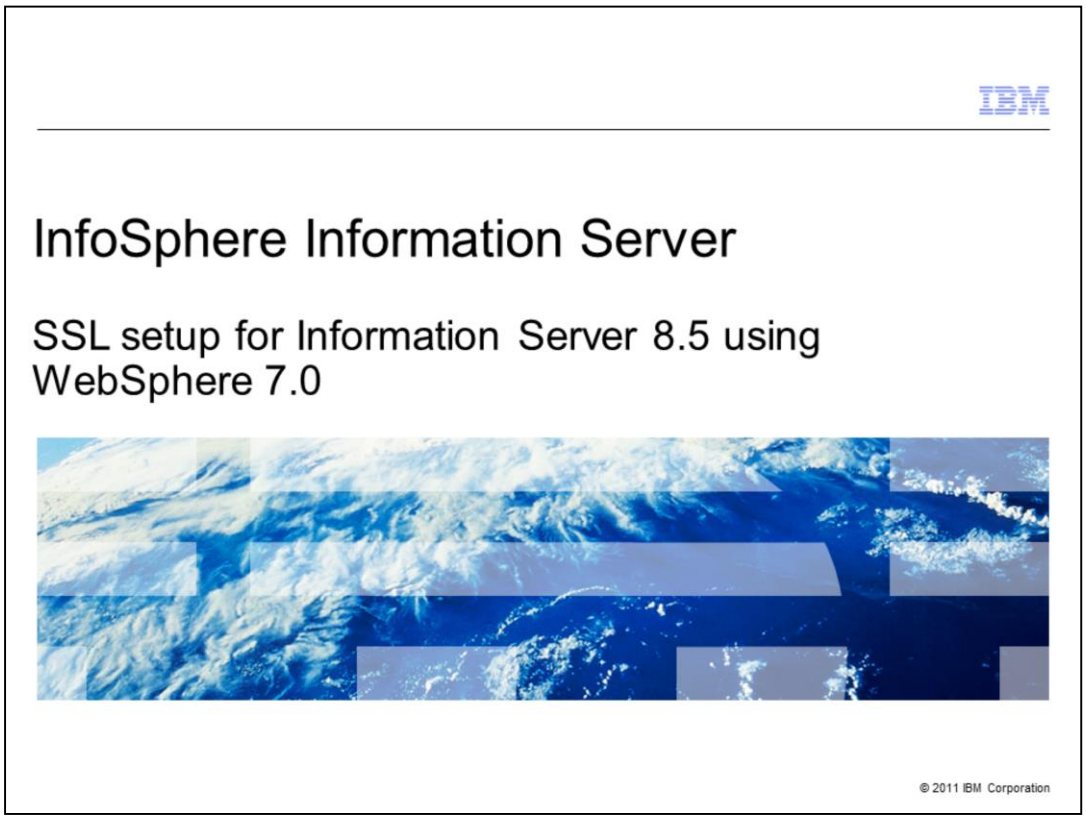
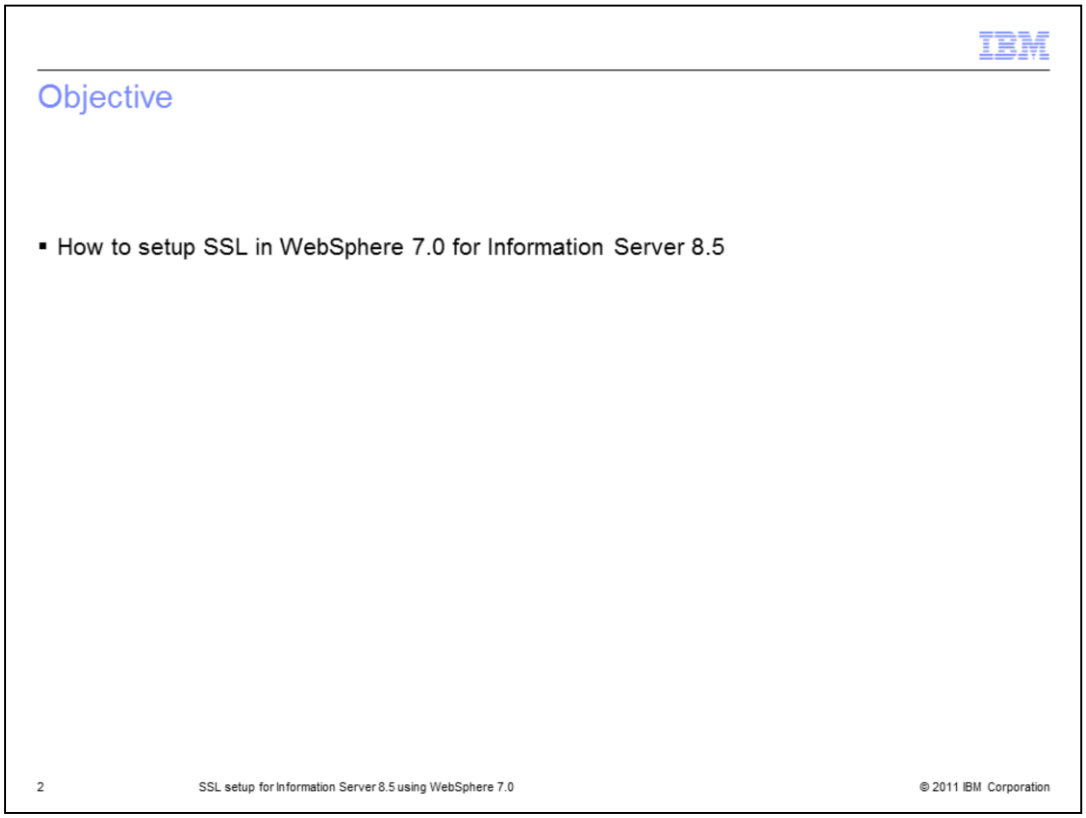


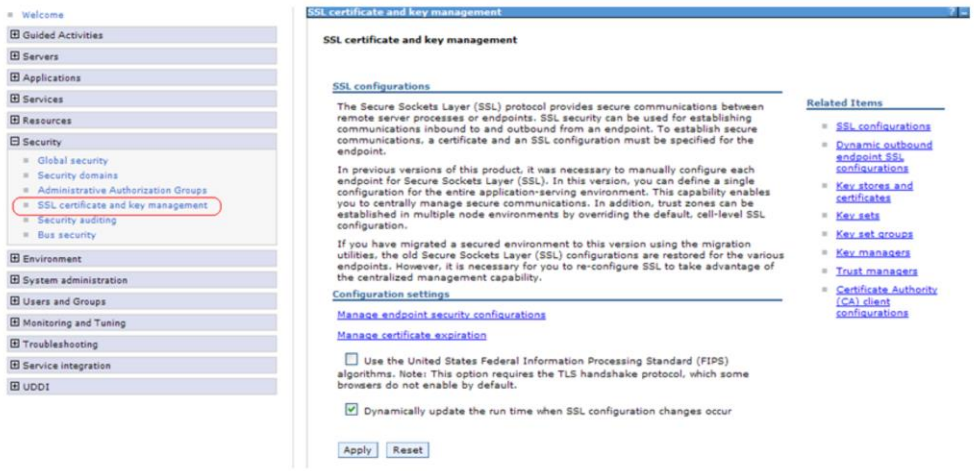

This is the SSL Setup for Information Server 8.5 using WebSphere® 7.0 presentation.




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







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

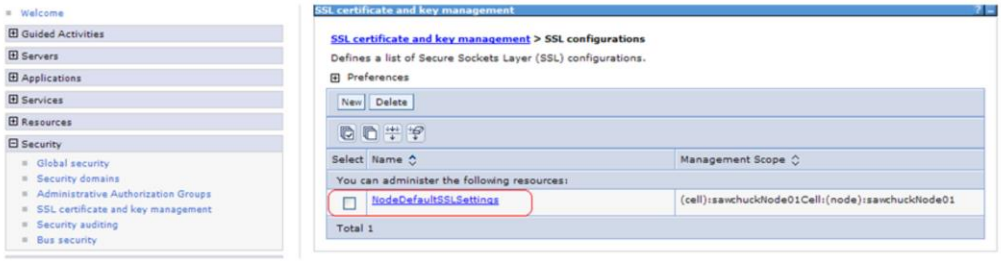




Click “SSL Configurations” on the right side of your screen under “Related Items”.

## Configuring SSL (3 of 8)

- Click NodeDefaultSSLSetings



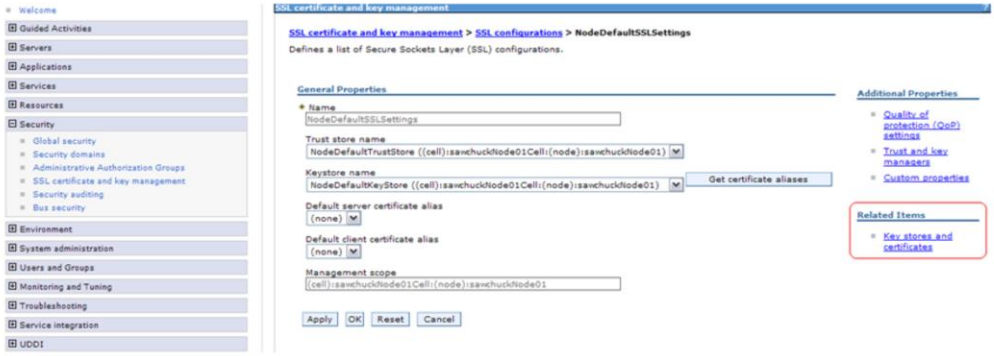




Next, click “NodeDefaultSSLSettings”.

## Configuring SSL (4 of 8)

- Click Key stores and certificates



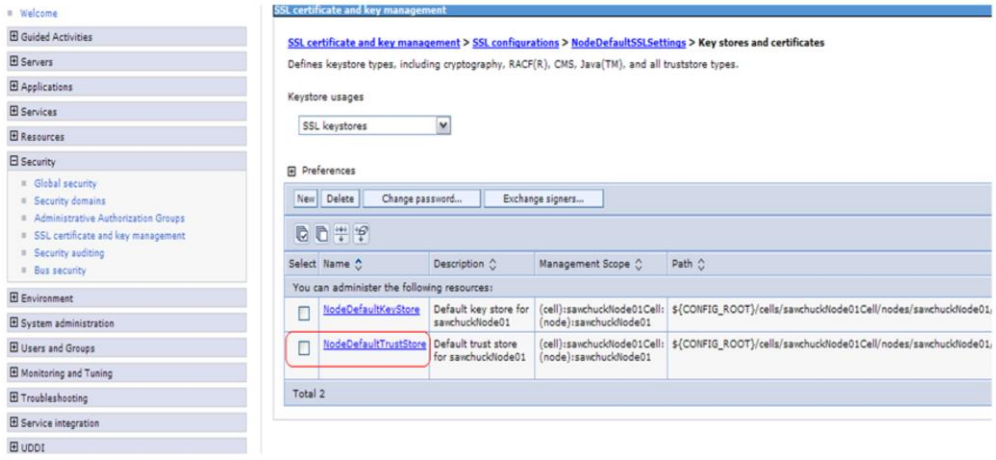




Click “Keystores and certificates” on the right side of your screen under “Related Items”.

## Configuring SSL (5 of 8)

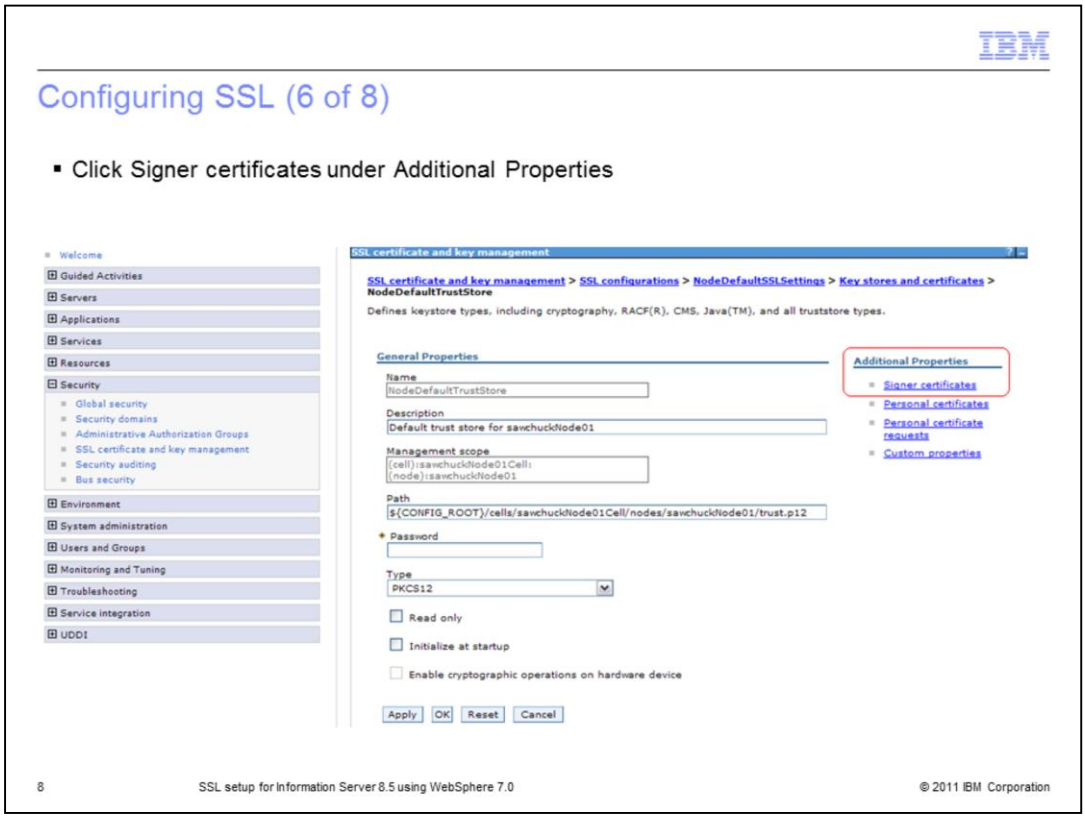
- Select NodeDefaultTrustStore







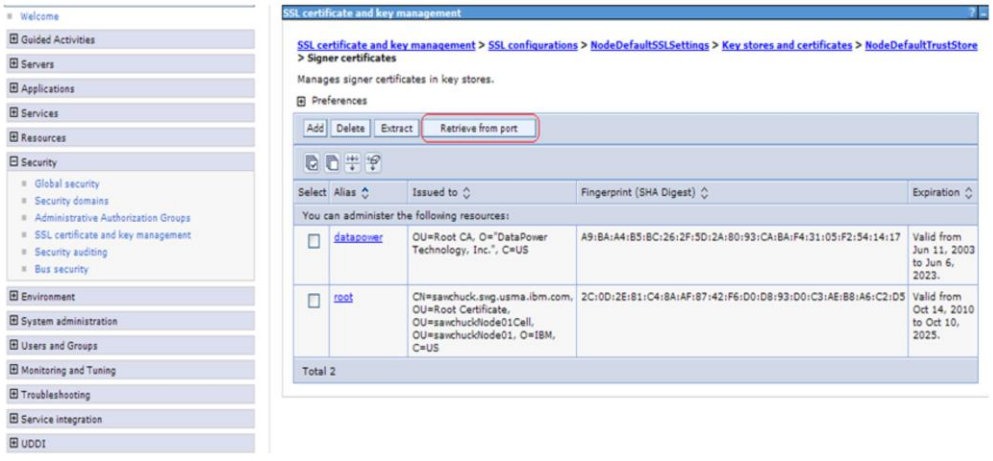
Next, click “NodeDefaultTrustStore”.




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

## Configuring SSL (7 of 8)

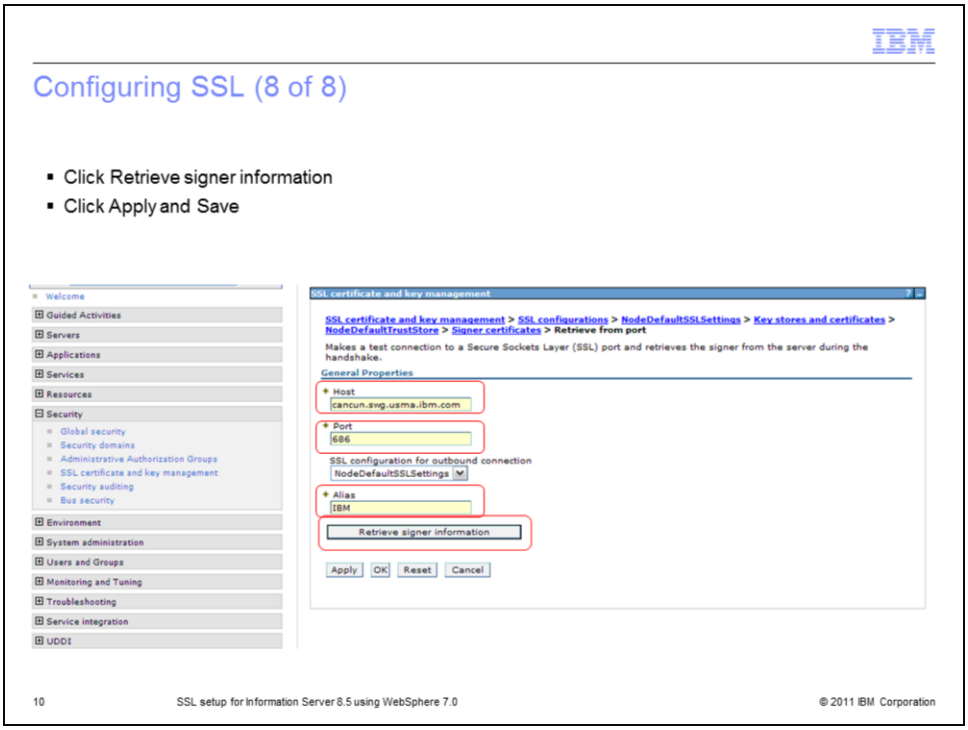
- Click Retrieve from port







Next, click Retrieve from port button.



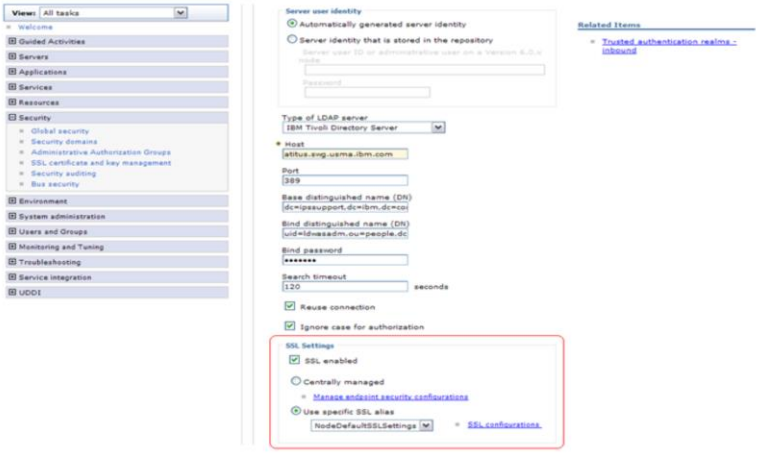

Next you need to fill in your LDAP server name and port number and add an Alias. The Alias specifies the certificate alias name that you want to use to reference the signer in the key store. This can be any name you like.

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



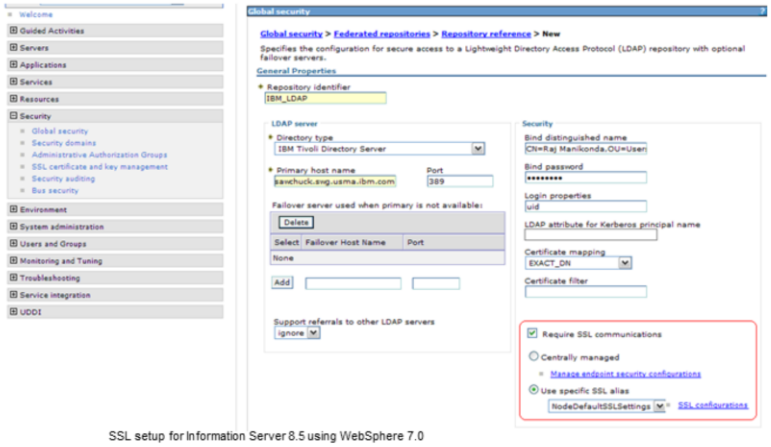




Once you have configured SSL, you need to enable it for your LDAP repository. When using a stand-alone LDAP registry, specific steps must be followed. Under Security, Global Security, select Stand-alone LDAP and click Configure. Next, check the SSL Enabled check box. Select the radio button “Use specific 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







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