

Kousec Server Certificate Manager Users' Guide

For Version: 1.0

Kousec Software, Inc.

April 30, 2010

Copyright 2009,2010 Kousec Software, Inc. All rights reserved.
All company names and product names are trademarks of their respective holders.

Table of Contents

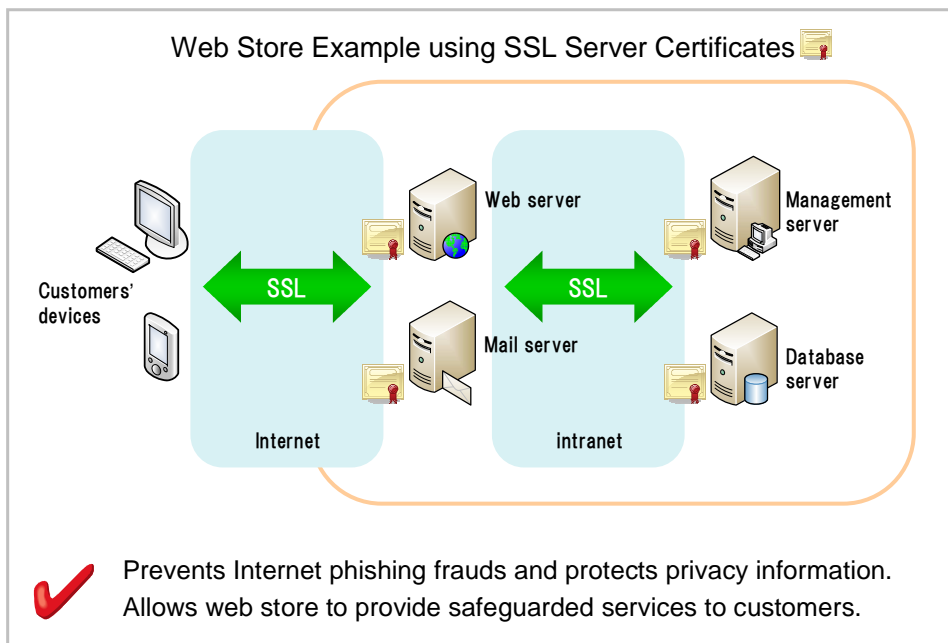
1.	About SSL Server Certificates	5
1.1.	Overview	5
1.2.	SSL Server Certificates.....	5
1.3.	Certificate Authority.....	6
1.4.	Server Certificate Reseller.....	6
2.	Concepts in Server Certificate Manager.....	7
2.1.	Server Certificate Repository.....	7
2.2.	Requirement Definitions, Acquisition Processes and Deployment Processes	7
2.3.	Certificate Definitions, Certificate Requests, and Certificates.....	9
2.4.	Lifecycle-Managed and Monitored-Only Certificates	10
2.5.	Certificate Monitoring.....	10
2.6.	Discovering Unmanaged Server Certificates on Network.....	11
2.7.	Importing an Existing Server Certificate	11
2.8.	Certificate Installation	12
2.9.	Built-in Private CA.....	13
2.10.	Selection and Purchase of Server Certificates	13
2.11.	Automated Certificate Request and Retrieval with Windows CAs	14
2.12.	Trusted CA Sets	14
3.	Setting Up Server Certificate Manager	16
3.1.	Basic Setup.....	16
3.2.	Changing Initial Password	16
3.3.	Restricting Access to the CertMgr Web Server	17
3.4.	SSL Certificate for the CertMgr Web Server	17
3.5.	Strong User Authentication using Client Certificate.....	18
3.6.	Users Management	20
3.6.1.	User Privileges	20
3.7.	Trusting Built-in Private CA.....	20
3.8.	Advanced Configuration	20
4.	Managing Certificates Using Server Certificate Manager	22
4.1.	Start Using Server Certificate Manager	22
4.2.	Summary Descriptions of Each Screens.....	25
4.2.1.	Certificate Definitions (Overall Status of All Certificates)	25
4.2.2.	Certificate Requests and Acquisition Processes.....	25
4.2.3.	Certificates and Deployment Processes	25
4.2.4.	Provider Accounts.....	25
4.2.5.	Private Keys.....	25

4.2.6.	Monitor Control	25
4.2.7.	Sent Emails.....	26
4.2.8.	Certificate Discovery.....	26
4.2.9.	CA Contracts.....	26
4.3.	Main Usage.....	27
4.3.1.	Import existing certificates and start managing them under Server Certificate Manager..	27
4.3.2.	Acquire a certificate	28
4.3.3.	Deploy the certificate	29
4.3.4.	Daily Operations	30
4.4.	Certificate Monitoring.....	32
4.4.1.	Server names	32
4.5.	Certificate Discovery	32
4.6.	Automated Enrollment with Windows CA.....	32
4.7.	Using Built-in Private CA	33
4.8.	Backing up Data in Server Certificate Manager	35
4.9.	[Optional] Configuring Private CA.....	35
Appendix A	Manual Deploy Checking.....	37

1. About SSL Server Certificates

1.1. Overview

SSL server certificates are a kind of digital certificates which web and other servers need to guarantee security and safety of network communications.



1.2. SSL Server Certificates

SSL server certificates are one type of digital certificates that server software use for SSL communications to authenticate communication peer and encrypt communication contents. A website operator proves its identity and guarantees communications authenticity and confidentiality by placing a server certificate on the website server.

When placing a server certificate, you also need to place a private key that pairs with the server certificate in order to prove that you are the legitimate owner of the certificate. A server certificate has a validity period (one to several years) and also it can be revoked by the issuing CA if the private key is stolen.

Other digital certificates include personal certificates for emails and user authentication at website and for IC cards.

1.3. Certificate Authority

Generally, SSL server certificates are issued by an entity called Certificate or Certification Authority (CA) to other party that requested for a certificate issuance. A CA verifies that the request is from the legitimate owner of subject identity before issuing a certificate. The issuing CA also revokes the certificate as necessary.

Many CAs require monetary compensation for the identity verification, issuance and maintenance of the certificate. In this document they are called **commercial CAs**. Prominent commercial CAs include VeriSign, Inc. On the other hand, when the requesting company issues server certificates for their own servers, the company operates their own **private CA**.

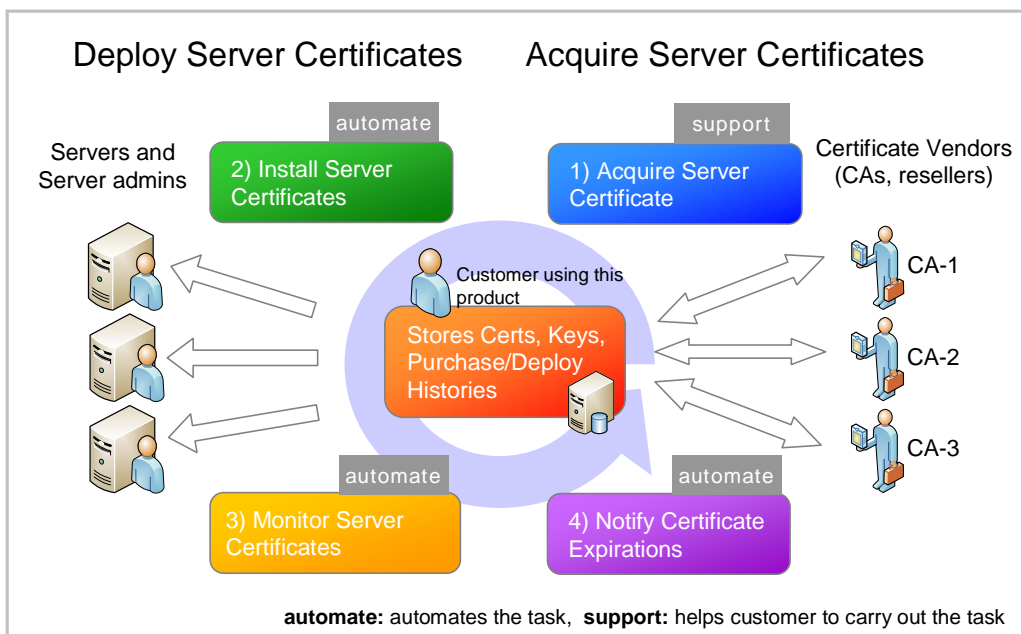
For websites and services intended for the internet and inter-organization applications, or for websites and services within a large multi-regional company, server certificates issued by commercial CAs are quite common.

1.4. Server Certificate Reseller

Certificate resellers sell server certificates issued by commercial CAs. Some certificate resellers offer certificate products from several commercial CAs. They help customers to choose optimal products for the customer and may also provide customer services for installing and maintaining certificates and their environments.

2. Concepts in Server Certificate Manager

Server Certificate Manager is a software product that helps a company to manage every aspect of server certificate lifecycle, from acquiring to deploying and monitoring certificates.



2.1. Server Certificate Repository

Server Certificate Manager has an internal database that stores generated private keys, acquired certificates, purchase history, deployment history, and monitoring data. It also has per-certificate document folder feature, in which you can store documents that you use when purchasing a certificate.

You can centrally store these certificate related information in one place, manage them under appropriate access control and backup operations, thereby minimizing risks of lost private keys and information leakage.

2.2. Requirement Definitions, Acquisition Processes and Deployment Processes

When you start a new online service, you collect requirements and study possible options for server certificate(s). Then you purchase certificate(s) and install them onto your server(s).

Acquiring and deploying server certificate	
Requirements	Collect requirements, Decide product
Acquisition Process	Generate private key / CSR
	Order(new/renew), Send documents
	Receive certificate
Deployment Process	Install certificate to server
	Backup certificate / private keys, etc
	Monitor deployed certificates

An acquisition process is a collection of steps to obtain a server certificate from a CA and store it in the certificate repository. It consists of generating a private key / CSR, placing an order for a certificate, receiving certificate file and registering it in the server certificate repository.

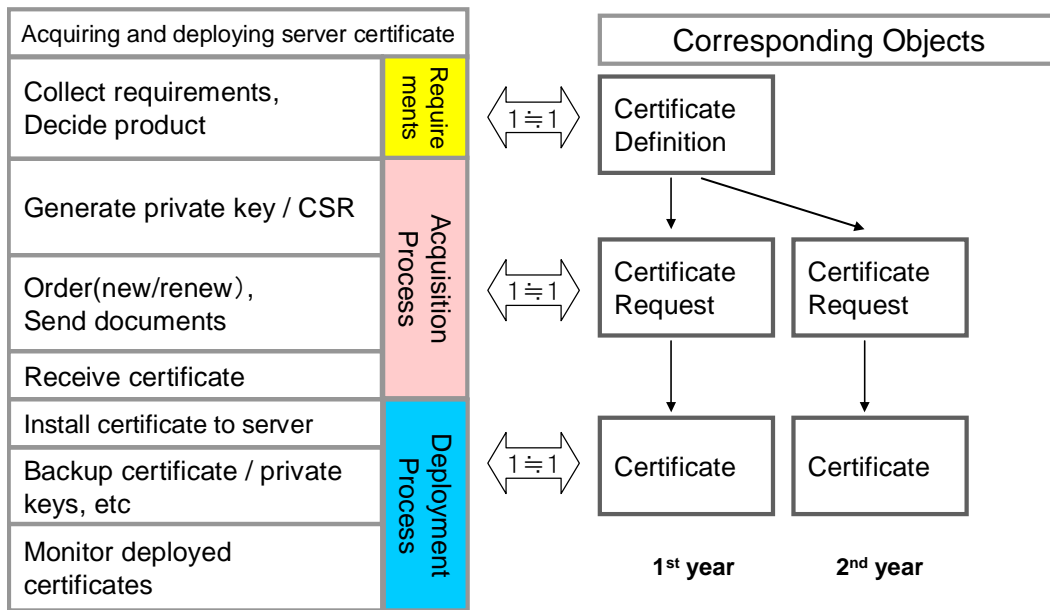
There are two types of acquisition process. They are **new acquisition** and **renewal acquisition**. When you are obtaining a certificate for a new server, it will be new acquisition. When you are obtaining one that will replace an existing server certificate, it will be renewal acquisition.

A deployment process is a collection of steps to transfer a server certificate from the certificate repository to a target server, install the certificate on the server and set up certificate monitoring.

An acquisition and deployment process can be in two process execution modes, one is **interactive** process mode and the other is **unattended** process mode. In the **interactive** mode, most steps in the process require a human operator to confirm the action to proceed to the next step. The operator may also have to fill in additional information to go forward. In the **unattended** mode, the process will be executed in the background by the system and run to the completion unless the process cannot proceed any further due to missing information or an error. If the process is interrupted halfway, the certificate administrator will be notified and he can pick up the process to execute it in the interactive mode. Or, he can just fill in missing information and let the Server Certificate Manager system will resume the process in the unattended mode in the next scheduled time.

2.3. Certificate Definitions, Certificate Requests, and Certificates

Server Certificate Manager manages processes mentioned above using software abstractions called **Certificate Definitions**, **Certificate Requests**, and **Certificates**. Requirement definition approximately corresponds to Certificate Definition, acquisition process to Certificate Requests, and deployment process to Certificate, respectively.



Each software abstraction object holds output of corresponding process and intermediate information as history records.

	Intermediate generated information	Output
Certificate Definition	-	Info about requestor, product requirements, target server
Certificate Request	CSR, order history	Private key, certificate received from CA
Certificate	Install request email, deploy history	Deployment and monitoring of certificate

(To be precise, private keys are also independent objects from certificate requests so that a private key can be reused)

2.4. Lifecycle-Managed and Monitored-Only Certificates

Aforementioned acquisition processes and deployment processes constitute the Server Certificate Manager's framework for server certificate lifecycle management. Server Certificate Manager will also allow you to set up continuous monitoring of SSL certificates placed on specified servers, without setting up lifecycle management of those certificates. This operation mode is preferable if your organization already has an operations management of SSL certificates in place and you only need a tool to monitor server certificates.

For each certificate definition, you can specify its operation mode from the following:

- **Lifecycle-Managed** : Server Certificate Manager will carry out all lifecycle management operations for this certificate definition.
- **Monitored-Only** : Server Certificate Manager will only monitor the server certificate placed on the server that is specified in the certificate definition. You cannot initiate an acquisition or deployment process on this certificate definition.

You can switch the operation mode when necessary.

2.5. Certificate Monitoring

Server Certificate Manager allows you to schedule periodic monitoring of deployed certificates (lifecycle-managed certificates) and monitored-only certificates. This interval can be specified by the administrator. During monitor execution, it connects to the servers and carry out several checks to determine their correct statuses.

Actual check items differ between lifecycle-managed certificates and monitored-only certificates.

- **Lifecycle-Managed** : Server Certificate Manager will basically check to see if the current certificate in the certificate repository is installed correctly on the server. It compares server certificate hash values and also checks if necessary intermediate CA certificates are also placed on the server. (For many server certificates, without intermediate CAs' certificate, web browsers' certificate verification fails.) The verification of the certificate itself is already done inside the Server Certificate Manager's certificate repository, so it is not done during certificate monitoring.
- **Monitored-Only** : Server Certificate Manager will primarily execute the following checks for the certificate found on the server.
 1. Standard certificate verification: Execute standard X509 certificate verification test using trusted CA certificates stored in Server Certificate Manager. You can create multiple sets of trusted CA certificates and associate a certificate definition with any one of them. See Trusted CA

Sets later in this chapter for more information.

2. DN Check: Compares common name, organization name and country code in the certificate against those specified in the certificate definition.
3. Validity period check: if the certificate's remaining validity period is shorter than a certain value (like 30 days), this check fails.

You can disable periodic monitoring for servers that cannot be accessed from the Server Certificate Manager computer (e.g., a server in another intra-net).

2.6. Discovering Unmanaged Server Certificates on Network

Server Certificate Manager is able to perform a network scan to uncover server certificates used on any SSL-enabled servers. It then analyzes all certificates found and determines whether they are valid and conform to the certificate trust policy set in Server Certificate Manager. The analysis result will be generated as a report.

From the report, you can also select certificates and initiate imports for them.

2.7. Importing an Existing Server Certificate

When you start managing an existing server certificate under Server Certificate Manager, you can import the existing certificate to the certificate repository of Server Certificate Manager. When importing an existing certificate, you can specify its operation mode, either **Lifecycle-Managed** or **Monitored-Only**. The import function in Server Certificate Manager serves two purposes.

1. Extract information (like DN) from the existing certificate and create a Certificate Definition based on them so that you can use it to monitor or manage lifecycle of the certificate.
2. (Lifecycle-managed Certificates only) Create a Certificate object with the imported certificate. This is to monitor the current certificate as installed on the server.

If you also import the corresponding private key, you can make the certificate re-deployable from Server Certificate Manager.

Bulk Import from Certificate Discovery Report

You can initiate importing multiple server certificates that are on a Certificate Discovery Report.

2.8. Certificate Installation

A server certificate issued from a CA , along with the private key, must be installed onto the target server. Server Certificate Manager will facilitate and automate this complicated and error-prone work as much as possible.

Server Certificate Manager offers three kinds of certificate installation methods as follows:

	Description	Conditions, Limitations
Automated certificate install	<ul style="list-style-type: none">• When AUTO-INSTALL button is clicked on Server Certificate Manager screen, the server certificate will be installed on the target server.• Server administrator does not need to do any work on the target server	Additional software and/or network configurations modifications (like firewall) may be required in some cases. Server software must be supported by Server Certificate Manager.
One-click certificate installer	<ul style="list-style-type: none">• The server administrator of target server receives an install request email along with the certificate install package via email, Web or FTP. Just executing it on the target server will install the certificate and the private key.	The Server Certificate Manager computer and target server don't need to be connected by network. Server software must be supported by Server Certificate Manager.
Conventional install method	<ul style="list-style-type: none">• The server administrator of target server receives an install request email along with the certificate install package via email, Web or FTP. He/she unzips it to extract files.• Install the certificate according to instructions from CA and/or server software manuals.	Can be used with any server software.

For the current list of supported server software and associated requirements are in explained in the product Read Me file (readme_en.html).

Kousec Software, Inc. will add support to more server software products for automated installation. We will also actively support disconnected environments where the Server Certificate Manager computer and target servers are not directly connected by networks. Using one-click installer, you can transport

the certificate package to your iDC in a USB memory stick. Because the certificate and private key are encrypted you can safely transport it.

2.9. Built-in Private CA

Server Certificate Manager has a built-in Private CA function. Using this function, the following operations are possible.

1. In development phase, using Server Certificate Manager define necessary server certificates.
2. Using the built-in Private CA, issue the server certificates.
3. Before the final testing phase, change product provider of all Certificate Definitions to a commercial CA, start renewal acquisitions for the certificates and deploy them.

Using this kind of operations, you can reduce certificate product costs during development phase while preventing any mistakes that could happen in migrating certificates.

Also in a large project where you maintain a smaller test system for the lifecycle of the production system, you can clone all Certificate Definitions for the production system and have the Private CA to issue certificates for the test system.

You can distribute the certificate of the private CA to all computers in your company if you are using a Windows ActiveDirectory domain by using Public Key Policies in Windows Group Policy. For other environments, Server Certificate Manager also provides the one-click installer to install the private CA's certificate in individual PCs.

Another option is that if you already have a PKI system in the company, the built-in Private CA can be configured to be a subordinate CA of one of the higher level CAs.

2.10. Selection and Purchase of Server Certificates

Server Certificate Manager contains a latest database of SSL certificate products available and you can utilize it to purchase one. When renewing a certificate, if you change a certificate product or provider, Server Certificate Manager still handles it as a renewal process.

First you will set up requirements in a Certificate Definition for to-be-acquired certificate. There are two ways as follows:

-
1. Specify a certain product from a commercial CA or the built-in private CA
 2. Set requirements only.

Requirements include buying from a specific CA, buying a certificate with specific assurance level (like EV).

In step of Product Selection and Purchase in acquisition process, choose a certificate product as follows:

- If a certain product is specified, select it.
- If requirements are specified, choose a product on Product Selector screen that will only list products that match requirements.

For actual order placement, use the website of the selected CA or one of its resellers. After placing an order, enter order date, order number and any other tracking information in Server Certificate Manager.

2.11. Automated Certificate Request and Retrieval with Windows CAs

Automated certificate acquisition from Windows Certificate Services is possible through its enrollment API. If you already have a Windows Certificate Services running on a Windows Server computer, you can issue server certificates from the Windows CA and deploy them to Linux servers using Server Certificate Manager.

To integrate with a private CA such as Windows CA, you need to create a **CA Contract** that holds integration information like CA's server string, username and password. Then, you create one or more **Certificate Products** (i.e., user defined certificate types) that are available under this CA contract. Typically you will enter in a Certificate Product definition the name of a certificate template that is defined on the Windows CA.

During an acquisition process, if you choose one of those certificate products, you will be directed to the CA contract screen to submit a **Request to CA** and obtain the certificate with just one click.

2.12. Trusted CA Sets

Server Certificate Manager uses one or more sets of trusted root CA certificates in validating server certificates during certificate monitoring and discovery. It manages its own set of trusted root CA certificates and does not use the trusted CA certificates of the host operating system.

On Server Certificate Manager, you associate a certificate definition with one Trusted CA Set. Then,

when checking a server certificate on the server for the certificate definition, Server Certificate Manager validates it against the root CA certificates stored in the Trusted CA Set.

One trusted CA set contains two kinds of root CA certificate collections:

1. **System-defined CAs:** Root CA certificates pre-populated by Server Certificate Manager
2. **User-defined CAs:** Root CA certificates that are defined by the certificate administrator

Technically there are no differences between CA certificates stored in each collection. It is only the way each collection is managed that is different. Typically, system-defined CAs include certificates from public and commercial CAs, while user-defined CAs include certificates from your private and enterprise CAs.

A system-defined CAs collection is stored as a file in Server Certificate Manager's install directory. One install-time default file will be installed with Server Certificate Manager. User-defined CA certificates will be stored in Server Certificate Manager's database when you add them to a trusted CA set.

You can modify the default trust CA set by adding user-defined CA certificates or he/she can create another trusted CA set for a different set of certificate definitions.

In Certificate Discovery, Server Certificate Manager uses the default trusted CA set when validating server certificates. You can specify which trusted CA set is to be used as the default trusted CA set in Certificate Policy settings.

3. Setting Up Server Certificate Manager

3.1. Basic Setup

Just after the installation, before start using Server Certificate Manager, you need to do basic set up. Open “Application” ⇒ “Settings” screen.

The following are required items. Please fill them in.

- CertMgr Administrator Information
Email address of the person who will be using this product primarily. Notification emails for certificate administrator will be sent to this address.
- Email Settings (Outbound)
Sender email address of the Server Certificate Manager computer when it sends out emails.

Sender Email Address	Email address used for From header
Sender Email Name	Name used in From header
SMTP Server Name	SMTP server name for sending. When specifying a port, follow it with a semicolon, e.g., servername:587
SMTP User Name	Username to connect to SMTP server
SMTP Password	Password to connect to SMTP server

When finished, you can click on “Send Test Email” button to check to see if you can actually send an email.

Tip: Trouble-shooting emails. These days, access to an SMTP server is severely restricted. If you have problem sending, use port 587 instead of the default port and also make sure that a security software (Anti-Virus/Firewall) on the Server Certificate Manager computer does not block outbound connection to port 587.

3.2. Changing Initial Password

It is strongly recommended to change the initial password for user **admin**. To do this, click **Change My Password** at the lower most position of “Settings” screen.

3.3. Restricting Access to the CertMgr Web Server

After the initial install, CertMgr allows web browser access from computers with any IPv4 address range. You can change these IP address range. You can restrict web access by client IPs with the following procedure.

- Open a command prompt by clicking the Open Command Prompt in the Kousec Server Certificate Manager start menu.
- Type **notepad ip_acl.txt** to edit the IP ACL file. Notation is documented as comments in the file. After saving the file, changes will be reflected immediately. For example, the following content will only allow web access from any computer with IP address of 192.168.x.x.

```
192.168.0.0/16
#0.0.0.0/0 # this line is commented out
```

You should also protect the CertMgr computer with the Windows firewall. The TCP port that needs to be opened is 23466.

3.4. SSL Certificate for the CertMgr Web Server

An SSL certificate for the CertMgr Web Server is issued from its built-in Private CA and installed in the CertMgr Web Server at the initial install time. There is no Certificate Definition created for this certificate.

You can obtain a new certificate from a commercial CA or issue a new one with different DN from the built-in Private CA. The following is the basic procedure.

1. Create a Certificate Definition by importing the existing certificate.
Import the certificate from the URL of CertMgr (<https://127.0.0.1:23466/>). You do not need to start a deployment process for the imported certificate.
2. On the Certificate Definition, start a new acquisition process to obtain a new certificate.
3. When deploying the obtained certificate, select **This CertMgr** as the Server Software Type. Also enter any character into **Username for Auto-Install** and **Password for Auto-Install** to enable automatic install of this certificate. Then, perform auto-installing this certificate.
4. Log out of CertMgr and restart the CertMgr service.
5. Log in again. When doing deploy check, specify port number **23466**. Then run the deployment

process to completion. If you obtained the certificate from a private CA, be sure to include the CA certificate in the default Trusted CA set. Otherwise, the deploy check will fail.

Trusting the Built-in Private CA

You will need to have your web browser to trust the Built-in Private CA so that your browser can authenticate the server that's running CertMgr. Click "Private CA" in the side menu to open the Private CA screen. You can download the Private CA's certificate either as a PEM file or a Windows-installer file.

3.5. Strong User Authentication using Client Certificate

To further strengthen user authentication to the CertMgr system, you can require users to present a client certificate when connecting to the CertMgr web console.

- You can specify the root CA(s) for allowed client certificates. You can selectively put the root CA certificate(s) into a file or you can direct CertMgr to use the Windows certificate store (Trusted Root).
- Each client certificate allowed needs to be specified with the certificate's thumb-print (i.e., SHA1 hash).
- You still have to use the username and password on top of this certificate authentication to use the CertMgr web console.
- You can use the built-in private CA to generate a client certificate. You can also use certificates from other sources.

The following is the basic procedure.

- You will modify the web server configuration file (**http.conf**), create a certificate map file (**certmap.txt**). If you want to specify one or more root CA(s), you will put those certificates into a file (**ssl.crt/client_auth_ca.crt**).
- Open a command prompt by clicking the Open Command Prompt in the Kousec Server Certificate Manager start menu.
- Type **notepad http.conf** to edit the web server configuration file. Find the four lines shown below.

```
# - SSL Client authentication -  
#http_ssl_clauth = require  
#http_ssl_cacertstore = file ssl.crt/client_auth_ca.crt  
#http_certmap_fname = certmap.txt
```

Remove '#' character at the beginning of each line for the three lines that begin with "http_".

If you want to use client certificates from commercial CAs, it is easier to use the Windows Trusted Root CA certificate store. In that case, replace the `http_ssl_cacertstore` line with the line below:

```
http_ssl_cacertstore = os
```

- Store the certificates of the root CA(s) in **ssl.crt\client_auth_ca.crt**.

(This step is necessary if you are not using Windows Trusted Root CA certificate store.)

You can put one or more root CA certificate(s) in PEM format.

If you are using the built-in private CA to generate a client certificate, enter the below command to store the root CA certificate in the file.

```
>copy myca\cacert.pem ssl.crt\client_auth_ca.crt
```

- Obtain a client certificate and install it in your web browser.

If you are using the built-in private CA to generate a client certificate, see the next paragraph.

- Create the **certmap.txt** file and store the list of thumb-prints (SHA1 hashes) for client certificates allowed. You can start with a file `certmap.example`.

```
> copy certmap.example certmap.txt
```

Each line in the file should look like this

```
* Hash_SHA1 2c 74 2e 10 b8 c0 7f d5 8e 2a ad 2d a9 7b 7f 1a ba e4 f6 dc
```

- Restart the Kousec CertMgr service.
- Configuration errors are written to **logs\httpd\event.log**. Request related errors are written to **logs\httpd\errors.log**.

The following is the procedure to have the built-in Private CA to generate a client certificate for your use.

- Open a command prompt by clicking the Open Command Prompt in the Kousec Server Certificate Manager start menu.
- Generate a certificate for client use

```
>gencert -gencli
```

The CA's private key is protected by the password "orenosp". You also need to give a password for your client certificate.

- Retrieve the generated certificate and private key in a PFX file.

Gencert will show you the filename (pfx file) for the certificate and private key. Copy the pfx file to a location where you can import it to your web browser. The password protecting the pfx file is the one that you entered when generating the certificate. The following command initiates importing of a PFX file.

```
> start pfx000000000000000002.p12
```

3.6. Users Management

You can administer users who can log in to CertMgr and carry out certificate operations. Click “Users Management” located lower-left corner of “Settings” screen.

3.6.1. User Privileges

You can set each user with a privilege level. Users with “Admin” privilege can do various user administration tasks like adding/modifying/deleting other users, while users with “User” privilege cannot do any of them.

3.7. Trusting Built-in Private CA

If you plan to use the built-in private CA to issue server certificates, add its CA certificate to the default Trusted CA set.

1. Open the Trusted CA Sets screen
2. Open the “Default-Trust” set
3. Edit the System List
4. Under the System Collection Files, add the following file to the System Collection Files:

```
kcertmgr-private-ca-at-install.pem
```

5. Click the Go Back button
6. Click the Save and Merge CA Set button

3.8. Advanced Configuration

For advanced configuration options, you can edit the following file:

`<CERTMGR_INSTALL_FOLDER>%htdocs%cake%cm%cmconfig.inc`

It includes many options such as setting an external server name in a reverse-proxy configuration and path to your Java environment.

4. Managing Certificates Using Server Certificate Manager

4.1. Start Using Server Certificate Manager

This subsection will give you overview and basic flows when starting to use Server Certificate Manager. We will describe three different scenarios so that you can choose one that fits your situation.

Scenario 1)

You have many secure web servers and want to introduce a certificate monitoring solution.

This scenario is applicable if you have a large number of server certificates that you want to monitor and you already have proper operations and management processes for provisioning server certificates. You will import all server certificates as **Monitored-only** certificates. In this scenario you will get a monitoring report on a daily basis that summarizes the certificate checking result.

Basic procedure

1. Discover server certificates on the network using Certificate Discovery. The certificate discovery can be initiated on the internal network or on the Internet.
2. Import discovered server certificates into Server Certificate Manager. This can be done from the discovery report by clicking **Bulk Import** button. Import the certificates as **Monitored-only** certificates.
3. Initiate an immediate certificate checking (“Deploy Check”) from the Monitor Control screen.
4. On the Certificate Definitions screen, switch to the monitor view. Review the check result (OK or otherwise) and edit the monitoring setting by editing the certificate definition as necessary.
5. Open the Monitor Control screen and set the monitoring interval as necessary.
6. Everyday, in the Monitor Execution History section on the Monitor Control screen you will see recent monitor results. There is a link named ‘Report’ that will show the monitoring report for that day.

Scenario 2)

You have many secure web servers and want to introduce a server certificate management solution.

This scenario is applicable if you have a certain number of server certificates that you want to automate the renewals. For other remaining server certificates, you want to just monitor certificate statuses. You will import those server certificates as **Lifecycle-managed** and the others as **Monitored-only**. You will also set the process execution mode for Lifecycle-managed certificates to **Unattended** so that

CertMgr will automatically start an acquisition and deployment processes for the renewal certificate. In this scenario, you will have certificate renewals fully automated if you are using a Windows CA or CertMgr built-in private CA. Otherwise, the certificate administrator must manually send the CSR and receive the certificate from the CA

Basic procedure

1. As in scenario 1, discover server certificates and bulk-import them. When importing, specify **Lifecycle-managed** for certificates that you want to automate certificate renewals. You can also create two certificate definitions for the same certificate, one as **Monitored-only** and another for **Lifecycle-managed**.
2. For each lifecycle-managed certificate definition, enter correct information regarding certificate deployment like server software type and user credential for accessing the server. After entering the server information and credential, click the Test button to check if CertMgr can log in to the server through its management interface.
Details: Not all server software types are supported for automated certificate installs. If the server software type is not supported, the unattended execution of the deployment process will be stopped and the certificate administrator will be notified via an email alert and/or the certificate install package will be sent to the administrator of the target server, requesting to install the certificate.
3. When the current (imported) certificate nears its expiration date, a certificate acquisition process will be started. If the acquisition process completes successfully, it will be followed by the deployment process. If the new certificate is issued from a Windows CA and automated install is supported for the target server, the renewal will be completed without administrator's intervention.
Details: If these conditions are not met or any of required information is missing or the target server is not accessible, the acquisition process or deployment process will be interrupted and the certificate administrator will be notified.
4. All lifecycle-management related events are logged in the Event Log from the Monitor Control screen. Once deployed, the certificate will be monitored and its check result will be shown in the Lifecycle-managed section on the Monitor Control screen.

Scenario 3)

You are starting a new project that requires SSL certificates.

This scenario is applicable if you do not have an existing server certificate..

You will create one or more certificate definitions from scratch and set their operation mode to **Lifecycle-managed** and process execution mode to **Unattended**. After creating one certificate definition you can duplicate it to save time.

This scenario is very similar to the scenario 2, except that you don't import existing certificates. When

starting to use CertMgr, your servers must have to be already configured for SSL communication. Many server software products are configured for SSL at install time using a self-signed server certificate. CertMgr will be able to replace those self-signed certificates with acquired certificates automatically.

Basic procedure

1. When installing server software programs on servers, be sure to configure them to use SSL using generated self-signed certificates. Many server software products will enable SSL using self-signed certificates by default. If you must enter DN information to generate a certificate, you can enter arbitrary information in most fields as you will replace it with a proper certificate later on using CertMgr.

If you are using open source server software on Linux, the following document on Kousec Software's web page will help you to configure Apache, Postfix, Dovecot, vsftpd for SSL:

Managing SSL Certificates for Linux Internet Server

(http://www.kousec.com/tj/tj_review_S1_en.pdf)

2. On CertMgr, create one certificate definition per one server software. You can also use Certificate Discovery to find all self-signed certificates that are installed at server software install-time and import them selectively.
3. Remaining procedure is the same as scenario 2.

4.2. Summary Descriptions of Each Screens

4.2.1. Certificate Definitions (Overall Status of All Certificates)

On this screen, you can view Certificate Definitions and associated status of acquisition and deployment processes.

4.2.2. Certificate Requests and Acquisition Processes

In Certificate Requests, you can see all recorded certificate requests.

In Acquisition Processes, you can see the list of ongoing acquisition processes and another list of certificate definitions that should have already started a next acquisition process but have not yet. From this screen, you can check progress of ongoing acquisitions.

4.2.3. Certificates and Deployment Processes

In Certificates, you can view all recorded certificates.

In Deployment Processes, you can see the list of deployment processes for current certificates. Among them, for certificates whose deploy status is either “Confirmed” or “Install Requested”, results of daily certificate monitor is also displayed.

From this screen, you can check progress of deployment processes and results of daily monitoring.

4.2.4. Provider Accounts

When purchasing a certificate product, you generally need to create an user account for the provider's website. In this screen, you can record them so as to make ordering and receiving processes easier. If you register at multiple providers with the same information, you can just create one entry.

4.2.5. Private Keys

You can view the list of generated private keys. By default, for each CSR generation, a new private key is generated. Imported private keys are also recorded here if the imported certificate went through the deployment process.

4.2.6. Monitor Control

In Monitor Control, you can manage monitoring functions and view history of certificate monitoring.

You can also adjust scheduling of periodic monitoring.

4.2.7. Sent Emails

In Sent Emails, you can view records of all emails sent out from Server Certificate Manager.

4.2.8. Certificate Discovery

In Certificate Discovery, you can initiate a network scan and search for any network-exposed SSL server certificates. Then you can analyze validity of those server certificates found and bring them in under the control of Server Certificate Manager by importing them.

4.2.9. CA Contracts

In CA Contracts, you can create and modify objects necessary for integrating with Windows Certificate Services. The objects are CA Contracts, Certificate Products and Requests to CA. For latest information on supported configurations, see the Readme file.

4.3. Main Usage

4.3.1. Import existing certificates and start managing them under Server Certificate Manager

You can import an existing certificate into Server Certificate Manager. By importing, a new Certificate Definition is created based on the information from the certificate. From the certificate definition, start an acquisition process at next renewal time.

Also, at your preference, you can start a deployment process for the imported certificate.

There are two cases for imported certificates:

1. You have the private key for the existing certificate and import the private key also.
2. You do not have or did not import the private key for the existing certificate.

In case 1, by starting a deployment process, you can re-deploy it from Server Certificate Manager.

In case 2, you cannot (re-)deploy it but you can still set up certificate monitoring for it.

If the existing certificate is not deployed on any server, or it is expired, there is no need to monitor it. Therefore you don't need to run the deployment process.

The following are the certificate file formats that can be imported:

- Apache-compatible text formats ("PEM")
Typically used in Apache servers, this is a set of files consisting of the server certificate, the corresponding private key and a single file containing all required certificates for intermediate CAs. These files are all in text. The private key file may be encrypted, in which case you need to provide the passphrase for it.
- Windows-compatible Backup format ("PKCS#12")
Often known as "P12" or "PFX" files, this type of certificate file contains all related files in a single encrypted file, whose file name ends in ".p12" or ".pfx". Files typically contained are, the server certificate, the corresponding private key, a set of required certificates for intermediate CAs. You need to provide the passphrase for it.
- Windows-compatible certificate formats ("CER" and "P7B")
This set of files is typically used when transporting certificates only, not private key. A "CER" file, a binary format called DER, can contain one certificate, so it's used to store the server certificate. A "p7b" file can contain multiple certificates so it's typically used to store certificates for intermediate CAs.

- Java Key Store format (“JKS”)

Most Java-based application servers support this format as a Key Store (storing the server’s private key and certificate) and as a Trust Store (storing the certificates of CAs that the server trusts). Server Certificate Manager allows you to import the private key, corresponding server certificate and any intermediate CA certificates from a JKS file that is used as a Key Store. You need to provide the key password for the JKS file.

Importing Certificates found in Certificate Discovery

Rather than specifying each certificate for import, you can also initiate a certificate discovery and import those that are found. Note that in that case you cannot import the corresponding private key.

4.3.2. Acquire a certificate

From the certificate definition that was created from importing, you can start an acquisition process for a new certificate. For renewal, the process is similar. Open the certificate definition, click on the button “Acquire New Certificate”. Then an acquisition process starts and a new certificate request screen opens up.

Product Selection : In Select and Purchase Product screen, you can see information of certificate products stored in Server Certificate Manager and you can jump to the provider’s product information page. Once you choose a product, pushing button “Go to Provider’s Buy Page” will open up a new window and shows provider’s website.

Order : Almost all public providers require you to create a provider’s account. Server Certificate Manager has “Provider Accounts” screen where you can record account information (username, password, registered email address, etc) and associate it with the certificate request (and certificate definition). Once an order has been placed, you go back to the Server Certificate Manager screen and record order number and other information.

Receiving : Once the CA has issued your certificate, you will receive an email notification from the provider at the email address registered with your provider’s account. Download the certificate, any intermediate CAs’ certificates and enter them in the Server Certificate Manager’s Received Files from Provider screen.

Switching Current Certificate : If the received certificate is already with its validity period, you can set this certificate as the current certificate. If an old certificate exists, it will be replaced with this certificate. In

Server Certificate Manager, you first specify which certificate should be the current certificate, and then you start a deployment process to actually replace the certificate deployed on the server.

Now the acquisition process is done. By switching the current certificate, the corresponding deployment process should be active now. Follow the instructions to proceed to the deployment process.

4.3.3. Deploy the certificate

Entering Deploy Information : Enter information necessary to deploy this certificate. There are three categories. The first one is about the target server, and second one is about how you will deliver the certificate install package to the server administrator, and the third one is information required for automated certificate installs. Automated installs (auto-install) is optional and are available only for some server software platforms. For the list of supported server software types and specific instructions for each server type, please see “Supported Server Software Products” section in Readme file.

When finished, click on “Prepare to Deploy” and the certificate install package will be created and you will proceed to the next step.

Requesting Certificate Install : Create an email requesting to install the certificate to the server. It also shows the button “Try auto-install” if you entered necessary info (username, password) for auto-install in the previous step. Pushing this button triggers executing auto-install and the execution result will be displayed. If auto-install succeeded, the request email will be changed to an install notification email. Proceed to the confirmation screen and send out the email.

Checking Deployment : In this step, you check to see if the certificate is correctly installed on the server as requested. By default, Server Certificate Manager will access the common name in the certificate. If you want to check with an alternative name (like internal hostname), enter the name in “Server name to Check”.

Tip: It will take some time (from hours to days) for the server engineer to install the certificate you requested. For daily operations, you can leave the deployment process screen and check “Deployment Processes” screen, say, once a day. In Deployment Processes screen, you will see a list of active deployment processes and their check results of periodic certificate monitoring. When “result” field has become “OK”, open the Certificate screen, do deploy check again and have the deployment process to complete.

In an environment where the Server Certificate Manager computer and target servers cannot have

network communications, you cannot execute deploy check or certificate monitoring from the Server Certificate Manager computer. In that case, you must execute deploy check manually from where you can access the target server. Instructions for carrying out manual deploy check is described in Appendix A of this Users Guide.

After manually checked deployment, on Server Certificate Manager, you push button “Manually Checked Deployment” and proceed to the next step. If network disconnection is permanent, you should also check “Disable Periodic Monitoring” to exclude the certificate from monitor targets.

Result of Deploy Check : The result of the check is displayed along with the check details. If successful, press “Done” button to complete the deployment process. If the result is failure, pressing “Send Result to Server Admin” button to email the result to the server administrator. Also you can show the screen shot to your network engineers and/or server engineers to solve the problem. If the check failed, you can also press “Continue without Checking” button to complete the deployment process. In that case, an alert for the certificate will most likely appear in periodic monitoring. As necessary, disable periodic monitoring by opening the Certificate screen after deployment process is done.

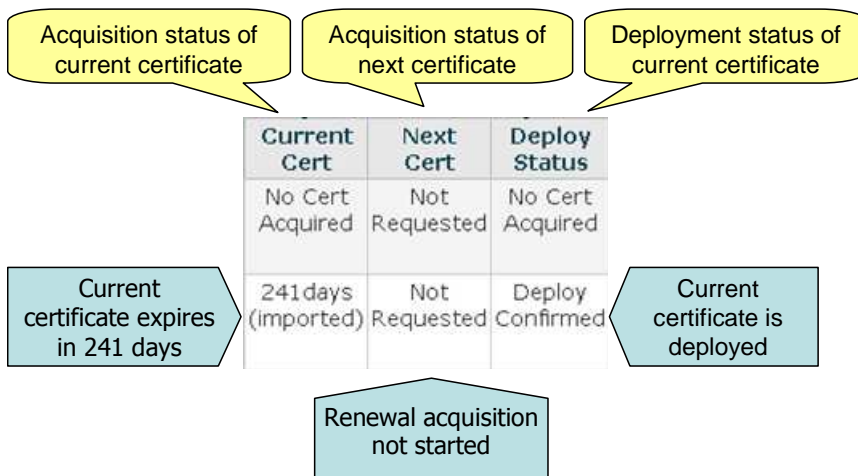
4.3.4. Daily Operations

Most events that need attention from the Certificate Administrator should be delivered as emails to the Certificate Administrator once a day. You can also log in and check a couple of screens for more up-to-minute information.

Screens you should check in daily operations are, Certificate Definitions (Overall Status of All Certificates), Acquisition Processes, and Deployment Processes.

Certificate Definitions : On this screen you can see, for all certificate definitions, acquisition status of current and next certificates and status of deployment of the current certificate, in simplified forms.

Part of Certificate Definition columns



Acquisition Processes : On this screen you can see the list of ongoing acquisition processes and the list of certificate definitions that have certificates expiring in 60 days and that has not started a next acquisition process. You can take the following actions on this screen:

1. Open the certificate definition and start a renewal acquisition process.
2. Open a certificate request that has not progressed well, expedite the process by resolving any issues found.

Deployment Processes : On this screen, you can see the list of ongoing deployment processes and the list of certificate definitions whose current certificates have failed deploy check (for some reason) in periodic monitoring. You can take the following actions on this screen:

1. Open the certificate that has not progressed well, expedite the process by resolving any issues found.
2. For deployment processes whose status is "Install Requested", if there are any with monitor result is "OK", open that certificate and do deploy check and complete the deployment process.
3. If there are any certificate whose deploy status is "Confirmed" but the monitor result is "NG", click on the monitor result to see the detailed result. Trouble-shoot the issue (e.g., email the server engineer).

Also, in Monitor Control, you may want to check results of daily certificate monitoring.

4.4. Certificate Monitoring

You can set up certificate monitoring for deployed certificates. Imported and deploy-checked certificates are also monitored.

4.4.1. Server names

It is important to know that Server Certificate Manager makes a distinction between multiple server name types.

Name Type	Description
Common name	Official computer name for end users (domain name)
Server name	Computer name as certificate install target
Server name for Check/Monitor	This can be either the common name, the server name or any other alternative name or IP address. It needs to be a name to which the Server Certificate Manager computer can access via network.

When doing a deploy check on a computer, Server Certificate Manager does not mandate that the server name match the common name or any name in Subject Alternative Names (SAN). Rather, it checks if the certificate on the server matches the certificate in the CertMgr repository that you declared as the current certificate. This check is done using SHA1 hashes of both certificates.

4.5. Certificate Discovery

In Certificate Discovery, you can initiate a network scan and search for any network-exposed SSL server certificates. Then you can analyze validity of those server certificates found and bring them in under the control of Server Certificate Manager by importing them.

4.6. Automated Enrollment with Windows CA

During a certificate acquisition process, you can automate certificate request and retrieval to/from a Windows CA. This is done by calling the Windows CA enrollment API. Before you start an acquisition process, you need to set up a **CA Contract** and define one or more **Certificate Products** that can be obtained under the CA contract. During an acquisition process, if you select one of those certificate products, you will be directed to the CA Contract screen in which you will submit a certificate request to the CA and retrieve the issued certificate. The retrieved certificate will be automatically registered in the ongoing acquisition process. You can then click the **Back to Cert Request** button to go back to the

acquisition process and continue.

On the Windows CA, prepare one or more certificate templates that you want to use. Those certificate templates can be set to either automatic issuance or manual issuance, which requires Windows CA manager approval.

For specific configuration requirements and latest supported combinations of products, see the Readme document.

4.7. Using Built-in Private CA

Distributing Certificate of Built-in Private CA

By default, the built-in Private CA operates as a root CA. Therefore you need to distribute the CA certificate to all computers that will be verifying certificates issued from the private CA.

You can distribute the certificate of the private CA to all computers in your company if you are using a Windows ActiveDirectory domain by using Public Key Policies in Windows Group Policy.

For details, see the following Microsoft article:

Policies to establish trust of root certification authorities

[http://technet.microsoft.com/en-us/library/cc775613\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc775613(WS.10).aspx)

For other environments, Server Certificate Manager also provides the one-click installer to install the private CA's certificate in individual PCs.

On the Private CA screen, there exists the button to generate the CA certificate installer for Windows. Click the button and download the installer executable. This installer contains public information only, so there is no encryption password necessary to run it.

Built-in Private CA as Subordinate CA

If you already have a private CA in your company that is running on Windows Server PKI, you can also make the built-in private CA part of your PKI hierarchy. This way, you do not have to deploy another trusted CA root certificate in your company. To do that, you need to obtain the certificate for this built-in private CA from one of your higher CAs. There is a supported procedure for this kind of deployment. Please contact Kousec Software for details.

User-Defined Certificate Extensions

The built-in private CA accepts custom extensions that will be put in all issued certificates.

Create a file called "ca_ext.conf" in the "myca" directory (i.e., "myca\ca_ext.conf"), and enter the following text (for example) in that file.

```
[default]
```

```
crlDistributionPoints=URI:http://privca.local:23456/privca_pub/1.crl
```

```
authorityInfoAccess=caIssuers;URI:http://privca.local:23456/privca_pub/ca-cert.cer
```

To make sure the ca_ext.conf file is recognized, start Open Command Prompt from the Kousec Server Certificate Manager group and type "gencert -info" in the command prompt.

4.8. Backing up Data in Server Certificate Manager

The data that need to be backed up are stored in the following three folders:

CERTMGR_HOME/db	(Main database. Contains everything other than the below)
CERTMGR_HOME/DocFolders	(Documents in document folders and generated certificate package files)
CERTMGR_HOME/myca	(Database of the built-in Private CA)

Stop Kousec CertMgr service and back up these folders.

If you restore the backup data to a Server Certificate Manager instance that's installed in another folder, copy the backup data over and then run "cm_config.bat" from CertMgr Command Prompt.

4.9. [Optional] Configuring Private CA

By default, the built-in Private CA is configured as follows:

CA's distinguished name (DN)

Organization Name : Kousec CertMgr Built-in Private CA

Common Name : Kousec CertMgr Auto-Generated CA <timestamp-of-CA-generation>

You can change this information with the following instructions. First open up a command window by clicking "Open Command Window" shortcut.

1. Backup the database of the current Private CA

Change the name of CA folder.

```
> ren myca myca_default
```

2. Create a new CA

Create a new root CA:

```
> gencert -setup_ca -2
```

Enter DN and other info for the new CA. When asked for CA's password, enter "orenosp". (no double-quotes)

Important: We recommend not using identical DN information. Specify a unique DN by putting a date or serial number in the common name, for example.

You can see information for the new CA:

```
> gencert -info
```

3. Add the certificate of the new CA to one or more Trusted CA Sets as necessary.

The following command will show the private CA's certificate in text format (PEM):

```
> gencert -show_rootcert
```

Add this certificate to a Trusted CA Set, either as a User Defined CA or a System Defined CA. When adding it as the latter, store the certificate to a file and place it as `CERTMGR_HOME¥trusted_cas¥system-list¥kcertmgr-private-ca-XXX.pem`, where XXX can be an arbitrary string.

Be sure to save and merge the CA certificates after modifying a Trusted CA set.

4. Generate a CRL file from the new CA

```
> gencert -gen_crl -p:orenosp -f
```

5. Log in to CertMgr and Open Private CA screen

Click the button "Create CA Cert Installer" to re-create the Private CA certificate installer package.

Appendix A Manual Deploy Checking

In an environment where the Server Certificate Manager computer and target computers cannot directory communicate via network, Server Certificate Manager cannot carry out a deploy check. In such a case, you need to carry out a manual deploy check. The procedure is described below.

Procedure when using Web Browsers like IE and Firefox

1. Obtain information of the target server to check
 - A) Open the Certificate screen and write down necessary info to access the target server (common name, host name, port number.)
 - B) Next, click "Show Cert" on the Certificate screen. A new window opens up. Write down the value of "Finger Print (SHA1)". It should be a 40-digit hexadecimal number.
2. Move to a PC from which you can access the target server
3. Using Internet Explorer (IE), open the URL of the target server. You should use the common name for the URL.
4. If IE shows a warning regarding the certificate, **the certificate is not correctly deployed.**
5. If IE doesn't show a warning, make sure that the SHA1 hash matches the one from CertMgr.
 - A) Open the Certificate dialog for the current page on IE. (This step differs in various IE versions)
 - B) Click the Details tab. Check to see if the value of Thumbprint matches the value of the Finger Print (SHA1) that you wrote down in step 1. If they don't match, **the certificate is not correctly deployed.**

If the certificate is not correctly deployed, take screenshots of the web browser's warning box and certificate dialog and send them to the server administrator.