CONFIGURING ENTRAPASS FOR THE MOBILE APPLICATION

The purpose of this application note is to describe the steps required to configure the EntraPass software in order to use the mobile application.

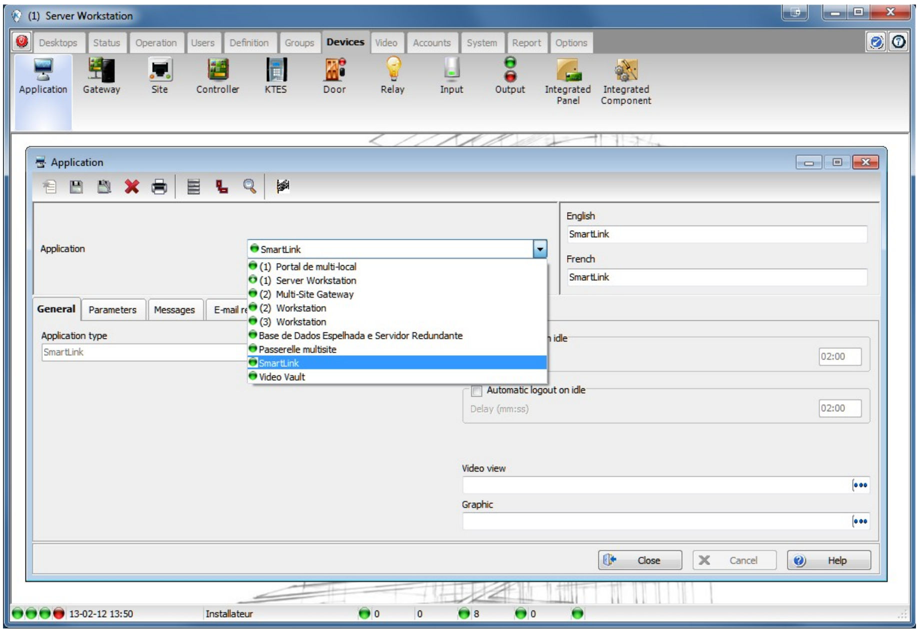
Requirements:

- EntraPass Global or Corporate Edition, version 5.01.40 or later
- The mobile application (Apple App Store® or Google Play Store)
- Kantech Smart Service and SmartLink running
- Opened 8801 port (TCP)

Note: SmartLink and WebStation applications must have been previously registered in EntraPass for the **SmartLink WebStation** tab to be available. Please refer to the EntraPass Reference Manual for more information.

Steps to Set Up Your Mobile Application:

1. Login to the Server Workstation.
2. Select **Devices | Application.**
3. From the **Application** drop-down list, select **SmartLink.**
4. Click the **SmartLink WebStation** tab.



Application: SmartLink

English: SmartLink

French: SmartLink

Application type: SmartLink

idle: 02:00

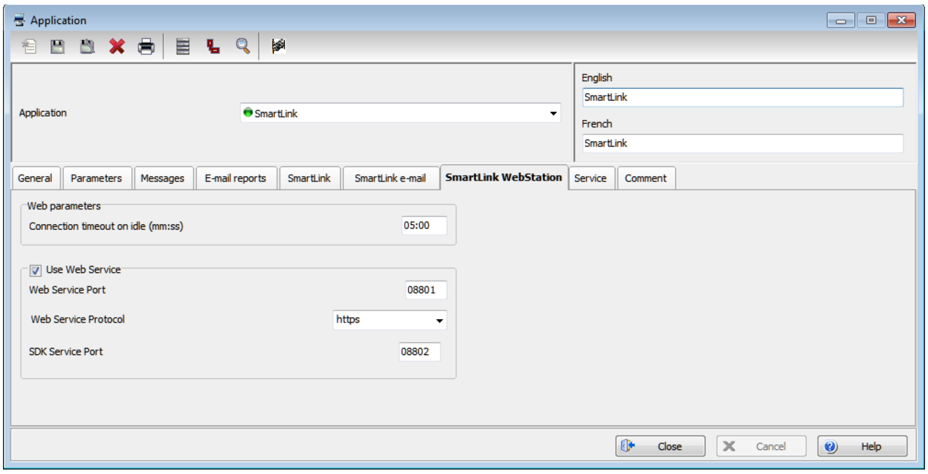
☐ Automatic logout on idle

Delay (mm:ss): 02:00

Video view

Graphic

5. Ensure that the *Use Web Service* checkbox is checked.



Application: SmartLink

English: SmartLink

French: SmartLink

Web parameters

Connection timeout on idle (mm:ss): 05:00

☑ Use Web Service

Web Service Port: 08801

Web Service Protocol: https

SDK Service Port: 08802

How To Configure a Port with an SSL Certificate:

If you are running Windows Server 2003 or Windows XP, use the HttpCfg.exe tool (this tool is installed with Windows Server 2003). For more information, see **Httpcfg Overview**. The **Windows Support Tools documentation** explains the syntax for the Httpcfg.exe tool.

Requirements:

- Opened 8801 port
- A valid SSL certificate on IIS
- Administrator privileges for the server

Note: Modifying certificates stored on the computer requires administrative privileges.

Getting a Certificate Thumbprint

<u>Viewing certificates in the MMC snap-in</u>:

1. Open a Command Prompt window.
2. Type **"mmc"** and press the ENTER key. Note that you must be in the Administrator role to view certificates in the local machine store.
3. On the File menu, click **Add/Remove Snap In**.
4. Click **Add**.
5. In the Add Standalone Snap-in dialog box, select Certificates.
6. Click **Add**.
7. In the **Certificates snap-in** dialog box, select **Computer account** and click **Next**. Optionally, you can select **My User account** or **Service account**. If you are not the administrator of the computer, you can manage certificates only for your user account.

8. In the **Select Computer** dialog box, click **Finish**.

9. In the **Add Standalone Snap-in** dialog box, click **Close**.

10. In the **Add/Remove Snap-in** dialog box, click **OK**.

11. In the **Console Root** window, click **Certificates (Local Computer)** to view the certificate stores for the computer.

12. Optional: To view certificates for your account, repeat steps 3 to 6. At step 7, instead of selecting **Computer account**, click **My User account** and repeat steps 8 to 10.

13. Optional: On the **File** menu, click **Save** or **Save As**. Save the console file for later use.

Retrieving a certificate's thumbprint:

1. Open the Microsoft Management Console (MMC) snap-in for certificates (see How to: "View Certificates with the MMC Snap-in").

2. In the Console Root window's left pane, click **Certificates** (Local Computer).

3. Click the **Personal** folder to expand it.

4. Click the **Certificates** folder to expand it.

5. In the list of certificates, note the **Intended Purposes** heading. Find a certificate that lists **Client Authentication** as an intended purpose.

6. Double-click the certificate.

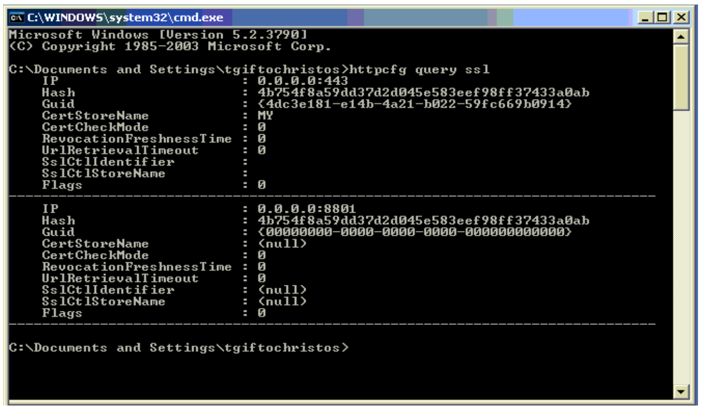
7. In the **Certificate** dialog box, click the **Details** tab.

8. Scroll through the list of fields and click **Thumbprint**.

9. Copy the thumbprint of the certificate into a text editor, such as Notepad.

10. Remove all spaces between the hexadecimal characters. One way to accomplish this is to use the text editor's find-and-replace feature and replace each space with a null character.

11. In Windows Server 2003 or Windows XP, follow the procedure required using the HttpCfg.exe tool to support clients that authenticate with X.509 certificates at the transport layer, as shown in the following example:



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\tgiftochristos>httpcfg query ssl
    IP                      : 0.0.0.0:443
    Hash                    : 4b754f8a59dd37d2d045e583eef98ff37433a0ab
    Guid                    : {4dc3e181-e14b-4a21-b022-59fc669b0914}
    CertStoreName           : MY
    CertCheckMode           : 0
    RevocationFreshnessTime : 0
    UrlRetrievalTimeout     : 0
    SslCtlIdentifier        :
    SslCtlStoreName         :
    Flags                   : 0
------------------------------------------------------------------------------
    IP                      : 0.0.0.0:8801
    Hash                    : 4b754f8a59dd37d2d045e583eef98ff37433a0ab
    Guid                    : {00000000-0000-0000-0000-000000000000}
    CertStoreName           : (null)
    CertCheckMode           : 0
    RevocationFreshnessTime : 0
    UrlRetrievalTimeout     : 0
    SslCtlIdentifier        : (null)
    SslCtlStoreName         : (null)
    Flags                   : 0
------------------------------------------------------------------------------

C:\Documents and Settings\tgiftochristos>
```

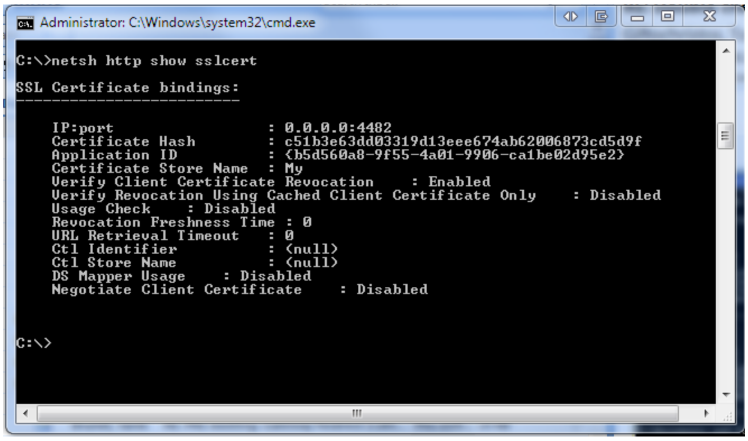
1. Click the **Start** button.

2. Click on **Run**.

3. Type **CMD** and then **OK**.
   (httpcfg set ssl -i 0.0.0.0:8801 -h 0000000000003ed9cd0c315bbb6dc1c08da5e6 -f 2)

Note: To view “httpcfg” settings, type the following command: **httpcfg query ssl**.

In Windows 7 Server 2008, follow the preceding procedure to support clients that authenticate with X.509 certificates at the transport layer, but with an additional parameter, as shown in the following example:



```
C:\>netsh http show sslcert

SSL Certificate bindings:
-------------------------

    IP:port                 : 0.0.0.0:4482
    Certificate Hash        : c51b3e63dd03319d13eee674ab62006873cd5d9f
    Application ID          : {b5d560a8-9f55-4a01-9906-ca1be02d95e2}
    Certificate Store Name  : My
    Verify Client Certificate Revocation    : Enabled
    Verify Revocation Using Cached Client Certificate Only    : Disabled
    Usage Check    : Disabled
    Revocation Freshness Time : 0
    URL Retrieval Timeout   : 0
    Ctl Identifier          : (null)
    Ctl Store Name          : (null)
    DS Mapper Usage    : Disabled
    Negotiate Client Certificate    : Disabled


C:\>
```

1. Click the **Start** button.

2. Click on **Run**.

3. Type **CMD** and then **OK**.
   (netsh http add sslcert ipport=0.0.0.0:8801 certhash=0000000000003ed9cd0c315bbb6dc1c08da5e6 appid={BEC17D90-C568-4670-8F09-57C496631605} clientcertnegotiation=enable)

Note: To view “httpcfg” settings, type the following command: **netsh http show sslcert**

Information furnished by Kantech is believed to be accurate and reliable. However, no responsibility is assumed by Kantech for its use, nor any infringements of other rights of third parties which may result from its use. No license is granted by implications or otherwise under any patent rights of Kantech.