

InfoSphere Information Server

SSL setup for Information Server 8.5 using WebSphere 7.0



© 2011 IBM Corporation

This is the SSL Setup for Information Server 8.5 using WebSphere® 7.0 presentation.

Objective

- How to setup SSL in WebSphere 7.0 for Information Server 8.5

The objective of this presentation is to explain how to configure WebSphere 7.0 to use Secure Sockets Layer to be used with Information Server version 8.5. This presentation assumes that the Secure Sockets Layer certificate has already been installed. Throughout this presentation, Secure Sockets Layer is referred to as SSL.

Configuring SSL (1 of 8)

- Login to WebSphere administrative console as administrative user
- Click Security → SSL certificate and key management

The screenshot displays the WebSphere administrative console interface. On the left is a navigation tree with the following items: Welcome, Guided Activities, Servers, Applications, Services, Resources, Security (highlighted), Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. Under the Security section, the following sub-items are listed: Global security, Security domains, Administrative Authorization Groups (highlighted), SSL certificate and key management (highlighted), Security auditing, and Bus security. The main content area is titled "SSL certificate and key management" and contains the following text:

SSL configurations

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

In previous versions of this product, it was necessary to manually configure each endpoint for Secure Sockets Layer (SSL). In this version, you can define a single configuration for the entire application-serving environment. This capability enables you to centrally manage secure communications. In addition, trust zones can be established in multiple node environments by overriding the default, cell-level SSL configuration.

If you have migrated a secured environment to this version using the migration utilities, the old Secure Sockets Layer (SSL) configurations are restored for the various endpoints. However, it is necessary for you to re-configure SSL to take advantage of the centralized management capability.

Configuration settings

[Manage endpoint security configurations](#)

[Manage certificate expiration](#)

Use the United States Federal Information Processing Standard (FIPS) algorithms. Note: This option requires the TLS handshake protocol, which some browsers do not enable by default.

Dynamically update the run time when SSL configuration changes occur

Buttons: [Apply](#) [Reset](#)

Related Items

- [SSL configurations](#)
- [Dynamic outbound endpoint SSL configurations](#)
- [Key stores and certificates](#)
- [Key sets](#)
- [Key set groups](#)
- [Key managers](#)
- [Trust managers](#)
- [Certificate Authority \(CA\) chain configurations](#)

3

SSL setup for Information Server 8.5 using WebSphere 7.0

© 2011 IBM Corporation

Login to WebSphere administrative console with your WebSphere administrative user ID. Next, navigate to Security → SSL Certificate and key management.

Configuring SSL (2 of 8)

- Click SSL configurations

SSL certificate and key management

SSL configurations

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

In previous versions of this product, it was necessary to manually configure each endpoint for Secure Sockets Layer (SSL). In this version, you can define a single configuration for the entire application-serving environment. This capability enables you to centrally manage secure communications. In addition, trust zones can be established in multiple node environments by overriding the default, cell-level SSL configuration.

If you have migrated a secured environment to this version using the migration utilities, the old Secure Sockets Layer (SSL) configurations are restored for the various endpoints. However, it is necessary for you to re-configure SSL to take advantage of the centralized management capability.

Configuration settings

[Manage endpoint security configurations](#)

[Manage certificate expiration](#)

Use the United States Federal Information Processing Standard (FIPS) algorithms. Note: This option requires the TLS handshake protocol, which some browsers do not enable by default.

Dynamically update the run time when SSL configuration changes occur

Related Items

- [SSL configurations](#)
- [Dynamic outbound endpoint SSL configurations](#)
- [Key stores and certificates](#)
- [Key sets](#)
- [Key set groups](#)
- [Key managers](#)
- [Trust managers](#)
- [Certificate Authority \(CA\) client configurations](#)

4

SSL setup for Information Server 8.5 using WebSphere 7.0

© 2011 IBM Corporation

Click “SSL Configurations” on the right side of your screen under “Related Items”.

Configuring SSL (3 of 8)

- Click NodeDefaultSSLSettings

The screenshot shows the IBM WebSphere Administration Console interface. On the left is a navigation tree with the following structure:

- » Welcome
- ▣ Guided Activities
- ▣ Servers
- ▣ Applications
- ▣ Services
- ▣ Resources
- ▣ Security
 - » Global security
 - » Security domains
 - » Administrative Authorization Groups
 - » SSL certificate and key management
 - » Security auditing
 - » Bus security

The main content area is titled "SSL certificate and key management" and contains the following elements:

- » [SSL certificate and key management](#) > SSL configurations
- Defines a list of Secure Sockets Layer (SSL) configurations.
- ▣ Preferences
- New Delete
- Icons for New, Refresh, Add, and Remove
- Select Name Management Scope
- You can administer the following resources:
- NodeDefaultSSLSettings (cell):sawchuckNode01Cell:(node):sawchuckNode01
- Total 1

Next, click “NodeDefaultSSLSettings”.

Configuring SSL (4 of 8)

- Click Key stores and certificates

6

SSL setup for Information Server 8.5 using WebSphere 7.0

© 2011 IBM Corporation

Click “Keystores and certificates” on the right side of your screen under “Related Items”.

Configuring SSL (5 of 8)

- Select NodeDefaultTrustStore

SSL certificate and key management

SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings > Key stores and certificates

Defines keystore types, including cryptography, RAC(R), CMS, Java(TM), and all truststore types.

Keystore usages

SSL keystores

Preferences

New Delete Change password... Exchange signers...

Select	Name	Description	Management Scope	Path
<input type="checkbox"/>	NodeDefaultKeyStore	Default key store for saanchucklode01	(cell):saanchucklode01Cell:(node):saanchucklode01	\${CONFIG_ROOT}/cells/saanchucklode01Cell/nodes/saanchucklode01
<input type="checkbox"/>	NodeDefaultTrustStore	Default trust store for saanchucklode01	(cell):saanchucklode01Cell:(node):saanchucklode01	\${CONFIG_ROOT}/cells/saanchucklode01Cell/nodes/saanchucklode01
Total 2				

Next, click “NodeDefaultTrustStore”.

Configuring SSL (6 of 8)

- Click Signer certificates under Additional Properties

The screenshot displays the IBM WebSphere Administration Console interface for configuring SSL. On the left is a navigation tree with categories like Guided Activities, Servers, Applications, Services, Resources, Security, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. The main content area is titled "SSL certificate and key management" and shows the configuration for "NodeDefaultTrustStore". The "Additional Properties" section is highlighted with a red box, and the "Signer certificates" link is selected. The configuration fields include Name, Description, Management scope, Path, Password, Type (PKCS12), and checkboxes for Read only, Initialize at startup, and Enable cryptographic operations on hardware device. Buttons for Apply, OK, Reset, and Cancel are at the bottom.

Click "Signer certificates" on the right side of your screen under "Additional Properties".

Configuring SSL (7 of 8)

- Click Retrieve from port

The screenshot shows the 'Signer certificates' page in the WebSphere Administration Console. The breadcrumb trail is: SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings > Key stores and certificates > NodeDefaultTrustStore > Signer certificates. The page title is 'Signer certificates' and the description is 'Manages signer certificates in key stores.' There are buttons for 'Add', 'Delete', 'Extract', and 'Retrieve from port', with the last one highlighted. Below the buttons is a table of certificates:

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
<input type="checkbox"/>	datapower	OU=Root CA, O="DataPower Technology, Inc.", C=US	A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17	Valid from Jun 11, 2003 to Jun 6, 2023.
<input type="checkbox"/>	root	CN=savchuck.svg.usma.ibm.com, OU=Root Certificate, OU=savchucknode01.Cell, OU=savchucknode01, O=IBM, C=US	2C:0D:2E:81:C4:8A:AF:87:42:F6:D0:D8:93:D0:C3:AE:B8:A6:C2:05	Valid from Oct 14, 2010 to Oct 10, 2025.
Total 2				

Next, click Retrieve from port button.

Configuring SSL (8 of 8)

- Click Retrieve signer information
- Click Apply and Save

SSL certificate and key management

SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings > Key stores and certificates > NodeDefaultTrustStore > Signer certificates > Retrieve from port

Makes a test connection to a Secure Sockets Layer (SSL) port and retrieves the signer from the server during the handshake.

General Properties

Host
cancun.svg.usma.ibm.com

Port
686

SSL configuration for outbound connection
NodeDefaultSSLSettings

Alias
IBM

Retrieve signer information

Apply OK Reset Cancel

10 SSL setup for Information Server 8.5 using WebSphere 7.0 © 2011 IBM Corporation

Next you need to fill in your LDAP server name and port number and add an Alias. The Alias specifies the certificate alias name that you want to use to reference the signer in the key store. This can be any name you like.

The last step is to click the “Retrieve signer information” button. WebSphere will make a test connection to the SSL port and retrieve the signer from the server during the handshake.

Click Apply and then click the save link on the top of the page. Your SSL configuration is now complete.

Enable SSL – Stand-alone LDAP repository

- Configure Stand-alone LDAP properties
 - Check SSL Enabled
 - Select “Use specific SSL alias”
 - Select “NodeDefaultSSLSettings
- Stop and restart WebSphere

The screenshot displays the 'Server ssl identity' configuration page in the WebSphere Administration Console. The left-hand navigation pane shows the 'Security' section expanded to 'Global security'. The main content area is titled 'Server ssl identity' and contains the following settings:

- Server ssl identity:**
 - Automatically generated server identity
 - Server identity that is stored in the repository
- Type of LDAP server:** IBM Tivoli Directory Server
- Host:**
 - Host:
 - Port:
- Base distinguished name (DN):**
- Bind distinguished name (DN):**
- Bind password:**
- Search timeout:** seconds
- Reuse connection
- Ignore case for authorization
- SSL Settings:**
 - SSL enabled
 - Centrally managed
 - Use specific SSL alias
 - NodeDefaultSSLSettings (selected)

11

SSL setup for Information Server 8.5 using WebSphere 7.0

© 2011 IBM Corporation

Once you have configured SSL, you need to enable it for your LDAP repository. When using a stand-alone LDAP registry, specific steps must be followed. Under Security, Global Security, select Stand-alone LDAP and click Configure. Next, check the SSL Enabled check box. Select the radio button “Use specific SSL alias” and select “NodeDefaultSSLSettings” from the drop down box. Click Apply and Save. Stop and restart WebSphere for all the changes to take effect.

Enable SSL - Federated LDAP repository

- Configure Federated Repositories
- Edit repository properties
 - Check SSL Enabled
 - Select “Use specific SSL alias”
 - Select “NodeDefaultSSLSettings”
- Stop and restart WebSphere

The screenshot displays the 'Global security' configuration page for a Federated LDAP repository. The left-hand navigation pane shows the 'Security' section expanded to 'Global security'. The main content area is titled 'Global security > Federated repositories > Repository reference > New'. Below this, the 'General Properties' section shows the repository identifier 'IBM_LDAP'. The 'LDAP server' section includes fields for 'Directory type' (IBM Tivoli Directory Server), 'Primary host name' (saxchuck.eng.usma.ibm.com), and 'Port' (389). The 'Security' section on the right has the 'Require SSL communications' checkbox checked. Underneath, the 'Use specific SSL alias' radio button is selected, and the dropdown menu shows 'NodeDefaultSSLSettings' selected. Other options include 'Centrally managed' and 'MessageEndpointSecurityConfigurations'. The bottom of the page shows the page number '12', the title 'SSL setup for Information Server 8.5 using WebSphere 7.0', and the copyright notice '© 2011 IBM Corporation'.

To enable SSL when using Federated Repositories, select Federated Repositories under Security -> Global Security. Click Configure and click the repository Identifier of the repository you want to enable SSL for. Next, check the SSL Enabled check box. Select the radio button “Use specific SSL alias” and select “NodeDefaultSSLSettings” from the drop down box. Click Apply and Save. Stop and restart WebSphere for all the changes to take effect.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, InfoSphere, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2011. All rights reserved.