

Enterprise Password Manager

Gopi Krishna Ganti

Installation Guide

Disclaimer

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of the author.

Apple, Android, Oracle, Microsoft are the trademarks of their respective organizations.

Table of Contents

1 INTRODUCTION	2
1.1 AUDIENCE.....	2
2 ABBREVIATION	3
3 INSTALLING ENTERPRISE PASSWORD MANAGER.....	3
3.1 PRE-REQUISITES.....	3
3.1.1 Web Server / Application Server.....	3
3.1.2 Database Server	4
3.1.3 Active Directory.....	4
3.1.3.1 Configuring an SSL Certificate for Microsoft Active Directory.....	4
3.1.3.1.1 Prerequisites.....	4
3.1.3.1.2 Install the Active Directory Certificate Services.....	5
3.1.3.1.3 Obtain the Server Certificate	15
3.1.3.1.4 Import the Server Certificate.....	16
3.1.3.1.4.1 Windows.....	16
3.1.3.1.4.2 UNIX	16
3.1.3.1.4.3 Mac OS X.....	17
3.2 PREPARING TO INSTALL	17
3.2.1 Run database scripts	18
3.2.2 Deploy application	18
3.2.3 Configure the application.....	18
4 LIST OF ALL FIGURES	19

1 Introduction

The Installation Guide covers complete installation steps like pre-requisites, etc. of Enterprise Password Manager.

1.1 Audience

This manual is targeted for users who are responsible for evaluating, installing and maintenance of Enterprise Password Manager in an organization. Typically, the user would be the Enterprise Password Manager Administrator.



2 Abbreviation

AD	Active Directory
LDAP	Lightweight Directory Access Protocol
EPM	Enterprise Password Manager
TCP	Transmission Control Protocol
SSL	Secure Socket Layer
URL	Uniform Resource Locator (web server address typed in a browser)
IP	Internet Protocol

3 Installing Enterprise Password Manager

3.1 Pre-Requisites

Before proceeding with the steps for installation of EPM, please go through System Requirements document and make sure the all the system requirements are met. Below mentioned is the list of pre-requisites that are required for EPM to be configured and start using it.

- Web Server / Application Server
- Database Server
- Active Directory (SSL enabled)

3.1.1 Web Server / Application Server

EPM application is bundled as WAR file that needs to be deployed in the web server/ application server. Supported webserver and application servers are

- ✓ Tomcat
- ✓ JBoss
- ✓ Websphere
- ✓ Weblogic



3.1.2 Database Server

Backend data source used is database server. Supported database servers are Oracle and MS SQL. EPM communicates with backend database over TCP. Hence TCP connection needs to be enabled for the database. Check with your DBA for the same.

3.1.3 Active Directory

Active Directory needs to be SSL enabled for EPM to work. This is required since AD needs to be SSL enabled for the creation of user and the change of user password.

3.1.3.1 Configuring an SSL Certificate for Microsoft Active Directory

For EPM to add users or change passwords in AD, you will need to install an SSL certificate generated by your Active Directory server and then install the certificate into your JVM keystore.

Steps on this:

- Prerequisites
- Install the AD Certificate Services
- Obtain the Server Certificate
- Import the Server Certificate

Updating user, group, and membership details in Active Directory requires that your application be running in a JVM that trusts the AD server. To do this, we generate a certificate on the Active Directory server, and then import it into Java's **keystore**.

3.1.3.1.1 PREREQUISITES

To generate a certificate, you need the following components installed on the Windows Domain Controller to which you're connecting.

Required Component	Description
Internet Information Services (IIS)	This is required before you can install Windows Certificate Services.
Windows Certificate Services	This installs a certification authority (CA) which is used to issue certificates. 3.1.3.1.2, below, explains this process.
Windows 2000 Service Pack 2	Required if you are using Windows 2000
Windows 2000 High Encryption Pack (128-bit)	Required if you are using Windows 2000. Provides the highest available encryption level (128-bit).



3.1.3.1.2 INSTALL THE ACTIVE DIRECTORY CERTIFICATE SERVICES

If Certificate Services are already installed, skip to **Error! Reference source not found.**, below. The screenshots below are from Server 2008, but the process is similar for Server 2000 and 2003.

- Log in to your Active Directory server as an administrator.
- Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
- In the **Roles Summary** section, click **Add Roles**.

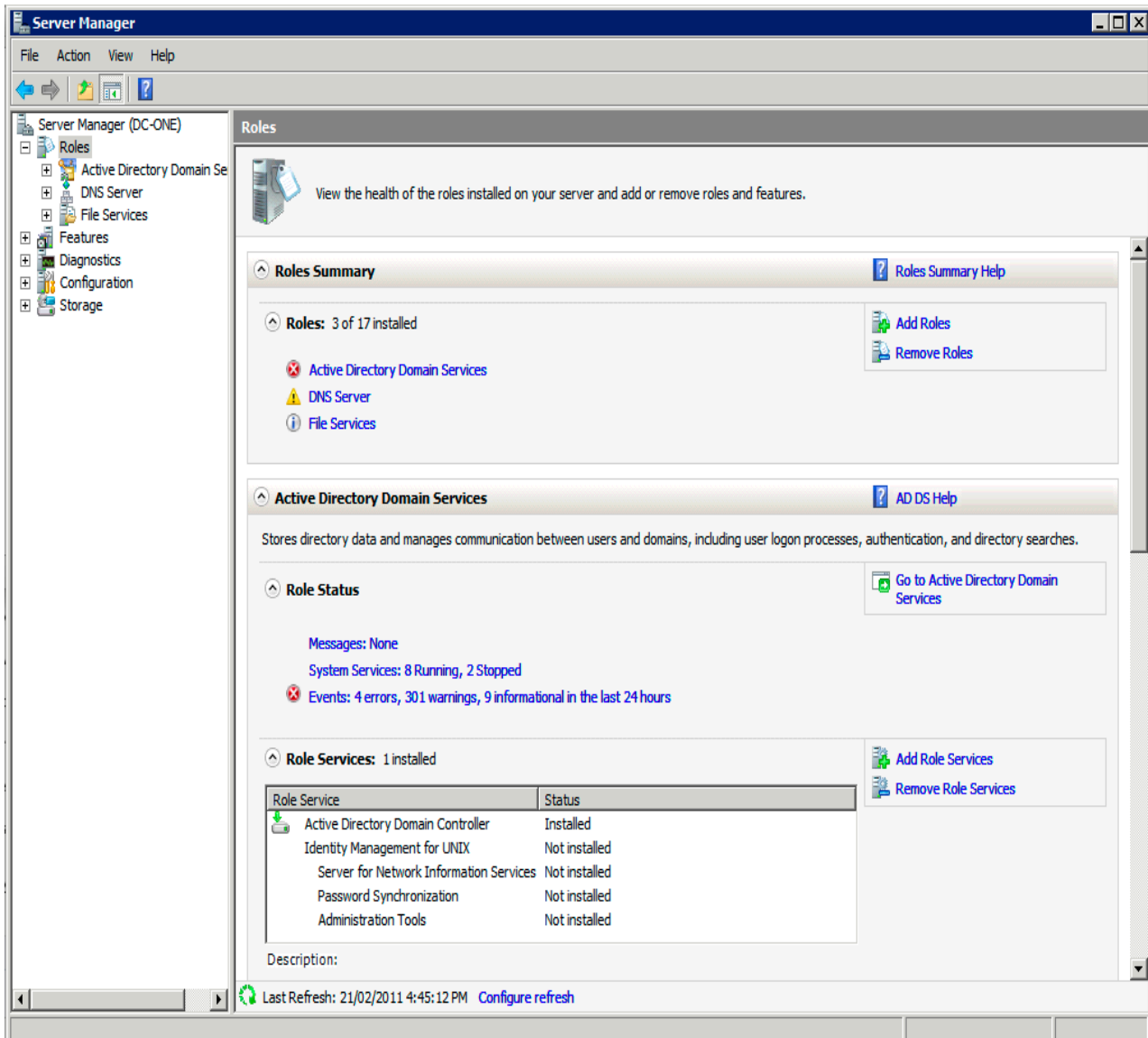


Figure 1 – Roles Summary



- On the **Select Server Roles** page, select the **Active Directory Certificate Services** check box. Click “Next” twice.

Add Roles Wizard

Select Server Roles

Before You Begin

Server Roles

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Certificate Request

Certificate Database

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

- ☒ Active Directory Certificate Services
- ☒ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☒ DNS Server (Installed)
- ☐ Fax Server
- ☒ File Services (Installed)
- ☐ Network Policy and Access Services
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description:

[Active Directory Certificate Service: \(AD CS\)](#) is used to create certification authorities and related role service that allow you to issue and manage certificates used in a variety of applications

[More about server roles](#)

< Previous Next > Install Cancel

Figure 2 – Server Roles



- On the **Select Role Services** page, select the **Certification Authority** check box, and then click “**Next**”.

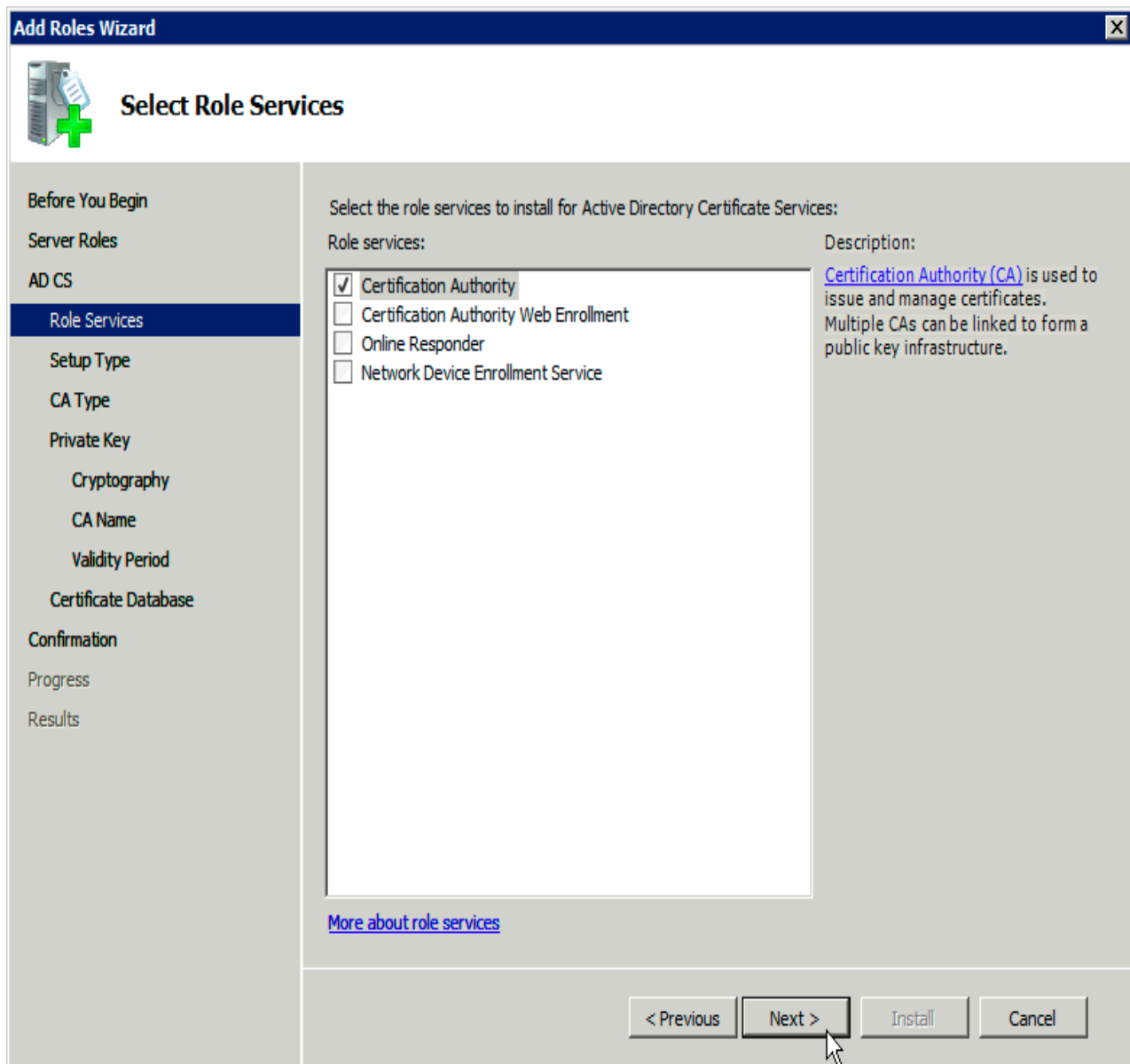


Figure 3 – Role Services



- On the **Specify Setup Type** page, click **Enterprise**, and then click “**Next**”.

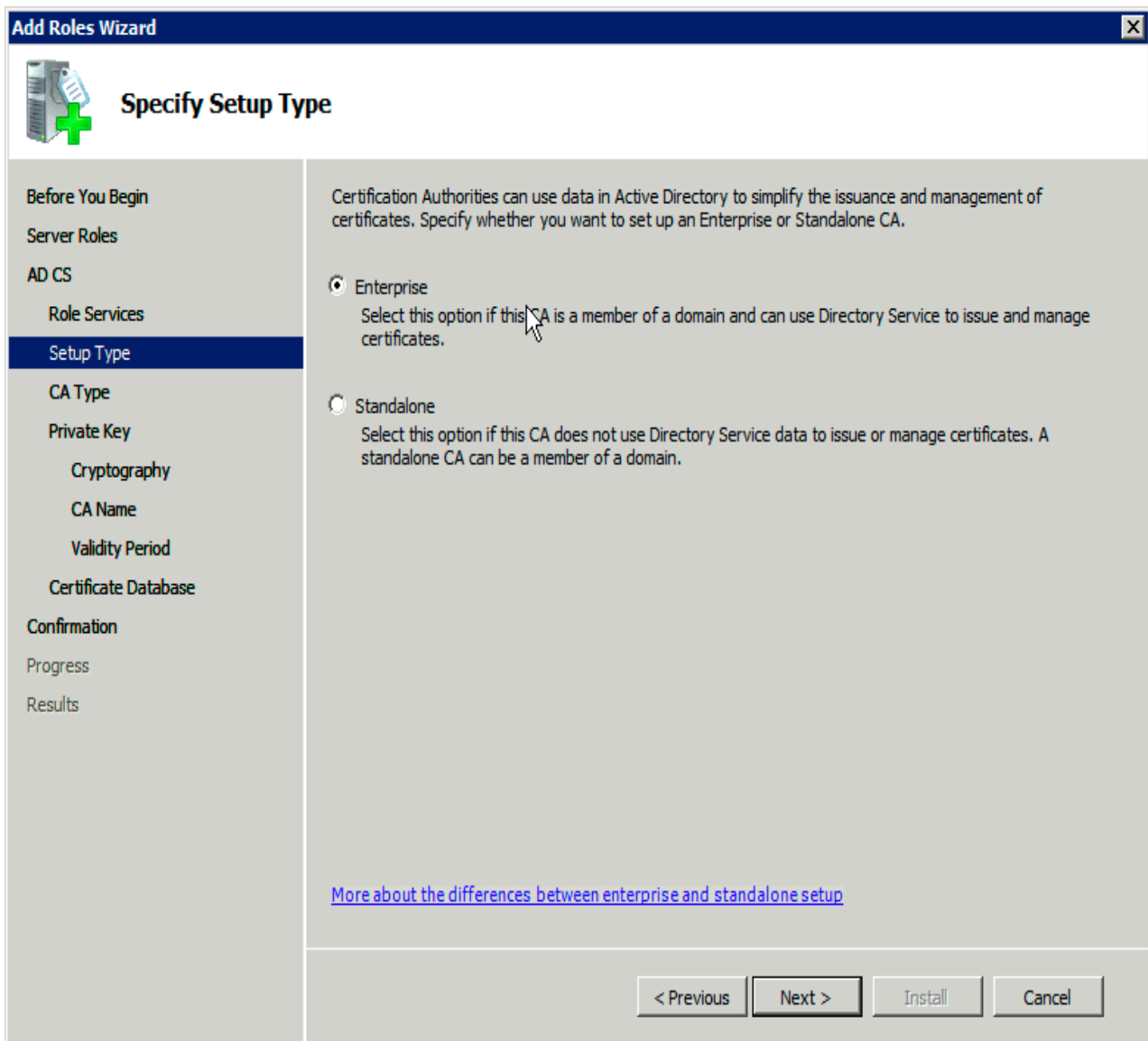


Figure 4 - Setup Type



- On the **Specify CA Type** page, click **Root CA**, and then click “Next”.

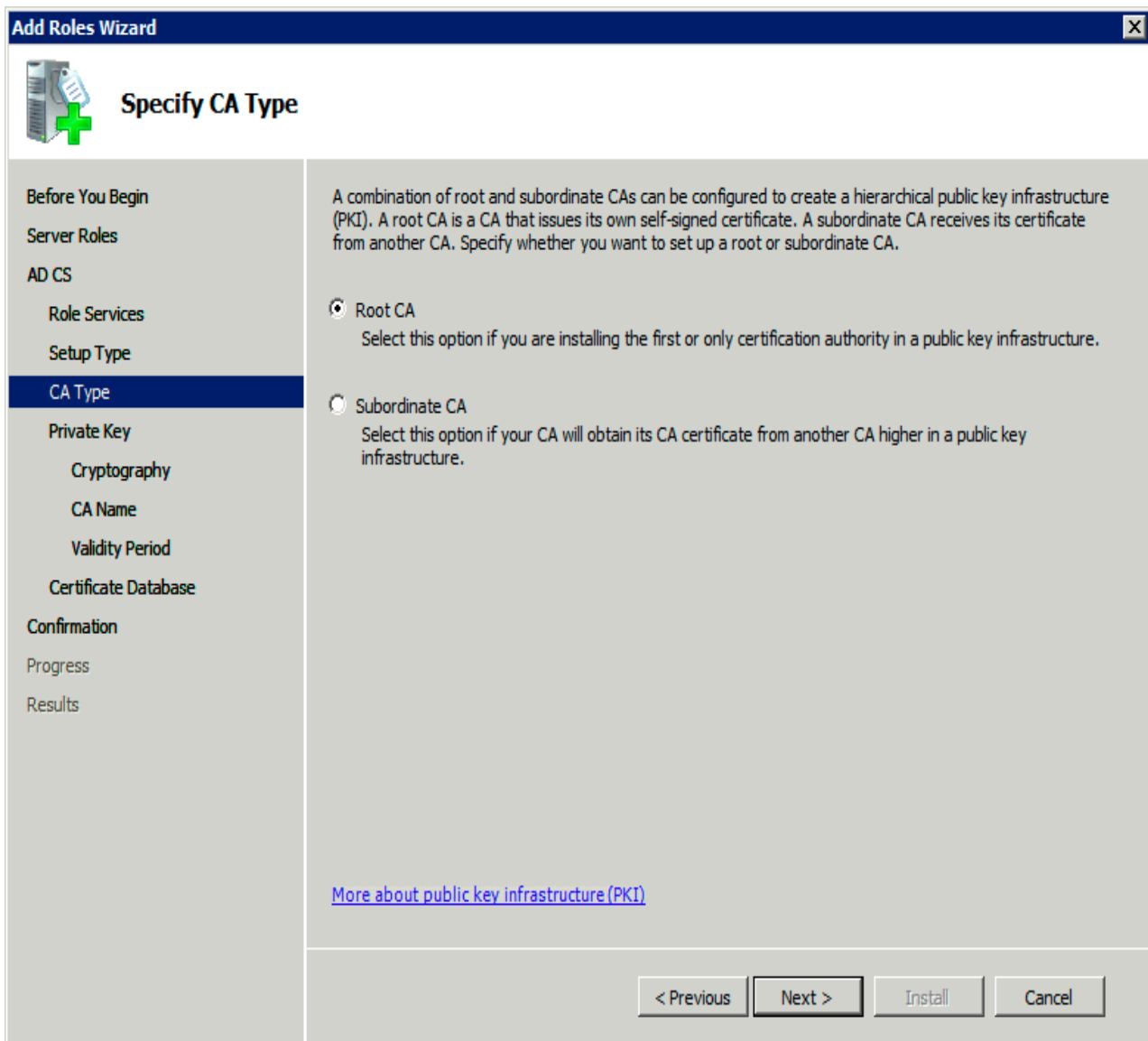


Figure 5 - Specify CA Type



- On the **Set Up Private Key** and **Configure Cryptography for CA** pages, you can configure optional configuration settings, including cryptographic service providers. However, the default values should be fine. Click “**Next**” twice.

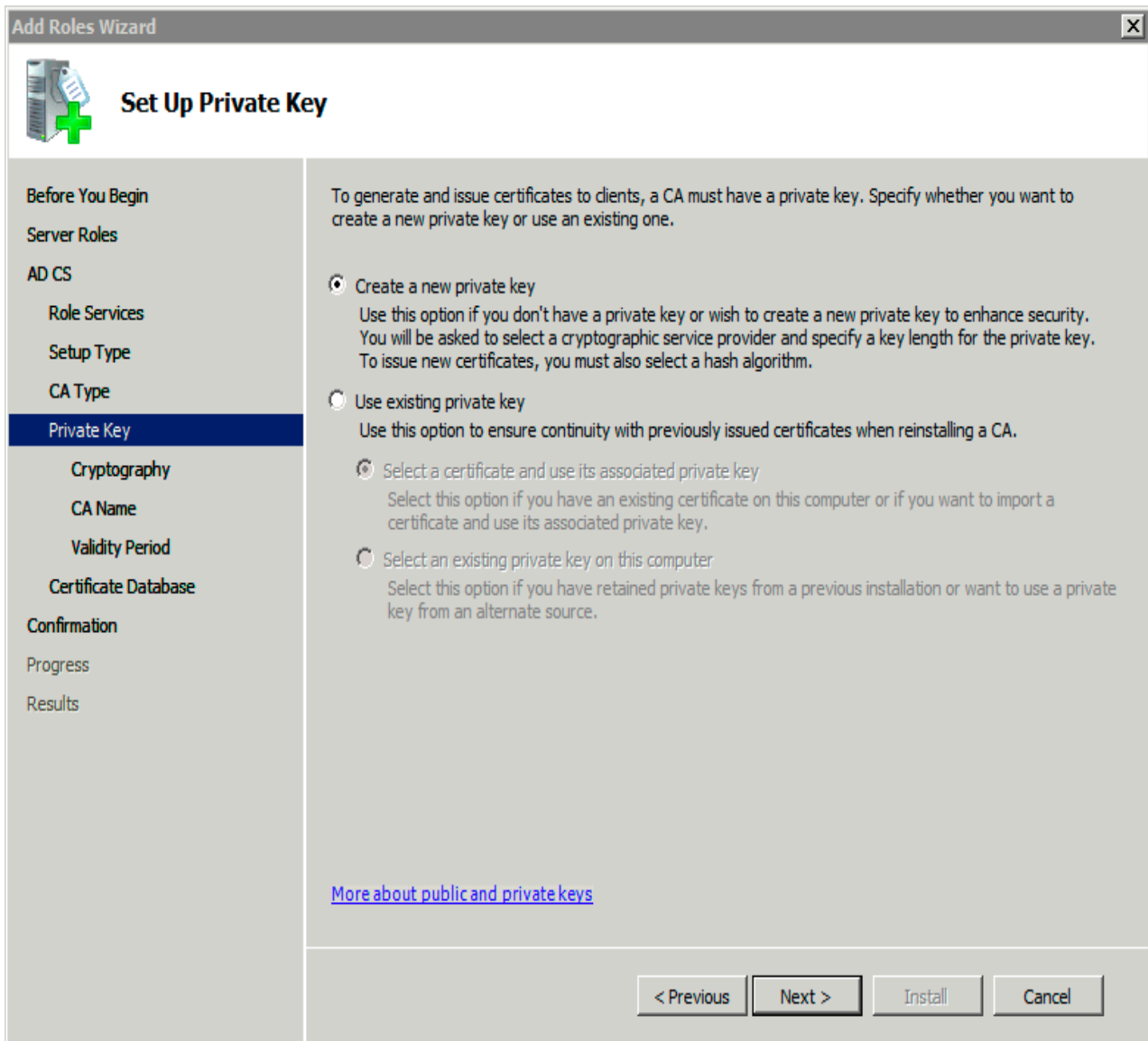
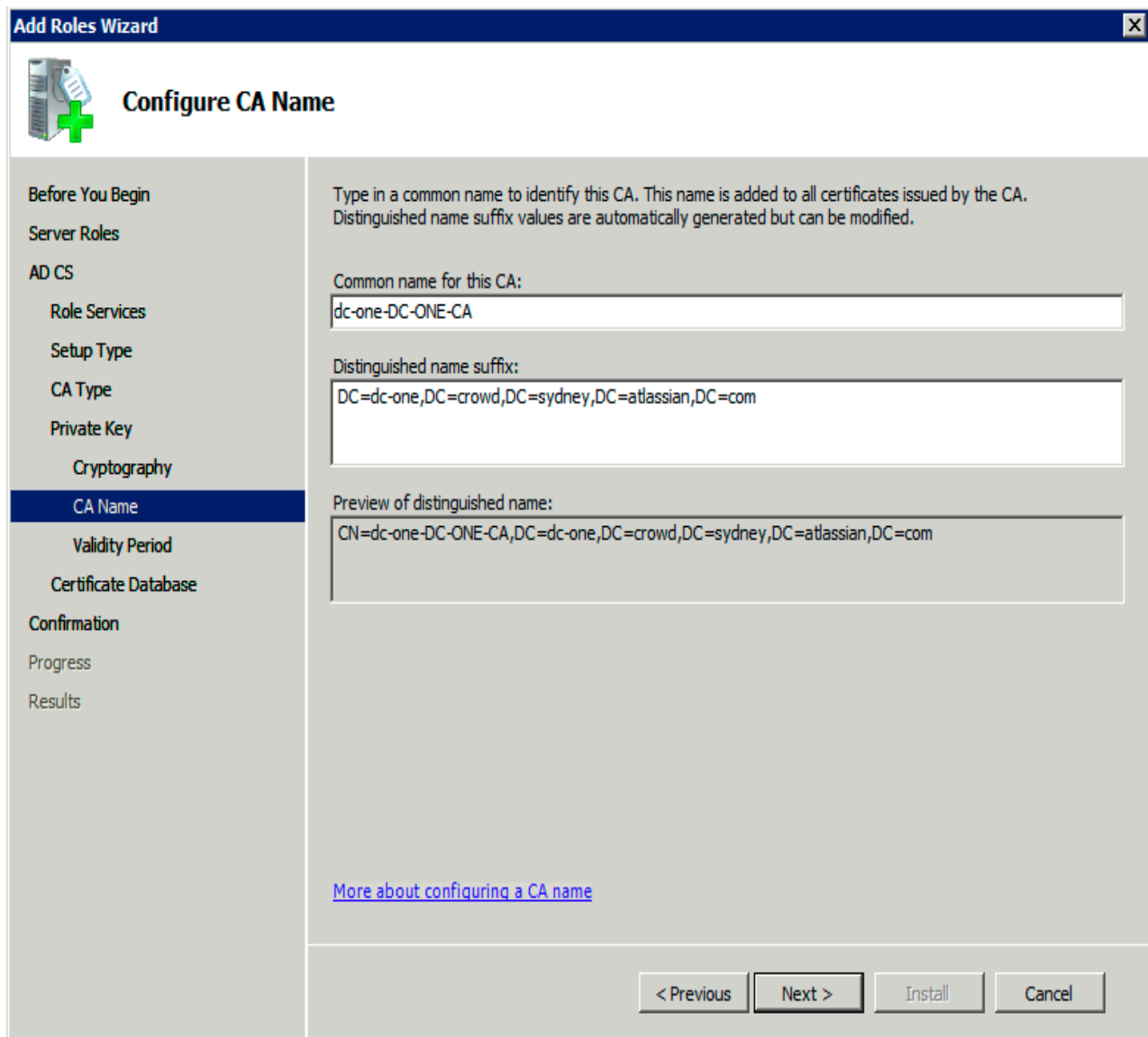


Figure 6 - Set Up Private Key



- In the **Common name for this CA** box, type the common name of the CA, and then click “Next”.

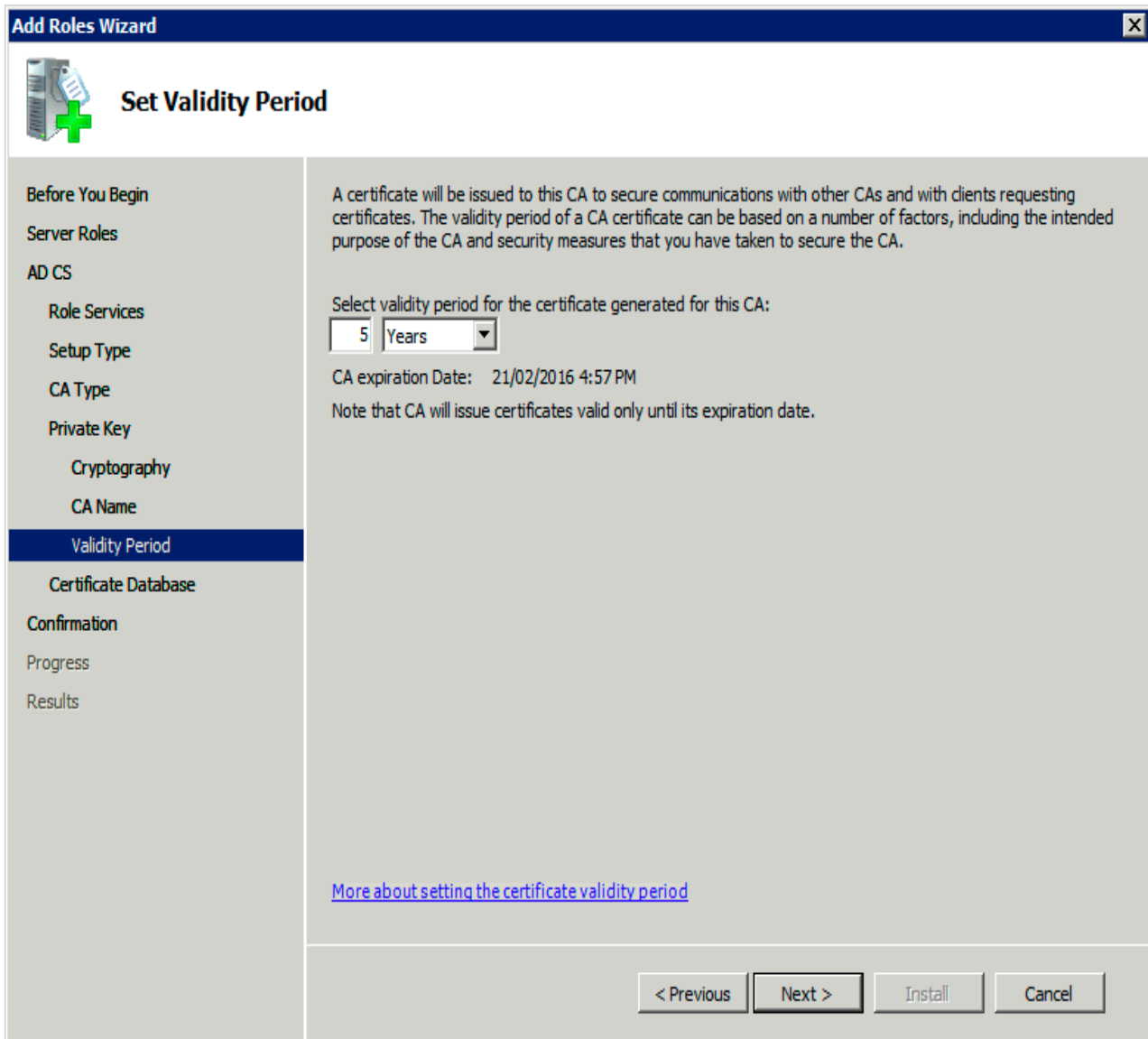


The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard' and a close button. The main window has a green plus icon and the title 'Configure CA Name'. On the left is a navigation pane with the following items: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name' (highlighted), 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area contains the following text: 'Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.' Below this are three text boxes: 'Common name for this CA:' with the value 'dc-one-DC-ONE-CA', 'Distinguished name suffix:' with the value 'DC=dc-one,DC=crowd,DC=sydney,DC=atlassian,DC=com', and 'Preview of distinguished name:' with the value 'CN=dc-one-DC-ONE-CA,DC=dc-one,DC=crowd,DC=sydney,DC=atlassian,DC=com'. At the bottom right are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about configuring a CA name' is located above the 'Next >' button.

Figure 7 - Configure CA Name



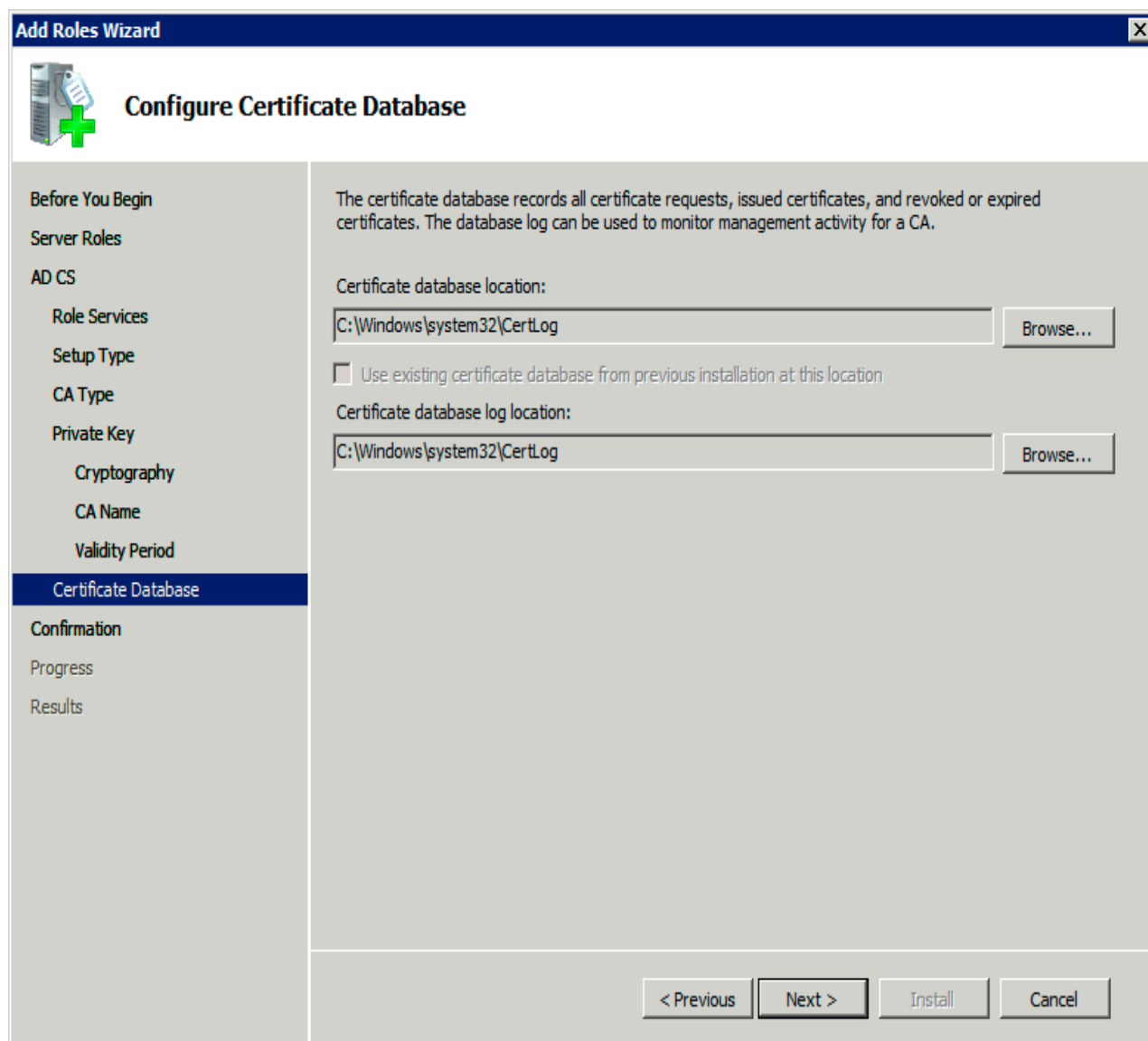
- On the **Set Validity Period** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and then click “**Next**”.



The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard' and a close button. The main window has a green plus icon and the title 'Set Validity Period'. On the left is a navigation pane with the following items: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period' (highlighted), 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area contains the following text: 'A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.' Below this is a label 'Select validity period for the certificate generated for this CA:' followed by a text box containing '5' and a dropdown menu showing 'Years'. Below that is the text 'CA expiration Date: 21/02/2016 4:57 PM' and a note 'Note that CA will issue certificates valid only until its expiration date.' At the bottom of the main area is a blue hyperlink 'More about setting the certificate validity period'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Figure 8 - Set Validity Period





Add Roles Wizard

Configure Certificate Database

The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

Certificate database location:
C:\Windows\system32\CertLog Browse...

☐ Use existing certificate database from previous installation at this location

Certificate database log location:
C:\Windows\system32\CertLog Browse...

Navigation: < Previous | Next > | Install | Cancel

Left Panel:

- Before You Begin
- Server Roles
- AD CS
 - Role Services
 - Setup Type
 - CA Type
 - Private Key
 - Cryptography
 - CA Name
 - Validity Period
- Certificate Database**
- Confirmation
- Progress
- Results

Figure 9 - configure Certificate Database



- After verifying the information on the **Confirm Installation Selections** page, click **Install**.

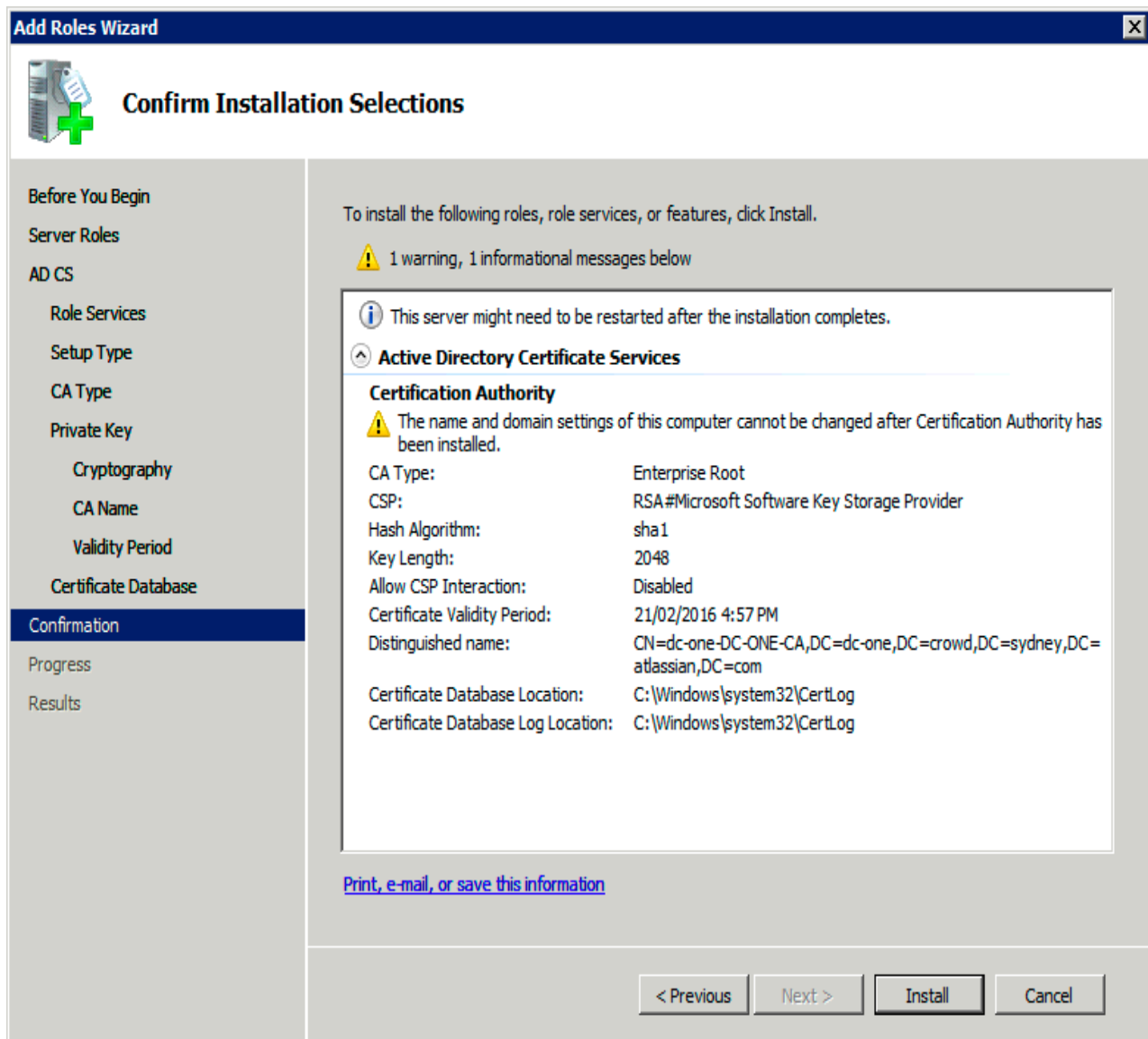


Figure 10 - Confirm Installation Selections



- Review the information on the results screen to verify that the installation was successful.

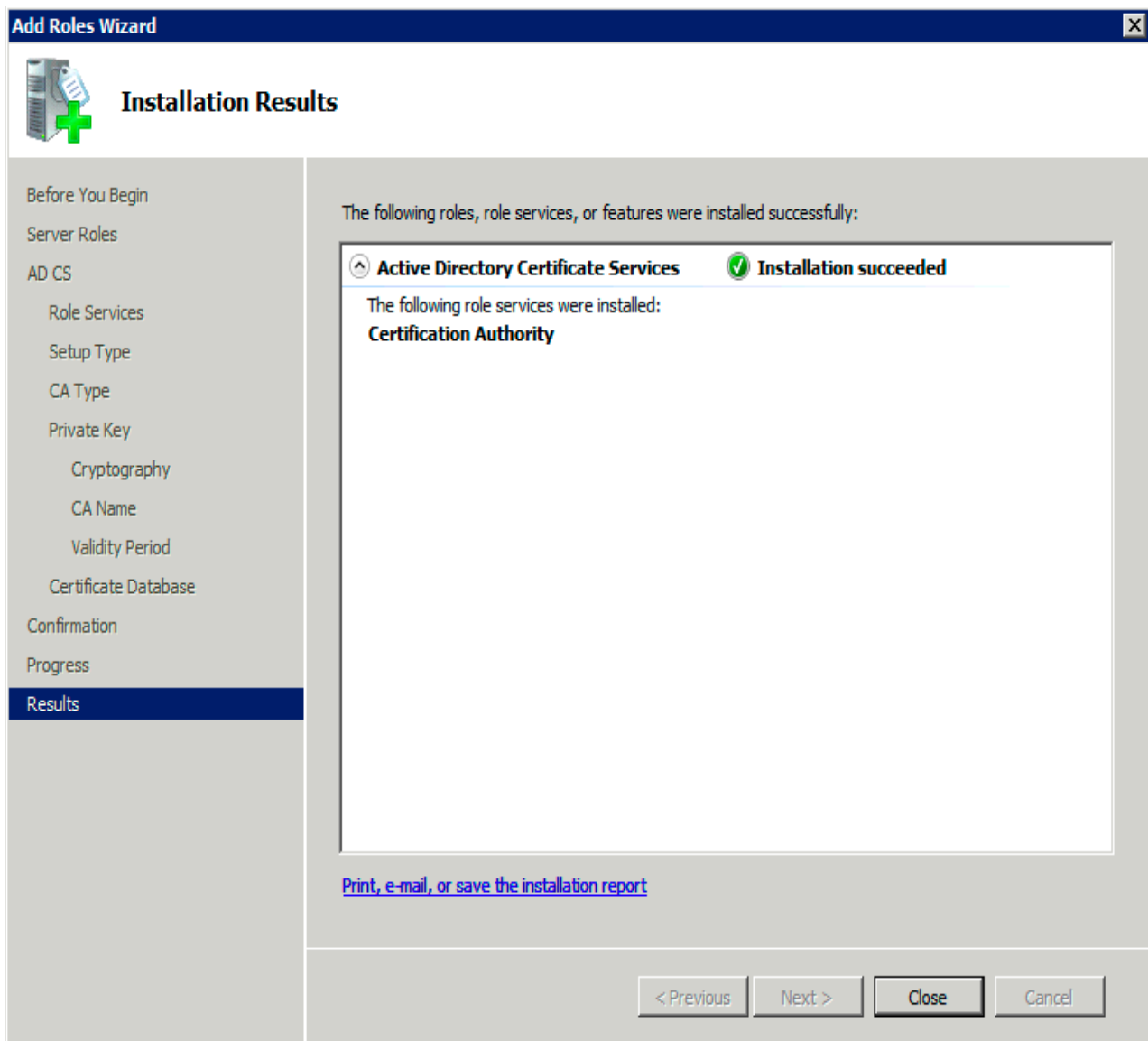


Figure 11 - Installation Results

3.1.3.1.3 OBTAIN THE SERVER CERTIFICATE

The steps above describe how to install the certification authority (CA) on your Microsoft Active Directory server. Next, you will need to add the Microsoft Active Directory server's SSL certificate to the list of accepted certificates used by the JDK that runs your application server.

The Active Directory certificate is automatically generated and placed in root of the C:\ drive, matching a file format similar to the tree structure of your Active Directory server. For example: C:\epmtest.epmdom.com_cauth.crt.



You can also export the certificate by executing this command on the Active Directory server:

```
certutil ca.cert client.crt
```

3.1.3.1.4 IMPORT THE SERVER CERTIFICATE

For an application server to trust your directory's certificate, the certificate must be imported into your Java runtime environment. The JDK stores trusted certificates in a file called a keystore. The default keystore file is called **cacerts** and it lives in the **jre/lib/security** sub-directory of your Java installation.

In the following examples, we use **server-certificate.crt** to represent the certificate file exported by your directory server. You will need to alter the instructions below to match the name actually generated. Once the certificate has been imported as per the below instructions, you will need to restart the application to pick up the changes.

3.1.3.1.4.1 Windows

- Navigate to the directory in which Java is installed. It's probably called something like `C:\Program Files\Java\jdk1.5.0_12`.
- Run the command below, where `server-certificate.crt` is the name of the file from your directory server:

```
C:\> keytool -import -keystore $JAVA_HOME\lib\security\cacerts  
file C:\ server-certificate.crt -alias epmkey
```

- `keytool` will prompt you for a password. The default keystore password is `changeit`.
- When prompted `Trust this certificate? [no]:` enter `yes` to confirm the key import:

```
Enter keystore password:  
Owner: CN=cauth, DC=epmdom, DC=com  
Issuer: CN=cauth, DC=epmdom, DC=com  
Serial number: 59a7289f7f5d868e4fe4c1e8913d2265  
Valid from: Wed May 15 08:12:26 GMT+05:30 2013 until:  
Tue May 15 08:19:10 GMT+05:30 2018  
Certificate fingerprints:  
MD5: 98:CB:DD:87:FF:C1:46:E4:45:75:50:38:81:7F:A8:2B  
SHA1: CD:1C:92:16:3C:3A:E4:BB:B5:9A:FB:41:61:E9:5E:D2:94:0D:DC:EB  
Signature algorithm name: SHA1withRSA  
Version: 3  
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

3.1.3.1.4.2 UNIX

- Navigate to the directory in which Java is installed. `cd $JAVA_HOME` will usually get you there. For latest java from Oracle it can be `/usr/lib/jvm/java-7-oracle`.
- Run the command below, where `server-certificate.crt` is the name of the file from your directory server:




```
$ sudo keytool -import -keystore /usr/lib/jvm/java-7-  
oracle/lib/security/cacerts file $HOME/server-certificate.crt  
-alias epmkey
```

- c. keytool will prompt you for a password. The default keystore password is changeit.
- d. When prompted Trust this certificate? [no]: enter yes to confirm the key import:

```
Enter keystore password:  
Owner: CN=cauth, DC=epmdom, DC=com  
Issuer: CN=cauth, DC=epmdom, DC=com  
Serial number: 59a7289f7f5d868e4fe4c1e8913d2265  
Valid from: Wed May 15 08:12:26 GMT+05:30 2013 until:  
Tue May 15 08:19:10 GMT+05:30 2018  
Certificate fingerprints:  
MD5: 98:CB:DD:87:FF:C1:46:E4:45:75:50:38:81:7F:A8:2B  
SHA1: CD:1C:92:16:3C:3A:E4:BB:B5:9A:FB:41:61:E9:5E:D2:94:0D:DC:EB  
Signature algorithm name: SHA1withRSA  
Version: 3  
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

3.1.3.1.4.3 Mac OS X

- a. Navigate to the directory in which Java is installed. Usually it would be /System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Home
- b. Run the command below, where server-certificate.crt is the name of the file from your directory server:

```
$ sudo keytool -import -keystore $JAVA_HOME/lib/security/cacerts  
file $HOME/Documents/ server-certificate.crt -alias epmkey
```

- c. keytool will prompt you for a password. The default keystore password is changeit.
- d. When prompted Trust this certificate? [no]: enter yes to confirm the key import:

```
Enter keystore password:  
Owner: CN=cauth, DC=epmdom, DC=com  
Issuer: CN=cauth, DC=epmdom, DC=com  
Serial number: 59a7289f7f5d868e4fe4c1e8913d2265  
Valid from: Wed May 15 08:12:26 GMT+05:30 2013 until:  
Tue May 15 08:19:10 GMT+05:30 2018  
Certificate fingerprints:  
MD5: 98:CB:DD:87:FF:C1:46:E4:45:75:50:38:81:7F:A8:2B  
SHA1: CD:1C:92:16:3C:3A:E4:BB:B5:9A:FB:41:61:E9:5E:D2:94:0D:DC:EB  
Signature algorithm name: SHA1withRSA  
Version: 3  
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

3.2 Preparing to Install

EPM is provided as a compressed file zipped using WinZip. Extract the contents to a location of your choice. Following directory structure would be present

- ⇒ **docs** (contains this document and other documents)
- ⇒ **scripts** (contains database scripts)
- ⇒ **war** (contains WAR file of the application)



Previous steps in this document are the pre-requisites for this application hence current step should be performed after the previous steps are completed.

Installing EPM involves very easy steps as mentioned below:

- Run database scripts, create database schema
- Deploy the application WAR file in Web/Application server (JAVA supported)
- Configure the application

3.2.1 Run database scripts

In the package provided, database scripts for creation of schema (database tables) is provided by the name **<DBType>_EPMSchema.sql**, e.g. Oracle_EPMSchema.sql. DB Administrator should firstly create a DB User specifically for EPM e.g. epmdb. After that login as this DB User “epmdb” run the above mentioned script such that the newly created tables etc. would be owned by this DB User for EPM.

3.2.2 Deploy application

The application is a WAR that needs to be deployed in a Web/Application server. It is recommended that for trial and test environments you use Tomcat /JBoss server. For production environments, it depends on your organization’s decision, yet recommended server would be Websphere / Weblogic. As mentioned earlier, the JVM used by the application server should have imported the AD certificate for secure connection.

3.2.3 Configure the application

EPM can be accessed by the URL <http://<hostname or host IP>:8080/ESPM> where hostname can be something like epm.mydomain.com, host IP can be 192.168.3.99. The context path for application on Tomcat/JBoss would be /ESPM. The context path on other Web/Application servers can be specified as needed at the time of deployment.

First time URL access would lead to the application configuration page as shown below.



Enterprise Password Manager

Sat May 18 2013 23:20:02 GMT+0530 (IST) Help ?

System Configuration

Provide information related to your AD/LDAP domain and database. Configure AD/LDAP EPM Admin (user with limited administrator privileges). Administrator id and password is required to create EPM Admin. Administrator id (or any AD/LDAP id with user create permissions) and password is not stored any where.

Configuration Settings

System Configuration

Required field, please provide appropriate information.

Database Domain Mail Company

Database Configuration

Database Type* -- Select --

Save Database Server

Instructions

Fill up the values for the appropriate Database chosen.

NOTE!! - For all hostnames please provide a fully qualified DNS name. E.g for your Oracle host, `orclsrv1.addomain.com`

- Enable TNS listener for Oracle.
- Enable TCP connection for MS SQL.
- Default Server Port :
 - MS SQL - 1433
 - Oracle - 1521
- Database instance name provided should be created by your DBA before configuring here. For MS SQL Server, instance name and database name are normally same, unless multiple instances are present. Please check with your SQL Server DBA.
- EPM DB User should be created in the above mentioned database instance by DBA and provide correct credentials.

Copyright © 2013 "New Organization" All rights reserved.

Figure 12 - EPM Configuration Page

From here on follow the Administrator guide to complete application configuration and start using EPM.

4 List of all figures

FIGURE 1 – ROLES SUMMARY	5
FIGURE 2 – SERVER ROLES.....	6
FIGURE 3 – ROLE SERVICES.....	7
FIGURE 4 - SETUP TYPE	8
FIGURE 5 - SPECIFY CA TYPE.....	9
FIGURE 6 - SET UP PRIVATE KEY	10
FIGURE 7 - CONFIGURE CA NAME.....	11
FIGURE 8 - SET VALIDITY PERIOD.....	12
FIGURE 9 - CONFIGURE CERTIFICATE DATABASE	13
FIGURE 10 - CONFIRM INSTALLATION SELECTIONS.....	14
FIGURE 11 - INSTALLATION RESULTS	15
FIGURE 12 - EPM CONFIGURATION PAGE.....	19