NotifySCM
Secure Content Management

Advanced Integration

TLS Certificate on the NotifySCM Server

TABLE OF CONTENTS

1 ENABLE A TLS CONNECTION BETWEEN NOTIFYSCM AND A REVERSE PROXY

This section describes how to install a certificate on NotifySCM in order to allow TLS connection from a reverse proxy.

1.1 Generate a self-signed certificate

1. Start the *portecle* application provided with NotifySCM installer package. (NotifySCM_INSTALLER/tools/portecle-launcher.bat)
2. To create a new keystore, select **File** -> **New keystore** and choose **JKS**.
3. Select **Tools** -> **Generate Key Pair**.
4. Use RSA algorithm with a key size of 4096.
5. Enter the required information.
6. Enter an alias name (NotifySCMserver) and a password.
7. Save the generated keystore (**File** -> **Save Keystore**) with the same password used for generation of the jks file.

1.2 Install the certificate

1. Copy and paste the Keystore into the folder: C:/NotifySCM/conf
2. Edit the following lines in the C:/NotifySCM/conf/server.xml file.

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
           port="8443" address="${jboss.bind.address}"
           scheme="https" secure="true" clientAuth="false"
           keystoreFile="<NotifySCM_HOME>/conf/mykeystore.jks"
           keystorePass="mypassword" sslProtocol = "TLS"

           ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA"/>
```

3. Set the path TLS to the keystore file for the variable keystoreFile and the keystore password (defined at step 1.1.6) for the variable keystorePass.

If you want to use TLS connection between the security server and the application server, your certificate must be added in the NotifySCM truststore as well.

1.3 Restart the server

1. Press the Windows button and enter "services" as the keyword.
2. Select **Services** program.
3. Find the service, SENSE-SERVER. Right click on it and press **Restart**.

2 ADDING BACKEND TLS CERTIFICATES IN THE NOTIFYSCM TRUST STORE

This section will help IT administrators to properly configure the TLS connections between NotifySCM and backend systems.

2.1 Creating a NotifySCM trust store

The first time you add a certificate, you need to create a trust store for NotifySCM. This store will contains all the certificate that must be trusted by NotifySCM. To ensure that NotifySCM will trust standard certificates and proprietary ones, we will use the JAVA trust store as a basis.

2.1.1 Copy the JAVA trust store

1. Copy the file C:/NotifySCM /jdk/jre/lib/security/cacerts.
2. Paste it in the folder C:/NotifySCM /conf and rename to sense.jks.

2.1.2 Change trust store password

1. Start the portecle application provided with the NotifySCM installer package (NotifySCM_INSTALLER/tools/portecle-launcher.bat)
2. Open sense.jks by selecting **File** -> **Open keystore file**) and enter the password "changeit".
3. Change the password by selecting **Tools** -> **Set Keystore Password**. Note it and keep it somewhere safe.
4. Click **File** -> **Save Keystore**.

2.1.3 Enable the trust store

Windows

- Start the NotifySCM service manager (NotifySCM_HOME/services/NotifySCM-SERVER_service_manager.bat)
- Select the Java tab and add the following lines and **set the path and the password**:

  -Djavax.net.ssl.trustStore=file:///NotifySCM_HOME/conf/sense.jks
  -Djavax.net.ssl.trustStorePassword=thepassword

- Apply and restart the SENSE service

Linux

- Edit the file *NotifySCM_HOME/*bin/setenv.sh
- Remove the # before the line where trust store option is defined and **set the path and the password**:

  *JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=*file:///NotifySCM_HOME/conf/sense.jks *-Djavax.net.ssl.trustStorePassword=thepassword"*

- Save the file and restart the SENSE service

2.2 Add a certificate in the NotifySCM trust store

When the trust store has been created and referenced in NotifySCM, you can add your backend certificates that NotifySCM must trust.

1. Start the *portecle* application provided with NotifySCM installer package. (NotifySCM_INSTALLER/tools/portecle-launcher.bat) Start the application *portecle.*
2. Open NotifySCM by clicking **File -> Open keystore file** and enter the password you set at installation.
3. If you have the certificate (*.pem, *.cer, *.crt, *.cert), jump to step 8.
4. The *Portecle* app provides a tool to retrieve the certificate to be added. Click **Examine** -> **Examine SSL/TLS Connection**.
5. Enter the backend hostname or ip address and the port number.
6. Select the certificate you want to add and click **PEM Encoding**.
7. Click **Save**, browse to NotifySCM_HOME/conf, and complete the save.
8. Select **Tools** -> **Import Trusted Certificate**. Select the certificate to import.
9. Click **File** -> **Save Keystore**.
10. **Restart the SENSE service.**

3 ENABLE A TLS CONNECTION BETWEEN NOTIFYSCM AND IBM DOMINO

This section describes how to setup NotifySCM to enable TLS connection and how to install the Domino certificate so it is trusted by NotifySCM.

3.1 Enable TLS on NotifySCM

1. Using a WEB browser, navigate to the PIM configuration administration console. (https://<your_ip>/sense/pim/).
2. Click on the server button and select the **PIM Parameters** tab.
3. In the Mail server section, check the box labeled, **Connect using TLS?**

3.2 Create a key ring on Domino

Open the Server Certificate Admin (certsrv.nsf) database on a Domino server and use its forms to create and populate a key ring. See *Administering the Domino System, Volume 2* or the Domino Administrator Help for detailed information. For testing purposes, you can use the CertAdminCreateKeyringWithSelfCert form to create a key ring with a self-certified certificate.

3.3 Move the keyring to the server

The keyring consists of a keyring file (KYR file) and stash file (STH file). These files are generated on the computer from which you are accessing the Server Certificate Admin database. Move or copy the two keyring files to the computer containing the Domino server. Place them in the server's data directory. For example, if you create a keyring with a self-certified certificate using default names and copy the files to a computer with a server whose data files are installed at C:\Lotus\Domino\Data, the server files would be:

```
C:\Lotus\Domino\Data\selfcert.kyr
C:\Lotus\Domino\Data\selfcert.sth
```

3.4 Enable SSL on Domino

In the Server document in the server's Domino Directory, select the Ports tab, then the Internet Ports tab. Under SSL settings, specify the SSL key file name (for example, selfcert.kyr). Select the DIIOP tab. Ensure that the SSL port number is correct-it defaults to 63149. Enable the SSL port. Set Name & password and Anonymous authentication as desired.

NOTE: Steps 3.2 to 3.4 has been copied from the following site:
http://blueteetech.wordpress.com/2007/08/02/configure-ssl-on-domino/

3.5 Install the certificate on NotifySCM

Once the keyring files are on the server, starting or restarting the DIIOP task generates a file named TrustedCerts.class in the Domino data directory. Copy that file to NotifySCM_HOME/lib.

3.6 Restart the SENSE service