Secure your web applications with Secure Sockets Layer (SSL) on IBM i

Configure SSL for Liberty based application servers using IBM Web Administration for i

Wang Hui Qin

June 30, 2016

To protect data during transmission, applications and web servers commonly use Secure Sockets Layer (SSL) for encrypted communication. IBM® Web Administration for i provides an easy-to-use wizard to configure SSL for the Liberty based application servers, such as Integrated Web Application Server for i (IAS), Integrated Web Services Server for i (IWS) and stand-alone Liberty servers. This article provides an example that illustrates how to secure web applications on IAS servers.

Introduction

To protect data from prying eyes during transmission, applications and web servers commonly use Secure Sockets Layer (SSL), now also known as Transport Layer Security (TLS) which is an updated and greatly improved version of SSL, for encrypted communication. In typical SSL usage, the server is configured with a certificate, which proves its identity and enables secure encryption of the data being sent between the server and clients to guarantee privacy and data integrity.

In this article, we describe how to use the wizard provided by IBM Web Administration for i to configure SSL for Integrated Web Application Server for i (IAS), Integrated Web Services Server for i (IWS) and stand-alone Liberty servers running on IBM i. IAS is a lightweight Java™ application server built on the Liberty web container that is integrated into the IBM i operating system. The IWS servers run on IAS to provide support in externalizing integrated language environment (ILE) program objects (such as RPG and COBOL programs and service programs) as web services quickly and easily. The Web Administration for i graphical user interface (GUI) provides many easy to use wizards to manage HTTP servers and application servers on IBM i. Now, it supports in configuring SSL for IAS v8.5, IWS v2.6 and later and stand-alone Liberty servers. Additionally, you can configure SSL for some admin instances, such as ADMIN2, ADMIN5, and ADMIN3, which run on a Liberty web container.

Prerequisites

To use the SSL configuration wizard on the IBM Web Administration for i GUI, you need to meet the following prerequisites:

Group PTF

- IBM i7.3 SF99722 Level 2 or later
- IBM i7.2 SF99713 Level 15 or later
- IBM i7.1 SF99368 Level 41 or later

Licensed program

Licensed program 5770SS1 with option 34, which is the product of Digital Certificate Manager (DCM), is required when the *SYSTEM store is used for SSL.

User profile

The user profile accessing the Web Administrator for i GUI must have access to the application server and the associated HTTP server or can be a user profile with the *ALLOBJ, *IOSYSCFG and *SECADM authorities, or a user who has been granted permission through the Permissions support in the Web Administrator for i GUI.

Terms

- **Certificate**: A digital certificate is a credential used as an identity of proof between the server and client. It consists of a public key and some identifying information that a certificate authority (CA), an entity to sign certificates, has digitally signed. Each public key has an associated private key and the server must prove that it has access to the private key associated with the public key contained within the digital certificate. A self-signed certificate means it is signed by the server itself. If a self-signed certificate is specified to a server, clients might not trust the connection. To obtain a signed certificate from a public CA, you need to generate a Certificate Signing Request (CSR) and send it to the CA. After a certificate is returned, it is imported to your keystore.
- **Keystore**: The keystore is a storage facility for cryptographic keys and certificates. A private key entry in a keystore file holds a cryptographic private key and a certificate chain for the corresponding public key. A private key entry can be specified to a server when configuring SSL. A trusted certificate entry contains a public key for a trusted party, normally a CA. A trusted certificate is used to authenticate the signer of certificates provided by a server or client. The keystore types that the Web Administrator for i GUI supports are: JKS, JCEKS, PKCS12, and CMS. Additionally, the Digital Certificate Manager (DCM) *SYSTEM is also supported.

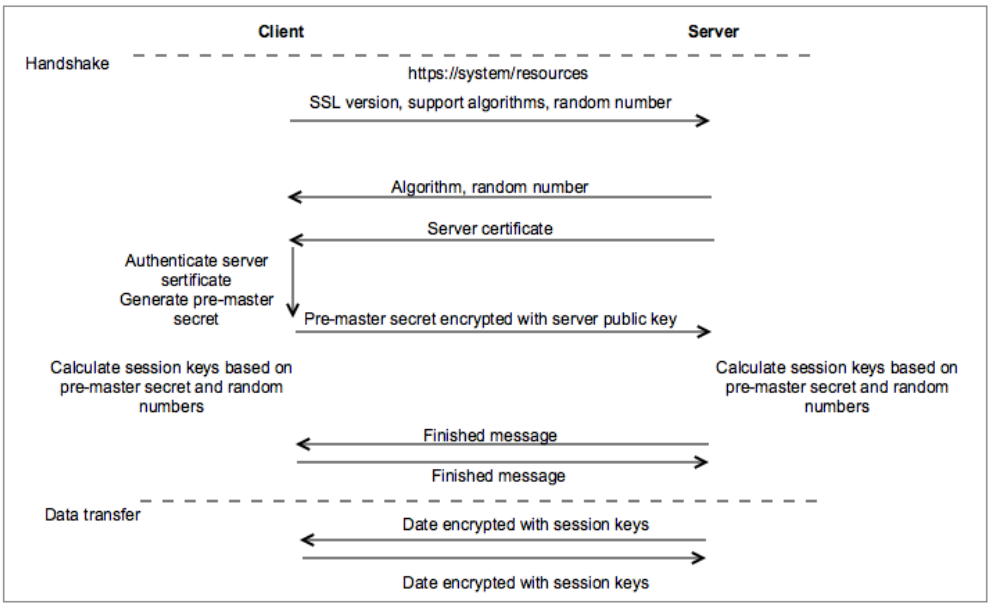
Overview of SSL

SSL secures communication by providing message encryption, integrity, and authentication. Figure 1 illustrates the SSL process for a client requesting an SSL connection to a server. This connection is secured and no client authentication is required.

1. The client sends a message with the SSL version, a list of supported algorithms, and a random number that will be used to generate the keys.

2. The server responds with the algorithm to use and a random number that will be used to generate the keys.
3. The server sends its server certificate containing its public key to the client.
4. The client authenticates the server certificate with its trust CA list. If the certificate is issued from an unknown CA, the browser normally warns the client to take the risk for the untrusted connection. In general, browsers maintain a default trust CA list, including public-known CAs. It is recommended to secure a server using a certificate signed by public-known CAs.
5. The client generates a pre-master secret, encrypts it using the server's public key, and sends it to the server.
6. The server uses its private key to decrypt and retrieve the pre-master secret.
7. The client and server separately calculates the symmetric keys that will be used in the SSL session based on the random numbers and pre-master secret.
8. The client and server sends a finished message and begins to transfer data with the symmetric keys.

Figure 1. Overview of the SSL process



Configure SSL wizard

The Web Administrator for i GUI now allows you to configure SSL for IAS V8.5, IWS V2.6, and stand-alone Liberty servers with an existing certificate or by issuing a new self-signed certificate with keystore types: JKS, JCEKS, PKCS12, CMS, or DCM *SYSTEM store for SSL using the Configure SSL wizard.

In the example discussed in this section, we have an integrated application server, INTAPPSVR (refer to the Web Administrator product website to find how to create an IAS server), with an application *myapp* deployed on it. By default, the application can only be accessed through the non-secure HTTP port for the INTAPPSVR server or front-end HTTP server. We have a certificate labeled MYKEY in the DCM *SYSTEM store and can use this certificate for setting up SSL for the IAS server. The information for this scenario is listed in Table 1.

Table 1. Information about the example scenario

Component	Value
IAS name	INTAPPSVR
Application name	MYAPP
Application context	/myapp
IAS HTTP port now listen on	10000
IAS SSL port to be configured	443
HTTP server name	INTAPPSVR
HTTP server HTTP port now listening on	80
HTTP server SSL port to be configured	4433
Certificate	MYKEY stored in DCM *SYSTEM store

If you do not have a certificate available in DCM, it can be easily created using the Create Certificate wizard in the Web Administrator for i GUI, as shown in Figure 2.

Figure 2. Creating a certificate

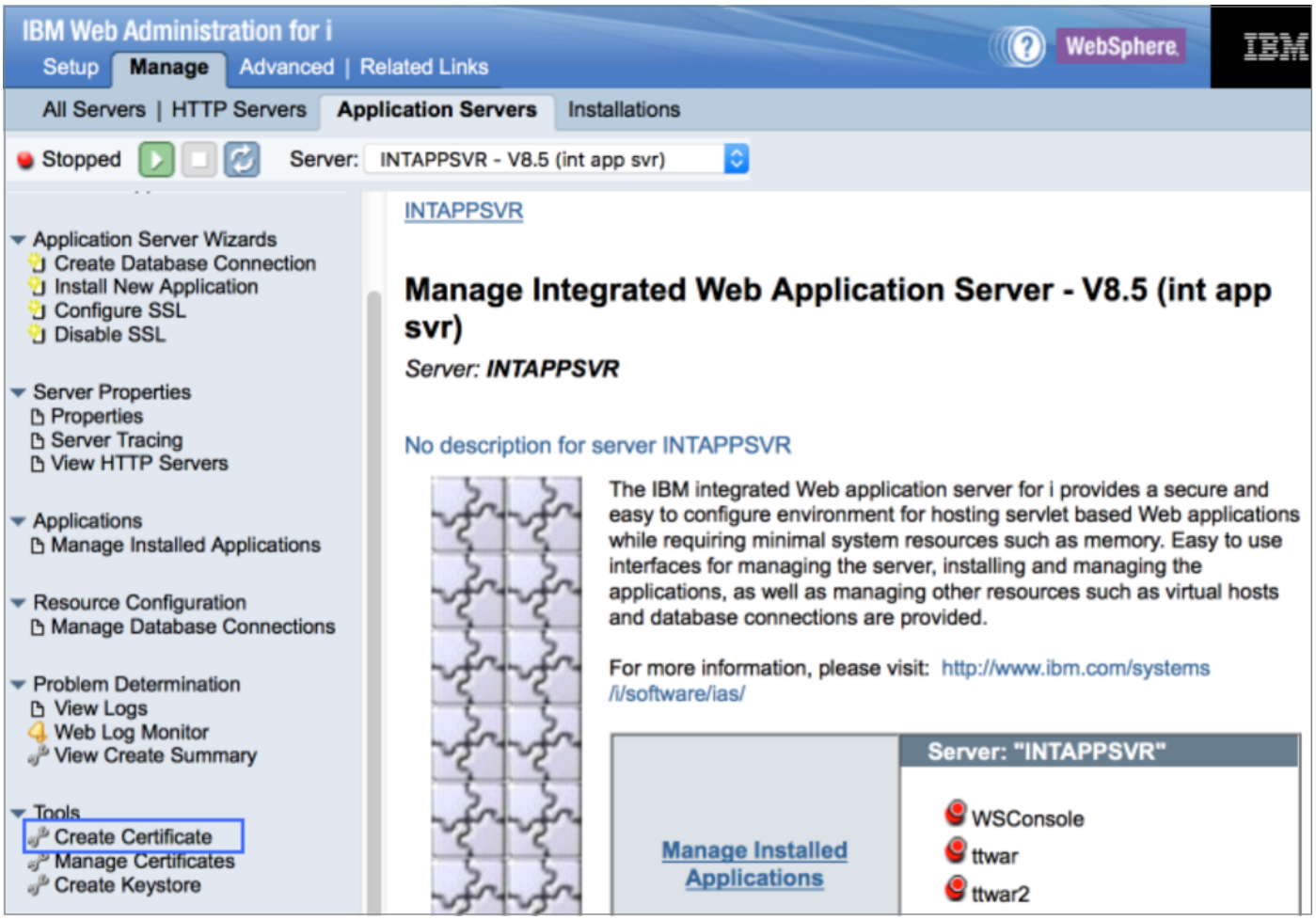
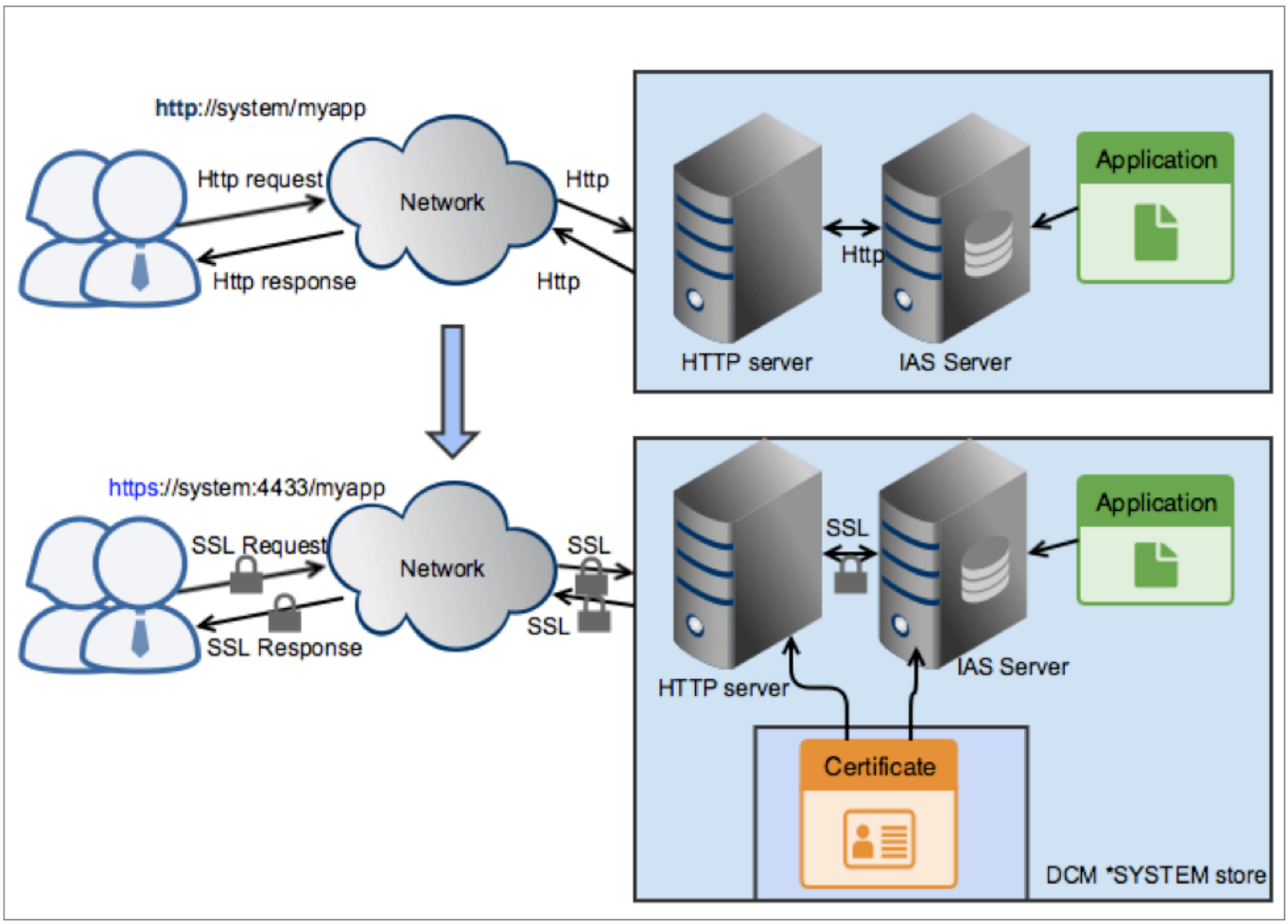


Figure 3. Scenario to set up SSL for INTAPPSVR



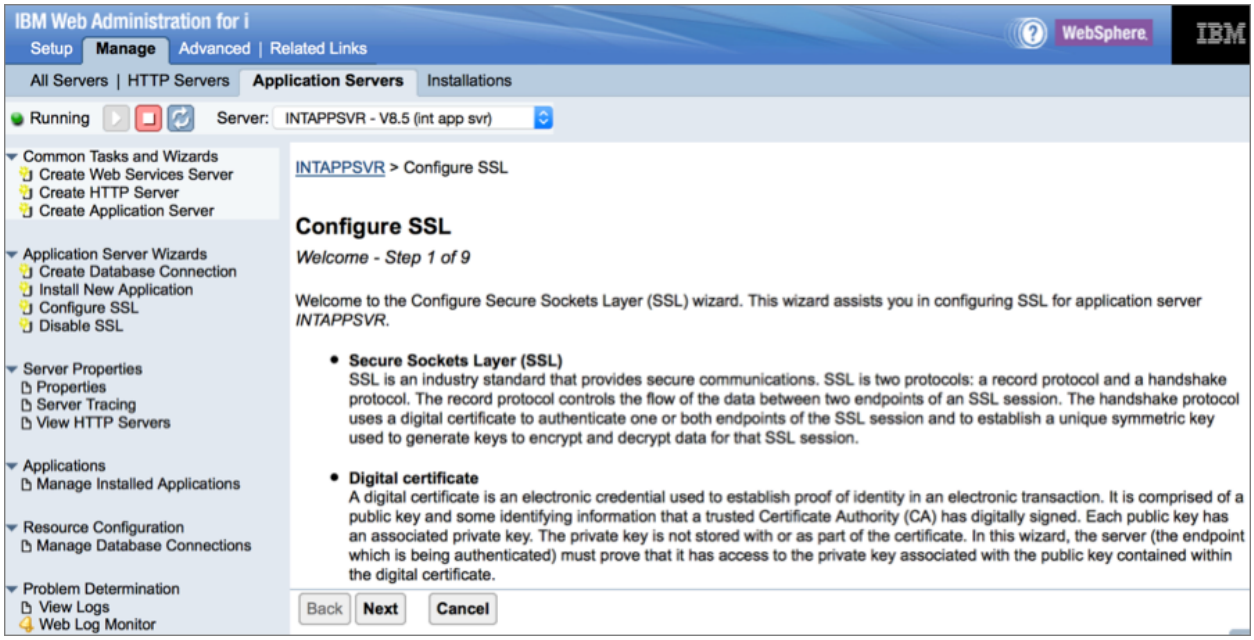
Configuring SSL for the INTAPPSVR IAS is accomplished using the Configure SSL wizard in nine steps. These steps are described below.

Step 1. Open the welcome page

Before using the Configure SSL Wizard, the Admin server must be started using the following command. (You can find more details about this in the Knowledge Center).
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
After the server is started, access the Web Administrator for i GUI using the following URL:
http://*system*:2001/HTTPAdmin

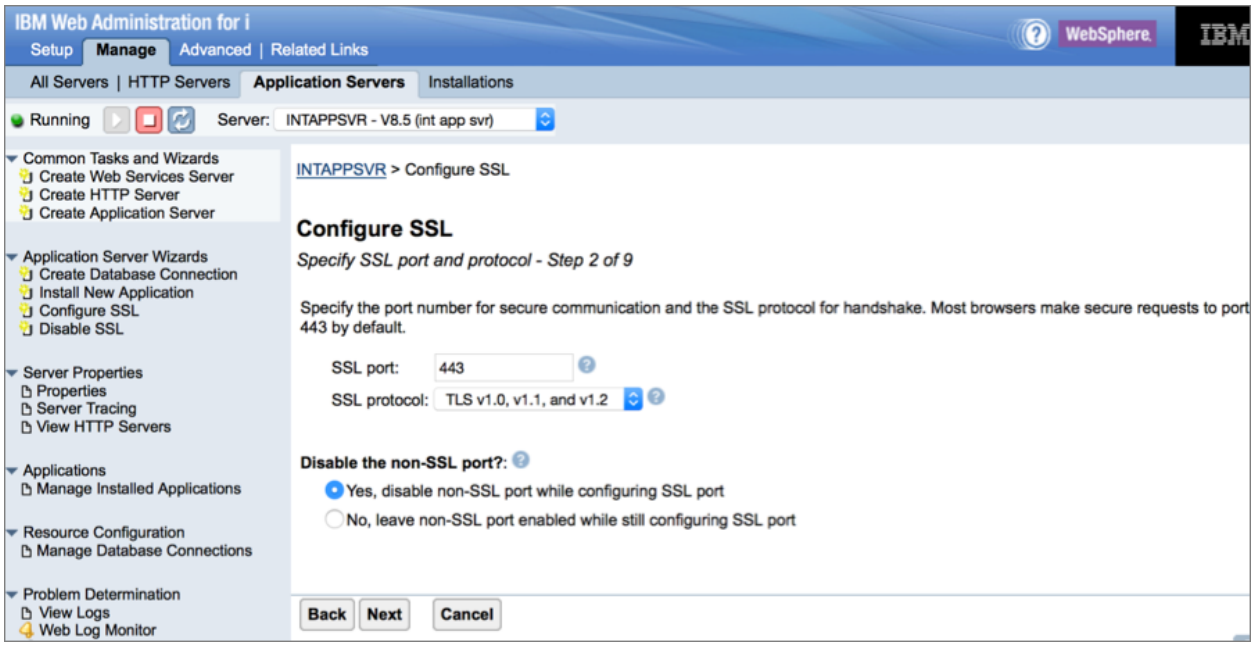
Click the **Manage** tab, and within that, click the **ApplicationServers** tab, and select the application server, **INTAPPSVR**. In the left pane, click **Configure SSL** under **Application Server Wizards** to launch the wizard. Step 1 of the wizard shows the welcome page as shown in Figure 4. Click **Next** to continue.

Figure 4. Configure SSL



Step 2. Specify SSL port and SSL protocol

Figure 5. Specify SSL port and SSL protocol



In step 2, we configure the SSL port and the SSL protocol as shown in Figure 5.
In this example, use the default value **443** as the SSL port and enable **TLS v1.0, v.1.1 and 1.2** for the SSL. Disable the non-SSL port so that the application can only be accessed through SSL. Keep the remaining default values on this page and click **Next** to continue to the next step.

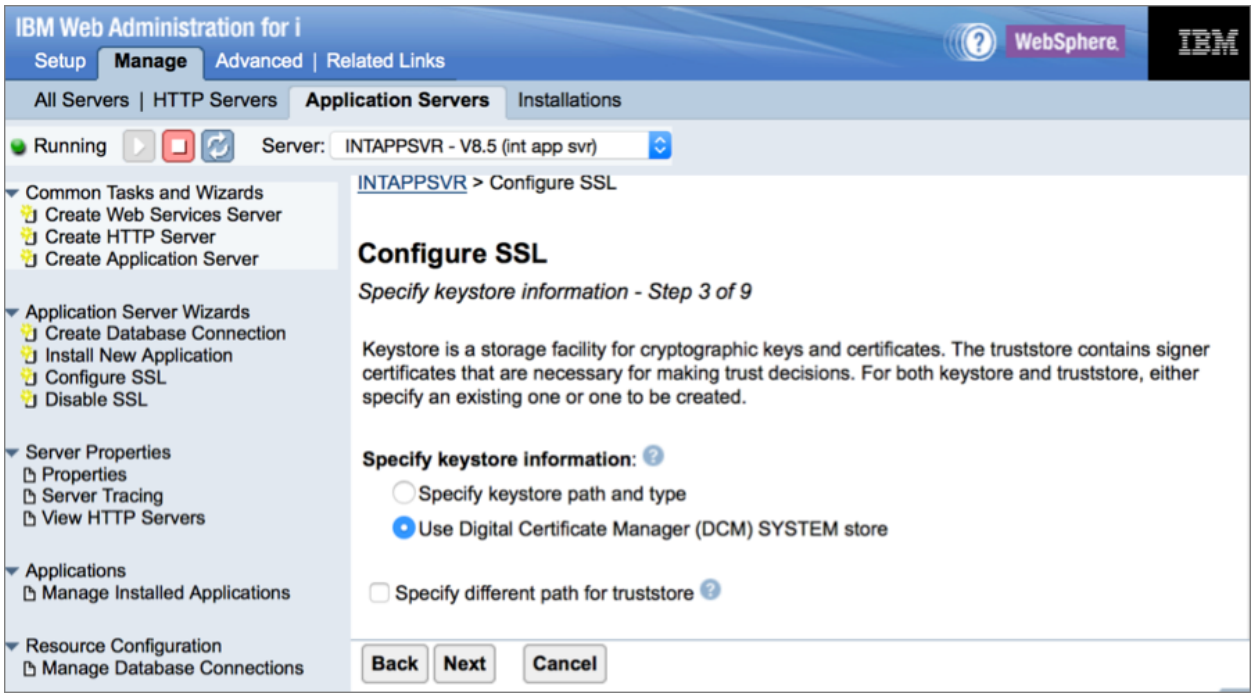
Note: For the ADMIN instances, the SSL port default value is as follows:

- ADMIN2: 2005
- ADMIN3: 2007
- ADMIN5: 2012

If the given default port is modified when configuring SSL, the redirection from the ADMIN HTTP server will fail. For example, IBM Navigator for i deployed on ADMIN2 , which is redirected from port 2001 to 2005. If ADMIN2 SSL port is updated from 2005 to some other port number, to make the redirection work, the ADMIN HTTP server *RewriteRule* directives must be updated manually.

Step 3. Specify keystore information

Figure 6. Specify keystore information



In step 3 of the wizard, the keystore information is configured as shown in Figure 6. Keystore is a storage facility for the SSL certificate. A keystore file must be specified to configure SSL for an application server. The keystore file that already exists on an IBM i system or a new file which does not yet exist can be used. For a new keystore file, the wizard helps to create the file and to create a self-signed certificate.

In the current example, select *Use Digital Certificate Manager (DCM) SYSTEM store* for the keystore information and click **Next**.

Note: If the SSL communication between the front-end HTTP server plug-in and the application server is required, only the CMS keystore and the DCM *SYSTEM store can be used. If there are no non-SSL ports available for the application server and a non-CMS or DCM type store is not specified, access from the front-end HTTP server will fail.

The DCM *SYSTEM store is located at /QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.KDB. By default *PUBLIC is *EXCLUDE to the DCM store file. If the DCM *SYSTEM store is used

to configure SSL for the application server, the application server runtime user profile (default QLWISVRT for IAS V8.5, default QWSERVICE for IWS2.6, and default QEJBSVR for stand-alone Liberty servers) and HTTP server runtime user QTMHHTTP will be updated with the *RX authority to the store path by the wizard.

Step 4. Specify the keystore password

Figure 7. Specify keystore password

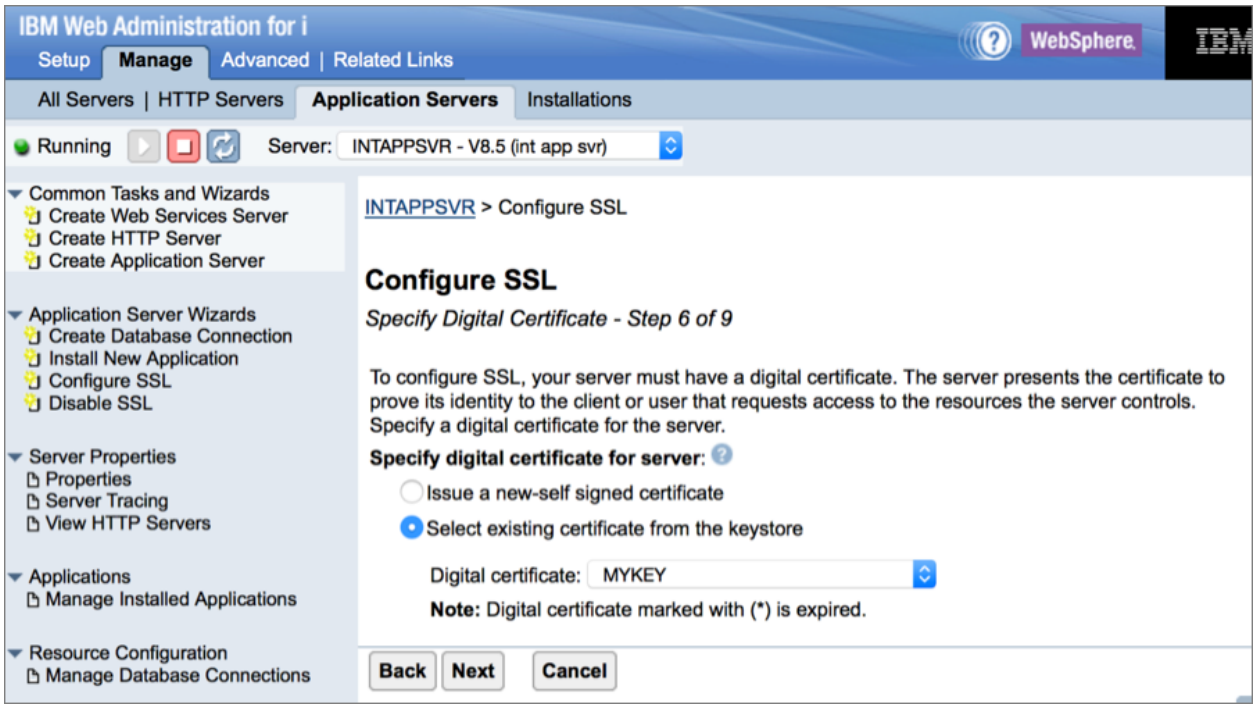
For an existing keystore, the password to access it must be provided. Specify the DCM *SYSTEM store password and click **Next**. For more information about DCM, refer to the Knowledge Center.

Step 5. Specify truststore password

Step 5 of this wizard is to specify the password for truststore. The wizard gets to this step only when the **Specify different path for truststore** check box is selected in step 3. In the current example, we did not specify a different path for truststore (which means to use the same file for the keystore and truststore for the application server), and therefore, the wizards will skip step 5.

Step 6. Specify digital certificate

Figure 8. Select digital certificate



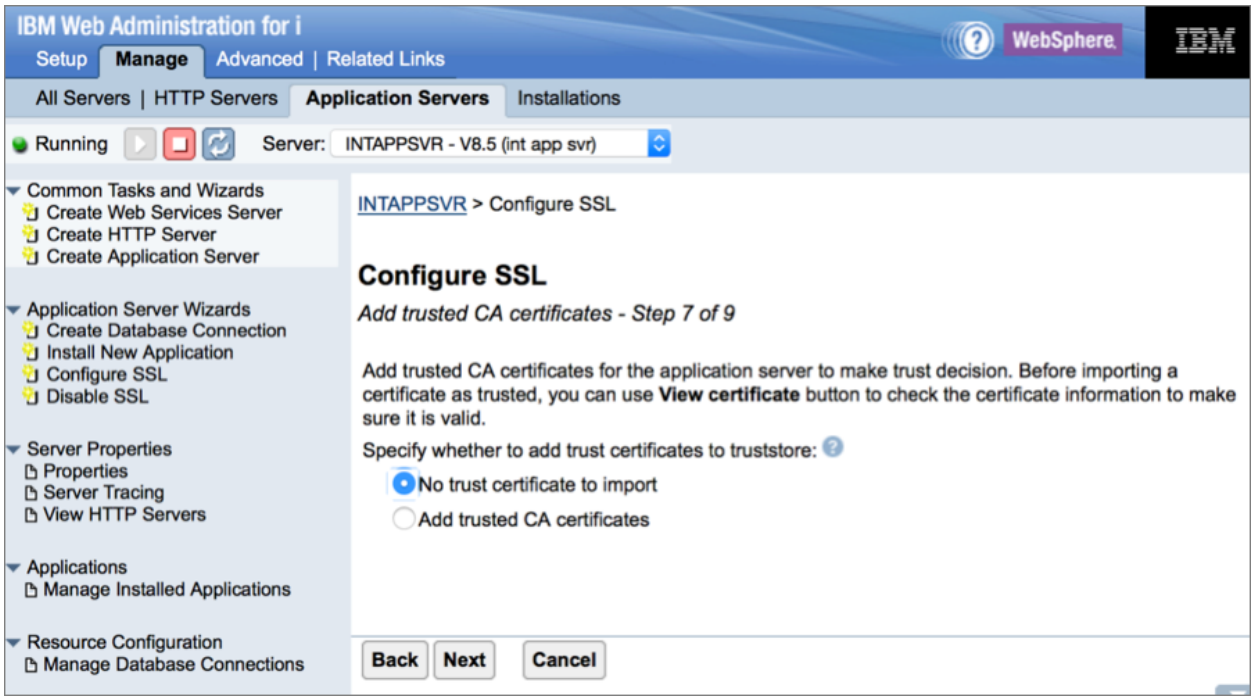
In step 6, as shown in Figure 8, select the existing certificate from the keystore and the digital certificate, **MYKEY**, and click **Next**.

The wizard provides this screen only when there is a certificate available in the specified keystore file. If no certificate is available, a self-signed certificate is created by this wizard. A self-signed certificate is generated with the following settings:

- DN: CN=*host_name*,O= IBM Web Administration for i,C=US
- Validity period: 365 days
- Algorithm: SHA256withRSA
- Key size: 2048 bits

Step 7. Add trusted CA certificates

Figure 9. Add trusted CA certificates

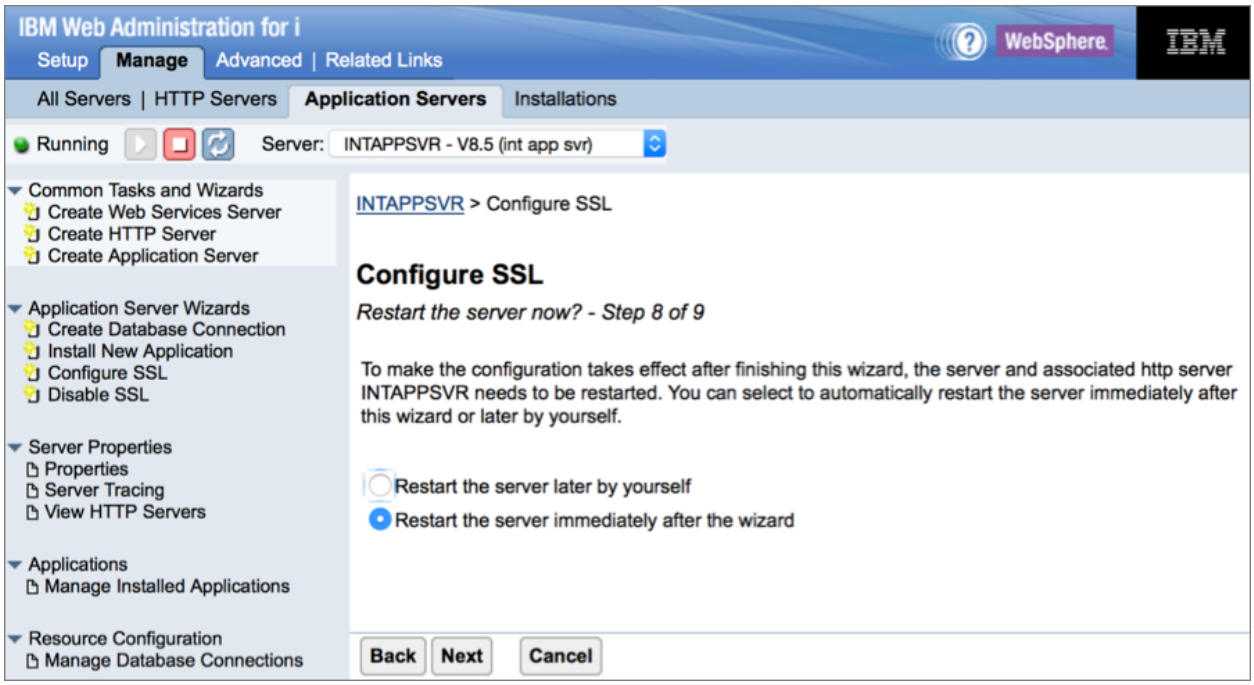


If an advanced client authentication is required for the SSL, trusted CA certificates should be imported to the truststore to help the server make the trust decision. Truststore is the same file as keystore, unless you specified a different file for it in step 3.

In this example, no client authentication is required. You can keep the default option on this page and click **Next**.

Step 8. Restart the server

Figure 10. Restart the server



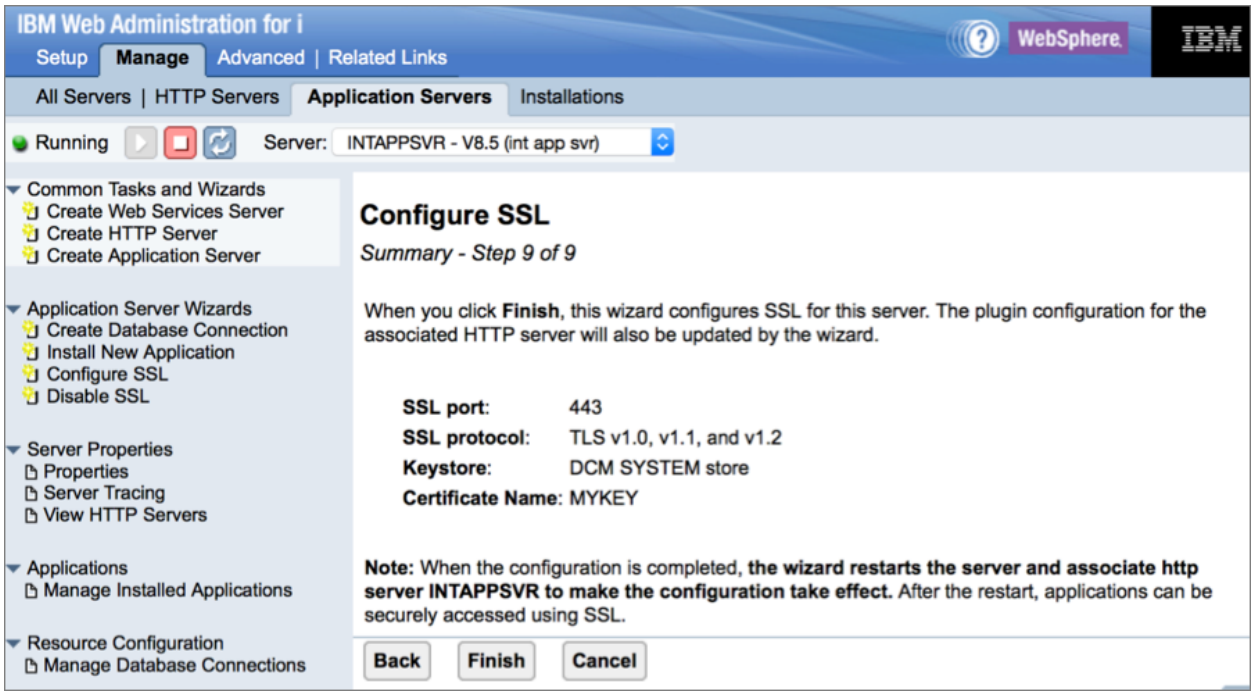
As shown in Figure 10, select the **Restart the server immediately after the wizard** option to enable the wizard to restart the server for the configuration changes to take effect. Click **Next**.

The IAS v8.5 and IWS 2.6 servers are based on the IBM WebSphere® Liberty profile container. If the dynamic update on the configuration is enabled for the application server (by default, the Web Administrator for i GUI created IAS v8.5 and IWS2.6 is disabled with dynamic updates.), even without restarting, the application server can detect the SSL configuration updates. But if a CMS keystore is used for the SSL, you must restart the server for the changes to take effect. This is because, the CMS keystore provider is not included by default in the Java security providers on IBM i and a Java virtual machine (JVM) restart is needed after the wizard added the provider for the application server.

Because there is a front-end HTTP server and the associated plug-in file was updated during the SSL configuration, we restart the server in this example for all the changes to take effect.

Step 9. Finish configuring the SSL wizard

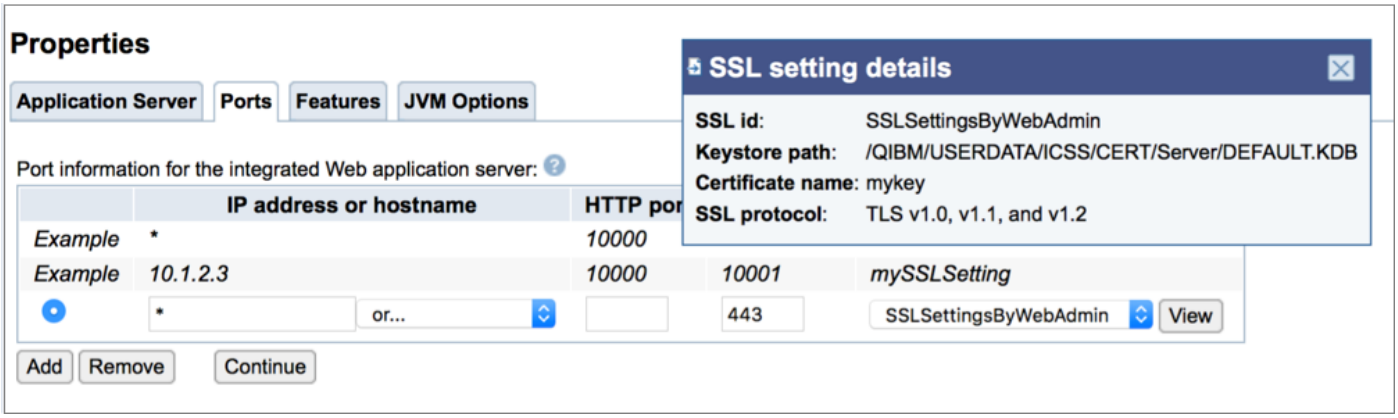
Figure 11. Summary of the Configure SSL wizard



As shown in Figure 11, the summary page shows all the information being used for the SSL configuration including the SSL port and protocol, the keystore, and the certificate name to be used. After clicking **Finish**, the wizard processes the configuration changes.

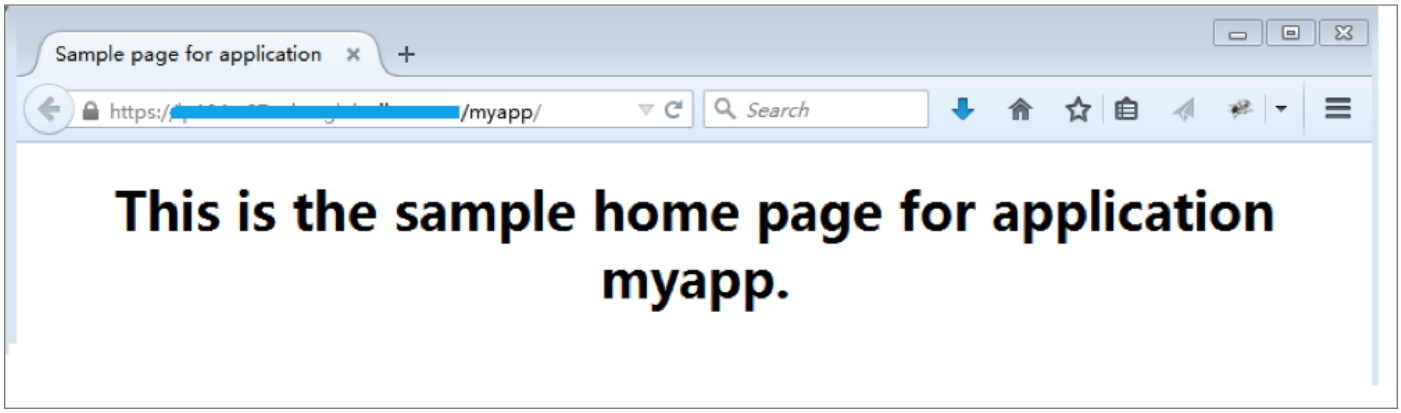
After the Configure SSL wizard completes and the server restarts, SSL is configured for the server, INTAPPSVR. Under **Properties**, click the **Ports** tab. You can find the server is listening on HTTPs port 443. Click **View** to check the details about the SSL settings. If there are several SSL settings configured for the server, you can also specify which SSL to use for a HTTPS port here.

Figure 12. SSL setting for a HTTPS port



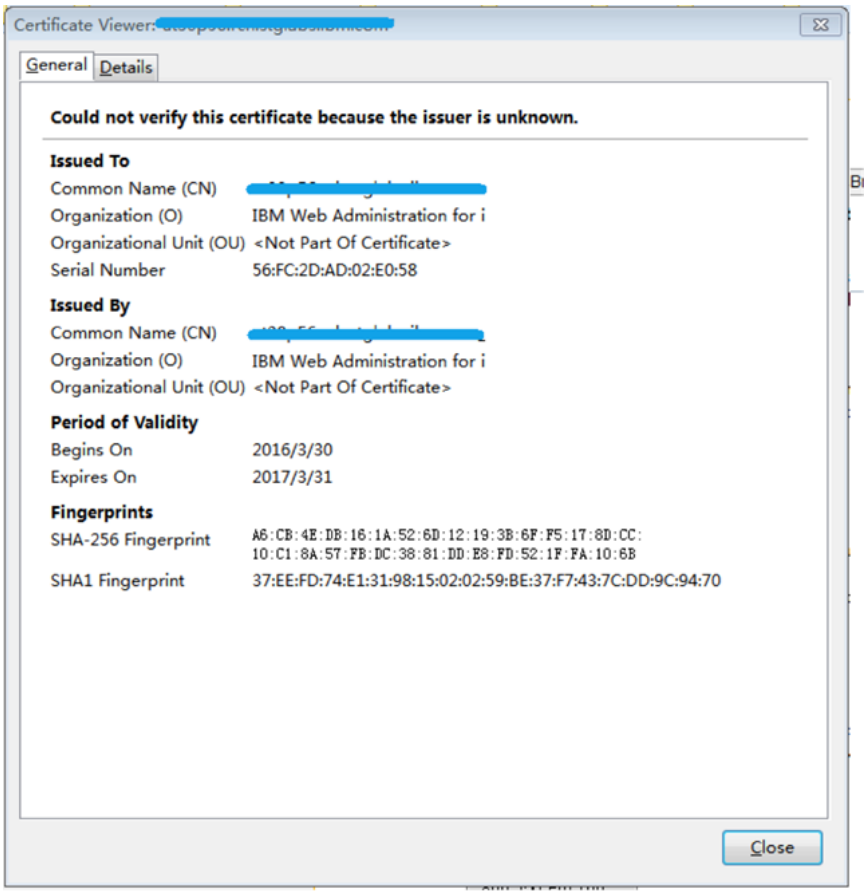
You can now access the *myapp* application through SSL with port 443.

Figure 13. Application accessed through SSL



You can also view the website certificate on your browser, as shown in Figure 14.

Figure 14. Certificate information



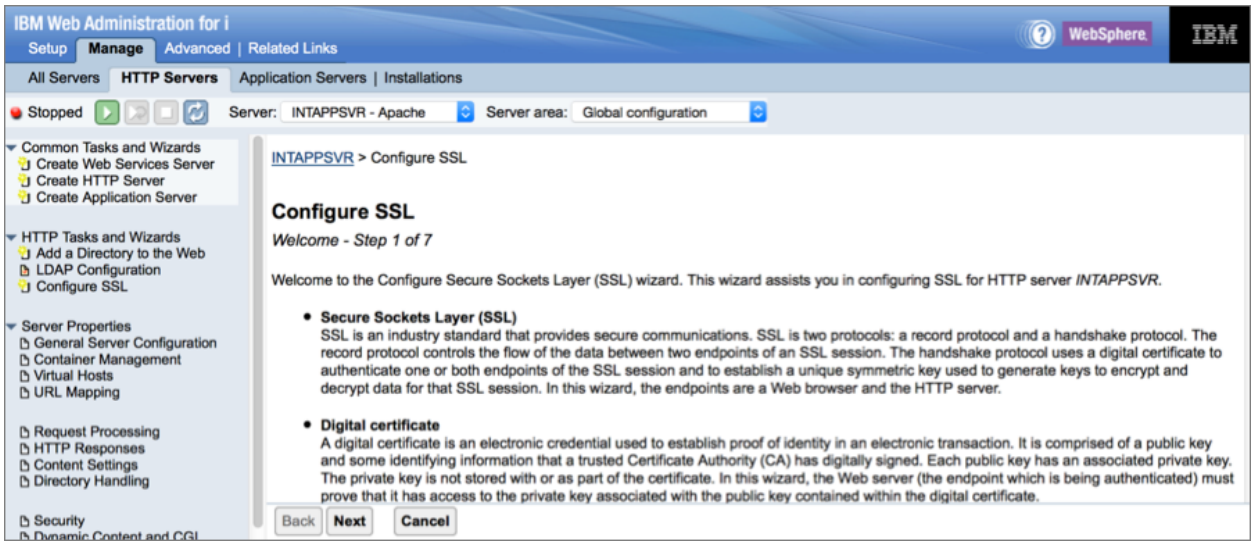
In the background, the SSL configuration is added to the server.xml file for a normal instance. For admin instances, the SSL configuration is added to a customized XML file that is included in the server.xml file and is located at resources/security/admin-cust.xml. For example, the configuration is as follows:

Listing 1. Sample code listing

```
<sslDefault sslRef="SSLSettingsByWebAdmin"/>

<keyStore id="KeyStoreByWebAdmin" location="/QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.KDB"
 password="{xor}Lz4sLChvLTs=" provider="IBMi5OSJSSEProvider" type="IBMi5OSKeyStore"/>

<ssl id="SSLSettingsByWebAdmin" keyStoreRef="KeyStoreByWebAdmin" serverKeyAlias="MYKEY"
 sslProtocol="SSL_TLSv2" trustStoreRef="KeyStoreByWebAdmin"/>

<httpEndpoint host="*" httpPort="-1" httpsPort="443" id="HttpEndpointByWebAdmin">

<sslOptions sslRef="SSLSettingsByWebAdmin"/>

</httpEndpoint>
```

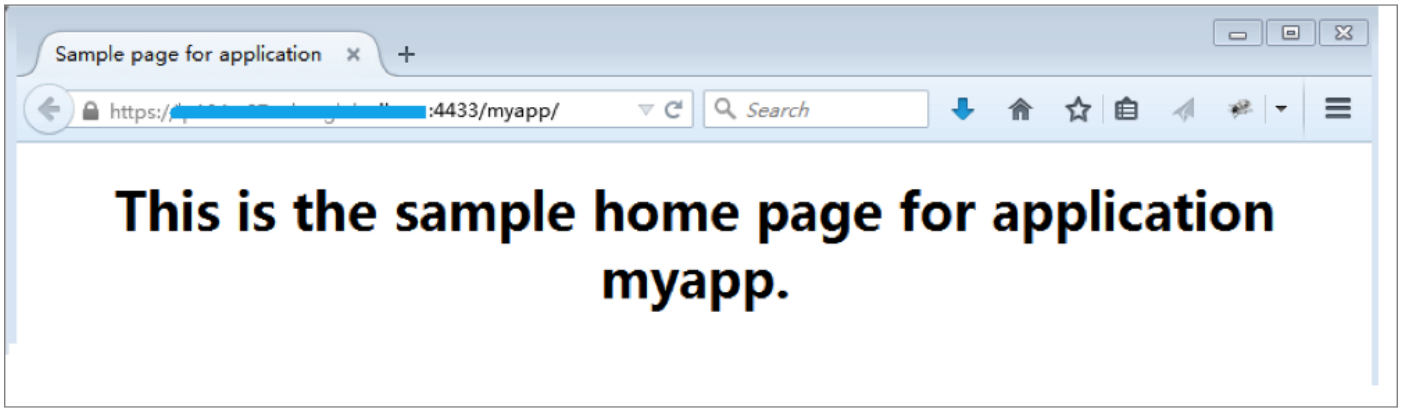
As there is an associated HTTP server with INTAPPSVR, we can set up SSL for the HTTP server to enforce SSL communication from the front-end HTTP server too. Click the **Manage** tab, and within that click the **HTTP Servers** tab, and then select the associated HTTP server, **INTAPPSVR**. In the left pane, click **Configure SSL** to launch the wizard and then follow the wizard to configure SSL with port 4433 for the HTTP server.

Figure 15. Configure SSL for HTTP server



After completing the wizard and restarting the server, you can access the application on the application server both from the front-end HTTP server and the application server through SSL.

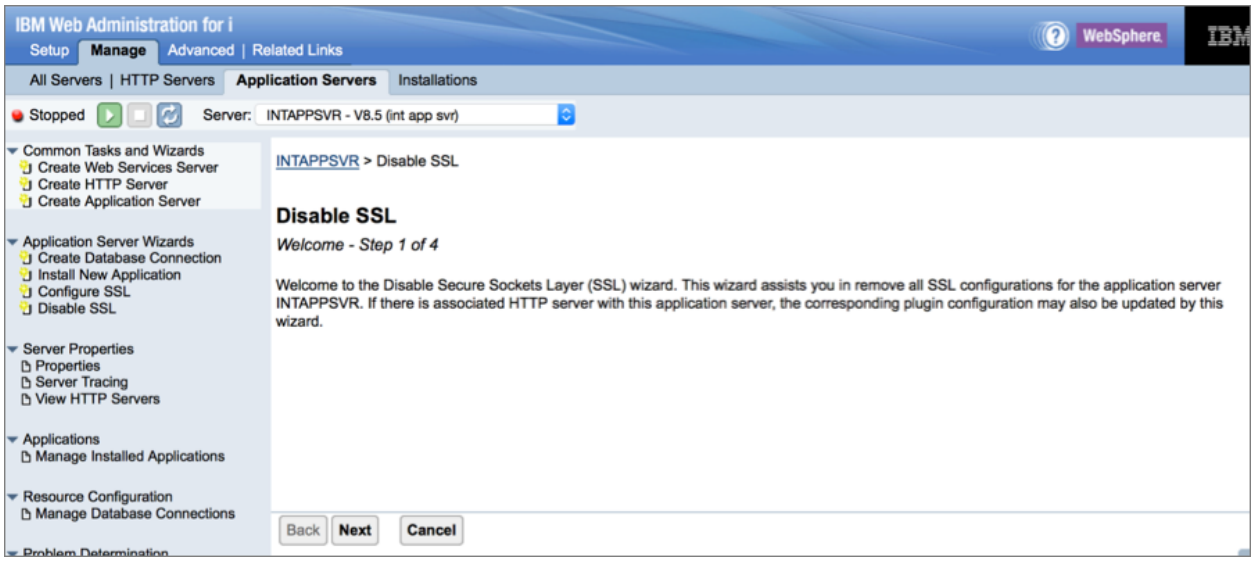
Figure 16. Application accessed through HTTP server with SSL



Disable SSL

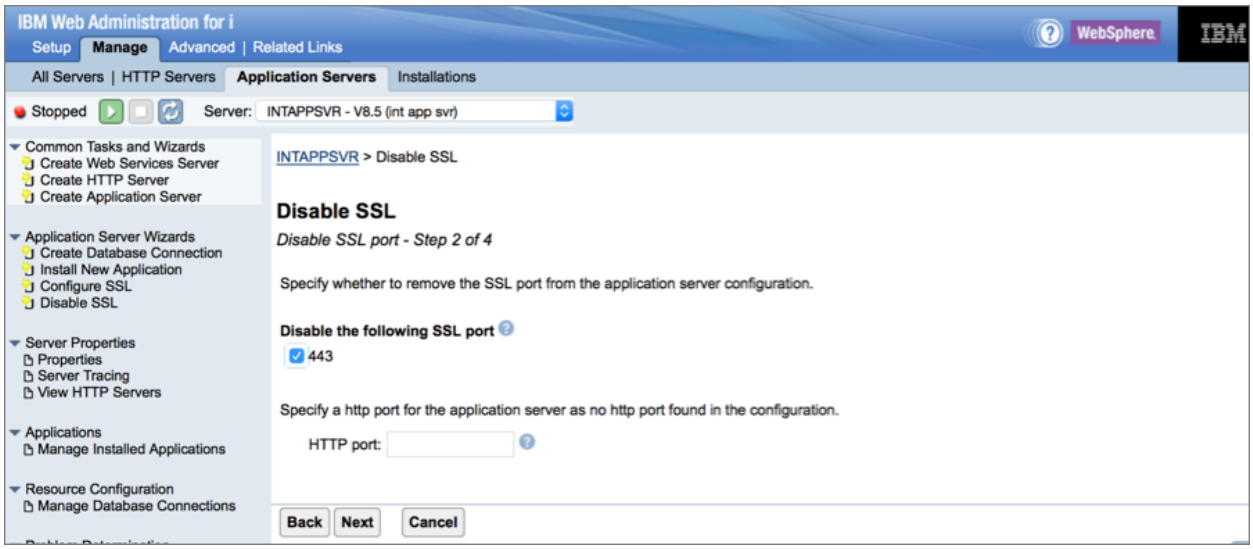
We earlier introduced how to configure SSL for the application server, INTAPPSVR. If you no longer require SSL, you can use the Disable SSL wizard to clear all SSL configurations for the server.

Figure 17. Disable SSL



Under **Manage**, click the **Application Servers** tab, and select the application server **INTAPPSVR**. In the left pane, click **Disable SSL** to launch the wizard. Then, click **Next** on the welcome page.

Figure 18. Disable SSL port

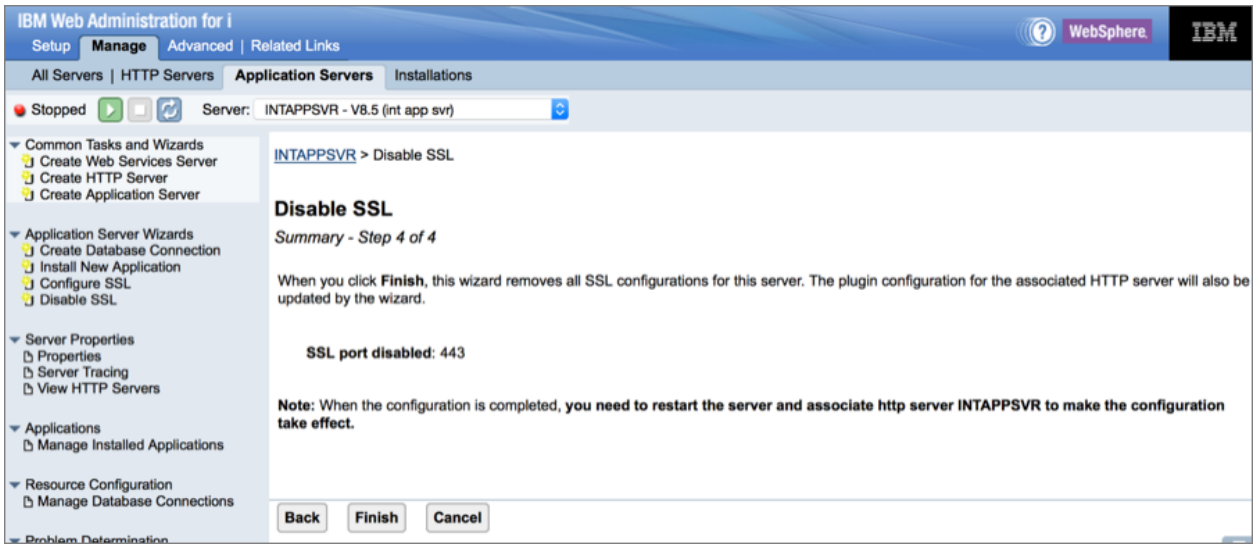


When disabling SSL for a server, the wizard can remove the SSL ports configured on the server from configuration if the ports are selected to disable (as shown in Figure 18). Ports that are not selected can be kept in the configuration for future use. If there is no HTTP port available for the current server, it is required to specify one. In this example, disable port 443 and specify a HTTP port for INTAPPSVR and click **Next**.

Figure 19. Restart server

Restart the server immediately after completing the wizard and click **Next**.

Figure 20. Summary of Disable SSL wizard



After clicking **Finish**, the wizard removes all SSL settings in server.xml for normal instances or admin-cust.xml for admin instances. Also, it updates the corresponding plug-in file in the associated HTTP server. Note that if there are other XML files configured with SSL setting are included, the Disable SSL wizard will not update any content.

Summary

This article has provided an example that illustrates the configuration of SSL for an integrated application server with an existing certificate in the DCM *SYSTEM store. You can easily set up SSL for your applications regardless of an existing certificate or without a certificate by using the Web Administrator for i GUI wizard. You can follow the steps provided in this article to set up your SSL.

Reference

- For IBM Web Administration for i introduction, refer to the product page and Knowledge Center.
- For more information about DCM, refer IBM Digital Certificate Manager.
- For WebSphere Liberty profile, refer Knowledge Center.