SimonsWare

SSL Certificate Management v2.0 Installation and Configuration Guide

Table of Contents

There are several components to SSL Certificate Management. The below diagram shows each component and how it communicates with the database. No component communicates directly with another component. All communication is handled through the database.

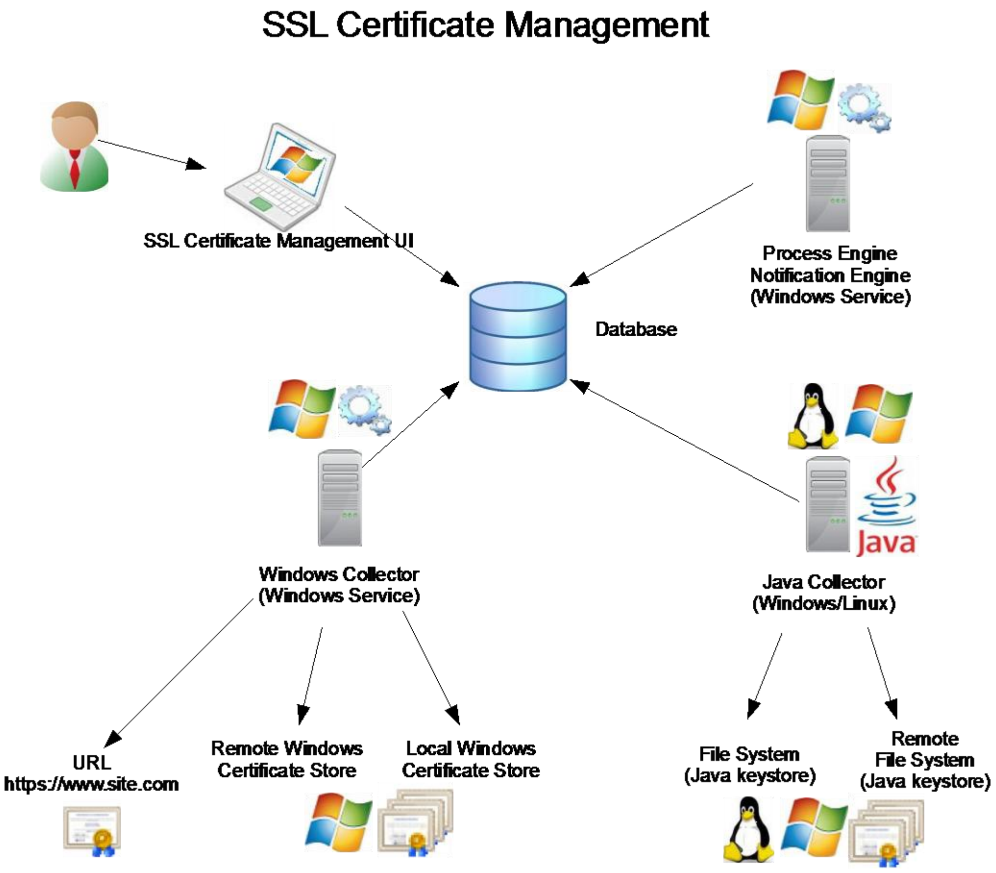


Figure 1 - SSL Certificate Management Components

System Requirements

- SSL Certificate Management UI
  - Windows 7/8
  - Windows Server 2003/2008/2012
  - .NET Framework 4

- Windows Collector
  - Windows Server 2003/2008/2012
  - .NET Framework 4

- Process Engine
  - Windows Server 2003/2008/2012
  - .NET Framework 4

- Java Collector
  - Java Runtime 7
  - Windows Server 2003/2008/2012, Linux, Unix
  - sshfs v2.4 (on Linux/Unix systems for mapping to remote systems)
    http://fuse.sourceforge.net/sshfs.html

- Database
  - Oracle 11g
  - Microsoft SQL Server 2008 R2
  - Microsoft SQL Server 2012
  - MySQL Server 5.6.x

Database Driver Download locations

Oracle:
http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html

Microsoft SQL Server:
http://www.microsoft.com/en-us/download/details.aspx?id=36434

MySQL:
http://www.mysql.com/downloads/connector/odbc/#downloads

SSL Certificate Management Components

DB Scripts – These are the scripts to create the database schema. The currently supported databases are Oracle, Microsoft SQL Server, and MySQL.

SSL Certificate Management UI – The user interface program. Install and run this program on a machine where you want to configure and manage the SSL Certificate Management solution.

Windows Collector – This program runs as a Windows service and is used to scan websites and Windows Certificate stores for certificates. It must be installed on a machine in a location where it can access all the systems it needs to read certificates from. You can install this collector on more than one machine and you can also install multiple collectors on a single machine (you must give them unique collector names). The full collector name will consist of the name of the computer the collector is installed on plus the unique collector name you provide during the collector installation.

Java Collector – This is a Java program that can run on Windows or Linux systems and will read certificates from Java keystores. It must be installed on a machine in a location where it can access all the systems it needs to read certificates from. You can install this collector on more than one machine and you can also install multiple collectors on a single machine (you must give them unique collector names). The full collector name will consist of the name of the computer the collector is installed on plus the unique collector name you create using the *Properties File Manager* program installed on the machine where you installed the SSL Certificate Management UI.

Process Engine/Notification Engine – This program runs as a service on a Windows machine and handles the certificate processing as well as sending expiring certificate notifications to certificate owners. This process will need access to your SMTP server to send emails.

Installation

Setup the database

1) Depending on the database you choose, Oracle, Microsoft SQL Server, or MySQL, use the provided Database Scripts located in the DBScripts folder to create the database schema

Note

If you are upgrading from an earlier version of SSL Certificate Management, use the appropriate script located in the 'DBScripts/v1.5 to v2.0 Update Scripts' folder to upgrade your current database.

2) Download the ODBC drivers for the selected database from the vendor site (all JDBC drivers are included with the Java Collector program)

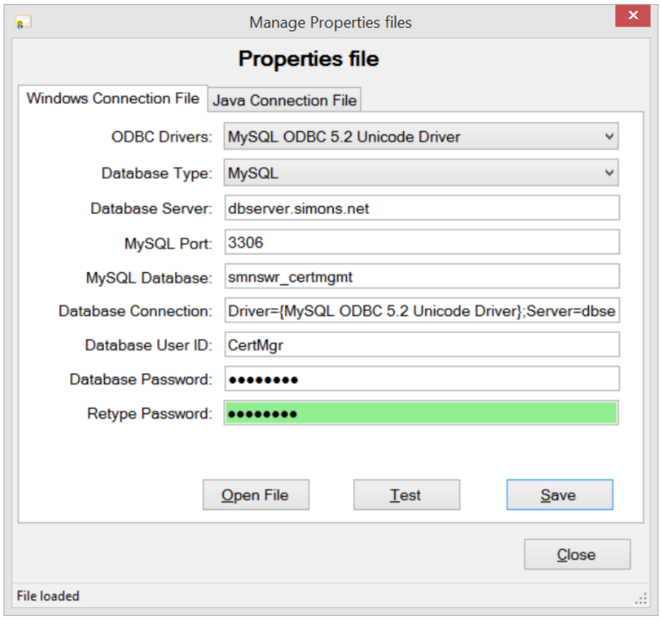
Oracle: http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html

Microsoft SQL Server: http://www.microsoft.com/en-us/download/details.aspx?id=36434

MySQL: http://www.mysql.com/downloads/connector/odbc/#downloads

Install the SSL Certificate Management User Interface (CMUI)

1) Install the ODBC driver on the computer where you will run the SSL Certificate Management UI application
2) Run CMUISetup.exe from the *User Application* directory and follow the prompts
3) The setup program will launch the *Manage Properties files* program
4) Fill in the database connection information for your selected database and click *Save*


Manage Properties files

Properties file

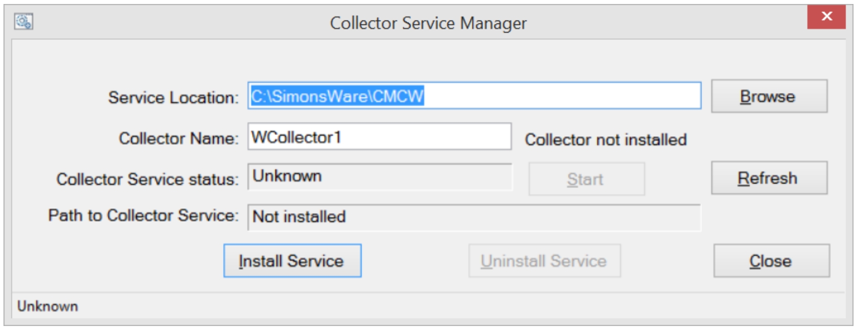
ODBC Drivers: MySQL ODBC 5.2 Unicode Driver
Database Type: MySQL
Database Server: dbserver.simons.net
MySQL Port: 3306
MySQL Database: smnswr_certmgmt
Database Connection: Driver={MySQL ODBC 5.2 Unicode Driver};Server=dbse
Database User ID: CertMgr
Database Password: ••••••••
Retype Password: ••••••••

File loaded

5) Click the *Test* button to test your configuration and connection to your database
6) Once the installation is complete, launch the application to ensure connectivity to your database

Install the SSL Certificate Management Collector for Windows (CMCW)

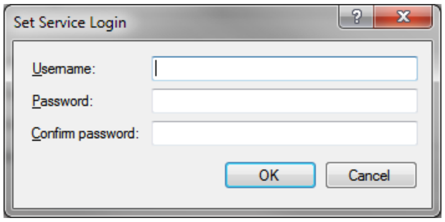
1) Determine the system or systems where you want to run the Windows Collector and copy the SSL Certificate Management *Windows Collector* folder to the system(s).
2) Copy and install the ODBC driver on the computer where you will run the Windows Collector application
3) Run CMCWSetup.exe from the *Windows Collector* folder and follow the prompts
4) The setup program will launch the *Manage Properties file* program. Complete the form the same as for the SSL Certificate Management UI application
5) The setup program will launch the *Collector Service Manager* program. Enter the Collector Name for this collector (or accept the default name of WCollector1). The collector name, along with the computer name is how you will identify this collector in the CMUI application and assign Scan Jobs to the collector.
6) Click *Install Service*.


Collector Service Manager

Service Location: C:\SimonsWare\CMCW
Collector Name: WCollector1
Collector not installed
Collector Service status: Unknown
Path to Collector Service: Not installed

Unknown

7) During the service installation, you will be prompted to enter credentials to run the service under. These credentials will need access to the Windows systems where you wish to retrieve certificates from the Windows Certificate Stores.



Username:
Password:
Confirm password:

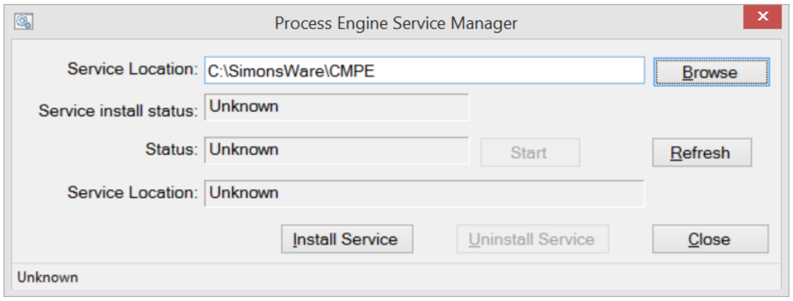
8) (Optional) Once the service is installed, you can start the service, by clicking *Start*
9) (Optional) You can click the *Refresh* button to refresh the service status
10) Click *Close* to exit
11) Exit the installation program

Install the SSL Certificate Management Process Engine (CMPE)

1) Determine the system where you want to run the Process Engine and copy the SSL Certificate Management *Process Engine* folder to the system.

Note **You should only have one process engine running at a time.**

2) Copy and install the ODBC driver on the computer where you will run the Process Engine application
3) Run CMPESetup.exe from the *Process Engine* folder and follow the prompts
4) The setup program will launch the *Manage Properties file* program. Complete the form the same as for the SSL Certificate Management UI application
5) The setup program will launch the *Process Engine Service Manager* program.
6) Click *Install Service*.



Service Location: C:\SimonsWare\CMPE
Service install status: Unknown
Status: Unknown
Service Location: Unknown
Unknown

7) (Optional) Once the service is installed, you can choose to start the service, by clicking *Start*
8) (Optional) Click the *Refresh* button to refresh the service status
9) Click *Close* to exit
10) Exit the installation program

Install the Java Collector

The Java Collector install is a little different since you can run the collector on Windows and Linux, and the flexibility of Java. In order to retrieve certificates on Linux/Unix machines, you will need to have a collector installed on a Linux server. To retrieve certificates from Windows machines, you will need to have a collector installed on a Windows server.

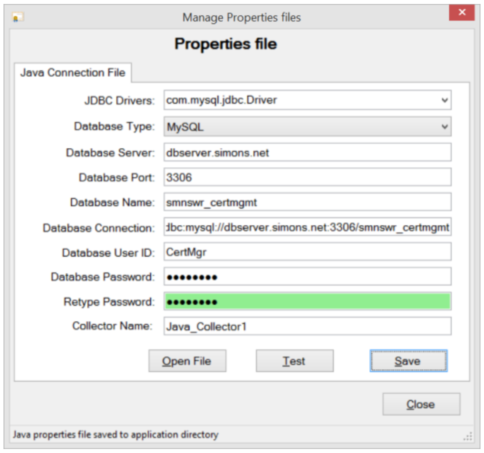
Note **If you need to scan IBM KDB keystores, see the Appendix for steps to enable those scans.**

Windows installation

You will need Java Runtime installed on the collector machine because the collector is written in Java. The Java Collector will install as a service on Windows machines. The collector will know it is installed on a Windows machine and will only try to connect to other machines by way of Windows UNC path name.

Note **This means you will need to create a share on all servers you wish to retrieve certificates from. You should use the same share name across all servers so one scan job can connect to all servers.**

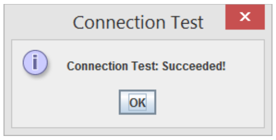
1) Install the supported version of Java Runtime (JRE) on the collector system
2) Run CMJCSetup.exe from the Java Collector\Windows folder and follow the prompts
3) The setup program will launch the Manage Properties file program.



JDBC Drivers: com.mysql.jdbc.Driver
Database Type: MySQL
Database Server: dbserver.simons.net
Database Port: 3306
Database Name: smnswr_certmgmt
Database Connection: dbc:mysql://dbserver.simons.net:3306/smnswr_certmgmt
Database User ID: CertMgr
Database Password: ••••••••
Retype Password: ••••••••
Collector Name: Java_Collector1

Java properties file saved to application directory

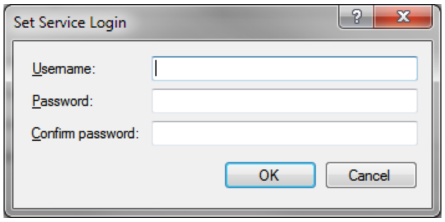
4) Fill in the connection information to configure the Java properties file.
5) In the *Collector Name* field enter a unique name for the Java Collector, or accept the default name
6) Click *Save*.
7) Click *Test* to test the connection (if everything is configured properly, you should see the following message)



Connection Test: Succeeded!

8) Click *OK.*

9) Click *Close*.
10) The setup program will launch the Java Collector Manager to install the collector as a service.
11) During the service installation, you will be prompted to enter credentials to run the service under. These credentials will need access to the Windows systems where you wish to retrieve certificates from the Java keystores.



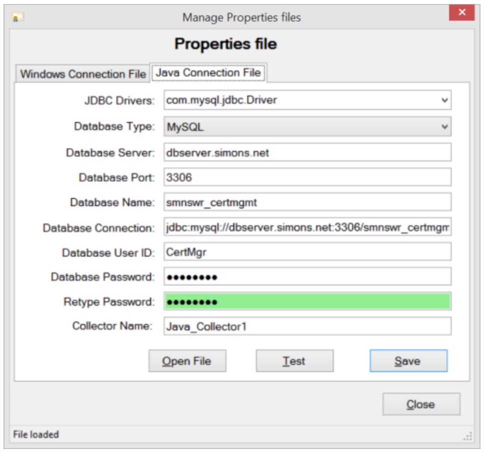
12) If all went well, the service will now be installed and running.

Note **The program will create a file called certmgmt.log with all logging information. View this file to check for any error messages.**

Linux installation

You will need Java Runtime installed on Linux as well. The collector will know it is installed on a Linux machine and will only try to connect to other machines by way of SSHFS (SSH File System).

1) Install the supported version of Java Runtime (JRE) on the collector system
2) Install FUSE and SSHFS (http://fuse.sourceforge.net/sshfs.html) on the collector system (See Appendix for installation steps)
3) You will need to enable certificate authentication from your Collector server to all Linux/Unix servers you want to retrieve certificates from (See Appendix for configuration steps)
4) Copy the *JavaCollectorInstall.tar* file to the collector system
5) Untar the file to the folder where you want to run the collector from
6) From the system where you have the SSL Certificate Management UI (CMUI) installed, run the *Properties File Manager* application, and click on the *Java Connection File* tab



JDBC Drivers: com.mysql.jdbc.Driver
Database Type: MySQL
Database Server: dbserver.simons.net
Database Port: 3306
Database Name: smnswr_certmgmt
Database Connection: jdbc:mysql://dbserver.simons.net:3306/smnswr_certmgm
Database User ID: CertMgr
Database Password: ••••••••
Retype Password: ••••••••
Collector Name: Java_Collector1

File loaded

7) Fill in the connection information to configure the Java properties file.
8) In the *Collector Name* field enter a unique name for the Java Collector, or accept the default name
9) Click *Save*.
10) Click *Close*.
11) Launch Windows Explorer and navigate to the folder where you have the SSL CMUI installed (default location is c:\SimonsWare\CMUI)
12) Copy the file CertMgmtJ.properties to the Linux collector system where you installed the Java Collector
13) On the Linux collector system, navigate to the folder where you installed the Collector
14) Execute *testconnection.sh* to test the connection (if everything is configured properly, you should see Connection succeeded!)

```
root@ulinux1:/simonsware# ./testconnection.sh
Connection succeeded!
```

15) If all went well, you can now launch the Java Collector by executing *startcertmgmt.sh* from the collector install location.

Log Settings

The Java Collector uses log4j for all logging. You can edit the *log4j.properties* file to change log settings. You can visit this site http://logging.apache.org/log4j/1.2/index.html for more information about log4j and the available settings.

Note **By default, DEBUG logging is turned on. To turn it off, edit the log4j.properties file and change the word DEBUG to INFO in the following line: log4j.logger.certmgmt=DEBUG, A**

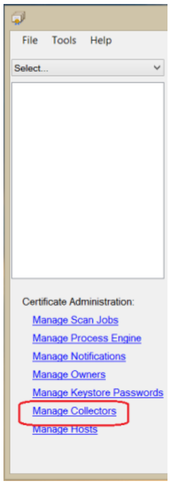
The Windows programs use log4net for all logging. You can edit the *CertMgmt.log4net* file to change log settings. You can visit this site http://logging.apache.org/log4net/ for more information about log4net and the available settings.

Note **By default, DEBUG logging is turned on. To turn it off, edit the CertMgmt.log4net file and change the word DEBUG to INFO on the following line:**

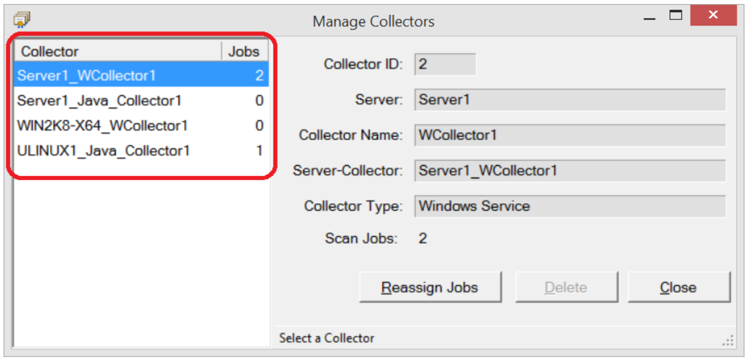
```
<filter type="log4net.Filter.LevelRangeFilter">
   <levelMin value="DEBUG"/>
</filter>
```

Configuration

1) Launch all Windows and Linux collectors. The collectors will automatically create Collector records in the database.
2) Launch *SSL Certificate Management UI* (CMUI).
3) Click the *Manage Collectors* link in the CMUI



3) Confirm the collector records were created (this could take a few minutes after launching the collectors)



Collector	Jobs
Server1_WCollector1	2
Server1_Java_Collector1	0
WIN2K8-X64_WCollector1	0
ULINUX1_Java_Collector1	1

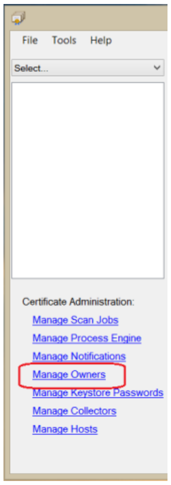
Collector ID: 2
Server: Server1
Collector Name: WCollector1
Server-Collector: Server1_WCollector1
Collector Type: Windows Service
Scan Jobs: 2

Select a Collector

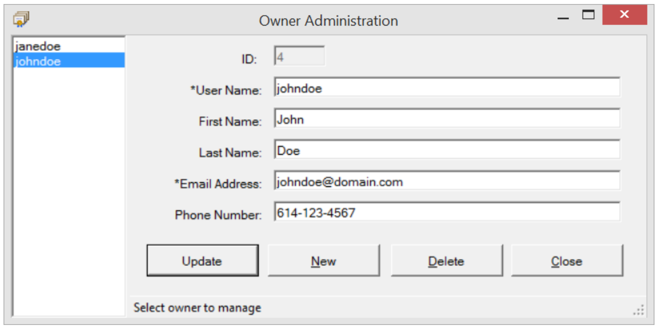
4) Click *Close* to exit the Manage Collectors form

Manage Owners

This is the form where you manage the list of users you want to notify of expiring certificates.



1) Click the *Manage Owners* link.



Owner Administration

janedoe
johndoe

ID: 4

*User Name: johndoe

First Name: John

Last Name: Doe

*Email Address: johndoe@domain.com

Phone Number: 614-123-4567

Select owner to manage

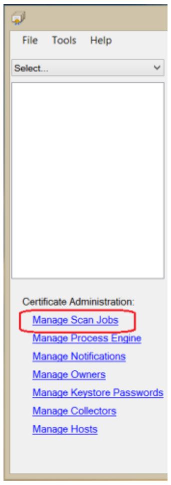
2) Fill in the user information. You must supply at least a User Name and properly formatted email address to add a user. All other fields are optional.

Note **It is not mandatory to create users at this time. You can create them and assign them at any time.**

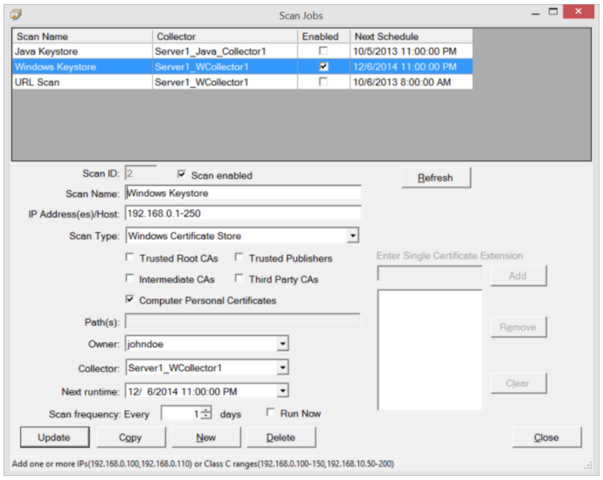
3) Once you have added users, click the *Close* button

Create Scan Jobs

The Scan Jobs are the jobs that the collectors process to pull certificates from the locations you specify.



1) Click the *Manage Scan Jobs* link in the CMUI (For detailed Scan Job configuration steps, please see the User Guide)

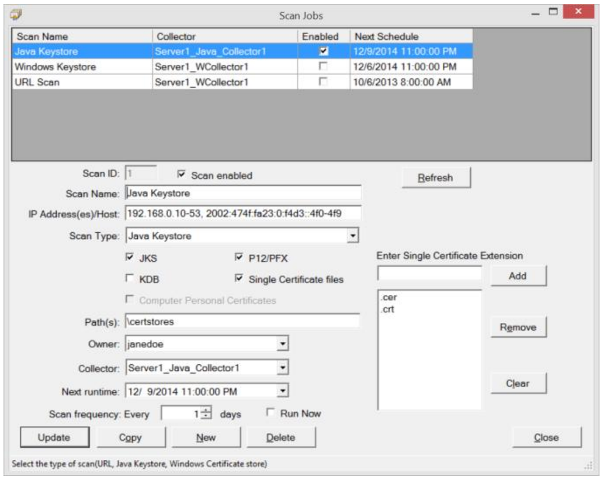


Scan Name	Collector	Enabled	Next Schedule
Java Keystore	Server1_Java_Collector1	☐	10/5/2013 11:00:00 PM
Windows Keystore	Server1_WCollector1	☑	12/6/2014 11:00:00 PM
URL Scan	Server1_WCollector1	☐	10/6/2013 8:00:00 AM

Scan ID: 2 ☑ Scan enabled
Scan Name: Windows Keystore
IP Address(es)/Host: 192.168.0.1-250
Scan Type: Windows Certificate Store
☐ Trusted Root CAs ☐ Trusted Publishers
☐ Intermediate CAs ☐ Third Party CAs
☑ Computer Personal Certificates
Path(s):
Owner: johndoe
Collector: Server1_WCollector1
Next runtime: 12/ 6/2014 11:00:00 PM
Scan frequency: Every 1 days ☐ Run Now

Add one or more IPs(192.168.0.100,192.168.0.110) or Class C ranges(192.168.0.100-150,192.168.10.50-200)

Windows Certificate Store



Scan Name	Collector	Enabled	Next Schedule
Java Keystore	Server1_Java_Collector1	☑	12/9/2014 11:00:00 PM
Windows Keystore	Server1_WCollector1	☐	12/6/2014 11:00:00 PM
URL Scan	Server1_WCollector1	☐	10/6/2013 8:00:00 AM

Scan ID: 1 ☑ Scan enabled
Scan Name: Java Keystore
IP Address(es)/Host: 192.168.0.10-53, 2002:474f:fa23:0:f4d3::4f0-4f9
Scan Type: Java Keystore
☑ JKS ☑ P12/PFX
☐ KDB ☑ Single Certificate files
☐ Computer Personal Certificates
Path(s): \certstores
Owner: janedoe
Collector: Server1_Java_Collector1
Next runtime: 12/ 9/2014 11:00:00 PM
Scan frequency: Every 1 days ☐ Run Now
.cer
.crt

Select the type of scan(URL, Java Keystore, Windows Certificate store)

Java Keystore

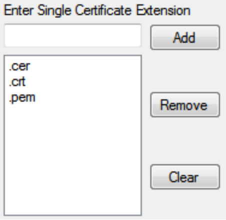
2) Scan Name – Enter a descriptive name for your scan job
3) Scan Enabled – You must check the *Scan enabled* checkbox to activate this job
4) IP Address(es)/Host – Enter a single IP address or host name, a range of IP addresses, or a comma separated list of IP addresses or hosts. (Supports both IPv4 and IPv6 addresses)

Note **You can add an IP address range at the last octet level (i.e. 192.168.0.1-250) only. However, you can add multiple ranges in the scan by separating them with a comma (i.e. 192.168.0.1-250,192.168.1.1-250,2002:474f:fa23:0:f4d3::4f0-4f9)**

5) Scan Type – Select the *Scan Type* from the dropdown list. A scan job can only process one scan type (Windows Certificate Store, Java Keystore, or URL).

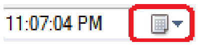
Note **Based on the scan type you choose, the checkboxes will be enabled for more granular specifications. Also, selecting anything other than *Windows Certificate Store* will enable the Port(s)/Path(s) field.**

6) Check the appropriate checkboxes for the types of certificates you want to scan. For Java Keystore, you can check the *Single Certificate files* box to enable the section to add single certificate types to be scanned (i.e. .cer, .crt, .pem, etc).



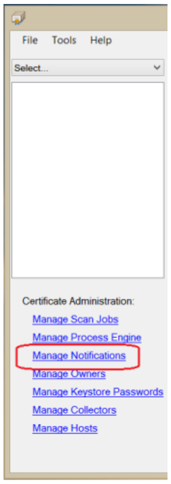
.cer
.crt
.pem

7) Port(s)/Path(es) – Enter the path or ports for the scan. For ports, this can be a comma separated list with port ranges specified as well (i.e. 443,8443-8447)

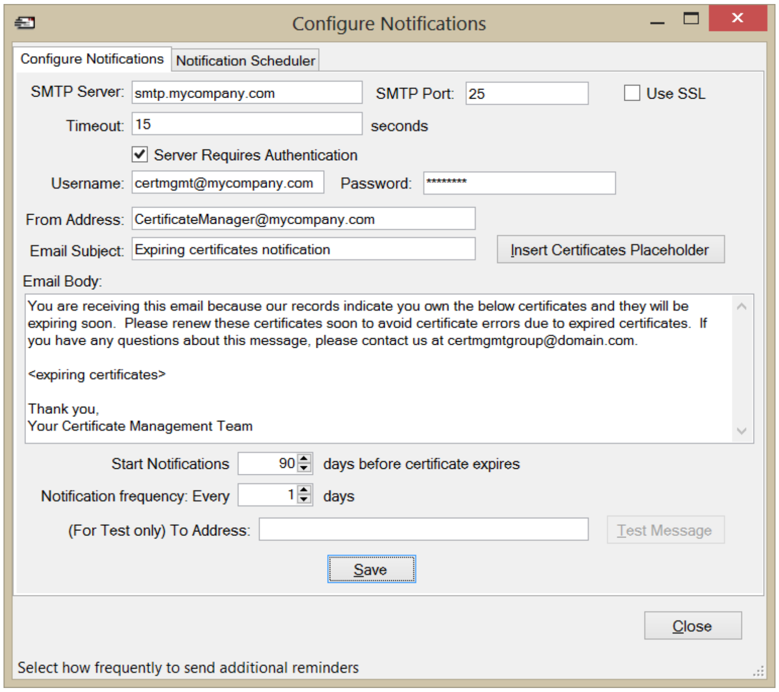
8) Owner – You can select a default owner for all certificates discovered by this scan job. You can change the owner on certificates later if needed.
9) Collector – Select the collector to execute this job from the list of collectors. The available collectors in the list are based on the type of scan you selected.
10) Next runtime – Set the next time you want this job to run. Click the calendar button  to change the date for the next run.
11) Scan frequency – Set how frequently you want this job to run. Because certificates are normally valid for a year or more, I recommend setting this to no less than 30-60 days.
12) Run Now – Check the *Run Now* box if you want the job to run immediately. (Scan must be enabled in order to select *Run Now*)
13) Click the *Add* button to create the scan job
14) Click *Close*

Configure Notifications

The Notification form is where you configure the SMTP server settings for sending email notifications to certificate owners. You also create the form letter that will be sent to a certificate owner when you are notifying them of expiring certificates.



1) Click the *Manage Notifications* link in the CMUI



SMTP Server: smtp.mycompany.com
SMTP Port: 25
☐ Use SSL
Timeout: 15 seconds
☑ Server Requires Authentication
Username: certmgmt@mycompany.com
Password: ********
From Address: CertificateManager@mycompany.com
Email Subject: Expiring certificates notification
Email Body:

You are receiving this email because our records indicate you own the below certificates and they will be expiring soon. Please renew these certificates soon to avoid certificate errors due to expired certificates. If you have any questions about this message, please contact us at certmgmtgroup@domain.com.

<expiring certificates>

Thank you,
Your Certificate Management Team

Start Notifications 90 days before certificate expires
Notification frequency: Every 1 days
(For Test only) To Address:

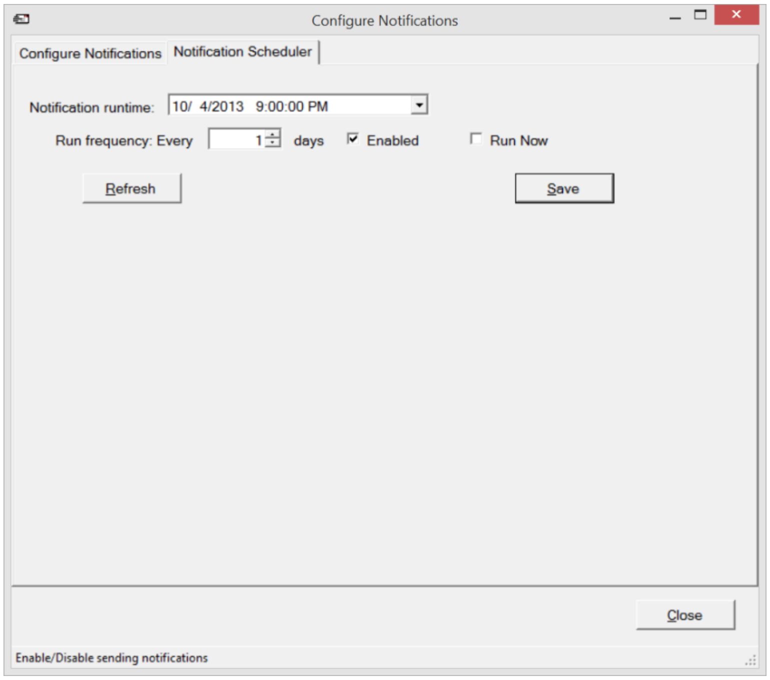
Select how frequently to send additional reminders

On the *Configure Notifications* tab:

2) Fill in the SMTP server connection information for your network
3) From Address – set the address you want the email to be sent from
4) Email Subject – set the subject for the email that will be sent to owners when they are being notified of expiring certificates
5) Email body – Enter email text you want to be included in the email message sent to the certificate owners
6) Insert Certificate Placeholder – ***Most important *** - Place the cursor at the location in the email body where you want the expiring certificate information to be inserted, then click the *Insert Certificate Placeholder* button

Note **Clicking the button will insert the text <expiring certificates> into the body of the email. This will be replaced at run time with the expiring certificate information.**

7) Start Notification – Set the number of days before a certificate expires that you want to start sending notifications to the owner to renew.
8) Notification frequency – Set the time interval for when you want to send additional notifications to the owner to renew their certificates.
9) Test – Once you have completed the form, you can enter an email address into the To Address field and send a test email message to ensure the notification process is working properly.
10) Click *Save*
11) Click the *Notification Scheduler* tab



Notification runtime: 10/ 4/2013 9:00:00 PM

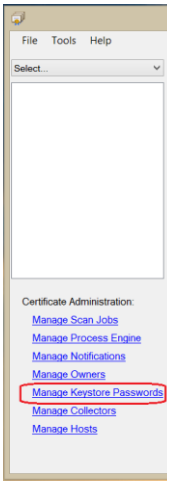
Run frequency: Every 1 days ☑ Enabled ☐ Run Now

Enable/Disable sending notifications

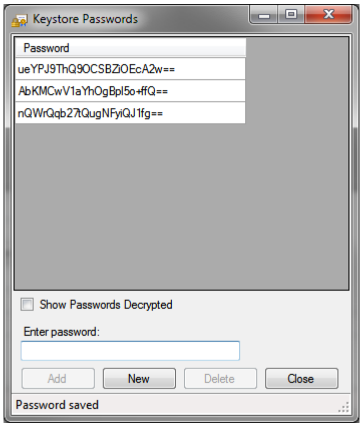
12) Notification runtime – Set the time you want the Notification process to run.
13) Set the frequency – Set the frequency for the job to run. I recommend daily or weekly.
14) Check the *Enabled* box to enable the Notification process. This is how you can enable or disable notifications without having to stop the service.
15) Run Now – Check the *Run Now* box if you want to run the Notification process immediately. (The Notification process must be enabled in order to select *Run Now*)
16) Click *Save*
17) Click *Close*

Manage Keystore Passwords

If you want to retrieve certificates from Java keystores, some keystores require you to enter the password before they will allow you to retrieve the certificates. You can create a list of passwords that will be used to unlock the keystores to retrieve certificates.



1) Click the *Manage Keystore Passwords* link in the CMUI



Password
ueYPJ9ThQ9OCSBZiOEcA2w==
AbKMCwV1aYhOgBpl5o+ffQ==
nQWrQqb27tQugNFyiQJ1fg==

Password saved

2) Type a keystore password in the field and click *Add*

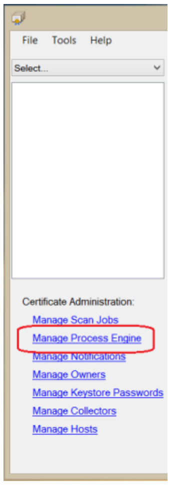
Note

By default, the passwords in the list will be encrypted. If you click the *Show Passwords Decrypted* checkbox, the passwords will display in plain text.

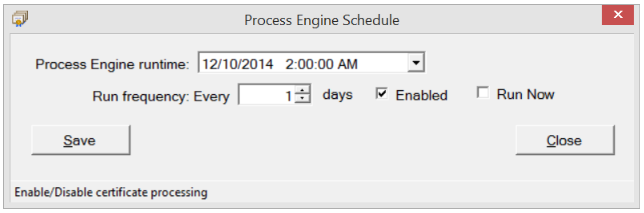
3) Click *Close* when done

Manage Process Engine

Use the *Manage Process Engine* link to manage the certificate processing schedule. The process engine will process the certificates imported by the Collectors and set them based on how you configured SSL Certificate Management to import them.



1) Click the *Manage Process Engine* link in the CMUI


Process Engine Schedule

Process Engine runtime: 12/10/2014 2:00:00 AM

Run frequency: Every 1 days ☑ Enabled ☐ Run Now

Enable/Disable certificate processing

2) Process Engine runtime – Set the time you want the Process Engine process to run
3) Set the frequency – Set the frequency for the job to run. I recommend daily or weekly.
4) Check the *Enabled* box to enable the Process Engine. This is how you can enable or disable the process engine without having to stop the service.
5) Run Now – Check the *Run Now* box if you want to run the Process Engine immediately. (The Process Engine must be enabled in order to select *Run Now*)
6) Click *Save*
7) Click *Close*

Appendix

FUSE and SSHFS installation and configuration

Download FUSE and SSHFS from here: http://fuse.sourceforge.net/sshfs.html

FUSE:

From the directory where you unzipped/untarred FUSE (View the README and INSTALL files for detailed installation instructions)

```
./configure
make
make install
modprobe fuse
```

SSHFS:

From the directory where you unzipped/untarred SSHFS (View the README and INSTALL files for detailed installation instructions)

```
./configure
make
make install (run this command as root)
```

Database Connection string samples

MySQL

JDBC - jdbc:mysql://192.168.0.201:3306/smnswr_certmgmt
ODBC - Driver={MySQL ODBC 5.1 Driver};Server=192.168.0.201;Database=smnswr_certmgmt;Port=3306

MSSQL

JDBC - jdbc:sqlserver://192.168.0.201;instanceName=SQLEXPRESS;databaseName=smnswr_certmgmt
ODBC - Driver={SQL Server};Server=192.168.0.201\SQLEXPRESS;Database=smnswr_certmgmt

Oracle

JDBC - jdbc:oracle:thin:@//192.168.0.201:1521/XE
ODBC - Driver={Oracle in instantclient_11_2};dbq=192.168.0.201:1521/XE

SSH Certificate Authentication configuration

CollectorServer – Server where the collector will be running
CertServer – Server CollectorServer will connect to and retrieve certificates

On CollectorServer, from the home dir of the ID CertMgmt.jar will be running under, type the following commands:

(For this example, the CertMgmt.jar program is running under the ID foo)

```
cd /foo
cd .ssh
ssh-keygen       (This will create one of two files: identity.pub or id_rsa.pub.  This example shows id_rsa.pub)
scp id_rsa.pub foo@CertServer:~foo/.ssh/CollectorServer.pub
ssh CertServer
cd .ssh
cat CollectorServer.pub >> authorized_keys
```

Enable KDB keystore scanning

If you are running an IBM Web/Application server that uses KDB keystore files, capabilities for reading those files is not built into Java. You will need to follow the below steps to enable KDB file scanning.

1) Locate the files **ibmcmsprovider.jar** and **ibmpkcs.jar** on your IBM Web/Application server and copy them to your $JAVA_HOME/jre/lib/ext folder on your Java Collector machine
2) Edit your java security file **$JAVA_HOME/jre/lib/security/java.security**
3) Add this line to the file **security.provider.N=com.ibm.security.cmskeystore.CMSProvider**

   where N is the next available number

   Example:

   ```
   …
   security.provider.10=sun.security.mscapi.SunMSCAPI
   security.provider.11=com.ibm.security.cmskeystore.CMSProvider
   ```