SimonsWare

# SSL Certificate Management v2.0 User Guide

# Table of Contents


Certificate Management tasks ..... 3

View Certificates ..... 3

Manage Certificates ..... 4

Ignoring Certificates ..... 5

Activity Log ..... 7

Save results ..... 7

Certificate Management Administration ..... 8

Manage Scan Jobs ..... 8

Windows Certificate Store ..... 9

Java Keystore ..... 10

URL ..... 12

Manage Process Engine ..... 13

Manage Notifications ..... 14

Manage Owners ..... 16

Manage Keystore Passwords ..... 17

Manage Collectors ..... 18

Reassign Scan Jobs ..... 20

Delete Collectors ..... 20

Manage Hosts ..... 21

Log Settings ..... 21

Windows programs ..... 21

Java Collector ..... 22

Appendix ..... 23

FUSE and SSHFS installation and configuration ..... 23

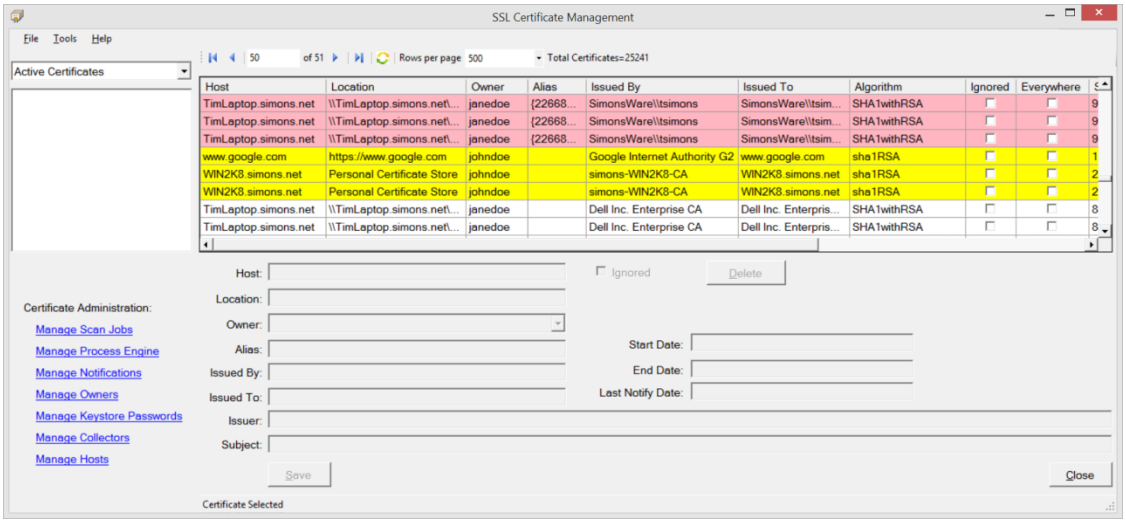
Database Connection string samples ..... 23

SSH Certificate Authentication configuration ..... 23

Enable KDB keystore scanning ..... 24

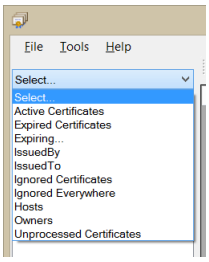
# Certificate Management tasks

This section defines the options for managing certificates already discovered with Scan Jobs.

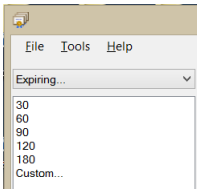



## *View Certificates*

There are many options for viewing certificates which will be described below. From the dropdown box, choose which certificates to view and manage.




- Active Certificates – This will show all currently active certificates in the system (excluding all certificates with the 'ignore' flag set)
- Expired Certificates – This will show all certificates that are expired(excluding ignored certificates)
- Expiring Certificates – Will present a list below the dropdown box where you can choose to show certificates expiring within the selected number of days

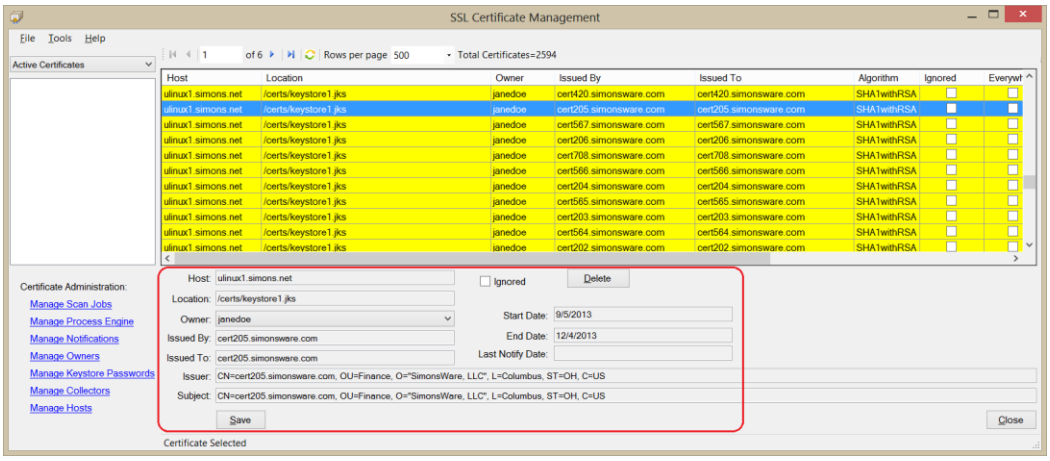


**Choosing *Custom…* will present you with an input box to set your own custom number of days**

- IssuedBy – Will present a list below the dropdown box where you can choose to show only certificates issued by a selected entity. You can select multiple entries to show certificates for multiple issuers
- IssuedTo – Similar to IssuedBy it will present a list of entities certificates have been issued to.
- Ignored Certificates – Will show you a list of all certificates currently being ignored by the system. The system will not send expiring notifications for any certificate in this list. Removing the checkmark in the *Ignored* column will stop ignoring the selected certificate and re-enable expiration notifications.
- Ignored Everywhere – Will show you a list of certificates you have elected to ignore anywhere they appear. Removing the checkmark in the *Ignored* column will stop ignoring the certificate everywhere and remove the ignored flag from all certificates matching the selection.
- Hosts – Will present a list below the dropdown box of all hosts in the system. Select a host to see all certificates retrieved from that host (you can select multiple hosts).
- Owners – Will present a list below the dropdown box of all owners in the system. Select an owner to see all certificates owned by that person (you can select multiple owners). This is the person who will be notified when it is time to renew the certificate.
- Unprocessed Certificates – This is the list of certificates that have been added by the collectors but not yet processed by the Process Engine. If you constantly have certificates in this list, you may want to run the Process Engine more frequently.

## *Manage Certificates*

To manage a single certificate, select the certificate from the table and you will see detailed information about that certificate in the form below the table.



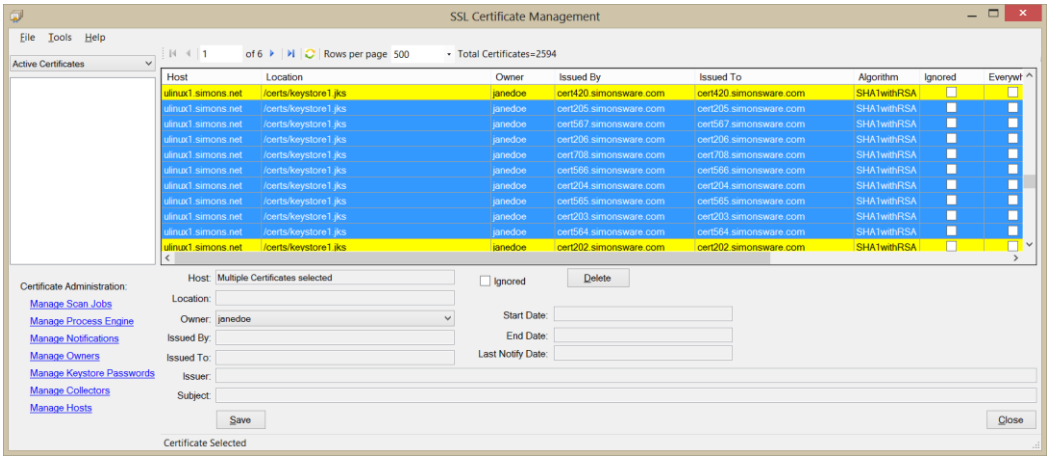

To modify a single certificate:

1) Select the certificate you want to manage from the table
2) Change the owner, set the Ignored flag, or both
3) Click *Save*

To delete a single certificate:

1) Select the certificate you want to delete from the table
2) Click *Delete*

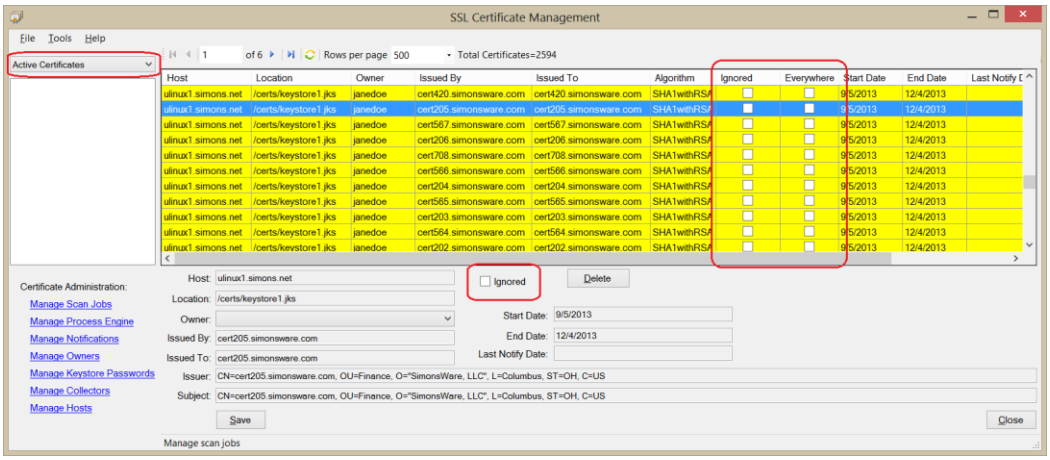
To modify multiple certificates:




1) Select all the certificates you want to manage by selecting the first one, then hold the shift or control key and select the rest
2) The Host field will show 'Multiple Certificates selected'. You can now manage multiple certificates the same as you did the single certificate

## *Ignoring Certificates*

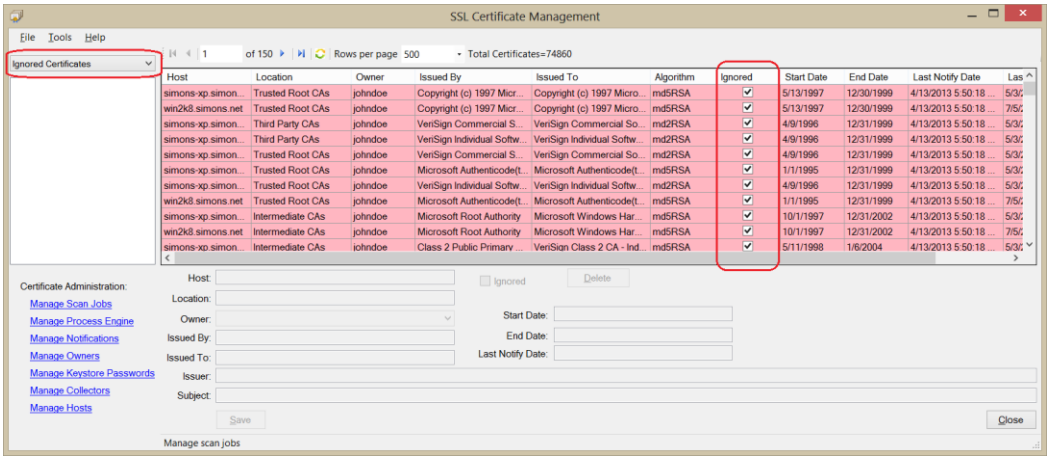
From Active Certificates view:




There are multiple ways to ignore certificates. The first was described in the above section *Manage Certificates* where you used the form below the table to set the ignored flag. The second option is to use your mouse and click the 'Ignored' checkbox in the table next to the certificate you want to ignore. This will tell the system to

ignore this specific certificate. You can also click the 'Everywhere' checkbox in the table next to the certificate you want to ignore. This will tell the system to ignore this certificate wherever it appears.

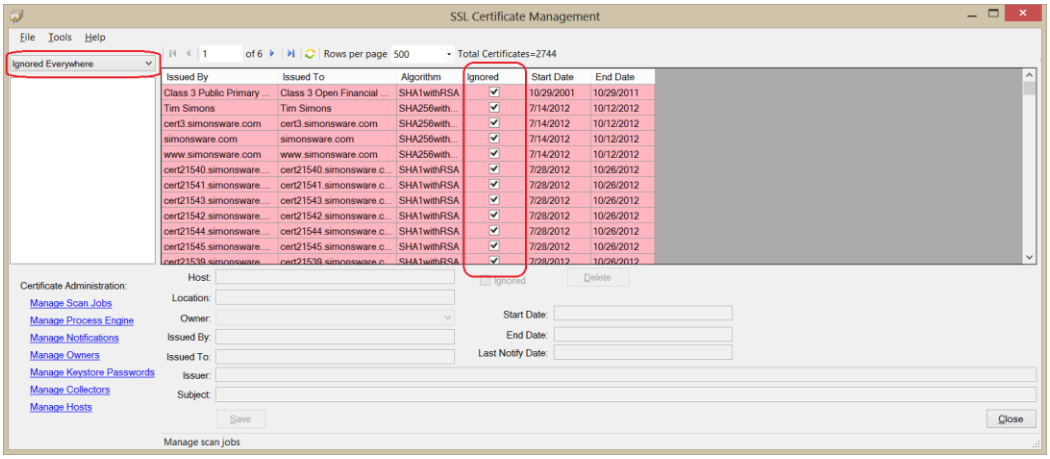
From Ignored Certificates view:



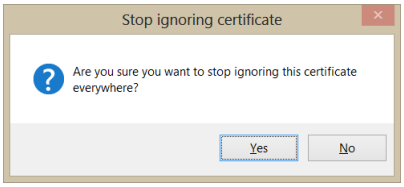

From the Ignored Certificates view, you can choose to stop ignoring a certificate. Click the Ignored column to remove the checkmark from the box. This will stop ignoring the certificate and allow expiration notifications to be sent for that certificate.

You can also select a single or multiple certificates and use the form below the table to remove the ignored flag. Just remember to click the *Save* button to save the change.

From Ignored Everywhere view:

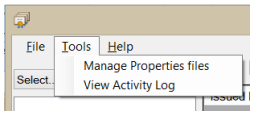



In the Ignored Everywhere view, you can only stop ignoring a certificate by clicking the Ignored column in the table view to remove the checkmark, you will be prompted to confirm you want to do this. SSLCM will immediately reset all certificates matching the selection to an active state. You cannot use the form below the table to manage certificates that are ignored everywhere and you cannot select multiple certificates and opt to stop ignoring the group.

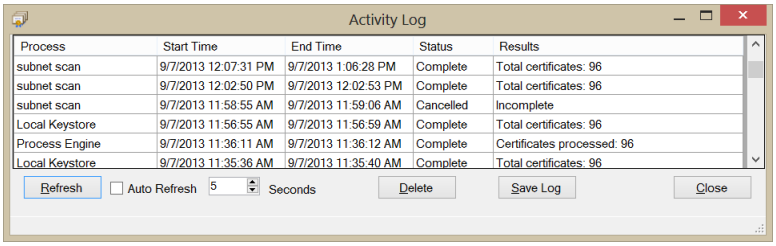



## *Activity Log*

The Activity log allows you to view the status of your scheduled tasks. You can monitor currently running tasks, as well as see the status of previously executed tasks.




1) Click *Tools* on the menu
2) Click *View Activity Log.* From here, you can see the status of all jobs as well as the results




3) Click the *Refresh* button to manually refresh the screen
4) You can also set the refresh interval and check the *Auto Refresh* checkbox to have the screen automatically refresh at the selected interval


**Selecting Auto Refresh disables the Delete and Save Log buttons. To re-enable them, deselect the Auto Refresh checkbox.**

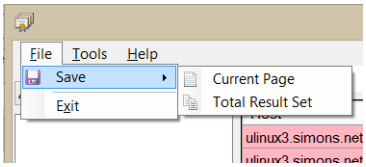
5) You can delete jobs from the log by selecting the jobs you wish to delete then clicking the *Delete* button

Click the *Save Log* button to save the entire log to a CSV file

## *Save results*

You can save your current certificate view to a CSV file for reporting or other purposes.

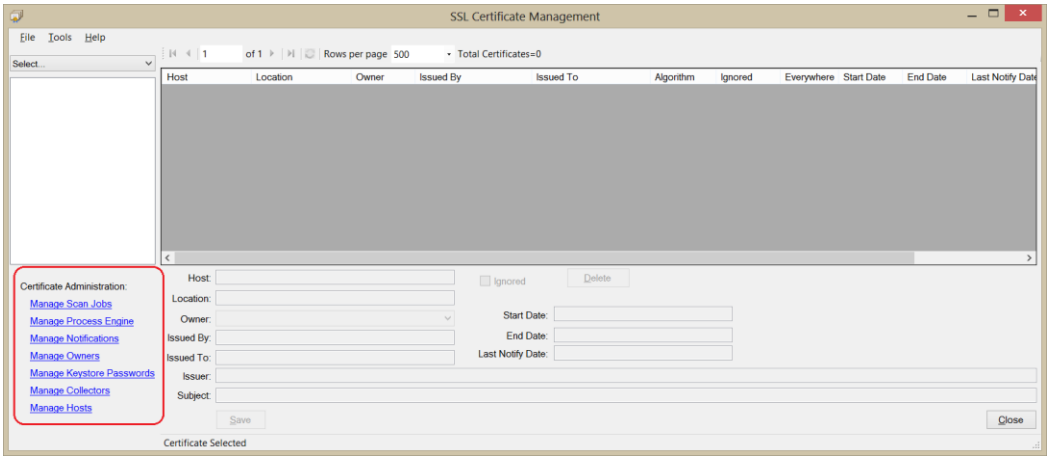
1) Select certificates to view from the dropdown list
2) Click File->Save



3) Choose *Current Page* or *Total Result Set*
4) Enter a file name to save the results
5) Click *Save*

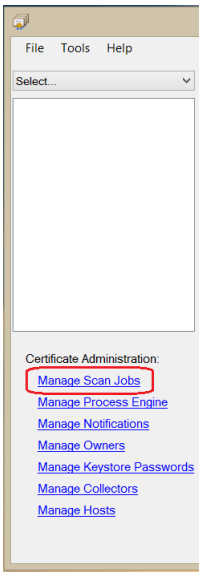
## Certificate Management Administration

This section will define all the administration tasks available in SSL Certificate Management. The administrative links are located in the lower left section of the main screen.




### *Manage Scan Jobs*

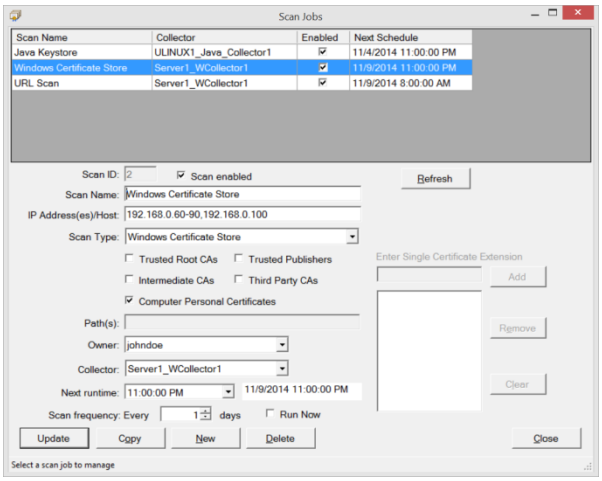
From the Scan Jobs screen, you can create, modify, and delete scan jobs. You can also enable and disable the execution of a job from this screen.




1) Click the *Manage Scan Jobs* link in the CMUI

The following sections explain the different Scan Job types (Windows Certificate Store, Java Keystore, URL).

## Windows Certificate Store




1) Scan Name – Enter a descriptive name for the scan job
2) Scan Enabled – Check the *Scan enabled* checkbox to activate this job, otherwise, this job will not be processed by the selected collector
3) 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 and/or hosts. (Supports both IPv4 and IPv6 addresses)

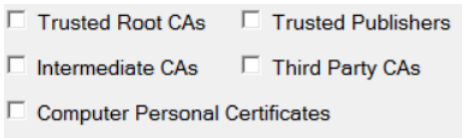

**You can add an IP address range at the last octet level (i.e. 192.168.0.1-250) only. You can add multiple ranges in the scan by separating them with a comma (i.e. 192.168.0.1-250, 192.168.1.1-250)**

Examples:

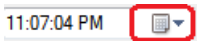
| | |
|---|---|
| Single IP | 192.168.0.22 |
| Multiple IPs | 192.168.0.22, 192.168.0.144, 2002:474f:fa23:0:f4d3::4f0 |
| Single IP Range | 192.168.0.1-250 |
| Multiple IP Ranges | 192.168.0.1-250, 2002:474f:fa23:0:f4d3::4f0-4f9 |
| Host name | www.mydomain.com |
| Combination | www.mydomain.com, 192.168.0.27 |

4) Scan Type – Select *Windows Certificate Store* from the dropdown list


**Choosing *Windows Certificate Store* will enable the following checkboxes.**

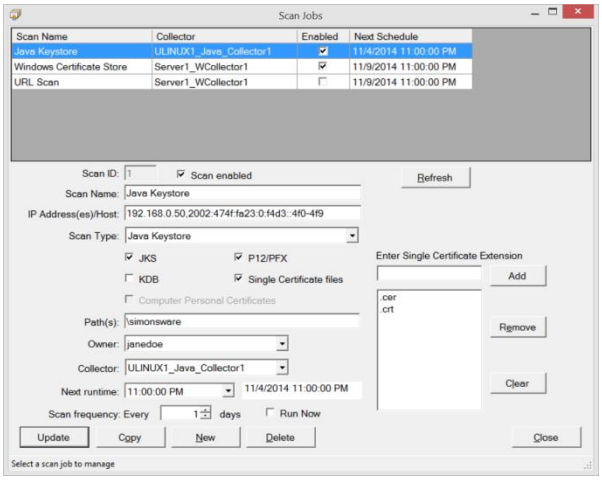



5) Check the appropriate checkboxes for the Windows Certificate Stores you want to scan.

6) Path(s) – This field is disabled as it is not used for Windows Certificate Stores
7) 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.
8) 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. Only collectors of type *Windows Service* will show in the list
9) Next runtime – Set the next time you want this job to run. Click the calendar button 

to change the date for the next run.
10) 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 days.
11) 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*)
12) Click the *Add* button to create the scan job
13) Click *Close*

## Java Keystore




1) Scan Name – Enter a descriptive name for your scan job
2) Scan Enabled – You must check the *Scan enabled* checkbox to activate this job, otherwise, this job will not be processed by the selected collector
3) 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)


**You can add an IP address range at the last octet level (i.e. 192.168.0.1-250) only. 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)**

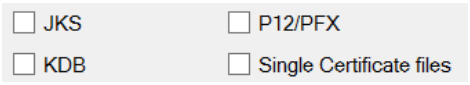
Examples:

| | |
|---|---|
| Single IP | 192.168.0.22 |
| Multiple IPs | 192.168.0.22, 192.168.0.144, 2002:474f:fa23:0:f4d3::4f0 |
| Single IP Range | 192.168.0.1-250 |
| Multiple IP Ranges | 192.168.0.1-250, 2002:474f:fa23:0:f4d3::4f0-4f9 |

| | |
|---|---|
| Host name | www.mydomain.com |
| Combination | www.mydomain.com, 192.168.0.27 |

4) Scan Type – Select *Java Keystore* from the dropdown list.

**Choosing *Java Keystore* will enable the following checkboxes.**




5) Check the appropriate checkboxes for the types of certificate keystores you want to scan. You can check the *Single Certificate files* box to enable the section to add individual certificate types to be scanned (i.e. .cer, .crt, .pem, etc).


If you select the KDB keystore, see the appendix for additional steps required to enable reading this keystore type.

6) Path(s) – Enter the file system path for the scan

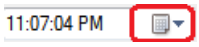
For Windows systems, you will need to create a file system Share for the scan and ensure the user id the scan is running under has read access to the file Share. The collector will start search the selected directory and all subdirectories for selected certificate types. Format \ShareName\Directory

Example: \CertStore\mycertificates – CertStore is the name of the file system share you created and mycertificates is the directory to start scanning from. If you want to search the entire share, you would enter \CertStore only for the path. Create all paths with a backslash (\); the collector will substitute forward slashes if the collector is running on Linux/Unix.

For Linux/Unix systems, you can specify the directory where you want to start scanning. The collector will start search the selected directory and all subdirectories for selected certificate types. Create all paths with a backslash (\);the collector will substitute forward slashes if the collector is running on Linux/Unix.

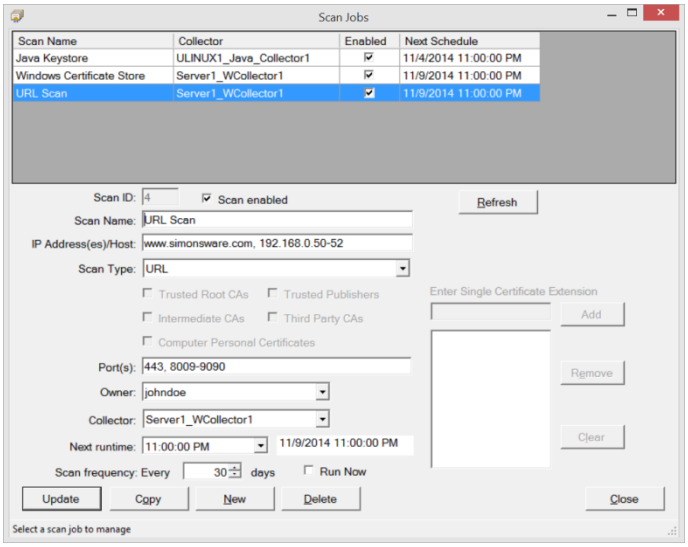
Examples:

| | |
|---|---|
| \ | Start searching for specified certificates at the root of the file system and search all subdirectories |
| \certificates | Start searching for specified certificates at the 'certificates' directory, which is located off the root directory and search all subdirectories |
| \certificates\subdirectory | Start searching for specified certificates at the directory 'subdirectory' which is under the 'certificates' directory |

7) 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.
8) 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.
9) Next runtime – Set the next time you want this job to run. Click the calendar button 

to change the date for the next run.
10) 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 60 days.
11) 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*)
12) Click the *Add* button to create the scan job
13) Click *Close*

## URL




1) Scan Name – Enter a descriptive name for your scan job
2) Scan Enabled – You must check the *Scan enabled* checkbox to activate this job, otherwise, this job will not be processed by the selected collector
3) 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)


**You can add an IP address range at the last octet level (i.e. 192.168.0.1-250) only. 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)**

Examples:

| | |
|---|---|
| Single IP | 192.168.0.22 |
| Multiple IPs | 192.168.0.22, 192.168.0.144, 2002:474f:fa23:0:f4d3::4f0 |
| Single IP Range | 192.168.0.1-250 |
| Multiple IP Ranges | 192.168.0.1-250, 2002:474f:fa23:0:f4d3::4f0-4f9 |

| | |
|---|---|
| Host name | www.mydomain.com |
| Combination | www.mydomain.com, 192.168.0.27 |

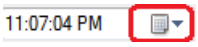
4) Scan Type – Select *URL* from the dropdown list.

**Because this is a URL scan, the four checkboxes below the Scan Type will be disabled.**

5) Port(s) – Enter the ports for the scan. This can be a comma separated list with port ranges specified as well (i.e. 443,8443-8447)

**You can add single ports, a range of ports, or a combination of both.**
Examples:

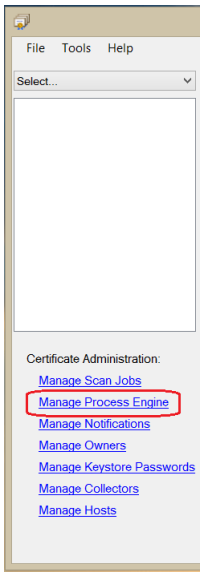
| | |
|---|---|
| Single port | 443 |
| Multiple ports | 443, 8009, 10000 |
| Port range | 8009-10000 |
| Multiple Port ranges | 4000-5000, 9000-10000 |
| Combination | 443, 8009-9000, 5150 |

6) 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.
7) 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.
8) Next runtime – Set the next time you want this job to run. Click the calendar button 

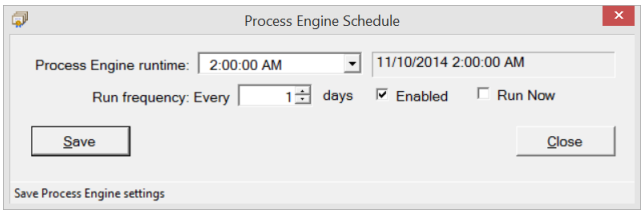
to change the date for the next run.
9) Scan frequency – Set how frequently you want this job to run. Because certificates are normally valid for a year or more, I recommend setting this to no less than 60 days.
10) Run Now – Check the *Run Now* box if you want the job to run immediately. (Scan must be enabled in order to select *Run Now*)
11) Click the *Add* button to create the scan job
12) Click *Close*

## *Manage Process Engine*

Use the *Manage Process Engine* link to manage the certificate processing. 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.



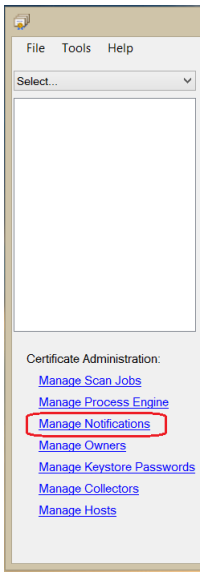

1) Click the *Manage Process Engine* link in the CMUI



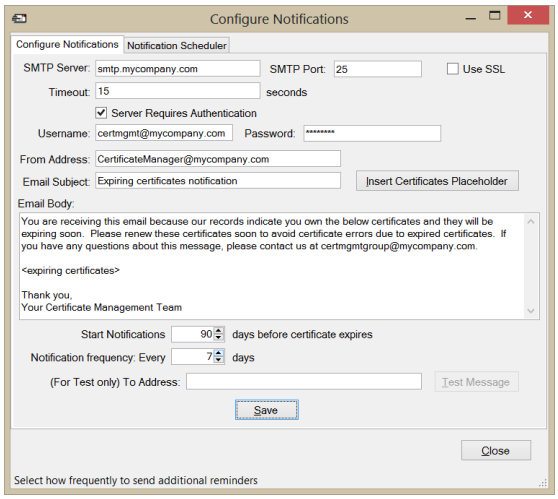

2) Process Engine runtime – Set the time you want the Process Engine process to run
3) Set the frequency – Set the frequency for the job to run. I recommend daily or weekly.
4) Check the *Enabled* box to enable the Process Engine. This is how you can enable or disable the process engine without having 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*

## ***Manage 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

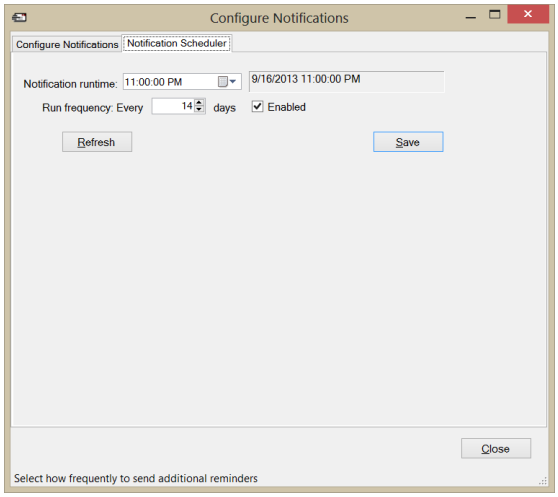



On the *Configure Notifications* tab:

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

**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.**

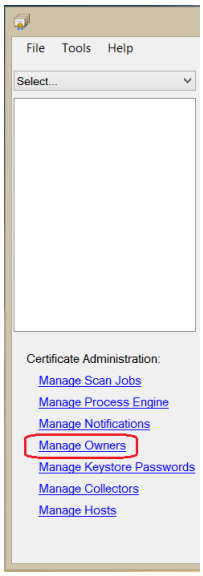
7) Start Notification – Set the number of days before a certificate expires that you want to start sending notifications to the owner to renew.
8) Notification frequency – Set the time interval for when you want to send additional notifications to the owner to renew their certificates.
9) Test – Once 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



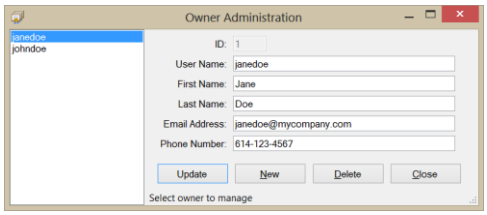

12) Notification runtime – Set the time you want the Notification process to run.
13) Set the frequency – Set the frequency for the job to run. I recommend daily or weekly.
14) Check the *Enabled* box to enable the Notification process. This is how you can enable or disable notifications without having to stop the service.
15) Click *Save*
16) Click *Close*

## ***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.



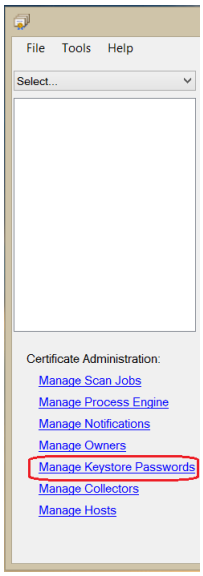

2) Fill in the user information. You must supply at least a User Name and properly formatted email address to add a user. All other fields are optional.


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

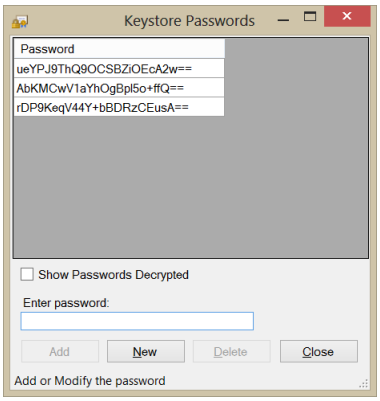
3) Once you have added users, click the *Close* button

## *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. When the Java collector is attempting to read Java keystores, it will cycle through this list of passwords until it finds one that unlocks the keystore.




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



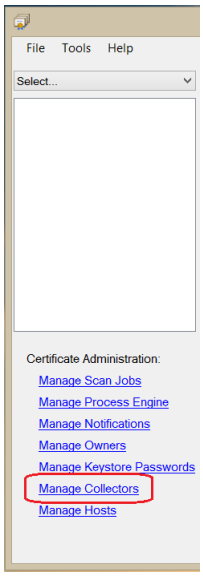

2) Type a keystore password in the field and click *Add*

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

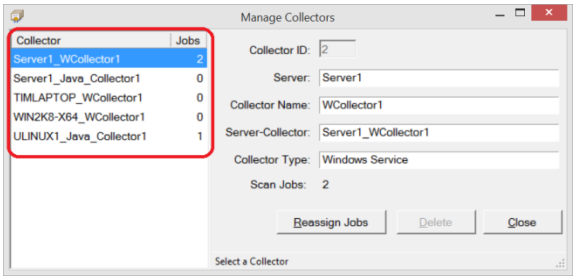
3) Click *Close* when done

## *Manage Collectors*

The Manage Collectors form is where you manage all collectors on the system. When you install and start a collector, it will automatically create a collector record for you and populate all the appropriate information.



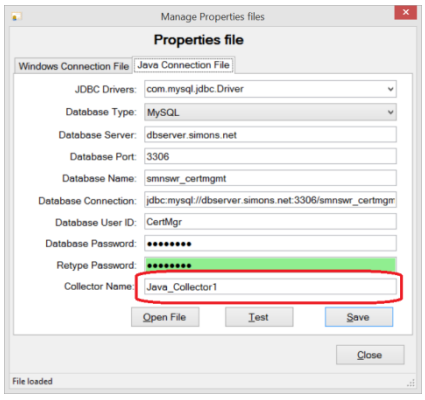

The following describes all the fields on this form.




The list on the left side of the window shows the collectors and the number of jobs assigned to that collector.

Server – This is the name of the server the collector is running on. The collector will automatically set this to the name of the server it is running on.

Collector Name – For the Windows Collector, this is the name you entered when you installed the collector. For Java Collector, this is the name you set in the Manage Properties files form under the *Java Connection File* tab.




Server-Collector – This value is automatically set based on the Server and Collector Name values provided

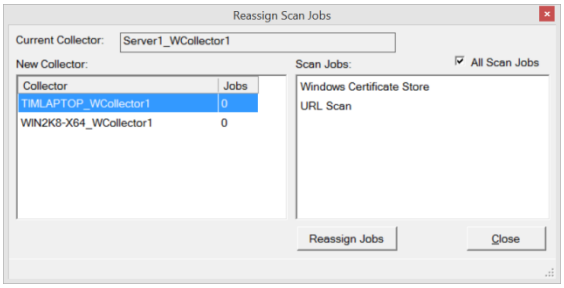
Collector Type – Specifies the type of collector this is, Windows Service or Java. This is used to determine which collectors to display on the Scan Jobs form when you select the Scan Type.

There are two actions you can perform on this screen: Reassign Scan Jobs, Delete Collectors

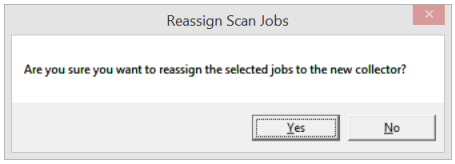
## Reassign Scan Jobs

You cannot delete a collector with jobs assigned. You must first reassign its jobs to a new collector.

1. Select the collector whose jobs you want to reassign
2. Click the *Reassign Jobs* button. You will see the *Reassign Scan Jobs* screen



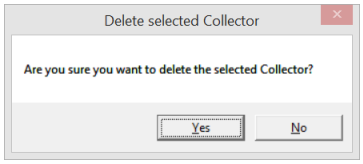

3. On the left side of the screen, select the new collector for the jobs
4. By default, the *All Scan Jobs* checkbox is checked (upper right side of the screen). If you uncheck this box, you can select individual jobs to reassign to the new collector. Once you have made your choices, click the *Reassign Jobs* button.
5. You will be prompted to confirm the reassignment, click *Yes* to reassign the jobs




6. Click *Close*

## Delete Collectors

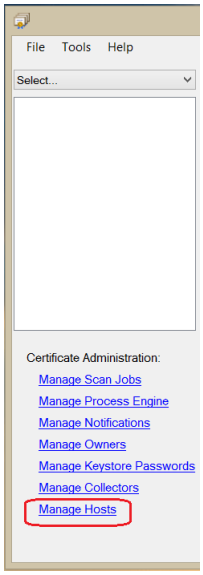
1. Select a collector with no jobs assigned; the Delete button will be enabled.
2. Click the *Delete* button to delete the collector
3. You will be prompted to confirm the deletion



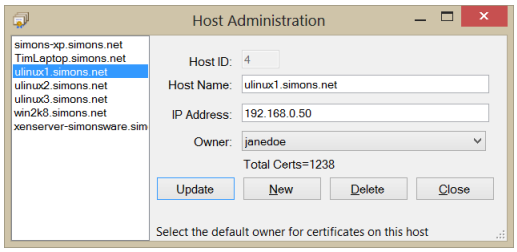

4. Click *Yes* to delete the collector

### *Manage Hosts*

Use the *Manage Hosts* link to manage host systems in SSL Certificate Management. Hosts are automatically created during a scan job execution.




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




2) Select the host you wish to manage, or enter a name for a new host
3) Enter the IP Address for the host
4) (Optional) Enter an owner for this host.

**If you enter an owner name for the host, all certificates discovered on this host will be assigned this owner. Setting the owner here overrides the Collector and Scan job owner entries.**

**Selecting a host from the list will also show the total number of certificates associated to that host.**

## Log Settings

### *Windows programs*

The Windows programs (Certificate Management UI, Windows Collector, Process Engine) 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.

There are two log files in each folder, CMGTLog4Net.log, CMPropertyLog4Net.log. **CMGTLog4Net.log** logs all activity for the main programs (Certificate Management UI, Windows Collector, Process Engine) and **CMPropertyLog4Net.log** logs all activity for the Property Files management program.


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

```
<logger name="CertMgmt">
  <level value="DEBUG" />
  <appender-ref ref="CertAppender" />
</logger>
```

### *Java Collector*

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.


**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**

# 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