

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

		IBM
Objective		
- 11 4	m COL in Mahanhara 7.0 far lafarmatian Comun 0.5	
 How to sett 	up SSL in WebSphere 7.0 for information Server 8.5	
2	SSL setup for Information Server 8.5 using WebSphere 7.0	© 2011 IBM Corporation

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 adn Click Security –> SSL ce	ninistrative console as administrative user rtificate and key management	
Welcome	SSL certificate and key management	- 2 =
Guided Activities	SSL certificate and key management	
E Servers		
Applications	SSI configurations	
Services	The Service Sockets Laver (SSL) protocol provides service communications between	Related Items
Resources	remote server processes or endpoints. SSL security can be used for establishing	SSL configurations
C Security	communications, a certificate and an SSL configuration must be specified for the	= Dynamic outbound
Global security Gecurity domains Administrative Authorization Groups SSL certificate and key management SSEcurity auditing Bes security	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.	endpoint SSL confurations Key stores and certificates Key sets Key set groups
Environment	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	 Key managers Trust managers
∃ System administration	the centralized management capability.	= Certificate Authority
Users and Groups	Manage endpoint security configurations	(CA) client configurations
E Monitoring and Tuning	Manage certificate expiration	
B Troubleshooting	I the the the back the second to formation from the formation	
Service integration	Use the United States Federal Information Processing Standard (FIPS) algorithms. Note: This option requires the TLS handshake protocol, which some	
IDDI I	browsers do not enable by default.	
	Dynamically update the run time when SSL configuration changes occur	
	Apply Reset	

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



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

Configuring SSL (3	3 of 8)	
Click NodeDefaultSSI S	atings	
Click NodeDelauliSSLS	eungs	
	CGL costificate and low management	
Welcome	SSE Ceroncate and key management	
El Guided Activities	SSL certificate and key management > SSL confi	gurations
ED Servers	Defines a list of Secure Sockets Layer (SSL) confi	gurations.
E Applications		
III services	New Delete	
Constant Con	D T T 7	
 Global security 	Select Name 🗘	Management Scope 🗘
Security domains	You can administer the following resources:	
 Administrative Authorization Groups SSL cartificate and leav management 	NodeDefaultSSLSettings	(cell):sawchuckNode01Cell:(node):sawchuckNode01
 Security auditing 	Total 1	
 Bus security 		
SSL setup for Inform	nation Server 8.5 using WebSphere 7.0	© 2011 IBM Corpora

Next, click "NodeDefaultSSLSettings".

Г

		TDM
Configuring	SSL (4 of 8)	
 Click Key sto 	res and certificates	
# Welcome	SSL certificate and key management	7
Guided Activities	SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings	
E Servers	Defines a list of Secure Sockets Layer (SSL) configurations.	
Applications		
E Services	General Properties	A day of the second sec
E Resources	+ Name	Additional Properties
E Security	NodeDefaultSSLSettings	 Quality of protection (QoP)
Global security Security domains Administrative Authorization (SSL cartificate and key manage Security auditing Bus security	Trust store name [NodeDefaulTrustStore ((cell):sawchucktode01Cell:(node):sawchucktode01)] reups smeat NodeOefaultrustStore ((cell):sauchucktode01Cell:(node):sawchucktode01) Default saws certificate alias Default saws certificate alias	settings Trust and key managers Custom properties
() Environment	(none) M	Related Items
System administration	Default client certificate alias	 Key stores and certificates
E Users and Groups	Nanananati srona	
Monitoring and Tuning	(cell):sawchuckNode01Cell:(node):sawchuckNode01	
I Troubleshooting		
E Service integration	Apply OK Reset Cancel	

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

ttings > Key stores and certificates			
Lingendie rykes.			
Keystore usages			
Path 0			
· •			
I: \${CONFIG_ROOT}/cells/sawchuckNode01Cell/nodes/sawchuckNode01,			
I: \${CONFIG_ROOT}/cells/sawchuckNode01Cell/nodes/sawchuckNode01,			

Next, click "NodeDefaultTrustStore".

Configuring SSL (6	of 8)	
 Click Signer certificates 	under Additional Properties	
Welcome	SSL certificate and key management	2 H
Guided Activities	SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings >	Key stores and certificates >
Servers	NodeDefaultTrustStore	
Applications	Gennes Reystore types, including cryptography, RACP(R), CMS, Java(TM), and all trustst	ore types.
3 Services		
E Resources	General Properties	Additional Properties
3 Security	Name NodeDefaultTrustStore	= Signer certificates
Global security Security domains Administrative Authorization Groups SEL certificate and key management Security auditing Bus security	Description Default trust store for samchuckNode01 Management scope [cell):samchuckNode01Cell1: [(node):samchuckNode01	 Personal certificates Personal certificate requests Custom properties
1 Environment	Path	
3 System administration	\${CONFIG_ROOT}/cells/sawchuckNode01Cell/nodes/sawchuckNode01/trust.p12	
D Users and Groups	* Password	
Monitoring and Tuning	Tuna	
1 Troubleshooting	PKCS12	
E Service integration	Read coly	
I UDDI	C read day	
	Initialize at startup Initialize at startup Enable cryptographic operations on hardware device Apply OK Reset Cancel	

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

Configuring SSL	(7 of	8)			
 Click Retrieve from 	port				
Welcome	SSL certi	ficate and key	management		2.
Guided Activities	551 ca	etificate and k	av management > SSI configuration	> NodeDefaultSSI Settings > Key stores and certificates > NodeDe	faultTructStore
Servers	> Sigr	er certificates	er management > 55c connegaration	Modebenancosciencies > Refisiones and certificates > modeben	a solution of the state of the
Applications	Manag	es signer certi	icates in key stores.		
E Services	e Pre	ferences			
Resources	Add	Delete Ext	act Retrieve from port		
E Security	D	6 # 9			
Global security	Select	Alias A	Issued to A	Finnermint (SHA Dinest) ^	Expiration ^
 Security domains Administrative Authorization Groups 	You	an administer	the following resources:		
 SSL certificate and key management 		datapower	OU=Root CA, O="DataPower	A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17	Valid from
 Security auditing 			Technology, Inc.", C=US		Jun 11, 2003 to Jun 6,
 Bus security 					2023.
Environment		root	CN=sawchuck.swg.usma.lbm.com, OU=Root Certificate,	, 2C:0D:2E:81:C4:8A:AF:87:42:F6:D0:D8:93:D0:C3:AE:88:A6:C2:D5	Valid from Oct 14, 2010 to Oct 10, 2025.
System administration			OU=savchuckNode01Cell, OU=savchuckNode01, O=IBM,		
Users and Groups			C=US		
Monitoring and Tuning	Total	2			
+ Troubleshooting					
E Service integration					

Next, click Retrieve from port button.

Γ

Configuring	SSL (8 of 8)
 Click Retrieve 	signer information
 Click Apply an 	l Save
	CE sublists and key management
Welcome	SSL certificate and key management
Guided Activities	SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings > Key stores and certificates > NodeDefaultTrustStore > Signer certificates > Retrieve from port
Servers	Makes a test connection to a Secure Sockets Layer (SSL) port and retrieves the signer from the server during the
Applications	handshake.
Services	General Properties
Resources	eancun.svg.usma.ibm.com
a Security = Global security = Security domains = Administrative Authorizatio = SSL certificate and key mar = Security auditing = Bus security	Groups genest SSL configuration for outbound connection IndoeDefaultSSLSettings M + Alias IBM
Environment	
System administration	Retrieve signer information
Users and Groups	Analo OV Recat Count
Monitoring and Tuning	Apply UK Reset Cancel
Troubleshooting	
Service integration	
a service integration	

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.

				IBN
able SSI -	Stand-	alone I DAP repositor	/	
	otunia	alone Lora repository		
onfigure Stand	-alone LL	AP properties		
- Check SSL E	nabled_			
- Select "Use	specific S	SL alias"		
Calcat "Nada	Defented			
- Select "Node	DefaultSt	SLSettings		
top and restart	WebSphe	ere		
Manar All tasks		Server user identity		
= Welcome		Automatically generated server identity	Related Items	
E Guided Activities		Server identity that is stored in the repository	Trusted authentication realms -	
E Servers			interne	
Applications				
E Services				
E Resources				
8 Security		Type of LDAP server		
= Global security		IBM Tivoli Directory Server		
 Security domains Administrative Authorizati 	an Groups	* Host		
* SSL certificate and key ma	inagement	atitus.avg.usma.ibm.com		
= Security auditing		389		
- use second		Base distinguished name (DN)		
ED Environment		de=ipsaupport, de=ibm, de=coi		
ED System administration		Bind distinguished name (DN)		
ED Osers and Groups		uid=ldwasadm.ou=people.dc		
ED Mentering and Tuning		Bind password		
		Rearch Emersed		
		120 seconda		
10 0001		Reuse connection		
		Ignore case for authorization		
		SSL Settings		
		SSL enabled		
		Centrally managed		
		 Manage endpoint accurity configurations 		
		O Use specific SSL alias		
		NodeOefaultSSLSettings 💌 = <u>SSL configurations</u>		
SSL set	up for Information S	Server 8.5 using WebSphere 7.0		© 2011 IBM Corpora

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.

			IB
nable SSL - Fede	erated LDAP reposit	torv	
Configure Federated F	Repositories		
Edit repository propert – Check SSL Enable – Select "Use specif – Select "NodeDefau	ies ed ic SSL alias" ⊔ltSSLSettings Sphere		
Stop and restart webs	sphere		
= Welcome	Global security	2	
Guided Activities	Global security > Federated repositories > Repository re	eference > New	
Servers	Specifies the configuration for secure access to a Lightwe failurer securer.	ight Directory Access Protocol (LDAP) repository with optional	
(T) + + + + + + + + + + + + + + + + + + +			
LI Applications	General Properties		
Services	General Properties * Repository identifier		
El Applications El Services El Resources	General Properties * Repository identifier IBM_LDAP		
13 Applications 13 Services 13 Resources 13 Security	Ceneral Properties * Repository identifier [B#_CA# LDAP server	Security	
D Apprications Bervices Becourtes Security Clobal security Security domains	Ceneral Properties	Security Bind distinguished name	
U Applications D Services Becarity = Security = Security density = Security density = Security density	Caneral Properties	Security Bird distinguished name Chieflaj Mankonda, OU-User	
Applications Security Constraints Security Constraints Security Constraints Advancement Security domains Advancement SSL certification of kay management SSL certification of kay management	Ceneral Properties	Servity Bind distinguished name (XrivRa) Manikonda, QU+Usen Bind password	
Bandise Bandise Bandise Bandise Bandise Besortes Security Society	Canneal Properties	Security Bind distinguished name Orivinaj Manikonda, Ul-Visen Bind gazardi Login properties	
Applicationa Bennices Bennices Besources clubal security	Canneal Properties Canneal Properties Canneal Content Viewer Content Viewe	Security Bind distinguished name Orkitaj Manikonda,OU+Usen Bind pasarond ******* Gojn properties uid	
Approxima Security Constants Security Constants Security Constants Security Constants Security Security Security Security Security Extraction Security Extraction Extraction Extraction Extraction Extraction	Canneal Properties Canneal Properties Control Vieter Control C	Servity Biod disripulabed name Disrikaj Manikanda OU-Usen Biod pesanod Indep properties Indep attribute for Keberos principal name	
Applications Bennice Bennice Benice Security Security Security Security Security Security Businement Security softman Security softman Security Businement Bystem administration	Canneal Properties Canneal Properties Containing Load LDAP server Containing toot name Port East-huck.org.usma.ibm.com Pallower serve used when primary is not available: Contains Easter: Fallower Host Name Port	Security Bind distinguished name Driving Manikanda, Ukuten Bind gasarod 	
Applicationa Bennices Bennices Security densmo Bennices Security densmo D	Canneal Properties Canneal Properties Constanty Identifier Dorschory hype Dorschory hype Dorschory hopt name Pathover server used when primary is not available: Dates Select Falower Host Name Port Name Name Pathover Set Name Port Name Pathover Name Port Pathover Pathover Name Port Pathover Pathover P	Security Bind distinguished name Officing) Marklanda, OU-Usen Bind passord Login properties Und LOAD attribute for Ketheros principal name Certificate mapping (SART, DM)	
Applicational Benvice Benvice Security Security Security Security Security solutions Security solutions Security solutions Envicement Security solutions	Canneal Properties Canneal Properties Canneal Properties Conclumy Identifier Conclumy type Canneal Properties Conclumy type Canneal Post Failower server used when primary is not available: Conten Eacher Server Hoat Name Port Name Rate Rate Rate Rate Rate Rate Rate Rat	Security Direct and the second Bind parameters Bind parameters Bind parameters Bind parameters Login properties UdD attribute for Ketheres principal name Certificate mapping DAT_DIR Certificate Inter	
Applications Bennices Bennices Bennices Bennices Bennices Bennices Bennices Bennices Security Benniceses Be	Canneal Properties Canneal Properties Constanty Identifier DAP Sever Constanty type Data Troot Directory Server Containe Pailover serve used when primary is not available: Containe Ealert: Failover Hoat Name Port None Add	Security Bind distinguished name Driving Manikonda, Urusen Bind passard 	
Applicational Bennices Bennices Security density Citabil security Citabil security Citabil security Citabil security Citabil security Security density Security density Security density	Canneal Properties Canneal Properties Conclose your Conclose y	Security Bind distinguished name Orking) Mankonda, OU-Usen Bind passend Loggin properties wa LOAD attribute for Ketheros printpal name CARTificate mapping EXACT ON N Certificate filter	
Applications Bennices Bennices Security Security Security Security Security Security Security Security Security solution Security	Ceneral Properties	Security Bind desinguished name (Drichag) Hanhunda (Diribler) Rind passes Login properties UdAP attribute for Kerbergs principal name Certificate mapping EXACT_DR Certificate filter Certificate filter	
Applications Aplications Ap	Canned Properties Canned Properties Containing Load LDAP server Donationy type Data Truck Directory Server Containing Nation name Port Reschuck.org.usma.iben.com Pallower server used when primary is not available: Containing Reschuck.org.usma.iben.com Resce	Security Bind distinguished name Diriking Manikanda, Durusen Tind passard Gala properties USAB attribute for Karbess principal name Certificate resping EXACT_DN Certificate filter P Require SSL communications Or name/or processed	
Applicational Bennices Bennices Security density Citabil security Citabil security Citabil security Citabil security Citabil security Security density Security density Security density	Canned Properties Canned Properties Constitut Vieterfor DDP server Constitut Vieterfor Server Server Server Server Server Serv	Servity Biod passwod Chinitaji Mankanda Ou-Uwar Biod passwod 	
Applications Bennices Bennices Bennices Security Security Security Security Security Security software Securi	Canned Properties Canned Properties Canned Properties LDAP server Donetary type Call Trivid Directory Server Parlover server used when primary is not available: Dates Select; Failover Host Name Port Hane Add Support referals to other LDAP servers ignore im	Security End distinguished name Circles itsochands.Ouroben inde parameter	
Applications Applications Bennices Account of the second of the secon	Canned Properties Canned Properties Containing Load Server Containing Note name Port Banchuck.erg.usma.iben.com Fallower aver used when primary is not availables Coleva Backet: Fallower Host Name Port Name Add Support referrals to other LDAP servers (prove W)	Severity Bind distinguished name Oriving Itanikonde, Ulusien Ind passes Usab attribute for Kerbess principal name Certificate mapping EXACT_ON Certificate filter P Require SSL communications Certificate filter P Require SSL communications Certificate filter Certificate filter D Centrally managed States and paints setup compositions Certificate filter States and paints setup compositions Certificate filter States and paints setup compositions D Centrally managed States and paints setup compositions D Centrally managed D	

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, intoSphere, 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 " <u>Copyright and trademarks information</u> " 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 INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT 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 REPRESENTATION IS INTENDED ROBIL FOR ANY AGREEMENT 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.
13 © 2011 IBM Corporation