5761-XH2 V6R1 System i Access for Web

Automating tasks – HTTPS/SSL

First Edition (April 2008)
This edition supplements the V6R1 System i Access for Web InfoCenter documentation.

Table of contents

1. Overview

System i™ Access for Web provides a program to automate the running of tasks. By automating the running of tasks, those tasks can also be scheduled to run when you need them to run. The V6R1 System i Access for Web InfoCenter Automating Tasks topic discusses how to automate and schedule System i Access for Web tasks. The InfoCenter topic should be reviewed before continuing with the information in this document.

System i Access for Web is a web application containing servlets that workstation users interactively use to access i5/OS® resources. Many of the System i Access for Web tasks can be configured to run with a single invocation and saved for repeated use. One example is to define a Database request to run an SQL statement generating the results as a PDF file. Another example is to define and save an i5/OS CL command that is run repeatedly.

Even though the invocation of these tasks can be simplified to a single click of an icon on a web page or the invocation of a web browser address, an interactive action by a workstation user is required. System i Access for Web now provides a program to automate the running of tasks.

The System i Access for Web tasks are automated using the java program iWATask.jar. This program can be used for either HTTP or HTTPS/SSL environments. To use System i Access for Web tasks that are secured using HTTPS/SSL, additional setup is required.

The information below discusses the additional setup for the HTTPS/SSL environment. The steps setup a Windows workstation using the Internet Explorer web-browser. The general concepts are then discussed relative to the i5/OS QShell environment.

---

2. Setting up the HTTPS/SSL environment

In the HTTPS/SSL environment, certificates are used to validate the authenticity and encrypt the communication between the server and client.

The sections below walk through the steps to setup a Windows workstation environment. Specifics for the i5/OS QShell environment are then discussed. The general concepts can be applied to other environments.

The information below is an example and may not completely address configuration requirements for your specific environment. Please refer to the IBM Information Center for additional information to address specifics for your environment.

2.1 Download the Certificate Authority

Download the Certificate Authority to your Windows workstation using the web-browser Internet Explorer.

1. Open the Internet Explorer (IE) web-browser to your System i Access for Web environment. Specify a web address such as https://<system>:<port>/webaccess/iWAPing where "system" is the name of your i5/OS system and "port" is the TCP/IP port your HTTP web server is listening for requests on.
2. You should be prompted with a security alert. If you are not prompted with a security alert…
    a. In the browser click Tools->Internet Options.
    b. Click Content tab.
    c. Click Certificates.
    d. Intended Purpose dropdown, select <All>.
    e. Click Trusted Root Certification Authorities.
    f. Scroll through the list looking for the <system> that as used in the URL in step 1.
    g. Select the <system> entry, click Remove.
    h. Confirm the removal/delete of the certificate.
    i. Close the browser dialogs and browser.
    j. Open IE to your "https://<system>:<port>/webaccess/iWAPing" web address.
    k. You should be prompted with a security alert.
3. Click View Certificate.
4. Click Install Certificate.
5. A wizard is started, click Next.
6. Select the option to automatically select the certificate store based on the type of certificate, click Next.
7. Click Finish.
8. You may be prompted with a warning asking you to confirm the installation of the certificate. Click the appropriate button(s) to accept the certificate. You should receive a dialog indicating the certificate was imported.
9. Accept/close any browser dialogs that are open.
10. In the browser click Tools->Internet Options.
11. Click Content tab.
12. Click Certificates.
13. Intended Purpose dropdown, select <All>.
14. Click Trusted Root Certification Authorities.
15. Scroll through the list looking for the <system> that as used in the web address in step 1.
16. Select the <system> entry, click Export.
17. A wizard is started, click Next.
18. Select Base-64 encoded, click Next.
19. Enter a file name, we suggest <system>.cer, click Next, click Finish.
20. Close the browser dialogs and browser.
21. Please note that <system>.cer is unique to the system and the port. If other systems/ports are being tested, those certificates should be downloaded to unique files.

2.2 Add the Certificate Authority to a keystore

The certificate authority that was downloaded must be added to a keystore on the Windows workstation.

1. A java tool will be used to add the downloaded certificate to a keystore. Locate JAVA_HOME/bin/keytool.exe on your Windows workstation.
2. Open a DOS Prompt window.
3. Create a directory and change to that directory.
4. Copy <system>.cer to this directory.
5. Create a local keystore file using the following command…

   JAVA_HOME\bin\keytool -import -alias <system> -trustcacerts -storetype jks -file <system>.cer -keystore <system>.jks

   -alias is just a label within the file to make this certificate unique among other entries in the keystore

   When keytool runs, you may be prompted for a password. One standard some use is to make the password the same name as the system on which the certificate was created. Please verify with your system administrator or other appropriate group what should be used for a password.

6. Invoke iWATask with this syntax where the <my_properties_file> is invoking an HTTPS URL…

   java -jar -Djavax.net.ssl.trustStore=<system>.jks iWATask.jar <my_properties_file>

2.3 Add the Certificate Authority to the system wide keystore

There is a default trusted keystore that can be used if a local keystore is not desired. The following steps walk through updating the default trusted keystore and how to use it.

1. A java tool will be used to add the downloaded certificate to a keystore. Locate JAVA_HOME/bin/keytool.exe on your Windows workstation.
2. Locate the file JAVA_HOME/…./cacerts
3. Open a DOS Prompt window.
4. Create a directory and change to that directory.
5. Copy <system>.cer to this directory.
6. Use keytool to add the downloaded certificate to cacerts…

   JAVA_HOME\bin\keytool -import -alias <system> -trustcacerts -storetype jks -file <system>.cer -keystore JAVA_HOME\…\security\cacerts

   -alias is just a label within the file to make this certificate unique among other entries in the keystore

   When keytool runs, you may be prompted for a password. Our standard is to make the password the same name as the system on which the certificate was created.

7. Invoke iWATask with this syntax where the <my_properties_file> is invoking an HTTPS URL…

   java -jar iWATask.jar <my_properties_file>

2.4 i5/OS QShell specifics

In general, the steps listed above to setup the Windows environment can be applied to the i5/OS QShell environment.

Below are specific considerations for the i5/OS QShell environment.

1. The Java 1.5 environment is installed to i5/OS under the path /QIBM/ProdData/Java400/jdk15/…
2. The "keytool" tool can be found in

/QIBM/ProdData/Java400/jdk15/bin/

3. Java 1.5 environment
   - Create a directory under the root directory /home and name it the same name as your user profile. For example:
     /home/<your_user_profile>
   - In /home/<your_user_profile> create a file named SystemDefault.properties and add the following to it:
     java.version=1.5

     This will cause the Java 1.5 environment to be used by default when a QShell session is started.
4. Copy /QIBM/ProdData/Access/Web2/lib/iWATask.jar to /home/<your_user_profile>
5. Copy your <system>.cer to /home/<your_user_profile>
6. Use the keytool tool to create your <system>.jks in /home/<your_user_profile>
7. When you invoke iWATask.jar, specify the properties

For example:

```
java -jar -Djavax.net.ssl.trustStore=/home/<your_user_profile>/<system>.jks
          -Dcom.ibm.as400.webaccess.iWATask.log.category=all iWATask.jar
/home/<your_user_profile>/iWAPing.properties
```

[END OF DOCUMENT]