IBM Security and Compliance Tools for IBM i
Certificate Expiration Manager Utility

User's Guide

IBM Systems Lab Services & Training
Thomas Barlen

Version 1.4.3

Table of Contents

1.0 Introduction....3
1.1 Change History....4
Version 1.0....4
Version 1.1....4
Version 1.2....4
Version 1.3....4
Version 1.4....4
Version 1.4.1....5
Version 1.4.2....5
Version 1.4.3....5
2.0 Implementation and use....6
2.1 Prerequisites....6
2.2 Installation....7
2.3 Using the Certificate Expiration Manager utility....9
2.3.1 Running the utility in graphics mode....9
2.3.1.1 Network Service configuration....11
2.3.1.2 IBM i certificate store setup....14
2.3.1.2.1 Adding a custom IBM i certificate store....16
2.3.1.3 Certificate expiration notification setup....18
2.3.1.4 Logging options....24
2.3.1.5 Running the SSL/TLS certificate expiration check....25
2.3.2 Running the utility in batch mode....27
2.3.2.1 Configuration....28
2.4 Expiration check result codes....28
2.5 Maintaining the default certificate key database....30
2.5.1 Displaying trusted CA certificates....31
2.5.2 Importing a CA certificate....31
2.5.3 Using your custom CA trust store file with CEM....32

1.0 Introduction

Network data encryption is an important service to protect sensitive and confidential information that traverse the Internet or corporate intranets. Many services, such as Telnet, FTP, and REXEC, transmit all data in clear text over the network. This includes also user and password information. The same is true for Web applications. Unless network data encryption is deployed, there is always a risk of gaining unauthorized access to information and systems.

Using the Secure Sockets Layer (SSL) or its successor protocol Transport Layer Security (TLS) is one of the common technologies that are used to encrypt network traffic between clients and server applications. When a client establishes a secure connection to a server application, a SSL handshake is performed. During the handshake the server sends a server certificate to the client. This server certificate has to be assigned to each server application service, such as the Telnet server, FTP server, LDAP server, etc. Digital certificates are valid for a certain period of time. When the certificate reaches its expiration date (notAfterDate or a.k.a valid until date) secure applications typically stop accepting new client connection requests, thus making the application unavailable. In this case the certificate has to be renewed.

Unless your Certificate Authority provides a service to remind you well in advance before a certificate expires, you probably run into the problem of expired certificates and therefore loosing access to your systems.

The Certificate Expiration Manager (CEM) utility has been written to automatically check for certificates that expire within a certain period of time. If a certificate will expire, a notification will be sent to a predefined list of e-mail accounts.

Details

The CEM utility is a Java application that can either be operated in graphical or batch mode. It can run on any platform that supports Java including AIX, IBM i, Windows, Linux, etc. The easiest way to configure the utility is by using the graphical user interface (GUI). It allows you to define a list of secure application hosts and ports that should be checked for expired certificates. These application service ports have to accept SSL/TLS connections and can run on any platform. For each configured application service you can specify if a notification should be sent in case the certificate expires in the given date range. It also provides a configuration option that only applies to an IBM i environment. When run within IBM i, the utility can also check for expiring certificates in the *SYSTEM, *OBJECTSIGNING, *SIGNATUREVERIFICATION, and custom IBM i certificate stores. The date range in which a certificate is determined to expire is defined by adding a number of days to the current date (program run date). If a certificate's *notAfterDate* is between the current date and the calculated expiration checking date, the certificate is reported as a candidate for expiration.

1.1 Change History

Version 1.0

Initial version of the tool.

Version 1.1

Maintenance version to improve some debugging messages and minor issues.

Version 1.2

The following functions have been added:

- The graphical interface has been changed on the *IBM i Certificate Stores* tab to include a new section to configure custom created IBM i certificate stores. The information that needs to be configured is a description, the IFS path of the certificate store (key database), and the certificate store password.
- Added new code to store the IBM i certificate store passwords in encrypted format.
- Added code to perform the expiration checking of certificates stored in custom IBM i certificate stores.

Version 1.3

The following changes and additions have been made:

- Updates documentation with more information about tested Java environments and possible errors when a restricted Java security policy is used.

Version 1.4

The following changes and additions have been made:

- The tool has been enhanced to support reporting of certificate expiration check results to a remote syslog server. Whether syslog messages are sent can be defined globally and overridden on a per service basis. The syslog messages sent comply with the Common Event Format (CEF) and therefore can be consumed by most SIEM solutions.
- The behavior for sending certificate expiration check results via e-mail has changed. Whether notifications are sent via e-mail can now be defined globally and overridden on a per service basis. Before this change, notifications could only be sent via e-mail.
- The tool has also been tested with Java version 1.8.0 (Oracle JRE)
- A new status code and message are reported for certificates that have already expired at the time of the expiration check.
- A new enhancement has been added to support in addition to direct SSL/TLS connections the connection for explicit FTPS and SMTP with AUTH TLS / STARTTLS.

- The Certificate Expiration Manager requires now a product access code that is provided by IBM to properly function. This enhancement also allows test or trial periods for the tool.

Version 1.4.1

- Added information about using a custom CA trust store to the user's guide.

Version 1.4.2

- Documentation update.

Version 1.4.3

- Added support for TLS protocol version TLSv1.3.
- Added a Java property for the startcem script/batch file to specify the supported TLS protocols. The startcem file contains a comment section with further information.
- Replaced e-mail function to solve issue with deprecated Java function from Java version higher than 1.8. CEM version 1.4.3 has been successfully tested with OpenJDK 11.

2.0 Implementation and use

The following sections guide you through installation, configuration, and usage if the CEM utility.

2.1 Prerequisites

The utility is a Java application that has been written and tested with the following Java environments:

- IBM Corporation JDK/JRE 1.6.0
  (including the com.ibm.crypto.provider.IBMJCE security provider)
- IBM Corporation JDK/JRE 1.7.0
  (including the com.ibm.crypto.provider.IBMJCE security provider)
- Sun Microsystems Inc. (Oracle) JDK/JRE 1.6.0
  (including the com.sun.crypto.provider.SunJCE security provider)
- Oracle JDK/JRE 1.8.0
  (including the com.sun.crypto.provider.SunJCE security provider)
- <<OpenJDK 11.0.11>>
- The java executable must be in the command line path environment
- The following PTFs are required when running the utility in an IBM i operating environment:
  - SI43881 (5770-SS1 V7R1)

Note that the tool can run on any platform including AIX, IBM i, Linux, and Windows.

Important note:

The Java SDK/JRE must have an unrestricted policy deployed. That is, the security policy must allow for AES 128-bit encryption. If the wrong policy is deployed, you might receive the following error: `java.security.InvalidKeyException: Illegal key size or default parameters` or an error such as `javax.net.ssl.SSLKeyException: RSA premaster secret error`

2.2 Installation

The utility comes in a ZIP file. The ZIP file *CertificateExpirationMgrVx_x.zip* contains required Java libraries, the utility programs, a save file for IBM i, and a sample configuration file.

Extract the entire contents of the zip file to a directory of your choice.

Note that the job/process environment must be set up to use one of the supported Java versions as listed in the prerequisite section.

Installation tip for IBM i users:

You can create the necessary environment as follows:

1. Sign on to your IBM i partition and create a user profile that has at least an *ALLOBJ and *SECADM special authority.
   Example: `CRTUSRPRF USRPRF(CEM) PASSWORD(<newpwd>)`
   `TEXT('Certificate Expiration Manager functional user')`
   `SPCAUT(*ALLOBJ *SECADM)`
2. FTP the CEMVx_x.SAVF from the directory you extracted the ZIP file to to the IBM i partition into a library of your choice (i.e. QGPL)
   Example:
   ```
   bin
   quote site nam 1
   put CEMVx_x.SAVF /QSYS.LIB/QGPL.LIB/CEMVx_x.SAVF
   ```
3. Restore the content to the Integrated File System (IFS) directory that you created (i.e. /home/cem)
   `RST DEV('/QSYS.LIB/QGPL.LIB/CEMVx_x.FILE') OBJ(('/home/cem' *INCLUDE *SAME))`

Note: x_x represents the version of the tool, i.e. 1_4.

Important: The tool requires a product access code file to be installed in the directory where the CertificateExpirationMgr.jar file resides. This file contains proof that you are authorized to use the tool. Copy the file `assetpac.info` file that you received from IBM to the product directory.

The package also contains two start Scripts. For a UNIX-type operating the shell script is named startcem and for the Windows environment it is called startcem.bat.

NOTE: In a UNIX-type environment you might have to set the Execute bit for the startcem script or start the tool with the shell command, i.e. for the bash shell you would start the tool like `bash startcem`.

The start scripts take the current CLASSPATH extending it with the current directory path. That means that the Java environment libraries have to be in the current CLASSPATH. The scripts accept up to four command line parameters:

-d This option sets the debugging level for the utility. Valid values are OFF, SEVERE, WARNING, INFO, CONFIG, and FINE.
Example: -d=CONFIG

-b Runs the utility in batch mode. Unless the utility is started in an IBM i operating environment, the utility starts by default in GUI mode. The batch option is very useful when you want to perform the certificate expiration checking on a scheduled basis. The utility will always start in batch mode when running in an IBM i environment.

-f The -f option allows you to specify your own utility XML configuration file. By default the utility looks for a configuration file named HostConfig.xml. You can specify your own configuration file by adding the -f command line option.
Example: -f=myconfig.xml

If the specified configuration file does not exist, you will get a corresponding error message. In this case, you can also specify the -c option to create a new configuration file with default values.

-c The -c options can be used in combination with the -f option to create a new configuration file with default configuration values. You have to customize the configuration file according to your needs and environment. The -c option will be ignored if the configuration file name at the -f option already exists.

Tip for IBM i users

If you have multiple Java versions installed, modify the startcem script and add the supported version with the export command as shown below:

Important: If you use the EDTF command to edit the startcem script, make sure that the line end characters are set to *CRLF. This can be set via editor function key F15 option 5.

Shipped version of startcem script:

```
#!/bin/sh
echo "Starting certificate expiration manager utility"
java -classpath $CLASSPATH:. -jar CertificateExpirationMgr.jar $1 $2 $3 $4
exit 0
```

Changed version (example shows Java version 1.8.0 32-bit)

```
#!/bin/sh
echo "Starting certificate expiration manager utility"
export JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk80/32bit
java -classpath $CLASSPATH:. -jar CertificateExpirationMgr.jar $1 $2 $3 $4
exit 0
```

2.3 Using the Certificate Expiration Manager utility

The utility can be started from a command line.

2.3.1 Running the utility in graphics mode

Open a command line and change your current directory path to the directory where you extracted the utility files to.
Note: *Remember that you need a graphical subsystem in order to display the tool's GUI. For example, IBM i does not support the GUI version. It only runs in batch.*
Tip: *Even if your operating environment does not provide a graphical interface, you can still install the tool on a workstation, i.e. a Windows or Linux PC, and use the graphical interface to set up the tool and generate the required XML configuration file. This file then needs to be transferred to the IBM i environment to the directory where you installed the tool. By default, this is* `/home/cem`.

Enter the following command from the directory where you stored the tool to start it:

```
startcem
```

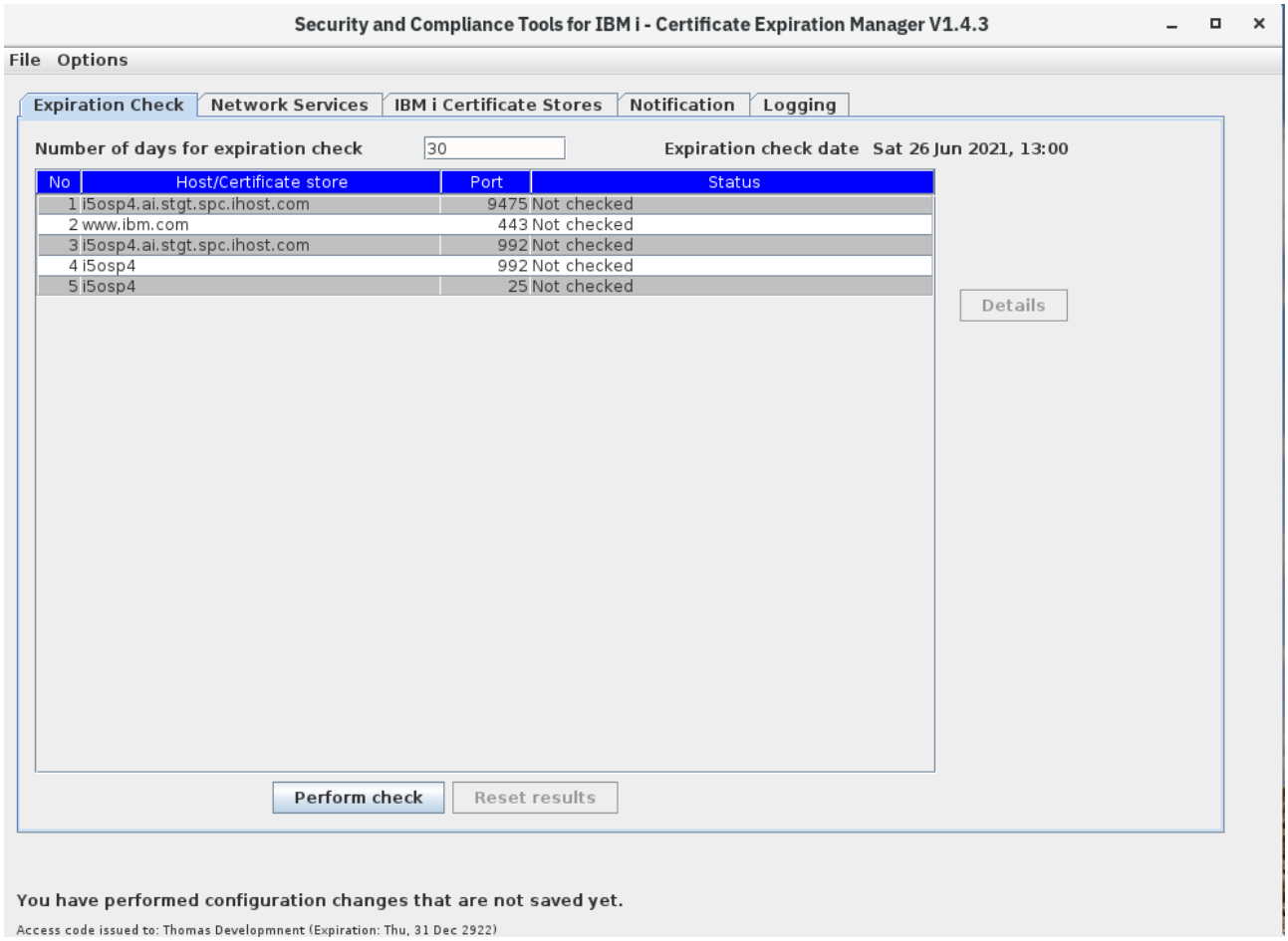

Figure 1: Expiration Check tab

Note: In a UNIX-type environment (i.e. Linux, AIX) you might need to start the utility with the comand ./startcem from the directory where you installed the tool. After the utility started you will be presented with the following screen (the listed systems vary according to your environment):

The **Options** menu option provides a checkbox that specifies if changes that you make during a session will be automatically saved when you exit the program.

The **File** menu provides options to save the configuration manually to the XML configuration file and an option to exit the program.

2.3.1.1 Network Service configuration

The Services configuration window lets you define SSL/TLS-enabled application services that should be checked for expired certificates.

From the initial window click the Network Services tab. Click **Add Service** to add a new system application service.

The input parameter window for a new systems appears:

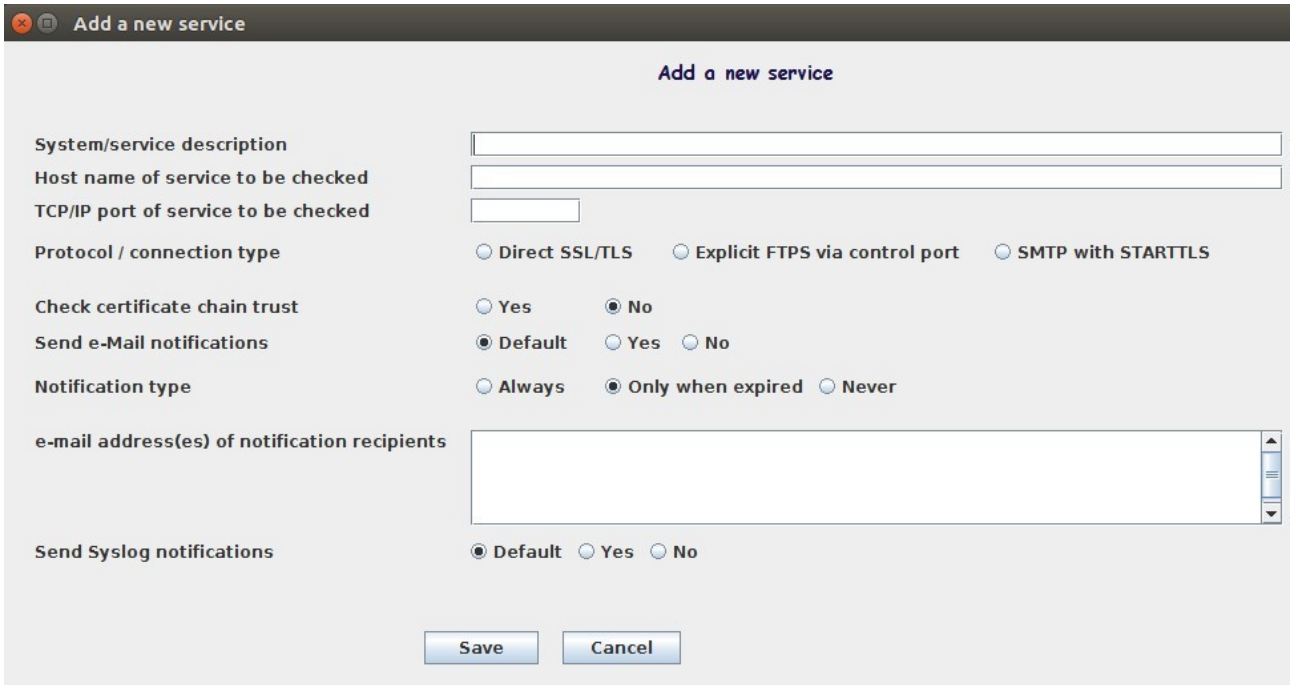

Figure 2: Adding a new network service

The definition for a new service provides the following parameters:

System/service description
This parameter specifies a meaningful description for the new application service entry.

Host name of service to be checked
Specifies the host name or IP address of the system where the application service to be checked resides.

TCP/IP port of service to be checked
Specifies the application service port of the service to be checked. For example, the default well-known port for an SSL-enabled Web server (https) is 443, for SSL Telnet 992, etc.

Protocol connection type
This parameter specifies the type of protocol the server network services uses. Depending on the chose type different handshakes are performed in order to obtain the server's certificate. Valid options are:

- **Direct SSL/TLS**
  This option requires that the port the network service listens on accepts a SSL/TLS handshake. This is the standard option as used by most network services.

- **Explicit FTPS via control port**
  FTP servers typically support implicit and explicit connection methods. Implicit means that the FTP listens for SSL/TLS connection requests on the default port 990. A direct SSL/TLS handshake is performed via this method. Using the explicit connection method, the client first establishes an unencrypted session to the FTP control port, by default 21, and then issues a AUTH TLS command to upgrade the session to a SSL/TLS encrypted session. If you want to use the explicit connection method, you have to select this option.
- **SMTP with STARTTLS**
  A SMTP server can also accept direct SSL/TLS connection requests, typically via port 465. This has been supported for quite some time and still is with many SMTP server implementations on the Internet. However, newer implementations use the standard port, i.e. 25, and establish an unencrypted session first. The SMTP server will then advertise the supported options when the client issues the EHLO command. One of the options is STARTTLS. If the server supports this option, the client can upgrade the unencrypted session to an encrypted session by issuing the STARTTLS command. If you have a SMTP server that supports the STARTTLS command, you could use this option.

Check certificate chain trust

Certificates are signed by a certificate authority (CA). During a SSL handshake, the client verifies the server certificate signature using the public key of the certificate authority that signed the server certificate. This public key is obtained from the local certificate key database. For security reasons it is always recommended to check the certificate trust. However, if the server certificate is issued by a non well-known CA, the trust check will fail and returns an error. If you do not have access to the corresponding CA certificate, you can turn off the certificate trust check by selecting No for this parameter. For information about importing a CA certificate into the default Java key database, refer to 2.5 Maintaining the default certificate key database on page 30.

Send e-Mail notifications

This configuration option determines if e-mail notifications will be sent for a given service. Note that the configuration option Notification type also determines when a notification is sent.
The available options are:

- **Default**
  This option specifies that the expiration manager tool determine whether to send certificate expiration notifications by the setting on the Notification tab. If the notification tab specifies Enabled, notifications will be sent otherwise not.
- **Yes**
  If this option is selected, e-Mail notifications are sent regardless of the tool-wide setting on the Notification tab.
- **No**
  If this option is selected, *no* e-Mail notifications are sent regardless of the tool-wide setting on the Notification tab.

Notification type

This configuration option determines under which circumstances a notification is sent for a given service. The first option ***Always*** specifies that a notifiassetcation will be sent every time an expiration check is performed, no matter what the check result is. If you select ***Only when expired***, a notification will only be sent to the specified recipients when the certificate expires before the expiration check date. If the certificate expires after the check date or any other error occurred during the check, you will not get a notification. When you select the last option ***Never***, the utility will never send a notification. You will only see the check results in the GUI window and, if enabled, in the log file. This configuration option applies to e-mail and syslog notifications.

e-mail address(es) of notification recipients

Specifies a single or multiple e-mail addresses of recipients that will receive notification mails. The e-mail address has to comply with the address format as defined in RFC822. If multiple recipients are specified, each address has to be separated by a comma (,).
Examples: “yourname@domain.com” or “Your Name<yourname@domain.com>”

Send Syslog notifications

This configuration option determines if Syslog notifications will be sent for a given service. Note that the configuration option Notification type also determines when a notification is sent.
The available options are:

- **Default**
  This option specifies that the expiration manager tool determines whether to send certificate expiration notifications by the setting on the Notification tab. If the notification tab specifies Enabled, notifications will be sent otherwise not.
- **Yes**
  If this option is selected, Syslog notifications are sent regardless of the tool-wide setting on the Notification tab.
- **No**
  If this option is selected, *no* Syslog notifications are sent regardless of the tool-wide setting on the Notification tab.

When finished click **Save** to add the new service entry to the list of services to be checked.

By selecting an existing item in the list of configured services, you can change an existing service or delete it.

2.3.1.2 IBM i certificate store setup

When run in an IBM i operating environment, the Certificate Expiration Manager can also check for expiring certificates in the following IBM i certificate stores.

Important: To be able for CEM to verify the expiration of certificates in local key databases, the user profile that runs the tool must have at least the *ALLOBJ and *SECADM special authorities.

- *SYSTEM store
  Used to store CA certificates and server/client certificates that are used for SSL/TLS enabled services and VPN connections that use RSA authentication.
- *OBJECTSIGNING store
  This store is not widely in use today. The store can contain object certificates and their CA certificates that are used for signing IBM i objects, such as programs, modules, service programs, commands, save files, etc.
- *SIGNATUREVERIFICATION store
  The third standard certificate store is used to hold certificates that are used to verify object signatures that were created on the same or another IBM i system using certificates from the object signing store.
- Custom IBM i certificate stores
  You can also add user defined IBM i certificate stores (also known as key databases) to the expiration checking configuration. The certificate stores must exist in the Integrated File System (IFS) in IBM i.

The IBM i certificate store expiration checking only works when the Certificate Expiration Manager runs within an IBM i system. When run on a system other than IBM i, the settings on the IBM i Certificate Stores tab are ignored.

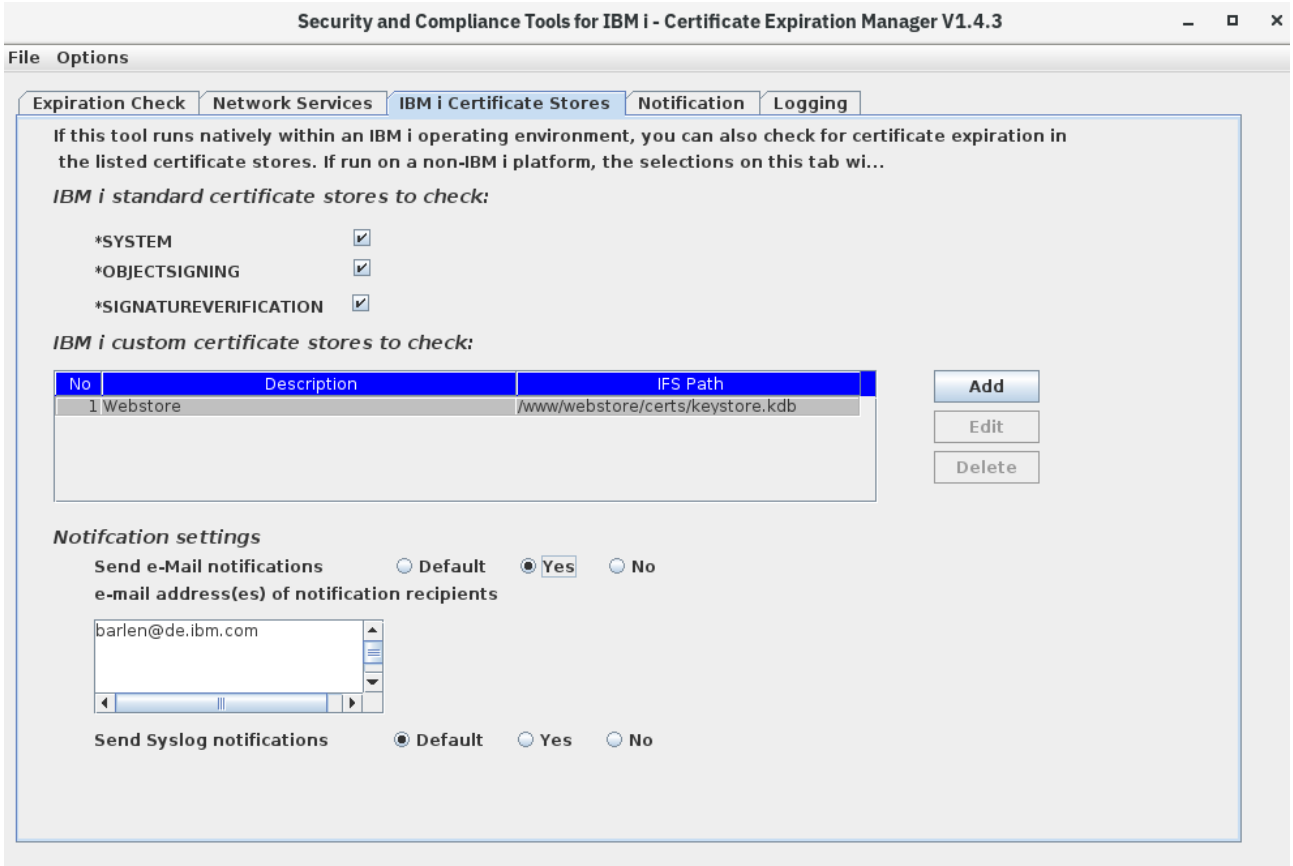

Figure 3: IBM i Certificate Stores tab

To configure the IBM i certificate expiration checking settings, click the IBM i Certificate Stores tab.

The IBM i certificate store settings are as follows:

IBM i standard certificate stores to check
This options lets you select the standard IBM i certificate stores that should be checked for expired certificates.

IBM i custom certificate stores to check
The section lists the custom certificate stores to be checked for expiring certificates. It also provided buttons to add, edit, and delete custom IBM i certificate store entries.

Send e-Mail notifications
This configuration option determines if e-mail notifications will be sent for expiring or already expired certificates. The option applies to all standard system and custom certificate stores.
Note that the configuration option Notification type also determines when a notification is sent.
The available options are:

- **Default**
  This option specifies that the expiration manager tool determine whether to send certificate expiration notifications by the setting on the Notification tab. If the notification tab specifies Enabled, notifications will be sent otherwise not.

- **Yes**
  If this option is selected, e-Mail notifications are sent regardless of the tool-wide setting on the Notification tab.
- **No**
  If this option is selected, *no* e-Mail notifications are sent regardless of the tool-wide setting on the Notification tab.

e-mail address(es) of notification recipients
Specifies a single or multiple e-mail addresses of recipients that will receive notification mails. The e-mail address has to comply with the address format as defined in RFC822. If multiple recipients are specified, each address has to be separated by a comma (,).
Examples: “yourname@domain.com” or “Your Name<yourname@domain.com>”

Send Syslog notifications
This configuration option determines if Syslog notifications will be sent for expiring or already expired certificates. The option applies to all standard system and custom certificate stores.
Note that the configuration option Notification type also determines when a notification is sent.
The available options are:

- **Default**
  This option specifies that the expiration manager tool determine whether to send certificate expiration notifications by the setting on the Notification tab. If the notification tab specifies Enabled, notifications will be sent otherwise not.
- **Yes**
  If this option is selected, Syslog notifications are sent regardless of the tool-wide setting on the Notification tab.
- **No**
  If this option is selected, *no* Syslog notifications are sent regardless of the tool-wide setting on the Notification tab.

2.3.1.2.1 Adding a custom IBM i certificate store

Checking for certificate expiration in custom IBM i certificate stores has been added with V1.2 of the Certificate Expiration Manager (CEM). The IBM i Certificate Stores tab contains the store entries to be checked. Perform the following steps to add a new customer IBM i certificate store.

1. In the *IBM i custom certificate stores to check* section, click **Add**.

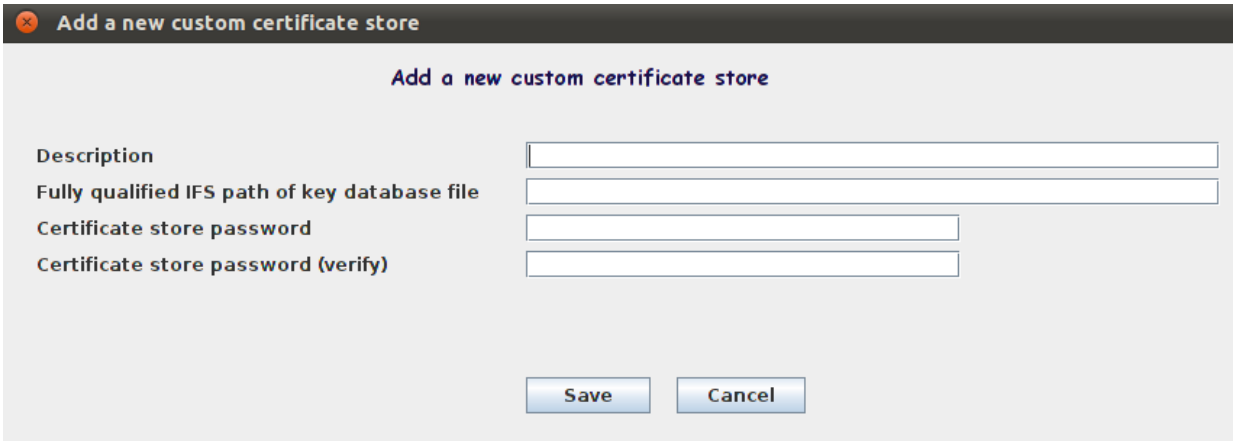

Illustration 4: Adding a custom IBM i certificate store

You need to enter information for the shown parameters:

Description:

Provide a meaningful description of the certificate store.

Fully qualified IFS path of key database file:

Enter a fully qualified path and file name of the custom IBM i certificate store. The store must exist in the Integrated File System (IFS) in IBM i. The value must contain the file name including extension. The standard extension for a certificate store is .KDB.

Example: `/security/certstores/webserver.kdb`

Certificate store password:

Enter the certificate store password that is used to encrypt the store. This password has been specified when the store was created. It is the same password as the one you have to enter when opening the store via the IBM i Digital Certificate Manager.

Certificate store password (verify):

Repeat the password from the previous field. This parameter is just for verification purposes.

Note: The password will be stored in encrypted format in the XML configuration file.

2. Click **Save** to save the settings.

2.3.1.3 Certificate expiration notification setup

The Notification tab of the graphical interface specifies the information needed for the CEM utility to send notifications about expiration check results.

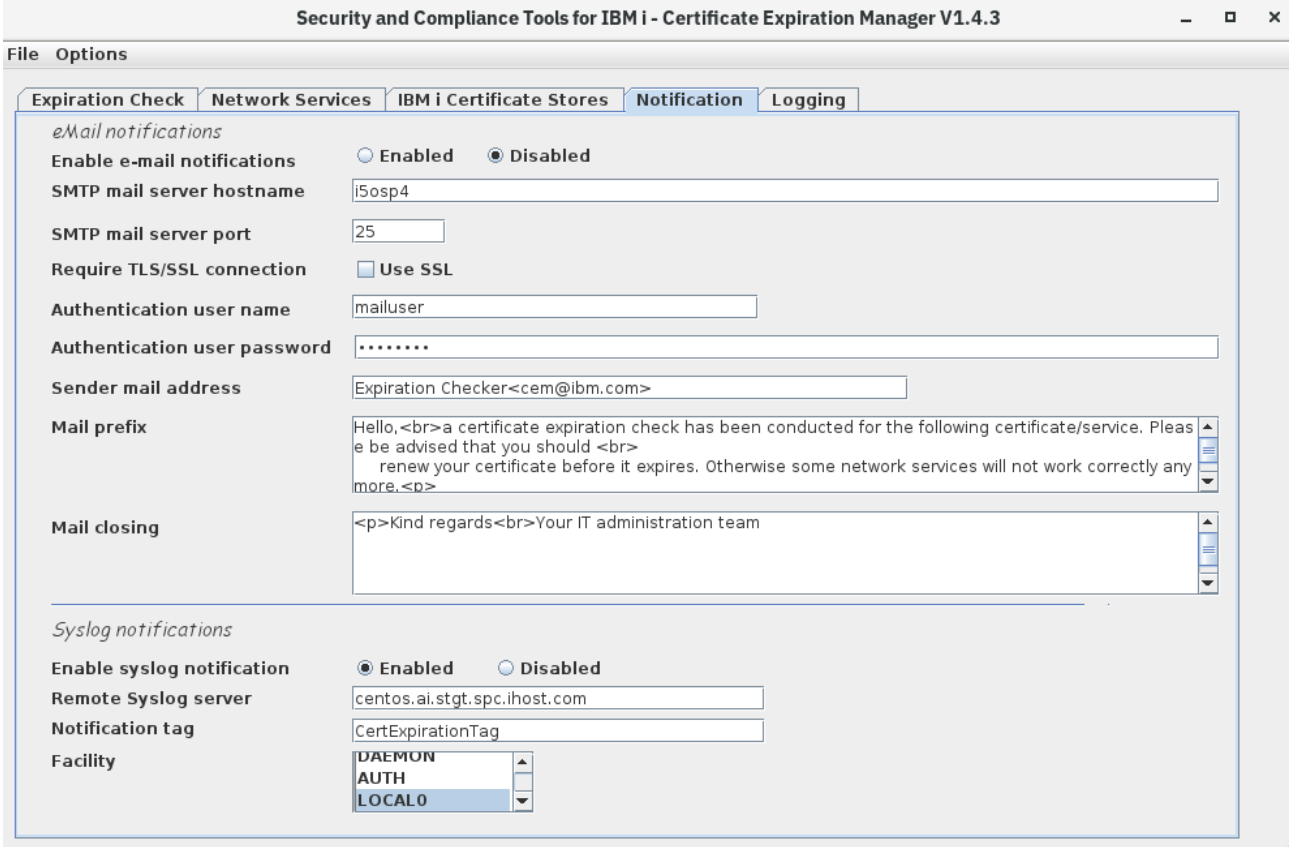

Figure 4: Notification tab

The available parameters are as follows:

Section *eMail notifications*

Enable e-Mail notifications

This configuration options specifies whether e-Mail notifications are enabled on a global basis. When enabled, for every network service or for IBM i certificate stores where the Send e-Mail notifications options is set to Default, a notification is sent. Note that you can always override the global setting on a network service or IBM i certificate store basis.>>

SMTP mail server hostname

Specifies the host name or IP address of the system that hosts the SMTP server that will be used to process outgoing mail notifications. Typically you already have an SMTP gateway installed in your network. Ask your helpdesk or mail administrator for the correct address.

Tip for users that want to create their own SMTP server environment:
In case you want to set up your own SMTP server for outbound mail relay processing, you need to make sure that the SMTP server allows relaying of e-mail from the IP address where the Certificate Expiration Manager tool runs on.

SMTP mail server port

Specifies the TCP/IP port number the SMTP server listens on. The well-known port for SMTP servers is 25.

Require SSL/TLS connection

Determines if the connection from the CEM utility to the SMTP mail server should be protected via an SSL/TLS connection. Note that the certificate authority that signed the SMTP server certificate must be in the list of trusted CAs on the system the utility runs (Java certificate key database).

Authentication user name (optional)

If the SMTP server (relay) requires authentication, enter a user name that is authorized to process outgoing mail through the SMTP mail server. As soon as a user name is entered in this parameter, the CEM utility tries to authenticate to the SMTP server when establishing a session. Leave this parameter empty if you do not want authentication.
Note: If the send mail process fails despite a valid user name and password, also select *Require SSL/TLS connection*. Many SMTP servers require a secure connection when authentication is used.
Note: This parameter only needs to be specified when the mail relay/gateway requires authentication.

Authentication user password (optional)

Enter the password of the user name that was entered in the Authentication user name parameter.
Note: This parameter only needs to be specified when the mail relay/gateway requires authentication.

Sender mail address

Specifies the e-mail address in RFC822 compliant format of the sender. Recipient of e-mail notifications will see this address as the sender address.

Mail prefix

The notification e-mail contains a fixed part that cannot be changed and a variable part that you can customize according to your needs. The mail prefix will be the text that will be added to the e-mail before the fixed part. The fixed part contains information about the checked certificates and results. e-mail notifications will be send as messages in HTML format. Therefore you have to enter your text including HTML tags in case you want to format your mail text.

Mail closing

Similar to the mail prefix, the mail closing is a variable text that you can customize. It will be added after the fixed part of the mail. Enter HTML tags for formatting.

Following is an example of a notification mail:

>>>>>>> Begin of mail <<<<<<<<

Hello,
a certificate expiration check has been conducted for the following network service. Please be advised that you should renew your certificate before it expires. Otherwise some network services will not work correctly anymore.

Host description:	IBM Web Server
Host address/name:	www.ibm.com
Service port:	443
Certificate subject DN:	CN=www.ibm.com, O=IBM, L=RESEARCH TRIANGLE PARK, ST=North Carolina, C=US, SERIALNUMBER=0JE6MMbOidGUm0VPK9K9ut6YhGwWp2SM
Certificate issuer DN:	OU=Equifax Secure Certificate Authority, O=Equifax, C=US
Certificate serial:	1258806
Certificate trust chain checked:	No
Certificate valid from:	Wed, 2 Jun 2016 21:55:32 +0200
Certificate valid until:	Fri, 5 Aug 2017 17:08:36 +0200
Expiration checking date:	Sat, 18 Dec 2016 09:31:31 +0100 (calculated by adding 130 to current date)
Expiration check results:	**Certificate still valid (0)**

Kind regards
Your IT administration team

>>>>>>>> End of mail <<<<<<<<<<

Section *Syslog notifications*

The certificate expiration manager sends syslog notifications over protocol UDP to the syslog server port 514.

Enable syslog notifications

This configuration options specifies whether syslog notifications are enabled on a global basis. When enabled, for every network service or for IBM i certificate stores where the Send Syslog notifications options is set to Default, a notification is sent. Note that you can always override the global setting on a network service or IBM i certificate store basis.

Remote syslog server

Enter the hostname or IP address of the syslog server that should receive certificate expiration notifications.
Important: Leave the remote syslog server parameter empty if you do not use syslog event reporting.

Notification tag

A syslog message can contain a tag. This tag is added as a prefix to the Syslog message data. For example, a tag can be used for filtering purposes on a central Syslog server.
Example:

```
Feb 14 16:00:09 i5osp4 auth|security:warn|warning
CertExpirationTag: CERT_WILL_EXPIRE::IBMi_system …..
```

Facility

This configuration options specifies the syslog facility that is used when sending syslog notifications to the syslog server. The supported syslog facilities in the tool are:

- USER
- DAEMON
- AUTH
- LOCAL1
- LOCAL2
- LOCAL3
- LOCAL4
- LOCAL5
- LOCAL6
- LOCAL7

Syslog messages are sent with three different priorities:

- **ALERT**
  This priority is used for notifications that report an already expired certificate at the time the tool was run.
- **WARN**
  This priority is used for notifications that report a certificate that expires between the time the tool was run and the expiration check date.
- **INFO**
  This priority is used for notifications that report a certificate whose expiration date (NotAfter attribute of the certificate) is after the expiration check date.

Each element of information that is sent to the syslog server is separated two colons (::).

Syslog message examples:

Example 1: Syslog notification for a certificate in the IBM i *SYSTEM certificate store that is already expired.

```
Apr 21 15:16:26 mailrelay.ai.stgt.spc.ihost.com local0:alert
   CertExpirationTag: CEF:0|IBM|CERTEXPMGR|1.4|100|
   CertificateExpirationCheck|10|result=CERT_ALREADY_EXPIRED
   IBMi_system_name=I5OSP4 Host_serial_number=102F5FV
   IBMi_CertStore=*SYSTEM Cert_Label=ThomasSSLCertFeb2017
   SubjectDN=CN\=i5osp4,OU\=Lab Services,O\=IBM,L\
   =Kelsterbach,ST\=Hessen,C\=DE IssuerDN=CN\
   =i5osp4.ai.stgt.spc.ihost.com_CERTIFICATE_AUTHORITY,OU\=,O\
   =IBM Web Administration for i,L\=,ST\=Any,C\=DE
   Cert_Serial=589DB3EC09B8D8 Key_Size=4096
   Private_Key_Info=Private key is available (1)
   NotAfterDate=Sat Feb 11 13:37:00 CET 2017 ExpCheckDate=Tue
   Jun 20 15:16:25 CEST 2017 Result_text=The certificate already
   expired(2)
```

Example 2: Syslog notification for a certificate that has been retrieved via a network connection that will expire within the expiration check date period.

```
Apr 21 17:11:51 ::ffff:172.17.8.120 local0:warn|warning
   CertExpirationTag: CEF:0|IBM|CERTEXPMGR|1.4|100|
   CertificateExpirationCheck|7|result=CERT_WILL_EXPIRE
   Service_name=Our secure Telnet server
   Host_name=i5osp4.ai.stgt.spc.ihost.com Port=992 SubjectDN=CN\
   =i5osp4.ai.stgt.spc.ihost.com, OU\=AI, O\=IBM, L\=Ehningen,
   ST\=Baden-Wuerttemberg, C\=DE IssuerDN=CN\
   =i5osp4.ai.stgt.spc.ihost.com_CERTIFICATE_AUTHORITY, O\=IBM
   Web Administration for i, ST\=Any, C\=DE
   Cert_Serial=24859050525237456 NotAfterDate=Thu Dec 14
   12:27:56 CET 2017 ExpCheckDate=Sun Dec 17 17:11:51 CET 2017
   Result_text=Certificate will expire before check date(1)
```

Example 3: Syslog notification for a certificate that has been retrieved via a network connection that is valid past the expiration check date period. This message gets only reported when you select Always for the notification type.

```
 Apr 21 15:16:21 mailrelay.ai.stgt.spc.ihost.com local0:info
   CertExpirationTag: CEF:0|IBM|CERTEXPMGR|1.4|100|
   CertificateExpirationCheck|1|result=CERT_OK Service_name=IBM i
   Signon Server Host_name=i5osp4.ai.stgt.spc.ihost.com
   Port=9475 SubjectDN=CN\=i5osp4.ai.stgt.spc.ihost.com, OU\=AI,
   O\=IBM, L\=Ehningen, ST\=Baden-Wuerttemberg, C\=DE
```

```
IssuerDN=CN\
=i5osp4.ai.stgt.spc.ihost.com_CERTIFICATE_AUTHORITY, O\=IBM
Web Administration for i, ST\=Any, C\=DE
Cert_Serial=24859050525237456 NotAfterDate=Thu Dec 14
12:27:56 CET 2017 ExpCheckDate=Tue Jun 20 15:16:19 CEST 2017
Result_text=Certificate still valid(0)
```

2.3.1.4 Logging options

The Certificate Expiration Manager utility provides logging functions for the following two options:

1. The utility can maintain a log file that contains an entry for every expiration check that was performed. New results will be appended to the existing log. No log maintenance will be performed.
2. In case you experience problems, i.e. no mail is sent, you can turn on debugging. Depending on the chosen debug level the debug output can be more or less verbose. Note that every time the CEM utility is started the existing log file will be overridden.

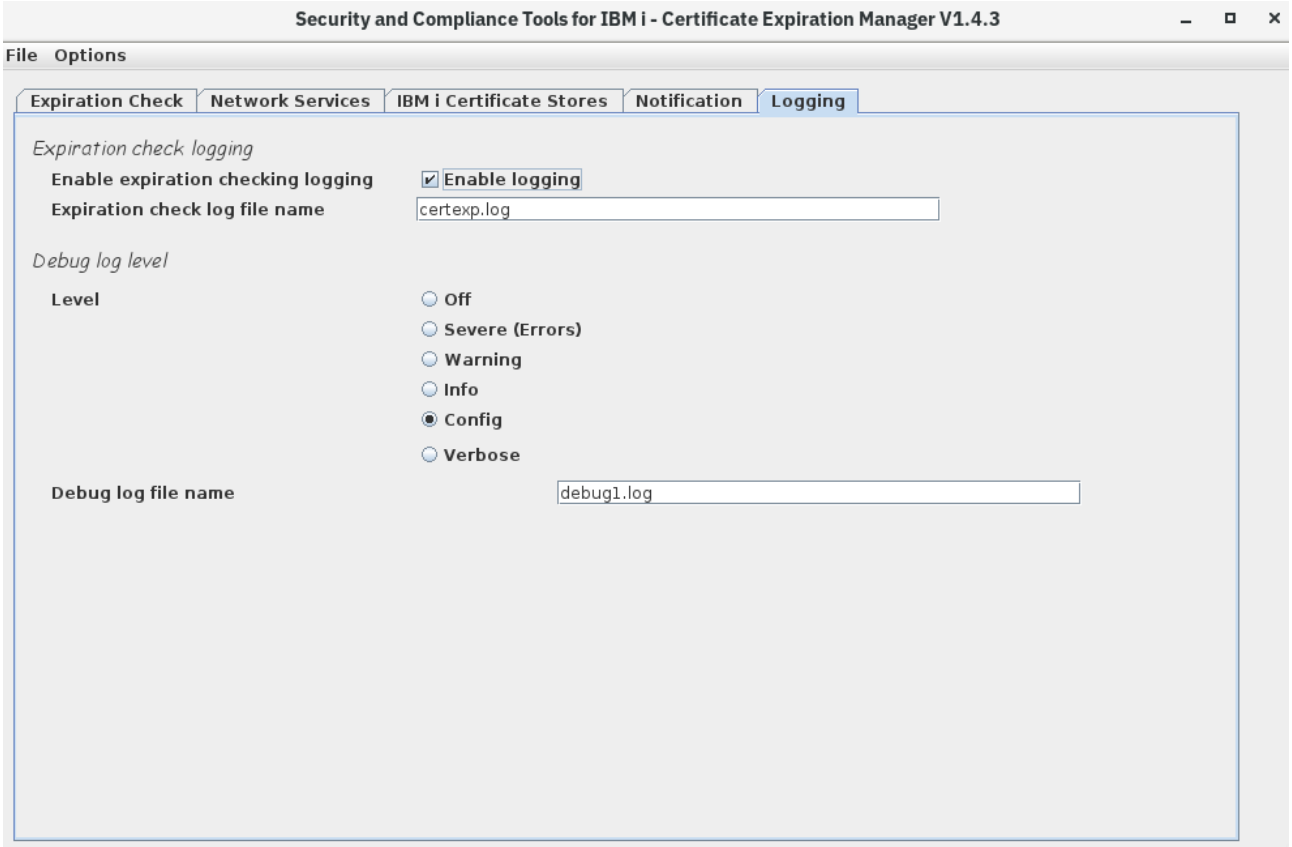

Figure 5: Logging tab

To set up the logging options click the Logging tab in the utility's graphical user interface.

The following parameters can be specified:

Enable expiration checking log
If checked, the utility maintains a log file and adds an entry for each performed expiration check.

Expiration check log file name
Specifies the name of the log file. If no pathname is specified, the log will be created in the program directory. The directory path has to exist if you specify a path for the log file.

Level
Determines the level of details that will be written to the debug log file. The recommended

value is Severe (Errors). In case you experience problems you might want to select a more comprehensive log option.

Debug log file name
Specifies the name of the debug log file. If no pathname is specified, the log will be created in the program directory. The directory path has to exist if you specify a path for the log file.

2.3.1.5 Running the SSL/TLS certificate expiration check

Performing the certificate expiration check is very easy.

1. You just need to start the utility. The Expiration Check tab is displayed.

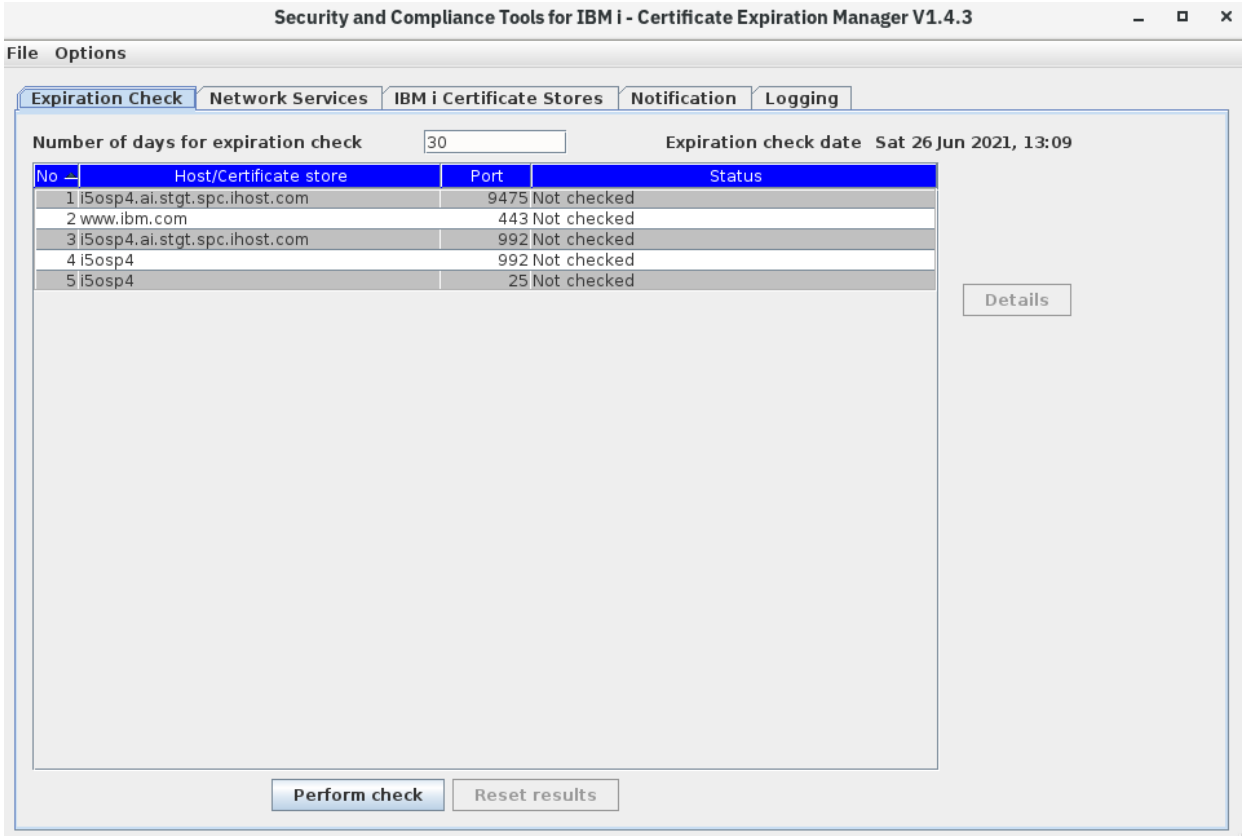

Figure 6: Expiration Check tab

2. If necessary change the number of days for the expiration check. The specified number of days will be added to the current date. The result will be the expiration check date as shown on the Expiration Check tab. All certificates that expire before the expiration check date will be reported as “Certificate expires before check date”.
3. When you are ready to perform the expiration check, click **Perform check**. The status field will update for each check that is performed. The check that is currently performed is marked as `>>> Checking <<<`.

   The results are displayed once the checking process is finished.

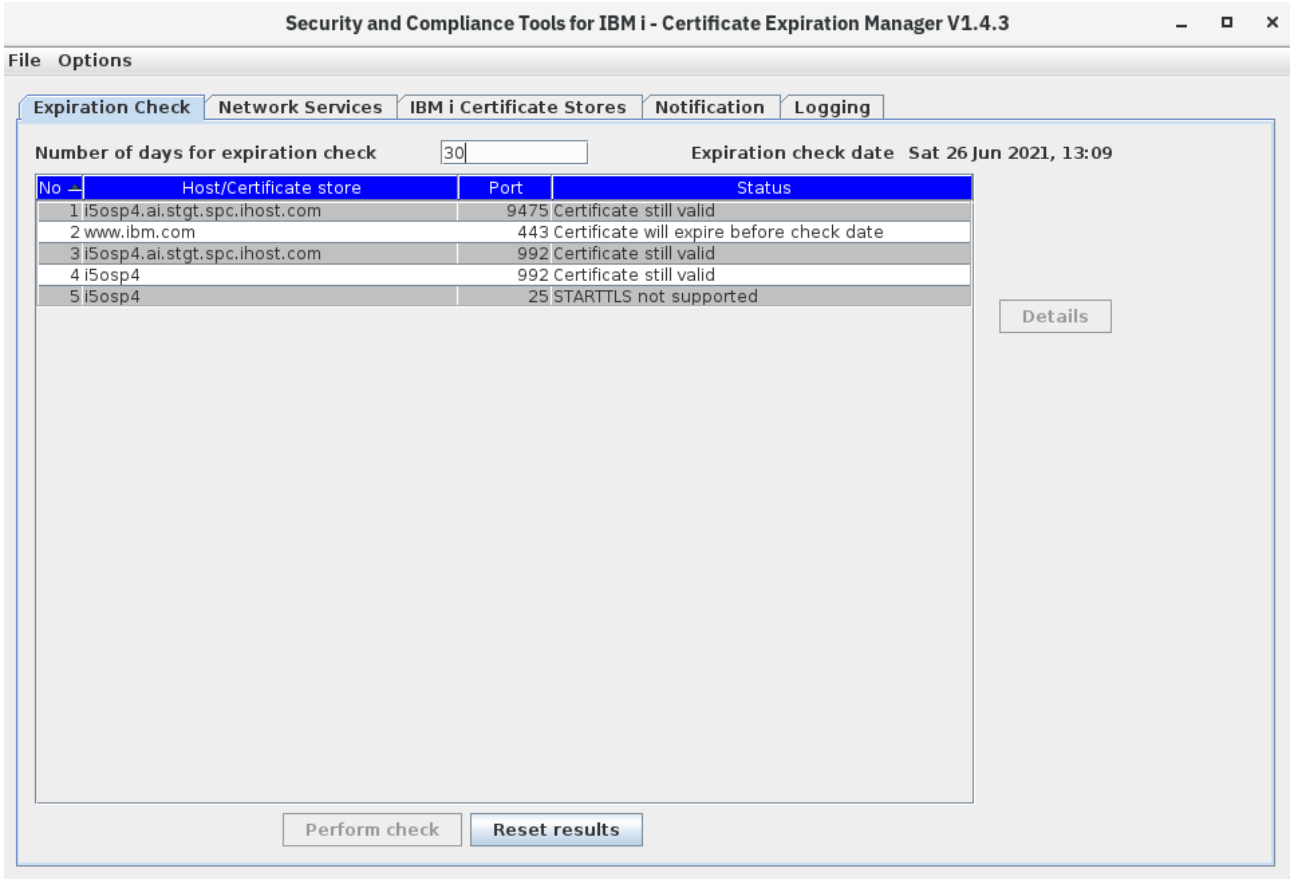

Figure 7: Checking results

4. When all registered services are checked, you can select an individual entry and click **Details** to get more information about the expired certificate.

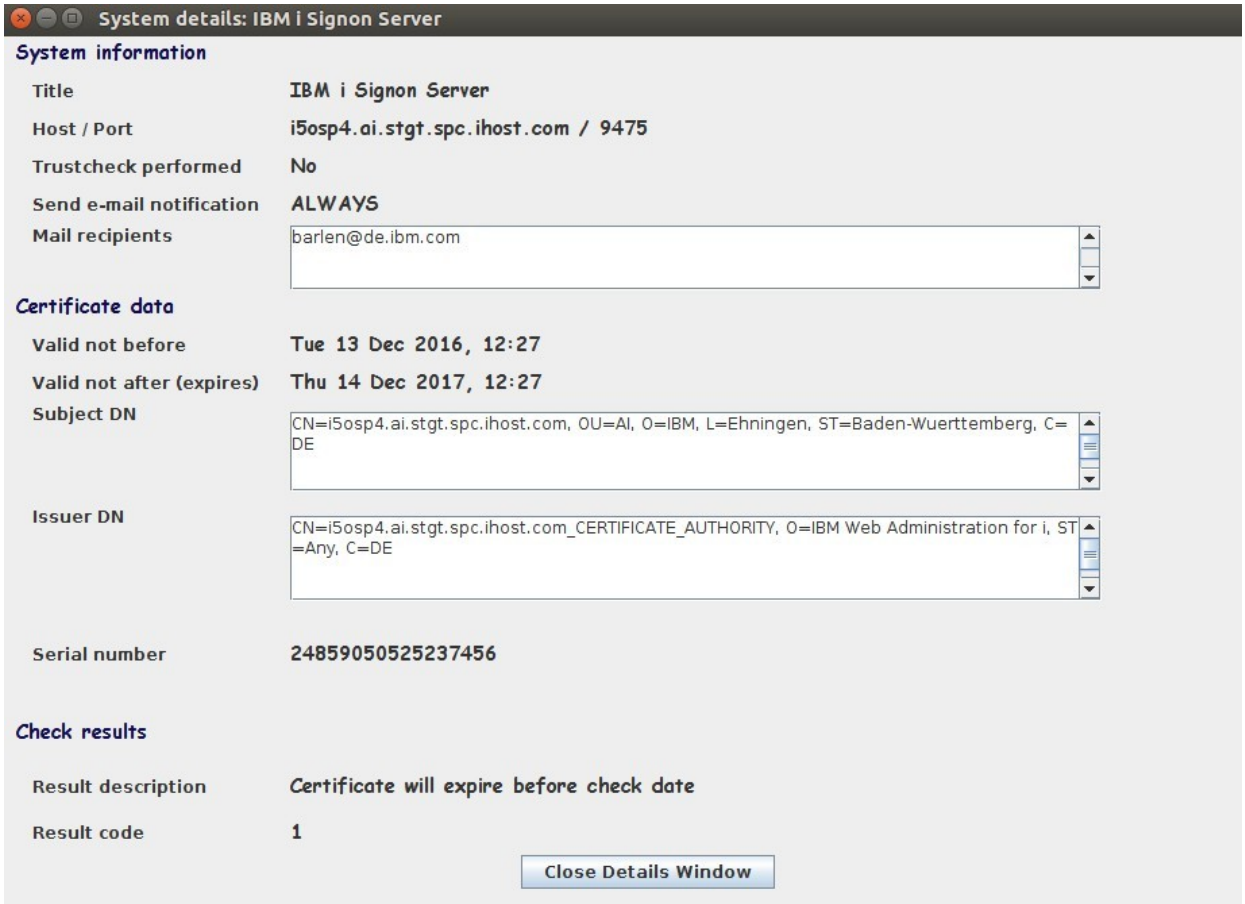

Figure 8: Details window

5. Click **Close Details Window**.
6. If you want to rerun the expiration check, click **Reset results** and then **Perform check** again.

2.3.2 Running the utility in batch mode

Open a command line and change your current directory path to the directory where you extracted the utility files to.

Enter the following command from the directory where you stored the code to start the tool:

```
startcem -b
```

Tip for UNIX-type users: In a UNIX-type environment (i.e. Linux, AIX) you might need to start the utility with the comand ./startcem. You can use cron to schedule the check on a regular basis.
You may need to change the startcem script to add a “cd” command to change to the directory whee you stored the code.

Tip for IBM i users: Assuming that you followed the setup instructions in 2.2 Installation on page 7, you can schedule the certificate expiration check by using the IBM i job scheduler:
Example (running the job every Monday and Thursday at 22:00:00):

```
ADDJOBSCDE JOB(CEM) CMD(QSH CMD('/home/cem/startcem')) FRQ(*WEEKLY)
SCDDATE(*NONE) SCDDAY(*MON *THU) SCDTIME(220000) USER(CEM) TEXT('Perform
```

```
certificate expiration checking')
```

The utility starts and performs the certificate expiration checking process for all application services that are configured in the XML configuration file. If run in an IBM i environment, the utility can also check for expiring certificates in the *SYSTEM, *OBJECTSIGNING, and *SIGNATUREVERIFICATION certificate store.

2.3.2.1 Configuration

It is strongly recommended to use the GUI mode to configure the utility. If you do not have access to a graphical environment, you can edit the HostConfig.xml file with an editor. The XML configuration file contains comments that explain each parameter.

NOTE 1: If you manually add custom IBM i certificate stores via the XML configuration file, the certificate store password must be specified. You need to enter the password in clear text and then run the Certificate Expiration Manager (CEM) once. When CEM detects a clear text password, it will encrypt the password and stores it encrypted in the XML configuration file.

NOTE 2: If you decide to perform the configuration through editing the configuration file keep in mind that any additional comments or elements that are not part of the standard file will be removed by the tool.

2.4 Expiration check result codes

The Certificate Expiration Checking utility handles common errors that can occur during an expiration checking process. For example, a configured service is not started. In this case, the target host will refuse the connection request. The following errors are common errors or normal checking results:

Result code	Result description	Comment
0	Certificate still valid	The certificate does not expire before the expiration check date. No further action is required.
1	Certificate expires before check date	The expiration check process has determined that the checked certificate expires before the expiration check date. Depending on the chosen check date, you might need to renew the certificate immediately. If you configured mail notifications to be sent, the subject line of the e-mail contains the words *** ACTION REQUIRED *** The syslog message contains at the beginning of the message the term **CERT_WILL_EXPIRE.**
2	Certificate has already expired	The expiration check process has determined that the checked certificate already expired at the time the check was performed. The certificate must be renewed immediately. In case

Result code	Result description	Comment
		of an IBM i certificate store the certificate could also be an unsed one. In this case you should cleanup the store to get rid of expired certificates. If you configured mail notifications to be sent, the subject line of the e-mail contains the words *** ACTION REQUIRED ***. The syslog message contains at the beginning of the message the term **`CERT_ALREADY_EXPIRED.`**
10	Connection refused	This error typically occurs when the target service is not started or a wrong port has been specified.
11	Certificate not trusted	The error indicates that you specified in the configuration for this service that the certificate trust chain should be checked. However, the server certificate that was received during the SSL handshake was issued by a certificate authority that Java does not trust. If you want Java to trust the issuer of the certificate, you need to add the issuer's CA certificate to the Java trusted key store (see 2.5 Maintaining the default certificate key database on page 30).
12	Unknown host	This is a typical error when the specified host name cannot be resolved to an IP address. Check the spelling of the host name.
13	Remote host closed connection during handshake	This error indicates that the remote system that hosts the service to be checked close the connection during the SSL handshake. Check that the remote host and port represent an SSL enabled service. Contact the administrator of the remote system to determine the cause of the problem.

Result code	Result description	Comment
14	Unrecognized SSL msg (plain text connection?)	This message might be shown when the service only supports clear text connections. If you want to check a FTP server, this error typically indicates that an explicit SSL FTP session has been established to port 21. This session type does not support an initial SSL handshake.
15	STARTTLS not supported	The network service has been configured to upgrade the SMTP session to an encrypted session with the STARTTLS command. However, the SMTP server does not support the STARTTLS command.
16	Explicit FTPS not supported	The network service has been configured to upgrade the FTP session via the control port to an encrypted session with the AUTH TLS command. However, the FTP server does not support the AUTH TLS command.
99	Unknown error	The checking utility received an error that is different from the previous error codes. Turn on verbose logging to find out what the problem is.

Table 1 Common error and result codes

2.5 Maintaining the default certificate key database

It is always recommended to check the certificate trust when performing a certificate expiration check. Whether a trust check is performed is specified in each individual service configuration. The corresponding parameter is called Check certificate chain trust (XML element <TrustCheck>).

NOTE: The certificate key database and therefore also the certificate trust status is not checked when checking the certificate expiration for an IBM i certificate store. In this case, the trust was already checked when a certificate was created or imported.

If you configured the service to check the certificate chain trust and you received error code 11 (Certificate not trusted), you have two options. The first one is to change the trust check option to No or to import the certificate's issuer CA certificate.

In Java, trusted CA certificates are stored by default in a file named *cacerts*. This file is stored in the Java directory <$Java_home>/jre/lib/security.

- Typical store location on IBM i:
  `/QOpenSys/QIBM/ProdData/JavaVM/jdk80/32bit/jre/lib/security`
- Tyical store location on Windows:
  `C:\Program Files\Java\jre1.8.0._nnn\lib\security`

Note: <$Java_home> represents the directory path where your Java implementation is stored. The

previously listed typical locations are just examples. Your particular directory depends on the installed and enabled version.

2.5.1 Displaying trusted CA certificates

Perform the following steps to display the currently stored CA certificates in file cacerts:

1. Change to the <$Java_home>/jre/lib/security directory.
   Example on Unix: `cd /usr/lib/j2sdk1.6-ibm/jre/lib/security`
   Example on Windows: `cd C:\Program Files\Java\jre1.8.0.151\lib\security`
2. Enter the following command to display the CA certificates.
   ```
   keytool -list -v -keystore cacerts
   ```
   On Windows the keytool is in the bin directory of the corresponding Java version. Example:
   `C:\Program Files\Java\jre1.8.0.151\bin\keytool.exe`
   Usually key stores are protected by a password. By default the password is set to *changeit*.

The CA certificates are displayed as shown in the following example:

```
****************************************
Alias name: equifaxsecureglobalebusinessca1
Creation date: Jul 18, 2003
Entry type: trustedCertEntry

Owner: CN=Equifax Secure Global eBusiness CA-1, O=Equifax Secure Inc., C=US
Issuer: CN=Equifax Secure Global eBusiness CA-1, O=Equifax Secure Inc., C=US
Serial number: 1
Valid from: 6/21/99 6:00 AM until: 6/21/20 6:00 AM
Certificate fingerprints:
      MD5:  8F:5D:77:06:27:C4:98:3C:5B:93:78:E7:D7:7D:9B:CC
      SHA1: 7E:78:4A:10:1C:82:65:CC:2D:E1:F1:6D:47:B4:40:CA:D9:0A:19:45
****************************************
```

2.5.2 Importing a CA certificate

Perform the following steps if you received error code 11 and you want to import a certificate's issuer CA certificate.

1. Obtain the CA certificate from the remote side. Typically the remote system administrator can extract the CA certificate from its keystore or provide information where to obtain the CA certificate. Typically the CA certificate is provided in a Base64 encoded format.
2. Change to the <$Java_home>/jre/lib/security directory.
   Example: `cd /usr/lib/j2sdk1.6-ibm/jre/lib/security`
3. Let's assume you received the CA certificate in a file named CACERT.CER and you want to provide an alias of *companyAcacert* for it. Enter the following command to import the CA certificate in to the cacerts file.
   ```
   keytool -import -alias companyAcacert -keystore cacerts -file CACERT.CER
   ```
   When prompted for the password, enter the keystore password. The default is *changeit*.
   The import process displays the CA certificate details:
   ```
   Enter keystore password:
   Owner: CN=LS CERT AUTH, O=IBM, ST=RLP, C=DE
   ```

```
Issuer: CN=LS CERT AUTH, O=IBM, ST=RLP, C=DE
Serial number: 43da5da2
Valid from: 8/8/10 9:12 PM until: 8/8/20 9:12 PM
Certificate fingerprints:
     MD5:  81:59:79:B6:20:F4:8F:D8:23:13:15:6D:83:3F:61:BC
     SHA1: 36:D1:22:F3:7C:7A:7A:47:2E:2F:33:A9:31:2E:52:67:2A:9F:15:B9
Trust this certificate? [no]:
```

4. Enter `yes` to import the certificate. The message *Certificate was added to keystore* indicates that the certificate was successfully imported.

From that point on the certificate trust check should complete without errors. Note that a change to the cacerts file requires a restart of the CEM utility.

2.5.3 Using your custom CA trust store file with CEM

The previous steps described the process of importing custom CA certificates into the default CA trust store that comes with every Java JRE/JDK. If you don't want to import your custom CA certificates whenever the Java version is updated on your system, you can once populate your CA trust store file and then override the default one when CEM starts as follows:

1. Follow the previous task to import your custom CA certificates into the cacerts file of your Java version.
2. Copy the cacerts file into the directory where the Certificate Expiration Manager code resides, i.e. /home/cem/mycacerts
3. Change the startcem script / startcem.bat file to specify the property for the custom CA trust store.
   Example:
   – Before
   ```
   java –classpath $CLASSPATH:. –jar CertificateExpirationMgr.jar $1 $2 $3 $4
   ```
   - After (with custom CA trust store file)
   ```
   java –Djavax.net.ssl.trustStore=./mycacerts –classpath $CLASSPATH:.
      –jar CertificateExpirationMgr.jar $1 $2 $3 $4
   ```