IIS TLS Certificate bindings

When ADSS Web RA Server installs, by default it installs a self-signed certificate and creates a binding in IIS for each of the Web Sites used by ADSS Web RA Server. The following table provides a summary of the site name, the ports used, and what purpose of the sites.

Make sure that all the ports, which you are using for your bindings, have access from the deployment server.

Site	TLS Port Binding	Usage
Admin	443	ADSS Web RA Administrative Operator Portal
API	82	ADSS Web RA API's
Device	83	SCEP, EST, ACME and CMP device enrolment
SSLDevice	85	EST with TLS authentication Certificate
Web	81	ADSS WEB RA Web Operator Portal
windowsIntegratedCepService	86	CEP service using Windows authentication
windowsIntegratedCesService	97	CES service using Windows authentication
windowsSsICepService	90	CEP service using Client authentication
windowsSsICesService	91	CES service using Client authentication
windowsUserNamePasswordCepService	88	CEP service using username and password authentication
windowsUserNamePasswordCesService	89	CEP service using username and password authentication

5.3.4.1 Update the TLS binding using Internet Information Services (IIS) Manager

To add/update the IIS TLS site bindings using the Microsoft Internet Information Server Management console, complete the following procedure.

- 1. Click Start, select Windows Administrative Tools, select Internet Information Services (IIS) Manager
- 2. Expand the server hosting Web RA > sites, highlight admin in the left panel, select Bindings from the right hand action panel



💐 Internet Information Services (IIS)	Manager										- 0
← →	A-02 🕨 Sites	admin)									📴 🖂 🟠 🖡
File View Help											
Connections										1	Actions
Start Page Start Page ASC-DEMO-WRA-02 (ASCERT Application Pools -10 Sites	Filter:		• 🦻 Go 👻	Show All	Group by: Are	ea 👘	• 📰 •		~	-	Explore Edit Permissions Edit Site Bindings
> 😔 admin > 😔 api > 😔 Default Web Site > 🚱 device > 🚱 ssldevice	.NET Authorizat	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	.NET Users	Application Settings		 Basic Settings View Applications View Virtual Directories Manage Website

3. The site bindings dialog will display, select the https site binding and click Edit

te Bindir	igs				?	×
Туре	Host Name	Port	IP Address	Binding Informa	<u>A</u> dd	
https		443	*		<u>E</u> dit	
					<u>R</u> emove	
					Browse	
					<u>C</u> lose	

4. Select the new certificate from the SSL certificate dropdown, click ok

Edit Site Binding				?	×
<u>Iype:</u> https A <u>H</u> ost name:	address: II Unassigned		P <u>o</u> rt:]	
Require Server <u>N</u> ame I	ndication				
Disable HTTP/2					
Disable OCSP Stapling					
SSL certificate:					
asc-demo-wra-02.ascerti	ademo.local	~	Select	<u>V</u> iew	
		_			
		L	ОК	Cancel	

5. You will be returned to the Site Bindings dialog, click Close

Site Bindir	ngs				?	×
Type https	Host Name	Port 443	IP Address *	Binding Informa	<u>A</u> dd <u>E</u> dit <u>R</u> emove <u>B</u> rowse	
					<u>C</u> lose	

6. Repeat this process for api, device, ssldevice, web and all other IIS sites that is installed for ADSS Web RA Server.



5.3.4.2 Update the TLS binding using PowerShell

To add/update the IIS TLS site bindings using Windows PowerShell, complete the following procedure.

- 1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
- Open an elevated PowerShell window. Select Start then right-click Windows PowerShell > More > Run as administrator.
- 3. Run the following command to install WebAdministration module.

PS C:\Users\administrator.ASCERTIADEMO>Import-Module WebAdministration

4. Run the following command, this will locate any certificate with asc-demo-wra-02 in the SDN.

\$cert = Get-ChildItem Cert:\LocalMachine\my | Where Subject -Like '*asc-demo-wra-02*'

5. Run the following command, to update all IIS TLS bindings.

```
Foreach ($Binding in (Get-ChildItem IIS:\SslBindings\)) {
    # Remove current binding
    $Binding | Remove-Item
    # Add the binding again using the new certificate
    # (Bindings using hostname instead of IP address use a slightly different path)
    if ($Binding.Host) {
        $cert | New-Item -path "IIS:\SslBindings\!$($binding.Port)!$($binding.Host)"
    }
    Elseif ($Binding.IPAddress) {
        $cert | New-Item -path "IIS:\SslBindings\$($binding.IPAddress)!$($binding.Port)"
    }
}
```

Example output

IP Address	Port Host Name	Store	Sites
0.0.0.0	443	my	admin
0.0.0.0	81	my	web
0.0.0.0	82	my	api
0.0.0.0	84	my	device
0.0.0.0	85	my	ssldevice
0.0.0.0	86	my	windowsIntegratedCepService
0.0.0.0	87	my	windowsIntegratedCesService
0.0.0.0	88	my	windowsUserNamePasswordCepServic
			e
0.0.0.0	89	my	windowsUserNamePasswordCesServic
			e
0.0.0.0	90	my	windowsSslCepService
0.0.0.0	91	my	windowsSslCesService



5.3.5 Configure Windows Authentication

Windows integrated authentication is also known as Kerberos authentication. This enables users to log in with their Windows credentials using Kerberos or NTLM. The client sends credentials in the Authorization header. Windows authentication is best suited for an intranet environment. It uses the security features of Windows clients and servers. The web browser supplies the current Windows user information on the client computer through a cryptographic exchange involving hashing with the web server. If you want to authenticate, you should deploy ADSS Web RA CEP Service on Windows Integrated authentication mechanism.

ADSS Web RA Server requires the windowsIntegratedCepService and windowsIntegratedCesService web sites to have Windows Authentication enabled and anonymous authentication disabled.

- 1. Expand Start > Administrative Tools > Internet Information Services (IIS) Manager.
- 2. The Internet Information Services (IIS) Manager management console will be displayed.
- 3. Expand the Server > Sites and select windowsIntegratedCepService.

internet Information Services (IIS) Manager												- 🗆 ×		
🗧 🕘 🖌 ASC-DEMO-WRA-02 🔸 Sites 🖡 windo	wsintegratedCa	pService +										a = 0 0 ·		
File View Help														
Connections											Actions			
Q.• ka 🖄 😣	S MI	ndowsint	egrated	epservice	e Home							Displore		
Start Page	Filter	Filter . W Go . Co Show All Group her, Anna										Edit Permissions		
ASC-DEMO-VIRA-02 (ASCERTIADEMO\edministrator) Application Pools Stes Ses Admin	ASPINET	٢	A			Ø	2	8	E	ß	1	Edit Site Sindings Beac Settings		
> 😌 api > 😌 Default Web Site	.NET Authorizet	.NET Compilation	NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	.NET Users	Application Settings	Connection Strings	Machine Key	View Applications View Virtual Directories		
	Pages and Controls	Providers	Session State	SMTP E-mail								Manage Website		
WindowsSalCepService WindowsSalCesService Ge windowsUsenNamePasswordCepService WindowsUsenNamePasswordCesService	ASP	Authentic	Authorizet	CGI	Compression	Default	Directory	Error Pages	Handler	нтр	ISAPI Filters	Browse Website Browse 1:86 (https) Advanced Settings		
	-	04.5		124	-	0	1					Configure		

4. Double-click on Authentication in the centre panel. Select Windows Authentication in the centre panel and select Enable from the actions panel on the right.

🐚 Internet Information Services (IIS) Manager							- 0	×	
← → ● ASC-DEMO-WRA-02 → Sites → windo		🛄 🔤 👌	9 10 -						
File View Help									
Connections	Authentication					Actions			
Start Page	Group by: No Grouping .						1 Help		
- 2 Application Pools	Name Anonymous Authentication	Status Enabled	Response Type						
> - e admin > - e api	ASP.NET Impersonation Forms Authentication	Disabled	HTTP 302 Login/Redirect						
Orault web site Orault site Orault site	Windows Authentication	Disabled	HTTP 401 Challenge						

5. Select Anonymous Authentication in the centre panel and select Disable from the actions panel on the right.

internet Information Services (IIS) Manager				- 0 ×		
Sites + winds	owsIntegratedCepService >			100 H G 8		
File View Help						
Connections	Authentication		Actions			
Q 2 8.	Authentication		Disable			
Start Page	Group by: No Grouping •			Edt.		
Application Pools	Name	Status	Response Type	10 Help		
🛩 🗑 Sites	Anonymous Authentication	Enabled				
> 😔 admin	ASP.NET Impersonation	Disabled				
5 🚱 api	Forms Authentication	Disabled	HTTP 302 Login/Redirect			
> 😌 Default Web Site	Windows Authentication	Enabled	HTTP 401 Challenge			
> 😜 device						
> 😌 ssidevice						
> O ssidevice						

6. Windows Authentication will now appear as enabled and Anonymous Authentication will now appear as disabled for the windowsIntegratedCepService. Repeat the same process for the windowsIntegratedCesService.

💐 Internet Information Services (IIS) Manager					
ASC-DEMO-WRA-02 > Sites > windo	wsIntegratedCepService				
File View Help					
Connections					
🔍 • 🔒 🖄 😥	Authentication				
📲 Start Page	Group by: No Grouping +				
 ASC-DEMO-WRA-02 (ASCERTIADEMO\administrator) Application Pools 	Name	Status	Response Type		
✓ - Sites	Anonymous Authentication	Disabled			
> 😔 admin	ASP.NET Impersonation	Disabled			
> 😔 api	Forms Authentication	Disabled	HTTP 302 Login/Redirect		
> 😌 Default Web Site	Windows Authentication	Enabled	HTTP 401 Challenge		
> 😔 device					
> 🕘 ssldevice					

💐 Internet Information Services (IIS) Manager			
ASC-DEMO-WRA-02 > Sites > windo	wsIntegratedCesService >		
File View Help			
Connections Conne	Group by: No Grouping		
ASC-DEMO-WRA-02 (ASCERTIADEMO\administrator) Application Pools Sites	Name Anonymous Authentication	Status Disabled	Response Type
 → admin → api > → Default Web Site > → device 	ASP.NET Impersonation Forms Authentication Windows Authentication	Disabled Disabled Enabled	HTTP 302 Login/Redirect HTTP 401 Challenge
 Sidevice Web WindowsIntegratedCepService WindowsIntegratedCesService 			

5.3.6 Configure IIS Application Pools

ADSS Web RA Server IIS application pools need to be configured to run using the Windows service account created in step 4.1.

- 1. Expand Start > Administrative Tools > Internet Information Services (IIS) Manager.
- 2. The Internet Information Services (IIS) Manager management console will appear.
- 3. Expand the Server and select Application Pools from the left panel.
- 4. Select windowsIntegratedCepService from the centre panel. Click Advanced Settings from Actions in the right panel.



5. The Advanced Settings dialog will display, select the ApplicationPoolIdentity field and click the Edit button.

Adva	inced Settings		?	×
~	(General)			^
	.NET CLR Version	v4.0		
	Enable 32-Bit Applications	False		
	Managed Pipeline Mode	Integrated		
	Name	windowsIntegratedCepServi	ce	
	Queue Length	1000		
	Start Mode	OnDemand		
~	CPU			
	Limit (percent)	0		
	Limit Action	NoAction		
	Limit Interval (minutes)	5		
	Processor Affinity Enabled	False		
	Processor Affinity Mask	4294967295		
	Processor Affinity Mask (64-bit o	4294967295		
~	Process Model			
>	Generate Process Model Event L			
	Identity	ApplicationPoolIdentity		
	Idle Time-out (minutes)	0		
	Idle Time-out Action	Terminate		~
lde (id as Ser	entity entityType, username, password] built-in account, i.e. Application I vice, Local System, Local Service,	Configures the application p Pool Identity (recommended) or as a specific user identity.	ool to ru I, Netwo	n rk
		ОК	Cancel	

6. The Application Pool Identity dialog will display. Select the Custom account radio button, and then click Set.

Application Pool Identity			?	×
O <u>B</u> uilt-in account:				
ApplicationPoolIdentity		\sim		
Output: <u>Custom account:</u>				
			<u>S</u> et	
		_		
	OK		Cancel	

7. The Set Credentials dialog will display. Enter the username as domain\username, then enter and confirm the password, click OK.

Set Credentials		? ×	:
User name:	hra svc		1
Password:			
•••••	••••		
Confirm password	d:		
•••••	••••		
	ОК	Cancel	

8. You will be returned to the Application Pool Identity dialog, click OK.

○ <u>B</u> uilt-in account:		
ApplicationPoolIdentity \sim		
<u>C</u> ustom account:		
ascertiademo\webra_svc	<u>S</u> et	
		_
OK OK	Cancel	

9. You will be returned to the Advanced Settings dialog, click OK.





10. You will be returned to the Internet Information Services (IIS) Manager management console, note the Identity for the windowsIntegratedCepService has now been updated to the new identity.

ASC DEMOLINE	A.02 Application Paols							0 0 0.
							-	
ne view nep							100	tions
	Application Pools						1	and a second sec
	EP						122	Add Application Pool
Wij Start Page	This page lets you view and manage the list	of applicati	on pools on the	server. Application	n pools are associated with w	orker		Set Application Pool Defaults
ASC-DEMO-WRA-U2 (ASCERI	processes, contain one or more applications	, and provis	de isolation amo	ing different applic	ations.			Application Pool Tasks
Sites	Filten • 🐨 Go + 🖓	Show All	Group by: No	Grouping			Þ	Start
	Name	Status	.NET CLR.V	Managed Pipel	Identity	Application		Stop
	12 NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0		THE POINT
	NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0	-	Edit Application Pool
	2 admin	Started	v4.0	Integrated	ApplicationPoolIdentity	1	123	Basic Settings
	💭 api	Started	v4.0	Integrated	ApplicationPoolIdentity	1		Recycling_
	DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	1	Advanced Settings Rename	Advanced Settings
	() device	Started	v4.0	Integrated	ApplicationPoolIdentity	1		Reneme
	() ssidevice	Started	v4.0	Integrated	ApplicationPoolIdentity	1	×	Remove
	(2) web	Started	v4.0	Integrated	ApplicationPoolIdentity	1		View Applications
	@windowsIntegratedCepService	Started	v4.0	Integrated	ascertiademo\webra_svc	0		
	@windowsIntegratedCesService	Started	v4.0	Integrated	ApplicationPoolIdentity	1		Help
	windowsSsICepService	Started	v4.0	Integrated	ApplicationPoolIdentity	3		
	() windowsSsICesService	Started	v4.0	Integrated	ApplicationPoolIdentity	1		
	@windowsUserNamePasswordCepService	Started	v4.0	Integrated	ApplicationPoolIdentity	3		
	@windowsUserNamePasswordCesService	Started	v4.0	Integrated	ApplicationPoolIdentity	1		

- 11. Repeat this process for the windowsIntegratedCesService.
- 12. Once complete, right-click Start > Run, type cmd, click OK.

🖅 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
Open:	cmd It is task will be created with administrative privileges.]
	OK Cancel Browse]
.	D 🛱 🧀 🧰 🌖 🏟 🍒	

The Windows command prompt will display, type the following command, press enter:





6 ADSS Web RA Server Configuration

Before configuring Web RA for Windows Enrolment, you will need the following:

- Root CA Certificate from ADSS Server.
- Certificate Templates, ADSS Certificate Profiles, Client ID and Secret from ADSS Server.
- Microsoft Certificate Templates to map to ADSS Server Certificate Templates.
- Microsoft Active Directory:
 - Domain controller host
 - Domain controller port
 - Domain User Id and password
- Simple Mail Transfer Protocol (SMTP):
 - SMTP Server Address
 - o SMTP Server Port

6.1 ADSS Web RA Admin Portal

Following the installation of ADSS Web RA Server, the Windows enrolment feature must be enabled for any role who will need access to this feature. Use the following process to enable Windows Enrolment for the desired role.

6.1.1 Access Control

The default roles that are installed with ADSS Web RA Server are not granted access to the Windows Enrolment feature; these must be enabled to configure the product.

1. Access Web RA administration portal as an administrator with permissions to assign the Windows Enrolment settings to roles. Navigate to Access Control > Roles > i > Edit.

WebRA				Live 🔵 Ard	ive English v	•••
	۹			Search by Home		
Dashboard						
🛱 System	¥	Name	Туре	Description		+
Configurations	¥	admin (4)	Administrator	Test		1
Agreements	Ť	Admin Basecamp (2)	Administrator	Test		
Ø External Services	~	Auditors (0)	Administrator			1
Service Plans		View Only (1)	Administrator	This role is for documentation person dont do any thing in it (Rizwan)		1
Lisers	Ť	ADSS team (2)	Administrator	Dont do any thing with this role (rizwan)		
题 Requests	~	Admin RAO (2)	Administrator			
Certificates Access Control	~	Super Admin (1)	Administrator		Edit	
Operators		Approval manager role (Q)	Administrator	Approval manager role	Delete	
Roles Personal Information	~	Administrators (5)	Administrator	Administrators		1
TSP Accounts					Showing:	2 / 32

2. Select Windows Enrolment and then click Save.

WebRA			Live 🔵 🗾 🖊	rchive PUBLISH OWNRES	English 🔹 <u> </u>
Search	Q				
⑦ Dashboard		ADMINISTRATORS			
🖶 System	×	Allowed Modules Read	i Ad	dd/Edit	Delete
Configurations	~				-
Agreements	×	ACME			- II
🕅 Vetting Forms		L EST			
Ø External Services	٣	Vindows Enrolment		✓	
(1) Service Plans		✓ Application Integration ✓		<i>✓</i>	
Enterprises	×				
Q Users				*	<u> </u>
Requests	~	✓ System Security ✓		\checkmark	·
B) Dual Controls	v	✓ Data Security ✓		\checkmark	- II.
@ Certificates		✓ HMAC Verification ✓		×	- II.
Access Control	^	✓ License ✓		\checkmark	- II
Operators		✓ Branding ✓		✓	
Roles					
Personal Information	×	SAVE CLOSE			
TSP Accounts					

6.1.2 Enable Windows Enrolment

By default, when ADSS Web RA Server installs the Windows enrolment feature, it is disabled and must be enabled and configured by an administrator.

- 1. Access Web RA administration as an administrator with permissions to enable the Windows enrolment feature, navigate Configurations > Windows Enrolment.
- 2. Tick the check box to enable Windows Enrolment, click the upload button for the CA Certificate field to import the Root CA Certificate. Ensure all the URLs reflect the fully qualified DNS name for the Web RA server installation, then click Save.

WebRA		Live 🍋 Archive English 🖡 🧾	·
	۹		
Dashboard System Configurations	v	WINDOWS ENROLMENT The Windows Fundment is a protect for automating 559 certificate issuance for public key inhabucture PRI directs. These include web serves, emporit devices and use identifies, and anywhee PR certificate are used, as will as the associated certificates from a tructed Certificate Automity (CN, Windows Enrolment use certificate enclosert, denoty	1
General Settings Default Settings Device Errolment Windows Errolment Application Integration Policy System Security License Branding	٠	ceri Kales based on aufhentiation scheme in deployment URLS. Cal Certificate Cal Cerificate Cal Certificate C	
Archiving Agreements Q Vetting Forms Variant Services (1) Service Plans	v	Username / Password UUILs for Windows certificate eventment using Username / Password authentication scheme. Contrificate Intennet Mark (201) https://localhost.82/JI.Service.scv/CEP Annual A	
窟 Enterprises	•		

Windows Integrated Authentication mechanism: (As displayed in the image above).

Field	Description
Certificate Enrolment Policy (CEP)	Enter URL to manage certificate enrolment policies, e.g. [Server URL]/Service.svc/CEP. For instance: https://dc2016.ascertia.local:449/Service.scv/CEP
Certificate Enrolment Service (CES)	Enter URL to manage certificate enrolment policies, e.g. [Server URL]/Service.svc/CES. For instance: https://dc2016.ascertia.local:447/Service.svc/CES



Username / Password Authentication mechanism: (As displayed in the image above).

Field	Description
Certificate Enrolment Policy (CEP)	Enter URL to manage certificate enrolment policies, e.g. [Server URL]/Service.svc/CEP. For instance: https://localhost:82/1/Service.scv/CEP
Certificate Enrolment Service (CES)	Enter URL to manage certificate enrolment policies, e.g.[ServerURL]/Service.svc/CES.Forinstance:https://localhost:83/Service.svc/CES

Client Authentication mechanism: (Scroll down to see the next image).

Field	Description
Certificate Enrolment Policy (CEP)	Enter URL to manage certificate enrolment policies, e.g.[ServerURL]/Service.svc/CEP.instance:https://localhost:84/1/Service.scv/CEP
Certificate Enrolment Service (CES)	Enter URL to manage certificate enrolment policies, e.g. [Server URL]/Service.svc/CES. For instance: https://localhost:85/1/Service.svc/CES



6.1.3 Create Active Directory Connector

In order to authenticate users and issue certificates using Kerberos to domain members, ADSS Web RA Server requires an Active Directory connector. This section provides the configuration steps to create this connector.

- 1. Expand External Services > Connectors > click +
- 2. The basic information page will display, Enter a name and select Active Directory from the provider drop-down, tick the Active check box, click >.

WebRA			Live ෩ Archive English 🕶 🕕 🗸
Search	۹		
② Dashboard		EDIT: ASCERTIA DEMO ACTIVE DIRECTORY	
📮 System	¥	0	2
Configurations	~	Basic Information	Details
S Agreements	*	Name+	
D. Vetting Forms		Ascertia Demo Active Directory	
Ø External Services	^	Provider Active Directory	
Connectors			
Authentication Profiles		✓ Active	
Certification Profiles			
P Service Plans			
Enterprises	÷	SAVE CLOSE	>
C Licent			



3. The Details page will display, enter the Domain Controller Host, Domain Controller Port, Web RA Service Account User ID and Password. Click Create.

WebRA		Live 🌑 Archive English 🖡	۰
Search	Q	Connectors	
② Dashboard		ADD	
💭 System	*	0	
Configurations	~	Basic Information Details	
S Agreements	*	- Domolo Pontrollar Mort a	
R. Vetting Forms		172.168.9	
₫ External Services	^	Domain Controller Port +	
Connectors		389	
Authentication Profiles		User ID	
Certification Profiles		webra_vvc@ascertiademo.local	
(1) Service Plans		User Password	
窗 Enterprises	~		
요 Users		1//23	
85 Requests	~		
E Certificates			
Access Control	*		
Personal Information	*		
TSP Accounts		CREATE TEST CONNECTION CLOSE	<
B. Logs			

6.1.4 Create ADSS Server Connector

ADSS Web RA Server issues certificates from ADSS Server based Certification Authorities. This section provides steps to create the connector between Web RA Server and the ADSS Server Certification Service.

- 1. Expand External Services > Connectors > click +.
- 2. The Basic information page will display, enter a name and select ADSS Server as the provider, tick the Active check box, click >.

WebRA			Live 🌒 Archive English 🕶 🌔 🕶
Search	Q		
② Dashboard		EDIT: ADSS SERVER - 172.16.8.113	
🖶 System	¥	0	(2)
Configurations	*	Basic Information	Details
S Agreements	*	Name+	
 Vetting Forms 		ADSS Server - 172.16.8.113	
P External Services	^	Provider	
Connectors		ADSS Server 🔻	
Authentication Profiles Certification Profiles		✓ Active	
Service Plans			
盒 Enterprises	÷		
🚊 Users			
EB Requests	¥	SAVE CLOSE	>
E Certificates			

- 3. The Details page will display, provide the following information, click create
- Server Address

Specify the address and port number of ADSS Server.

Client ID

Specify the Client ID configured in the Client Manager module of the ADSS Server for this connector

Client Secret

Specify the client secret generated in the ADSS Server against this Client ID.



WebRA			Live ෩ Archive English 🔻 🕕 🗸
Search	٩		
Dashboard			
System	÷	<u></u>	0
Configurations	~	Basic Information	Details
Agreements	*	Server Address •	Timeout (seconds) *
[]t. Vetting Forms		http://adss.pki.acme.com/8777/	90
Ø External Services	^	Client ID -	Client Secret
Connectors			
Certification Profiles		TLS Mutual Auth Key (PFX / PKCS#12)	TLS Mutual Auth Key Password
(1) Service Plans			
1 Enterprises	~	Request Signing Key (PFX / PKCS#12)	Request Signing Key Password
오 Users			
El Requests	*		
E Certificates			
Access Control	*		
Personal Information	*		
TSP Accounts		CREATE TEST CONNECTION CLOSE	< <u>(</u>)
B Logs			

6.1.5 Create an Authentication Profile

Microsoft requires that ADSS Web RA Server authenticates to Active Directory in order to access the Microsoft Certificate Templates and information about users and computers that will be submitted to the CA as part of a certificate request. This section provides the steps to create an authentication profile that is used by Web RA Server to authenticate to Active Directory using a Windows Service Account.

- 1. Expand External Services > Authentication Profiles > click +
- 2. The Details page will display, enter a name, tick the Active check box, and click >.

WebRA			Live 🔵 Archive English 🕶 🕕 🗸
Search	٩		
⑦ Dashboard		EDIT: ASCERTIA DEMO	
System	~	0	
Configurations	~	Basic Information	Details
S Agreements	*	Name	
R Vetting Forms		Ascertia Demo	
P External Services	^	13/255	
Connectors		Description	
Authentication Profiles			
Certification Profiles			
Service Plans			
盒 Enterprises	*	✓ Active	
⊈ Users			
Elio Requests	*	SAVE CLOSE	>
E Certificates			~

- 3. The Details page will display, set the following information, and click Create.
- Method Active Directory.
- Active Directory Connectors Select the Active Directory Connector created in step 6.1.3.
- Fully Qualified Domain Name Enter the Fully Qualified Domain Name.
- Allowed Groups Domain Users.

WebRA			Live 🍋 Archive English 🕶 🍈 🕶
Search	Q,	Authentication Profiles ADD	
Deshboard System	÷		
Configurations	*	Basic Information	Details
Agreements	*	Method •	
 Vetting Forms External Services 	•	Active Directory Connectors •	
Connectors Authentication Profiles		Ascertia Demo Active Directory	
Certification Profiles		ascertiademo.local ×	
Service Plans		Fully qualified domain name is a specific domain that will be used for authentication	
Losers	Ť	Allowed Groups domain users ×	
IEB Requests	*	Allowed groups include active directory groups used for authentication	
E Certificates		Use this authentication as a second factor	
Access Control Personal Information	÷		
TSP Accounts		CREATE CLOSE	<



6.1.6 Create a Certification Profile

Active Directory and ADSS Server maintain certificate templates that are used to generate keys and certificates for people, devices and applications. ADSS Web RA Server requires a certification profile for each type of certificate. It will be issuing using the Windows Enrolment feature, the following section provides steps on how to create a certification profile that maps a Windows Certificate Template to an ADSS Server Certification profile and template to ensure that certificates are issued with the correct attributes, extensions, and validity periods.

The following is an example of creating a profile to support TLS User Authentication.

- 1. Expand External Services > Certification Profiles > click +.
- 2. The Basic information page will display, enter Windows TLS User 1 Year the following information, tick the Active check box, click >.

WebRA					Live ෩ Archive English 🕶 🕕 🕶
Search	۹				
② Dashboard		EDIT: ADSS TLS SERVER – 1 YEAR			
System	~	2	3		(5)
Configurations	~	Basic Information Profile Settin	gs Deta	ils Authentications	Advance Settings
Agreements	~	Name*			
R Vetting Forms		ADSS TLS User - 1 Year			
Ditternal Services	^		22/255		
Connectors		Description			
Authentication Profiles					
Certification Profiles					
Service Plans					
盒 Enterprises	*	✓ Active			
🖳 Users					
EB Requests	*	SAVE CLOSE			>
E Certificates					

3. The Profile Settings page will display, set the following, click >:

ADSS Service	Certification Service
ADSS Certification Server	Set the ADSS Server connector
	configured in step 6.1.4
ADSS Certification service Profile	Set the ADSS Server Certification
	Service Profile Name
	e.g. Windows TLS User - 1 Year
Certificate Purpose	Is auto set by ADSS Server
Certificate Enrolment	Windows Enrolment
Active Directory Profile	Set to the Active Directory Connector
	created in step 6.1.3
Certificate Template	Set to the Windows Certificate Template
	created in step 4.4.3
Windows Device Certificate	Check this tick box if the certificate
	template if for a server, desktop or
	device.



WebRA						🔵 Archive English 🗸 🌔
learch	ď					
② Dashboard						
System	v	0	2	3	4	5
Configurations	*	Basic Information	Profile Settings	Details	Authentications	Advance Settings
SP Agreements	~	ADD Fundas -				
R. Vetting Forms		Certification Service		•		
Ø External Services	•	ADSS Certification Server +				
Connectors		ADSS Server - 172.16.8.113		@ •		
Authentication Profiles		ADSS Certification Service Profile *				
Certification Profiles		Windows TLS User - 1 Year				
Service Plans		Certificate Purpose				
Enterprises	~	TLS Client Authentication				
오 Users		Certificate Enrolment •				
E) Requests	÷	Windows Enrolment		•		
E Certificates		Active Directory Profile •				
		Ascertia Demo		@ •		
Access control	Ť	Certificate Template •				
② Personal Information	ř	ADSSTLSUser		0 •		
15P Accounts		Windows Device Certificate				
🛱 Logs						
		close				00

- 4. The Details page will display, these values are only editable if the ADSS Server Certification Profile Allows, if editable set the following, click >:
 - Key Algorithm

Key Algorithm that will be used to generate the key pair in the smart card/token. This configuration is coming from the ADSS Server so it cannot be changed

Key Length

Key Length that will be used to generate the key pair in the smart card/token. This configuration is coming from the ADSS Server so it cannot be changed.

- Validity Period Type
 - Validity period type can be configured as a Fixed to restrict the enterprise user to change the certificate validity or it can be set as Custom if enterprise RAO allow an enterprise user to set validity period while creating a certificate request.
 - These Fixed and Custom values can only be used on ADSS Web RA admin, if the selected ADSS Certification profile has set over ridable option in certification profile. It will be shown as fixed validity period type otherwise.
- Validity Period

Set the certificate validity period.

WebRA					Live	🔵 Archive English 🛛 🚺 🗸
Search	۹					
② Dashboard						
🖶 System	÷				4	5
Configurations	*	Basic Information	Profile Settings	Details	Authentications	Advance Settings
S Agreements	~	Key Algorithm *				
R Vetting Forms		RSA		•		
Ø External Services	^	Key Length •				
Connectors		2048		•		
Authentication Profiles		Validity Period Type				
Certification Profiles		Custom		•		
Service Plans		Validity Period •				
	~	12	1	Months 🔻		
요 Users						
85) Requests	~	CLOSE				< >
E Certificates						

5. The Authentications page will display. Accept the details, click >



WebRA						🍋 Archive English 🛛 🌔 🗸
Search	٩					
② Dashboard						
🖶 System	*	0	0	0	0	5
Configurations	*	Basic Information	Profile Settings	Details	Authentications	Advance Settings
S Agreements	~					
B. Vetting Forms		Enable authentication for new re	quest			
Ø External Services	^	Enable authentication for revoca	tion request			
Connectors						
Authentication Profiles						
Certification Profiles						
() Service Plans						
Enterprises	*					
율 Users						
IE5 Requests	*	CLOSE				< >
E Certificates						

6. The Advance Settings page will display, accept the default, click Create.

WebRA						🔵 Archive English 🗸 🕕
Search	Q					
② Dashboard						
₽ System	÷	0	0	0	0	6
Configurations	*	Basic Information	Profile Settings	Details	Authentications	Advance Settings
S Agreements	~	Agreement				
Vetting Forms		Subscriber Agreement		•		
Ø External Services	^	Select a schoriber annament if an Admir	wants a user to annee to cartain terms helf	•		
Connectors		certificate request	- name a spectra spectra de las recipios des			
Authentication Profiles Certification Profiles		Vetting Vetting Option				
영 Service Plans		None		Ŧ		
旨 Enterprises	*	Certificates will generate automatically. N	o vetting and no admin verification will be n	equired.		
🖳 Users						
E5 Requests	~	CREATE CLOSE				<
E Certificates						

7. Repeat this process for any other certificate templates that are required.

6.1.7 Configure a Service Plan

ADSS Web RA Server uses service plans to govern which services and features are available to a given enterprise. This section provides example steps on how to create a basic service plan that will enable the issuance of certificates to Windows domain members, for a detailed reference on service plan settings, please refer to the <u>ADSS Web RA Server</u> product documentation.

- 1. Expand Service Plans click +
- 2. The Basic Information page will display, enter a name, tick the Active check box, click >.

WebRA					Live 📄 Archive English 🕶	۰ 🕕
Search	۹					
② Dashboard						
5ystem	*	0	2	3		
Configurations	*	Basic Information	Profile Settings	Notification	Advance Settings	
S Agreements	~	Name+				
I. Vetting Forms		Ascertia Demo				
Ø External Services	*	a second				
Service Plans		Description				
Ⅲ Enterprises	*					
요 Users						
E5 Requests	*	 Active 				
E Certificates						
Access Control	*					
Personal Information	*					
TSP Accounts						
🗒 Logs		_				
		CLOSE				>
						_

3. The Profile Settings page will display.

Under the Services section, there two types of profiles:

Profile to create certificates for Windows user enrolment	Configure this profile for user-based certificates
Profile to create certificates for Windows device enrolment	Configure this profile for device-based certificates

4. Click the Profile to create certificates for Windows user enrolment drop down and select the profile created in step 6.1.6, repeat for Profile to create certificates for Windows device enrolment, click >.

earch	Q			
Dashboard				
System	÷	0 0		
Configurations	~	Basic Information Profile Settings	Notification	Advance Settings
Agreements	~	• Configure has will be control and shared on second		
E. Vetting Forms		Deplication and states and states of server		
P External Services	~	Select Certification Profile		•
Service Plans		Certificate keys are already created and stored by the user		
Enterprises	~	Profiles for creating keys on smartcards/tokens		
Users		Select Certification Profile		•
6 Requests	~	Certificate keys will be created and stored in Sexart card/token		
Certificates		Services		
Access Control		Default certificate profile for Virtual ID (remote authorization) Select	Default certificate profile for csp (remote desktop si Select Certification Profile	gning)
Personal information	÷	Profile will be used to create default certificate for Virtual ID	Selected profile is used to create default certificate for CSP	(remote desktop signing)
TSP Accounts		Profile to create certificates for Windows User Enrolment	Profile to create certificates for Windows Device En	olment
Logs		ADSS TLS User – 1 Year ×	ADSS TLS Server – 1 Year ×	•
		Profile used to generate Windows Enrolment (WE) certificate for Users	Profile used to generate Windows Enrolment (WE) certification	te for Devices.
		SigningHub Connector Select		
		SigningHub instance where the users are to be enroled and certificates are to be provisioned		

5. The Notifications page will display, enable the notification providers you require for user notifications to be sent, click >.

SMS Gatew	ay			SMS gateway connector to receive OTP via SMS.			
Email Gate	way	/		SMTP connector to receive email notifications.			
WebRA					Live ෩ Archive English 🛛 🕕 🗸		
Search	٩	Service Plans ADD					
Dashboard System	÷		0	- 0			
Configurations	~	Basic Information	Profile Settings	Notification	Advance Settings		
S Agreements	~	SMS Gateway					
[]t. Vetting Forms		Select	•				
dP External Services	×	Email Gateway Arcertia Demo SMTP Server	A				
Service Plans							
Enterprises	×						
♀ Users							
IES Requests	*	CLOSE			< >		
javascript;							

- 6. The Advance Settings page will display, Web RA Server provides primary and secondary authentication profiles. "Primary Authentication Profiles" are used to control how a user authenticates to Web RA to access the user portal. "Secondary Authentication Profiles" are used when an enterprise wishes to use an additional separate authentication mechanism to authorise an action, such as certificate rekey or revocation.
- 7. Set the Primary Authentication Profile to the authentication profile you created in step 6.1.6.
- 8. Set the Default Authentication Profile to the authentication profile you created in step 6.1.6, click Create.



WebRA					Live 🔵 Archive English 🕶 🌔
Search	ď				
② Dashboard					
System	÷				0
Configurations	~	Basic Information	Profile Settings	Notification	Advance Settings
Agreements	~				
R. Vetting Forms		Primary Authentication Profiles *			
External Services	÷	Ascertia Demo ×	•		
Service Plans		Default Primary Authentication Profile •			
Enterprises	~	Ascertia Demo	Ø T		
Users		Secondary Authentication Profiles			
B Requests	~	Select	•		
9 Certificates		Default Secondary Authentication Profile			
Access Control		Select	*		
Personal Information	•	Enterprise Registration			
TSP Accounts		Enable Vetting, Administrators can appr	rove enterprise requests after vetting		
Logs					
		CREATE CLOSE			
		Close			·

6.1.8 Create an Enterprise.

ADSS Web RA Server is a multi-tenanted product that enables different organisations or different departments to be created, each have their own administrative users that can create and manage user invites, and user and device certificates. This section provides steps to create an enterprise that will be used to connect to Active Directory to issue and manager digital certificates for domain members.

- 1. Access Web RA administration as an administrator with permissions to create enterprises, navigate to Enterprises > Requests click on +
- 2. The Organisation Information page will display, provide the following information, click >
 - Legal Name

Legal Name is the official name of the organisation under which the organization is registered with the government and it is the name that is used when submitting tax to the government e.g. Ascertia Limited.

Assumed Name

Assumed Name could be the short hand name of the organisation that is commonly used e.g. Ascertia

- Organisation Phone Number
 Official phone number of the organisation that is registered in the government documents.
- Address

Complete address of the organisation as it was provided to government at the time of company registration.

The following fields should be filled as part of Address:

- Country
- o State
- o City
- o Postal Code
- o Address 1
- o Address 2
- Service Plan

Select a service plan for this enterprise that you created for Windows enrolment.



• Create Default Role

Tick this checkbox to create a default role while creating a new enterprise.

WebRA		Live Archive English •	0.
Search	٩	Enterprise	
② Dashboard		ADD	
🖶 System	*		
Configurations	*	Organisation Information Account Owner License	
S Agreements	*	Land Name a	
[]t. Vetting Forms		Ascertia Demo	
dP External Services	*	Legal name is the official registered name of the business entity Assumed name is a name that a company uses to do business instead of its legal name	
(9) Service Plans		Organisation Phone Number •	
盒 Enterprises	^	The full and valid international number must be entered, e.g. 0044234334334 or +44234334334	
Requests		Country •	
Registered		United kingdom	
🚊 Users		City • Postal Code • Sw13XI	
EB) Requests	ř		
E Certificates		Address 1 • 123 Sample Street Address 2	
Access Control	*		
Personal Information	*		
ISP Accounts		Service Plan +	
₿ Logs		Ascertia Demo 👁 🔻 🗸 Create Default Role	
		CLOSE	>

- 3. The Account Owner page will display, enter the following information, click >
 - Name

Name of the enterprise owner. It could be any representative of the organisation but ideally, it should be the CEO. The enterprise owner should initiate any change requested in the enterprise.

Email

Email address of the enterprise owner. An email will be sent to this email address to create an account on the ADSS Web RA Web.

Mobile Number

Mobile number of the enterprise owner to send the OTP code if enabled in the profile.

• Job Title

The role of the enterprise owner in his organisation.

WebRA			Live Mrchive	English 🔻	• •
Search	Q				
② Dashboard					
E System	*	00	3		
Configurations	*	Organisation Information Account Owner	License		
S Agreements	*	< Name+			
R. Vetting Forms		Mark Thompson			
Ø External Services	*	Email •			
😰 Service Plans		maricthompson@ascertiademo.local			
Enterprises	^	Mobile Number •			
Requests		The full and valid international number must be entered, e.g. 0044234334334 or +44234334334			
Registered		Job Title			
🔒 Users		CEO			
IEb Requests	~	2055			
E Certificates		CLOSE		<	>
Access Control	~				

- 4. The License page will display, enter the certificate quota and expiry for the Enterprise, click create.
 - Name

Name of the certification profile for which an enterprise wants to use ADSS Web RA to create certificates.

• Unlimited

A check box can be used to allow a user to create unlimited certificates. This field will appear only if a user is allowed to create unlimited certificates.

Certificates Quota



This defines the total number of certificates an enterprise is allowed to generate from ADSS Web RA against each certification profile.

• Expiry

This defines the duration for which these certificates are valid.

WebRA				Live 🌖 Archive English 🗸
Search	٩	Enterprise		
Dashboard				
System	÷			0
Configurations	*	Organisation Information	Account Owner	License
S Agreements	*			
Vetting Forms		Name	Certificates Quota	Expiry
Disternal Services	*	ADSS TLS User – 1 Year	50	1 Years
Service Plans		ADSS TLS Server – 1 Year	500	1 Years
Enterprises	^			
Requests				
Registered				
🖳 Users				
E5 Requests	~			
Certificates		CREATE CLOSE		Remaining Application Certificates: 100

5. A confirmation dialog will display, click Yes to create the enterprise.

CONFIRM	Л	×
Are you sure enterprise?	you want to approve the enterprise request and c	reate an
YES	NO	

6.1.9 Edit the Enterprise Default Role

Windows Users are automatically registered in the default enterprise role during the autoenrolment of certificates, this section provides step to control which certificates will be displayed to a user I the Web RA Server User Portal

- Access Web RA administration as an administrator with permissions to edit roles, expand Enterprises > Registered > select the Enterprise Name > Roles > click the it to edit the Default Role > Certificate Management.
- 2. Check the Windows Enrolment check box and select the certificate profiles from the Profile to create certificates for Windows User Enrolment or Profile to create certificates for Windows Device Enrolment.

Note: If the role is for end users who you only wish to see their certificates, do not enable the Profile to create certificates for Windows Device Enrolment check box.

If you are creating a role to manage device certificates, only then only check the Profile to create certificates for Windows Device Enrolment

3. Click Save when complete.



WebRA			Live 🔵 Archive	English 🔻	•••
iearch	ά	Roma DEFAULT ROLE 🖌			
Dashboard	v	MODULE CRETERATE MANAGEMENT LOGIN AUTHENTICATIONS			
En Approval Requests 2: Users 3: Roles	*	Key Stores Centicutes with COR Windows Enrolment			
P Integrations	÷	✓ Windows Enrolment			
Windows Errolment Advance Settings	٠	Peelle to crust certificate for Windows Davie Evolument ADDS TLS User - 1 Year X	t		•
3 Licenses		Certificate Details Certificate Details Nore Other of Market Details Other Detai			
		Certificate Sharing Shers Certificate			
		900 COM			
					Activ

Users can access Web RA to manage certificates issued to them by the Windows Enrolment process. The Profile to create certificates for Windows User Enrolment drop-down enables Web RA Administrators to define which user profiles a user can access via the Web RA user portal. The Profile to create certificates for Windows User Enrolment drop-down enables Web RA Administrators to define which device profiles a user can access via the Web RA user portal.

Certificate Sharing (and filter)

This setting allows you to configure profiles to share certificates. Once configured this profile will enable you to apply a filter based on elements of a certificates subject distinguished name, these include, All, common name, first name, country, etc. on basis of which certificate requests will appear on the ADSS Web RA web portal, and the user will only be able to manage according to the filters applied here. Once the required filters have been defined, click Save.

Certificate Sharing is a setting that is used to enable administrators to have a view on multiple certificates, for example, Certificate Sharing enables you to create a role that can see all device TLS Certificates with OU=TLS Devices in the SDN.

Certificate Sharing			
✓ Share Certificate			
Certification profiles to share certificates + ADSS TLS Server - 1 Year × ADSS TLS User - 1 Year ×	Window enrolment certificate filter by Shared certification profiles of window errolment will be filtered on this field	1	
Certificate profiles with Document Signing purpose will not be included in this list		Country	
		Subject Serial Number	-
SAVE CLOSE		Unique Identifier	11
		Business Category	\vdash

6.1.10 Create Web RA Service Account

ADSS Web RA Server uses a windows service account to access Active Directory Certificate Templates and domain member information. This account must be activated in Web RA, the following provides steps to create and enable the service account.

- 1. Access the ADSS Web RA Server as the Enterprise RAO where you have enabled Windows Enrolment.
- 2. Expand Enterprises. Click Registered from the left menu and click on the Enterprise Name from the centre panel.

WebRA							Live 🔵 Archive	English 🕶 🌔 🕶
Search	Q,							
Oashboard					Search			
5 System	*	Creat	ted On Enterprise Name	Account	Country	Service Plan	Status	
Configurations OP Agreements	ž	2023 03:17:	-06-22 Ascertia Demo	Mark Thompson mark.thompson@ascertiademo.local	United Kingdom	Ascertia Demo	Active	1
R. Vetting Forms								



3. Click Users > User Invitations from the left menu. The User Invitations page will display. Click on the + to create a new invitation.

WebRA							English 🔻	•••
Search	۹				Court Instrum Court			
Main Menu		USER INVITATION			Search by Name, Email	Search by Hame, Email		
② Dashboard		Created On	Name	Email	Role	Status		+
Profile	*							
85 Approval Requests	*							
🚊 Users	^							
Registered Users								
User Invitations								
A Roles								

- 4. The Invite User page will display. Enter the following information to invite the Windows Web RA Service account that was created in step 4.1. Click Invite User.
 - Name: webra_svc
 - Email: <u>webra_svc@ascertiademo.local</u>
 - Role: Default Role

INVITE USER BULK INVITE		
nformation		
Name * webra svc		
Email webra_svc@ascertiademo.local		
	28/255	
Role • Default Role	@ *	
ertification Details		
	No Certificate Details available	
	These details will be available when added in Role	

5. The user invitation will be generated and sent. The service account will need to be activated using the email sent to the service accounts email address.

6.1.11 Subject Distinguished Name Controls

Digital Certificates contain information about people, devices, and applications, to identify a certificate holder their identity information is first verified and then it is sent to a certification authority in a certificate request, the identity information is contained in the subject field in a digital certificate.

ADSS Web RA Server CEP and CES services work together to authenticate users and computers, and then collects information about them to place into the subject field in certificates. This section will cover Web RA Server's default behaviours for constructing the subject field in the certificates issued during Enrolment.

ADSS Web RA Server will enforce the following Subject Distinguished Name elements:

- Country Code
- Organisation

These will appear in a digital certificate in the following format:

C=GB

O=Ascertia Demo

Both, Country code and organisation name are defined by the Enterprise Legal Name and the Enterprise Country.

Ascertia Limited 2023



Users and Devices can exist in Active Directory in different locations, administrators group users and devices by department, by user or device type, or other groupings, this information also needs to be added to a user or devices digital Certificate. When the Web RA CES service receives a certificate request, it will query Active Directory and search for the user or the device that is enrolling, it will retrieve the following information:

- Common Name
- Organisation Unit

The Web RA CES service will also query active directory to populate the Subject Alternative Name in a digital certificate, these are created as follows:

User Subject Alternative Name

- Email Address
- User Principal Name

Device Subject Alternative Name

• DNS name



6.1.12 Activate ADSS Web RA Server enterprise service account

1. Access the Web RA invitation email that has been sent to the inbox for the webra_svc service account and click on the Join Now button.

Ascertia Limited	WebRA
Hi webra_svc,	
You are invited to join the enterprise Ascertia Demo on A joining Ascertia Demo you will become a member of Asc Click the button below to join	scertia Limited. By ertia Demo team.
JOIN NOW	
Regards,	
Ascertia Limited Team	
This invitation is sent by Mike Hathaway - Ascertia Demo Ent RAO(mike.hathaway@ascertiademo.local)	
If you have any questions or need any help, feel free to contact administrati 02@ascertiademo.local	ors at asc-demo-wra-

2. The Account Activation page will display, provide a mobile account number for the account and check the I agree to the Terms of Service and Privacy Policy check box on the activation form, and click Activate.

	ACTIVATE ACCOUNT	
Em ve	all +	
Mo +4	Alle Number - 4789456123	
O M	oble number is used for OTP authentication and device registration. Include country code in your mobile number, e.g. 004423433434 or +4423433434	
√ I agree to the Terms of Service and Privacy Policy		
	criser	

3. You will be returned to the login page, enter the Web RA service account email address, click Next.

Email • webra_svc@ascertiademo.local	
Remember Me	28/255
NEXT	

4. The Windows authentication dialog will display, enter the Windows user id and password for the Web RA service account, and click Sign in.

Email • webra_svc@ascertia	idemoliocal
	😵 asc-demo-wra-502.ascertiademo.local.81/bd/40.luthRequest?userEmail=webra_sv — 🛛 🛛 🗙
Remember Me	asc-demo-wra-02.ascertiademo.local.81/ad/ADAuthRequest?userEmail=webra_svc@asc
ND7	Sign in https://asc-demo-war-Q2.ascetiademo.local@1
	Usemanne webra_suc
	Pessed
	Sign in Cancel

5. The ADSS Web RA Server User Dashboard will display.

WebRA			ender• 🗘 🕕•
	٩	OVERVIEW	
C Dashboard			
🖽 Certificate Center	*	EXPIRING CERTIFICATES	CERTIFICATE REQUESTS
E Windows Enrolment	٠	10	
Personal information	*	* *	
窗 Enterprise	٠	7	
		5	You don't have any certificate requests
		4	
		2	
		8	
		Recently Expired 30 Days 60 Days 90 Days	

6. You have successfully created the Web RA Service Account.

7. Select the down arrow next to the user's silhouette and select Logout.





7 Active Directory Configuration

7.1 Create an enrolment service in Active Directory

Microsoft requires an enrolment service for each CA that will issue certificates via ADSS Web RA Server to users and devices.

For the following process, you will need a copy of the Root CA certificate that will be copied to the domain controller.

- 1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
- 2. Right-click Start > Run, type cmd and click OK.

	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.		
Open:	cmd 🗸		
	This task will be created with administrative privileges.		
	OK Cancel Browse		

3. At the command prompt run the following command where the CA certificate is located at c:\certs

certutil -f -dspublish C:\certs\RootCA.cer RootCA

Expected output



4. Right-click Start > Run, type adsiedit.msc and click OK.



5. ADSI Edit will launch. Right-click ADSI Edit and click Connect To.



6. A Connection Settings dialog will display. Click the Select a well known Naming Context dropdown and select Configuration. Click OK.

Connection Settings ×				
Name: Configuration				
Path: LDAP://ASC-DEMO-AD-01.ascertiademo.local/Configuration				
Connection Point				
Select or type a Distinguished Name or Naming Context:				
Select a well known Naming Context:				
Configuration \checkmark				
Computer				
Default (Domain or server that you logged in to) Use SSL-based Encryption				
Advanced OK Cancel				

 ADSI Edit will connect to the Configuration instance of Active Directory. From the left panel, expand Configuration > CN=Configuration, DC=ascertiademo, DC=local > CN=Services > CN=Public Key Services > CN=Certificate Authorities, the Root CA will display in the centre panel.



8. In ADSI Edit right-click CN=Enrollment Services > New > Object.



		T1 11 11 11	
CN=Configuration,DC=ascertiademo,DC=local			
CN=DisplaySpecifiers			
CN=Extended-Rights			
CN=ForestUpdates			
CN=LostAndFoundConfig			
CN=NTDS Quotas			
CN=Partitions			
CN=Physical Locations			
✓ [™] CN=Services			
CN=AuthN Policy Configuration			
CN=Claims Configuration			
CN=Group Key Distribution Service			
CN=Microsoft SPP			
CN=MsmqServices			
CN=NetServices			
✓ CN=Public Key Services			
CN=AIA			
CN=CDP			
CN=Certificate Templa	ates		
CN=Certification Auth	orities		
CN=Enrollment Servic	Move		
CN=KRA	New Connection from User		
	New Connection from Here		
<u>ΓΝ-RRΔS</u>	New	> Object	
reates a new item in this container.		, , , , , , , , , , , , , , , , , , , ,	

9. The Create Object dialog will prompt you to Select a class list, highlight pkIEnrolmentService, click Next.

Create Object	×
Select a dass:	
msIWMI-WMIGPO	
< Back Next > Cancel	Help

10. The Create Object dialog will prompt you to provide a Common-Name, enter ADSS Web RA Server, click Next.

Create Object	×	<
A 44-16-14-1	_	
Attribute:	61	
Syntax:	Unicode String	
Description:	Common-Name	
<u>V</u> alue:	ADSS Web RA Server	
	< Back Next > Cancel Help	

11. The Create Object dialog will prompt you to complete the process, and then click More Attributes.

Create Object	×
To complete the creation of this object, click Finish	
To set more attributes, click More Attributes.	More Attributes
< Back Finish	Cancel Help

12. The Attributes dialog will display. Set the Select a property to view drop down to Certificate Templates and enter ADSSTLSUser in the Edit Attribute field. Click Add.

cn=ADSS We	eb RA Server		×
Attributes			
Path:			
Class: pK	(IEnrollmentService		
Select wh	nich properties to view:	Optional \checkmark	
Select a	property to view:	certificate Templates \checkmark	
Attribute	Values		
Syntax:	DirectoryString		
Edit Attrib	ute: ADSSTLSUser		
Value(s):	<not set=""></not>		
		Add Remove	
		OK Cance	I

- 13. Repeat this for ADSSTLSServer.
- 14. Note: These names must match the Template Name field from the Microsoft Certificate Templates created in step 4.4.3.
- 15. Click OK when complete, you will be returned to the Create Object dialog, click Finish.

7.2 Configure Certificate Enrolment

Microsoft clients support two types of certificate enrolment:

- Manual certificate enrolment.
- Certificate auto-enrolment.

7.2.1 Manual Certificate Enrolment



When using this method, users can manually enrol certificates for clients by performing using Microsoft Management Console (MMC) for personal certificates.

7.2.1.1 Define an Enrolment Policy for Domain Computer

- 1. Access ADSS Web RA Server as the Web RA Service Account.
- 2. Navigate to Windows Enrolment > Settings copy the Windows Integrated Certificate Enrolment Policy URL.

WebRA		English 🔻 🔒	д (D •
Search				
🕑 Dashboard	SETTINGS			
🖭 Certificate Center	The Windows Enrolment is a protocol for automating x.509 certificate issuance for public key infrastructure (PKI) clients. These include web servers, endpoint devices a anywhere PKI certificates are used, as well as the associated certificates from a trusted Certificate Authority (CA). Windows Enrolment uses certificate enrolment policy	and user identities, / to enrol identity	and	
E Windows Enrolment	certificates based on authentication scheme in deployment URLs.			
Certificate Requests Issued Certificates Revocation Requests Settings	Windows Integrated URLs for Windows certificate enrolment using Windows Integrated authentication scheme. Certificate Enrolment Pelloy (CEP) https://WebRa-WCC-Client.WebRAlocal&9/Service.svc/CEP?Ignite		C [®]	
Personal Information	 Service address use for windows certificate enrolment service. Copy URL to configure policy service e.g. Service URLJ/Service.svc/CEP 	configure certificate s	.rvice	
Enterprise	Username / Password URLs for Windows certificate enrolment using Username / Password authentication scheme. Certificate terrolment Pelicy (CEP) https://WebRa-WCC-Client.WebRA.locat89/Service.svc/CEP/Ignite Service address use for windows certificate enrolment service. Copy URL to configure policy service e.g. Service address use for windows certificate enrolment service. Copy URL to configure policy service e.g. Service address use for windows certificate enrolment service. Copy URL to configure policy service e.g. Service address use for windows certificate enrolment service. Copy URL to configure policy service e.g. Service address use for windows certificate enrolment service. Copy URL to e.g. [Service URL/Service.svc/CES	configure certificate s	c.	
Terms of Service ট Privacy Policy ট Help ট About	Client Authentication URLs for Windows certificate enrolment using client authentication scheme. Cartificate Enrolment Pelicy (CEP) https://WebRa-WCC-Client.WebRAlocat90/Service.swc/CEP/Ignite Cartificate Enrolment Service (CES) https://WebRa-WCC-Client.WebRAlocat91/Service.swc/CEP/Ignite Cartificate Enrolment Service (CES) https://WebRa-WCC-Client.WebRAlocat91/Service.swc/CEP/Ignite Cartificate Enrolment Service (CES) https://WebRa-WCC-Client.WebRAlocat91/Service.swc/CEP/Ignite Cartificate Enrolment Service (CES) https://WebRa-WCC-Client.WebRAlocat91/Service.swc/CES/Activ	rate Windows Settings to activate Wi	e ndgws.	

3. Access the domain controller as an administrator and access the Group Policy Management console by executing gpmc.msc in Run.

🖅 Run	×	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	gpmc.msc ~	
	OK Cancel <u>B</u> rowse	

Group Policy Management Console will be open.

4. Navigate to Linked Group Policy Objects.



📓 Group Policy Management									-			×
📓 File Action View Window Help											-	б×
(+ 2) 📰 🖸 🔢 📰												
File Action View Window Help Image: State S	WebRA.I Status A V	ocal Linked Group Policy Link Örder 1	Objects GPO	Group Policy Inhe fault Domain Policy	ritance Dele Enforced No	egation Link Enabled Yes	GPO Status Enabled	WMI Filter None	Modified 7/3/2023	Domair WebRA	- 1 A	5 ×

- 5. Make it sure that the link is enabled against the group policy object in which you are going to configure ADSS Web RA enrolment policy.
- 6. If link is not enabled then right click on the Policy object and click on Link Enabled.



7. Right click on the Policy in which you are going to configure the ADSS Web RA Enrolment Policy and click Edit. Group Policy Editor will open.

📓 File Action View Window Help	_ 8 ×
Group Policy Management Default Domain Policy ✓ A Forest WebRAlocal ✓ Momains ✓ Domains ✓ Default Domain Policy ✓ WebRAlocal ✓ Momain Policy ✓ WebRAlocal ✓ Momain Policy ✓ WebRAlocal ✓ Momain Controllers ✓ Edit ✓ Enforced ✓ Enforced ✓ Save Report_ No Yes WebRAlocal	×
Image: Stress View Image: Stress View Image: Stress New Window from Here Image: Stress New Window from Here Image: Delete Delete Remain nly apply to the following groups, users, and computers: Refresh Image: Stress	
Help	
Add Remove Properties WMI Filtering This GPO is linked to the following WMI filter: <	

 In the Group Policy Management Editor expand Computer Configuration > Policies > Windows Settings > Security Policies > Public Key Policies, double click on Certificate Services Client – Certificate Enrolment Policy.



9. The "Certificate Services Client – Certificate Enrolment Policy" will display, click Add.

Certificate Servi	ces Client - Certifica	ate Enroll	ment Polic	?	×
Enrollment Polic	y	Console	Root\Default	Domain	Policy [
Configuration	Model:	Enabled	ł		~
Certificate e	nrollment policy list —				
Default	Name		Automatic En	ollment	
	Active Directory Enr	ollmen	Enabled		
Add	Remove		Pro	operties	
- Additional ce	rtificate enrollment n	nlicy confi	uration		
Disable	user configured enrol	lment polic	v servers		
					- 1
	0	к	Cancel	App	bly

10. The Certificate Enrolment Policy Server properties dialog will display. Paste the ADSS Web RA Server Windows Integrated Certificate Enrolment Policy URL into the Enter enrolment policy server URI field and click Validate Server, the connection test will take place, click Add.

Certificate Enrollment Policy Server	×
Certificate enrollment policy server configuration	
Enter URI for a certificate enrollment policy server and select the correct authentication type, then click 'Validate Server'.	
Use default Active Directory domain controller URI Configure Friendly Name	
Enter enrollment policy server URI:	
https://asc-demo-wra-02.ascertiademo.local:86/Service.svc/CEP?Ascertia%20Demo	
Authentication type:	_
Windows integrated Validate Server	
Priority:	
Certificate enrollment policy properties Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.	
The URI "https://asc-demo-wra-02.ascertiademo.local:86/Service.svc/CEP?Ascertia %20Demo" was validated successfully.	•
Errolment ID (032/7011-100A-4955-885D-AC945184658C) Errolment Findly Name	,
Add Cancel	

11. You will be returned to the Certificate Enrolment Policy Server properties, tick the check box to mark this policy server as the default, OK.

Certificate Serv	ices Client - Certificat	e Enroll	ment Polic	?	×
Enrollment Polic	У				
Configuration	Model:	Enable	d		~
Certificate e	nrollment policy list				
Default	Name		Automatic Enr	ollment	
	ADSS WEBRA Enrollm	ent	Enabled		
Add	Remove		Pro	perties	
Additional co	ertificate enrollment poli	cy confi	guration		
Disable	user configured enrollm	ent poli	cy servers		
	ОК		Cancel	Арр	bly



7.2.1.2 Define Enrolment Policy for Domain User

- 1. Access ADSS Web RA Server as the Web RA Service Account.
- 2. Navigate to Windows Enrolment > Settings copy the Windows Integrated Certificate Enrolment Policy URL.

WebRA		English 🔹 🗘 🍈 🗸
Search	۹	Windows Enrolment
🕑 Dashboard		SETTINGS
🖭 Certificate Center	~	The Windows Enrolment is a protocol for automating x.509 certificate issuance for public key infrastructure (PKI) clients. These include web servers, endpoint devices and user identities, and
🖽 Windows Enrolment	^	anywhere FXL certificates are used, as we as the associated certificates from a trusted Lertificate Authority (CA). Windows enrolment uses certificate enrolment policy to enrol identity certificates based on authentication scheme in deployment URLs.
Certificate Requests Issued Certificates Revocation Requests Settings		Windows Integrated URLs for Windows certificate enrolment using Windows Integrated authentication scheme. - Certificate Enrolment Folicy (CEP) https://WebRa-WCC-Client.WebRAlocal86/Service.svc/CEP1gnite © Service address use for windows certificate enrolment service. Copy URL to configure policy service e.g. © Service address use for windows certificate enrolment service. Copy URL to configure policy service e.g.
Personal Information Enterprise	*	Service URL/Service.ser/CEP e.g. [Service URL/Service.ser/CES USername / Password URLs for Windows certificate enrolment using Username / Password authentication scheme.
		Certificate Enrolment Policy (CEP) Certificate Enrolment Service (CES) https://WebRa-WCC-Client.WebRaLocal88/Service.svc/CEP?Ignite thtps://WebRa-WCC-Client.WebRaLocal89/Service.svc/CES
		Service address use for windows certificate enrolment service. Copy URL to configure policy service e.g Service address use for windows certificate enrolment service. copy URL to configure certificate service e.g. Service URL/Service.se/CEP
Terms of Service 🖸 Privacy Policy 🖸 Help 🖸 About		Client Authentication URLs for Windows certificate enrolment using client authentication scheme. Certificate Enrolment Service (CES) https://WebRa-WCC-Client.WebRa.local30/Service.sw/CEP/Ignite Certificate Enrolment Service (CES) https://WebRa-WCC-Client.WebRa.local31/Service.sw/CESActivate Windows Certificate Enrolment Service (CES) https://webRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Client.WebRa-WCC-Clie

3. Access the domain controller as an administrator and access the Group Policy Management console by executing gpmc.msc in Run

🖅 Run	>	<
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	gpmc.msc ~	-
	OK Cancel <u>B</u> rowse	

Group Policy Management Console will be open.

4. Navigate to Linked Group Policy Objects



📓 Group Policy Management									-			×
📓 File Action View Window Help											-	б×
(+ 2) 📰 🖸 🔢 📰												
File Action View Window Help Image: State S	WebRA.I Status A V	ocal Linked Group Policy Link Örder 1	Objects GPO	Group Policy Inhe fault Domain Policy	ritance Dele Enforced No	egation Link Enabled Yes	GPO Status Enabled	WMI Filter None	Modified 7/3/2023	Domair WebRA	- 1 A	5 ×

- 5. Make it sure that the link is enabled against the group policy object in which you are going to configure ADSS Web RA enrolment policy.
- 6. If link is not enabled then right click on the Policy object and click on Link Enabled.



7. Right-click on the Policy in which you are going to configure the ADSS Web RA Enrolment Policy and click Edit. Group Policy Editor will open/.

Image: Services File Action View Window Help	ēΧ
 Torest: WebRAlocal WebRAlocal WebRAlocal Default Domain Policy Scope Details Settings Delegation Links Default Domain Policy Bornain Controllers Editnnd OUs are linked to this GPO. 	
Group Policy Management Default Domain Policy ✓ ▲ Forest: WebRAlocal Scope ✓ ▲ Bomains Default Domain Policy ✓ ▲ WebRAlocal Display links in this location: ✓ ▲ WebRAlocal Default Domain Policy ▲ Domain Controllers Edit ★ a Services Enforced	
	~
Group Policy Object Ink Enabled Link Enabled Link Enabled Link Enabled	
> With Filters Save Report_ > Stater GPOs View > States View W Group Policy Modeling New Window from Here	
Group Policy Results Delete Rename Refresh Refresh	
Help	
Add Remove Properties WMI Filtering This GPO is linked to the following WMI filter: <none> Open</none>	

 In the Group Policy Management Editor expand User Configuration > Policies > Windows Settings > Security Policies > Public Key Policies, double click on Certificate Services Client – Certificate Enrolment Policy.

File Action View Help Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Configuration Image: Computer Confi	Group Policy Management Editor		-	×
Image: Solution of the second seco	File Action View Help			
Image: Computer Configuration ○ Image: Configuration ○ Image: Configuration ○ Image: Configuration ○ Image: Configura	🗢 🌩 🙇 📷 🙆 🗟 🖬			
	 Default Domain Policy [WEBRA-WCC-DC.WEBF Computer Configuration Policies Preferences Verse Configuration Policies Software Settings Software Settings Software Settings Software Settings Software Restriction Policies Software Restriction Policies Folder Redirection Policy-based QoS Deployed Printers Administrative Templates: Policy del Preferences 	Diject Type Tuste Trust Trusted People Certificate Services Client - Certificate Enrollment Policy Certificate Services Client - Credential Roaming Certificate Services Client - Auto-Enrollment		

9. The Certificate Enrolment Policy Server properties dialog will display. Paste the ADSS Web RA Server Windows Integrated Certificate Enrolment Policy URL into the Enter enrollment policy server URI field and click Validate Server, the connection test will take place, click Add.


Certificate Enrollment Poli	cy Server	×
Certificate enrollment policy serv	er configuration	
Enter URI for a certificate enrolle click 'Validate Server'.	ment policy server and select the correct authenti	cation type, then
Use default Active Directory	domain controller URI Configure	e Friendly Name
Enter enrollment policy server U	RI:	
https://asc-demo-wra-02.ascer	tiademo.local:86/Service.svc/CEP?Ascertia%20[Demo
Authentication type:		
Windows integrated	~	Validate Server
Priority:		
Priority: Default Certificate enrollment policy prop Information regarding the validat properties returned from the serv	verties ion of the server URI will be presented below. En er match the expected values before proceeding	sure that the
Priority: Certificate enrollment policy prop Information regarding the validat properties returned from the serv The URI "https://asc-demo-wr %20Demo" was validated succ	verties ion of the server URI will be presented below. En er match the expected values before proceeding s-02 ascertiademo local:86/Service.svc/CEP?As esefully.	sure that the
Priority: Default Certificate enrollment policy prop Information regarding the validat properties returned from the serv "The URI "https://asc-demo-wri	veties ion of the server URI will be presented below. En er match the expected values before proceeding +02 ascettademo local:86/Service svc/CEP?As esefully. D-AC345184658C)	sure that the

10. You will be returned to the Certificate Enrolment Policy Server properties, check the tick box to mark this policy server as the default, OK.

Certificate Serv	vices Client - Certifica	te Enroll	ment Polic ?	×
Enrollment Polic	Ξy			
Configuration	Model:	Enable	d	~
Certificate	enrollment policy list —			
Default	Name		Automatic Enrollmen	t
	ADSS WEBRA Enrolln	nent	Enabled	
Add	Remove		Propertie	s
Additional c	ertificate enrollment po	licy confi	guration	
Disable	user configured enroll	ment poli	cy servers	
	O	(Cancel	Apply

7.2.1.3 Test Computer-based Certificate Enrolment

Computer certificates are enrolled for using the local system security context. For manual enrolment, the certificate enrolment will need to be initiated by the Windows Local System account. The following steps include the use of a Microsoft tool to initiate and test this process.

- 1. Download PsExec from Microsoft.
- 2. Extract PSExec to a suitable disk location.
- 3. Click Start, type cmd, right click Command Prompt and select Run as administrator, enter the administrator credentials at the User Account Control dialog if prompted.

All	Apps	Documents	Web	More 🔻	
Best m	atch				
	Comma App	nd Prompt		- Run as	s administrator
Search	the web			🛛 Open	file location
, С сп	nd - See v	veb results		-⇔ Pin to	Start
				-⇔ Pin to	taskbar

4. Change directory to the disk location where PsExec was extracted and run the following command.

C:\sw\PSTools>PsExec.exe -sid mmc

5. The PsExec license agreement dialog will display, click Agree.



6. The Microsoft Management Console will display, press ctrl+m.

🚰 Console1 - [Console Root]				_		$\langle $
🚟 File Action View Favorites Window Hel	p				- 8	×
← ⇒ 🗔 🗟 🖬						
Console Root	Name		Actions			
	There are no items to sho	w in this view.	Console Root			•
			More Actions			•

7. The Add or Remove Snap-ins dialog will display, select Certificates.

Add or Remove Snap-ins						х
You can select snap-ins for t extensible snap-ins, you can	his console from the configure which e	nose xter	available on you nsions are enable	r computer and configure the selected ed.	set of snap-ins. For	
Available gnap-ins:			_	Selected snap-ins:		
Snap-in	Vendor	^		Console Root	Edit Extensions	
ActiveX Control	Microsoft Cor Microsoft Cor				<u>R</u> emove	
Certificates	Microsoft Cor					_
Component Services	Microsoft Cor				Move Up	
Computer Managem	Microsoft Cor				Move Down	
Device Manager	Microsoft Cor		<u>A</u> dd >			- 1
Disk Management	Microsoft and					
Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
Group Policy Object	Microsoft Cor					
IP Security Monitor	Microsoft Cor					
P Security Policy M	Microsoft Cor					
Link to Web Address	Microsoft Cor	\mathbf{v}			Advanced	
Description:			-			
The Certificates snap-in allo	ows you to browse	the	contents of the	certificate stores for yourself, a service	e, or a computer.	
					OK Cancel	

8. Click Add, select the Computer account radio button, click Next.





9. The Select Computer dialog will display, accept the default, click Finish.

Select Computer	×
Select the computer you want this snap-in to manage. This snap-in will always manage:	
Another computer: Allow the selected computer to be changed when launching from the comma only applies if you save the console.	and line. This
< Back Finish	Cancel

10. You will be returned to the Add or Remove Snap-ins dialog, click OK.



11. You will be returned to the Microsoft Management Console with the Local Computer certificate snap-in added. In the left panel, expand Certificates (Local Computer), right click Personal, select Request New Certificate.

Console1 - [Cons	sole Root]		
🚟 File Action V	iew Favorites Window	Help	
🗢 🄿 🔂 🔂	?		
Console Root		^ Nam	e
✓ ☐ Certificates (L	ocal Computer)	a C	- ertificates (Local Computer)
> 🦳 Trust	Find Certificates		
> C Ente	All Tasks	>	Find Certificates
> 📫 Trust	New Window from Here		Request New Certificate
> Untr	Refresh		Import
Contains actions	Help		Advanced Operations >
C.exe - Cisonarst	ore contains a certificates.		

12. The Certificate Enrolment wizard will launch, click Next.



13. The Select Certificate Enrolment Policy dialog will display, accept the default of ADSS WEBRA Enrollment Policy, click Next.

	-		×
🙀 Certificate Enrollment			
Select Certificate Enrollment Policy			
Certificate enrollment policy enables enrollment for certificates based on predefi Certificate enrollment policy may already be configured for you.	ned certificate	e templat	es.
Configured by your administrator			
ADSS WEBRA Enrollment Policy			*
Configured by you		Add N	lew
	Next	Can	cel

14. The Request Certificates dialog will display, this will list all certificate templates in Active Directory that the computer has the enrol permission set for, check the tick box next to the certificate template for which you are enrolling, click Enrol.

lequest Certificates		
ou can request the following types o lick Enroll.	f certificates. Select the certificates you want t	o request, and then
ADSS WEBRA Enrollment Policy		
ADSSTLSServer	i) STATUS: Available	Details
IPSECIntermediateOnline	(i) STATUS: Available	Details
Machine	(i) STATUS: Available	Details
TLSComputer	(i) STATUS: Available	Details
_	CTATUC A	Details

15. The Certificate Installation Results dialog will display, the certificate enrolment will display a status Succeeded, click Finish.

		-		×
📮 Certificate Enrollment				
Certificate Installation Result	ts			
The following certificates have been	enrolled and installed on this computer.			
ADSS WEBRA Enrollment Policy				
ADSSTLSServer	STATUS: Succeeded		Details	•
			<u>E</u> in	ish

16. You will be returned to the Certificates – (Local Computer) management console, expand Personal and click on Certificates, from the right-hand panel, you will see listed the new certificate that was installed as part of the enrolment process.

🚰 Console1 - [Console Root\Certificates (Local Co	omput	ter)\Personal\Certificates]			-	ο×
🚟 File Action View Favorites Window H	Help					- 8 ×
🔶 🏟 📶 🛅 🔯 📑 🚺 📆						
Console Root	^ I:	ssued To	Issued By	Actions		
✓	2	ASC-DEMO-W10-01	ACME Issuing CA	Certificates		•
V Personal			-	More Actions		
Certificates				Wore Actions		
Figure 2 Contraction Authorities 2 Contraction Authorities 2 Contraction Trust						
Enterprise Irust						
Trusted Publishers						
> Untrusted Certificates						
Third-Party Root Certification Authoritie						
> 🧾 Trusted People						
> Client Authentication Issuers						
> Preview Build Roots						
> 🚞 Test Roots						
> 🧮 AAD Token Issuer						
> SIM Certification Authorities	J					
K Homegroun Machine Certificater	<	C	>			
Personal store contains 1 certificate.						

17. Double-click on the certificate to view its contents, select the details tab to view the detailed properties, click ok to close the certificate viewer.

Certificate X	🙍 Certificate	×
General Details Certification Path	General Details Certification Path	
Certificate Information	Show: <all></all>	
This certificate is intended for the following purpose(s):	Field Value	^
Proves your identity to a remote computer Ensures the identity of a remote computer	Version V3 Serial number 07bafaf7edsf89f41cds9150 Signature algorithm sha256R5A Signature hash algorithm sha256 Issuer shake not be the shading CA, Certificati Vald from Thursday, June 29, 2023 ST	ad pn 30
Issued to: ASC-DEMO-W10-01	Subject CR Ascertia Demo ASC-DE	и и
Issued by: ACME Issuing CA		
Valid from 6/29/2023 to 6/29/2024		
$\ref{eq: product}$ You have a private key that corresponds to this certificate.		
Issuer Statement	Edit Properties Copy to	File
OK	[[ОК

During this process, the computer certificate details will be automatically added to the ADSS Web RA Server Enterprise.



Access the Web RA User Certificate Portal, as a user who is in a role with the permissions to see device certificates, in the left hand menu, expand Windows Enrolment, select Issued Certificates, Web RA will display the certificate that was just issued to the user.

WebRA								English	A 🕕
Search	٩	Windows Enrolment	CATES		Search by r	equest no			
Certificate Center	~	Request No	Common Name	Certificate Alias	Certificate Type	Request By	Status	Expiry Date	
El Windows Enrolment	^	649DB1AF-07	ASC-DEMO-W10-01 07bafaf7ed6f89f41cdc9150a dcfceaf59504c45	5d8ad121-a5ed-4b1d- bc83-9b683645136b	ADSS TLS Server – 1 Ye	ASC-DEMO-W10- 01	Issued 2023-06-29	2024-06-29	1
Revocation Requests		649DA64F-E0	ASC-DEMO-W10-01 76f6c2935fd28a3ed953d12 3b1b14e0ea78c26cc	825a83c7-13d8-4c68-8aed- f2e822d12525	ADSS TLS Server – 1 Ye	ASC-DEMO-W10- 01	Issued 2023-06-29	2024-06-29	ı
Personal Information	×	649C57AB-93	ASC-DEMO-W11-1 0f9c11cf29f857548283d284 15960701cb8d34ca	a0bc3187-db24-466c-9fbc- 03096b80e15f	ADSS TLS Server – 1 Ye	ASC-DEMO-W11-1	Issued 2023-06-28	2024-06-28	1
ZX Enterprise	Ŷ	649C53B0-3C	ASC-DEMO-W10-01 455b1a866ad5cbd4a89o4f3 19ea638a0721030bb	f77096c1-52c8-43fa-904b- 9d38124ebb01	ADSS TLS Server – 1 Ye	ASC-DEMO-W10- 01	Issued 2023-06-28	2024-06-28	1
		649C4F9D-F6	ASC-DEMO-WRA-02 0af7c3da94c601af9fc8d224 e31387023e85a50c	d083d68e-a022-41a6-82a6- 5e04db81b9c1	ADSS TLS Server – 1 Ye	ASC-DEMO-WRA- 02	Issued 2023-06-28	2024-06-28	1
Terms of Centine 12		649C4F05-F0	ASC-DEMO-AD-01 5fa3386ff908842e46b38108 028202890d386796	b45c87fd-30a4-4a9f-b29f- da14e12026b1	ADSS TLS Server – 1 Ye	ar ASC-DEMO-AD-01	Issued 2023-06-28	2024-06-28	1
Privacy Policy 🖸		649C04AD-53	ASC-DEMO-W11-1 48946b735d8e9593eedecfb	ec508bce-d860-4195-813c- a171558c1f46	ADSS TLS Server – 1 Ye	Nar ASC-DEMO-W11-1	Issued 2023-06-28	2024-06-28	1
Help C About ttos://manuals.ascertia.com/Web	RA-v2.8/							Sh	wing: 8/8

18. Select [‡] and click View Certificate to see the certificate contents in Web RA, click Close.

This certificate is	s intended for the following purpo	ose(s):		
 Key Enciph 	erment			
 Digital Sigr 	nature			
 Client Auth 	nentication			
 Server Auth 	hentication			
Refer to the certification authority's statement for details.				
Issued to	: ASC-DEMO-W10-01			
Issued by	ACME Issuing CA			
Valid from	m: 2023-06-29 To 2024-06-29			



7.2.1.4 Test User-based Certificate Enrolment

The following steps explain manual certificate enrolment for user-based certificates:

- 1. Access a windows desktop or server as a user who has been granted enrol permission on a certificate template in Active Directory.
- 2. Click Start and type certmgr.msc, press Enter.



3. The Certificates - Current User management console will launch.



4. From the left panel, right click Personal > All Tasks > Request New Certificate.

📓 certmgr	🖀 certmgr - [Certificates - Current User\Personal]						
File Action	n View Help						
(= =) 🖄	📅 🛍 🙆 🔒 🔽						
Certifica	Certificates Certificates Tificates Certificates Cert						
> 📫 Er	All Tasks	Find Certificates					
> 📫 A	View	Request New Certificate					
> = u	Refresh	Import					
ר 🔛 🗧 און	Export List	Advanced Operations >					
⇒ 📫 C	C Heip C C Heip C C Heip C C C C C C C C C C C C C C C C C						
> 📫 C > 📫 Certi	C Heip C Certificate Enrollment Reque:						

5. The Certificate Enrolment Wizard will launch, click Next.



6. The Select Certificate Enrolment Policy dialog will display, accept the default of ADSS WEBRA Enrolment Policy, click Next.

	-		×
🔄 Certificate Enrollment			
Select Certificate Enrollment Policy			
Certificate enrollment policy enables enrollment for certificates based on predef Certificate enrollment policy may already be configured for you.	ined certificat	e templat	es.
Configured by your administrator			
ADSS WEBRA Enrollment Policy			~
Configured by you		Add N	lew
	Next	Can	cel

7. The Request Certificates dialog will display, this will list all certificate templates in Active Directory that your user has the enrol permission set for, check the tick box next to the certificate template for which you are enrolling, click Enrol.

		-		×
📮 Certificate Enrollment				
Request Certificates				
You can request the following type: click Enroll.	s of certificates. Select the certificates you wa	nt to request, a	and then	
ADSS WEBRA Enrollment Policy	1			
ADSSTLSUser	STATUS: Available		Details	~
Show <u>a</u> ll templates				
		<u>E</u> nroll	Cane	:el

8. The Certificate Installation Results dialog will display, the certificate enrolment will display a status of Succeeded, click Finish.

		-		×
📮 Cer	tificate Enrollment			
C	Certificate Installation Results			
1	The following certificates have been enrolled and installed on this compu	iter.		
ı [ADSS WEBRA Enrollment Policy			
	ADSSTLSUser 🧹 STATUS: Succeeded	H	Details (•
			Fini	sh
			- Turn	

You will be returned to the Certificates – Current User management console, expand Personal and click on Certificates, in the right-hand panel, you will see listed the new certificate that was installed as part of the enrolment process.



9. Double-click on the certificate to view its contents, select the Details tab to view the detailed Properties, click OK to close the certificate viewer.

🚛 Certificate	×	Certificate	×
General Details Certification Path		General Details Certification Path	
Certificate Information		Show: CAI>	^
This certificate is intended for the following purpose(s): • All application policies		Head Value Serial number 4969a-4831dbf3e0acf46b0fdd Signature algorithm sha256RSA Signature hash algorithm sha256RSA Valid from 29 June 2023 16:48:07 Valid from 29 June 2023 16:48:07	
Issued to: Philip Fry		GR Ascretia Demo. Web RAII	~
Issued by: ACME Issuing CA			
Valid from 29/06/2023 to 29/06/2024			
You have a private key that corresponds to this certificate.			
Issuer Statement	1	Edit Properties Copy to File	
OK		0	<

During this process, the user will be automatically added to the ADSS Web RA Server Enterprise, access the user's inbox and follow the instructions in the email to activate their account.



10. Access the Web RA User Certificate Portal, in the left hand menu, expand Windows Enrolment, select Issued Certificates, Web RA will display the certificate that was just issued to the user.

WebRA									English 🔻	• 🕕 🗘
Search	۹									
🕐 Dashboard		ISSUED CERTIFICATES			Search by request no					ų
E Certificate Center	¥	Request No	Common Name	Certificate Alias	Certific	ate Type	Request By	Status	Expiry Date	
Windows Enrolment Certificate Requests	^	649DA7B7-78	Philip Fry 4989a4831dbf3e0acf46b0f dd0bf44c44d7dafd5	3a5c25d0-8d5f-4b0b- a3e4-7624b538d703	ADSS TI	_S User – 1 Year	Philip Fry	Issued 2023-06-29	2024-06- 29	:
Revocation Requests	_									

11. Select [‡] and click View Certificate to see the certificate contents in Web RA, click Close.

CERTIFICATE INFORMATION	×
This certificate is intended for the following purpose(s): Key Encipherment Digital Signature	
Refer to the certification authority's statement for details.	_
Issued to: Philip Fry Issued by: ACME Issuing CA Valid from: 2023-06-29 To 2024-06-29	
CLOSE	



7.2.2 Certificate Auto-Enrolment

Certificate auto-enrolment is a function of Active Director Certificate Services (ADCS) enabled by Group Policy that allows users and devices to enol for certificates. No user interaction is required.

Microsoft auto-enrolment uses the settings configured in Active Directory Group Policy. Group Policy is automatically refreshed when you restart the domain member computer, or when a user logs on to a domain member computer. In addition, Group Policy is periodically refreshed. By default, Group Policy is refreshed every 90 minutes.

Certificate auto-enrolment using Microsoft Group Policy requires the following:

- Windows Certificate templates should be configured with the Auto-enrol permission set for users\computers or a Windows active directory group.
- Windows users\computers to be domain members, and have an email address configured in the Active Directory account.
- Active Directory Group Policy needs the URL for the ADSS Web RA Server Certificate Enrolment Policy Service.
- Microsoft Certificate Services Client Auto-Enrolment needs to be enabled in Active Directory Group Policy.

7.2.2.1 Configure certificate auto-enrolment for computers

- 1. Access Web RA as a user with permissions to access Windows Enrolment settings for your enterprise
- 2. From the dashboard, expand Windows Enrolment > Settings and copy the URL from the Certificate Enrolment Policy (CEP) field in the Windows Integrated section.

WebRA			Ingish + 44
	Q		
Dashboard			
E Certificate Center	~	The Windows Envolment is a protocol for automating x509 certificate issuance for public key	infrastructure (PKI) clients. These include web servers, endpoint devices and user
E Windows Enrolment	•	identities, and anywhere PKI certificates are used, as well as the associated certificates from a to enrol identity certificates based on authentication scheme in deployment URLs.	trusted Certificate Authority (CA). Windows Enrolment uses certificate enrolment policy
Certificate Requests		Windows Integrated	
issued Certificates		URLs for Windows certificate enrolment using Windows Integrated authentication scheme	
Revocation Requests		Certificate Enniment Policy (CEP)	Certificate Ennihment Service (CES)
Settings		https://aoc-demo-wea-02.aocertiademo.local.06/Service.svc/CBP7Accertia/620Dr 🗗	https://asc-demo-wra-02.ascartiademo.localt87/Service.avc/CE5
Personal Information		 Service address use for windows certificate enrolment service. Copy URL to configure policy service a.g. (Service URL/Service.vc/CEP) 	Service address use for windows certificate environment service, copy URL to certificate service e.g. (Service URL/Service.scc/CES)
🚊 Enterprise		Human (Dermand	
		Osername / Password	
		UKLs for Windows certificate enrolment using Username / Password authentication schem	6.
		Contribution Environment Policy (CEP) https://acc-domo-wra-02.accertiademo.tocal.00/Service.ovc/CEP?Accerto/%20Dr 💋	Certificate Envelopent Service (CES) https://asc-demo-wra-02.ascortiademo.locali09/Service.sec/CES
		• Service address use for windows certificate envolvent service. Copy URL to configure policy service URL/Service.ver/CEP	Service address use for windows certificate electionent service, copy URL to configure certificate service e.g. (Service URL)Service.xxx/CES
		Client Authentication	
Terms of Service 🖻		UBLs for Windows certificate enrolment using client authentication scheme.	
Privacy Policy 🛃		Cartificate Ferniement Bolicy (CSE)	Cartificate Foodment Service (CFS)
		https://ast-demo-w/a-02.ascer0ademo.locab90/Service.svc/CEP7Ascer0af620Dr @	Mtps://asc-demo-wra-62.ascertiademo.local/91/Service.avg/CES
unt C		Service address use for windows certificate emplayed service. Copy URL to configure policy	Service address use for Windows certificate enrolment service, copy URL to configure certificate
About			

- 3. Access the domain controller as a member of the domain administrators group.
- 4. Click Start > Windows Administrative Tools, double click Group Policy Management.
- 5. The Group Policy Management tool will display, right-click the Default Domain Policy from the left panel, and click Edit.





6. The Group Policy Management Editor will display.



7. Expand Computer Configuration > Policies > Windows Settings > Security Settings, select Public Key Policies.

File Action View Hep File Action View Hep	Group Policy Management Editor	📓 Group Policy Management Editor 🛛 🗖 🖸								
 Computer Configuration Concentrate Configuration Policies Policies Software Settings Warne Resolution Policy Software Settings Marne Resolution Policy Software Settings Software Retriction Policies Software Retrictino Policies Software Retriction Policies <	File Action View Help									
 Computer Configuration Seftware Settings Settware Settings Manne Resolution Policy Serticity Statup/Shuttown) Settings Manne Resolution Policy Settings Macounthy Policies Settings Macounthy Policies System Settings Settings Settings Settings Settings Settings Settings Settings Manne Resolution Policy Settings Settings Macounthy Policies System Services System Services System Services Settings Settings<!--</td--><td>← ⇒ 2 📷 Q 🔒 🖬 🖬</td><td></td><td></td><td></td><td></td><td></td>	← ⇒ 2 📷 Q 🔒 🖬 🖬									
	Computer Configuration Policie Software Settings Mindows Mindows	*	Cloject Type Charaypting File System Data Protection Bittocker Drive Encryption Bittocker Drive Encryption Bittocker Drive Encryption Network Unlock Certificate Automatic Certificate Automities Trustee Stock Certification Authorities Trustee Policitate Certification Authorities Intermediate Certification Authorities Trustee Policitates Certificate Services Client - Certificate Enrollment Policy Certificate Services Client - Auto-Enrollment Certificate Services Client - Auto-Enrollment							
		_								

8. In the right hand panel, right-click on Certificate Server Client - Auto-Enrolment Properties:



9. The Enrolment Policy dialog will display, set the Configuration Model drop down to Enabled, and click the Add button.

Certificate Services Client - Certificate Enrollment Polic ? X								
Enrollment Policy								
Configuration Model: Enabled								
Certificate enrollment policy list	Certificate enrollment policy list							
Default Name	Automatic Enrollment							
Add Remove	Properties							
Additional certificate enrollment policy configuration								
OK	Cancel Apply							

10. The Certificate Enrolment Server properties dialog will display, paste the CEP URL into the Enter enrollment policy server URI field and click Validate Server, the connection will be validated and the results displayed, click Add.

	ficate enrollment policy server and se	elect the correct authen	tication type, then
Use default Acti	ve Directory domain controller URI	Configu	re Friendly Name
Enter enrollment po	icy server URI:		
https://asc-demo-v	vra-02.ascertiademo.local:86/Service	svc/CEP?Ascertia%20)Demo
Authentication type			
Windows integrate	d	~	Validate Server
Certificate enrollmer Information regardin properties returned	it policy properties g the validation of the server URI will from the server match the expected v	be presented below. E alues before proceedin	insure that the
The URI "https://a %20Demo" was va	sc-demo-wra-02.ascertiademo.local: lidated successfully.	86/Service.svc/CEP?A	scertia 🔺
120000110 1103 10			
Enrollment ID {083C7011-1D0	A-4855-885D-AC945184658C}		

11. You will be returned to the Enrollment Policy properties dialog, check the Default check box, click OK.

Configuration	Model:	Enable	d	~
Certificate e	enrollment policy list			
Default	Name		Automatic Enrolln	nent
	ADSS WEBRA Enr	ollment	Enabled	
Add	Remove		Proper	rties

12. You will be returned to the Group Policy Management Editor, right-click Certificate Services Client – Auto-Enrollment, select Properties.

Trusted People				
Certificate Services Client - Certificate Enrollment Policy				
Certificate Path Validation Settings				
Certificate Services Client - Auto-Enrollment				
	Properties			
	Help			

- 13. The Enrolment Policy Configuration properties will display. Set the configuration model to Enabled and select the checkboxes for both of the following settings, click OK:
 - a. Renew expired certificates, update pending certificates, and remove revoked certificates.
 - b. Update certificates that use certificate templates.



Certificate Services Client - Auto-Enr	ollment Properties	? ×
Enrollment Policy Configuration	Console Root\Defaul	t Domain Polic
Enroll user and computer certificates	automatically	
Configuration Model:	Enabled	~
Renew expired certificates, updat revoked certificates	e pending certificates, an	d remove
Update certificates that use certif	icate templates	
Log expiry events and show expiry n remaining certificate lifetime is	otifications when the perc	entage of
10 🔺 %		
Additional stores. Use "," to separate "Store1, Store2, Store3"	multiple stores. For exan	ıple:
ОК	Cancel	Apply

7.2.2.2 Test auto enrolment for computer certificates

Follow these steps to test computer-based auto-enrolment:

- 1. Log into the Windows machine where you wish to test auto-enrolment.
- 2. Click Start, type certlm.msc, and press Enter.

Windows 10		Windows 11	
All Apps Documents Web More	··· ×	D certim.msd	
certim.msc Microsoft Common Console Document		(b) Chat All Apps Documents Web Settings F	olders Photos 🕨 🜔
Search the web	certim msc	Best match	
	Microsoft Common Console Document	Gertlm.msc Microsoft Common Console Document	
	·		
, ○ certIm.msc current user	Location C:\WINDOWS\system32	Search the web	certim.msc crosoft Common Console Document
O continu mass united anna 11		O continuing Source to any security	

3. The Certificates – Local Computer management console will display, select Personal, the certificate store is currently empty.

ᡖ certlm - [Certificates - Local Com	puter\Personal]	_	×
<u>File Action View H</u> elp			
🗢 🔿 🙍 📆 📋 🧟 😽	? 🖬		
Certificates - Local Computer Personal Trusted Root Certification Certification Certification Certification Certification Certification Certification Trusted Publishers Certificat Trusted Publishers Certificat Certificat	Object Type	There are no items to show in this view.	
Personal store contains no certificates.			

To trigger an update to Group Policy, perform one of the following actions:

- Restart the machine
 - Rebooting a domain member login to the system will trigger a refresh of group policy.
- Updating the group policy using the command line

- Users can force an updated to Group Policy via an administrative command line.
- 4. Click Start, type run, click on Run as administrator.

Windows 10		Windows 11
All Apps Documents Web More ▼ Best match Image: Command Prompt App App Settings Settings Replace Command Prompt with Windows PowerShell in the Win + X > Search the web	··· × Command Prompt App □ copen □ copen □ copen file location	
L.		

- 5. Authenticate using domain administrator credentials if promoted by User Access Control.
- 6. Run the following command.



Computer	Policy	update	has	completed	successfully.				
Return to	Cortific	atos — l	ocal	Computer	management co	nsolo s	oloct Pors	onal and	

 Return to Certificates – Local Computer management console, select Personal and press refresh, now expand Personal and click on Certificates, the machine certificate will display.

🖀 certlm - [Certificates - Local Com	puter\Personal\Certificates]	-	×
File Action View Help			
🗢 🔿 🙍 📆 📋 🙆 😽	? 📧		
🙀 Certificates - Local Computer 🔨	Issued To	Issued By	E
🗸 🚞 Personal	10-01	ACME Issuing CA	
Certificates		Active Issuing CA	
> 📔 Trusted Root Certification			
> 📔 Enterprise Trust			
> 🦳 Intermediate Certification			
> Trusted Publishers			
> Intrusted Certificates			
> 🚞 Third-Party Root Certifical			
> 🧮 Trusted People			
> Client Authentication Issu			
> Preview Build Roots			
> 🧮 Test Roots			
> 📔 AAD Token Issuer			
> 📔 eSIM Certification Authori			
> 🧾 Homegroup Machine Cer			
> 🚞 Remote Desktop 🗸 🗸			
< >	<		>
Personal store contains 1 certificate.			

8. Double-click on the certificate to view its General Properties, select the Details tab to view all of the certificate contents.

💭 Certificate	×	🐖 Certificate			×
General Details Certification Path		General Details	Certification F	Path	
Certificate Information This certificate is intended for the following purpose(s): Proves your identity to a remote computer Ensures the identity of a remote computer	-	Show: CAIS Field Serial numb Signature a Signature to Issuer	ier Igorithm iash algorithm	Value V3 67460a22d4d15f25942413e sha256RSA sha256 ACME Issuing CA, Certificat 30 June 2023 10:37:40	:2
Issued to: ASC-DEMO-W10-01		Subject		GR Ascertia Demo ASC-DE	м 👻
Issued by: ACME Issuing CA					
Valid from 30/06/2023 to 30/06/2024					
$\ref{eq: relation}$ You have a private key that corresponds to this certificate.	. [
Issuer Statement	1			Edit Properties Copy to	File
OK				[ОК

7.2.2.3 Configure certificate auto-enrolment for users

- 1. Access Web RA as a user with permissions to access Windows Enrolment settings for your enterprise.
- 2. From the dashboard, expand Windows Enrolment > Settings and copy the URL from the Certificate Enrolment Policy (CEP) field in the Windows Integrated section.

WebRA			tinglish + 🚨 🌔
iearch	Q	Weslows Encomment SETTINGS	
② Dashboard			
E Certificate Center		The Windows Enrolment is a protocol for automating v.509 certificate issuance for public key	infrastructure (PI0) clients. These include web servers, endpoint devices and user
Windows Enrolment	•	identities, and anywhere PKI certificates are used, as well as the associated certificates from a to enrol identity certificates based on authentication scheme in deployment URLs.	trusted Certificate Authority (CA). Windows Enrolment uses certificate enrolment policy
Certificate Requests		Windows Integrated	
Issued Certificates		URLs for Windows certificate enrolment using Windows Integrated authentication scheme	
Revocation Requests		Certificate Environment Policy (CEP)	Certificate Environment Service (CES)
Settings		https://asc-demo-web-02.socertisdomo.local.th/Service.avc/CEP1Ascentus%20De 🗗	https://ase-demo-wra-62.ascartiademo.localt87/Service.ave/CES
Personal Information		 Service address use for windows certificate enrolment service. Copy URL to configure policy service a.g. [Service URL/Service.vcc/CEP 	 Service address use for windows certificate ensument service, copy URL to configure certificate service e.g. [Service URQ/Service.swiTES
Enterprise		Username / Password	
		IRIs for Windows certificate enrolment using Username / Passaord authentication schem	
		Curtificate Enrolment Policy (CEP)	Cartificata Eurolment Service (CES)
		https://asc-demo-wra-02.ascertiadwmo.local.fill/Service.avc/CEP?Ascertia%20D+ 🕏	https://www.demo-wra-02.aucortiadamo.local/05/Service.sec/CES
		O Service address use for windows certificate envolvent service. Copy URL to configure policy service URL/Service.URL/Servi	 Service address use for windows centificate enconvent service, copy UPL to configure centificate tervice e.g. (Service URL) Service.acc/CES
		Client Authentication	
ierms of Service 🕑		URLs for Windows certificate enrolment using client authentication scheme.	
rivacy Policy 🖉		Cartificate Envolvment Policy (CEP)	Cartificate Explorant Service (CES)
sin Pt		https://asc-demo-wra-Q2.accertuidems.local.90/Service.svc/CEPTAscenturh20Dc	https://acc-demo-wra-62.accertiademo.localc91/Service.avc/CE5
		O Service address use for windows certificate enrolment service. Copy URL to configure policy	Service address use for windows certificate enrolment service, copy URL to configure certificate
About		• Your open of the antique country were own or a standard built	

- 3. Access the domain controller as a member of the domain administrators group.
- 4. Click Start > Windows Administrative Tools, double click Group Policy Management.
- 5. The Group Policy Management tool will display, right-click the Default Domain Policy from the left panel, and click Edit.





6. The Group Policy Management Editor will display.

Group Policy Management Editor			-	×
File Action View Help				
(+ + 🔐 🖾 🗟 🖬				
Default Domain Policy (AS-COE Default Domain Policy (AS-COE Select an item to: Default Dom Default Dom Default Dom Default Dom Default Dom Default Dom Select an item to: Default Dom Pedefault Pedefault	nain Policy (ASC-DEMO	→AD-01 ASCERTIADEMOLO Name Computer Configuration Beer Configuration	CAL] Policy	
< >> Extended Stan	dard /			

7. Expand User Configuration > Policies > Windows Settings > Security Settings, select Public Key Policies.

 Group Policy Management Editor File Action View Help 		-	×
Peter Domain Policy (JAS-DEMO-AD-D1.ASCERTIADEM) # Computer Configuration >> Petervecss >> Software Settings >> With Configuration >> Petervecss >> User Configuration >> Policies >> Software Settings >> With User Configuration >> Policies >> Software Settings >> Worksy Settings >> Software Settiction Policies >> Policie Policies >> Policies	Object Type Enterpoint Fruit Trusted People Certificate Services Client - Certificate Enrollment Policy Certificate Services Client - Auto-Enrollment Certificate Services Client - Auto-Enrollment		
< >>	<		>

8. From the right panel, right-click on Certificate Server Client - Auto-Enrolment Properties.



9. The Enrolment Policy dialog will display, set the Configuration Model drop down to Enabled, and click the Add button.

Certificate Services Client - Certificat	te Enrollment Polic ?	×			
Enrollment Policy					
Configuration Model:	Enabled	\sim			
Certificate enrollment policy list	Certificate enrollment policy list				
Default Name	Automatic Enrollment				
Add Remove	Properties				
Additional certificate enrollment po	icy configuration	- 1			
Disable user configured enroll	nent policy servers				
OK	Cancel Ap	ply			

10. The Certificate Enrolment Server properties dialog will display. Paste the CEP URL into the Enter enrolment policy server URI field and click Validate Server. The connection will be validated and the results displayed, click Add.

	ient policy server conliguration		
Enter URI for a c click "Validate Se	ertificate enrollment policy server and select t rver'.	the correct authentication type, the	nen
Use default A	ctive Directory domain controller URI	Configure Friendly Nan	ne
Enter enrollment p	policy server URI:		
https://asc-demo	o-wra-02.ascertiademo.local:86/Service.svc/	/CEP?Ascertia%20Demo	
Authentication typ	pe:		
Windows integra	ated	✓ Validate Serv	rer
	- Diddit		
Certificate enrollm Information regard properties returne	ent policy properties ting the validation of the server URI will be p d from the server match the expected values	resented below. Ensure that the s before proceeding.	
Certificate enrollm Information regare properties returne "A20Demo" was Enrollment ID {083C7011-11 Forrollment Frenz	ent policy properties drag the validation of the server URI will be p dram the server match the expected values //acc.demo.wra-02.ascertiademo.local.86/Se validated successfully. DDA.4855.885D.AC345184658C) the Name	resented below. Ensure that the before proceeding. envice.svc/CEP?Ascertia	Í

11. You will be returned to the Enrollment Policy properties dialog, check the Default check box, click OK.

Certificate Serv	ices Client - Certificat	e Enroll	ment Polic	?	×
Enrollment Polic	У				
Configuration	Model:	Enable	d		\sim
Certificate e	Certificate enrollment policy list				
Default	Name		Automatic Enr	ollment	
	ADSS WEBRA Enrollm	ent	Enabled		
Add	Add Remove Properties				
Additional certificate enrollment policy configuration					
	garca cirroni		.,		
	OK		Cancel	App	oly

12. You will be returned to the Group Policy Management Editor, right-click Certificate Services Client – Auto-Enrolment, select Properties.

Trusted People		
Certificate Services Client - Certificate Enrollment Policy		
Certificate Path Validation Settings		
Certificate Services Client - Auto-Enrollment		
Properties		
Нер		

- 13. The Enrolment Policy Configuration properties will display. Set the configuration model to Enabled and select the checkboxes for both of the following settings, click OK:
- Renew expired certificates, update pending certificates, and remove revoked certificates.
- Update certificates that use certificate templates.



Certificate Services Client - Auto-Enrollment Properties \qquad ? \qquad X			
Enrollment Policy Configuration	Console Root\Defau	ılt Dom	ain Polic
Enroll user and computer certificates automatically			
Configuration Model:	Enabled		~
Renew expired certificates, update pending certificates, and remove revoked certificates			
Update certificates that use certifi	cate templates		- 1
Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is			
10 🔺 %			
Additional stores. Use "," to separate multiple stores. For example: "Store 1, Store 2, Store 3"			
			- 1
			- 1
			- 1
ОК	Cancel	Ap	ply

7.2.2.4 Test auto-enrolment for user certificates

- 1. Log into the windows machine where you wish to test auto-enrolment.
- 2. Click Start, type certmgr.msc, and then press Enter.

Windows 10 Windows 11			
All Apps Documents Web More ← Best match Certifigr.msc Microsoft Common Console Document Search the web Ø certmgr.msc - See web results >	Control Contro Control Control Control Control Control Control Control Control Co	 Certingunud, Chan, Apps, Documents, Web Best match Restructurement Moresoft, Console Document Search the web O certingunuc, See web results 	Settings Folders Protos • •• (b)
		-	Copen Run as administrator

3. The Certificates – Current User management console will display, select Personal, the certificate store is currently empty.

Certmgr - [Certificates - Current U File Action View Help ← ➡ 2 ☐ ➡ 2 ☐ ■ 2 ☐ ■	Jser\Personal\Certificates]		-	
Certificates - Current User Personal Certificates Trusted Root Certification Au Intermediate Certification Au Active Directory User Object Trusted Publishers Untrusted Publishers Untrusted Certificates Truide Park Root Certification Truide People Cilent Authentication Issuers Smart Card Trusted Roots	Issued To	Issued By There are no items to show in this view.	Expiration Date	Intended Pu
< >	<			>

To trigger an update to Group Policy, perform one of the following actions.

• Restart the machine

Rebooting a domain member login to the system will trigger a refresh of group policy.

• Updating the group policy using the command

Users can force an updated to Group Policy via the command line.



- 4. Click Start, type run, type cmd, and then press Enter.
- 5. Run the following command:



Example Output



6. Return to Certificates – Current User management console, select Personal and press refresh, now expand Personal and click on Certificates, the user certificate will display.



7. Double-click on the certificate to view its General Properties, select the Details tab to view all of the certificate contents.

🖬 Certificate X	Certificate X
General Details Certification Path	General Details Certification Path
Certificate Information	Show: <all> ~</all>
This certificate is intended for the following purpose(s): • All application policies	Field Value A Version V3 Serial number 2b4aacbb8376cc7f50d48cdb Signature algorithm sha256R5A Signature hash algorithm sha256 Itsuer ACME Issuing CA, Certification Valid from 30 June 2023 10:54:44
Issued to: Philip Fry	Valid to 30 June 2024 10:54:44
Issued by: ACME Issuing CA	
Valid from 30/06/2023 to 30/06/2024	
$\ref{eq:product}$ You have a private key that corresponds to this certificate.	
Issuer Statement	Edit Properties Copy to File
OK	OK

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

*** End of Document ***