DigiCert® PKI Enterprise Gateway Deployment Guide

Version 8.22.5

February 15, 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 PKI Enterprise Gateway.

Revision History

No.	Date	Summary
1.	2021/05/31	Added support for Oracle OpenJDK 8 (Java Runtime Environment) for Key escrow and recovery service.
2.	2021/08/26	Removed the PKI Enterprise Gateway and Autoenrollment Server dependencies within the PKI Manager portal.
3.	2021/12/06	• Registration Authority certificates have been removed from the zip package and moved to https://knowledge.digicert.com/solution/ca-hierarchies-for-production-and-test-drive-ra-certificates.html. The following sections have been fixed to accommodate the change. • “2.4.1 Obtaining an RA Certificate to Store in the Microsoft Certificate Store" • “2.4.2 Obtaining an RA Certificate to Store in an HSM” • “2.5.4 Securing Communications Between your Enterprise Gateway and Local Key Escrow and Recovery Service” • “4.3 (Optional) Configuring the Key Escrow and Recovery Service” Fixed references to wrong pages and links at multiple locations.
4.	2022/05/25	• Support for Windows Server 2022
5.	2022/06/28	• Support for Oracle 21c and OpenLDAP 2.6 as data stores • Support for OpenLDAP 2.6 as user store
6.	2023/02/15	• Removed references to unsupported operating systems.

CHAPTER 1

1 DigiCert PKI Enterprise Gateway

This chapter includes the following topics:

- PKI Enterprise Gateway Components
- Audience

1.1 PKI Enterprise Gateway Components

PKI Enterprise Gateway is comprised of the following components:

- RA Service - The RA Service authorizes the user based on the certificate profiles that you configured in the PKI Manager. It then communicates with the DigiCert CA to request certificate issuance. The RA Service secures communications with the DigiCert Certification Authority using an RA certificate to enable SSL Client Authentication.

  If the RA Service is configured to do so, it also publishes the certificate to your user store.
- RA Agent - The RA Agent communicates with the RA Service to perform certificate issuance on behalf of the user. The RA Agent is required if your certificate profile is configured for OS\browser certificate management (non-PKI Client enrollment). DigiCert recommends you secure communications between the RA Agent and the RA Service using an SSL certificate.
- Authentication service - This service authenticates the user, based on the user's Windows credentials, and then it forwards the request to the RA Service. It must be installed on the same server as the RA Agent. DigiCert recommends that you secure communications between the authentication service and the RA Service using an SSL.
- Key escrow and recovery service - The key escrow and recovery service receives requests to enroll for certificates. The key escrow and recovery service generates and escrows the private key for the certificate enrollment request. It then sends the request and public key to DigiCert CA for certificate enrollment. The new certificate with the private key is then returned in the enrollment response. When the key escrow and recovery service receives a request to recover a key, it forwards the request to DigiCert CA for verification. DigiCert CA returns the information that is required to retrieve the key from the key escrow data source. The key escrow and recovery service recovers the private key from the key escrow data source and returns it in the response. Communications to the key escrow and recovery service are secured using client authentication and SSL. Communications from the key escrow and recovery service to DigiCert CA are secured using an RA certificate. The certificate is stored on a Hardware Security Module (HSM). For test installations, the RA certificate can reside in a software-based Java keystore.

- Foreign key import - The foreign key import enables non-DigiCert issued certificates to import into DigiCert PKI Platform. You must create a new certificate policy and assign the certificates based on the selected keystore. You can store the imported certificates in a local keystore or in the DigiCert keystore.

1.1.1 Single and Multiple Server Deployments

You can install the PKI Enterprise Gateway on a single server, where users access the PKI Certificate Service from within the network. Or you can install it across multiple servers, where users may access the PKI Certificate Service from outside the network.

Figure 1-1 illustrates how PKI Enterprise Gateway is typically deployed on an enterprise site in a single-server deployment.

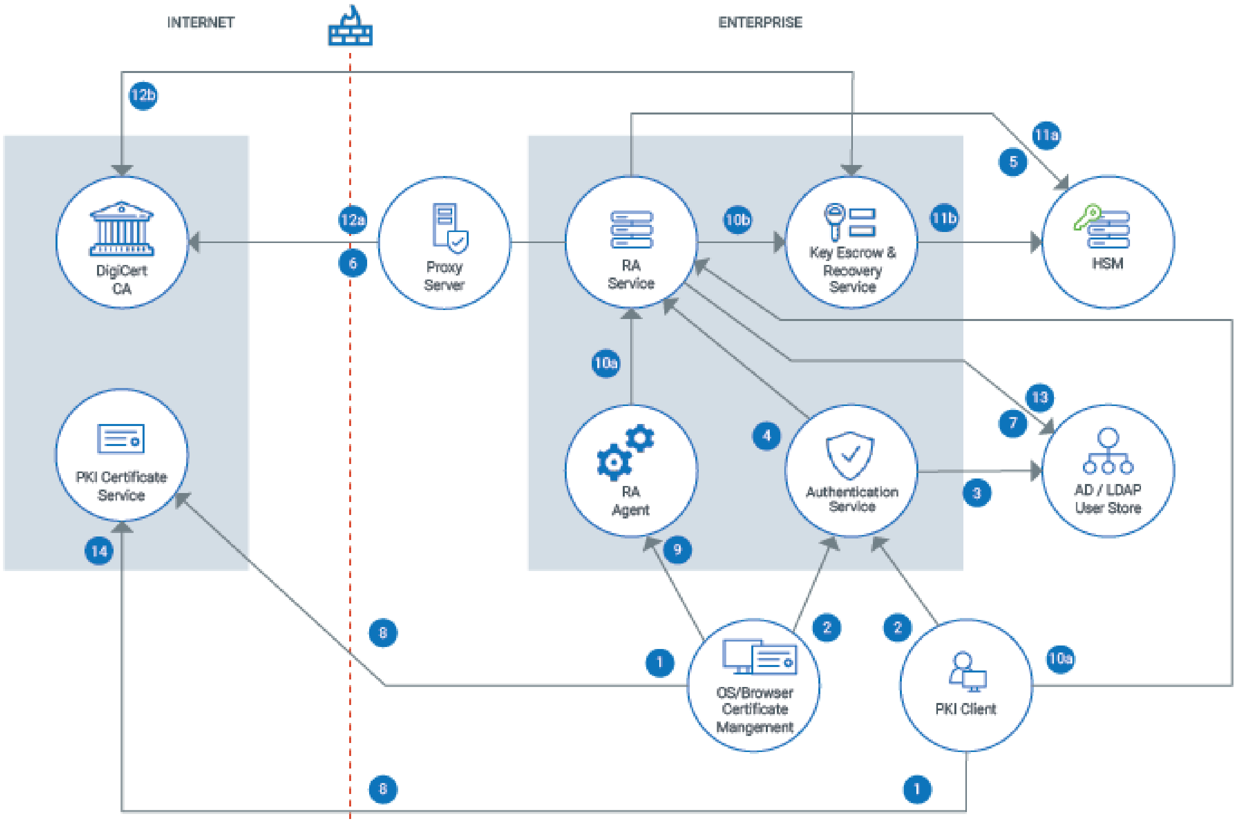


Figure 1-1 PKI Enterprise Gateway Single-Server Deployment

Figure 1-2 illustrates how PKI Enterprise Gateway is typically deployed on an enterprise site in a multiple-server deployment. The flows for users are identical both within the enterprise network and outside of the enterprise network.

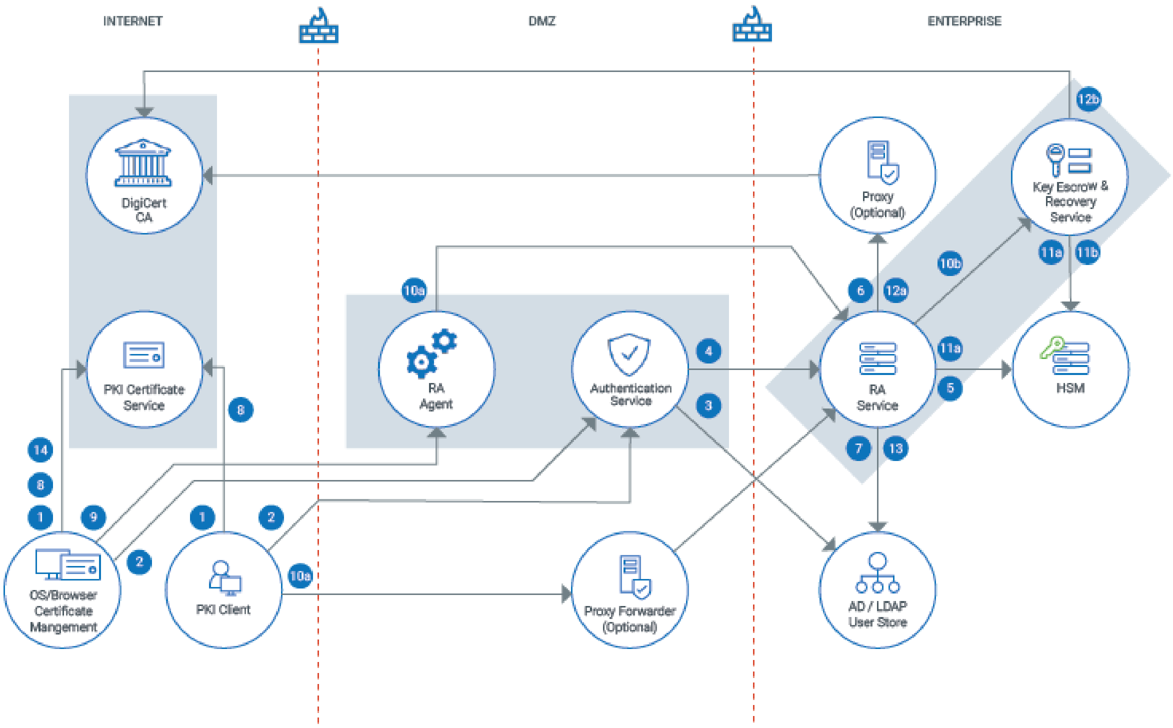


Figure 1-2 Multiple-Server Deployment

In both of these deployments, a typical certificate enrollment flow would be as follows:

1. The user accesses the PKI Certificate Service to enroll for a certificate.
2. The user's Windows credentials are sent to the authentication service.
3. The user's Windows credentials are verified against the enterprise user store.
4. The authentication service communicates with the RA Service to obtain a security token. The security token is used for authentication for the remainder of the enrollment flow.
5. The RA Service communicates with the Hardware Security Module (HSM) to use the RA certificate to secure communications with the DigiCert CA.
6. The RA Service communicates with the DigiCert CA to obtain the appropriate certificate policy.
7. Based on the certificate policy, the RA Service retrieves the user data that is needed for certificate enrollment from the user store.
8. The user is redirected to the PKI Certificate Service, where they are prompted to submit the enrollment request.
9. For OS\browser certificate management only, the user is redirected to the RA Agent to complete the enrollment request.

10. The system makes a request to issue the certificate from the DigiCert CA:
    a) Either the RA Agent or the PKI Client sends the request to the RA Service.
    b) If the key escrow and recovery service is configured, the RA Service sends the request to the key escrow and recovery service.
11. The system communicates with the HSM to use the RA certificate to secure communications with the DigiCert CA.
    a) The RA Service communicates with the HSM.
    b) If key escrow and recovery service is configured, then the key escrow and recovery service communicates with the HSM.
12. The system communicates with the DigiCert CA to request the certificate.
    a) If key escrow and recovery service is not configured, the RA Service communicates to the DigiCert CA.
    b) If key escrow and recovery service is configured, the key escrow and recovery service communicates with the DigiCert CA.
13. If the RA Service is configured to do so, then it publishes the certificate to the user store.
14. The user is redirected to the PKI Certificate Service to install the certificate and for any post-processing.

1.1.2 Key Recovery Deployments

Figure 1-3 illustrates how the key escrow and recovery server is typically deployed in your PKI Enterprise Gateway deployment. Although this diagram illustrates a single-server deployment, the key escrow and recovery service deployment is identical for both the single-server and the multiple-server deployments.

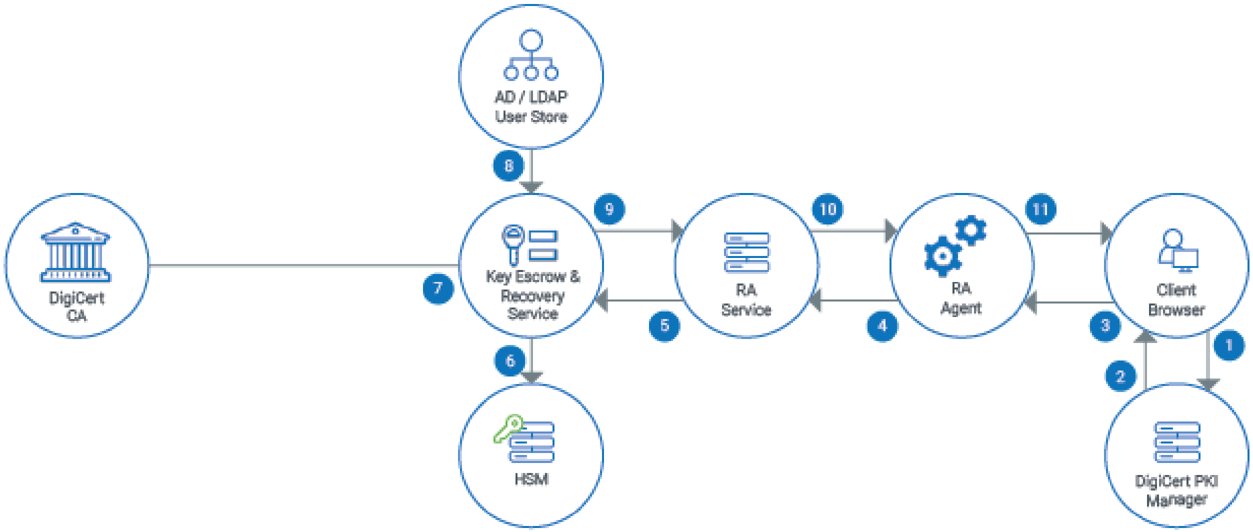


Figure 1-3 Key Escrow and Recovery Service Flow from PKI Manager

A typical certificate recovery flow would be as follows:

1. The administrator accesses the DigiCert PKI Manager to recover the private key for an escrowed certificate profile that is on the Enterprise Gateway.
2. PKI Manager authenticates the request from Enterprise Gateway, before redirecting it to a page on the RA Agent.
3. The administrator gets redirected to a page on the RA Agent.
4. The RA Agent sends a key recovery request to the RA Service.
5. The RA Service forwards the request to the key escrow and recovery service.
6. The key escrow and recovery service communicates with DigiCert CA using the RA Certificate on the HSM.
7. The key escrow and recovery service communicates with the PKI Certificate Service to retrieve the credentials for the enrolled certificate profile.
8. The key escrow and recovery service communicates with the configured user datastore to construct the certificate with the recovered private key.
9. The key escrow and recovery service returns the certificate with the recovered private key and password back to the RA Service.
10. The RA Service forwards it to the locally-hosted page on the RA Agent.
11. The certificate and password are available for download from the locally-hosted page.

1.2 Audience

This guide is written for installers who deploy the PKI Enterprise Gateway. This guide assumes that the reader has the following skills:

- Strong familiarity with networks in general and your enterprise networks and client applications in particular.
- Strong familiarity with LDAP directories or Microsoft Active Directory in general, and your enterprise user store configuration in particular.
- Knowledge of PKI (public key infrastructure).
- Knowledge of Microsoft® Internet Information Server (IIS).

CHAPTER 2

2 Prerequisites

This chapter includes the following topics:

- Hardware and Software Requirements
- Configuring HTTP Proxy Access
- Preparing to Configure PKI Manager
- Obtaining Your Registration Authority Certificate
- Securing Communications with the Key Escrow and Recovery Service

2.1 Hardware and Software Requirements

This chapter describes the hardware and software that has been tested for use with the PKI Enterprise Gateway. This chapter also describes the steps that you need to complete before installing the PKI Enterprise Gateway.

2.1.1 PKI Enterprise Gateway Machine

The PKI Enterprise Gateway machine can be any computer that runs the following operating system and applications:

- Windows Server 2016, Windows Server 2019 and Windows Server 2022.
- .NET Framework 4.7.1. Installer automatically retrieves and installs this application, but it requires internet connection. If the server has no internet connection, obtain and install this application from Microsoft beforehand.
- Microsoft Internet Information Server (IIS) 8.5 and 10.0.

  Also following roles and features are required:

  - **Windows Integrated Authentication** – Open **Add Roles and Features Wizard** form **Server Manager**, click **Next** until **Server Roles** page, scroll down to **Web Server (IIS) > Web Server > Security** and select the **Windows Authentication** check box.
  - **IIS 6 Management Compatibility** – At **Server Roles** page in **Add Roles and Features Wizard**, open **Web Server (IIS) > Management Tools** and click **IIS 6 Management Compatibility** and select all of the check boxes in the group.
  - **ASP .NET 4.5/4.6/4.7** – At **Server Roles** page in **Add Roles and Features Wizard**, open **Web Server (IIS) > Web Server > Application Development and** click **ASP .NET 4.6** for Windows Server 2016, **ASP .NET 4.7** for Windows Server 2019 and **ASP .NET 4.8** for Windows Server 2022.
  - **WCF Services** – In **Add Roles and Features Wizard**, click **Next** until **Features** page, open **.NET Framework 4.5 Features > WCF Services** and select **HTTP Activation**.

  NOTE: Install all roles required by the selected roles also.

- VMware vSphere 4 and 5.
- (Optional) Key escrow and recovery service work with the Apache Tomcat 8.5 web application server and Java SE 1.8 or Oracle OpenJDK 8 (Java Runtime Environment).

The following components of PKI Enterprise Gateway (RA Service, RA Agent, authentication service) are IIS web applications. The optional key escrow and recovery service runs as a Web service application on a Tomcat server.

In a single-server deployment, one computer hosts all of the components of PKI Enterprise Gateway. This computer communicates with the PKI Certificate Service outside of the network. It also communicates with the user data source and the Hardware Security Module (HSM) in the enterprise back end. In a multiple-server deployment, you need two computers:

- One computer resides in the enterprise back end and hosts the RA Service and the (optional) key escrow and recovery service. This computer communicates with the Active Directory and HSM.
- One computer resides in the DMZ and hosts the RA Agent and authentication service. This computer accepts requests from the user outside the network. This computer also communicates with the Active Directory, and with the back-end RA Service.

2.1.2 Supported Windows Topologies

PKI Enterprise Gateway 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.

2.1.3 User Store

The user store contains the user data that is required to authenticate the certificate enrollment request and to populate certificate data.

Active Directory User Store

The Active Directory user store can be Windows Server 2016, 2019 or 2022.

For multiple-server deployments, the Active Directory domains must be available to the authentication service. This domain is in the DMZ (for example, using a read-only AD domain controller).

The Active Directory user store can be used to escrow private keys if using the key escrow and recovery service.

LDAP User Store

The LDAP user store must be Net IQ 9.0.3, Oracle Identity Management 12c (12.2.1.3.0), or OpenLDAP 2.6.

NOTE: Dynamic groups for user authorization are not supported.

For multiple-server deployments, the LDAP directory server must be available to the authentication service that is hosted in the DMZ.

The LDAP User Store can be used to escrow keys if using the key escrow and recovery service.

RDBMS Data Store

The RDBMS key escrow datastore database is used to escrow private keys when you use the optional key escrow and recovery service. It also supports Microsoft SQL Server 2017 or 2019 and Oracle 19c or 21c.

DigiCert has also qualified the key recovery datastore with OpenLDAP 2.6, Net IQ 9.0.3, and Oracle Identity Management 12c (12.2.1.3.0). DigiCert expects that the key escrow datastore supports other LDAP-based directories.

2.1.4 Key Escrow Prerequisites

You need to obtain the following additional applications to support the tasks that are performed by the optional key escrow and recovery service.

1. Java SE 1.8 or Oracle OpenJDK 8 (Java Runtime Environment)

   NOTE: All DigiCert PKI Platform components must run the same version of Java. For example, if your key escrow and recovery service of the PKI Enterprise Gateway is running Java SE 1.8, then your Web service must also run Java SE 1.8

   - To support high grade encryption, you must also download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction policy files 8 from http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html
   - Extract the local_policy.jar and US_export_policy.jar files from the zipped file you downloaded, and use them to replace the existing versions in your
   - $JRE_HOME/lib/security folder.
   - Database drivers (if deploying RDBMS databases as the key escrow data source). Once you have obtained these, you must place them in your system classpath or your Tomcat web server classpath.

NOTE: Oracle OpenJDK 8 (Java Runtime Environment) can be downloaded and installed from https://openjdk.java.net/install/ URL

2. Apache Tomcat - The Apache Tomcat web server hosts the key escrow and recovery service. DigiCert has qualified version 8.5.

2.1.5 Hardware Security Module (HSM)

The HSM stores the RA certificate, used to authenticate the PKI Enterprise Gateway, to the DigiCert CA. It also performs the cryptographic operations required by PKI Enterprise Gateway, such as key generation and signing.

NOTE: If you test your deployment or DigiCert PKI Platform profile configuration, you can use the Microsoft certificate store rather than an HSM. However, it is recommended to use an HSM if you deploy DigiCert PKI Platform to issue production certificates.

The PKI Enterprise Gateway supports several HSMs. Refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html.

2.1.6 Connectivity Requirements

Depending upon your deployment, you need to configure your network firewalls to allow the appropriate connectivity for the PKI Enterprise Gateway components.

Unless otherwise mentioned, all communications should be secured using SSL (server authentication).

Single-server Deployment

- Your users must be able to access the DigiCert PKI Certificate Service.
- The RA Service must be able to access the DigiCert Certificate Authority. Communications should be secured using your RA certificate.
- (Optional) Key escrow and recovery service should talk to the PKI Certificate Service.

Multiple-server Deployment

- Users outside your network domain that enroll for and store certificates in their browsers must be able to access the authentication service. They must also be able to access the RA Agent in the DMZ.
- Users outside your network domain that use the PKI Client must be able to access the authentication service in the DMZ and the RA Service in the back end.
- All your users must be able to access the PKI Certificate Service.
- The RA Service in your back end must be able to reach the DigiCert Certificate Authority. Communications should be secured using your RA certificate. If the RA certificate resides on an HSM, the RA Service must be able to access the HSM.
- (Optional) Key escrow and recovery service should talk to the PKI Certificate Service.

- The authentication service in your DMZ must be able to access the user store. For Active Directory user stores, you must use Windows Integrated Authentication.

  See "PKI Enterprise Gateway Machine".

2.1.7 Default ports

Table 2-1 lists the default ports that PKI Enterprise Gateway expects. If these ports are in use during the installation, the installation script uses the next available ports. Additionally, you can configure PKI Enterprise Gateway to use different ports.

See "Modifying the RA Service".

See "Modifying the RA Agent and Authentication Service".

Table 2-1 Default PKI Enterprise Gateway ports

Component	Port Number
RA Service	9100
Authentication service	9101
RA Agent	9102
Signing Service	9105
Key escrow and recovery service	8443

2.2 Configuring HTTP Proxy Access

You may choose to configure an HTTP proxy between the RA Service and DigiCert Certificate Authority. PKI Enterprise Gateway supports HTTP Basic Authentication and Anonymous Authentication. If your proxy uses HTTP Basic Authentication, you need to provide the password to PKI Enterprise Gateway. You provide the password either as part of the installation or manually after the installation.

See "Installing PKI Enterprise Gateway".

See "Updating Encrypted Settings".

2.3 After installation of the PKI Enterprise Gateway, you need to configure it to recognize your HTTP proxy.Preparing to Configure PKI Manager

The first time you access PKI Manager, you are prompted to set up your account. You also configure PKI Manager to recognize your gateway and to identify the user groups to whom you issue certificates.

Initially, you only need to identify to PKI Manager that your account uses PKI Enterprise Gateway (from the Set-up your account link). You can return to the PKI Manager at any time to download the PKI Enterprise Gateway software and installation instructions (this document). You can also complete the remaining PKI Enterprise Gateway configuration. Refer to the instructions in PKI Manager and the sections that are listed for more details.

1. Set up your account: Select this link to identify that your PKI Manager account is set up for PKI Enterprise Gateway.
2. Download Software: Select this link to download the PKI Enterprise Gateway installation package and documentation.
3. Download RA Certificate: Select this link to request and download your RA certificate, required to secure communications with the DigiCert Certificate Authority.

   See "Obtaining Your Registration Authority Certificate".

4. Configure PKI gateway: Select this link to configure the PKI Manager to recognize your PKI Enterprise Gateway.

   See "Configuring PKI Manager to Recognize PKI Enterprise Gateway".

5. Manage authorized user lists: Select this link to identify the user groups to which you issue certificates. Refer to the instructions in PKI Manager for detailed procedures.
6. Create Certificate Profile: Select this link to create the certificate profile that the DigiCert Certificate Authority uses to issue certificates to your users. See the instructions in PKI Manager for detailed procedures.
7. Enroll Users: Select this link to obtain the enrollment URL that you send to certificate recipients. Refer to the instructions in PKI Manager for detailed procedures.

Contact your DigiCert representative if you do not already have access to PKI Manager.

2.4 Obtaining Your Registration Authority Certificate

You need a Registration Authority (RA) certificate to secure communications and identify yourself to the DigiCert Certificate Authority. You have the option of storing your RA certificate in a software keystore or on a hardware security module (HSM). The method 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. Securing your RA certificate and private key are very important because anyone who has access to the RA certificate and private key can act on your organization's behalf.

When you test your deployment or DigiCert PKI Platform profile configuration, you can use the Microsoft certificate store rather than an HSM. You must store the RA certificate in the Microsoft certificate store. Also, you should use an HSM if you deploy DigiCert PKI Platform to issue production certificates.

- See “Obtaining an RA Certificate to Store in the Microsoft Certificate Store”

2.4.1 Obtaining an RA Certificate to Store in the Microsoft Certificate Store

If you store your RA certificate in the Microsoft certificate store, for key escrow and recovery service, complete the following steps. These steps are completed on the IIS computer where you install the RA Service. The user who performs these steps must have administrator rights to the PKI Enterprise Gateway computer.

Complete the following steps to store your RA certificate in the Microsoft certificate store for key escrow and recovery service.

1. The root and issuing CAs for the RA certificate can be found on the web page at https://knowledge.digicert.com/solution/ca-hierarchies-for-production-and-test-drive-ra-certificates.html. These CAs are also available by clicking on the DigiCert PKI Resources icon in the lower left corner of PKI Manager. You need to import these CAs as trusted root CAs into the Microsoft certificate store. This ensures that the RA certificate that you install is correctly trusted.

   - Copy the root and issuing CAs for the RA certificate by accessing KB article to a directory on the local computer (<install_dir> is the location where you have extracted the PKI Enterprise Gateway installation package) or by clicking on the DigiCert PKI Resource icon in the lower left corner of PKI Manager. you can also copy by clicking on the DigiCert PKI Resources icon in the lower left corner of PKI Manager.
   - Open Microsoft Management Console (MMC) and add the Certificates snap-in for the local computer (select **Add Snap in for Certificates**, select **Computer Account** and click **OK**).

- Click **Certificates** > **Local Computer** > **Trusted Root Certification Authorities** > **Certificates**.
- Click **All Tasks** > **Import**.
- Select the root CA you copied to your local computer at the beginning of this step and click **OK**.
- Click **Certificates** > **Local Computer** > **Trusted Intermediate Certification Authorities** > **Certificates**.
- Click **All Tasks** > **Import**.
- Select the issuing CA you copied to your local computer at the beginning of this step and click **OK**.

2. Create a text file named `softwarecert.inf` and the name/value pairs. Save it to a temporary location. The following table describes the possible values you can configure for this file. Unless the values are identified, you must use the values in the following table.

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
Providertype = 0
RequestType = PKCS10
ProviderName = "Microsoft Software Key storage provider"
Subject = "CN=Registration Authority"
KeyContainer = "racertificate"
MachineKeySet = true
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
```

Value	Description
KeyUsageProperty	"NCRYPT_ALLOW_ALL_USAGES"
Providertype	0
RequestType	PKCS10
ProviderName	"Microsoft Software Key storage provider"
Subject	"CN=Registration Authority"
KeyContainer	"racertificate"
MachineKeySet	true
HashAlgorithm	SHA256
KeyAlgorithm	RSA
KeyLength	2048

3. From a command prompt, run the following command to generate the CSR in .pem format. The command outputs the CSR to the file racertificate.req.

   You can run this utility from any location. However, unless you run it from the location where you saved the softwarecert.inf file, you must specify the path to this file.

   ```
   certreq -new softwarecert.inf racertificate.req
   ```

   This command writes the racertificate.req file to the directory where you ran the command. Specify the full path to a different location.

4. Copy the racertificate.req file to the computer that has access to the PKI Manager.

   - Open racertificate.req in a text editor and copy the contents of the file into your Clipboard.
   - Access PKI Manager and select **Set up your account > Get an RA certificate**.
   - Paste the contents of your Clipboard into the request field. Click **Submit**.
   - When you are prompted, download the resulting .p7b certificate file.

5. Copy the .p7b certificate file to the PKI Enterprise Gateway computer.
6. Import the new certificate into your PKI Enterprise Gateway computer's Microsoft certificate store as follows:

   - Open MMC and click on **Certificates (Local Computer) > Personal > Certificates**.
   - Right-click **All Tasks** and select **Import**.
   - Import the new certificate.
   - Double-click the certificate and make sure that the following message appears: **You have a private key that corresponds to this certificate**.

   NOTE: You can skip step 7 as the new certificate is already imported.

7. Install the new certificate:

   ```
   certreq -accept -machine RA-Certificate.p7b
   ```

8. Verify the private key. Use the certutil command line (-verifystore) and note that there is a "Key Container" and the message "Private key is NOT exportable".

   ```
   certutil -verifystore MY
   MY
   ================ Certificate 0 ================
   Serial number:
   Issuer:
   NotBefore:
   NotAfter:
   Subject:
   Registration Authority
   Non-root Certificate
   Template:
   Cert Hash(sha256):
   Key Container =
   Unique container name:
   Provider =
   Private key is NOT exportable
   Encryption test passed
   Verified Issuance Policies:
   Verified Application Policies
   Certificate is valid
   ```

2.4.2 Obtaining an RA Certificate to Store in an HSM

Complete the following steps if you store your RA certificate in an HSM. The user who performs these steps must have administrator rights to the computer on which the HSM is running.

You need to install the HSM hardware and register the KSP. Refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html.

1. The root and issuing CAs for the RA certificate can be found on 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. By downloading there, you ensure that the RA certificate you install is correctly trusted.

- Copy the root and issuing CAs for the RA certificate by accessing KB Article to a directory on the local computer (where <install_dir> is the location where you have extracted the PKI Enterprise Gateway installation package). You can also copy by clicking on the DigiCert PKI Resources icon in the lower left corner of PKI Manager.
- Open the Microsoft Management Console (MMC). Add the Certificates snap-in for the local computer (Select **Add Snap in for Certificates**, select **Computer Account**, and click **OK**).
- Click Certificates > Local Computer > Trusted Root Certification Authorities > Certificates.
- Click **All Tasks > Import**.
- Select the root CA you copied to your local computer at the beginning of this step and click **OK**.
- Click Certificates > Local Computer > Trusted Intermediate Certification Authorities > Certificates.
- Click **All Tasks > Import**.
- Select the issuing CA you copied to your local computer at the beginning of this step and click **OK**.

2. Generate the CSR in .pem format.

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

   See "Hardware Security Module (HSM)"

3. Copy the CSR file to the computer that has access to the PKI Manager.

   - Open the CSR file in a text editor and copy the contents of the file into your Clipboard.
   - Access PKI Manager and select **Set up your account > Get an RA certificate**.
   - Paste the contents of your Clipboard into the request field. Click **Submit**.
   - When you are prompted, download the resulting .p7certificate file.

4. Import the new certificate into your local computer's keystore.

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

   See "Hardware Security Module (HSM)".

5. Open MMC and click on **Certificates > Local Computer > Personal > Certificates store**. Double-click the certificate and make sure that the message, "You have a private key that corresponds to this certificate" appears.

   If the message does not appear, right-click on **Certificates** and click **Refresh**

2.5 Securing Communications with the Key Escrow and Recovery Service

This section describes the steps you need to complete to secure communications between your Enterprise Gateway and the key escrow and recovery service. Secure communication is also needed between the key escrow and recovery service and DigiCert PKI Platform Web services.

2.5.1 Setting up the LDAP Data Store

Complete the following steps to install and configure your LDAP-based key escrow data source. These procedures apply to Microsoft Active Directory and LDAP datastores.

1. Install the LDAP datastore according to the vendor instructions.
2. Determine the base DN of the LDAP datastore in which to store the key management data. The base DN is the value in the key escrow and recovery service configuration file.
3. Create a new RDN under the base DN named **KeyRecoveryData**. The ou value is in the key escrow and recovery service configuration file.

   The following example (from the key escrow and recovery service configuration file) shows an Active Directory LDAP datastore using KeyRecoveryData as the ou value.

   ```
   kms.keyrecovery.ldap.keyescrowcontainer.ou=KeyRecoveryData
   ```

4. Modify the key escrow and recovery service configuration file to point to the LDAP datastore. See "(Optional) Configuring the Key Escrow and Recovery Service" on page 51.

2.5.2 Setting up the RDBMS datastore

Complete the appropriate steps to install and configure your database key escrow data source:

To set up the RDBMS datastore for Oracle databases

1. Install the database according to the vendor instructions. If you use an existing database, ensure that the database does not include a table named KeyRecovery. These procedures overwrite the data in that table.
2. Back up any data that resides on the database.
3. As a user with sufficient rights to the database to be able to create tables, switch to the <install_dir>/key escrow and recovery service/database directory of the .zip file. <install_dir> is the location where you extracted the PKI Enterprise Gateway installation package.
4. Use an administrator tool such as sqlplus to run the script to update the schema. For example:

```
sqlplus <userid>/<userpassword>@<hostname> @oracleKeyRecovery Schema.sql
```

5. Modify the key escrow and recovery service configuration file to point to the Oracle datastore.

   See ..

To set up the RDBMS datastore for SQL databases

1. Install the database according to the vendor instructions. If using an existing database, ensure that the database does not include a table named KeyRecovery. These procedures overwrite the data in the table.
2. Back up any data that resides on the database.
3. Use an administrator tool such as Microsoft Query Manager, to update your Microsoft SQL Server User Store. The script is located in the <install_dir>/key escrow and recovery service/database directory of the .zip file. <install_dir> is the location where you have extracted the PKI Enterprise Gateway installation package.
4. Launch the Microsoft Query Manager.

- Copy and paste the contents of sqlServerKeyRecoverySchema.sql into the Query Manager window.
- Execute the script.
- Modify the key escrow and recovery service configuration file to point to the SQL datastore.

  See "(Optional) Configuring the Key Escrow and Recovery Service".

2.5.3 Obtaining an SSL certificate

Complete the following steps to set up the secure channel between your Enterprise Gateway and the key escrow and recovery service.

NOTE: To renew your SSL certificates, you must re-enroll and repeat the directions in this chapter.

Task 1. Generate the certificate request	Generate a certificate request on your Tomcat web server. Refer to the documentation that is provided with your Tomcat Web server for procedures. The Common Name in the certificate request must exactly match the name of the Tomcat Web server host. For example, if you access the host by fully qualified domain name (host.domain.com), then use the fully qualified domain name here. If you access the host by host name only (host), then use the host name here.
Task 2. Acquire the SSL certificate	You can obtain an SSL certificate from https://www.digicert.com. Refer to the instruction available on the site for procedure on installing and enabling SSL certificates.
Task 3. Install the SSL certificate on your Tomcat Web server	Once you receive the SSL certificate from DigiCert, install it on your Tomcat Web server. Install it according to the procedures that are provided with your Tomcat server.

2.5.4 Securing Communications Between your Enterprise Gateway and Local Key Escrow and Recovery Service

Communications between your enterprise application and the key escrow and recovery service are authenticated and encrypted using client authentication and SSL using an RA Certificate.

Enable Client Authentication on your Tomcat Server

DigiCert provides the client authentication that enables secure communication between your Enterprise Gateway and the local key escrow and recovery service on the Tomcat Web server. For enrollment and recovery operations, you need a client RA Certificate for authentication.

If client authentication fails, you must keep your client certificate in the Apache Tomcat trust store.

Install the HSM for Key Escrow and Recovery Service

DigiCert recommends that you install your RA certificate on an HSM for greater security. If you use a production RA certificate, you must install it on an HSM.

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

If you store your RA certificate on an HSM, install the HSM following the vendor instructions with the following special considerations:

- You can configure the same HSM to work with both the enterprise gateway and the key escrow and recovery service. Modify the key escrow and recover service configuration file to identify the RA certificate based on the alias. Refer to the vendor instructions for details on determining the alias.
- The enterprise gateway and the key escrow and recovery service can use the same HSM for signing operations. However, the HSM used for key generation cannot be shared.

For a description of the FIPS 140-2 approved operation mode and these policies, refer to the vendor documentation.

Using an RA Certificate on HSM

If you use an RA Certificate already configured with your Enterprise Gateway on your HSM, you must follow these steps. Follow these steps to configure the same certificate to both your key escrow and recovery service.

1. Run ckdemo.
2. After your session begins and you log in, option 21 lets you copy your private keys.
3. Find the handle of the key (the private key of the RA Certificate) and enter that handle as the object to copy. Choose (1)Add Attribute and Select 3 CKA_LABEL to edit the template. You need to specify a new label, which is unique from the other objects in the partition. For example, if the ksp container name is "kspkeys", copy the private key as "kspkeysJava". The alias is important to complete the next step. Then Choose (0) Accept Template and EXIT/Quit
4. Import the certificate with cmu. The certificates should be imported in proper Java Certificate chain order. The certificate for the private key comes first and then signer certificates follow in the chain.
5. The certificate for the private key should be given the alias from #2 with "--cert0" appended. For example, with the private key kspkeysJava:

- The certificate would have the alias kspkeysJava--cert0.
- The intermediate certificate would have the alias kspkeysJava--cert1, and the root certificate would have the alias kspkeysJava--cert2.
- If there were no intermediate certificates, then the root would have the alias kspkeysJava--cert1.
- If the certificate was self-signed, then there would only be a "kspkeysJava--cert0".

6. The arguments for cmu for importing certificates in this scenario are:

```
cmu import -label <myLabel> -inputfile <certFile>
```

Refer to *"DigiCert PKI Platform Web Services Developers Guide"* for instructions on how to import the CAs to the Java keystore file.

Obtaining an RA Certificate to Store in a Java Keystore File

Complete the following steps if you have implemented the key escrow and recovery service and store your RA certificate in a software-based Java keystore. These procedures require the Java keytool to generate the keys and import them into your keystore.

DigiCert recommends that you use strong passwords. Use six or more characters with a mixture of numbers and upper-case and lower-case letters. Store your passwords in a secure location.

1. Generate a key pair as follows:

   ```
   keytool -genkey -alias pki_ra -keyalg RSA -keysize 2048 -sigalg SHA256withRSA
   -dname "O=<company>, OU=<dept>, CN=<common name>"
   -validity 365 -keypass <password> -keystore <keystore name>
   -storepass <password>
   ```

2. Generate a CSR as follows:

   ```
   keytool -certreq -alias pki_ra -sigalg SHA256withRSA -file
   racertificate.req -keypass <password> -keystore <keystore name>
   -storepass <password>
   ```

3. Copy the racertificate.req to the computer that has access to the PKI Manager.

   - Open racertificate.req in a text editor and copy the contents of the file into your Clipboard.
   - Access PKI Manager and select **Set up your account > Get an RA certificate**.
   - Paste the contents of your Clipboard in to the request field. Click **Submit**.
   - When you are prompted, download the resulting .p7certificate file.

4. Save the cert.p7b file to a temporary location.
5. Import the certificate into your keystore by using the following command:

   ```
   keytool -import -alias pki_ra -file cert.p7b -noprompt -keypass
   <password> -keystore <keystore name> -storepass <password>
   ```

6. You need the root CA for the RA certificate in your truststore. They can be found in the web page at https://knowledge.digicert.com/solution/ca-hierarchies-for-production-and-test-drive-ra-certificates.html. You can import these CAs into your truststore.

Refer to "*DigiCert PKI Platform Web Services Developers Guide*" for instructions on how to import the CAs to the Java keystore file.

CHAPTER 3

3 Installing PKI Enterprise Gateway

This chapter includes the following topics:

- Deployment Modes
- Required Administrator Permission
- Installing PKI Enterprise Gateway
- Post-installation Procedures
- Uninstalling PKI Enterprise Gateway

3.1 Deployment Modes

You can install PKI Enterprise Gateway on a single server or on multiple servers:

- Install PKI Enterprise Gateway on a single server if your users are within your network domain.
- Install PKI Enterprise Gateway on multiple servers if some of your users are not joined to a domain.

3.2 Required Administrator Permission

3.2.1 Required Administrator Permission for Active Directory User Store

If your user store is on Active Directory, one of following is required to perform a full installation:

- Built-in Enterprise Administrator of the root domain.
- User member of both "Domain Admins" Group for the root domain and Local "Administrators" Group of the server machine.

But the installer provides an option to install without the above privilege by skipping the changes required to be performed to Active Directory. If you chose to skip this step, required permission drops to at least Local Administrator privilege of the server machine. This step can be performed by user with higher privilege described above later.

User with Local Administrator privilege can be either one of following:

- Built-in Local Administrator.
- User in Local "Administrators" Group (installer will ask for elevated privilege after executing the installer).

See "3.3 Installing PKI Enterprise Gateway", step 19 for details about switching the option.

See "3.4 Running triggerADChanges.vbs" for details about the script required to run after the installation has finished while skipping Active Directory changes.

NOTE: This option is especially useful in the case of performing an installation to multiple servers, where you will be only required to call user with higher permission only once during the deployment.

3.2.2 Required Administrator Permission for LDAP User Store

If your user store is on LDAP, it is required that user performing the installation have at least Local Administrator privilege of the server machine.

User with Local Administrator privilege can be either one of following:

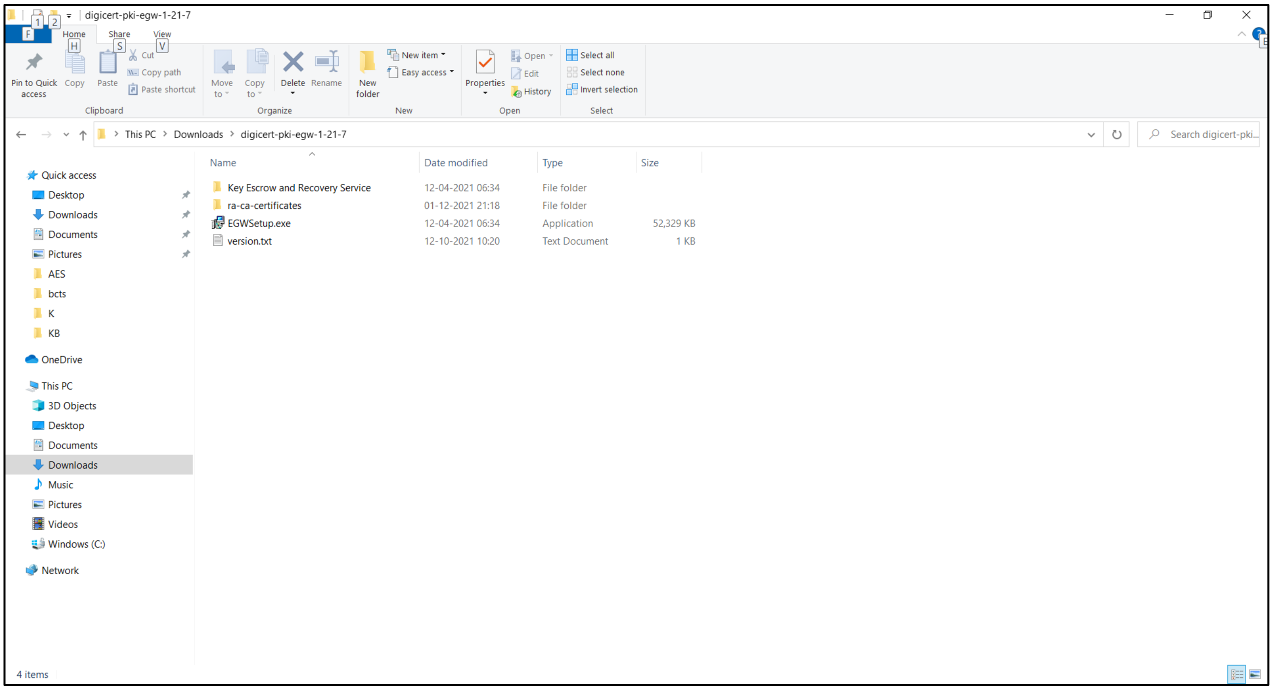
- Built-in Local Administrator.
- User in Local "Administrators" Group (installer will ask for elevated privilege after executing the installer).

3.3 Installing PKI Enterprise Gateway

Complete the following general steps to install PKI Enterprise Gateway. Refer to the sections that are listed for detailed procedures.

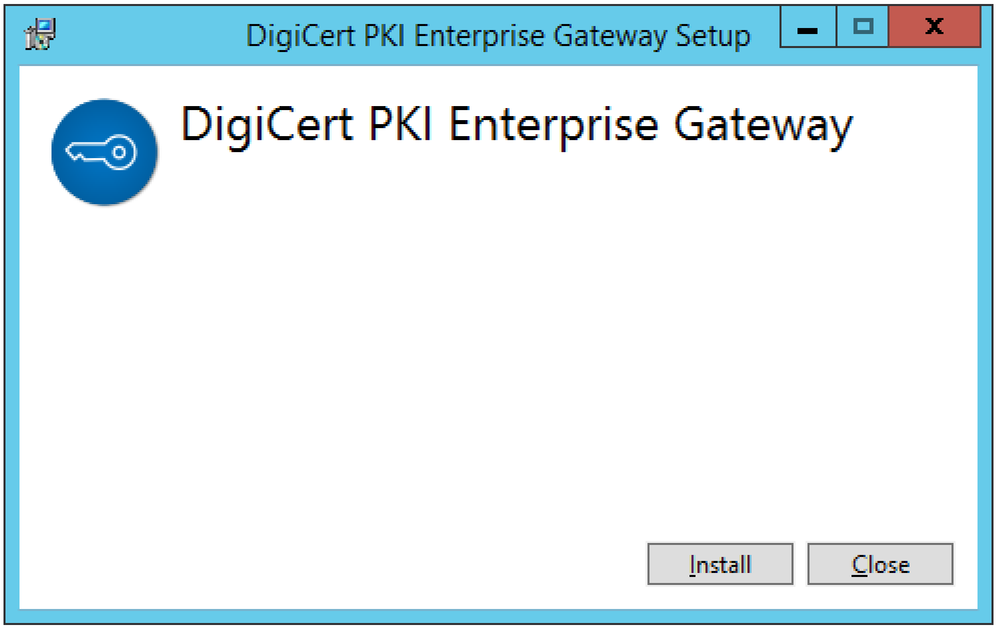
NOTE: Before running the installer for an LDAP SSL connection over a 636 port, you must trust the server CA on the PKI Enterprise Gateway computer.

1. Obtain and install an RA Certificate.
2. Obtain the PKI Enterprise Gateway package from the **Resources** page of PKI Manager.
3. Obtain the PKI Enterprise Gateway documents from the link '**DigiCert PKI Enterprise Gateway & Autoenrollment Server Deployment Guides (External Link)**' from the Resources page of PKI Manager.
4. Unzip the PKI Enterprise Gateway package into a temporary location on the computer.
5. As a user with administrator rights to the local computer, run **`EGWSetup.exe`** from the temporary location. The exact options you provide depend on how you deploy PKI Enterprise Gateway.



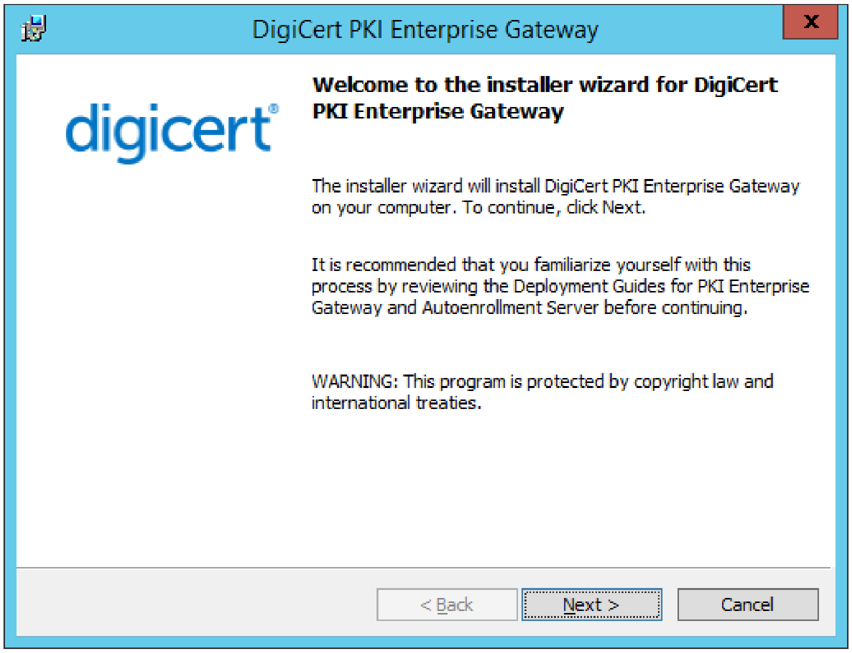
Name	Date modified	Type	Size
Key Escrow and Recovery Service	12-04-2021 06:34	File folder	
ra-ca-certificates	01-12-2021 21:18	File folder	
EGWSetup.exe	12-04-2021 06:34	Application	52,329 KB
version.txt	12-10-2021 10:20	Text Document	1 KB

6. Click **Install**.


DigiCert PKI Enterprise Gateway Setup
DigiCert PKI Enterprise Gateway
Install
Close

NOTE: If .Net Framework 4.7.1 is not installed in your system, the PKI Enterprise Gateway installer will automatically retrieve and install it from the internet. If there is no internet connection, obtain .Net Framework 4.7.1 from Microsoft and install it before continuing.

7. Click **Next**.



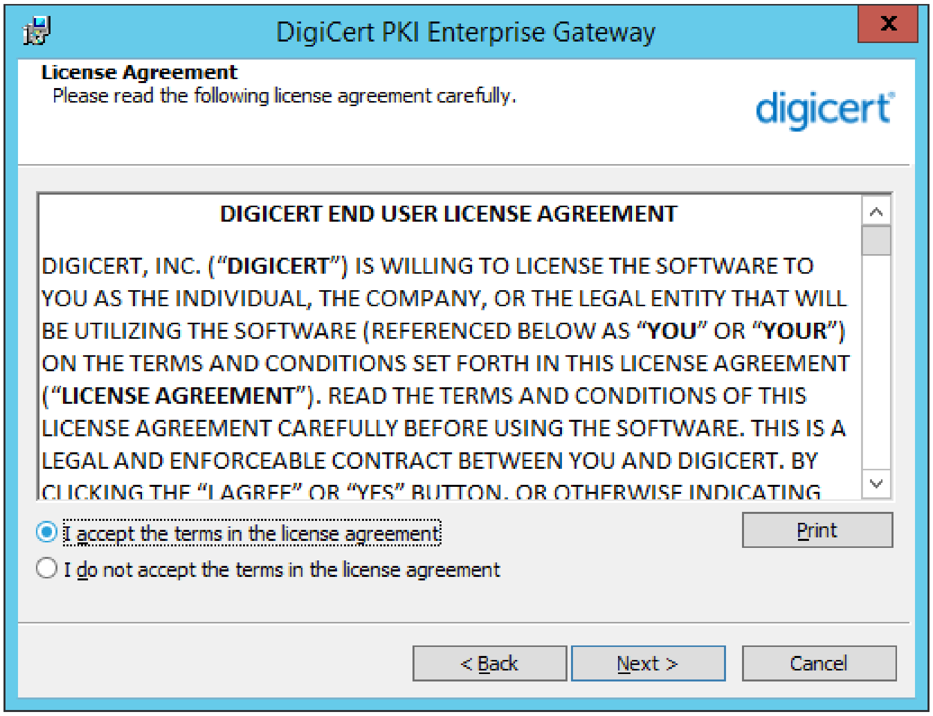
Welcome to the installer wizard for DigiCert PKI Enterprise Gateway

The installer wizard will install DigiCert PKI Enterprise Gateway on your computer. To continue, click Next.

It is recommended that you familiarize yourself with this process by reviewing the Deployment Guides for PKI Enterprise Gateway and Autoenrollment Server before continuing.

WARNING: This program is protected by copyright law and international treaties.

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



License Agreement

Please read the following license agreement carefully.

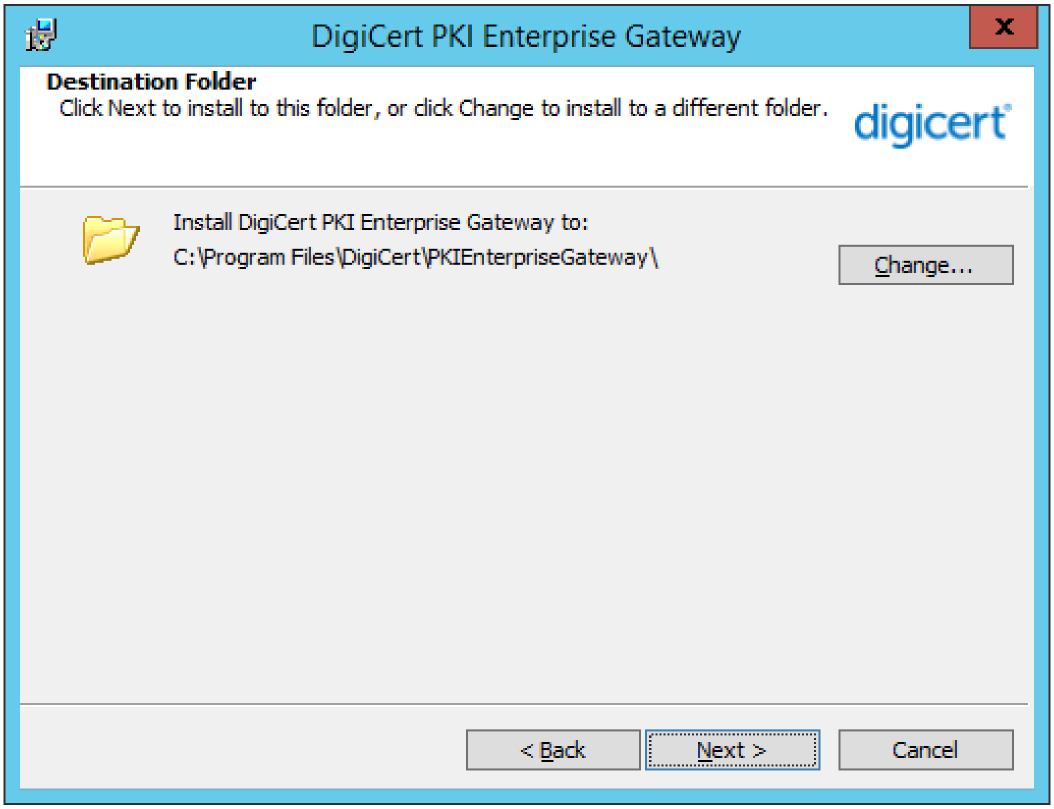
DIGICERT END USER LICENSE AGREEMENT

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 BETWEEN YOU AND DIGICERT. BY CLICKING THE "I AGREE" OR "YES" BUTTON, OR OTHERWISE INDICATING

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

9. Click **Change** to select the destination folder, and then click **Next**.



DigiCert PKI Enterprise Gateway

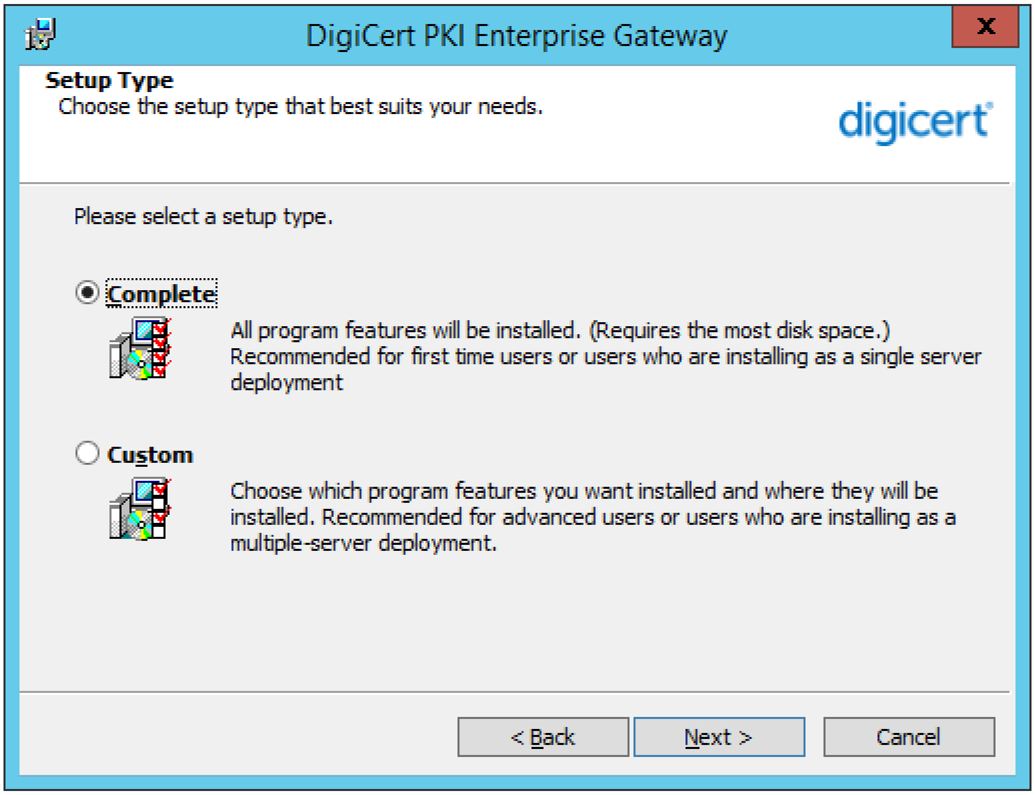
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install DigiCert PKI Enterprise Gateway to:
C:\Program Files\DigiCert\PKIEnterpriseGateway\

NOTE: The default location is "C:\Program Files\DigiCert".

10. The **Setup Type** window appears.



DigiCert PKI Enterprise Gateway

Setup Type
Choose the setup type that best suits your needs.

Please select a setup type.

● **Complete**

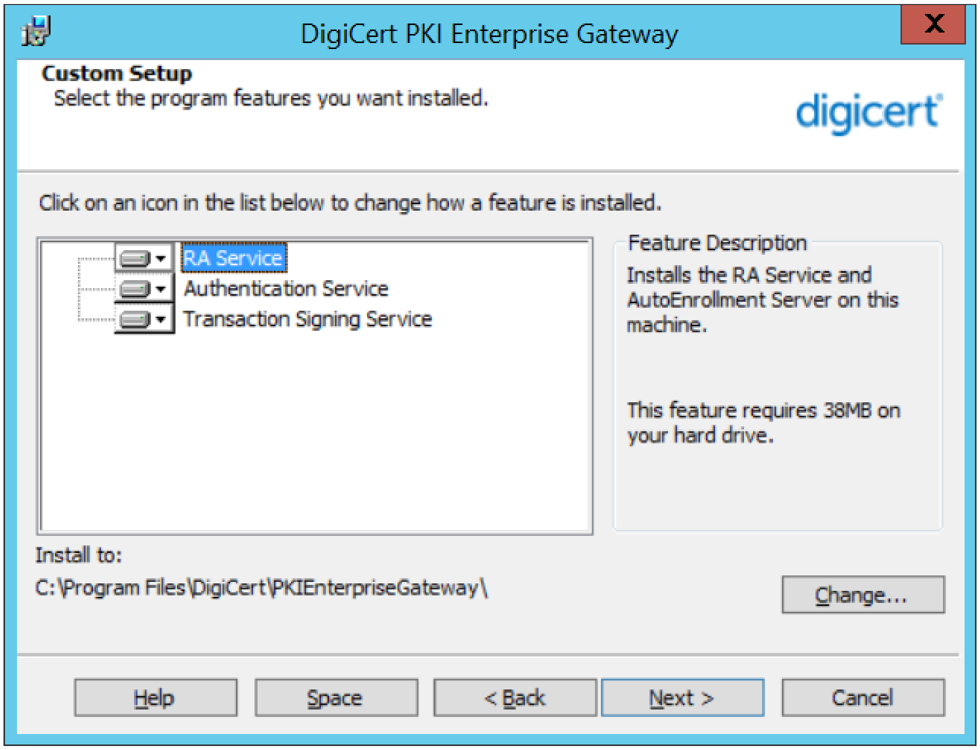
All program features will be installed. (Requires the most disk space.) Recommended for first time users or users who are installing as a single server deployment

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users or users who are installing as a multiple-server deployment.

- Choose **Complete** for a single-server deployment
- Choose **Custom** to install PKI Enterprise Gateway as a multiple-server deployment where you can set up authentication service and RA Service on different computers. For Custom deployments, ensure:
  - If you select **Active Directory** for the User Type, all servers are in the same forest.
  - If your user certificates are stored in PKI Client, the PKI Client is able to communicate with the RA Service on the back end. You may choose to install a proxy forwarder in your DMZ.

11. If you selected a **Custom** installation, the **Custom Setup** window opens. Select the feature or combination of features that you want to install.



DigiCert PKI Enterprise Gateway

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- RA Service
- Authentication Service
- Transaction Signing Service

Feature Description

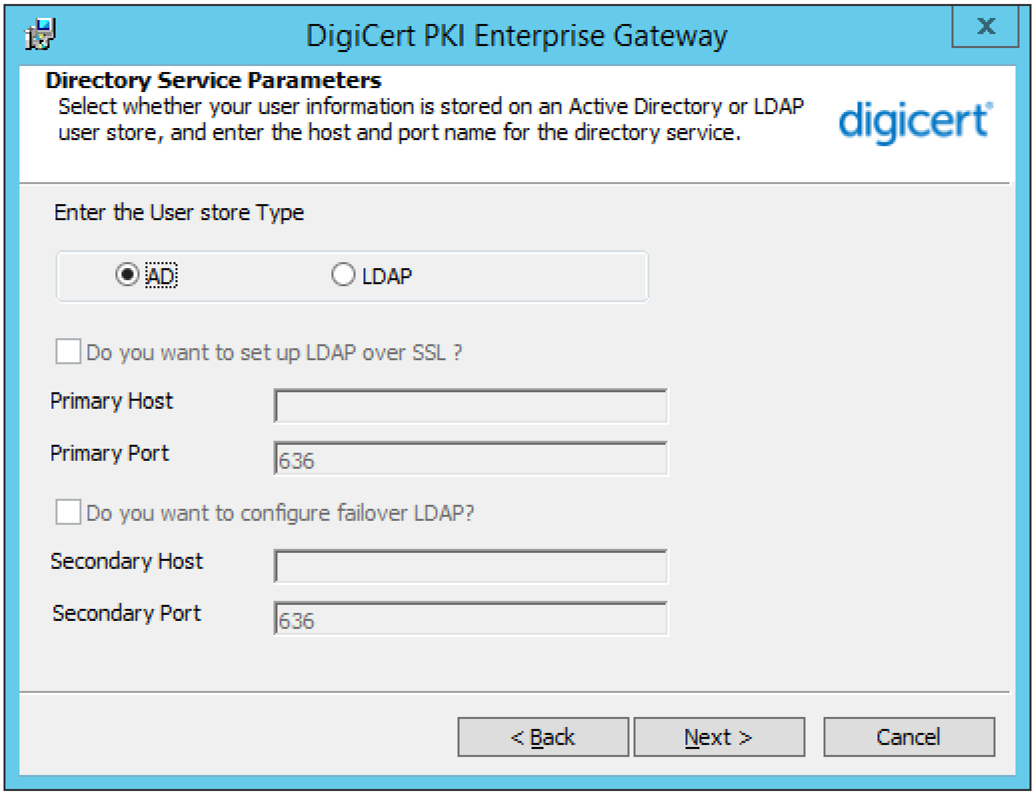
Installs the RA Service and AutoEnrollment Server on this machine.

This feature requires 38MB on your hard drive.

Install to:

C:\Program Files\DigiCert\PKIEnterpriseGateway\

12. The **Directory Service Parameters** window appears. Complete the following and click **Next**.



DigiCert PKI Enterprise Gateway

Directory Service Parameters

Select whether your user information is stored on an Active Directory or LDAP user store, and enter the host and port name for the directory service.

Enter the User store Type

● AD ○ LDAP

□ Do you want to set up LDAP over SSL ?

Primary Host

Primary Port 636

□ Do you want to configure failover LDAP?

Secondary Host

Secondary Port 636

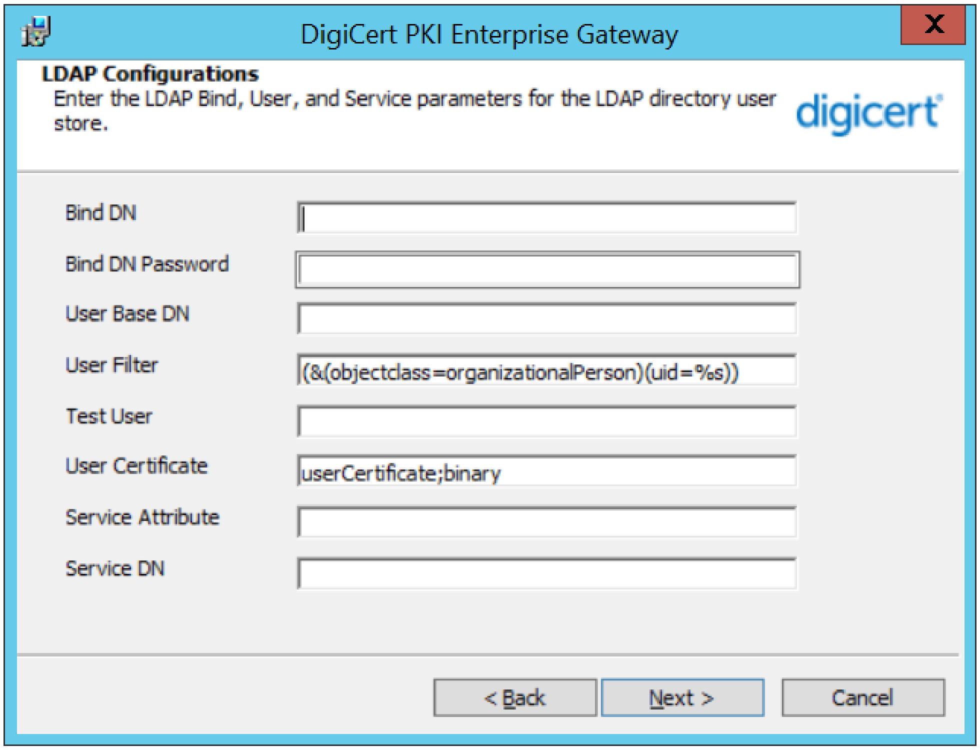
- Choose **AD** if your user information is stored on an Active Directory.
- Choose **LDAP** if your user information is stored on another LDAP directory. Also provide the following:

  - **Primary Host**. Host name or the IP of the computer that hosts the LDAP server
  - **Primary Port**. Port on which the LDAP directory listens.

  If you configure failover LDAP, select the check box and fill in the **Secondary Host** and **Secondary Port**.

- Choose **Do you want to set up LDAP over SSL?** to configure the Enterprise Gateway to communicate to the LDAP over a secure SSL connection.

13. If you selected **LDAP** as the User Type, the **LDAP Configurations** window appears. The following table describes the fields you must complete in this window.



DigiCert PKI Enterprise Gateway

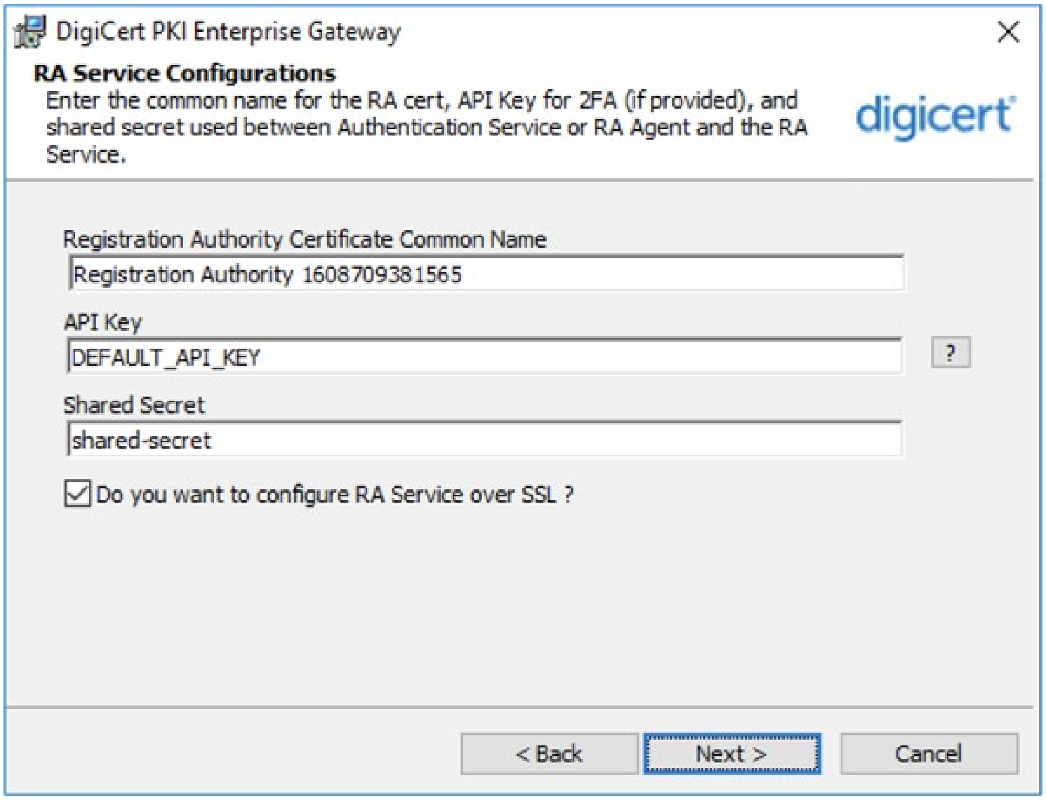
LDAP Configurations

Enter the LDAP Bind, User, and Service parameters for the LDAP directory user store.

Bind DN	
Bind DN Password	
User Base DN	
User Filter	(&(objectclass=organizationalPerson)(uid=%s))
Test User	
User Certificate	userCertificate;binary
Service Attribute	
Service DN	

Attributes	Description
Bind DN	The full Distinguished Name of a user with enough privileges to write updates to the LDAP user store (usually an administrator user)
Bind DN Password	The password for the bind user DN account.
User Base DN	The field where you start searching for the user information in LDAP. Example: DC=acme, DC=COM
User Filter	The LDAP user store filter for restricting access to users. Example: (&(UID=%s)(objectclass=organizationalPerson))
Test User	An existing user ID to verify that the Bind User has the correct write permissions.
User Certificate	Attribute where user certificates are published, if configured to do so.
Service Attribute	Any Octet attribute that is accessible to the bind user. After the encryption key value is populated, the object should not be deleted. If it is deleted, the PKI Enterprise Gateway can no longer use the data in the user store. This attribute stores the service key for PKI Enterprise Gateway.
Service DN	Any LDAP object that is accessible by the bind user. PKI Enterprise Gateway uses this object to save the encryption key that was created during the installation process (the key is used to encrypt communications with DigiCert PKI Platform). Once the encryption key value is populated, the object should not be deleted, or PKI Enterprise Gateway cannot use the data in the user store.

14. For Complete installations, or if you selected to install the RA Service as part of a Custom installation, the **RA Service Configuration** window appears. The following table describes the fields you must complete in this window.



DigiCert PKI Enterprise Gateway

RA Service Configurations

Enter the common name for the RA cert, API Key for 2FA (if provided), and shared secret used between Authentication Service or RA Agent and the RA Service.

Registration Authority Certificate Common Name: Registration Authority 1608709381565

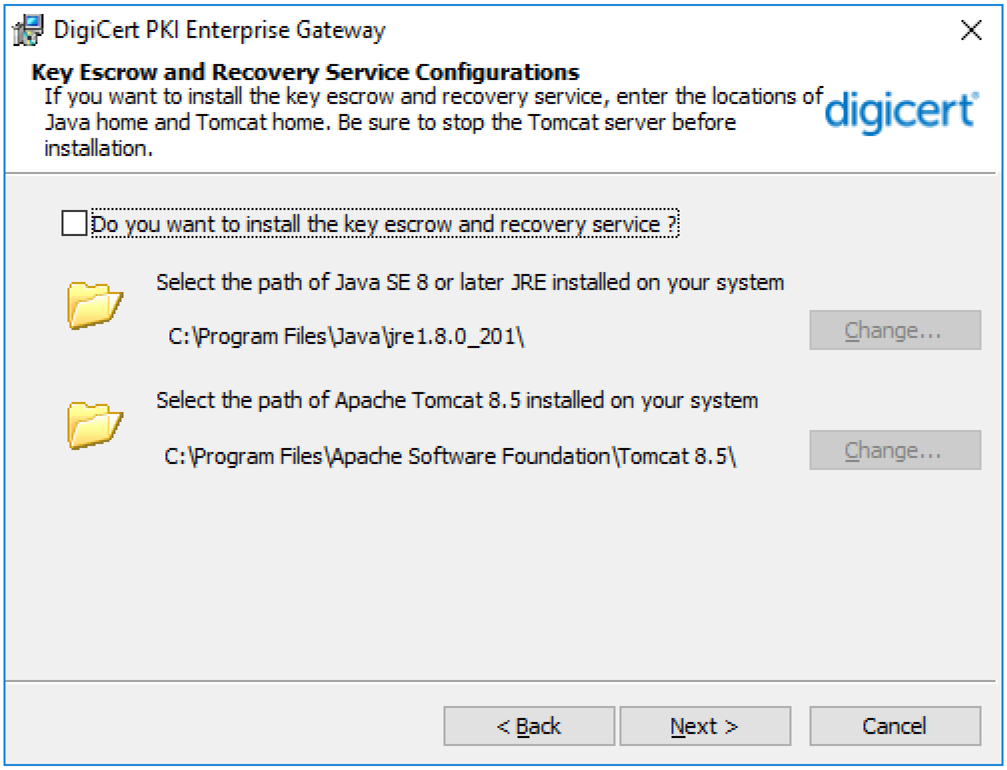
API Key: DEFAULT_API_KEY

Shared Secret: shared-secret

☑ Do you want to configure RA Service over SSL ?

Attributes	Description
Registration Authority Certificate Common Name	Common Name of the Subject DN for the RA certificate. To obtain this value, open MMC and click on **Certificates (Local Computer) > Personal > Certificates**. To change this information after installation, see "Modifying the Subject Name of the RA Certificate".
API Key	API Key used for two factor authorization to submit requests to DigiCert. If API Key was provided with RA certificate, enter that value. Otherwise leave it as the pre-populated "DEFAULT_API_KEY". To change this information after installation, see "Updating Encrypted Settings".
Shared Secret	The "shared secret" is used between the RA Service and the authentication service or RA Agent (from 1 to 30 alpha-numeric characters). To change this information after installation, see "Updating Encrypted Settings". For multiple server deployments, you must use the same shared secret for the RA Service and authentication services.
Do you want to configure RA Service over SSL?	By selecting this option, the Enterprise Gateway communicates with the RA service over a secure SSL connection.

15. For Complete installations, or if you select to install the key escrow and recovery service as part of a custom installation, the **Key Escrow and Recovery Service Configurations** window appears. The following table describes the paths you will need to provide in this window.



DigiCert PKI Enterprise Gateway

Key Escrow and Recovery Service Configurations

If you want to install the key escrow and recovery service, enter the locations of Java home and Tomcat home. Be sure to stop the Tomcat server before installation.

□ Do you want to install the key escrow and recovery service ?

Select the path of Java SE 8 or later JRE installed on your system

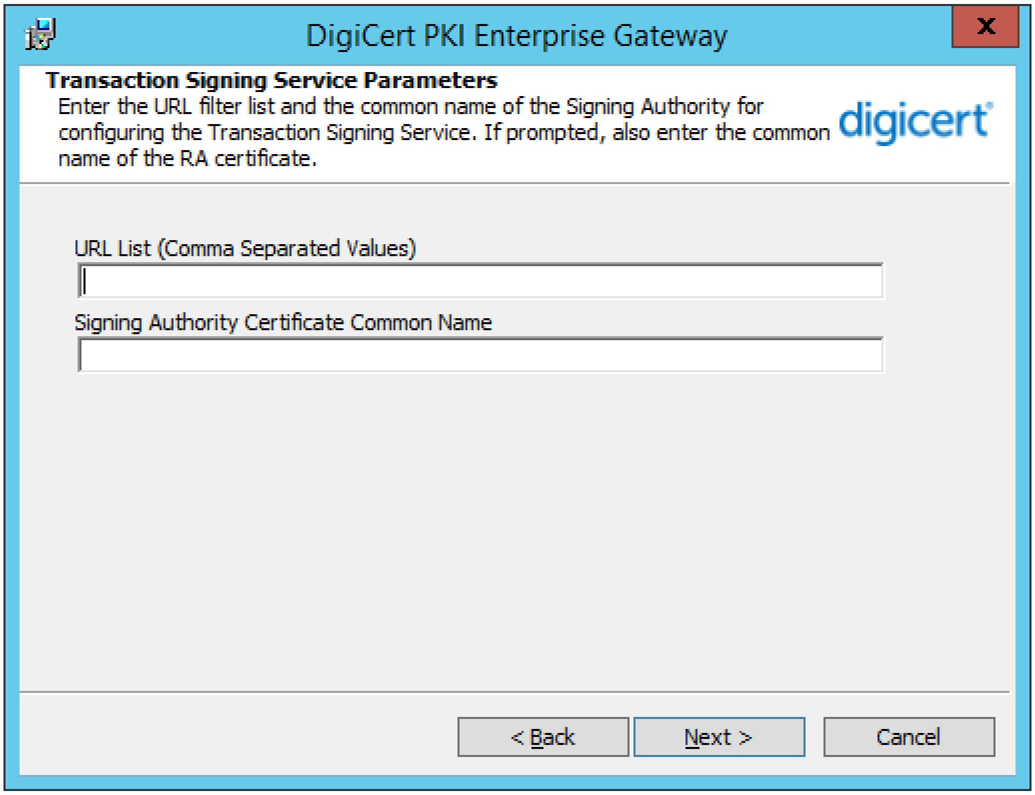
C:\Program Files\Java\jre1.8.0_201\

Select the path of Apache Tomcat 8.5 installed on your system

C:\Program Files\Apache Software Foundation\Tomcat 8.5\

Attributes	Description
Do you want to install the key escrow and recovery service?	The check box selection to install the optional key escrow and recovery service.
Select the path of Java SE 8/ Oracle OpenJDK 8 (Java Runtime Environment) or later SE installed on your system	The location where you have installed Java on the server (Java home).
Select the path of Apache Tomcat 8.5 installed on your system	The location where you have installed Tomcat on the server (Tomcat home).

16. For Complete installations, or if you selected to install the Transaction Signing Service as part of a Custom installation, the **Transaction Signing Service Parameters** window appears. The following table describes the fields you must complete in this window.



DigiCert PKI Enterprise Gateway

Transaction Signing Service Parameters

Enter the URL filter list and the common name of the Signing Authority for configuring the Transaction Signing Service. If prompted, also enter the common name of the RA certificate.

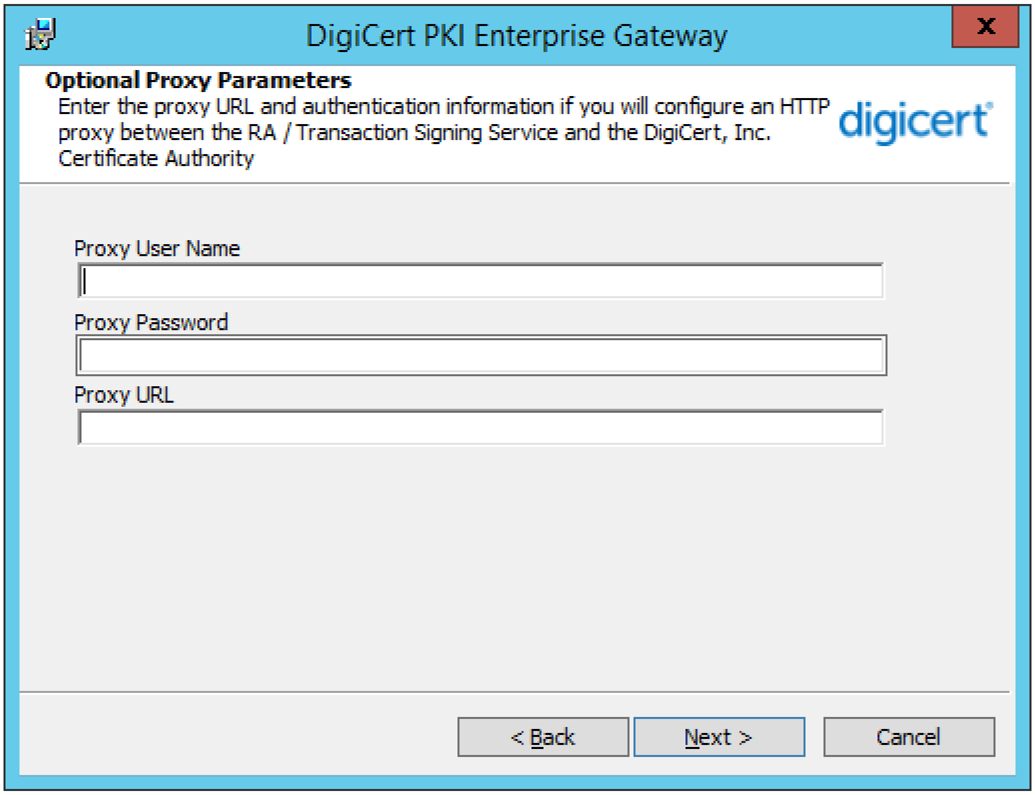
URL List (Comma Separated Values)

Signing Authority Certificate Common Name

Attributes	Description
URL List	Specifies the list of URLs from which your web application can expect to receive the VerifySignedData response. The URLs must be in ASCII text. Use commas to separate multiple URLs.
Signing Authority Certificate Common Name	Common Name of the Signing Authority Certificate. To obtain this value, open MMC and click on **Certificates (Local Computer) > Personal > Certificates**.

17. For Complete installations, or if you selected to install the RA Service or the Transaction Signing Service, the **Optional Proxy Parameters** window appears.

    Complete this window only if you intend to configure an HTTP proxy between the RA /Transaction Signing Service and the DigiCert Certificate Authority. The following table describes the fields you complete in this window.



Optional Proxy Parameters

Enter the proxy URL and authentication information if you will configure an HTTP proxy between the RA / Transaction Signing Service and the DigiCert, Inc. Certificate Authority

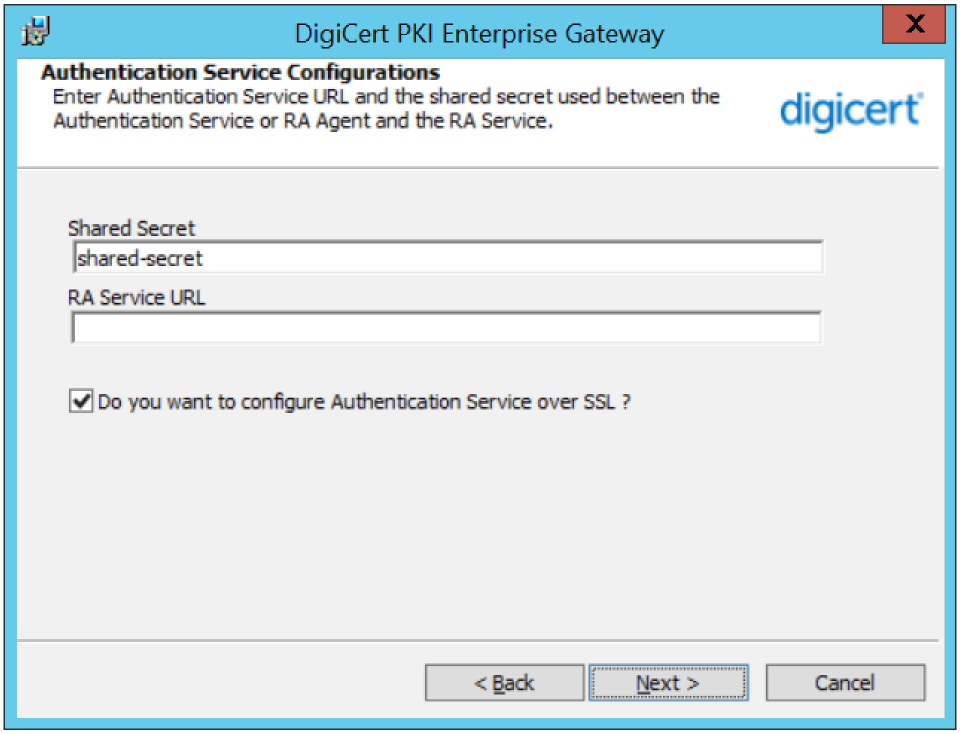
Proxy User Name

Proxy Password

Proxy URL

Attributes	Description
Proxy user name	(Optional) Proxy user name if an HTTP proxy is configured. See "Modifying Proxy Settings".
Proxy Password	(Optional) Proxy password if an HTTP proxy is configured. See "Modifying Proxy Settings".
Proxy URL	(Optional) Proxy URL if an HTTP proxy is configured. See "Modifying Proxy Settings".

18. If you selected to install the authentication service and did not select to install the RA Service, the **Authentication Service Configuration** window appears. The following table describes the fields you must complete in this window.



Authentication Service Configurations

Enter Authentication Service URL and the shared secret used between the Authentication Service or RA Agent and the RA Service.

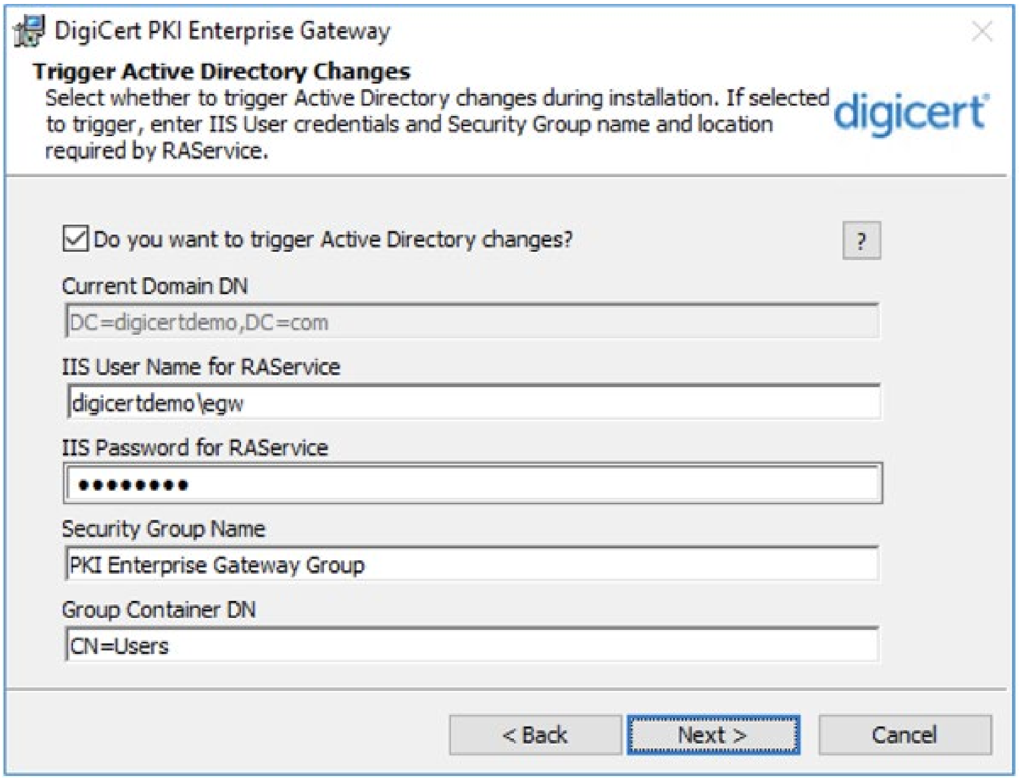
Shared Secret: shared-secret

RA Service URL:

☑ Do you want to configure Authentication Service over SSL ?

Attributes	Description
Shared Secret	"Shared secret" that is used between the RA Service and the authentication service or RA Agent (from 1 to 30 alpha-numeric characters). To change this secret manually, See "Updating Encrypted Settings". For multiple server deployments, you must use the same shared secret for the RA Service and authentication services.
RA Service URL	Lets you specify the URL for the RA Service application. This option is only applicable for multiple-server deployments.
Do you want to configure authentication service over SSL?	By selecting this option, the Enterprise Gateway communicates with the Authentication service over a secure SSL connection.

19. For Complete installations, or if you selected to install the RA Service as part of a Custom installation, and if you selected **AD** in **Directory Service Parameters** window, the **Trigger Active Directory Changes** window appears.



DigiCert PKI Enterprise Gateway

Trigger Active Directory Changes

Select whether to trigger Active Directory changes during installation. If selected to trigger, enter IIS User credentials and Security Group name and location required by RAService.

☑ Do you want to trigger Active Directory changes?

Current Domain DN: DC=digicertdemo,DC=com

IIS User Name for RAService: digicertdemo\egw

IIS Password for RAService: ●●●●●●●●●

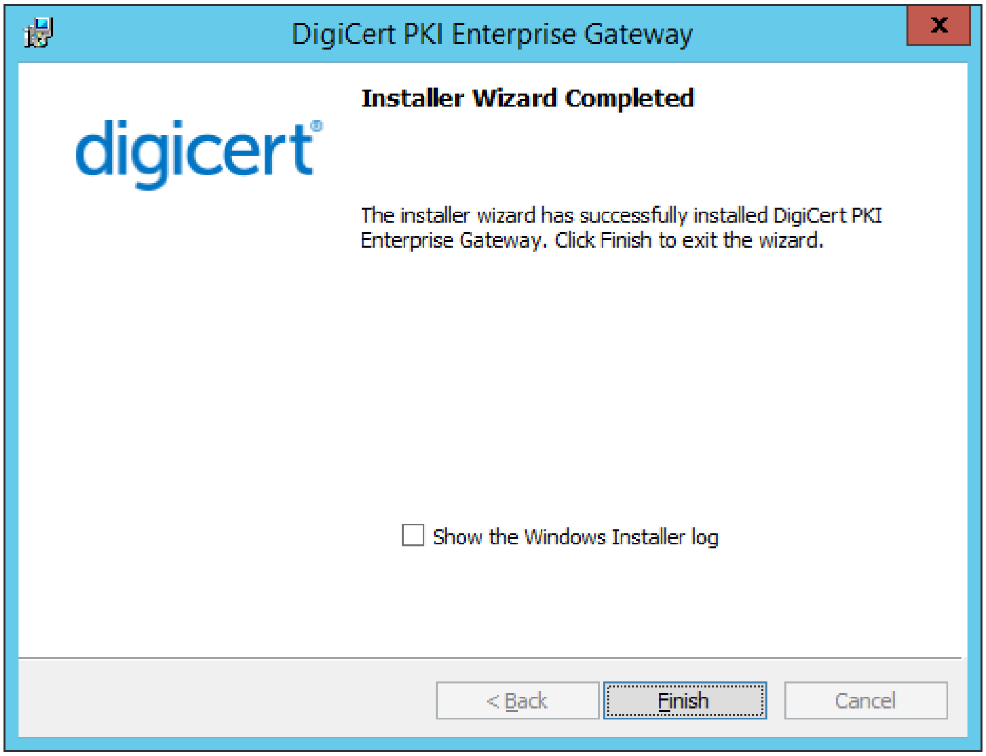
Security Group Name: PKI Enterprise Gateway Group

Group Container DN: CN=Users

Attributes	Description
Do you want to trigger Active Directory changes?	The check box selection to trigger Active Directory changes. If you select this checkbox, it is required that the user has enough privilege to execute the changes. See "3.2.1 Required Administrator Permission for Active Directory User Store " for details about the privilege.
Current Domain DN	Distinguished name of the domain where the user is currently logged into. If there is no distinguished name shown, it indicates that the user executing the installer is not logged into a domain.
IIS User Name for RAService	Domain user's log-on name for the IIS computer running the RA Service (required to run the RA Service). The format must

	be domain\UID. Maximum length allowed is 40, and any character in UTF-8 is allowed. To change this information after installation, see “Updating the Windows User Name and Password (Connectivity Pool Information)”.
IIS Password for RAService	Domain user logon password for the IIS computer running the RA Service. Maximum length allowed is 40, and any character in UTF-8 is allowed. To change this information after installation, see “Updating the Windows User Name and Password (Connectivity Pool Information)”.
Security Group Name	The name of security group which is created by the installer. Default is **PKI Enterprise Gateway Group**. This group will have permission to publish certificates to the domains where users enroll for certificates. Also, user specified in **IIS User Name for RAService** will be set as a member of this group during the installation. Maximum length allowed is 40 and any character allowed for Active Directory security group.
Group Container DN	Distinguished name relative to current logged in domain, where the group specified in **Security Group Name** will be created. Default is set as 'CN=Users'. This needs to be in proper distinguished name format and needs to exist in current domain. Maximum length allowed is 100.

20. Click **Finish**.



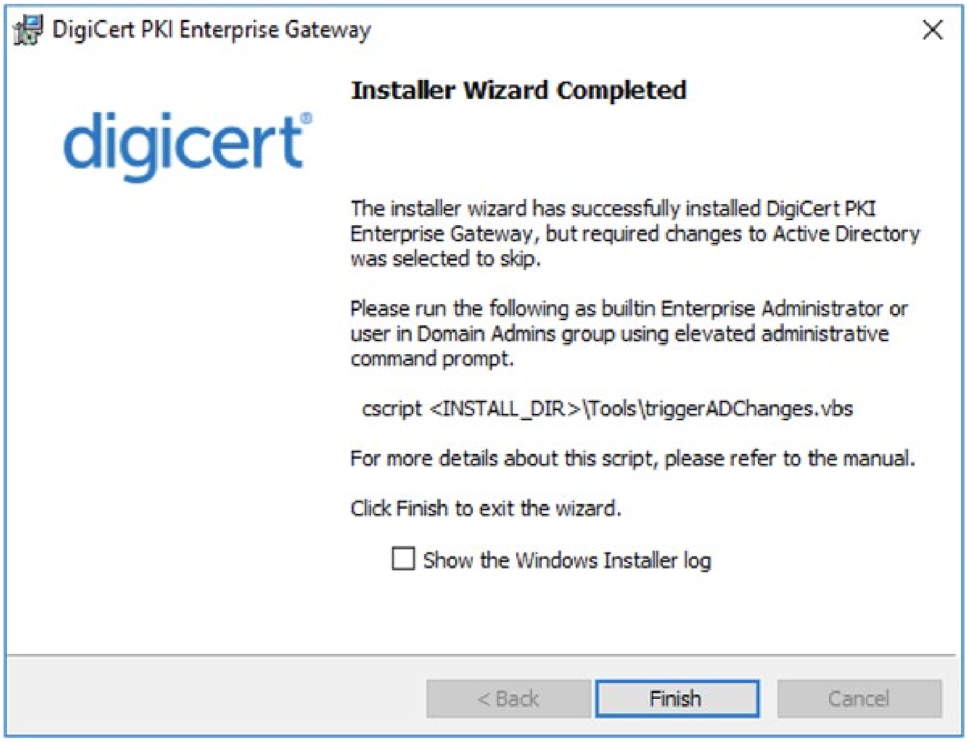
DigiCert PKI Enterprise Gateway

Installer Wizard Completed

The installer wizard has successfully installed DigiCert PKI Enterprise Gateway. Click Finish to exit the wizard.

□ Show the Windows Installer log

NOTE: Following window appears if you unchecked the Do you want to trigger Active Directory changes? checkbox at Trigger Active Directory Changes window.



DigiCert PKI Enterprise Gateway

Installer Wizard Completed

The installer wizard has successfully installed DigiCert PKI Enterprise Gateway, but required changes to Active Directory was selected to skip.

Please run the following as builtin Enterprise Administrator or user in Domain Admins group using elevated administrative command prompt.

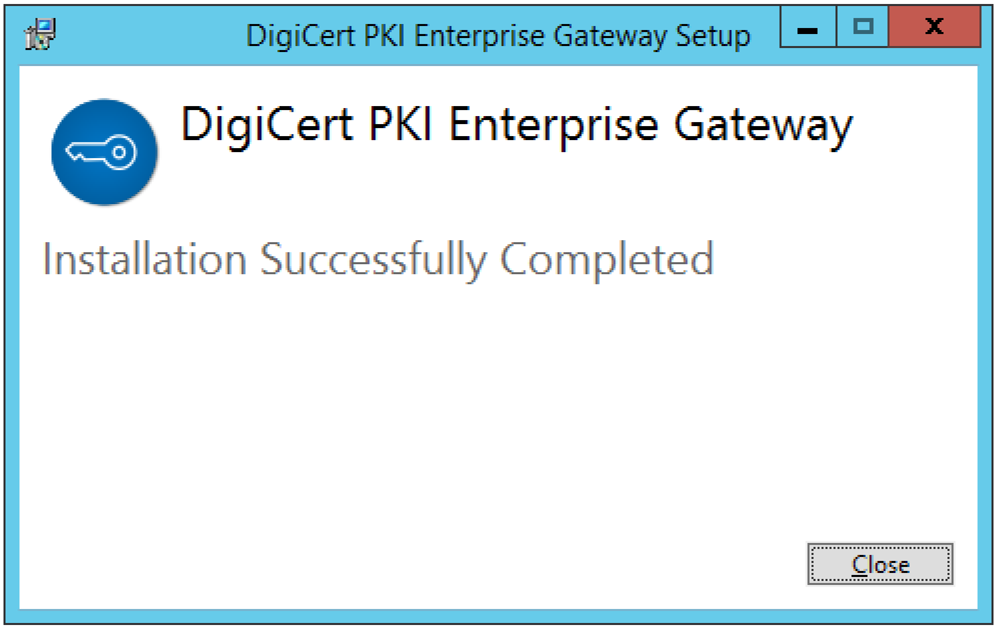
```
cscript <INSTALL_DIR>\Tools\triggerADChanges.vbs
```

For more details about this script, please refer to the manual.

Click Finish to exit the wizard.

□ Show the Windows Installer log

21. Click **Close**.



DigiCert PKI Enterprise Gateway Setup

DigiCert PKI Enterprise Gateway

Installation Successfully Completed

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

22. After you have installed PKI Enterprise Gateway, you must configure the implementation, including:

- Securing communications between your client applications and the gateway. See "Configuring SSL".
- Configuring PKI Manager to recognize PKI Enterprise Gateway and to identify the user groups to which you deploy digital certificates. See "Configuring PKI Manager to Recognize PKI Enterprise Gateway".
- Configuring HTTP proxy access (if needed). See "Modifying Proxy Settings"
  .

23. Test your deployment. See "(Optional) Configuring the Key Escrow and Recovery Service".

3.4 Running triggerADChanges.vbs

3.4.1 When is triggerADChanges.vbs required?

This script only applies when User Store is Active Directory. Also, it is required to run only if you unchecked the **Do you want to trigger Active Directory changes?** checkbox at **Trigger Active Directory Changes** window during the installation.

NOTE: If this script has been already run in another server for multi-server deployment, you do not have to run this script. Instead, it is required that you configure the RAService application pool identity manually. See "Updating the Windows User Name and Password (Connectivity Pool Information)".

3.4.2 What is triggerADChanges.vbs?

PKI Enterprise Gateway requires the following to operate properly:

- Security group with permission to publish certificates to the domains where users enroll for certificates
- ServiceConnectionPoint in root domain to store the Service Key used during enrollment operation

This script **triggerADChanges.vbs** creates the above objects in your Active Directory domain, enabling certificate operation to run properly. Also, it sets user as RAService pool identity if specified, and adds the user to the created security group.

3.4.3 Permission Requirement for triggerADChanges.vbs

One of following user is required to run the script:

- Built-in Enterprise Administrator of the root domain.
- User member of both "Domain Admins" Group for the root domain and Local "Administrators" Group of the server machine.

3.4.4 How to Run triggerADChanges.vbs

This utility is available in the <install_dir>\Tools directory.

Open the command prompt with elevated privilege. To open the elevated command prompt, follow the direction below:

1. Click Start.
2. In the search box, type **cmd**.

3. Right-click on **cmd**.exe and choose **Run as Administrator**. If done properly, the **User Account Control** window opens.
4. Click **Yes** to run the Windows Command Prompt as Administrator.

From the elevated command prompt, run the following command:

```
cscript triggerADChanges.vbs [options]
```

This script takes the following options:

- **[groupname:<groupname>]** The name of security group, which is required by RAService for certificate management. If omitted, default 'PKI Enterprise Gateway Group' is used.
- **[groupcontainerdn:<groupcontainerdn>]** The container where the group is created. Specify without domain DN. If omitted, default 'cn=Users' is used.
- **[iisuser:<iisuser>]** Specify account for RAService pool identity. The script will assign the security group to the specified user. Also, it will set the specifed user as RAService pool identity. Must be in NetBIOS format using backslash '\'. iispass is required when specifed. If omitted, will skip assigning user to the group.
- **[iispass:<iispass>]** Specify password for account entered for iisuser. iisuser is required when specifed.

Example:

```
cscript triggerADChanges.vbs groupname:”PKI Group” groupcontainerdn:”CN=PKI
Container” iisuser:acme\admin iispass:password
```

3.5 Post-installation Procedures

The installer writes Summary files containing information about the components it installed. The Summary files contain information that you will need when installing other components. You will also need the Summary files and multiple-server deployments when you configure PKI Manager to recognize the gateway. The files are written to the %PUBLIC% folder.

After installing PKI Enterprise Gateway, you may need to configure the associated components and options:

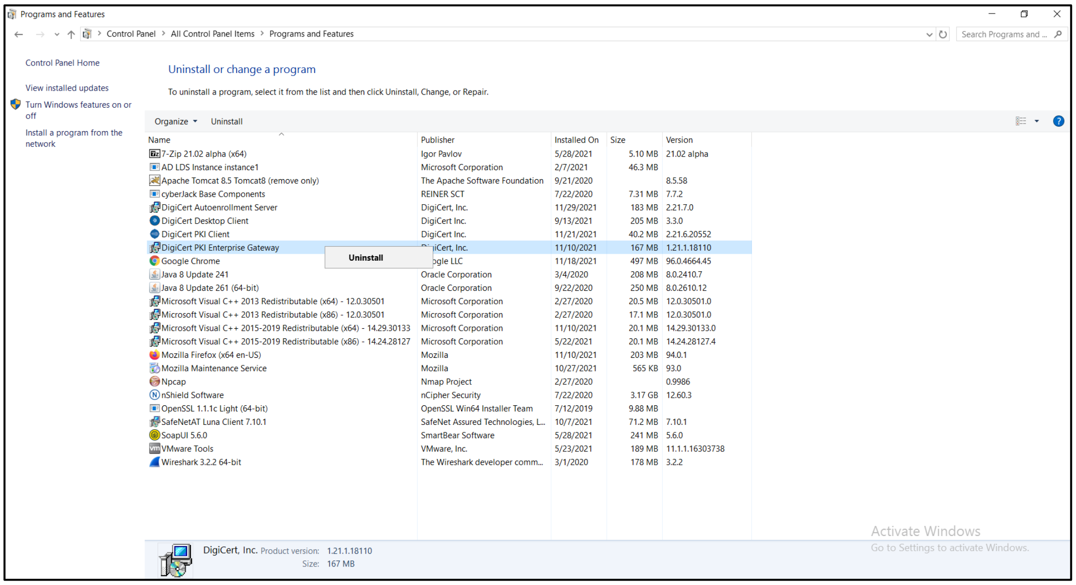
- If you have configured an HTTP proxy, you can manually edit the RA Service web.config file to add the proxy URL. See “Modifying Proxy Settings” .
- If you have enabled SSL, you must configure PKI Enterprise Gateway for SSL. See “Configuring SSL”.
- If you want to configure your PKI Enterprise Gateway for high availability. See “Configuring PKI Enterprise Gateway”.

3.6 Uninstalling PKI Enterprise Gateway

To uninstall the PKI Enterprise Gateway, perform the following steps:

1. Do one of the following:

   - Run **EGWSetup.exe**.
   - Go to **Control Panel > Program and Features**, right-click **DigiCert PKI Enterprise Gateway**, and then click **Uninstall**.

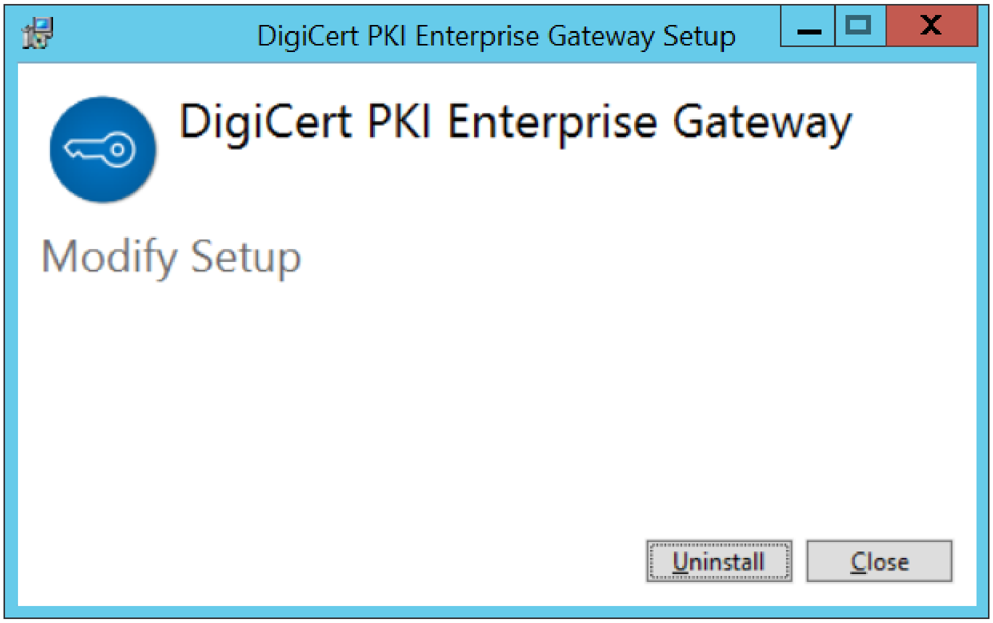

Programs and Features
Control Panel > All Control Panel Items > Programs and Features
Search Programs and ...
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Uninstall or change a program
Organize
Uninstall
Uninstall
Activate Windows
Go to Settings to activate Windows.

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

Name	Publisher	Installed On	Size	Version
7-Zip 21.02 alpha (x64)	Igor Pavlov	5/28/2021	5.10 MB	21.02 alpha
AD LDS Instance instance1	Microsoft Corporation	2/7/2021	46.3 MB	
Apache Tomcat 8.5 Tomcat8 (remove only)	The Apache Software Foundation	9/21/2020		8.5.58
cyberJack Base Components	REINER SCT	7/22/2020	7.31 MB	7.7.2
DigiCert Autoenrollment Server	DigiCert, Inc.	11/29/2021	183 MB	2.21.7.0
DigiCert Desktop Client	DigiCert Inc.	9/13/2021	205 MB	3.3.0
DigiCert PKI Client	DigiCert Inc.	11/21/2021	40.2 MB	2.21.6.20552
DigiCert PKI Enterprise Gateway	iCert, Inc.	11/10/2021	167 MB	1.21.1.18110
Google Chrome	ogle LLC	11/18/2021	497 MB	96.0.4664.45
Java 8 Update 241	Oracle Corporation	3/4/2020	208 MB	8.0.2410.7
Java 8 Update 261 (64-bit)	Oracle Corporation	9/22/2020	250 MB	8.0.2610.12
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	Microsoft Corporation	2/27/2020	20.5 MB	12.0.30501.0
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	Microsoft Corporation	2/27/2020	17.1 MB	12.0.30501.0
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30133	Microsoft Corporation	11/10/2021	20.1 MB	14.29.30133.0
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.24.28127	Microsoft Corporation	5/22/2021	20.1 MB	14.24.28127.4
Mozilla Firefox (x64 en-US)	Mozilla	11/10/2021	203 MB	94.0.1
Mozilla Maintenance Service	Mozilla	10/27/2021	565 KB	93.0
Npcap	Nmap Project	2/27/2020		0.9986
nShield Software	nCipher Security	7/22/2020	3.17 GB	12.60.3
OpenSSL 1.1.1c Light (64-bit)	OpenSSL Win64 Installer Team	7/12/2019	9.88 MB	
SafeNetAT Luna Client 7.10.1	SafeNet Assured Technologies, L...	10/7/2021	71.2 MB	7.10.1
SoapUI 5.6.0	SmartBear Software	5/28/2021	241 MB	5.6.0
VMware Tools	VMware, Inc.	5/23/2021	189 MB	11.1.1.16303738
Wireshark 3.2.2 64-bit	The Wireshark developer comm...	3/1/2020	178 MB	3.2.2

DigiCert, Inc. Product version: 1.21.1.18110
Size: 167 MB

2. Click **Uninstall**.

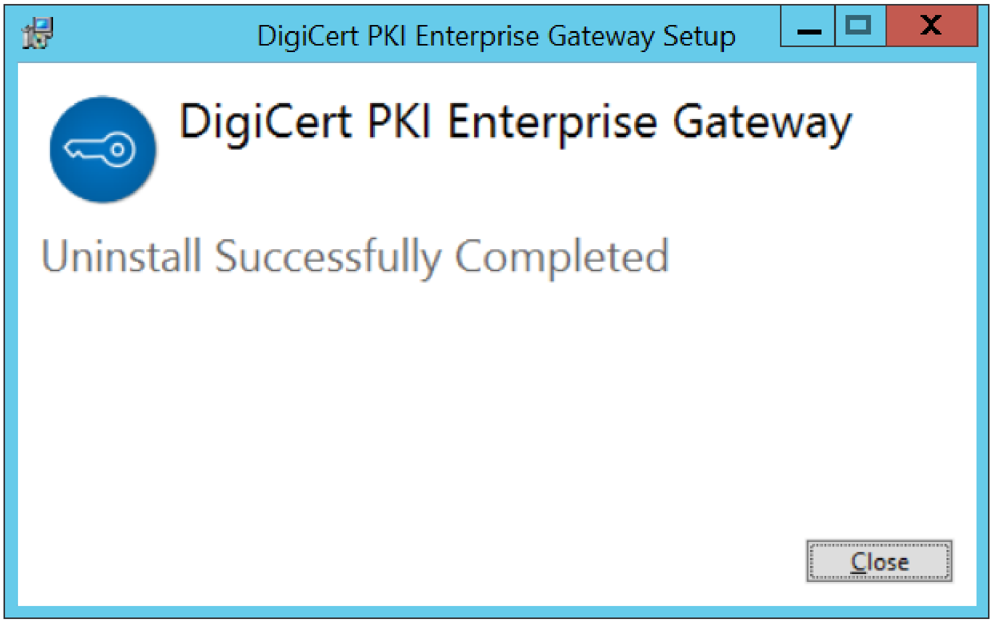


DigiCert PKI Enterprise Gateway Setup

DigiCert PKI Enterprise Gateway

Modify Setup

3. Click **Close**.



DigiCert PKI Enterprise Gateway Setup

DigiCert PKI Enterprise Gateway

Uninstall Successfully Completed

CHAPTER 4

4 Configuring the PKI Enterprise Gateway

This chapter includes the following topics:

- Configuring SSL
- Configuring PKI Manager to Recognize PKI Enterprise Gateway
- (Optional) Configuring the Key Escrow and Recovery Service
- Testing the PKI Enterprise Gateway

4.1 Configuring SSL

For testing purposes, PKI Enterprise Gateway is configured without SSL when first installed. However, DigiCert recommends that you secure communications between all of your PKI Enterprise Gateway components using SSL. You can obtain SSL certificates from https://www.digicert.com. Refer to the instructions available on this site for procedures on installing and enabling SSL certificates.

Once you enable SSL for the RA Service, you must complete the following:

- Configure the service URLs in PKI Manager to specify https://. See "Configuring PKI Manager to Recognize PKI Enterprise Gateway".
- Update the service URLs in the Web.config files for the authentication service and RA Agent. See "Modifying Service URLs or Port Numbers".

4.2 Configuring PKI Manager to Recognize PKI Enterprise Gateway

You need to configure PKI Manager to recognize PKI Enterprise Gateway, and to identify the user groups to which you issue certificates. Refer to Table 4-1.

Table 4-1 Required information for PKI Manager configuration

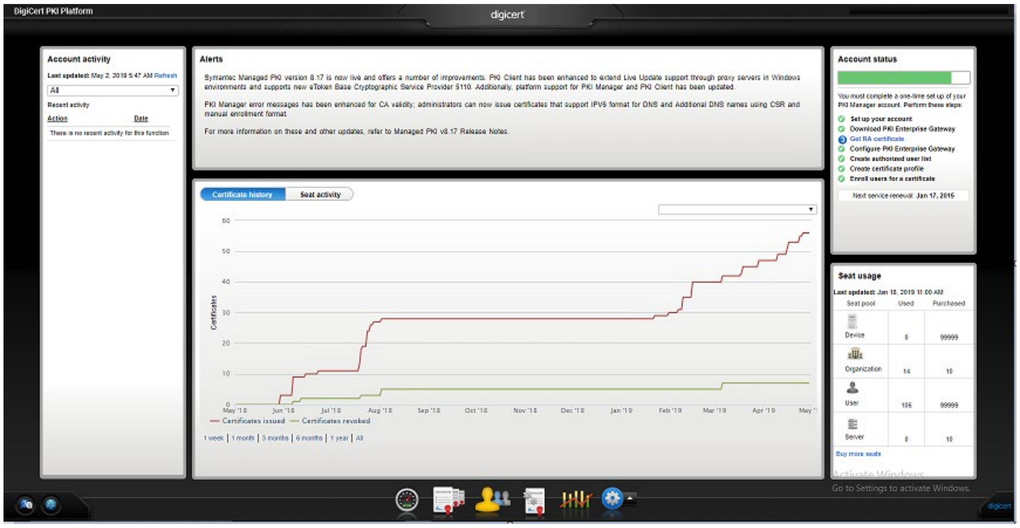
Item	Description
PKI Enterprise Gateway friendly name	Select a unique name to identify this gateway. Multiple gateways are useful. For example, one to use when you test the service and one to issue production certificates. The friendly name cannot include spaces or the following special characters: < > ; . & ‘ ".
PKI Enterprise Gateway description	Enter a description for the enterprise gateway.
Type of user store	Select whether your user store is an AD or an LDAP user store.
Set as default for new profiles?	Identify if this PKI Enterprise Gateway is configured for all new certificate profiles by default.
Deployment mode	Identify whether you plan to install PKI Enterprise Gateway in single-server or multiple-server mode. For single-server deployment, See Figure 1-1. For multiple-server deployment, See Figure 1-2. See “Deployment Modes”.
PKI Enterprise Gateway component URLs and port numbers	For single-server deployments, you must have the URL and port number to the IIS server instance hosting the PKI Enterprise Gateway. This information is provided in the Summary files written to the %PUBLIC% folder by the installation script.

Item	Description
	For multiple-server deployments, you must have the URL and port number to the IIS server instance hosting the authentication service and RA Agent. Also, you must have the URL and port number to the IIS server instance hosting the RA Service. For deployments with an HTTP proxy forwarder, the RA Service URL and port number are the URL and port number for the HTTP proxy forwarder. Also, you must point your HTTP proxy forwarder to the URL and port number for the RA Service. DigiCert recommends that you enable SSL. If you do, use https://. For example, https://companydomain.com. See "Default ports". See "Modifying Service URLs or Port Numbers".
Key escrow and port number	Use the port number of the Apache Tomcat running on the PKI Enterprise Gateway computer where the key escrow and recovery service is hosted.

Complete the following general steps to configure PKI Manager. These steps assume that you have already set up your account in PKI Manager and downloaded the PKI Enterprise Gateway software and RA certificate

Refer to the PKI Manager and associated help for detailed configuration procedures.

1. Access PKI Manager at https://pki-manager.symauth.com/pki-manager using your administrator certificate. The PKI Manager Dashboard appears.



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.

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

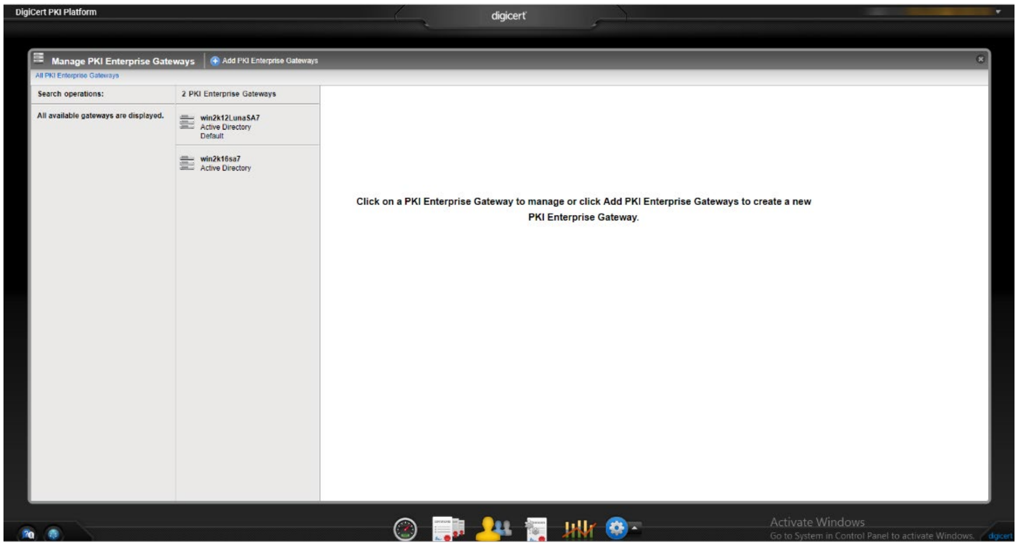
- ✓ Set up your account
- ✓ Download PKI Enterprise Gateway
- 3 Get RA certificate
- ✓ Configure PKI Enterprise Gateway
- ✓ Create authorized user list
- ✓ Create certificate profile
- ✓ Enroll users for a certificate

Next service renewal: Jan 17, 2015

Last updated: Jan 18, 2019 11:00 AM

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

2. Under **Account Status** on the PKI Manager dashboard, click **Configure PKI Enterprise Gateway**. The **Manage PKI Enterprise Gateway** screen appears


DigiCert PKI Platform
digicert
Manage PKI Enterprise Gateways
Add PKI Enterprise Gateways
All PKI Enterprise Gateways
Search operations:
2 PKI Enterprise Gateways
Activate Windows
Go to System in Control Panel to activate Windows.
digicert

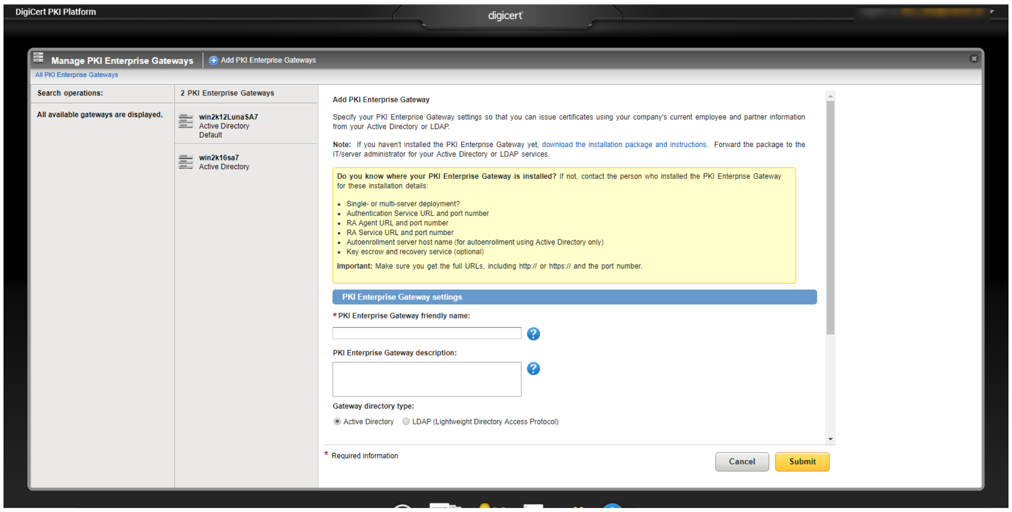
All available gateways are displayed.

win2k12LunaSA7
Active Directory
Default

win2k16sa7
Active Directory

Click on a PKI Enterprise Gateway to manage or click Add PKI Enterprise Gateways to create a new PKI Enterprise Gateway.

3. Click **Add PKI Enterprise Gateways.** The **Add PKI Enterprise Gateway** window appears.



All available gateways are displayed.

Add PKI Enterprise Gateway

Specify your PKI Enterprise Gateway settings so that you can issue certificates using your company's current employee and partner information from your Active Directory or LDAP.

Note: If you haven't installed the PKI Enterprise Gateway yet, download the installation package and instructions. Forward the package to the IT/server administrator for your Active Directory or LDAP services.

Do you know where your PKI Enterprise Gateway is installed? If not, contact the person who installed the PKI Enterprise Gateway for these installation details:

- Single- or multi-server deployment?
- Authentication Service URL and port number
- RA Agent URL and port number
- RA Service URL and port number
- Autoenrollment server host name (for autoenrollment using Active Directory only)
- Key escrow and recovery service (optional)

Important: Make sure you get the full URLs, including http:// or https:// and the port number.

PKI Enterprise Gateway settings

* PKI Enterprise Gateway friendly name:

PKI Enterprise Gateway description:

Gateway directory type:

● Active Directory ○ LDAP (Lightweight Directory Access Protocol)

* Required information

4. Enter the PKI Enterprise Gateway configuration information you gathered in Table 4-1 and click **Save**.

4.3 (Optional) Configuring the Key Escrow and Recovery Service

The key escrow and recovery service configuration file (kmsconfig.properties) defines the behavior of the key escrow and recovery service. The kmsconfig.properties is located under the `conf` directory where Apache Tomcat is installed. If you implement key escrow and recovery, you need to modify this file to match your deployment and environment.

Use the information in this section and the comments in the configuration file to modify the `kmsconfig.properties` file.

NOTE: By default, the values in the configuration file are stored in clear text. Since the key escrow and recovery service resides at your enterprise site, it should be protected from unauthorized access by your existing security practices. However, DigiCert provides the camouflage utility to enhance the security of this file. This utility lets you encrypt the values in the configuration file.

See "Encrypting Sensitive Values in the Key Escrow and Recovery Service Configuration File".

Observe the following conventions when editing the kmsconfig.properties file.

- Use the # character at the beginning of a line to comment the line.
- Use the equal sign (=) as a delimiter between a name and its value.
- If you do not use a parameter in this file, DigiCert recommends that you comment it out.

1. Open the `kmsconfig.properties` file in a standard text editor.

2. Modify the values in this file to match your deployment and environment. Refer to Table 4-2 for details on these values.
3. Save the modified kmsconfig.properties file.

Table 4-2 Parameters for the kmsconfig.properties file

Parameter	Description
enroll.urlendpoint=	The HTTP endpoint for the enrollment request that is sent to the DigiCert PKI Platform: https://pki-ws.symauth.com
enroll.urlendpoint.proxy.host=	The name of the proxy host. Configure this value if the key escrow and recovery service communicates with DigiCert PKI Platform through an HTTP proxy.
enroll.urlendpoint.proxy.port=	The name of the port number of the proxy host. Configure this value if the key escrow and recovery service communicates with DigiCert PKI Platform through an HTTP proxy.
enroll.urlendpoint.proxy.username=	The user name for the user that can access the proxy server. Configure this value if the key escrow and recovery service communicates with DigiCert PKI Platform through an HTTP proxy.
enroll.urlendpoint.proxy.password=	The password for the user that can access the proxy server. Configure this value if the key escrow and recovery service communicates with DigiCert PKI Platform through an HTTP proxy.
enroll.ssl.mechanism=	Identifies how the RA certificate is stored. Use one of the following values:

Parameter	Description
	Hardware if it is stored in an HSM Software if it is stored in a software-based Java keystore.
enroll.ssl.software.keystore=	Indicates the keystore where the RA certificate is stored. Do not use this value if the certificate is stored in an HSM.
enroll.ssl.software.keystorepass=	The password for the software-based keystore containing the RA certificate. Do not use this value if the certificate is stored in an HSM.
enroll.ssl.hardware.slotid=	If the RA certificate is stored on an HSM, Indicates in which slot the token containing the certificate resides. Do not use this value if the certificate is stored in a software-based keystore.
enroll.ssl.hardware.label=	If the RA certificate is stored on an HSM, Indicates in which Partition Label the token containing the certificate resides. Do not use this value if the certificate is stored in a software-based keystore
enroll.ssl.hardware.password=	If the RA certificate is stored on an HSM, the password for the token containing the SSL certificate. Do not use this value if the certificate is stored in a software-based keystore.
enroll.ssl.preferredCertAlias=	The keystore alias of the RA certificate that is preferred for RA communications. This value must match the alias of a certificate in the certificate keystore or HSM. If no value is selected, a certificate is selected automatically.

Parameter	Description
enroll.ssl.truststore=	Indicates the truststore where the root CA certificates for the RA certificate are stored. 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 can import these CAs into your truststore.
enroll.ssl.truststorepass=	The password for the truststore where the root CA certificates for the RA certificate are stored.
enroll.ssl.apikey=	API Key used for two factor authorization to submit requests to DigiCert. If API Key was provided with RA certificate, enter that value. Otherwise leave it as the pre-populated "DEFAULT_API_KEY".
kms.keyrecovery.dataSource=	Indicates the type of Key Escrow data source. Use either **LDAP** or **Database**.
kms.keyrecovery.database.type=	If the Key Escrow data source type is Database, indicate the type of database. Use either **Oracle** or **SQLServer**.
kms.keyrecovery.database.url=	Indicates the URL for the key recovery datastore, if the datastore type is Database (otherwise, this entry is ignored): For Oracle, the format must be [hostname]:[port]:[SID] For SQLServer, the format must be [servername]\\[instance name]:[port]; database=KeyRecovery; selectMethod=cursor

Parameter	Description
kms.keyrecovery.database.username=	Indicates the user name for the Key Escrow data source. This value is ignored if the datastore type is not Database.
kms.keyrecovery.database.password=	The password for the Key Escrow data source. This value is ignored if the datastore type is not Database.
kms.keyrecovery.ldap.url=	Indicates the URL for the key recovery datastore, if the datastore type is LDAP (otherwise, this entry is ignored). For LDAP over SSL, use ldaps:// instead of ldap:// This value is ignored if the datastore type is not LDAP.
kms.keyrecovery.ldap.port=	Indicates the port number for the Key Escrow data source. This value is ignored if the datastore type is not LDAP.
kms.keyrecovery.ldap.pooled=false	Indicates if pooling is enabled for the key recovery datastore. Do not modify this value. This value is ignored if the datastore type is not LDAP.
kms.keyrecovery.ldap.base.dn=	Indicates the base Distinguished Name (DN) for the Key Escrow data source. It specifies the LDAP subtree entry point at which to begin a directory search. This value is ignored if the datastore type is not LDAP.
kms.keyrecovery.ldap.user.dn=	Indicates the user DN for the Key Escrow data source. This value is ignored if the datastore type is not LDAP.

Parameter	Description
kms.keyrecovery.ldap.password=	The password for the user DN for the Key Escrow data source. This value is ignored if the datastore type is not LDAP.
kms.keyrecovery.ldap.objclass=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.webpin=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.common_name=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.mask=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other

Parameter	Description
	purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.iv=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.pkcs12_password=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.private_key=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.cert=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.

Parameter	Description
kms.keyrecovery.ldap.cert_status=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.event_time=	This value maps the key escrow data to the location in the data source where it is later stored. These values are ignored if the data type is not LDAP. Modifying this value breaks backward compatibility. If you need to modify this value, choose the attributes that are not used for any other purpose. Attributes must have sufficient size to contain the stored values.
kms.keyrecovery.ldap.keyescrowcontainer.ou=	Indicates the name for the LDAP Key Escrow data source container. This value should be the OU in the LDAP directory. DigiCert recommends setting the value to KeyRecoveryData. However, if a value already exists for your LDAP directory, use this value.
pkcs12.password.generate=	Indicates if the key escrow and recovery service generated the PKCS12 password. If **YES** is specified, pkcs12.password.length= must be set.
pkcs12.password.length=	Defines the length (between 8 and 50 alphanumeric characters) of the randomly generated password for each PKCS#12 file. This value must be set if pkcs12.password.generate= is set to **YES**. Do not set this value if the key escrow and recovery service does not generate the PKCS#12 file password.

Parameter	Description
hardware.vrsn.provider=com.verisign.pki.service.common.cryptography.impl.PKCS11CryptographyProvider	Indicates the cryptographic providers for all cryptographic operations. Do not modify these values.
software.vrsn.provider=com.verisign.pki.service.common.cryptography.impl.SoftwareCryptographyProvider	Indicates the cryptographic providers for all cryptographic operations. Do not modify these values.
asymmetrickey.keygen.algorithm=RSA	Indicates the algorithms that are used for asymmetric key and symmetric key generation. Not all of the algorithms are supported. If an algorithm is not supported, an Algorithm Not Supported error is generated. Do not modify this value.
asymmetrickey.keygen.algorithm=RSA	Indicates the algorithms that are used for asymmetric key and symmetric key generation. Not all of the algorithms are supported. If an algorithm is not supported, an Algorithm Not Supported error is generated. Do not modify this value.
kms.keygen.mechanism=	Indicates how the private key is later generated; in software or on the HSM. For hardware generation, use **Hardware**. For software generation, use **Software**.
software.jca.provider=	Indicates the JCA/JCE providers, if the key is later generated in software. Otherwise, this value is ignored.
software.jce.provider=org.bouncycastle.jce.provider.BouncyCastleProvider	Indicates the JCA/JCE providers, if the key is later generated in software. Otherwise, this value is ignored.
kms.keygen.maxKeyLength	Indicates the maximum key length that the key escrow and recovery service can generate. The default value is 4096. The key escrow and recovery service has been qualified up to 4096 bits.

Parameter	Description
	The minimum key length is 1024 bits.
hardware.keygen.library=	Indicates the implementation library, if the key is later generated on the HSM. Otherwise, this value is ignored. A C library implementation of the PKCS#11 APIs, and should be loadable by the key escrow and recovery service: For Windows, include the location of the library in the PATH system variable.
hardware.keygen.slotId=	Indicates the slot ID for the token being used for key generation, if the key is later generated on the HSM. Otherwise, this value is ignored.
hardware.keygen.tokenLabel=	Indicates the slot label used for key generation, if the key is later generated on the HSM. Otherwise, this value is ignored. The slot label must match the slot of the key export partition on the device.
hardware.keygen.password=	Indicates the password for the token being used for key generation, if the key is later generated on the HSM. Otherwise, this value is ignored.

NOTE: For HSMs, you can configure either token label (recommended) or slot Id. If both token label and slot Id are configured, token label will take precedence over slot Id.

4.3.1 Start the Tomcat Web Server Hosting the Key Escrow and Recovery Service

Start your Tomcat Web Server using the startup script provided (start_kmsws.bat) to start the Tomcat web server hosting the key escrow and recovery service. start_kmsws.bat is located under the "bin" directory where Apache Tomcat is installed. You must manually edit the environment variable (for a .zip installation) or change the Java options (for a .exe installation) to add the pkiservices.configuration.path. The value should be the Tomcat path.

Example: "C:\Program Files\Apache Software Foundation\Tomcat 8.5\conf"

Check the Tomcat web server logs, as well as PKIService.enterpriseService.log to make sure that there were no errors. If you used a .exe installer, the Tomcat logs are located at C:\Program Files\Apache Software Foundation\logs. If you used a

.zip installer, the logs are found at C:\Program Files\Apache Software Foundation\Tomcat\logs.

When you start the key escrow and recovery service, you may need to wait for several minutes before sending your first requests. The server application needs this time to load the key escrow and recovery service components. You can check your log files to verify that the service has started successfully.

To stop the Tomcat web server hosting the key escrow and recovery service, stop the Tomcat web server. Use the stop script provided (stop_kmsws.bat, located under the "bin" directory where Apache Tomcat is installed).

NOTE: After installing key escrow and recovery service, you must make sure to stop the Tomcat web server and start it to avoid errors like SSLHandshakeException: decrypt_error.

4.3.2 Encrypting Sensitive Values in the Key Escrow and Recovery Service Configuration File

The kmsconfig.properties file contains sensitive information about your key recovery data source and your key escrow and recovery service. After you have configured these files, you can use the camouflage utility prevent unauthorized individuals from reading them. The camouflage utility uses password-based AES encryption to mask information in the kmsconfig.properties file.

NOTE: This tool is not a substitute for installing the key escrow and recovery service in a secure environment. Protecting access by good security practices is an additional security tool that you can use.

For example, after use of the camouflage utility, the following lines are in kmsconfig.properties:

```
kms.keyrecovery.database.username=wsuser
kms.keyrecovery.database.password=wspwd
```

would look similar to the following:

```
kms.keyrecovery.database.username=<encrypted>5dg0rlwhNCpDjVmZomhdE==

</encrypted>kms.keyrecovery.database.password=<encrypted>

t8XpMuhzeDnK4=wuFj9qoc1n</encrypted>
```

Once encrypted, the data in the kmsconfig.properties file is decrypted only by

DigiCert PKI Platform. Before encrypting your configuration files, you should make a copy of them and store them in a secure location. A copy makes configuration changes easier, as you can work from the backup copy instead of the masked data.

4.3.3 Using the Camouflage Tool

1. Back up the unencrypted version of the kmscomfig.properties file.
2. Switch to the <install directory>/key escrow and recovery service subdirectory of the .zip file.
3. Identify the values in the file that you want to encrypt.
4. Run the tool with the following command:
5. java -jar camouflage.jar <value to encrypt>
6. Replace the value in the kmsconfig.properties file with the encrypted value generated by the tool.
7. Save the modified kmsconfig.properties file with the encrypted values.

4.4 Testing the PKI Enterprise Gateway

Complete the following steps to test your PKI Enterprise Gateway deployment.

1. Log into the computer where the user store resides and create a new group. Or select an existing group other than the **PKI Enterprise Gateway Group** (or group name you specified during the installation). Create or add test users to this group, if needed.

   Make sure that the user objects you add include data for the attributes needed by the certificate profile. For example, if testing with an SMIME-enabled certificate profile, provide an email address for all users.

2. Access PKI Manager:

   - Create a new user group List by clicking **Create authorized user list** under **Account status** and pointing it to the user group you selected in 1. Enter the group name exactly as it appears in user store:

     - For Active Directory user stores, typically: <NETBIOS_name\group_name>.
     - For LDAP user stores, use the fully-qualified domain name (FQDN) of the test group.

   - Select **Create Certificate Profile** and create a new certificate profile.
   - Select **Enroll Users**, then select the certificate profile you created to obtain the enrollment URL.

3. As the test user:

   - Navigate to the enrollment URL provided.

     - For LDAP user stores, you are prompted for the user's LDAP credentials.
     - For Active Directory user stores, if the test user is not connected to the network domain, you are prompted for the user's Windows credentials.

   - You are automatically taken to a page displaying the user details. Click **Continue**. The **Install Certificate** page appears.
   - Click **Install**. The certificate is downloaded or installed on your computer.

4. Verify that the new certificate is correct.

APPNEDIX A

5 Modifying PKI Enterprise Gateway Configuration

This appendix includes the following topics:

- Modifying Service URLs or Port Numbers
- Modifying the Subject Name of the RA Certificate
- Updating the Windows User Name and Password (Connectivity Pool Information)
- Modifying Proxy Settings
- Updating Encrypted Settings
- Adding User Domains (Active Directory User Stores Only)

5.1 Modifying Service URLs or Port Numbers

PKI Enterprise Gateway uses the fully-qualified domain names and ports that are listed in Table 2-1. You may change the URLs and port numbers for the PKI Enterprise Gateway components using the following procedures.

5.1.1 Modifying the RA Service

Complete the appropriate procedures to modify the ports or enable SSL for the RA Service.

Modifying RA Service Ports

1. Modify the ports in IIS. Refer to the IIS product documentation for procedures.
2. Update PKI Manager:

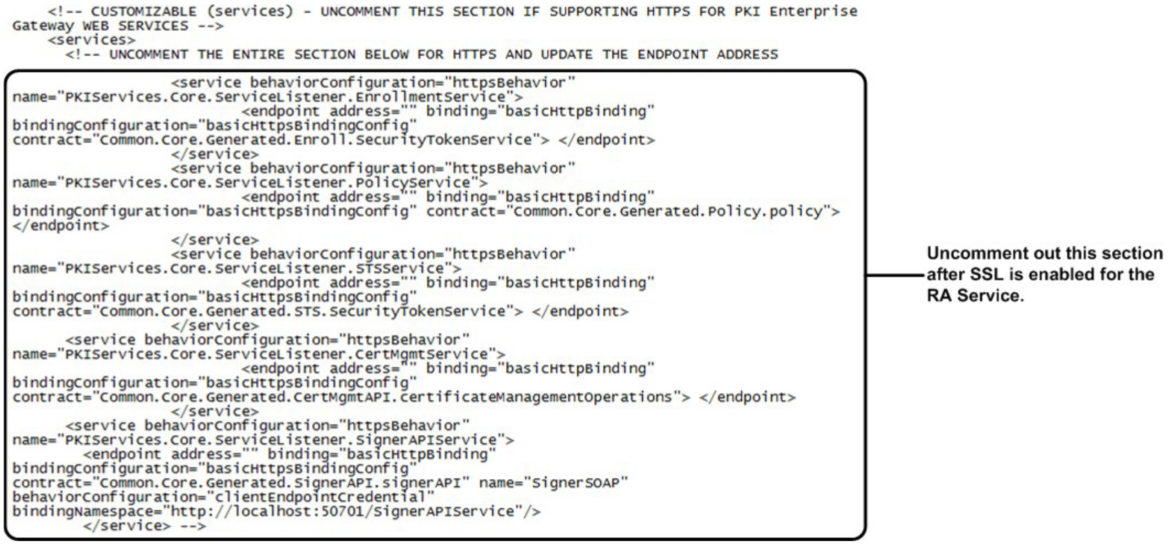
   - Access PKI Manager and select **Configure PKI gateway**.
   - Select your PKI Enterprise Gateway, and click **Edit settings**.
   - Update the port for the RA Service.

3. Update the web.config file for the authentication service and RA Agent with the new RA Service port number.

   See "Modifying the Authentication Service Ports".
   See "Modifying the RA Agent and Authentication Service".

Configuring SSL for the RA Service

1. Enable SSL in the IIS instance hosting your RA Service. Refer to the IIS product documentation for procedures.
2. Using a text editor, modify the web.config file for the RA Service. The file is in the <install_dir>/Applications/RAService folder on the computer on which the RA Service is installed. Refer to the following image for an example of web.config file for the RA service. Uncomment the HTTPS endpoint address elements.



```
    <!-- CUSTOMIZABLE (services) - UNCOMMENT THIS SECTION IF SUPPORTING HTTPS FOR PKI Enterprise
Gateway WEB SERVICES -->
    <services>
      <!-- UNCOMMENT THE ENTIRE SECTION BELOW FOR HTTPS AND UPDATE THE ENDPOINT ADDRESS
                  <service behaviorConfiguration="httpsBehavior"
name="PKIServices.Core.ServiceListener.EnrollmentService">
                          <endpoint address="" binding="basicHttpBinding"
bindingConfiguration="basicHttpsBindingConfig"
contract="Common.Core.Generated.Enroll.SecurityTokenService"> </endpoint>
                  </service>
                  <service behaviorConfiguration="httpsBehavior"
name="PKIServices.Core.ServiceListener.PolicyService">
                          <endpoint address="" binding="basicHttpBinding"
bindingConfiguration="basicHttpsBindingConfig" contract="Common.Core.Generated.Policy.policy">
</endpoint>
                  </service>
                  <service behaviorConfiguration="httpsBehavior"
name="PKIServices.Core.ServiceListener.STSService">
                          <endpoint address="" binding="basicHttpBinding"
bindingConfiguration="basicHttpsBindingConfig"
contract="Common.Core.Generated.STS.SecurityTokenService"> </endpoint>
                  </service>
      <service behaviorConfiguration="httpsBehavior"
name="PKIServices.Core.ServiceListener.CertMgmtService">
                          <endpoint address="" binding="basicHttpBinding"
bindingConfiguration="basicHttpsBindingConfig"
contract="Common.Core.Generated.CertMgmtAPI.certificateManagementOperations"> </endpoint>
                  </service>
      <service behaviorConfiguration="httpsBehavior"
name="PKIServices.Core.ServiceListener.SignerAPIService">
        <endpoint address="" binding="basicHttpBinding"
bindingConfiguration="basicHttpsBindingConfig"
contract="Common.Core.Generated.SignerAPI.signerAPI" name="SignerSOAP"
behaviorConfiguration="clientEndpointCredential"
bindingNamespace="http://localhost:50701/SignerAPIService"/>
        </service> -->
```

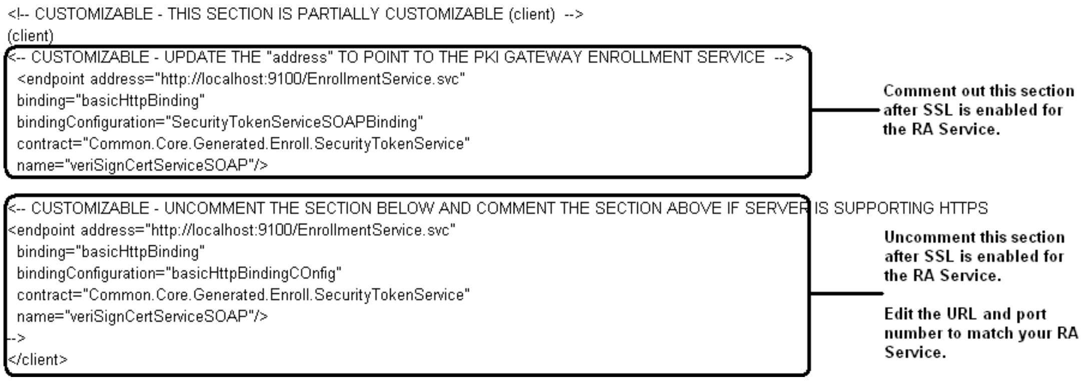
Uncomment out this section after SSL is enabled for the RA Service.

3. Using a text editor, modify the web.config file for the RA Service. The file is in the <install_dir>/Applications/RAService folder on the computer on which the RA Service is installed. Refer to the following code as an example of web.config file for the RA service. Comment the following block of code and save the file.

```
<service behaviorConfiguration="customQuotaBehavior"
name="PKIServices.Core.ServiceListener.CertMigrationService">
<endpoint address="" binding="basicHttpBinding"bindingConfiguration=
"customSecurityTokenServiceSOAPBinding"contract="Common.Core.
Generated.CertMigrationAPI.EnterpriseCertificateMigration ServiceOperations">
  </endpoint>
    </service>
```

4. Using a text editor, modify the web.config file for the RA Agent. The file is in the <install_dir>/Applications/RAAgent folder on the computer on which the RA Agent is installed. Refer the following image for an example web.config file for the RA Agent.

- Comment out the two HTTP endpoint address elements and uncomment the HTTPS endpoint address elements in the same section.
- Under **client** in the **system.serviceModel** section, replace the values for the two **endpoint address** elements with your RA Service URL and port number.



```
<!-- CUSTOMIZABLE - THIS SECTION IS PARTIALLY CUSTOMIZABLE (client)  -->
(client)
<-- CUSTOMIZABLE - UPDATE THE "address" TO POINT TO THE PKI GATEWAY ENROLLMENT SERVICE  -->
 <endpoint address="http://localhost:9100/EnrollmentService.svc"
 binding="basicHttpBinding"
 bindingConfiguration="SecurityTokenServiceSOAPBinding"
 contract="Common.Core.Generated.Enroll.SecurityTokenService"
 name="veriSignCertServiceSOAP"/>

<-- CUSTOMIZABLE - UNCOMMENT THE SECTION BELOW AND COMMENT THE SECTION ABOVE IF SERVER IS SUPPORTING HTTPS
<endpoint address="http://localhost:9100/EnrollmentService.svc"
 binding="basicHttpBinding"
 bindingConfiguration="basicHttpBindingCOnfig"
 contract="Common.Core.Generated.Enroll.SecurityTokenService"
 name="veriSignCertServiceSOAP"/>
-->
</client>
```

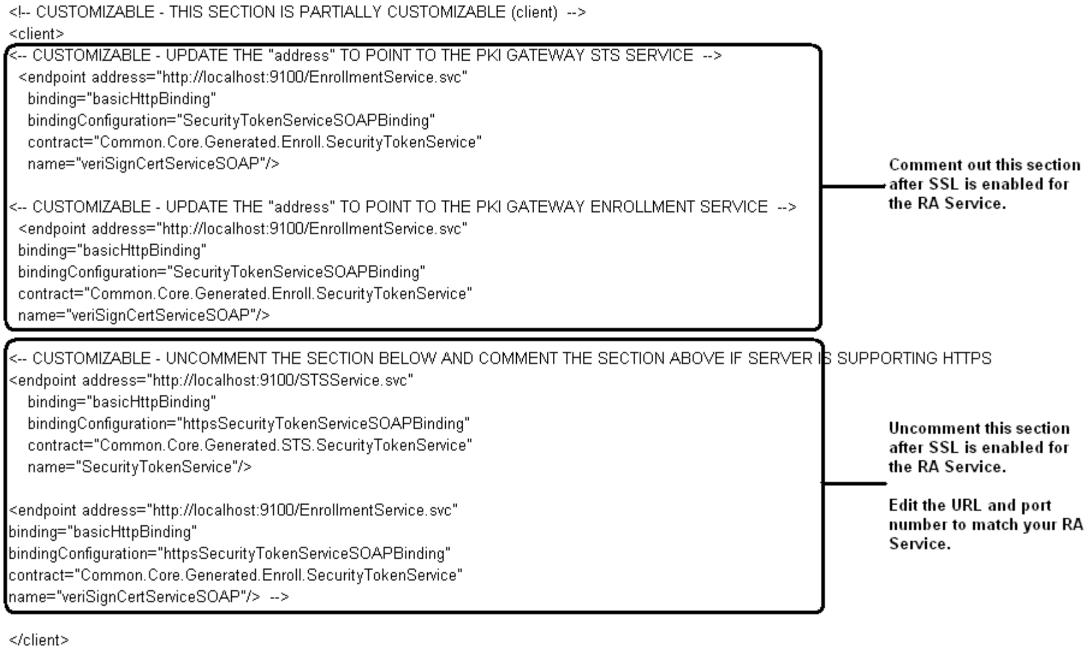
Comment out this section after SSL is enabled for the RA Service.

Uncomment this section after SSL is enabled for the RA Service.

Edit the URL and port number to match your RA Service.

5. Using a text editor, modify the web.config file for the authentication service. The file is in the <install_dir>/Applications/AuthenticationService folder on the computer on which the authentication service is installed. Refer the following image for an example web.config file for the authentication service.

   - Comment out the two HTTP endpoint address elements and uncomment the HTTPS endpoint address elements in the same section.
   - Under the **client** in the **system.serviceModel** section, replace the values for the two **endpoint address** elements with your RA Service URL and port number.



```
<!-- CUSTOMIZABLE - THIS SECTION IS PARTIALLY CUSTOMIZABLE (client)  -->
<client>
<-- CUSTOMIZABLE - UPDATE THE "address" TO POINT TO THE PKI GATEWAY STS SERVICE  -->
  <endpoint address="http://localhost:9100/EnrollmentService.svc"
    binding="basicHttpBinding"
    bindingConfiguration="SecurityTokenServiceSOAPBinding"
    contract="Common.Core.Generated.Enroll.SecurityTokenService"
    name="veriSignCertServiceSOAP"/>

<-- CUSTOMIZABLE - UPDATE THE "address" TO POINT TO THE PKI GATEWAY ENROLLMENT SERVICE  -->
  <endpoint address="http://localhost:9100/EnrollmentService.svc"
  binding="basicHttpBinding"
  bindingConfiguration="SecurityTokenServiceSOAPBinding"
  contract="Common.Core.Generated.Enroll.SecurityTokenService"
  name="veriSignCertServiceSOAP"/>

<-- CUSTOMIZABLE - UNCOMMENT THE SECTION BELOW AND COMMENT THE SECTION ABOVE IF SERVER IS SUPPORTING HTTPS
<endpoint address="http://localhost:9100/STSService.svc"
    binding="basicHttpBinding"
    bindingConfiguration="httpsSecurityTokenServiceSOAPBinding"
    contract="Common.Core.Generated.STS.SecurityTokenService"
    name="SecurityTokenService"/>

<endpoint address="http://localhost:9100/EnrollmentService.svc"
binding="basicHttpBinding"
bindingConfiguration="httpsSecurityTokenServiceSOAPBinding"
contract="Common.Core.Generated.Enroll.SecurityTokenService"
name="veriSignCertServiceSOAP"/>  -->

</client>
```

Comment out this section after SSL is enabled for the RA Service.

Uncomment this section after SSL is enabled for the RA Service.

Edit the URL and port number to match your RA Service.

6. On the computer or computers on which these services are installed, run iisreset to pick up the changes.

5.1.2 Modifying the RA Agent and Authentication Service

Complete the procedures to modify the ports for the RA Agent or authentication service. Or, complete the procedures to enable SSL for the RA Agent and Authentication server computer.

Modifying the RA Agent Ports

1. Modify the ports in IIS. Refer to the IIS product documentation for procedures.
2. Update PKI Manager:

- Access PKI Manager and select **Configure PKI gateway**.
- Select your PKI Enterprise Gateway, and click **Edit settings**.
- Update the port for the RA Agent.

Modifying the Authentication Service Ports

1. Modify the ports in IIS. Refer to the IIS product documentation for procedures.
2. Update PKI Manager:

- Access PKI Manager and select **Configure PKI gateway**.
- Select your PKI Enterprise Gateway, and click **Edit settings**.
- Update the port of the authentication service.

Configuring SSL for the RA Agent and Authentication Service

1. Enable SSL in the IIS instance hosting your RA Service. Refer to the IIS product documentation for procedures.
2. Update PKI Manager:

- Access PKI Manager and select **Configure PKI gateway**.
- Select your PKI Enterprise Gateway, and click **Edit settings**.
- Update the URL to specify https://.

5.2 Modifying the Subject Name of the RA Certificate

You need to configure PKI Enterprise Gateway with the Subject Name of the RA certificate. Typically, configuration is done when the RA Service is installed.

However, if you skipped configuration during installation, complete the following steps to manually update the Subject Name.

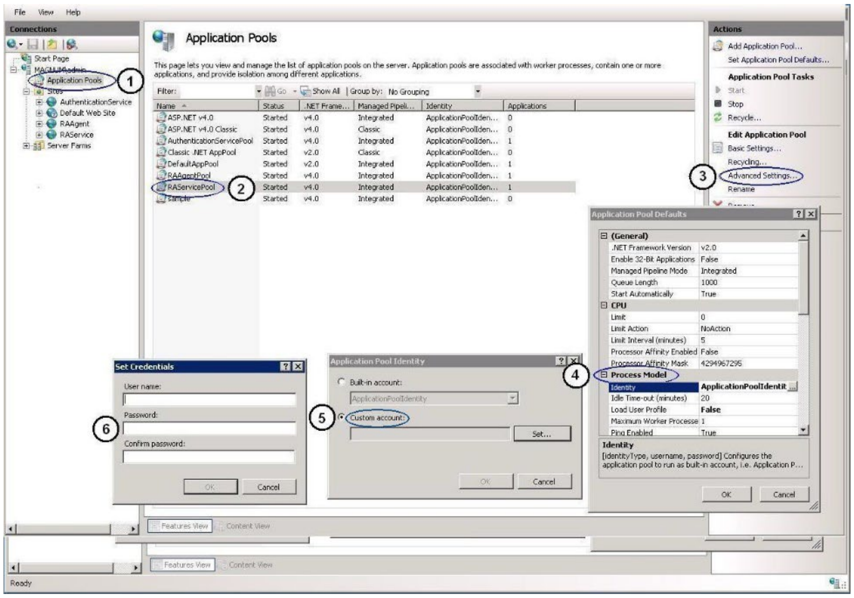
You may also need to update the Subject Name. The update is needed when you renew or replace the RA certificate that secures communications between PKI Enterprise Gateway and DigiCert Certificate Authority. Updating the Subject Name is part of the normal RA certificate lifecycle.

1. Open MMC and click on **Certificates > Local Computer > Personal > Certificates store**.
2. If the certificate is a renewal RA certificate or a replacement RA certificate, import the new RA certificate.
3. Double-click the certificate in MMC and make a note of the RA certificate's Common Name (CN) value of the Subject attribute.
4. Using a text editor, modify the web.config file for the RA Service. The file is in the <install_dir>/Applications/RAService folder on the computer on which the RA Service is installed. Follow these steps to modify the web.config file:
   - Under **pgwConfigSection**, change **RASubjectName** to the Common Name value. The value is obtained in Step 3.
   - Under **clientCredentials**, change **clientCertificate findValue** to the Common Name value. See Step 3.
5. Using a text editor, modify the web.config file for the Authentication Service. The web.config file is in the <install_dir>/Applications/AuthenticationService folder on the computer where the Authentication Service is installed.
   - Under the **pgwConfigSection**, change **RASubjectName** to the Common Name value from Step 3.
6. Save the web.config file.
7. Restart your IIS server.

5.3 Updating the Windows User Name and Password (Connectivity Pool Information)

You need to configure PKI Enterprise Gateway with the user name and password for the domain user running the RA Service application pool. You need to update these credentials if you need to change them. For example, if your security policies require that you change the password periodically.

Complete the following steps to manually change the Windows user name and password on your IIS server computer:



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET Frame...	Managed Pipeli...	Identity	Applications
ASP.NET v4.0	Started	v4.0	Integrated	ApplicationPoolIden...	0
ASP.NET v4.0 Classic	Started	v4.0	Classic	ApplicationPoolIden...	0
AuthenticationServicePool	Started	v4.0	Integrated	ApplicationPoolIden...	1
Classic .NET AppPool	Started	v2.0	Classic	ApplicationPoolIden...	0
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIden...	1
RAAgentPool	Started	v4.0	Integrated	ApplicationPoolIden...	1
RAServicePool	Started	v4.0	Integrated	ApplicationPoolIden...	1
sample	Started	v4.0	Integrated	ApplicationPoolIden...	0

Application Pool Defaults

(General)	
.NET Framework Version	v2.0
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Queue Length	1000
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	ApplicationPoolIdentit
Idle Time-out (minutes)	20
Load User Profile	False
Maximum Worker Processe	1
Ping Enabled	True

Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application P...

Figure A-1 IIS console open to the Application Pools page

1. Open the IIS console and under **Roles > Web Server (IIS) > Internet Information service (IIS),** select **Application Pools** in the left pane.
2. Select **RAServicePool** in the center pane.
3. Click on **Advanced Settings** in the right pane.
4. Under **Process Model > Identity**, select the domain user who is assigned to run the RA Service.

   - Make sure that this user is a member of local Administrators group on the IIS server. Also, ensure that the user is a member of the security group **PKI Enterprise Gateway Group** (or group name you specified during the installation) in the user store.
   - Select **Identity**, then select the icon that appears to the right of the Identity name. The **Application Pool Identity** dialog box appears.

5. In the **Application Pool Identity** dialog box, select **Custom Account** and click **Set**. The **Set Credentials** dialog box appears.

6. Enter the new domain\username and password. Re-enter the password to confirm it and click **OK**.

5.4 Modifying Proxy Settings

If you use an HTTP proxy to communicate between PKI Enterprise Gateway and the DigiCert Certificate Authority, you must configure the proxy URLs and proxy user name in PKI Enterprise Gateway.

- If you configured your proxy settings during installation, the proxy password is encrypted. To modify the proxy password.

  See "Updating Encrypted Settings".

- If you configured your proxy settings after installation, the proxy password is shown in clear text.

Complete the following steps to change the proxy URL and user name.

1. Using a text editor, modify the web.config file for the RA Service. The file is in the <install_dir>/Applications/RAService folder on the computer on which the RA Service is installed. It is under **pgwConfigSection**:
   - Change **proxyUrl** to your HTTP proxy URL. Use the format `http://<proxy IP address>:<proxy port>`.
   - Change **proxyUser** to your HTTP proxy user name.
   - Change **defaultProxy** enabled to `"true"`. The resulting line should be:

   ```
   <defaultProxy enabled="true" useDefaultCredentials="false">
   ```
2. Save the web.config file.
3. Restart your IIS server.

5.5 Updating Encrypted Settings

For security purposes, the following configuration settings are encrypted. However, you may need to modify these values periodically. Use the changeConfig.vbs utility on the computers hosting the RA Service and authentication service to modify these encrypted values.

- Shared secrets
- Proxy passwords
- LDAP bind user password
- API Key

For security purposes, proxy passwords are encrypted. However, you may need to modify these values periodically. Use the changeConfig.vbs utility on the computers hosting the Signing Service to modify these encrypted values.

NOTE: This utility is available in the <install_dir>\Tools directory.

To update encrypted setting

1. From a command prompt, run the following command:

   ```
   cscript changeConfig.vbs <install_dir> [options]
   ```

   - This script takes the following options:
     - [sharedsecret:<sharedsecret>] Specify the new shared secret. This value must be from 1 to 30 alpha-numeric characters and must be the same for the RA Service and authentication service.
     - [proxypassword:proxypassword] Specify the new proxy password.
     - [primaryadminpassword:<primaryadminpassword>] Specify the LDAP bind user password.
     - [secondaryadminpassword:<secondaryadminpassword>] If configured for failover, specify the second LDAP bind user password.
     - [apikey:<apikey>] Specify API Key provided with RA certificate.

For example, the following command changes the shared secret to mysharedsecret.

```
cscript changeConfig.vbs "C:\My Programs" sharedsecret:mysecret
```

2. Close the command shell window. Closing the window prevents the command from being recovered from the command history.

The command may display errors for the components that were not installed. For example, if you run this utility to change a shared secret proxy password on a computer where no proxy has been configured. You may safely ignore these errors.

For updating encrypted settings for the optional key escrow and recovery service, refer to Using the Camouflage Tool.

5.6 Adding User Domains (Active Directory User Stores Only)

The installation script creates the PKIEGWGroup in the Active Directory domain on which it is run. This group has permissions to publish certificates for users in this domain. If you want your PKI Enterprise Gateway deployment to support users from other domains, you must set the same permissions on each domain. Use the setMPKIGroupPermissions.vbs to set these permissions on each domain that you support.

Complete these procedures as an Enterprise Administrator for the domains that you support.

1. Copy the setMPKIGroupPermissions.vbs script from the <installation folder>\Tools directory onto the computer on which the new domain resides.
2. From a command prompt, run the following command:

   ```
   setMPKIGroupPermissions.vbs <domain>\PKIEGWGroup
   ```

   where <domain> is the NetBIOS name of the domain where you installed PKI Enterprise Gateway.

This script generates a log file named setMPKIGroupPermissions.log_yyyyMMddhhmmss under the user's %PUBLIC% directory.

APPNEDIX B

6 Configuring PKI Enterprise Gateway for High Availability

This appendix includes the following topics:

- Pre-requisites
- Configuring PKI Enterprise Gateway

6.1 Pre-requisites

You must complete the following pre-requisites before configuring PKI Enterprise Gateway for high availability:

- Install and configure your PKI Enterprise Gateways on each computer, according to the procedures in and of this guide. Do not install the RA certificate at this time.
- Install the HSM hardware and register the KSP. The HSMs must reside in the same network (or subnet) and partitions must be created on each of the devices. The partitions must have the same domain name and password. Refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html on installing and configuring the HSMs and registering the KSP.
- If you use a load balancer, you must configure it to balance the PKI Enterprise Gateway URLs. These URLs are the authentication service URL, the RA Service URL and the RA Agent URL. Refer to the documentation for your load balancer for procedures on installing and configuring the load balancers.

6.2 Configuring PKI Enterprise Gateway

Complete these procedures to configure PKI Enterprise Gateway for high availability.

1. Set the partitions on each of the HSMs to HA mode. The steps include:

   - Registering the partition on each of the PKI Enterprise Gateway computers (Microsoft IIS 8.5 and 10.0).
   - Verifying the partitions.
   - Creating an HA group and adding one of the partitions. Then, adding the other partitions as additional members.
   - Synchronizing the partitions.

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

2. Enable high availability only as a group:

   - From a command line, run `vtl haAdmin -listGroups` to verify the existence of the HA group you created in Step1. You can enter the password to view detailed information about the group.

- Run `vtl haAdmin -HAOnly -enable` to enable the HA group.
- Run `vtl haAdmin -status -show` to verify that the HA group was enabled.

3. Enable high availability for the PKI Enterprise Gateway:

- Obtain the RA certificate following the procedures in "Obtaining an RA Certificate to Store in an HSM".
- Install the RA certificate on your first PKI Enterprise Gateway computer.
- From a command line, run `certutil -repairstore` to associate the RA certificate with the private key. Refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html.
- Install the RA certificate on your other PKI Enterprise Gateway computers.
- From a command line, run `Certutil -repairstore` on each of the other PKI Enterprise Gateway computer. Use the same command that you used in Step 3. Refer to https://knowledge.digicert.com/tutorials/hsm-configuration.html.

NOTE: The key generation slot for the (optional) key escrow and recovery service should be configured as an HA virtual slot if HA needs to be supported for your key escrow and recovery service.

APPNEDIX C

7 Configuring PKI Enterprise Gateway for Non-DigiCert Key Import

This appendix includes the following topics:

- Non-DigiCert key deployments
- Setup and Configuration
- Error codes
- Known Issues

7.1 Non-DigiCert key deployments

Figure C-1 illustrates how the import certificate feature is typically deployed in your PKI Enterprise Gateway deployment.

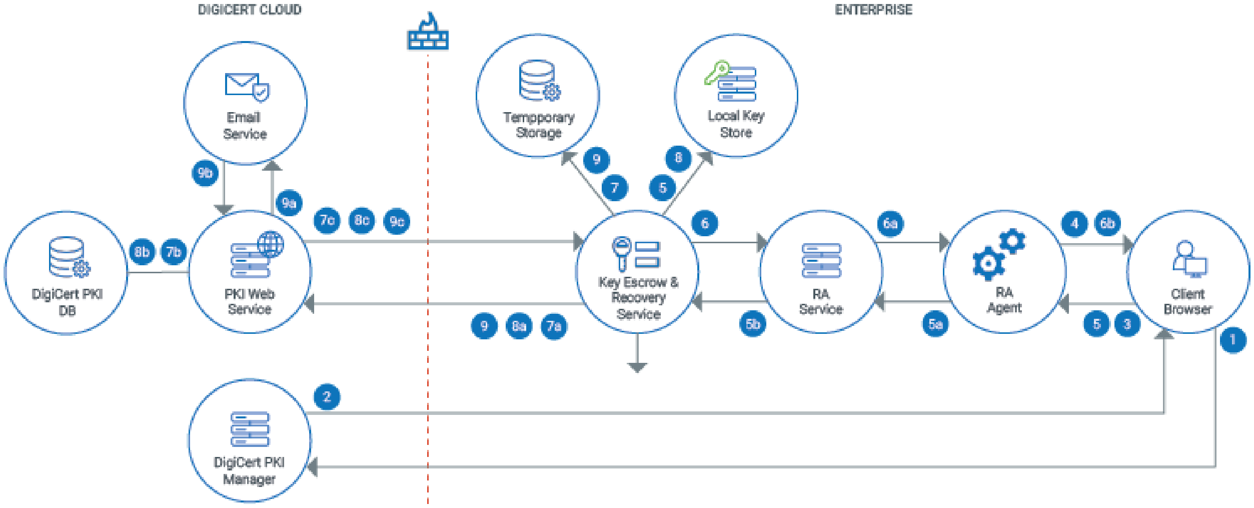


Figure C-1 Import certificate flow

A typical import certificate flow would be as follows:

1. The DigiCert PKI Platform administrator in Enterprise Gateway accesses the DigiCert PKI Manager to migrate the foreign keys to the local key escrow and recovery service.
2. PKI Manager authenticates the request from Enterprise Gateway and generates a response.
3. The administrator sends the response to the Enterprise Gateway RA Agent.
4. The RA Agent validates the request and sends the response to the administrator.
5. The administrator selects a compressed file to upload the imported certificates.

   a) The RA Agent forwards the request to Enterprise Gateway RA Service.
   b) The RA Service submits the compressed file to key escrow and recovery service.

6. The key escrow and recovery service creates and queues a job to process the certificate that is compressed. It imports certificates and sends a response to the RA service.

   a) The RA Service sends the response to the RA Agent.
   b) The RA Agent redirects the administrator.

7. The executor in key escrow and recovery service picks up the job for execution and starts it. It extracts contents of the certificate that is compressed in a temporary storage location.

   a) The key escrow and recovery service communicates with PKI Web service to import the certificates of the issuer chain.
   b) The PKI Web service validates the certificates of issuer chain and stores the information of issuer certificates in DigiCert PKI Platform database.
   c) The PKI Web service returns a reference identifier of the imported issuer CA to the key escrow and recovery service.

8. The key escrow and recovery service job parses and extracts the private key from p12 using the password. It generates a random session key and mask. It encrypts the private key using the session key, and stores the encrypted private key and mask in the local keystore.

   a) For each end-user cert, the job extracts the public key from p12. It masks the session key using mask. And, it sends the public key, masked session key and issuer's reference identifier to PKI Web service.
   b) The PKI Web service stores the public key and masked session key in DigiCert PKI Platform database. The PKI Web service returns a reference identifier of the imported end-user certificate. The key escrow and recovery job updates the reference identifier of end-user certificate in the local keystore.
   c) The key escrow and recovery service job logs the details of the import in a report log file in temporary storage.

9. The job sends a request to send a summary email to the administrator to the PKI Web service. The request contains the information that is required to generate and send the summary email.

   a) The PKI Web service sends the request to send a summary email to the administrator to the Email Service.
   b) The Email Service sends the status of email request to the PKI Web service.
   c) The PKI Web service sends the status of email request to the key escrow and recovery service job.

7.2 Setup and Configuration

7.2.1 Prerequisites

- Administrator account should be created in DigiCert PKI Platform
- Administrator should set up Enterprise and key escrow and recovery service on the enterprise servers
- Administrator should configure Enterprise Gateway and key escrow and recovery service in the administrator account

7.2.2 Configuration

The following is the non-DigiCert key import configuration in the kmsconfig.properties file.

Table C-1 Non-DigiCert key import configuration for the kmsconfig.properties file

Parameter	Required	Default value	Description
common.certificate. zip. extrator.location	Yes	N/A	Full absolute path of the folder where Local Key Management Service extracts the contents of compressed file that is uploaded for certificate import. • LKMS generates a unique jobId for each compressed file uploaded. It then creates a subfolder with the name as <jobId> inside the given folder location. • LKMS extracts the contents of the compressed file inside the subfolder. • LKMS deletes the extracted contents once the import is complete. • LKMS creates a log file with name <jobId>.log inside the given folder location. The administrator should assign appropriate access privileges on the given folder to protect from unauthorized users accessing the private keys. The administrator may encrypt the folder for additional protection. The administrator should periodically delete the log files to prevent the storage from filling up.

Parameter	Required	Default value	Description
common.certificate.import.thread_pool.size	No	5	Number of threads to process compressed the files that are uploaded for certificate import in Local Key Management Service. It also denotes the maximum number of compressed files that can be processed concurrently. If more compressed files are uploaded than the number of available threads, the compressed files wait before they are processed. The customer is allowed to upload any number of compressed files. Each file can have a maximum size of 20 MB. All uploaded compressed files are kept in memory until they are picked up for processing. The maximum number of compressed files that can be uploaded is approximately "Max JVM heap size in MB"/ 40. The customer's administrator can increase "Max JVM heap size" by modifying the value of VM property -Xmx. It is done in the following line in `%TOMCAT_HOME%\bin\start_kmsws.bat:` set JAVA_OPTS=- Dpkiservices.configuration.path=%kmsConfigPath% -Dfile.encoding=UTF-8 -Xmx1024M -Xms256M

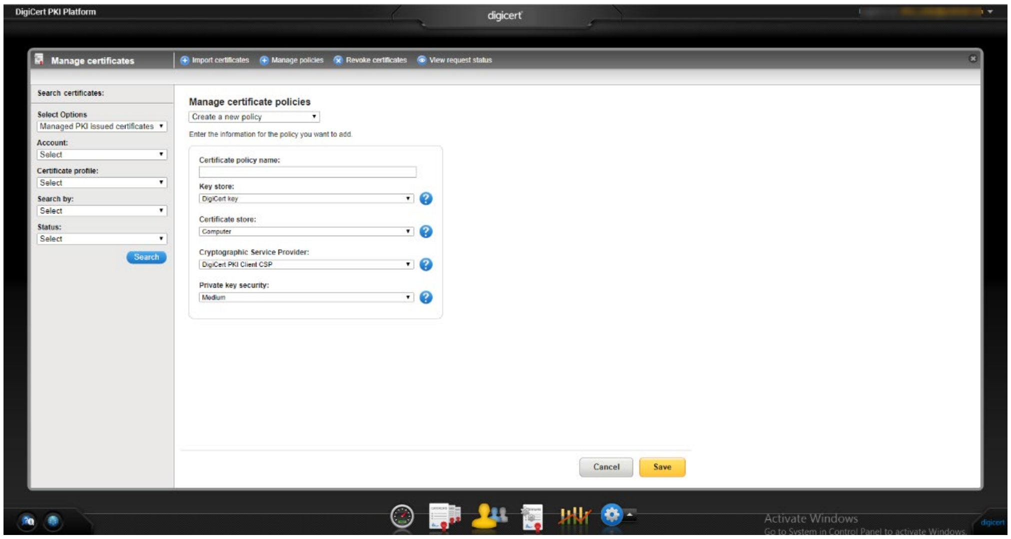
7.2.3 Configuring the keystore

If you plan to use LDAP or Active Directory as a keystore, your administrator should configure the properties kms.keyrecovery.ldap.base.dn and kms.keyrecovery.ldap.keyescrowcontainer.ou in the LKMS `kmsconfig.properties` configuration file. The purpose is to point to a new forest root to store the imported keys. If the properties point to an existing "forest root" that contain data (users' private keys), the data may get overwritten. It may get overwritten during key import and the data might get lost forever.

7.2.4 Manage policies

On the Managed certificates page, you can create a certificate policy.

1. On PKI Manager, click **Manage Certificates** or select **Manage Certificates** from the **Tasks** menu on the bottom navigation bar.
2. Click **Manage policies** from the top of the resulting page. The Manage certificate policies page is displayed.



Search certificates:

Select Options: Managed PKI issued certificates

Account: Select

Certificate profile: Select

Search by: Select

Status: Select

Manage certificate policies

Create a new policy

Enter the information for the policy you want to add.

Certificate policy name:

Key store: DigiCert key

Certificate store: Computer

Cryptographic Service Provider: DigiCert PKI Client CSP

Private key security: Medium

To create a policy:

1. Select Create a new policy from the drop-down list.
2. Enter the information for the policy you want to add. You can choose either DigiCert keystore or local keystore to store your keys.
3. Click **Save**.

To edit a policy:

1. Select the policy from the drop-down list.
2. Edit the certificate policy name. If you have selected a local keystore to store your keys, you cannot edit the other fields.
3. Click **Save**.

7.2.5 Import Certificates

On the Managed certificates page, you can import non-DigiCert certificates. You can use this feature to manage certificates from other solution providers.

1. Select a certificate policy from the drop-down list. The certificate policy settings are displayed based on the keystore that is defined in the Manage policies page.

2. If you have selected your keystore as DigiCert, choose a certificate by selecting **Choose**. The file must be in .zip format and contain certificates as .p12 files. The file size cannot exceed 50 MB.
3. Click **Continue**.
4. If you have selected your keystore as local, then select this check box to access RA Agent to import certificates.
5. Click **Browse** to choose a certificate. The file must be in .zip format and contains certificates as .p12 files. Include any root or intermediate CAs as p7b files. The file size cannot exceed 20 MB.
6. Click **Submit and return to PKI Manager** after the import job is complete.

NOTE: Do not click **Back** or close the browser window as the certificate import operation may take longer time.

7.3 Error codes

PKI Enterprise Gateway returns error codes and the exceptions that may be logged in various emails and reports

Figure C-2 Error codes

Error message code	Exception	Error message
0xA300	WSException	Failed to authenticate request.
0xA301	WSException	Authentication certificate has expired.
0xA302	WSException	Authentication certificate has been revoked.
0xAC01	WSException	The request failed due to an internal error.
0xBF03	ImportCertException	The compressed file data in the request has an invalid format. Correct the request and try again.
0xBF04	ImportCertException	The end-user certificates that are not found in the request. Correct the request and try again.
0xBF05	ImportCertException	The PKCS#7 object that is provided for issuer certificate is not valid or cannot be constructed from the information

Error message code	Exception	Error message
		provided. Rebuild the object correctly and retry the operation.
0xBF06	ImportCertException	The issuing CA information that is not found in the request. Correct the request and try again.
0xBF07	ImportCertException	The PKCS#7 object that is provided for user certificate is not valid or cannot be constructed from the information provided. Rebuild the object correctly and retry the operation.
0xBE01	ImportCertException	The XML file that is uploaded is not valid. Correct the XML file and try again. Refer to the instructions for creating the XML file for the correct format.
0xBE02	ImportCertException	The XML file is not provided in the .zip file uploaded. Add the file and try again.
0xBE03	ImportCertException	The issuing CA (.p7b file) is not listed in the XML file. Add the CA to the XML file and try again.
0xBE04	ImportCertException	The certificate (.p12 file) is not listed in the XML file. Update the XML file or create a new .zip file for this certificate and try again.
0xBE05	ImportCertException	The password for the certificate (.p12 file) is invalid or missing from the XML file. Update the XML file or create a new .zip file for this certificate and try again.
0xBE06	ImportCertException	The issuing CA (.p7b file) for these certificates is not present in the .zip file. Add the issuing CA and try again.
0xBE07	ImportCertException	The issuing CA (.p7b file) is invalid. Provide the correct issuing CA and try again.

Error message code	Exception	Error message
0xBE0B	ImportCertException	The password that is provided does not match the certificate (.p12 file). Update the XML file or create a new .zip file for this certificate and try again.
0xBE0D	ImportCertException	The certificate (.p12 file) is not present in the .zip file. Remove the certificate from the XML file or create a new .zip for this certificate and try again.
0xBE15	ImportCertException	The issuing CA (.p7b file) did not issue the certificate (.p12 file). Provide the correct issuing CA and try again. Or, remove the certificate from the XML file or create a new .zip for this certificate and try again.
0xBE19	ImportCertException	An internal error was made while the .zip file loaded. Try again. If the problem persists, then contact DigiCert customer support.

7.4 Known Issues

The following issue occurs only when the non-DigiCert issued certificates is imported to DigiCert PKI Platform.

Issue: When a non-DigiCert certificate is imported to DigiCert PKI Platform and if it has multi attribute Subject DN and issuer DN attributes, the certificate details in PKI Manager displays + as separator.

Resolution: There is no workaround for this issue.

APPNEDIX D

8 Error Codes and Troubleshooting

This appendix includes the following topics:

- PKI Enterprise Gateway Logging
- PKI Enterprise Gateway Error Codes
- Common PKI Enterprise Gateway Issues

8.1 PKI Enterprise Gateway Logging

PKI Enterprise Gateway writes the following logs. Use these logs to assist with troubleshooting errors.

8.1.1 Installation Script Logs

The PKI Enterprise Gateway installation script writes logs for all installation operations (such as EGWSetup.exe) to the %PUBLIC% folder. These scripts are useful for troubleshooting. However, EGWSetup.exe writes the logs (called Summary files) that also include the system information that is needed when configuring the PKI Enterprise Gateway.

8.1.2 Component Logs

PKI Enterprise Gateway components (RA Service, RA Agent, and authentication service) write the following log files on the computer on which they are installed:

- <install_dir>/Applications/RAService/log/RAService.log
- <install_dir>/Applications/AuthenticationService/log/AuthenticationService.log
- <install_dir>/Applications/RAAgent/log/RAAgent.log

By default, logs include details at the INFO level. The log includes the informational messages that identify the health and status of the service. When troubleshooting an issue, you may want to change the logs to report more detail.

1. In a standard text editor, open the web.config file for the component you want to troubleshoot. This file is in the <install_dir>/Applications/<component name> folder, where <component name> is RA Agent, RAService, or authentication service.
2. Locate the **level** element under **configuration > log4net > root**.
3. Change the value of this element from INFO to DEBUG.
4. Restart the component on the IIS server.

Once you have completed troubleshooting, change DEBUG back to INFO, as the DEBUG level causes the log files to use more space.

8.2 PKI Enterprise Gateway Error Codes

PKI Enterprise Gateway returns most errors directly to the PKI Certificate Service. The Service displays user-readable messages rather than the error code and string. Your end users should refer to the displayed error message and associated help in PKI Certificate Service for resolution of these errors. However, the following PKI Enterprise Gateway errors are displayed as the original error code and string by PKI Certificate Services. If your end users encounter one of these errors, they need to contact an administrator for assistance. Refer to Table D-1 for information on how to resolve these errors.

Table D-1 PKI Enterprise Gateway error codes

Error Code	Error message	Solution
A901	SERVICE_INTERNAL_ERROR	An unexpected error in the PKI Enterprise Gateway. One possible cause is that the password for the domain user running the RA Service has expired or has been reset in the user store. Update the password in the Connectivity Pool (See "Updating the Windows User Name and Password (Connectivity Pool Information)"). If your security policies allow, you can set the password to never expire to avoid this issue in the future. Otherwise, review your PKI Enterprise Gateway logs and contact DigiCert Technical Support.
A902	SERVICE_AUTHENTICATION_ERROR	The end user was not authenticated against the enterprise user store. Verify that the end user uses the correct credentials to access the PKI Certificate Service. Also, verify that the end user's account is not locked out.
A903	SERVICE_AUTHORIZATION_ERROR	The end user does not belong to the user store user group that is

Error Code	Error message	Solution
		assigned to the requested certificate profile. The error occurs when the user accesses an incorrect PKI Certificate Service URL.
A904	SERVICE_ATTRIBUTE_NOT_FOUND	The user store service that is configured in the certificate profile does not exist in the user store. Correct the certificate profile in PKI Manager.
A905	SERVICE_PROFILE_ID_INCORRECT	The certificate profile ID does not belong to the account. Contact DigiCert Technical Support.
A906	SERVICE_CONNECTION_ERROR	The RA Service cannot connect to the DigiCert Certificate Authority. Verify that the RA Service is running and is able to access the DigiCert Certificate Authority. Also, verify if your certificate profile is mapped to the RA certificate. On the RA Service computer, log in as the user that installed the RA Service. • Open a browser window and enter the following URL in the address bar: https://pki-ws.symauth.com /pki-ws/enrollmentService?wsdl • The browser returns a response indicating if the RA Service can access the DigiCert Certificate Authority
A907	SERVICE_USER_NOT_FOUND	The end user was not found in the user store. The error can happen if you use multiple user stores for

Error Code	Error message	Solution
		failover and your user data is not replicated correctly.
A908	SERVICE_MISSING_DATA	Your user store has an empty value for an attribute that is marked as required in your certificate profile. Populate the data for that user attribute in your user store or correct the certificate profile in PKI Manager.
A909	SERVICE_MISMATCHED_DATA	The data in your end user's certificate enrollment request does not match the data in your user store. Contact DigiCert Technical Support.
A90A	SERVICE_CONFIGURATION_ERROR	Your PKI Enterprise Gateway is configured incorrectly. Review your PKI Enterprise Gateway logs to correct the issue.
A90B	SERVICE_CERTIFICATE_PUBLISH_FAILED	The RA Service cannot write the certificate data to the user store. Make sure that the user running the RA Service has the correct permissions to write to the user store. Make sure that the user store is running and accessible by the RA Service.
A90C	SERVICE_CERTIFICATE_RECOVERY-FAIL	PKI Manager is not able to authenticate the recover private key request coming from Enterprise Gateway. To resolve this issue, make sure that the user certificate is not already recovered or expired.
A91B	SERVICE_TOKEN_AUTHENTICATION_ERROR	Enterprise Gateway is not able to authenticate the KeyRecovery token request coming from PKI Manager. To resolve this issue,

Error Code	Error message	Solution
		make sure KeyRecovery has a valid value for token attribute or contact DigiCert Technical Support.
A919	SERVICE_CERTIFICATE_IMPORT_IMPORT_FAIL	Insufficient parameters are passed from PKI Manager. Retry the operation. If it still fails, contact DigiCert Technical Support with RA Agent log.

8.3 Common PKI Enterprise Gateway Issues

The following are some of the common issues that you may encounter when you install or run PKI Enterprise Gateway, along with typical solutions.

8.3.1 Overwriting Existing Instances of PKI Enterprise Gateway

From version 1.4 of PKI Enterprise Gateway onwards, you are only able to install one instance of the gateway on a computer. Additionally, the installer now tracks instances of PKI Enterprise Gateway. As a result:

- If you attempt to install the PKI Enterprise Gateway in the same directory as an existing instance, you are prompted to uninstall the existing program.
- If you install PKI Enterprise Gateway and later attempt to install another instance, the installer prompts you to uninstall the first instance before you continue. You are prompted regardless of where on the computer the first instance was installed.

However, the installer does not prompt you to uninstall instances of the previous versions that were installed in different directory locations.

See "Installing PKI Enterprise Gateway".

8.3.2 My users are not able to access the PKI Enterprise Gateway from the browser.

PKI Enterprise Gateway uses the fully-qualified domain name (FQDN) of the IIS servers hosting the gateway components. If your security policy disallows revealing your fully-qualified domain name (FQDN) to people outside your domain, PKI Enterprise Gateway users are not allowed access.

You must modify your DNS configuration so that your FQDN can be resolved correctly.

8.3.3 My end users are prompted for their Windows user name and password as they enroll for certificates.

For Active Directory only: If the authentication service URL is not set as a trusted intranet site for your user's browsers. Users are prompted for their Windows user name and password when you enroll for certificates. They are prompted even if they are already logged into the network domain. While this prompt does not affect enrollment, you may want to turn off this prompt for your end users. To do so, have your end users add the authentication service URL as a trusted intranet site to their browsers.

Optionally, you can configure this setting on behalf of your users. Refer to your Active Directory documentation for instructions on how a network administrator may push browser configuration changes to remote users.

For Internet Explorer:

1. Click **Tools > Internet** Options.
2. In the resulting **Internet Options** dialog box, click the **Security** tab.
3. Click **Sites** under **Trusted sites**.
4. Enter the Authentication Aervice URL and click **Add**.

For Firefox:

1. Enter **about:config** in the address bar. You may be prompted to accept a security warning.
2. Type **network.automatic-ntlm-auth.trusted-uris** in the Filter box.
3. Double-click **network.automatic-ntlm-auth.trusted-uris** and enter the Authentication Service URL.

8.3.4 Certificate Enrollment Failures

Enrollments fail, if user store objects have NULL values in the attributes that the certificate profile defines as mandatory attributes. Make sure that all mandatory user attributes are populated in the user store. Optionally, you may change the mandatory attributes in your certificate profile.

8.3.5 Handling multi-valued user store Attributes in PKI Enterprise Gateway

If you have mapped a multi-valued attribute to a Subject Alternative Name or Subject Distinguished Name in PKI Manager, multiple values may be returned. In this situation, PKI Enterprise Gateway picks the first value from the list. Active Directory and LDAP user stores do not guarantee the same order for each fetch operation. Therefore, the value may not be the same with each operation call.

You must plan for these value selections.

NOTE: If you map the proxyAddresses attribute, PKI Enterprise Gateway always uses the primary SMTP address from this attribute list.

8.3.6 Authorization fails for Internet Explorer for Active Directory users

On PKI Enterprise Gateway, when you try to do enrollment using Internet Explorer browser, an error is displayed after you enter user credentials.

To configure Internet Explorer to avoid this issue:

1. Click **Tools > Internet Options**.
2. In the resulting **Internet Options** dialog box, click the **Advanced** tab.
3. You must deselect **Enable Integrated Windows Authentication** under Security settings.
4. Click **OK**.

The authorization or enrollment should work after these changes are made.

8.3.7 Performance improvement on LDAP server

On PKI Enterprise Gateway: When you use LDAP user store to enroll certificates, you should index your LDAP server with 'dn' or 'member' attributes to improvethe query.

For example, for Novell eDirectory LDAP:

```
ndsindex add [-h hostname] [-p port] -D <bind DN> -W|[-w password]
[-l limit] -s <Server DN> <indexDefinition1> [<indexDefinition2> ...]
ndsindex delete [-h hostname] [-p port] -D <bind DN> -W|[-w password]
      [-l limit] -s <Server DN> <indexName1> [<indexName2> ...]
```

8.3.8 Enable directory browsing in IIS

You need to enable directory browsing when you want browsers to display the PKI Manager web page. By default, directory browsing is disabled in IIS.

Complete the following steps to enable the **Directory Browsing** setting in IIS Manager.

1. From IIS Manager, click **Site** from the left navigation pane.
2. Double-click **Directory Browsing** and select all the available options from the check box.
3. Click **Enable**.
4. Enter the URL https://<MPKI server>:9100/PolicyService.svc?wsdl.

9 Index