

Configuring SSL/HTTPS in InfoSphere Information Server

versions 8.5 - 11.3

Scott Brokaw
04/21/2015



Speaker Introduction

Agenda

- Background
- Personal Certificate Requests
- Security enhancements to Information Server 11.3
 - Storing certificates for client applications
 - Additional 11.3 client configuration (Optional)
- Configuring client tiers (IIS version 8.5-9.1)
- Configuring services and engine tiers (IIS versions 8.5-9.1)
- Configuring WebSphere (IIS versions 8.5-9.1)

3



This presentation will cover some background on SSL/HTTPS. We will briefly discuss what SSL is and how Information Server implements it.

We will briefly cover Personal Certificate requests – which is available as an option through WebSphere if you wish to replace the default certificate.

We'll discuss the security enhancements made to 11.3 including how to store the default certificate for client applications.

We'll cover how to configure the client tiers for SSL in Information Server 8.5-9.1

We'll cover how to configure the services and engine tiers for SSL in Information Server 8.5-9.1

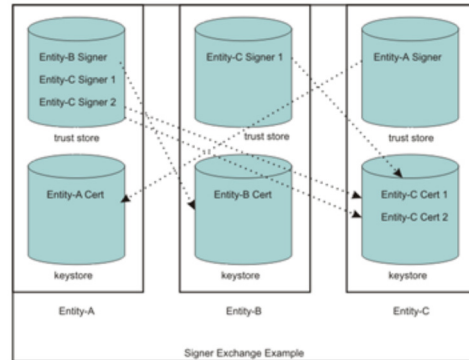
Lastly we'll cover possible configuration changes available within WebSphere for WebSphere versions bundled with Information Server 8.5-9.1

Background

- InfoSphere Information Server supports SSL (Secure Socket Layer) communication between client and application components
- SSL provides Encryption and Identification benefits
 - **Encryption:** Data sent over a SSL connection
 - **Identification:** Communication is permitted only if the server is positively verified (i.e. a certificate)
- At version 8.5, 8.7, and 9.1 SSL is not enabled by default
 - By default, WebSphere will be listening for requests on a secure port (default 9443)
 - To configure SSL communication, configuration needed on the client components
- At version 11.3, SSL is enabled by default

Background

- SSL Certificates
 - Self-signed
 - Publically-signed, typically by a CA (Certificate Authority)
- Certificate is stored in the keystore
- Signer is stored in the truststore
- Information Server has several places where a valid truststore/keystore exchange must exist
 - Client tier -> Services tier
 - ASBNode -> Services tier
 - ASBServer -> Services tier
 - IMAM



5

As discussed on the previous slide, SSL communication involves not only encryption of data but a validation of trust (i.e. identification). Self-signed certificates are certificates that are provided by or created by the entity that is being trusted, i.e. there is no third party verification to establish trust.

In order for a successful SSL handshake to occur, the client must have a signer in it's trust store that matches a certificate in the target server's keystore.

This screenshot is taken from WebSphere's documentation. Entity A can connect to both Entity B and Entity C because Entity A's trust store contains signers that match certificates on Entity B and Entity C. However, Entity B can't connect to Entity A because Entity B does not have a Signer for Entity A's certificate.

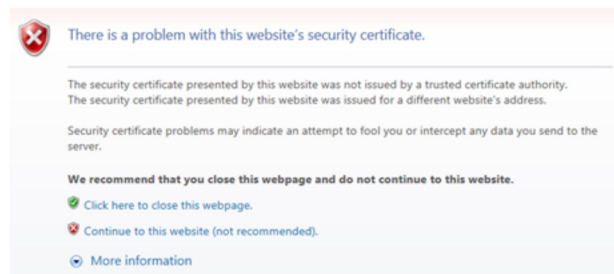
To put this in perspective for InfoSphere Information Server, several truststore/keystore exchanges must exist. On the client tier, Designer, Director, and Administrator clients at 11.3 leverage the Windows trust store and must have a signer that corresponds to the certificate in WebSphere. The Designer Client at 9.1 also leverages the Windows trust store. For command line tools on the client tier at 11.3 and for all other clients at 8.5, 8.7, and 9.1 a

trust store is maintained in ASBNode. For the Engine and Services tiers, trust stores are maintained in both ASBNode and ASBServer

IMAM (IBM InfoSphere Metadata Asset Manager) is installed with self-signed certificates that are used to encrypt the communication between components running in WebSphere Application Server and Apache Tomcat (or WebSphere Liberty for 11.3)

Background

- SSL Certificates in WebSphere (post WAS 6.1) are unique chained certificates
 - For most scenarios, this is sufficient
 - [Replacing default “self-signed” certificates in WebSphere](#)



- IMAM
 - [Apache Tomcat \(LWAS at 11.3\) -> WAS](#)
 - [WAS -> Apache Tomcat \(LWAS at 11.3\)](#)

6



By default, WebSphere Application Server creates a unique chained certificate for each node. The chained certificate is signed with a root, self-signed certificate stored in WebSphere. In most cases this is sufficient, steps can be taken to store the certificate at each client machine so the warning message on this slide no longer appears. This procedure will be covered later in the presentation.

This presentation will not cover in detail replacing the default personal certificate in WebSphere. We will briefly cover Personal Certificate requests on the next slide, but consult your specific WebSphere's version's documentation for instructions and work with your WebSphere Administrator and System Administrator to acquire a certificate. A link to Information Server 11.3 documentation (WebSphere 8.5.5.x) is provided on this page.

For replacing the certificates used in IMAM in either direction, two technotes are provided on the slide. Consult the backup slides for specific considerations when using 11.3 since WAS Liberty (LWAS) replaces Apache Tomcat.

The screenshot on this slide demonstrates an example of a warning generated

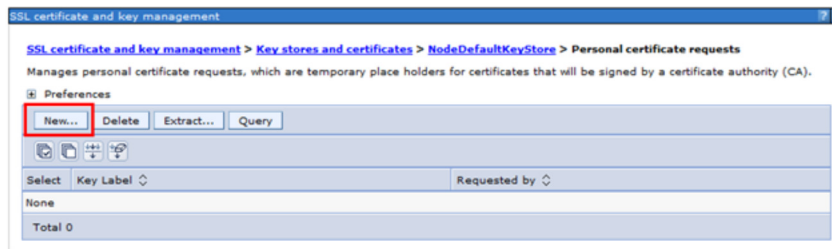
by a browser. Similar warnings can be generated by the operating system, indicating that the certificate being used was not issued by a trusted certificate authority. Browser and Operating System vendors such as Microsoft, Mozilla, or Google trust certain certificate authorities (CAs). These CAs provide a “chain of trust”. An oversimplified example for a Windows desktop: Microsoft “trusts” Verisign (a certificate authority) if Verisign “trusts” your site, the certificate your server provides the client, is then “trusted”. This trust is typically gained by paying for a validation in order for a CA to “trust” you are who you say you are.

Using a certificate that is signed by a CA will prevent this warning message. Some companies have internal CAs that are installed on all company laptops/desktops as part of the company image. This allows for internal certificates to be generated against an internal CA. This may be one option to pursue with your System Administrator if you wish to resolve the warning displayed on this slide.

Personal Certificate Requests

- Generate a certificate request to pass to your CA provider

Security > SSL certificate and Key Management > Under Related Items Key stores and certificates > NodeDefaultKeyStore > Under Additional Properties Personal Certificates



General Properties

* File for certificate request

Certificate information

* Key label

Signature algorithm
SHA1withRSA

Key size
2048 bits

* Common name

Organization

Organizational unit

Locality

State or province

Zip code

Country or region
(none)

Apply OK Reset Cancel

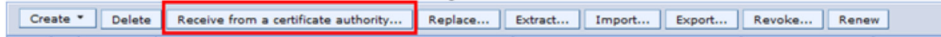
7

One way to generate a personal certificate is to create a certificate request through WebSphere that can be passed to your CA and signed. This step will generate an actual certificate request file that is to be sent to your CA.

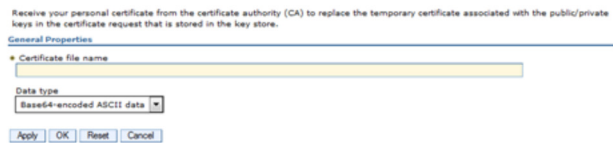
Personal certificate requests are temporary place holders for certificates that will be signed by a certificate authority (CA). The private key is generated during the certificate request generation, but only the certificate is sent to the CA. The CA generates a new certificate, signed by the CA.

Personal Certificate Requests

- Receive certificate from a certificate authority



- Provide the path to the certificate file provided by the CA



- Replace the default certificate

Select	Alias	Issued To	Issued By	Serial Number	Expiration
<input type="checkbox"/>	mlcavm139	OID.0.9.2342.19200300.100.1.3=albrokaw@us.ibm.com, UID=904892897, CN=mlcavm139.avg.usma.ibm.com, OU=IIGSupport, O=IBM.com, L="Littleton, MA", ST="Littleton, MA", C=US	CN=IBM INTERNAL INTERMEDIATE CA, O=International Business Machines Corporation, C=US	21125	Valid from Apr 14, 2015 to Apr 12, 2018.
<input checked="" type="checkbox"/>	default	CN=mlcavm139.avg.usma.ibm.com, OU=mlcavm139Node01Cell, OU=mlcavm139Node01, O=IBM, C=US	CN=mlcavm139.avg.usma.ibm.com, OU=Root Certificate, OU=mlcavm139Node01Cell, OU=mlcavm139Node01, O=IBM, C=US	7453509363085194	Valid from Oct 23, 2014 to Oct 23, 2015.
<input type="checkbox"/>		CN=mlcavm139.avg.usma.ibm.com, OU=Root Certificate, OU=mlcavm139Node01Cell, OU=mlcavm139Node01, O=IBM, C=US	CN=mlcavm139.avg.usma.ibm.com, OU=Root Certificate, OU=mlcavm139Node01Cell, OU=mlcavm139Node01, O=IBM, C=US	7453508120274236	Valid from Oct 23, 2014 to Oct 19, 2029.

Replace with: mlcavm139

Once you receive the certificate back move the file to the filesystem where WebSphere is installed.

If using WAS standalone, Open NodeDefaultKeyStore, select Personal Certificates. Select the option Receive from a certificate authority and provide the certificate file name of the certificate that was provided by the CA.

If using a WAS Cluster, you'll need to manage this on the Webserver you've configured.

Once the certificate is in WebSphere, replace the default certificate with the new CA signed certificate. You can choose at this point to delete the old certificate and signers – if you do not delete them it will not impact the configuration.

Restart WebSphere for the changes to take affect. By default, WAS prompts you to accept the certificate if it is not trusted when you run WAS command line utilities, such as the serverStatus command or the stopServer command. The certificate can be accepted by directly running the stopServer.sh[.bat] command i.e. do not run it from a Windows Service or from a wrapper script like MetadataServer.sh where you can not interact with the prompt. You can also use the WebSphere retrieveSigners command to avoid this initial prompt.

Once WebSphere is restarted, be sure to run UpdateSignerCerts in ASBNode/bin and ASBServer/bin on all tiers. This will be covered in detail later in the presentation

Security enhancements to Information Server 11.3

- SSL/HTTPS enabled by default for every installation
 - https communication is enforced
 - http communication is not permitted
- Windows client presents a self-signed certificate warning
- Windows needs to be told to trust this self-signed certificate
- Two methods to install self-signed certificates
 - Windows (through the DataStage client prompts)
 - Internet Explorer



9



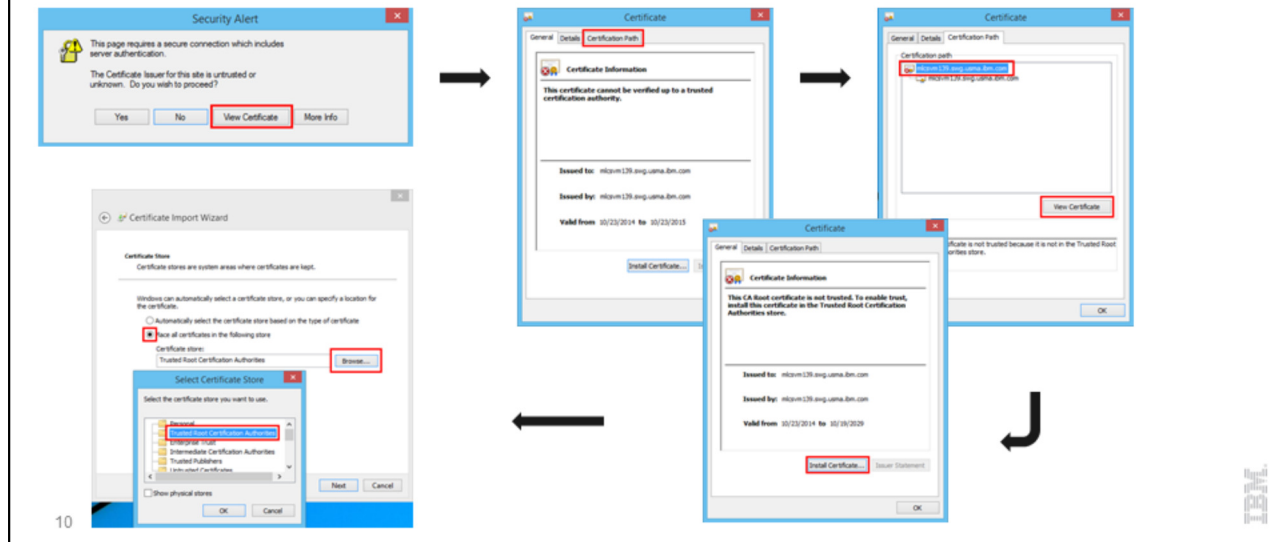
Information Server 11.3 enabled SSL/HTTPS by default. If using the default certificate, a certificate warning, similar to the warning when navigating to a webpage in a browser with an untrusted certificate, will be displayed when logging into the Windows clients (DataStage Designer, Director, Administrator)

If you are not going to replace the certificate with one trusted by a CA, the certificate needs to be added to the Windows trust store manually on each Windows client. Please note that a similar prompt will be seen for the Information Server 9.1 Designer client. You can follow the same steps as 11.3 to install the certificate for the Designer.

There are two methods to install self-signed certificates. The first is through the Windows alert that is displayed when trying to login. The second method is to use Internet explorer to access the Windows trust store.

Storing certificates for client applications

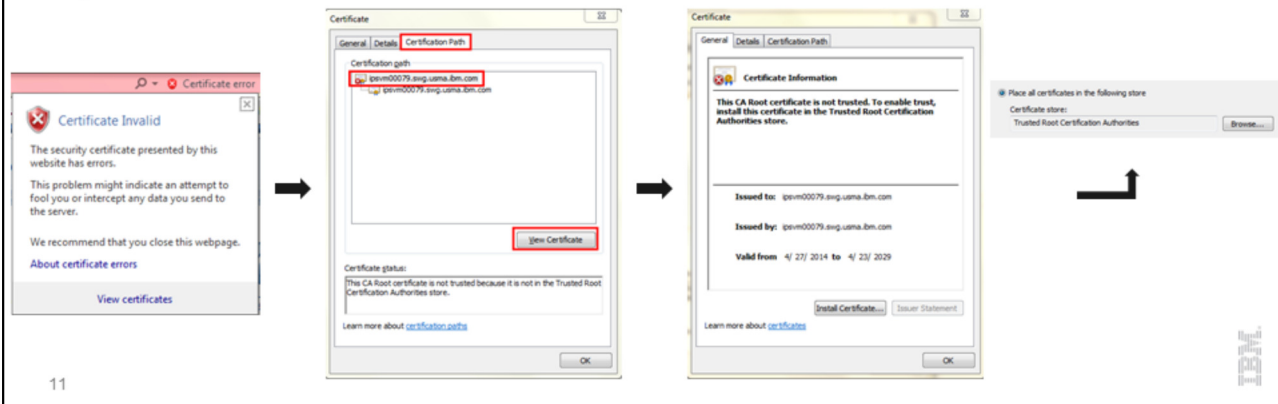
- Storing certificates through Windows (through the DataStage client prompts)



This slide displays the prompts you can access through the Windows Security Alert that is launched by the DataStage client. Ensure to install the root certificate by selecting it on the Certification Path. Install the certificate into the Trusted Root Certification Authorities in the Windows trust store.

Storing certificates for client applications

- Storing certificates through Internet Explorer
- Navigate to:
<https://hostname:9443/ibm/iis/console>



The certificate can be accessed by navigating to <https://hostname:9443/ibm/iis/console> in Internet Explorer. Once the page loads, click on the certificate error to view the certificate. The steps to install the certificate from this point are identical to the Windows method discuss on the previous slide.

Additional 11.3 Client Configuration (Optional)

- [Optional] Change the `com.ibm.ssl.protocol` property
 - Default of `SSL_TLSv2`
 - `iis.client.site.properties` file is located:
 `<install location>/ASBNode/eclipse/plugins/com.ibm.iiis.client`
- [Optional] `UpdateSignerCerts.bat`
 `<install location>/ASBNode/bin/UpdateSignerCerts.bat -url https://hostname:port
 -user USERNAME -password PASSWORD`

You may choose to change the `com.ibm.ssl.protocol` property to force a particular protocol to be used (i.e. to remediate POODLE vulnerability)

If other client side utilities need to be run such as command line tools, run `UpdateSignerCerts`

Configuring SSL/HTTPs

Versions 8.5-9.1

Configuring client tiers (version 8.5-9.1)

Ensure port 9443 or equivalent is open in your firewall

- To determine the port, execute the following command on your services tier:
`grep was.secure.default.host.port Version.xml`
- It is also possible to check the port from within WebSphere
 - Within the WAS Admin console select **Servers > WebSphere application servers > *server_name***, Under Communications select **Ports**
 - Port name is `WC_defaulthost_secure`



Application servers

Application servers > *server1* > Ports

Specifies the TCP/IP ports this server uses for connections.

Preferences

New... Delete

Select Port Name Host Port Transport Details

You can administer the following resources:

Select	Port Name	Host	Port	Transport Details
<input type="checkbox"/>	WC_defaulthost_secure	*	9443	View associated transports
<input type="checkbox"/>	WC_defaulthost	*	9080	View associated transports
<input type="checkbox"/>	WC_adminhost_secure	*	9043	View associated transports
<input type="checkbox"/>	WC_adminhost	*	9060	View associated transports

14



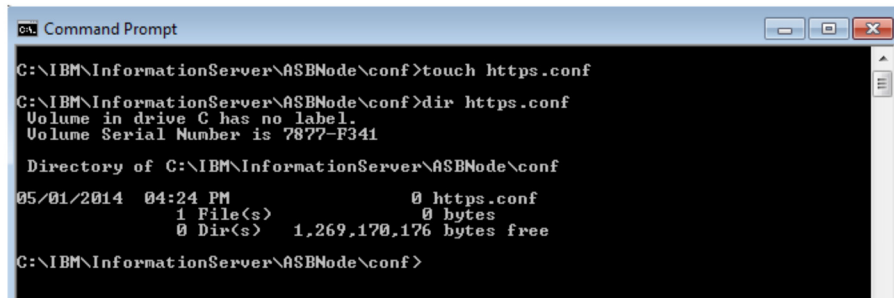
The secure port (9443 by default) should already be listening at releases 8.5-9.1. The first step is identifying the port so then you can ensure it is opened in any firewall rules that have been configured.

You can look in the `Version.xml` file by using the `grep` command displayed on this slide, or you can check the `WC_defaulthost_secure` port from within the WebSphere Administration console.

Configuring client tiers (version 8.5-9.1)

- Create 0 byte file https.conf in the following directory:

C:\IBM\InformationServer\ASBNode\conf



```
Command Prompt
C:\IBM\InformationServer\ASBNode\conf>touch https.conf
C:\IBM\InformationServer\ASBNode\conf>dir https.conf
Volume in drive C has no label.
Volume Serial Number is 7877-F341

Directory of C:\IBM\InformationServer\ASBNode\conf
05/01/2014  04:24 PM                0 https.conf
             1 File(s)                0 bytes
             0 Dir(s)  1,269,170,176 bytes free

C:\IBM\InformationServer\ASBNode\conf>
```

15



Create a zero byte file called https.conf in C:\IBM\InformationServer\ASBNode\conf directory (please note the installation might vary depending where the client was installed). This file will tell the client tier to use SSL. Once this file is present the client will only use SSL and to go back to unsecure connections, this file needs to be deleted or moved. After the https.conf file has been created, the Signer Certificate can be retrieved from the WebSphere Application Server.

Configuring client tiers (version 8.5-9.1)

- Modify the sas.client.props file:
<install location>/ASBNode/eclipse/plugins/com.ibm.isf.client/sas.client.props
- Change the properties:
 - com.ibm.CSI.performTransportAssocSSLTLSRequired=true
 - com.ibm.CSI.performTransportAssocSSLTLSSupported=true
- [Optional] Change the com.ibm.ssl.protocol property
 - Default of SSL_TLSv2
 - ssl.client.props file is located:
<install location>/ASBNode/eclipse/plugins/com.ibm.isf.client/ssl.client.props

16



The next step is to modify the sas.client.props file changing the properties that are displayed on this slide to true.

An optional step, like the 11.3 configuration, is to modify the come.ibm.ssl.protocol property to change the protocol used for the connection. The property can be changed on the client tier at 8.5-9.1 in the ssl.client.props file located in the com.ibm.isf.client plugin in the ASBNode/eclipse directory.

Configuring client tiers (version 8.5-9.1)



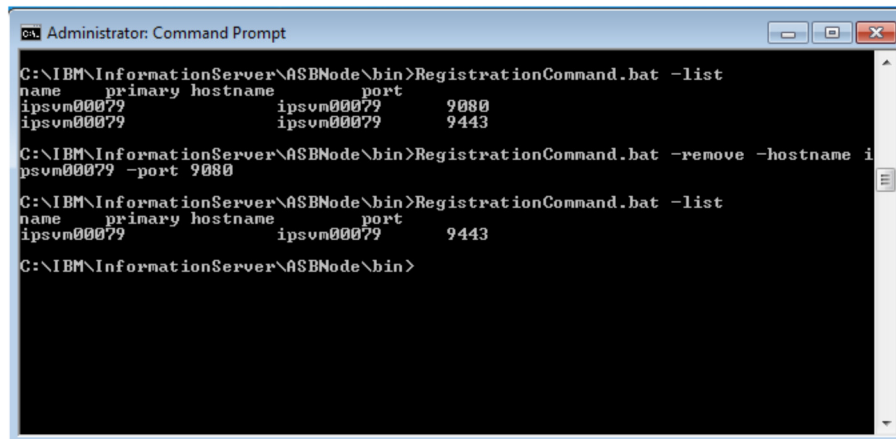
18



Login to the DataStage clients using the secure port.

Configuring client tiers (version 8.5-9.1)

- [Optional] Remove the non-secure entry for the services tier



```
Administrator: Command Prompt
C:\IBM\InformationServer\ASBNode\bin>RegistrationCommand.bat -list
name      primary hostname      port
ipsvm00079      ipsvm00079      9080
ipsvm00079      ipsvm00079      9443
C:\IBM\InformationServer\ASBNode\bin>RegistrationCommand.bat -remove -hostname i
psvm00079 -port 9080
C:\IBM\InformationServer\ASBNode\bin>RegistrationCommand.bat -list
name      primary hostname      port
ipsvm00079      ipsvm00079      9443
C:\IBM\InformationServer\ASBNode\bin>
```

19



An optional step is to remove the non-secure entry from the Client's history.

Open a command prompt and navigate to the C:\IBM\InformationServer\ASBNode\bin directory and run RegistrationCommand.bat -list command to get the current list of registered services tiers.

Any hostnames on the non-secure ports can be removed to minimize the drop down for registered services tiers. To remove unwanted entries, simply run the following command: RegistrationCommand.bat -remove -hostname <your host name> -port <unsecure port> (typically 9080).

At this point in the presentation, your client tier is configured to authenticate using SSL/HTTPs. The rest of the steps can be followed if you wish to configure the remaining tiers to also communicate over SSL/HTTPs although they do not have to be configured in order for the client tier to use SSL/HTTPs i.e. both secure and non-secure connections can co-exist.

Configuring services and engine tiers (version 8.5-9.1)

- Create 0 byte file https.conf in the following directories:
 - Engine Tier(s):
 <install location>/ASBNode/conf
 - Services Tier(s):
 <install location>/ASBServer/conf

- Use the commands:
 touch https.conf <install location>/ASBServer/conf
 touch https.conf <install location>/ASBNode/conf

20



Just as you did with the client, create a 0 byte file, https.conf in both the ASBNode and ASBServer conf directories on your Engine and Services tier. If you have the Engine and Services tier on the same machine, you would be creating two https.conf files, one in the ASBNode/conf directory and one in the ASBServer/conf directory.

You can use the touch command to create the https.conf file.

Configuring services and engine tiers (version 8.5-9.1)

- Modify the sas.client.props file:
 - Engine Tier(s):
 <install location>/ASBNode/eclipse/plugins/com.ibm.isf.client/sas.client.props
 - Services Tier(s):
 <install location>/ASBServer/conf/sas.client.props

Change the properties:

```
com.ibm.CSI.performTransportAssocSSLTLSRequired=true  
com.ibm.CSI.performTransportAssocSSLTLSSupported=true
```

- [Optional] Change com.ibm.ssl.protocol property
 - Default value of SSL_TLS
 - ssl.client.props file is located:
 - Engine Tier(s):
 <install location>/ASBNode/eclipse/plugins/com.ibm.isf.client/ssl.client.props
 - Services Tier(s):
 <install location>/ASBServer/conf/ssl.client.props

21



Again as we did on the client tier, we need to modify the sas.client.props file changing the properties that are displayed on this slide to true. There is a sas.client.props file in both ASBNode and ASBServer – the exact locations are shown on this slide.

The optional step of modifying the come.ibm.ssl.protocol property is also available for the Engine and Services tiers. The location of the ssl.client.props file is shown on the slide

Configuring services and engine tiers (version 8.5-9.1)

- Retrieve certificate from by running:
UpdateSignerCerts.sh[bat] -v -host *host_name* -port *port_number*
- Run the UpdateSignerCerts command as root in all of the Engine and Services tiers from the following directories
 - Engine:
<install location>/ASBNode/bin
 - Services:
<install location>/ASBServer/bin
- This ensures the truststore for each tier is updated with the certificate
- UpdateSignerCert must be run:
 - After enabling SSL for RMI/IIOP or HTTPS for the first time
 - After replacing or updating a server certificate
 - After installing a new client or engine tier (Command to be run on new client or engine tier only)
 - After adding a new managed node to the cluster and a new custom profile is created (horizontal clustering)

22



You will also need to run UpdateSignerCert to update the truststore in ASBNode and ASBServer. UpdateSignerCert should be run as root as by default, the truststore is owned by root. You need to run UpdateSignerCert from both ASBNode/bin and ASBServer/bin.

The same requirements we spoke about for the client tier for running UpdateSignerCert apply to the Engine and services tiers. They're displayed on this slide again for convenience.

Configuring WebSphere

- [Optional] For Information Server 8.5-9.1, the embedded WebSphere profile will contain the following setting:
 - CSiv2 Transport Layer – SSL-supported

The screenshot displays the 'Global security > CSiv2 inbound communications' configuration page. It is divided into several sections:

- CSiv2 Attribute Layer:** Includes checkboxes for 'Propagate security attributes' (checked), 'Use identity assertion' (unchecked), and a 'Trusted identities' text field.
- CSiv2 Transport Layer:** Features a 'Client certificate authentication' dropdown set to 'Supported'. Below it, a 'Transport' dropdown menu is highlighted with a red box, showing the following options: 'SSL-supported' (selected), 'TCP/IP', 'SSL-required', and 'SSL-supported'.
- CSiv2 Message Layer:** Includes a 'Message layer authentication' dropdown set to 'Supported' and a section for 'Allow client to server authentication with:' containing checkboxes for 'Kerberos' (unchecked), 'LTPA' (checked), and 'Basic authentication' (checked).
- Additional Properties:** Includes a 'Login configuration' text field with the value 'RMI_INBOUND' and a checked 'Stateful sessions' checkbox.

At the bottom left, there is a 'Centrally managed' indicator. At the bottom right, there is a small icon representing a server stack.

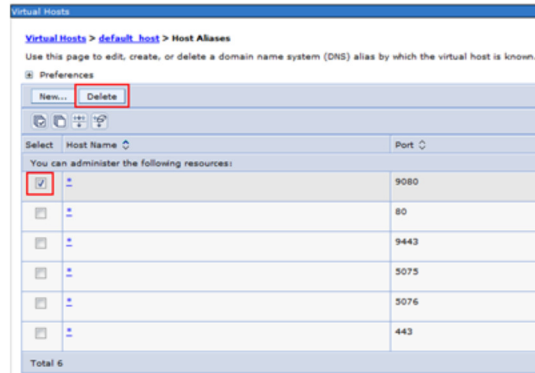
23

If you want to change the CSiv2 Transport Layer settings to require SSL or use TCP/IP – this is the place to do so within WebSphere.

Most of the time leaving the default SSL-supported setting is recommended.

Configuring WebSphere

- [Optional] For Information Server 8.5-9.1, remove the WC_defaulthost port (default 9080)
 - Identify your WC_defaulthost port:
 - Open **Servers > Servers Types > WebSphere application servers > server_name > Ports**
 - Delete the host alias
 - Open **Environment > Virtual hosts**. Select **default_host** and then **Host Aliases**



24



After removing the WC_defaulthost port, users will get an error when trying to access 9080

If you have a shortcut icon for the IS Web Console anywhere, you may wish to update the port in that shortcut to 9443 and the protocol to https

You can also simply block 9080 via the firewall.

Questions?

Join us for our next Support Technical Exchange!

Topic: Configuring the Complex Flat File Stage in InfoSphere Information Server

Date and Time: May 21, 2015, 11:00am ET

Presenter: Marcia Stewart, Senior Support Engineer, InfoSphere Information Server

Registration Link: <https://events.na.collabserv.com/register.php?id=af1636f1e7&l=en-US>

Backup Slides – IMAM Certificate replacement at 11.3

Follow the steps in the [technote](#) with the following modified steps:

2. Directory for the truststore,

C:\IBM\InformationServer\wlp\usr\servers\mis\resources\security

6. Considering the password remains same for the certificate, there is no need to change anything.

– If you decided to use a trust store password that was different than the previous truststore password (the default password is *changeit*), then you need to update the IBM LWAS *bootstrap.properties* file with the new password.

- Open a new command prompt and run the following command to encrypt your new password:

C:\IBM\InformationServer\ASBNode\bin\encrypt.bat

- The command will prompt you to enter the value to encrypt and output the encrypted value.

For example: *imam -> {iisenc}cniLiNhvTEKhQwtEwhZmUQ==*

- Edit the file to add the truststore password:

C:\IBM\InformationServer\wlp\usr\servers\mis\bootstrap.properties

These are the steps for IMAM with LWAS.