DigiCert® Autoenrollment Server Deployment Guide

Version 8.22.4

February 16, 2023

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. DIGICERT, INC. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The licensed software and documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the licensed software and documentation by the U.S. Government shall be solely in accordance with the terms of this documentation.

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
https://www.digicert.com

Table of Contents

Abstract

This document describes the installation and configuration steps for DigiCert Autoenrollment Server Deployment Guide.

Revision History

No.	Date	Summary
1.	2021/08/26	- Removed PKI Enterprise Gateway and Autoenrollment Server dependencies within the PKI Manager portal. - Updated the section "Importing the Autoenrollment Configuration file" as per the new User Interface.
2.	2021/12/06	- Added support for Windows Hello for Business: o Added new section "1.5 About Integration with Windows Hello for Business" o Added template v4 support at "5.4 About the Preparation of Certificate Templates" - Product renamed from "DigiCert PKI Enterprise Gateway Autoenrollment Server" to "DigiCert Autoenrollment Server" and removed reference to PKI Enterprise Gateway throughout the document. - At "2.2 Required Software ", required VC version changed from "Visual C++ 2015 Redistributable Update 3 (x64)" to "Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019 (x64)". - The Autoenrollment Server zip package has now been separated from Enterprise Gateway zip package. Fixed section "3.1 Install the Autoenrollment Server" with current information. - Moved "3.6 Setting the Autoenrollment Permissions" to "3.3 Setting the Autoenrollment Permissions" and added screenshots for clarification. - Registration Authority certificates has been removed from the zip package and moved to https://knowledge.digicert.com/solution/ca-hierarchies-for-production-and-test-drive-ra-certificates.html. Section

		“4.2.1 Obtaining an RA Certificate to Store in an HSM“ has been fixed to accommodate the change. • Log configuration support using log4cpp added: o Added new section “4.4 Log Properties Configuration Options” o Cleaned up and consolidated logging information from following sections: ▪ “7.1 About Troubleshooting“ removed ▪ “7.2 Format of Log File Messages“ removed ▪ Fixed following sections: ▪ “5.2 Files Written by the Autoenrollment Process“ ▪ “7.1 Repeating an Action with a Higher Log Level“ ▪ “7.2.6 Catastrophic Error When Restarting the Autoenrollment Server“ o Added “6.2 Configuring Autoenrollment Server for Syslog” • Added information about how to create profile for AE Server at “4.5 Creating Autoenrollment Certificate Profile”. • Fixed references to wrong pages and links at multiple locations.
3.	2022/05/25	• Support for Windows Server 2022 • Support for EOBO (Enroll On Behalf Of)
5.	2023/02/15	• Removed references to unsupported operating systems.

CHAPTER 1

2 Introduction

This chapter includes the following topic:

2.1 About DigiCert PKI Platform

You can use DigiCert® PKI Platform to issue certificates to end users. These certificates can be used for smart card logon, SSL connections, encrypted file system (EFS) transactions, and to exchange encrypted mail, among other applications. By specifying group policy settings for domains, users, and machines, you can define the certificate templates that automatically enroll your users for certificates when they log on to Windows operating systems.

The DigiCert Autoenrollment Server connects the network infrastructure with the DigiCert Certification Authority (CA). Therefore, you can easily create certificate templates and issue certificates automatically using the PKI Cloud Service.

2.2 Intended Audience

It is assumed that you have a thorough knowledge about Windows domain and network administration, as well as an understanding of PKI components, workflows, and cryptographic systems. However, it is not necessary to have an in-depth knowledge about how cryptographic algorithms or other technical details work.

2.3 About the DigiCert Autoenrollment Server Deployment

The DigiCert Autoenrollment Server handles the following aspects of the autoenrollment process:

- Requesting certificates
- Tracking pending requests and certificate renewals
- Renewing a certificate

DigiCert Autoenrollment Server enables you to provide your network computers and end users with certificates issued by DigiCert PKI Platform.

DigiCert Autoenrollment Server needs to be installed on a supported Windows server within a Windows domain. DigiCert Autoenrollment Server includes a domain controller and an Active Directory (AD) server to provide information on policies, certificate templates, and users. The operating system uses the Windows autoenrollment client to automatically request certificates for users of the domain when they log onto the network. The system keeps track of the certificates' validity and requests a renewal when a certificate is about to expire.

See “Supported Windows Operating Systems”.

2.4 About the Autoenrollment Process

The Windows autoenrollment client sends a certificate request to the Autoenrollment server. The server verifies the information that is contained in the request against the user's account details. Autoenrollment Server can retrieve information from Active Directory to perform further checks or to enforce restrictions regarding the certificate's content. The Autoenrollment server then submits the request to the DigiCert Certificate Authority (CA) and waits for the request to be processed.

The DigiCert CA processes the request, issues the certificate, and returns it to the Autoenrollment server. The Autoenrollment server then returns it to the client. If configured to do so, the Autoenrollment server also publishes the certificate to the Active Directory.

2.4.1 About Interoperation with Active Directory

Your installation of the Autoenrollment server interacts with your Active Directory server as follows:

- When users log on to the system, the Windows autoenrollment client contacts your Active Directory to see which certificates are required. This applies to new as well as renewal certificates. The information that is contained in the templates identifies the CA that the client must use to obtain the required certificates.
- The client passes the request on to the Autoenrollment server, which validates the information that is contained within the request. The server may correct or add data it obtains from the Active Directory.
- Once the DigiCert CA has issued the certificate, the Autoenrollment server populates the Active Directory with the newly-created certificates.

Figure1-1 illustrates the data flow that is involved with the autoenrollment process.

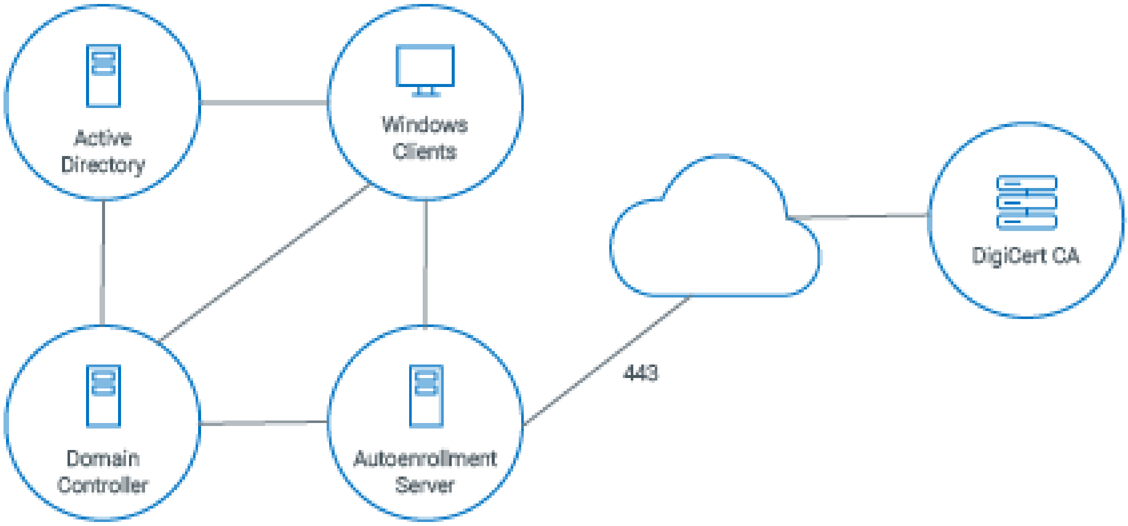


Figure 1-1 Autoenrollment Process

2.4.2 About Renewal of Certificates and Private Keys for Autoenrollment Clients

The process of renewing expiring certificates is nearly identical to the process of requesting a new certificate. The only exception is that the autoenrollment client includes a reference to the certificates that must be renewed. You configure the certificate renewal period in PKI Manager. The Windows autoenrollment client automatically requests renewal of certificates when 80% of the certificate's validity period has expired. Autoenrollment client also requests for renewal when the certificate renewal period has been reached, whichever time frame is smaller.

2.4.3 Autoenrollment Deployments

Figure 1-2 illustrates how the Autoenrollment server is typically deployed. Although this diagram illustrates a single-server deployment, the Autoenrollment server deployment is identical for both the single server and the multiple server deployments.

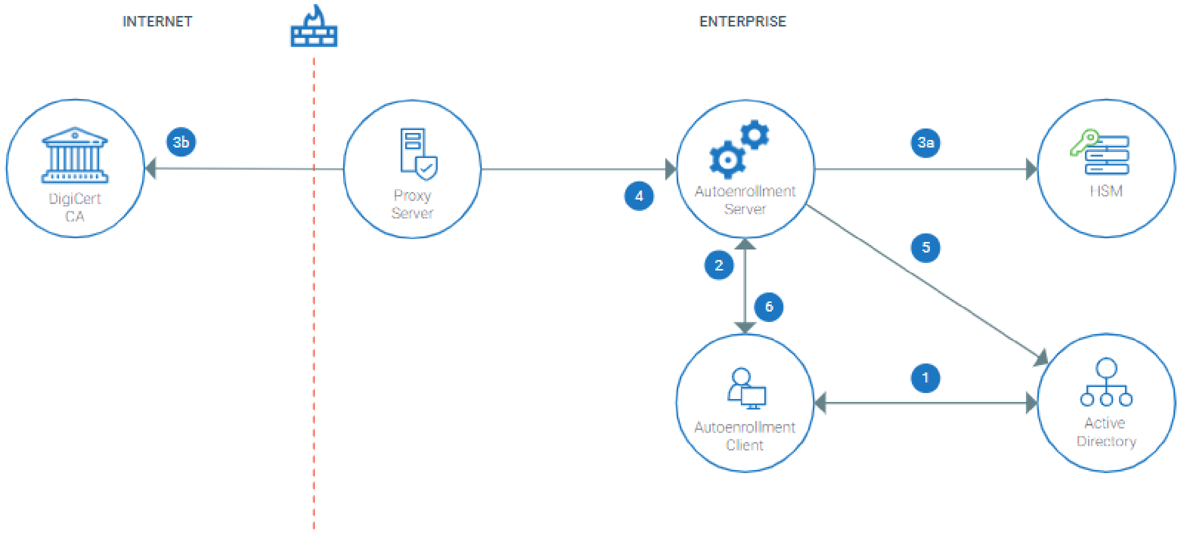


Figure 1-2 Autoenrollment server in an Enterprise deployment

A typical certificate enrollment flow would be as follows:

1. When an end user logs into a computer, the autoenrollment client checks the Active Directory. Or, when a certificate policy is pushed to an end-user computer, the autoenrollment client checks the Active Directory. It then checks the local certificate store to determine the certificate template to which the end user can enroll.
2. Based on this determination, the autoenrollment client requests the Autoenrollment server to initiate an enrollment request for the appropriate certificate type.
3. The Autoenrollment server requests a certificate from the DigiCert CA:

   a) The Autoenrollment uses the RA certificate that is stored on the HSM to secure communications with the DigiCert CA.
   b) The Autoenrollment server sends a Web service call to the DigiCert CA to request the certificate.

4. If the user data and certificate request are correct, the DigiCert CA returns the end-user certificate to the Autoenrollment server.
5. If the Autoenrollment server is configured to do so in the certificate profile, it publishes the certificate to the Active Directory.
6. The Autoenrollment server provides the certificate to the autoenrollment client for installation into the end user's certificate store.

2.5 About Integration with Windows Hello for Business

The Autoenrollment Server has the potential to integrate with Windows Hello® for Business, a feature by Microsoft® starting from Windows 10, and issue certificates from the DigiCert PKI Platform hosted Certificate Authorities.

Refer to https://knowledge.digicert.com/solution/integration-for-windows-hello-for-business.html for more details.

2.6 About support for Enroll On Behalf Of

The Autoenrollment Server now supports EOBO (Enroll On Behalf Of) feature, with v2.21.7 and onwards.

Refer to https://knowledge.digicert.com/generalinformation/digicert-autoenrollment-server-support-for-eobo.html for more details.

CHAPTER 2

3 Prerequisites

This chapter includes the following topics:

- Supported Windows Operating System
- Required Software
- Supported HSMs
- Firewall Settings

3.1 Supported Windows Operating Systems

Table 2-1 lists the versions of Windows operating systems for client and server installations on which the Autoenrollment server can operate.

Table 2-1 Supported Windows Operating Systems

User	Supported Operating Systems
Client	• Windows 10 • Windows 11 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Server	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022

3.1.1 About Preparing the Windows Environment

The Autoenrollment server integrates with the Windows operating system. Autoenrollment Server handles the certificate requests that the native Windows autoenrollment client software generates. Autoenrollment Server passes them on to the DigiCert's CA and stores the issued certificates in your domain's Active Directory.

DigiCert recommends that you carefully plan the forest structure of your network. The recommended best practice is to install CAs as a member of the root domain in the forest to provide centralized administration and control of the PKI services.

For additional best practices, see the Microsoft documentation.

Additionally:

- The Autoenrollment server machine must be in a Microsoft Windows domain that runs Active Directory and contains at least one domain controller.
- If you have installed Microsoft Certificate Service, do not install the Autoenrollment server on the same machine.
- If you install your RA certificate as a P12/PFX file (not recommended), you must install OpenSSL.

  See "Obtaining the RA Certificate".

- The user configuring and running processes on the Autoenrollment server machine requires the appropriate permissions to the Active Directory. Typically, the Enterprise Administrator group has the required permissions.

  NOTE: DigiCert recommends that you create a group with these permissions and assign all administrators who need access to the Active Directory to this group (alternatively, this user can be a member of the Enterprise Administrators group). For the purposes of the documentation, this user is called the AE Administrator.

3.1.2 Supported Windows Topologies

Autoenrollment server is supported on the following windows topologies:

- Single Forest with Single Domain
- Single Forest with Multiple Domains
- Multiple Forest with Single Domain in each
- Multiple Forests with Multiple Domains in each

For sample steps followed to create trust between forests in QA environment, refer: KB article.

3.2 Required Software

If the server machine that runs the Autoenrollment installer has access to internet, it will acquire and install them. If not, you need to acquire the following from Microsoft and install them to the server machine before the installation of Autoenrollment installer.

- .NET Framework V4.7.1
- Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019 (x64)

3.3 Supported HSMs

Refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html for details.

3.4 Firewall Settings

See “Adapting the Firewall Settings”.

CHAPTER 3

4 Installing the Autoenrollment Server Software

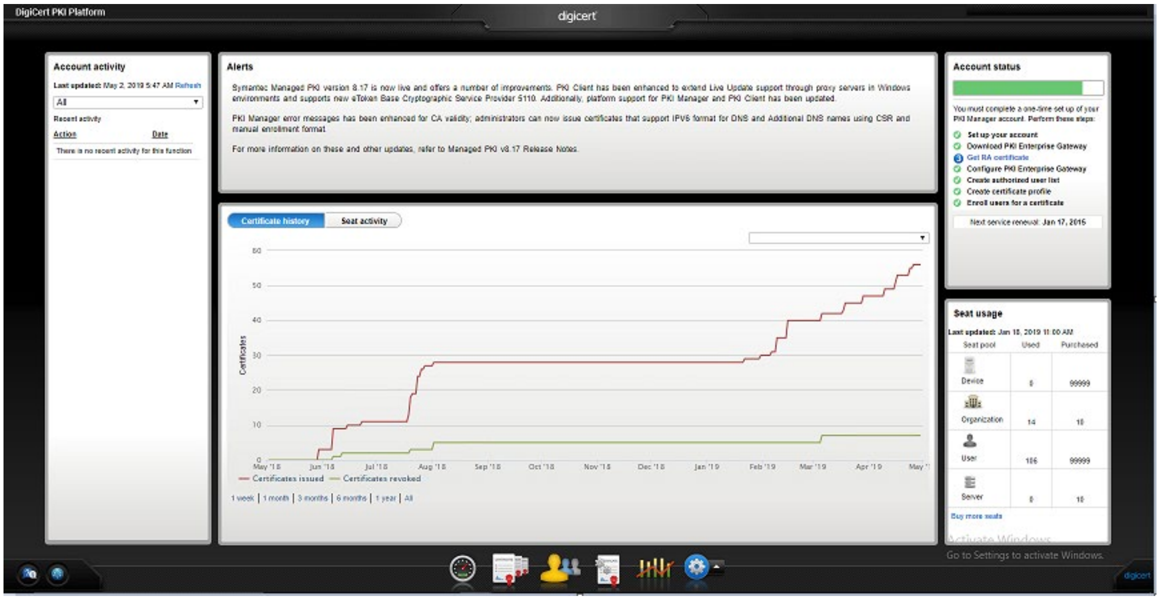
This chapter includes the following topics:

- Install the Autoenrollment Server
- Configuring DCOM Access Rights
- Setting the Autoenrollment Permissions
- Adapting the Firewall Settings
- Setting the Group Policies
- Adding the Certificate Template Snap-In
- Allow Publishing to Active Directory
- Uninstall the Autoenrollment Server

4.1 Install the Autoenrollment Server

To install the Autoenrollment Server, perform the following steps:

1. Access PKI-Manager as administrator, and then click at lower-left corner of the window.



Account activity

Last updated: May 2, 2019 5:47 AM Refresh

All ▾

Recent activity

Action	Date
There is no recent activity for this function	

Alerts

Symantec Managed PKI version 8.17 is now live and offers a number of improvements. PKI Client has been enhanced to extend Live Update support through proxy servers in Windows environments and supports new eToken Base Cryptographic Service Provider 5110. Additionally, platform support for PKI Manager and PKI Client has been updated.

PKI Manager error messages has been enhanced for CA validity; administrators can now issue certificates that support IPV6 format for DNS and Additional DNS names using CSR and manual enrollment format.

For more information on these and other updates, refer to Managed PKI v8.17 Release Notes.

Account status

You must complete a one-time set up of your PKI Manager account. Perform these steps:

- ✓ Set up your account
- ✓ Download PKI Enterprise Gateway
- 3 Get RA certificate
- ✓ Configure PKI Enterprise Gateway
- ✓ Create authorized user list
- ✓ Create certificate profile
- ✓ Enroll users for a certificate

Next service renewal: Jan 17, 2016

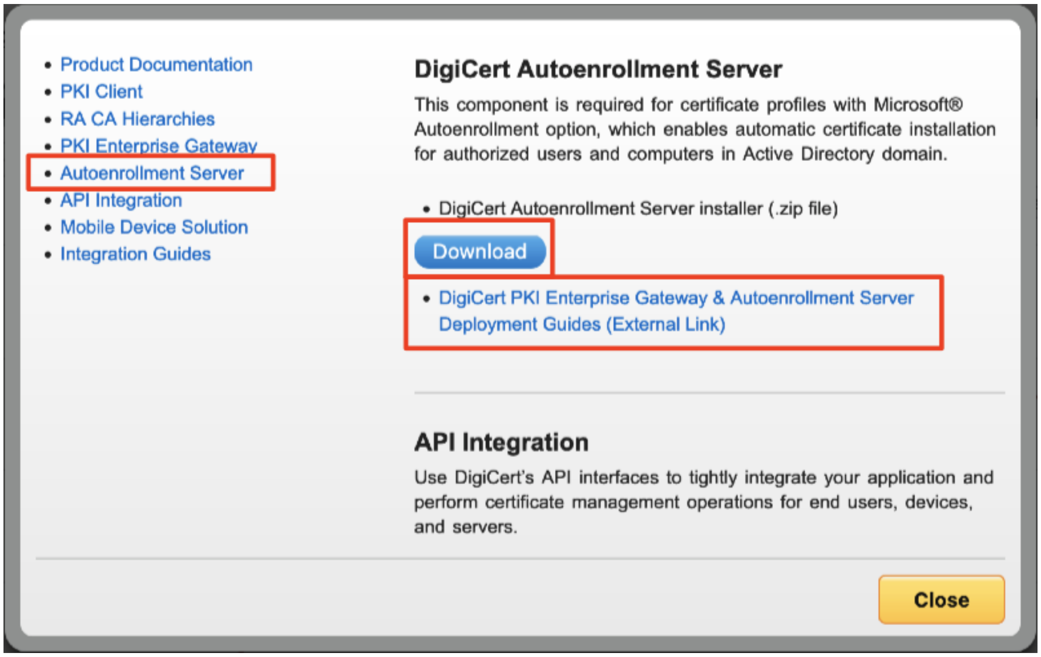
Seat usage

Last updated: Jan 18, 2019 11:00 AM

Seat pool	Used	Purchased
Device	0	99999
Organization	14	10
User	106	99999
Server	0	10

Buy more seats

2. Click **Autoenrollment Server** and click **Download** installer package (digicert-pki-aes-<version>.zip). The link "DigiCert PKI Enterprise Gateway & Autoenrollment Server Deployment Guides (External Link)" will take you to DigiCert hosted web page where this this guide can be downloaded.



- Product Documentation
- PKI Client
- RA CA Hierarchies
- PKI Enterprise Gateway
- Autoenrollment Server
- API Integration
- Mobile Device Solution
- Integration Guides

DigiCert Autoenrollment Server

This component is required for certificate profiles with Microsoft® Autoenrollment option, which enables automatic certificate installation for authorized users and computers in Active Directory domain.

- DigiCert Autoenrollment Server installer (.zip file)

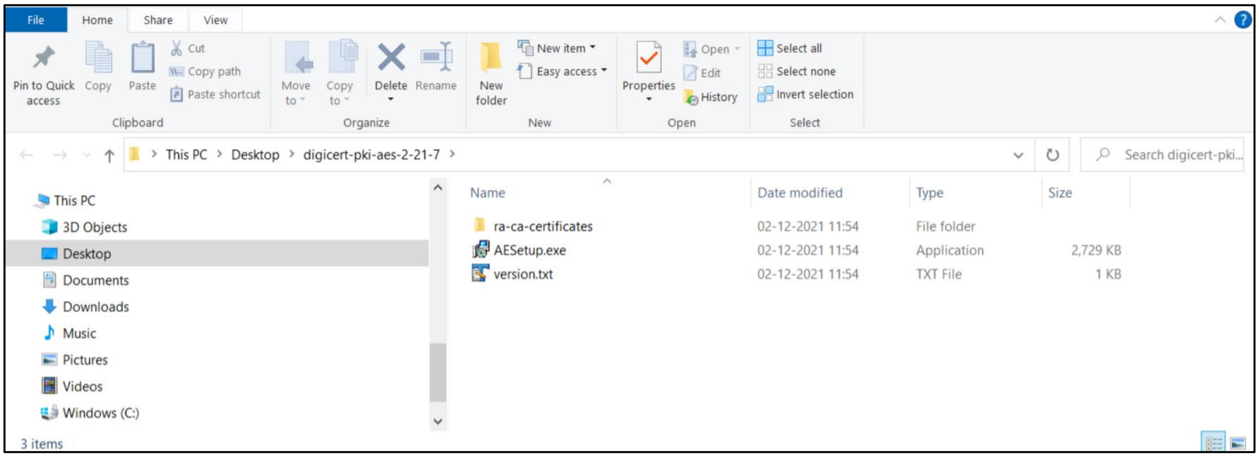
Download

- DigiCert PKI Enterprise Gateway & Autoenrollment Server Deployment Guides (External Link)

API Integration

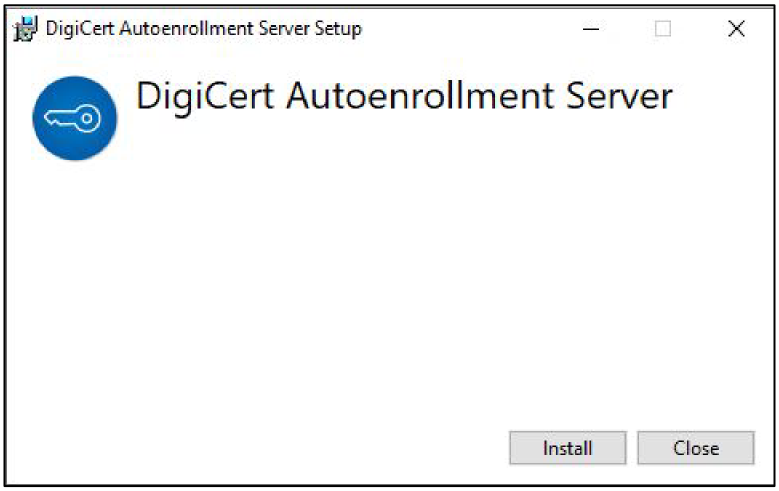
Use DigiCert's API interfaces to tightly integrate your application and perform certificate management operations for end users, devices, and servers.

3. Extract the installer package to your preferred destination.



Name	Date modified	Type	Size
ra-ca-certificates	02-12-2021 11:54	File folder	
AESetup.exe	02-12-2021 11:54	Application	2,729 KB
version.txt	02-12-2021 11:54	TXT File	1 KB

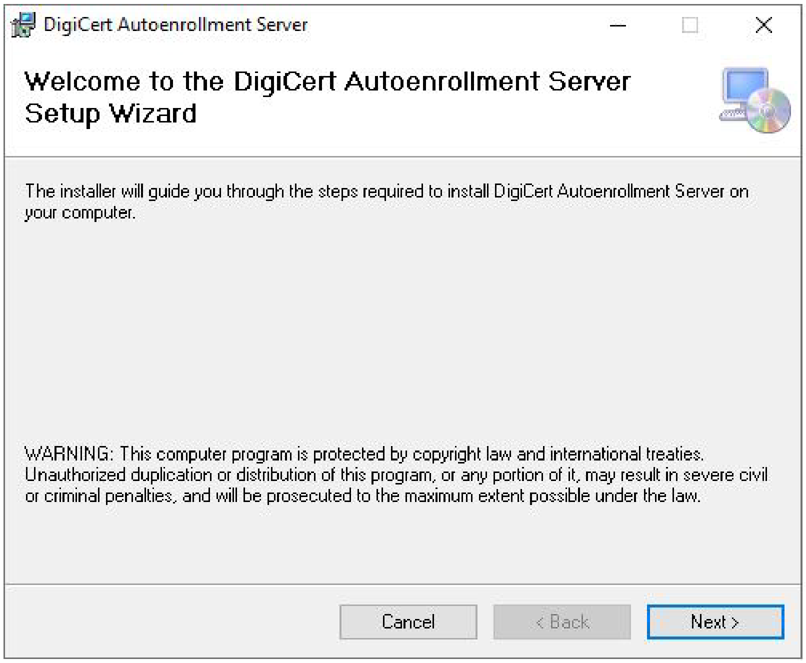
4. Launch "**AESetup.exe**" as administrator (Local Admin), and then click **Install**.


DigiCert Autoenrollment Server Setup
DigiCert Autoenrollment Server
Install
Close

NOTE:

- "Enterprise Admin" is not required during installation.
- If there is no internet access, install the "Required Software" before you launch **AESetup.exe**.

5. Click **Next**.

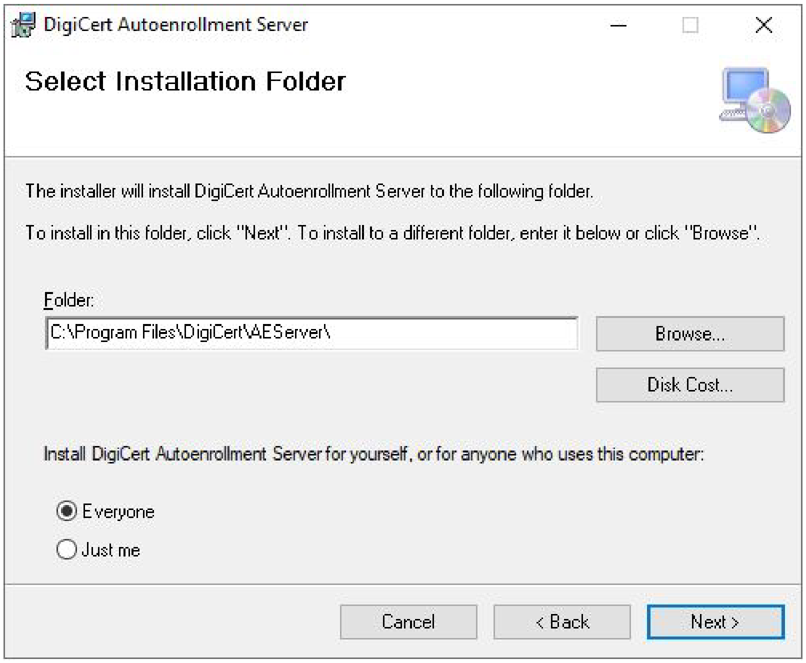


Welcome to the DigiCert Autoenrollment Server Setup Wizard

The installer will guide you through the steps required to install DigiCert Autoenrollment Server on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

6. Click **Browse** to select the installation folder, and then click **Next**.



DigiCert Autoenrollment Server

Select Installation Folder

The installer will install DigiCert Autoenrollment Server to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\DigiCert\AEServer\

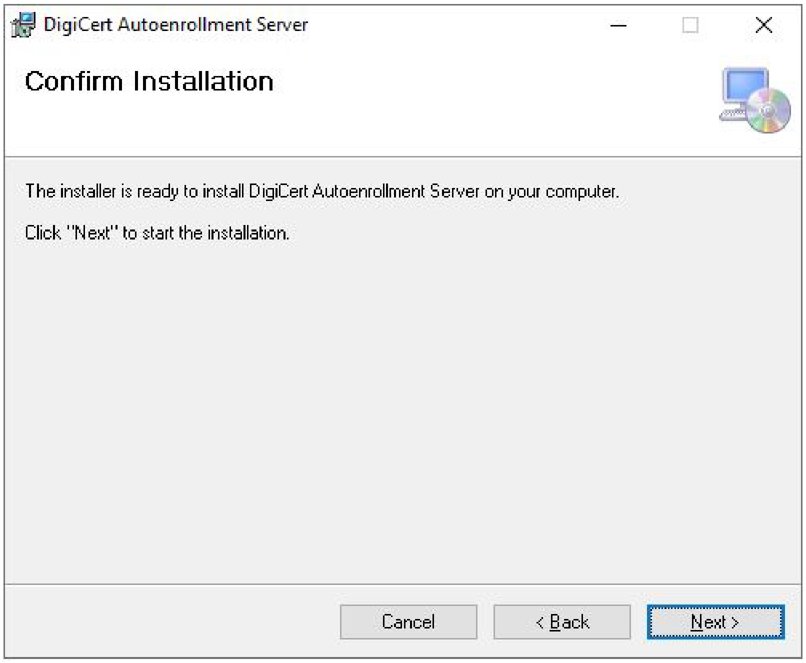
Install DigiCert Autoenrollment Server for yourself, or for anyone who uses this computer:

● Everyone

○ Just me

NOTE: The default location of the installer folder is "C:\Program Files\DigiCert\AEServer\".

7. Click **Next**.



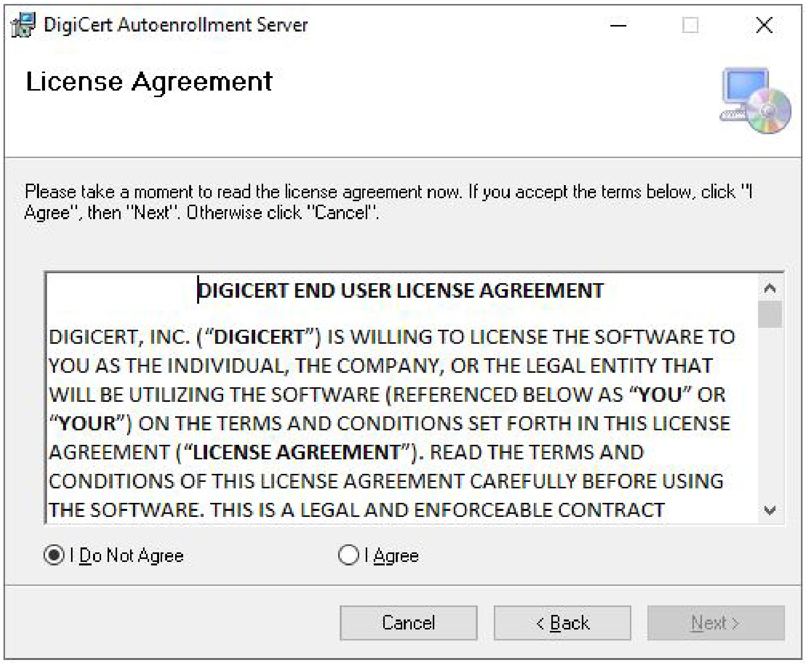
DigiCert Autoenrollment Server

Confirm Installation

The installer is ready to install DigiCert Autoenrollment Server on your computer.

Click "Next" to start the installation.

8. Click **I Agree** on the **License Agreement** window, and the click **Next**.



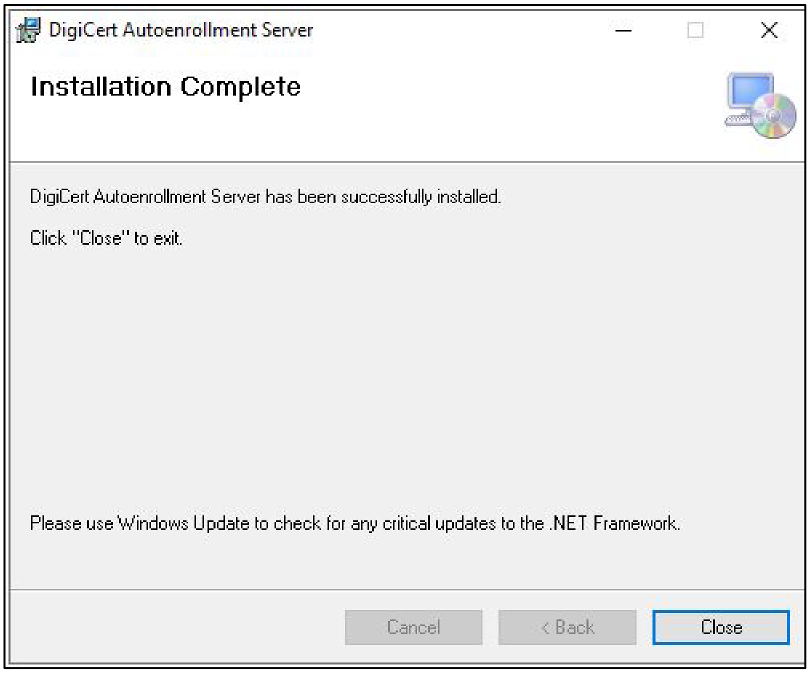
Please take a moment to read the license agreement now. If you accept the terms below, click "I Agree", then "Next". Otherwise click "Cancel".

DIGICERT END USER LICENSE AGREEMENT

DIGICERT, INC. ("**DIGICERT**") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "**YOU**" OR "**YOUR**") ON THE TERMS AND CONDITIONS SET FORTH IN THIS LICENSE AGREEMENT ("**LICENSE AGREEMENT**"). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT

● I Do Not Agree ○ I Agree

9. Click **Close**.



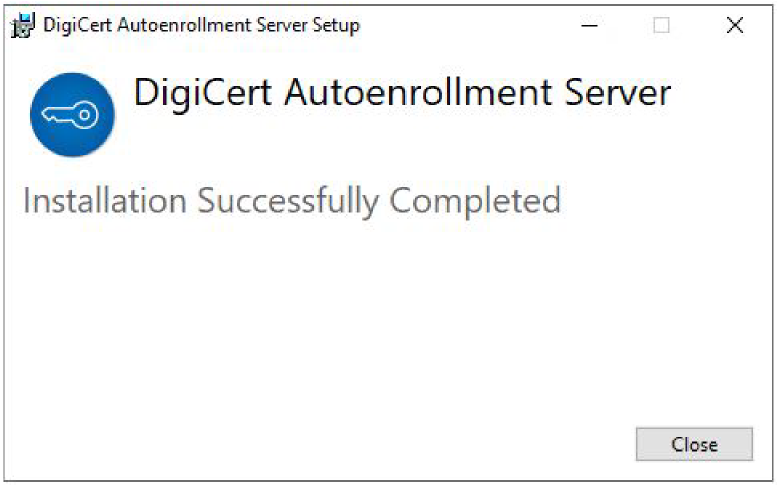
DigiCert Autoenrollment Server has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

NOTE: This window will appear only when installation is successfully completed.

10. Click **Close**.



DigiCert Autoenrollment Server Setup

DigiCert Autoenrollment Server

Installation Successfully Completed

4.2 Configuring DCOM Access Rights

The Autoenrollment server is invoked by using the Distributed Component Object Model (DCOM). It is important to ensure that Microsoft Windows is configured for local DCOM access for system processes and accounts with administrative privileges.

On the **My Computer > Default Properties** tab, select the **Enable Distributed COM** check box. Then, use certutil to ping "config", and autoenrollment works fine. If you do not enable DCOM, then autoenrollment fails with the error "RPC server unavailable."

The usage of certutil command is as follows:

- To find the value of the config attribute, run the following command:

  C:> certutil -dump
  The command will list name-value pairs including "config". For example, `‘SERVER\my ca’`. You must ignore the single quotes while copying the value.

- In the config file, enter the name-value pair value within double quotes if there are any spaces:

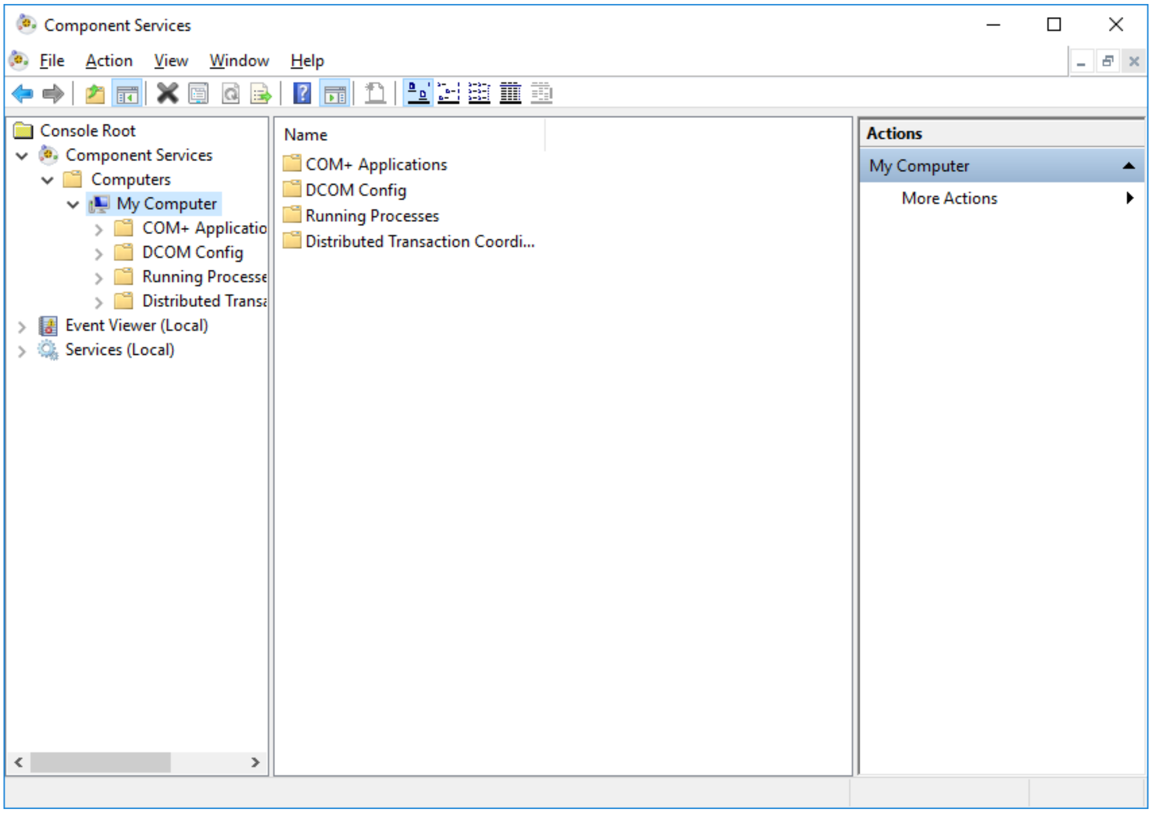
  C:> certutil -ping -config "SERVER\my ca"
  For example, the output will be displayed as follows:

```
Connecting to SERVER\my ca Server "<serverName>" ICertRequest2 interface is
alive CertUtil: -ping command completed successfully
```

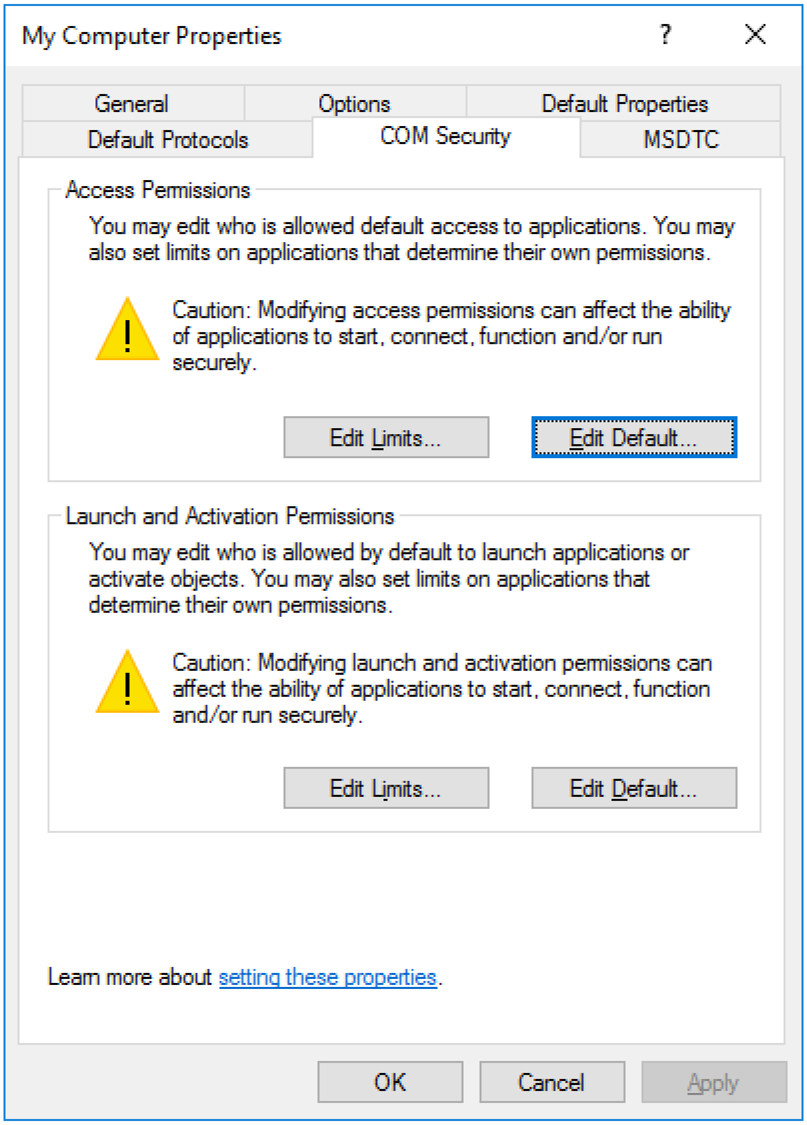
If you want to use the autoenrollment services, you need to configure the system to allow global DCOM object access. You must also allow remote DCOM access to use the Autoenrollment server across multiple machines.

To Configure DCOM access rights as the domain administrator on the machine on which the Autoenrollment server is installed

1. In the **Administrative Tool > Component Services**, click **Component Services** in the left pane, and expand the tree view to the left of **Computers**.



2. Right-click **My Computer** and select **Properties**.



My Computer Properties

Access Permissions

You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

Launch and Activation Permissions

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

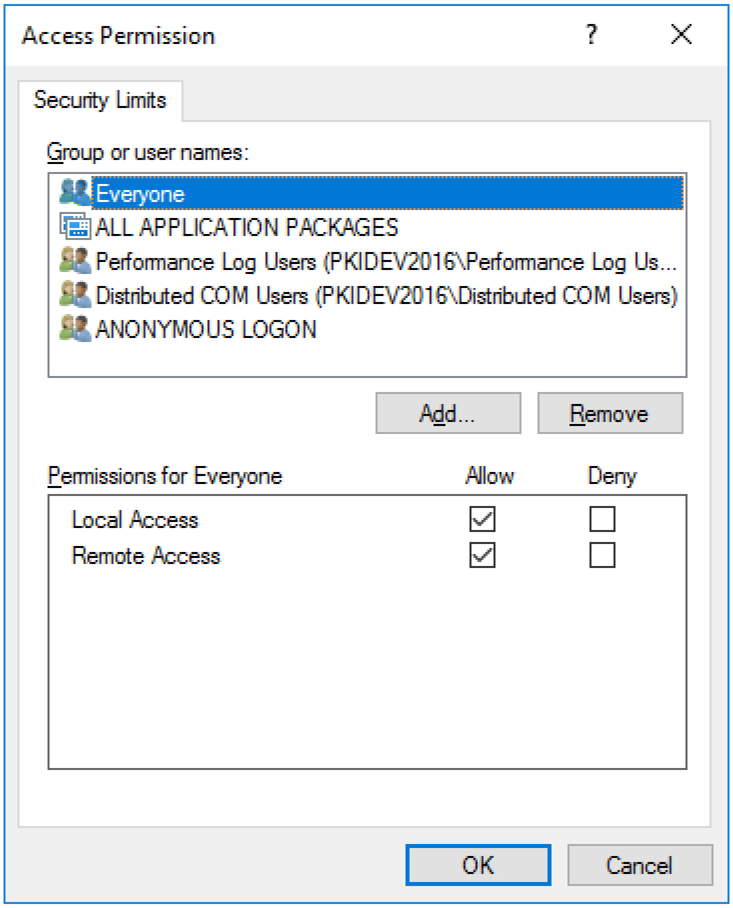
Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Learn more about setting these properties.

3. Select the **COM Security** tab.
4. Modify the access permissions:

- In the **Access Permissions** dialog, click **Edit Limits**.
- Set **Configure Domain Computers: Allow Local and Remote Access**.
- Set **Configure Domain Controllers: Allow Local and Remote Access**.
- Set **Configure Domain Users: Allow Local and Remote Access**.

If the groups for which you want to configure access permissions are not listed, you must add them (click **Add** and enter the group names). If you are not able to add the desired groups, you may need to add the object type by clicking **Object Types**.



Group or user names:

- Everyone
- ALL APPLICATION PACKAGES
- Performance Log Users (PKIDEV2016\Performance Log Us...
- Distributed COM Users (PKIDEV2016\Distributed COM Users)
- ANONYMOUS LOGON

Permissions for Everyone	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

5. Perform the following steps to adjust the launch and the activation permissions:

   - Click **Edit Limits** under the **Launch and Activation Permissions** group.
   - Set **Configure Domain Computers: Activate Local Activation and Remote Activation**, and clear the **Local Launch and Remote Launch** check box.
   - Set **Configure Domain Controllers: Activate Local Activation and Remote Activation**, and clear the **Local Launch and Remote Launch** check box.
   - Set **Configure Domain Users: Activate Local Activation and Remote Activation**, and clear the **Local Launch and Remote Launch** check box.

NOTE: You can add Active Directory users or groups that are authorized for configuring client certificate profile. Once added, assign them appropriate permissions similar to Domain Computers.

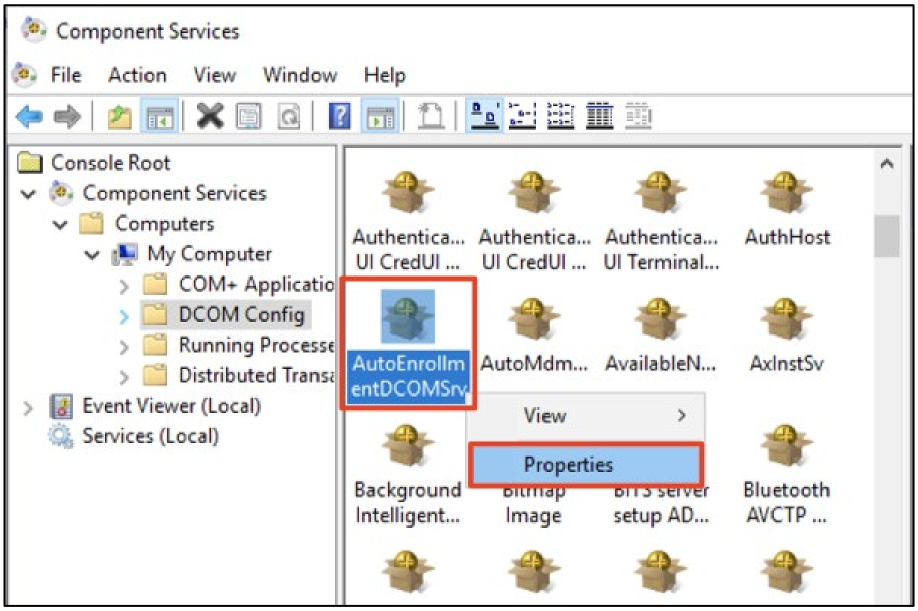
4.3 Setting the Autoenrollment Permissions

You need to set the permissions to allow the Autoenrollment server to perform autoenrollment

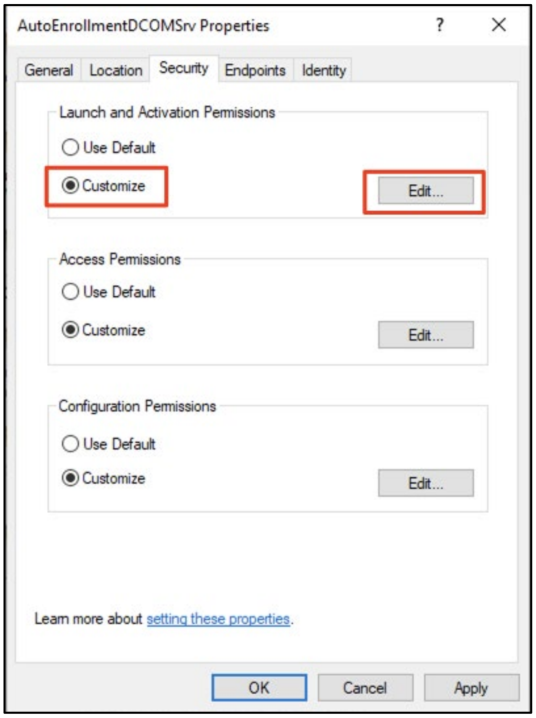
NOTE: Any time that you update or reinstall the Autoenrollment server, you must re-apply the changes as described in this section.

To set autoenrollment permissions as the domain administrator,

1. Click **Start** > **Administrative Tools** > **Component services** and navigate to **DCOM Config**.
2. In the right pane, right-click **AutoEnrollmentDCOMSrv**. Select **Properties**.



3. Select the **Security** tab.
4. Under **Launch and Activation Permissions**, select **Customize** and click **Edit**.


AutoEnrollmentDCOMSrv Properties

Launch and Activation Permissions

○ Use Default

● Customize

Access Permissions

○ Use Default

● Customize

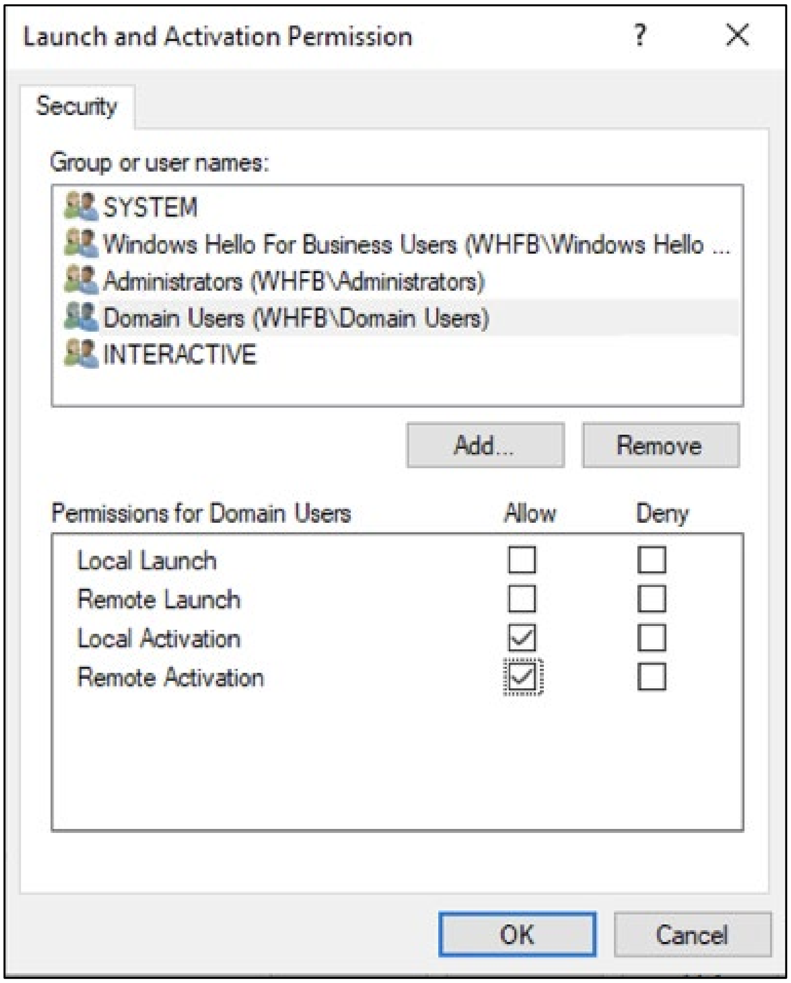
Configuration Permissions

○ Use Default

● Customize

Learn more about setting these properties.

5. Select the **Local Activation** and **Remote Activation** check box and clear the **Local Launch** and **Remote Launch** check box for each group of users and computers that you want to be able to enroll for certificates.



Launch and Activation Permission

Security

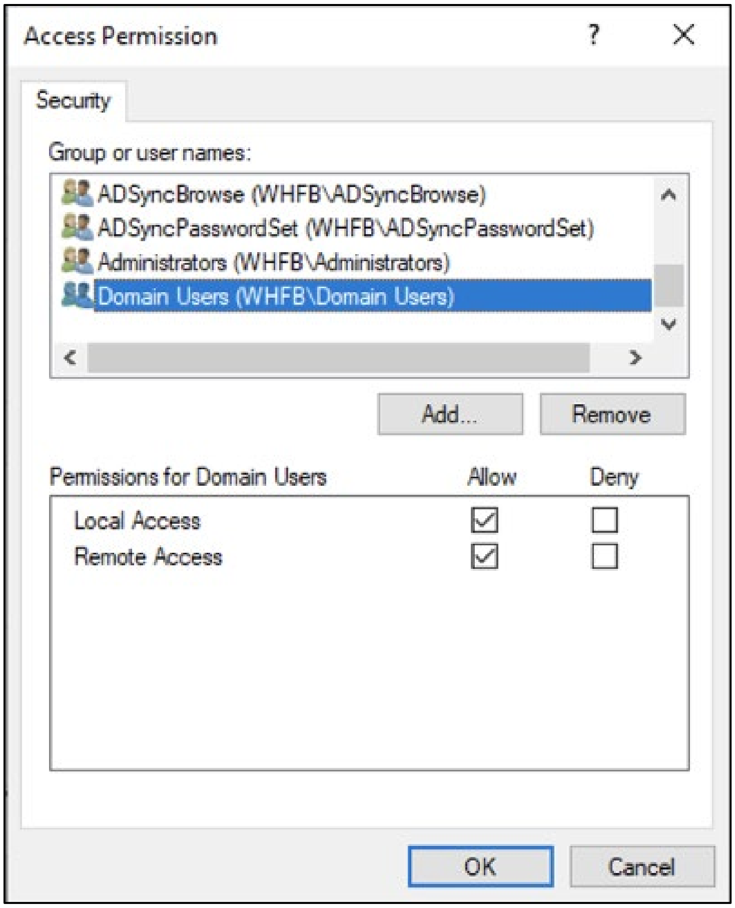
Group or user names:

- SYSTEM
- Windows Hello For Business Users (WHFB\Windows Hello ...
- Administrators (WHFB\Administrators)
- Domain Users (WHFB\Domain Users)
- INTERACTIVE

Permissions for Domain Users	Allow	Deny
Local Launch	□	□
Remote Launch	□	□
Local Activation	☑	□
Remote Activation	☑	□

If the groups for which you want to configure launch and access permissions are not listed, you must add them (click **Add** and enter the group names).
If you have no special security requirements, you may want to grant local and remote activation to the group **Everyone** and remove the other trustees from the list.

6. Under **Access Permissions**, select **Customize** and click **Edit**.
7. Check **Local Access** and **Remote Access** for each group of users and computers that you want to enroll for certificates.



Group or user names:

- ADSyncBrowse (WHFB\ADSyncBrowse)
- ADSyncPasswordSet (WHFB\ADSyncPasswordSet)
- Administrators (WHFB\Administrators)
- Domain Users (WHFB\Domain Users)

Permissions for Domain Users	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

If the desired groups are not listed, click **Add** and supply their names in the dialog box. If you have no special security requirements, you may want to grant local and remote access to the group **Everyone** and remove the other trustees from the list.

8. Click **OK** to close the dialog and apply the changes.

4.4 Adapting the Firewall Settings

To enable an exception on the firewall of the computer on which the Autoenrollment server runs

1. Open **Start** > **Control Panel** > **System and Security** > **Windows Firewall**.
2. Select **Allow a program or feature through Windows Firewall**.
3. Select **Allow another program**.
4. Click **Browse**.
5. Navigate to the directory where you installed the Autoenrollment server and select the `AutoEnrollmentDCOMSrv.exe` file.
6. Click **Add**.

4.5 Setting the Group Policies

In addition to assigning groups access to templates, you must set autoenrollment permissions for the groups to which your users and computers belong. For example, you must configure the permission settings for the respective domain or user group to enable the autoenrollment mechanism for its members.

To set up group policies as the domain administrator on the domain controller,

1. Click **Start > Administrative Tools > Group Policy Management** and navigate to the relevant Group Policy Object (GPO). Right-click the object and select **Edit**.
2. Access the relevant GPO settings by double-clicking **Certificate Services Client - Auto-Enrollment** under **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
3. You must configure the following options to enable certificate management and publishing in Active Directory:

- Enable **Configuration Model**.
- Select **Renew expired certificates, update pending certificates, and remove revoked certificates**.
- Select **Update certificates that use certificate templates**.

Repeat these steps for any additional site, domain, or OU object for which you want to enable autoenrollment.

Repeat this procedure under **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies** if you plan to autoenroll Computer certificates, such as domain controller certificates.

NOTE: GPOs are valid within a single domain. If you have set up a forest domain structure you need to copy the GPO to every domain controller to which the GPO should apply.

4.6 Adding the Certificate Template Snap-In

You must install the Certificate Template Snap-In for mmc to edit certificate template permissions.

To add the certificate template snap-on as a domain administrator

1. Select **Start > Administrative Tools > Server Manager**, right click **Server Manager** and choose **Add Features**.
2. Open **Remote Server Administration Tools > Role Administration Tools > Active Directory Certificate Services Tools** and select **Certification Authority Tools**.
3. Click **Next**, and then click **Install**.

4.7 Allow Publishing to Active Directory

The computer that runs the Autoenrollment server must be a member of the Active Directory group Cert Publishers for all domains, including the root domain. This allows the computer to publish newly issued certificates to the Active Directory.

To make the server's computer a member of the Cert Publishers group on the machines which have the AD Domain Services role enabled

1. Log on as the AE Administrator or as another user who is a member of the Enterprise Administrator group.
2. Select **Administrative Tools > Active Directory Users and Computers**.
3. Expand the tree view on the left to display your domain and click **Users**.
4. Double-click the **Cert Publishers** group in the right panel and select the **Members** tab.
5. Click **Add** and add the computer running the server.

   You may have to add **Computers** to the **Object Types** to search for the computer's name.

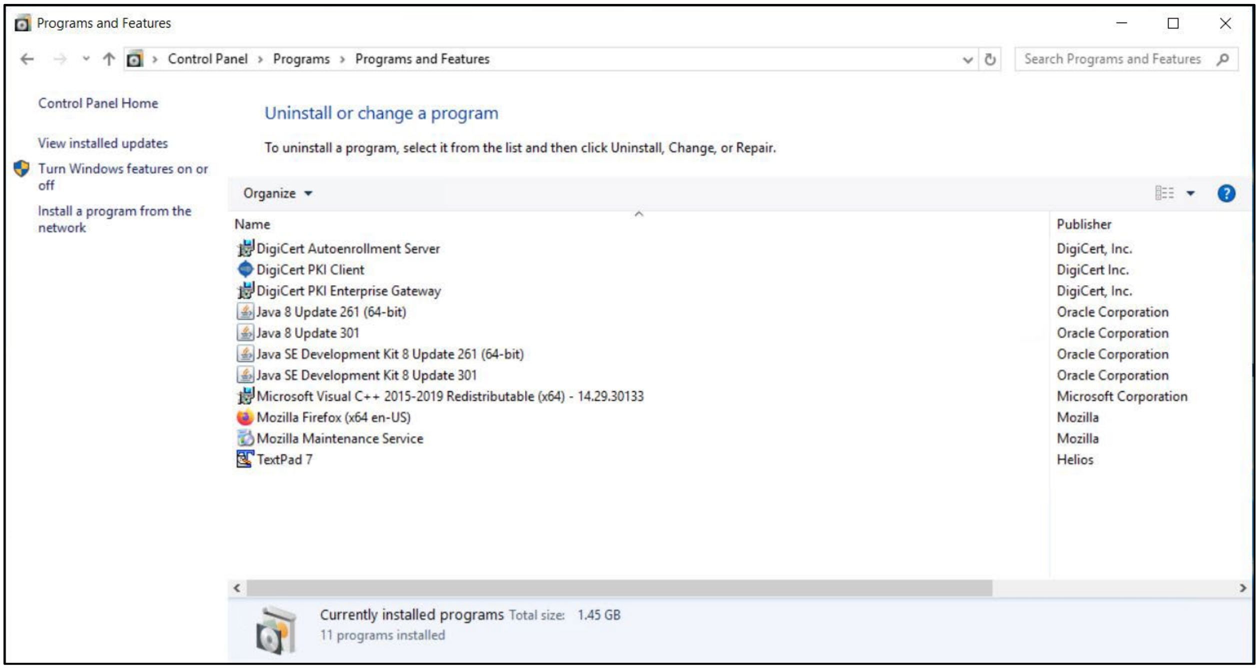
Repeat these steps for the Cert Publishers group of every domain in your forest, including the root domain. For the new group membership to take effect, `run gpupdate /force` from the machine where the Autoenrollment server is installed.

4.8 Uninstall the Autoenrollment Server

To uninstall the Autoenrollment Server, perform the following steps:

1. Go to **Control Panel > Program and Features**.

   Right-click **Autoenrollment Server**, and then click **Uninstall**.


Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize

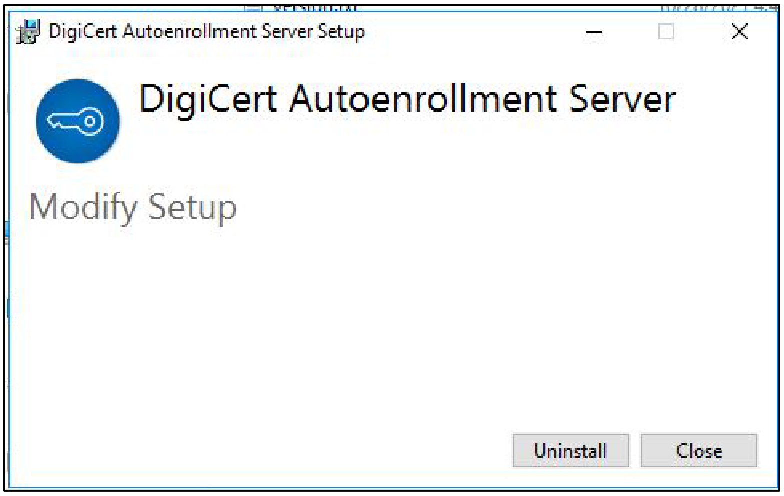
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

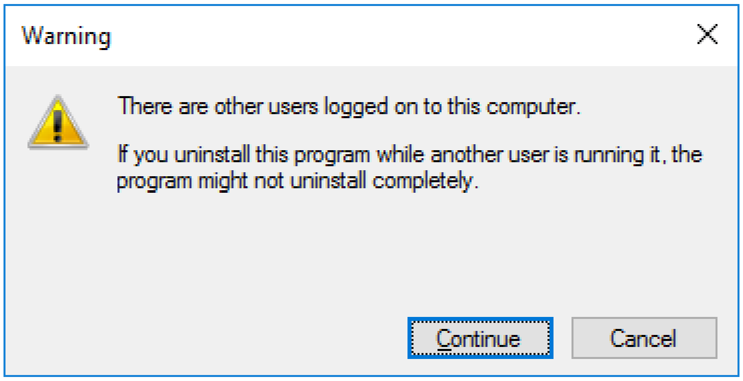
Name	Publisher
DigiCert Autoenrollment Server	DigiCert, Inc.
DigiCert PKI Client	DigiCert Inc.
DigiCert PKI Enterprise Gateway	DigiCert, Inc.
Java 8 Update 261 (64-bit)	Oracle Corporation
Java 8 Update 301	Oracle Corporation
Java SE Development Kit 8 Update 261 (64-bit)	Oracle Corporation
Java SE Development Kit 8 Update 301	Oracle Corporation
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30133	Microsoft Corporation
Mozilla Firefox (x64 en-US)	Mozilla
Mozilla Maintenance Service	Mozilla
TextPad 7	Helios

Currently installed programs Total size: 1.45 GB
11 programs installed

2. Click **Uninstall**.


DigiCert Autoenrollment Server Setup
DigiCert Autoenrollment Server
Modify Setup
Uninstall
Close

NOTE: If other users are logged on to this computer. Click **Continue** if you want to enforce the uninstallation.

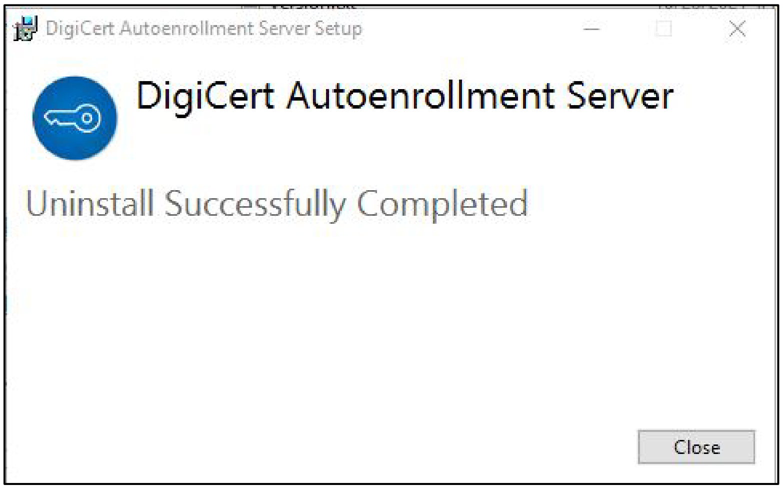


Warning

There are other users logged on to this computer.

If you uninstall this program while another user is running it, the program might not uninstall completely.

3. Click **Close**.



DigiCert Autoenrollment Server Setup
DigiCert Autoenrollment Server

Uninstall Successfully Completed

CHAPTER 4

5 Configuring the Autoenrollment Server

This chapter includes the following topics:

5.1 About the Configuration of the Autoenrollment Server

After you install the software and setting up autoenrollment permissions, you need to configure the DigiCert Autoenrollment Server for your enterprise. This chapter guides you through the following steps to configure your new Autoenrollment server.

- Obtaining the RA certificate
- Setting the configuration utility
- Importing the autoenrollment configuration file

5.2 Obtaining the RA Certificate

You need a Registration Authority (RA) certificate to secure communications and identify yourself to the DigiCert Certificate Authority. The RA certificate you obtain for PKI Enterprise Gateway is also valid for autoenrollment. You do not need to obtain a separate RA certificate.

You have the option of storing your RA certificate in a software key store or on a hardware security module (HSM). The method that you choose in storing your RA certificate has implications on how you obtain your RA certificate.

NOTE: DigiCert recommends the use of a hardware security module to ensure the security of the RA certificate and its corresponding private key. You must secure your RA certificate and private key. Anyone who has access to the RA certificate and private key can act on your organization's behalf.

- You may want to familiarize yourself with procedures that describe how to obtain and install an RA certificate if you store your RA certificate on an HSM.

  See “Obtaining an RA Certificate to Store in an HSM”.

- You may want to familiarize yourself with procedures on how to obtain an RA certificate if you store your RA certificate as a software P12 or PFX file.

  See "Obtaining an RA Certificate as a Software File".

5.2.1 Obtaining an RA Certificate to Store in an HSM

Refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html for details.

The root and issuing CAs for the RA certificate can be found in the web page at https://knowledge.digicert.com/solution/ca-hierarchies-for-production-and-test-drive-ra-certificates.html. You must import these CAs as trusted root CAs into the Microsoft Certificate Store. This ensures that the RA certificate that you install is correctly trusted.

1. On the machine on which you installed the Autoenrollment server, generate a CSR in `.pem` format:

   - Create a text file named `newRAreq-csp.inf` that contains the following information.

     ```
     [NewRequest]
     KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
     Providertype = 1
     RequestType = PKCS10
     ProviderName = <PROVIDER-NAME>
     Subject = "C=DE,O=Your Org, CN=Registration Authority"
     KeyContainer = "racertificate-1"
     MachineKeySet = true
     HashAlgorithm = sha256
     KeyAlgorithm = RSA
     KeyLength = 2048
     ```

     If the `<PROVIDER-NAME>` is not clear, refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html.

   - Generate a PKSC10 request using the command:

     ```
     certreq -new newRAreq-csp.inf ra-request.req
     ```

2. Copy the created CSR file (`ra-request.req`) to the machine that has access to the PKI Manager. Get an RA certificate from PKI Manager using this CSR file. In PKI Manager, click the **Tasks** icon and select **Get an RA certificate**.
3. Import the new certificate into your local machine's CSP. To do this:

   - Open mmc and click on **Certificates (Local Computer)** > **Personal** > **Certificates**.
   - Right click on **Certificates** and select **All Tasks** > **Import**.
   - Browse for the `.p7b` certificate file downloaded from PKI Manager.
   - Complete the import.

4. Make sure that the RA certificate appears in the Certificates list, and then double click the certificate and make sure that the following message appears:

```
You have a private key that corresponds to this certificate
```

Importing CAs as trusted root CAs

Copy the root and issuing CAs for the RA certificate from https://knowledge.digicert.com/solution/ca-hierarchies-for-production-and-test-drive-ra-certificates.html to a directory on the local machine.

1. Open Microsoft Management Console (mmc) and add the Certificates snap-in for the local computer. To do this select **Add Snap in for Certificates**, select **Computer Account**, and click **OK**.
2. Click **Certificates > Local Computer > Trusted Root Certification Authorities > Certificates**.
3. Click **All Tasks > Import**.
4. Select the root CA you copied to your local machine at the beginning of this step and click **OK**.
5. Click **Certificates > Local Computer > Trusted Intermediate Certification Authorities > Certificates**.
6. Click **All Tasks > Import**.
7. Select the issuing CA you copied to your local machine at the beginning of this step and click **OK**.

Continue to Step 2 of "To obtain an RA Certificate to store in an HSM".

NOTE: The RA hierarchy will be updated in the Knowledge Base article at https://knowledge.digicert.com/solution/ca-hierarchies-for-production-and-test-drive-ra-certificates.html when RA hierarchy gets updated. Make sure you download and import the latest chain for your RA certificate.

5.2.2 Obtaining an RA Certificate as a Software File

If you store your RA certificate in a software P12 or PFX file, you must generate and convert your RA certificate. You will need to install OpenSSL.

To obtain an RA certificate as a software file

1. On the machine on which you installed the Autoenrollment server, run the following command to generate a CSR.

   ```
   openssl req -out ra-request.req -new -newkey rsa:2048 -nodes -keyout ra-
   request.key
   ```

2. Copy the created CSR file (`ra-request.req`) to a machine that has access to the PKI Manager
3. Get an RA certificate from PKI Manager using this CSR file. In PKI Manager, click the **Tasks** icon and select **Get an RA certificate**.
4. Download the PKCS7 file from PKI Manager and save it to the directory where you created the CSR as listed in Step 2.
5. Convert the PKCS7 received from PKI Manager:

   ```
   openssl pkcs7 -print_certs -in <certificate downloaded from PKI Manager> -out
   RAcertificate.pem
   ```

6. Run the following commands from the directory where you created the CSR as listed in "To obtain an RA Certificate to store in an HSM".

   ```
   openssl pkcs12 -export -out myRA.pfx -inkey < Private Key File Name> -in
   RAcertificate.pem -passout pass:password
   ```

   These commands output your RA certificate to the file myRA.pfx. You need this file and password when you set the RA certificate in the Autoenrollment Config utility.
   See “Setting the Autoenrollment Configuration Utility”.

5.3 Setting the Autoenrollment Configuration Utility

Use the Autoenrollment Config utility to set the Autoenrollment server configuration values. You must have administrator rights to use this utility to write data to Active Directory.

The Autoenrollment server runs as a Windows service. You must set the configuration settings in the utility before you start the Autoenrollment service.

To set the Autoenrollment Configuration utility

1. Log on to the computer as AE Administrator or as another user who is a member of the Enterprise Administrators group.

   You need write access to `CN=Public Key Services,CN=Services,CN=Configuration` in the Configuration partition of Active Directory.

2. Access the machine on which you have installed the Autoenrollment Server.
3. On the **Start** menu, click **All Programs > DigiCert > AutoEnrollmentServer > Autoenrollment Configuration**.
   (AutoEnrollmentServer directory will only appear in classic Start Menu).
4. Complete or review the following settings:

   - Click **Choose** to set the RA certificate and select your RA certificate from the drop-down list. For HSMs, leave the PIN field empty. Optionally, you can use the software certificates that are stored as a P12 or as a PFX file. This is for test or demonstration purposes and is not recommended for production systems.
   - The validity of the RA certificate is displayed. You can also check the RA certificate by clicking **View**.
   - The **API Key** is pre-populated with default key. If API Key was provided with RA certificate, enter that value. Otherwise leave it as is. The Autoenrollment server uses this key for two factor authorization to submit requests to DigiCert.
   - The **CA Server Name** and **CA Server Port** are pre-populated with the URL and the port number of the DigiCert PKI Platform Web Service. Do not change these values. The Autoenrollment server uses these values to submit requests to DigiCert.
   - Verify the location and contents of the **Log Properties** file.
     This file defines the logging configuration such as log file path and log level. The default is specified as **logger.properties** in the installation directory of Autoenrollment Server. Click **Browse** to choose a different log properties file. Click **View** to check and modify the log properties file contents. Refer to section "Log Properties Configuration Options" for details about the configuration.

5. Click **OK** to save the configuration settings.

   Do not start the service until after you import the autoenrollment configuration file from PKI Manager.
   See "Importing the Autoenrollment Configuration File".
   If you are connected to the internet through a proxy server, you may need to configure proxy settings. Since the DigiCert Autoenrollment Server runs as a service, it is not aware of proxy settings.

6. Use the netsh utility with command `winhttp set proxy` to configure proxy settings.

5.3.1 Additional Configuration Utility Options

You can perform the following additional operations with the Autoenrollment Config utility:

- Service state indicates whether the Autoenrollment service is currently running or not. You must manually start the service after initial configuration.

- Start/Stop Service allows you to start or stop the Autoenrollment service. You must restart the Autoenrollment service whenever you make changes to the configuration settings using this utility.
- Pending Requests in Queue: This indicates the number of pending certificate requests. Click Refresh to update the number.
- Cancel enables you to exit the utility without saving the configuration.

5.4 Log Properties Configuration Options

This section includes information about configuring the log properties file. You can skip this section if there is no need to change the logging configuration.

The log properties file is specified using the Autoenrollment Configuration utility Log Properties setting. Following shows the contents of the default properties file:

```
# A line starting with # is a comment and ignored.
# Define with log-level (DEBUG, INFO, WARN, or ERROR) and appender name
log4cpp.rootCategory=INFO, DAILY
# Configured appender type
log4cpp.appender.DAILY=DailyRollingFileAppender
# File name and path
# AE Server requires write permission, and directory must exist
log4cpp.appender.DAILY.fileName=C:\Program Files\DigiCert\AEServer\logs\AEServer.log
# Max days to keep the old log files
log4cpp.appender.DAILY.maxDaysKeep=30
# Output pattern (see http://log4cpp.sourceforge.net/#faq for format details)
log4cpp.appender.DAILY.layout=PatternLayout
log4cpp.appender.DAILY.layout.ConversionPattern=%d{%Y-%m-%d %H:%M:%S} %-5p [%t] %m%n
```

Table 4-4 shows the details about each property.

Table 4-4 Log Property Details

Property Key	Description
log4cpp.rootCategory	Specifies log level and name to use for the configuration. The value is in following format: `<log_level>, <logger_name>` • log_level describes the logging level. ○ This can be set to DEBUG, INFO, WARN, or ERROR, with DEBUG log level being the most verbose.

Property Key	Description
	○ Setting the level to **DEBUG** will increase the amount of log output significantly, so should be careful when using this in production environment. • **logger_name** describes the name of the configuration, which is also used in other property keys. This can be any value, but **DAILY** is used as default.
log4cpp.appender.<logger_name>	Specifies the type of log appender. Currently `DailyRollingFileAppender` and `SyslogAppender` are supported. Using `DailyRollingFileAppender` appender will allow the log file to rotate daily at 0 AM (local time) every day, creating a log file with name **<log_filename>.yyyy-MM-dd**. **Note**: Log file rotation occurs only when there is new log entry after 0 AM. Using `SyslogAppender` appender will allow the Autoenrollment server to dump log messages to the configured syslog server. See "Configuring Autoenrollment Server for Syslog" for more details about this appender.
log4cpp.appender.<logger_name>.fileName	Specifies the log file name with path. Default location will be `<installation directory>\AEServer.log`. This will change depending on where Autoenrollment Server was installed. **Notes**: • The log file directory must exist. • Autoenrollment service requires write permission for the file.
log4cpp.appender.<logger_name>.maxDaysKeep	Specifies the days to keep for the log files. The log entries exceeding the max days will be deleted from the file system.

Property Key	Description
log4cpp.appender.<logger_name>.layout	Specifies the log layout class. Currently only `PatternLayout` is supported.
log4cpp.appender.<logger_name>.ConversionPattern	Specifies the output format of the logs. See http://log4cpp.sourceforge.net/#faq for details about possible format characters for the custom log messages. The default log format is set as "<Date{yyyy-mm-dd}> <Time{hh:mm:ss}> <LogLevel> [<TheadID>] <LogMessage>". Example below: `2021-09-22 04:15:28 INFO [6176] Using CA backend at pki-ws.symauth.com:443`

Notes:

- Any modifications in the file contents will only become effective after restarting the Autoenrollment service.
- Line starting with # is ignored.

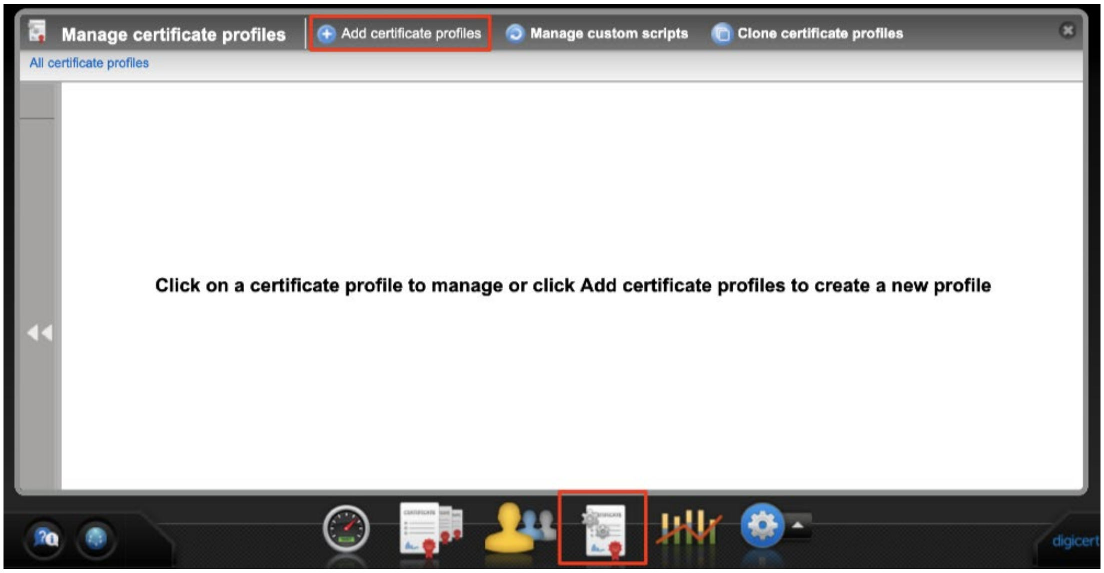
5.5 Creating Autoenrollment Certificate Profile

Once you have configured the RA certificate and prepared the configuration utility you will need to create a certificate profile in the PKI Manager.

To create a certificate profile:

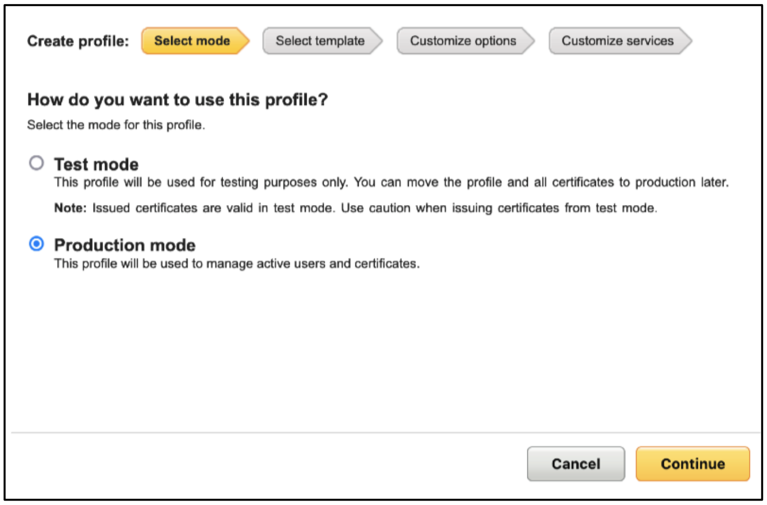
1. Login to PKI-Manager with your administrator certificate. The administrator needs **Certificate profile manager** role and at least **Manage profiles** permission to create certificate profiles.

2. Go to **Manage certificate profiles** page and click **Add certificate profiles** at the top menu.



Click on a certificate profile to manage or click Add certificate profiles to create a new profile

3. Select mode radio button and click **Continue**.



How do you want to use this profile?

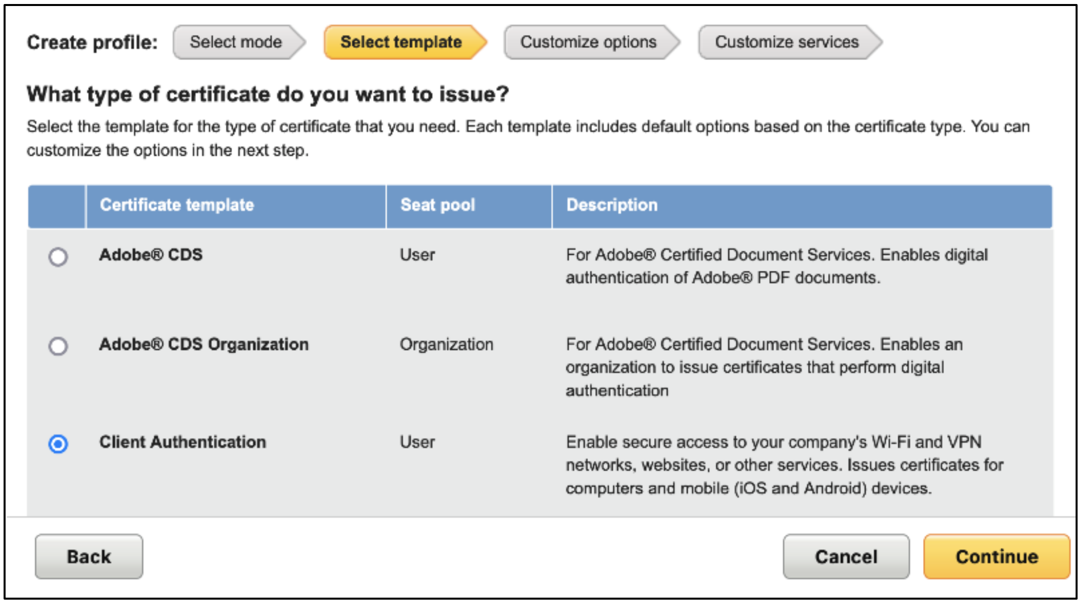
Select the mode for this profile.

○ **Test mode**
This profile will be used for testing purposes only. You can move the profile and all certificates to production later.
Note: Issued certificates are valid in test mode. Use caution when issuing certificates from test mode.

● **Production mode**
This profile will be used to manage active users and certificates.

a) Test mode - Mode for testing purpose
b) Production mode - Mode for daily usage

4. Select **Certificate template** from the list and click **Continue**. Example shows selecting **Client Authentication** certificate.

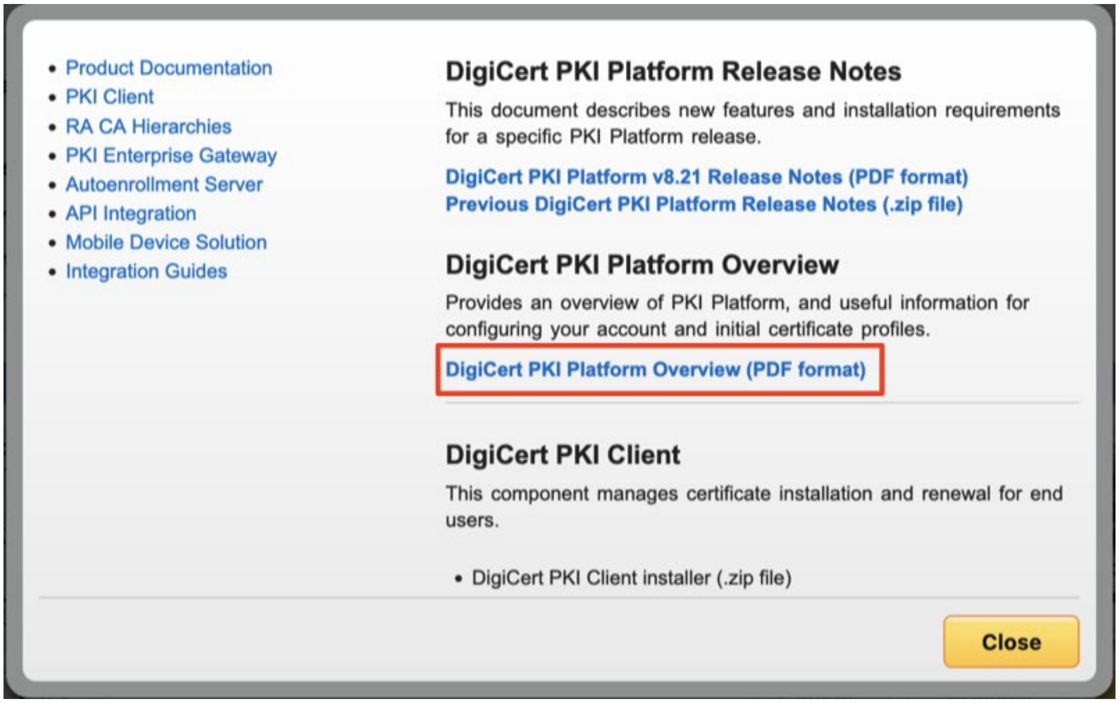


What type of certificate do you want to issue?

Select the template for the type of certificate that you need. Each template includes default options based on the certificate type. You can customize the options in the next step.

	Certificate template	Seat pool	Description
○	Adobe® CDS	User	For Adobe® Certified Document Services. Enables digital authentication of Adobe® PDF documents.
○	Adobe® CDS Organization	Organization	For Adobe® Certified Document Services. Enables an organization to issue certificates that perform digital authentication
●	Client Authentication	User	Enable secure access to your company's Wi-Fi and VPN networks, websites, or other services. Issues certificates for computers and mobile (iOS and Android) devices.

NOTE: For full list of available certificate profile templates, see document "*DigiCert® PKI Platform Overview*" section "*2.5.1 Available Certificate Profile Templates*". This document is downloadable from Resources section in the lower left corner of PKI Manager.



DigiCert PKI Platform Release Notes

This document describes new features and installation requirements for a specific PKI Platform release.

DigiCert PKI Platform v8.21 Release Notes (PDF format)
Previous DigiCert PKI Platform Release Notes (.zip file)

DigiCert PKI Platform Overview

Provides an overview of PKI Platform, and useful information for configuring your account and initial certificate profiles.

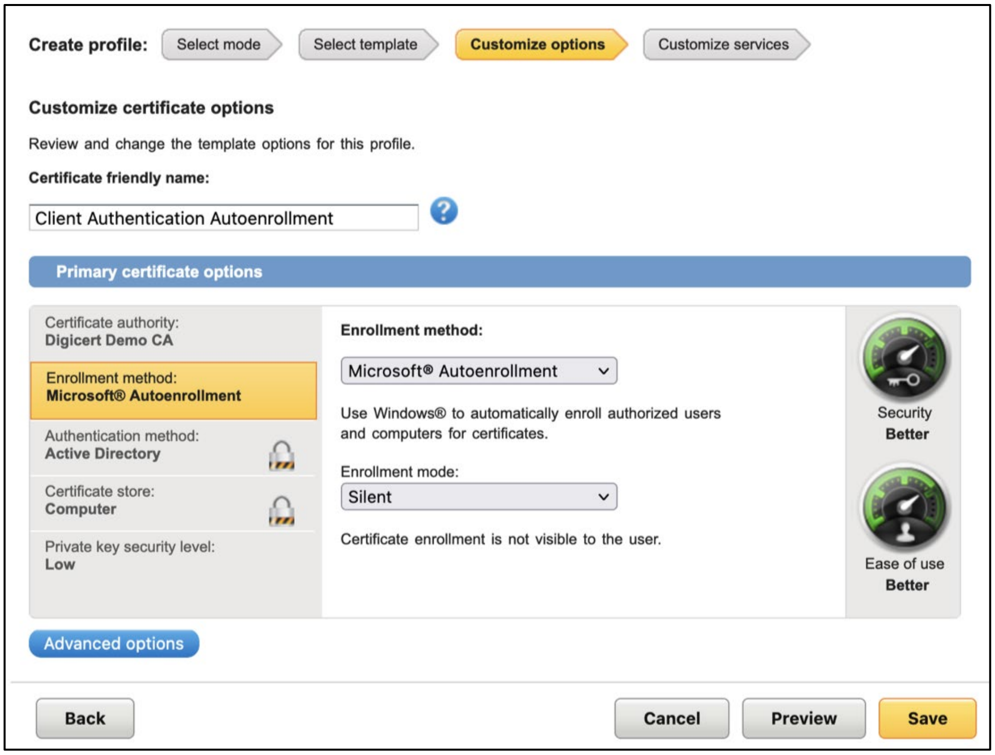
DigiCert PKI Platform Overview (PDF format)

DigiCert PKI Client

This component manages certificate installation and renewal for end users.

- DigiCert PKI Client installer (.zip file)

5. In the **Customize certificate options** page, enter **Certificate friendly name**. Also, make sure to select **Microsoft® Autoenrollment** for **Enrollment method**. For **Authentication method**, only **Active Directory** is allowed for Autoenrollment profile, so it is locked.



Customize certificate options

Review and change the template options for this profile.

Certificate friendly name: Client Authentication Autoenrollment

Primary certificate options

Certificate authority: Digicert Demo CA

Enrollment method: Microsoft® Autoenrollment

Authentication method: Active Directory

Certificate store: Computer

Private key security level: Low

Enrollment method: Microsoft® Autoenrollment

Use Windows® to automatically enroll authorized users and computers for certificates.

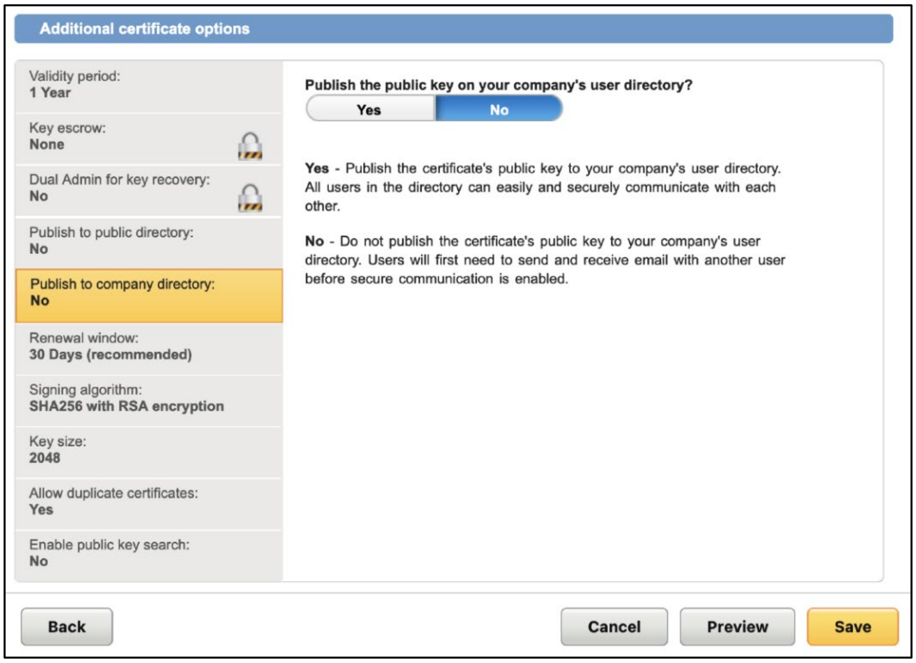
Enrollment mode: Silent

Certificate enrollment is not visible to the user.

Security Better

Ease of use Better

6. Selecting **Yes** for **Publish to company directory** will publish the issued certificates into your Active Directory.



Additional certificate options

Validity period: 1 Year

Key escrow: None

Dual Admin for key recovery: No

Publish to public directory: No

Publish to company directory: No

Renewal window: 30 Days (recommended)

Signing algorithm: SHA256 with RSA encryption

Key size: 2048

Allow duplicate certificates: Yes

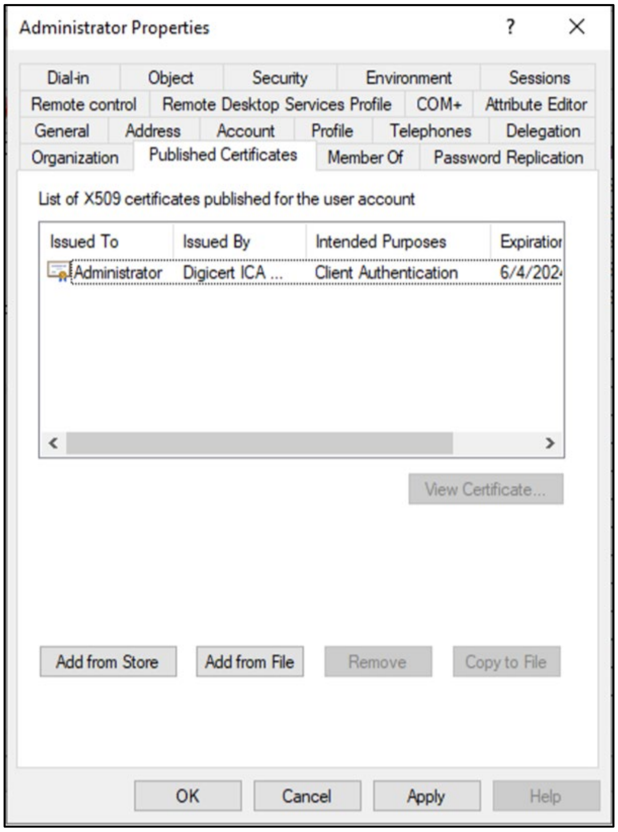
Enable public key search: No

Publish the public key on your company's user directory? Yes [✓ No]

Yes - Publish the certificate's public key to your company's user directory. All users in the directory can easily and securely communicate with each other.

No - Do not publish the certificate's public key to your company's user directory. Users will first need to send and receive email with another user before secure communication is enabled.

Screenshot below shows published certificate for Administrator using **Advanced** property in **Active Directory Users and Computers** Tool.



List of X509 certificates published for the user account

Issued To	Issued By	Intended Purposes	Expiratior
Administrator	Digicert ICA ...	Client Authentication	6/4/202

When selecting **Yes**, you will need to assign a special permission to the Autoenrollment Server afterwards to allow publishing. Refer to section "Allow Publishing to Active Directory" for more details.

7. Configure other options accordingly. For details about these options, refer to "*DigiCert® PKI Platform Overview*" section "*2.5.2 Primary Certificate Options* ", "*2.5.3 Certificate Fields* ", and "*2.5.4 Additional Certificate Options* "for details.

8. Click **Save** to save the profile and finish the creation process.

5.6 Importing the Autoenrollment Configuration File

Once you have configured the RA certificate, prepared the configuration utility, and created the Autoenrollment certificate profile, import the Autoenrollment configuration file. You can download the configuration file from PKI Manager.

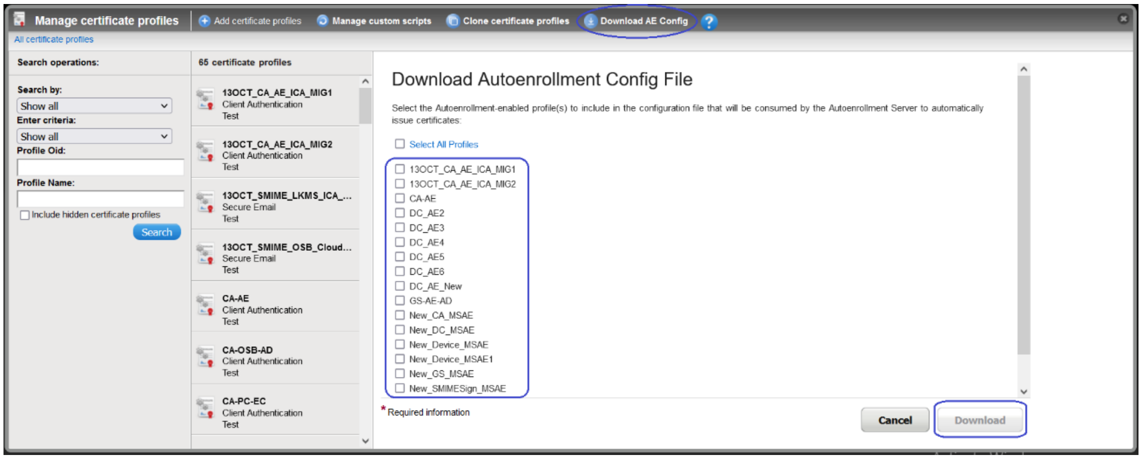
The autoenrollment configuration file publishes data to the Active Directory, which includes:

- Details about the enrollment service and the templates it supports.
- The list of certificate templates that CA offers.
- DigiCert's trusted CA certificates.

NOTE: The user running the Autoenrollment Config utility must have administrator rights to successfully store the configuration data in Active Directory and the system's registry. If the user has insufficient privileges to write to these resources, the Autoenrollment Config utility cannot publish and install the configuration data.

To import the Autoenrollment configuration file:

1. Download the autoenrollment configuration file by clicking the **Download AE Config** link on the **Manage certificate profiles** page of PKI Manager.
2. Choose the profiles by clicking checkbox and Click on **Download** button.



Download Autoenrollment Config File

Select the Autoenrollment-enabled profile(s) to include in the configuration file that will be consumed by the Autoenrollment Server to automatically issue certificates:

☐ Select All Profiles

☐ 13OCT_CA_AE_ICA_MIG1
☐ 13OCT_CA_AE_ICA_MIG2
☐ CA-AE
☐ DC_AE2
☐ DC_AE3
☐ DC_AE4
☐ DC_AE5
☐ DC_AE6
☐ DC_AE_New
☐ GS-AE-AD
☐ New_CA_MSAE
☐ New_DC_MSAE
☐ New_Device_MSAE
☐ New_Device_MSAE1
☐ New_GS_MSAE
☐ New_SMIMESign_MSAE

* Required information

3. Store the configuration file in the installation directory of Autoenrollment server.

   This file must be accessible by the Autoenrollment service.

4. Log on to the computer as AE Administrator or as another user who is a member of the Enterprise Administrators group.
5. On the **Start** menu, open the Autoenrollment Config utility by clicking **All Programs > DigiCert > AutoEnrollmentServer > Autoenrollment Configuration**. (AutoEnrollmentServer directory will only appear in classic Start Menu).
6. Click **Import Config**.

   The Autoenrollment Config displays a warning message telling you that importing configuration data may overwrite already existing templates, certificates, and enrollment service settings. Templates and the settings that are not a part of the Autoenrollment server do not change in any way.

7. Click **OK** to proceed with the download or click **Cancel** to abort.

CHAPTER 5

6 Using the Autoenrollment Server

This chapter includes the following topics:

6.1 About Using the Autoenrollment Server

After you install and configure the DigiCert Autoenrollment Server, you can start to use the service to request certificates from the DigiCert CA.

6.2 Files Written by the Autoenrollment Process

While running and processing requests, the autoenrollment process writes the following files:

- The file **RequestBufferFile.dat** that is located in the installation directory. This file includes information about certificate requests.
- The log file as configured in Autoenrollment Config Log Properties configuration file. Refer to section “Log Properties Configuration Options“ for details.

6.3 Starting and Stopping the Autoenrollment Server

You can start and stop the Autoenrollment server by starting and stopping the Autoenrollment service.

NOTE: Although you can use Windows Service Manager to start and stop the Autoenrollment service, the service status may not always display accurately. DigiCert recommends that you use the Autoenrollment Config utility to start and stop the service. Optionally, click **Refresh** in the utility to display the current status.

By default, the Autoenrollment service is started automatically upon system startup. You cannot configure the Autoenrollment Config tool or import an autoenrollment configuration file while the autoenrollment service is running.

To start and stop the Autoenrollment server,

1. Log on to the computer as the AE Administrator or as another user who is a member of the Enterprise Administrators group.
2. On the **Start** menu, run Autoenrollment Config by clicking **All Programs > DigiCert > AutoEnrollmentServer > Autoenrollment Configuration**.
   (AutoEnrollmentServer directory will only appear in classic Start Menu).
3. Depending on the service's current status, click **Start Service** or **Stop Service**, as appropriate.

6.4 About the Preparation of Certificate Templates

The set of certificate templates that you configured in PKI Manager is automatically installed in the Active Directory when you import the configuration file downloaded from PKI Manager. To deploy certificates, you must assign the enroll and/or autoenroll permissions to the appropriate groups or users for each certificate template separately.

See “About the Assignment of Group/User Access to Templates”.

Autoenrollment server supports v2 and v4 certificate templates.

You cannot use the older v1 or v3 templates for autoenrollment as the Autoenrollment server has not been fully qualified for them. However, you can supersede older templates to newer templates.

6.4.1 About the Assignment of Group/User Access to Templates

Use the **mmc** and the **Certificate Templates Snap-In** to set the security settings (enroll/autoenroll rights) for the templates.

Note: Do not change any of the template values other than the security settings. Editing templates leads to failure of all requests for this template.

To change template settings, edit the corresponding certificate profile in PKI Manager, and then download and import a new autoenrollment configuration file.

The **Certificate Template** property page contains the **Security** tab. The **Security** tab allows you to define the DACL (Discretionary Access Control List) for a specific certificate template. The permissions that you assign to the certificate template define which security principals can read, modify, enroll, or auto-enroll for a specific certificate template.

The **Group or user names** dialog lists all groups and users holding privileges on the currently-opened certificate template.

You can add your own network-specific group names if you do not use the default group names (such as Domain Users and Domain Computers). Once you have added your domain-specific groups, assign the appropriate combinations of enroll and auto-enroll permissions to them.

Important permissions are:

- Read: This permission allows a security principal to see the certificate template when they enroll for certificates. It is required for a security principal to enroll or auto-enroll a certificate. The certificate server also requires finding the certificate templates in Active Directory.
- Enroll: This permission allows a security principal to enroll for a certificate based on the certificate template. To enroll for a certificate, the security principal must also have Read permissions for the certificate template.
- Autoenroll: This permission allows a security principal to receive a certificate through the auto-enrollment process. Autoenrollment permissions require that the user has both Read and Enroll permissions in addition to the Autoenroll permission.

Depending on the specific certificate template, you should assign the appropriate permissions to all of the desired groups of users or computers.

NOTE: You should use global or universal groups instead of individual users or computer accounts when assigning template access permissions. Especially in large infrastructures, this facilitates administration of access rights. This also helps minimize conflicts and inconsistencies across multiple domain controller contexts.

Additionally:

- Make sure that the Autoenrollment server belongs to a group that also has permission to enroll the template it uses to process requests.
- You should assign Read permission to Authenticated group for all certificate templates. Then all users and computers can read the certificate templates in Active Directory.
- Restrict Write and Full Control permissions to only those people who require them to ensure that the templates are not improperly configured.

6.5 About the Replication of Certificate Templates and Policies

Use Active Directory's replication mechanism to make certificate templates and policies available to multiple domain controllers existing in your domain. All domain controllers in the forest receive a copy of any updated configuration container automatically.

Certificates are also stored in Active Directory and they are replicated to each domain controller in the forest. The process of replicating data can take up to eight hours across Active Directory instances. Replication for all computers occurs earlier if the domain controller computer is rebooted. The policy information of a particular machine is refreshed whenever that computer is rebooted.

You can use the certutil tool to force a client to refresh its policy information:

```
certutil -pulse
```

You have to repeat this replication step each time that you modify your certificate templates to have the changes be effective immediately.

Automatic replication needs more time, especially if you are in a sub-domain.

6.6 Testing Certificate Enrollment

After you install the server and start the autoenrollment service, you need to request a few certificates from the DigiCert CA for testing purposes. This topic takes you through the process of manually triggering the certificate autoenrollment process.

To test certificate enrollment

1. Log on to the system as Administrator and click **Start > Run**.
2. Type **mmc** in the **Open** field and press **Enter**.
3. Click **File > Add/Remove Snap-in**. The available snap-ins are displayed.
4. Select **Certificates** and click **Add**.
5. Select **My user account** from the option group.
6. Click **Finish > Close > OK** to return to the MMC console.
7. Expand the tree view on the left to display **Console Root > Certificates - Current User > Personal > Certificates**.
8. Right-click in the right pane and then click **All Tasks > Request New Certificate**.

   The **Certificate Enrollment wizard** opens.

9. Select **Active Directory Enrollment** Policy.
10. Click **Next**. The list of available certificate templates displays. Mark every template you want to enroll.
11. Click **Enroll**.

    You are informed about the progress of the enrollment. After a successful enrollment, you can view your new certificate in the **Certificates** node of MMC.

6.7 Monitoring Enrollment Activities

The following topics describe how to monitor the Autoenrollment server's activities and ways to track activities and events of the autoenrollment process.

6.7.1 Analyzing the Log File

Both Autoenrollment Config and the Autoenrollment service write logging information to the configured log file.

To analyze the log file

- Check the log file as needed to track autoenrollment activities.

6.7.2 Displaying System Events with the Windows Event Viewer

You can use the Windows Event Viewer to display information about the certificate requests that have been created during the autoenrollment process.

To display system events with the Windows Event Viewer

1. Click **Start > Administrative Tools > Event Viewer**.
2. Highlight the **Application** node and search for entries that includes **Autoenrollment** in the **Source** column.

APPENDIX A

7 Additional Configurations for Autoenrollment Server

This appendix includes the following additional configurations for Autoenrollment Server:

- Configuring Autoenrollment Server for High Availability
- Configuring Autoenrollment Server for Syslog

7.1 Configuring Autoenrollment Server for High Availability

7.1.1 About Configuring the Autoenrollment Server for High Availability

The Autoenrollment server and DCOM protocol can support high availability by default. To configure multiple instances of the Autoenrollment server for high availability, you only need to configure the HSMs to recognize the same RA certificate across all instances of Autoenrollment server.

This appendix describes how to configure multiple instances of the Autoenrollment server for high availability.

7.1.2 Configuring the Autoenrollment Server for High Availability

To configure the Autoenrollment server for high availability

1. On all machines hosting an instance of the Autoenrollment server, register the CSP. Refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html for details.
2. From your initial Autoenrollment server machine, obtain and install an RA certificate.

   This is a separate RA certificate from the one that you obtained for the PKI Enterprise Gateway.
   See "Obtaining the RA Certificate".

3. Install the same RA certificate that you obtained in Step 2 on all of the other Autoenrollment server machines.
4. From a command line, run the following command on all Autoenrollment server machines to associate the RA certificate in each machine with the private key on the initial HA partition:

   ```
   certutil -f -v -repairstore -csp <PROVIDER-NAME> My "<Certificate
   thumbprint>"
   ```

5. On each of the Autoenrollment server machines, modify the registry setting under `HKEY_LOCAL_MACHINE/SOFTWARE/DigiCert/Autoenrollment`.

   The value of this entry is appended to the Name of the Enrollment Service (Service-CN). Set a different value for each of the instances. The main instance should have an empty string. A registry key, named **ServiceCN-Postfix**, needs to be added with the type of string in the registry. Then this key needs to be set to a unique value.

6. Download the Autoenrollment server configuration file and install it onto each of the Autoenrollment server machines.

   See "Importing the Autoenrollment Configuration File".

7. Start the Autoenrollment server.

   See "Starting and Stopping the Autoenrollment Server".

7.2 Configuring Autoenrollment Server for Syslog

Autoenrollment server can use syslog as logging output by using the Autoenrollment Configuration **Log Properties** settings. Change the contents of the **logger.properties** file or change the target property file path to enable logging to syslog. See "Setting the Autoenrollment Configuration Utility" on how to configure this.

The sample syslog properties file can be found as **syslogger_sample.properties** in the installation directory of the Autoenrollment Server. The following shows the contents of the sample:

```
# A line starting with # is a comment and ignored.
# Define with log-level (DEBUG, INFO, WARN, or ERROR) and appender name
log4cpp.rootCategory=INFO, SYSLOG
# Configured appender type
log4cpp.appender.SYSLOG=SyslogAppender
# Remote syslog server IP address
log4cpp.appender.SYSLOG.syslogHost=192.168.1.1
# Remote syslog server port number
log4cpp.appender.SYSLOG.portNumber=514
# Syslog facility number
log4cpp.appender.SYSLOG.facility=1
# Output pattern (see http://log4cpp.sourceforge.net/#faq for format details)
log4cpp.appender.SYSLOG.layout=PatternLayout
log4cpp.appender.SYSLOG.layout.ConversionPattern=[AESRV]: %d{%Y-%m-%d %H:%M:%S}
%-5p [%t] %m%n
```

Table 6-2 shows the details about each property.

Table 6-2 Syslog Property Details

Property Key	Description
log4cpp.rootCategory	Default sets **logger_name** as **SYSLOG**. See Table 4-4 Log Property Details for more detailed description about this property.
log4cpp.appender.<logger_name>	The value must be `SyslogAppender` to use for syslog. See Table 4-4 Log Property Details for more detailed description about this property.
log4cpp.appender.<logger_name> .syslogHost	Specifies the remote syslog server IP address. **Note:** The remote syslog server must be accessible from the machine where Autoenrollment server is installed.
log4cpp.appender.<logger_name> .portNumber	Specifies the remote syslog server port number.
log4cpp.appender.<logger_name> .facility	Specifies the remote syslog server facility number. Default value is 1 (user-level messages).
log4cpp.appender.<logger_name> .layout	See Table 4-4 Log Property Details for more detailed description about this property.
log4cpp.appender.<logger_name> .ConversionPattern	The default log format is set as **"[AESRV]: <Date{yyyy-mm-dd}> <Time{hh:mm:ss}> <LogLevel> [<TheadID>] <LogMessage>"**. Every log message is intentionally prepended with [AESRV]: string, to differentiate Autoenrollment server logs from other logs. The following shows an example: `[AESRV]: 2021-09-22 04:15:28 INFO  [6176] Service started, waiting for requests.` See Table 4-4 Log Property Details for more detailed description about this property.

APPENDIX B

8 Troubleshooting

This appendix includes the following topics:

- Repeating an Action with Higher Log Level
- Common Problems

8.1 Repeating an Action with a Higher Log Level

The Autoenrollment server process keeps a log file to document its activities. When a problem occurs (for example, a certificate cannot be issued although apparently nothing is wrong with the corresponding request), you need to review the autoenrollment process log file. In most cases, it provides details about what went wrong.

However, sometimes the information in the log file may not be detailed enough to thoroughly investigate and resolve a specific problem.

In this case it can be useful to retry the failed action, but this time with a higher log level. The higher the log level the more information is stored in the log file about a particular action or error.

Use the Autoenrollment Config **Log Properties** file configuration to change the log file level. Refer to section “Log Properties Configuration Options” for details.

8.2 Common Problems

The following topics describes some common issues that may occur and provide some solutions.

8.2.1 Certificate is Pending in the Client or the Autoenrollment Config Utility

If the Autoenrollment server cannot complete a request with the DigiCert CA, (for example, due to connection problems or to heavy server traffic), it sends a pending response to the client. The Autoenrollment server retries the request periodically until a response is received from the DigiCert CA. The request also appears as pending in the Autoenrollment Config utility.

Once the Autoenrollment server can re-establish connection to the DigiCert CA, the request is processed normally.

8.2.2 Certificate Templates do not Appear for Autoenrollment

If your certificate templates do not appear for your end users after you have imported them with the Autoenrollment Config utility and configured the correct autoenroll permissions, you may need to import the root and the issuer CAs of your RA certificate into your enterprise Trust Store.

The root and issuing CAs for the RA certificate are provided in the `certificates` folder from the location where installer package is extracted.

As a member of the Enterprise Administrator group in the root domain, run the following commands to import these certificates:

```
certutil -f -dsPublish <root ca file name> RootCA certutil -f-dsPublish
<intermediate cert file name> SubCA
```

8.2.3 Certificates Cannot be Published (Permission Denied)

If your end-user certificates are not published to Active Directory and see the following error message in your log files, the Autoenrollment server does not have sufficient privileges in Active Directory.

ERROR in Publish Certificate: Cannot commit data to Active Directory: permission denied 0x80070005

Add the domain computer that runs the Autoenrollment server to the Active Directory group Cert Publishers. You may want to force Active Directory replication and perform a group policy update to make these changes available immediately.

8.2.4 Importing the Autoenrollment Configuration File Across Subdomains

While importing the autoenrollment configuration file, you may encounter an error that states that the objects that have previously been created cannot be accessed for setting the Discretionary Access Control List (DACL) on the new object. Your Autoenrollment server may be installed on a machine in part of a subdomain of your network. If this is the case, you need to force AD replication across your forest.

The following is a sample command that forces Active Directory replication for an Active Directory forest using the repadmin.exe utility. Use the appropriate command or mechanism for your implementation.

```
Repadmin /syncall
```

This command forces Active Directory replication between the root domain controller and any subdomain domain controllers.

Once replication is complete, click OK in the Autoenrollment Config utility to retry setting the DACL on the object.

8.2.5 Handling Multi-Valued Active Directory Attributes in the Autoenrollment Server

If you have mapped a multi-valued attribute to a certificate Subject Alternative Name or Subject Distinguished Name in PKI Manager, multiple values may be returned for these attributes from the Active Directory. In this situation, the Autoenrollment server does not pick any value from the list, and autoenrollment fails if this attribute is mandatory. The Autoenrollment server log displays a warning message similar to the following:

```
WARN Wed Oct 05 15:57:07 2011 [828] Attribute <CertificateProfile Configured AD attribute> has unexpected type: 8204
```

To avoid this issue, make sure that the multi-value attribute contains only one value.

8.2.6 Catastrophic Error When Restarting the Autoenrollment Server

If the Autoenrollment Server configuration file is not available when you restart the Autoenrollment Server, it does not start. The Windows services report a catastrophic error for the AutoEnrollmentDCOMSrv service.

Additionally, the following error is written to the log file:

```
AutoEnrollmentDCOMSrv: cannot run: AEException: Could not access CA interface (plugin): Could not initialize connection to CA. Check connection parameters and network connectivity!
```

If you want to avoid this issue, make sure that the location where you imported the configuration file when you configured the Autoenrollment Server is accessible to the server when you restart it.

Index