

## Update WebSphere 7.x and 8.X

1. Login to websphere console goto Security -> SSL certificate and key management





## 2. Click on Manage certification expiration

**SSL certificate and key management**

### 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 endpoint SSL configurations
- Key stores and certificates
- Key sets
- Key set usage
- Key managers
- Trust managers
- Certificate Authority (CA) client configurations

## 3. If you have “Enable checking” websphere automatically manages your ssl key expirations based on the options you selected.

**SSL certificate and key management**

[SSL certificate and key management](#) > **Manage certificate expiration**

Configures the certificate expiration monitor.

**General Properties**

\* Expiration notification threshold  days

Enable checking

**Expiration checking**

Scheduled time of day to check for expired certificates

:   A.M.  P.M.  24-hour

Check by calendar

Weekday  \* Repeat interval  weeks

Check by number of days

\* Repeat interval  days

Next start date

**Expiration check notification**

Automatically replace expiring self-signed and chained certificates

Delete expiring certificates and signers after replacement

**Related Items**

- Notifications



## Initial install of SSL Certs on Websphere

1. Login to WebSphere console
2. Goto SSL Security -> certificate and key management





### 3. Go to Keystores and certificates

SSL certificate and key management

#### 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 inbound endpoint 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. Go to NodeDefaultTrustStore (If you are on a clustered environment make sure you do these steps for both nodes.)

SSL certificate and key management

#### SSL certificate and key management > Key stores and certificates

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

##### Keystore usages

SSL keystores

##### Preferences

Select	Name	Description	Management Scope	Path
<input type="checkbox"/>	<a href="#">NodeDefaultKeyStore</a>	Default key store for HAWKEYENode01	(cell):HAWKEYENode01Cell:(node):HAWKEYENode01	\${CONFIG_...
<input type="checkbox"/>	<a href="#">NodeDefaultTrustStore</a>	Default trust store for HAWKEYENode01	(cell):HAWKEYENode01Cell:(node):HAWKEYENode01	\${CONFIG_...

Total 2



## 5. Go to Signer certificates

[SSL certificate and key management](#) > [Key stores and certificates](#) > [NodeDefaultTrustStore](#)

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

General Properties	Additional Properties
Name <input type="text" value="NodeDefaultTrustStore"/>	<a href="#">Signer certificates</a>
Description <input type="text" value="Default trust store for HAWKEYENode01"/>	<a href="#">Personal certificates</a>
Management scope <input type="text" value="(cell):HAWKEYENode01Cell:(node):HAWKEYENode01"/>	<a href="#">Personal certificate requests</a>
Path <input type="text" value="\${CONFIG_ROOT}/cells/HAWKEYENode01Cell/nodes/HAWKEYENode01/trust.p12"/>	<a href="#">Custom properties</a>

## 6. Click on “Retrieve from port”

**SSL certificate and key management**

[SSL certificate and key management](#) > [Key stores and certificates](#) > [NodeDefaultTrustStore](#) > [Signer certificates](#)

Manages signer certificates in key stores.

⊕ Preferences

## 7. Enter the details requested

**SSL certificate and key management**

[SSL certificate and key management](#) > [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

\* Port

SSL configuration for outbound connection

\* Alias



## 8. Hit “Retrieve signer information”

**SSL certificate and key management**

[SSL certificate and key management](#) > [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

\* Port

SSL configuration for outbound connection

\* Alias

**Retrieved signer information**

Serial number

Issued to

Issued by

Fingerprint (SHA digest)

Validity period

## 9. Cert information is retrieved and you can Apply the certs and save the configuration

**SSL certificate and key management**

Messages

- ⚠ Changes have been made to your local configuration. You can:
  - [Save](#) directly to the master configuration.
  - [Review](#) changes before saving or discarding.
- ⚠ The server may need to be restarted for these changes to take effect.

[SSL certificate and key management](#) > [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

\* Port

## 10. Once the cert information is applied you have to restart the JVM. (On a Network Deployment you may not have to restart the JVM but if you are using Express we might have to do a restart. You can test CSM connection without a restart and see if it works if not you can restart the JVM)