SSL Configuration on WebSphere
Oracle FLEXCUBE Universal Banking

Release 11.83.03.0.0

[November] [2016]

Table of Contents

1. Configuring SSL on WebSphere

1.1 Introduction

This chapter guides you through the process of configuring SSL on IBM WebSphere application server.

1.2 Certificates

1.2.1 Creating SSL Connection between Application Server and Client

To establish SSL connection between WebSphere and client work stations, follow the steps given below:

- Create SSL certificate (this certificate is required during real time production)
- Self signed certificate (SSL) will be used for testing purpose

1.2.2 Creating Self Signed Certificate

To create a self signed certificate, you may use various tools including IBM (Keyman). For illustration purpose, this guide explains the method of generating SSL using a tool available in JAVA. The keytool is available in the folder ‘JAVA_HOME\jdk\bin’.

Go to the folder ‘bin’ of JRE from command prompt and type the following command.

```
keytool -genkeypair -alias alias -keyalg keyalg -keysize keysize -sigalg
sigalg -validity valDays -keystore keystore
```

Note: The texts highlighted in blue are placeholders. You need to replace them with the suitable values while running the command.

In the above command,

- ***alias*** is used to identify the public and private key pair created. This *alias* is required for configuring the SSL attributes for the managed servers in Oracle WebLogic application server.
- ***keyalg*** is the key algorithm to generate the public and private key pair. The RSA key algorithm is recommended.
- ***keysize*** is the size of the public and private key pair generated. A key size of 1024 or more is recommended. Consult your CA on the key size support for different types of certificates.
- ***sigalg*** is the algorithm used to generate the signature. This algorithm must be compatible with the key algorithm. This has to be one of the values specified in the Java Cryptography API Specification and Reference.
- ***valdays*** is the number of days for which the certificate is considered to be valid. Consult your CA on this period.
- ***keystore*** is to specify the location of the JKS file. If JKS file is not present in the path provided, this will create it.

The command will prompt for the following attributes of the certificate and keystore:

- **Keystore password**: Specify a password that will be used to access the keystore. This password needs to be specified later, when configuring the identity store in Oracle WebLogic Server.

- **Key password**: Specify a password that will be used to access the private key stored in the keystore. This password needs to be specified later, when configuring the SSL attributes of the managed server(s) in Oracle WebLogic Server.
- **First and last name (CN)**: Specify the domain name of the machine used to access Oracle FLEXCUBE UBS. For instance, www.example.com.
- **Name of your organizational unit**: Specify the name of the department or unit making the request. For example, BPD. Use this field to identify the SSL Certificate you are creating. For example, by department or by physical server.
- **Name of your organization:** Specify the name of the organization making the certificate request. For example, Oracle Financial Services Software. It is recommended to use the formal name of the company or organization. This name must match the name in the official records.
- **Name of your City or Locality**: Specify the name of the city in which your organization is physically located. For example Mumbai.
- **Name of your State or Province**: Specify the state/province in which your organization is physically located. For example Maharashtra.
- **Two-letter country code for this unit**: Specify the country in which your organization is physically located. For example, US, UK, IN etc.

Example

Listed below is the result of a sample execution of the command:

```
C:\Program Files\IBM\WebSphere\AppServer\bin>keytool -genkeypair -
alias cvrhp0729 -keyalg RSA -keysize 1024 -sigalg SHA1withRSA -
validity 365 -keystore D:\keystores\FCUBSKeyStore.jks

Enter keystore password:<Enter a password to protect the keystore>

Re-enter new password:<Confirm the password keyed above>

What is your first and last name?

  [Unknown]:  cvrhp0729.i-flex.com

What is the name of your organizational unit?

  [Unknown]:  BPD

What is the name of your organization?

  [Unknown]:  Oracle Financial Services

What is the name of your City or Locality?

  [Unknown]:  Mumbai

What is the name of your State or Province?

  [Unknown]:  Maharashtra

What is the two-letter country code for this unit?

  [Unknown]:  IN

Is CN=cvrhp0729.i-flex.com, OU=BPD, O=Oracle Financial Services,
L=Mumbai, ST=Maharashtra, C=IN correct?

  [no]:  yes
```

```
Enter key password for <cvrhp0729>

        (RETURN if same as keystore password):<Enter a password to
protect the key>

Re-enter new password:<Confirm the password keyed above>
```

The self signed certificate needs to be added to the web server.

1.2.3 Path Details

You need to copy or move the keystore file <*name of the file*>*.jks* to the application server location given below:

/oracle1/WAS61/Appserver_ND/profiles/AppSrv01/config/cells/ips014dorCell01/nodes/ips014dorNode02

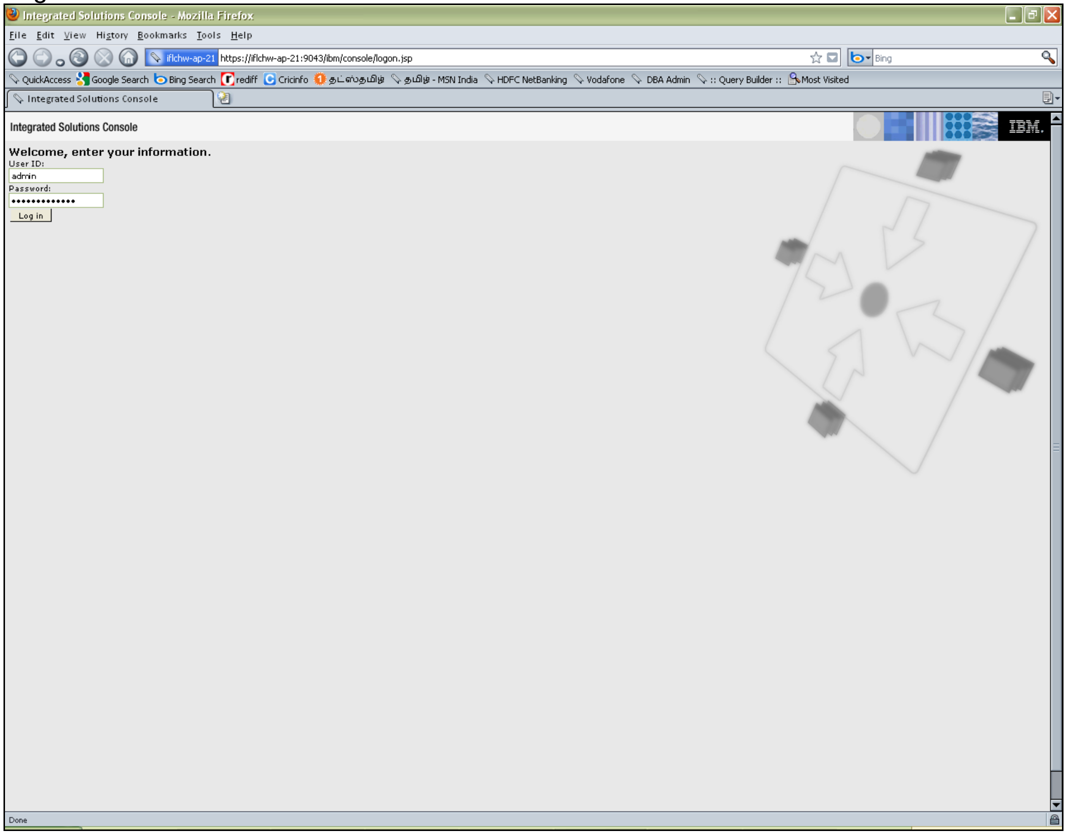
ips014dorCell01 --> <ips014dor> name of the machine and < Cell01>

ips014dorNode02 --> < ips014dorNode > name of the machine and <Node02>

1.3 Adding Key Store to Application Server

To add keystore to the WebSphere application server, follow the instructions given below.

Log in to the WAP console as the user 'admin'.



https://iflchw-ap-21:9043/ibm/console/logon.jsp

Integrated Solutions Console

Welcome, enter your information.

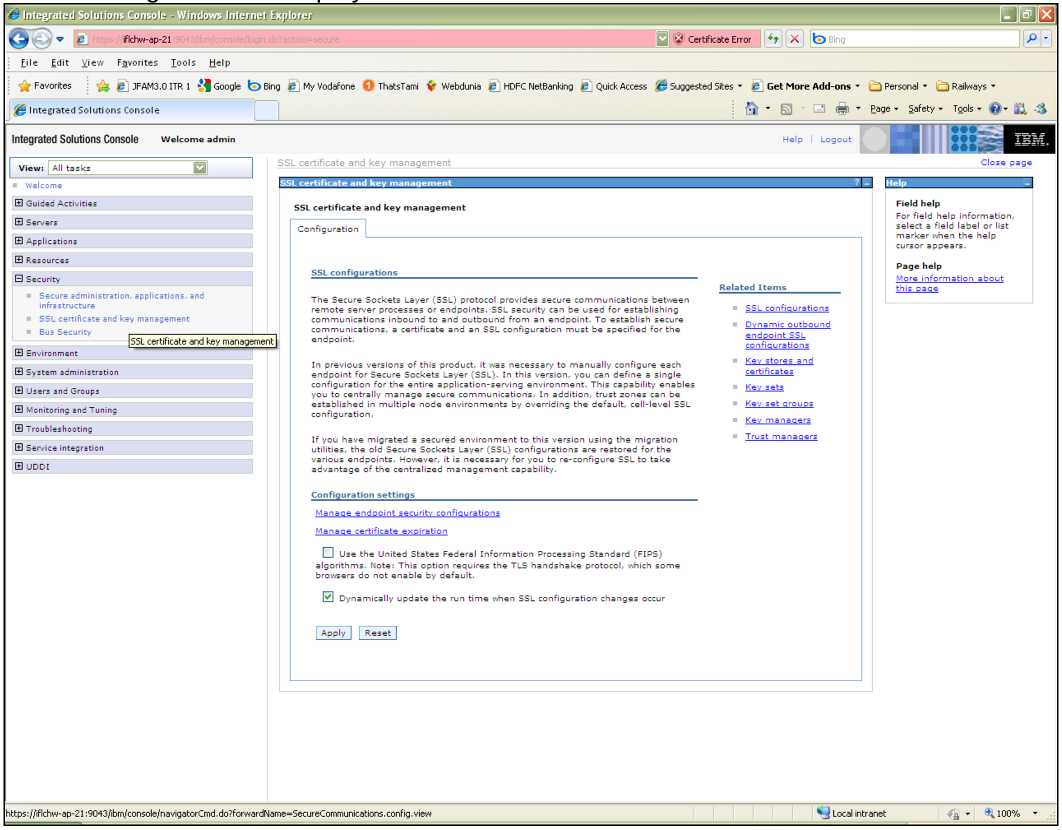
User ID: admin

Password: •••••••••••••

Log in

Specify the user ID of the administrator and the password set while installing the software. Click 'Log In'.

The following screen is displayed:


Integrated Solutions Console - Windows Internet Explorer
https://iflchw-ap-21:9043/ibm/console/login.do?action=secure
Certificate Error
File Edit View Favorites Tools Help
Integrated Solutions Console
Welcome admin
Help | Logout
View: All tasks
Welcome
Guided Activities
Servers
Applications
Resources
Security
Secure administration, applications, and infrastructure
SSL certificate and key management
Bus Security
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Close page
https://iflchw-ap-21:9043/ibm/console/navigatorCmd.do?forwardName=SecureCommunications.config.view
Local intranet
100%

SSL certificate and key management

SSL certificate and key management

Configuration

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

Apply Reset

Related Items

- SSL configurations
- Dynamic outbound endpoint SSL configurations
- Key stores and certificates
- Key sets
- Key set groups
- Key managers
- Trust managers

Help

Field help

For field help information, select a field label or list marker when the help cursor appears.

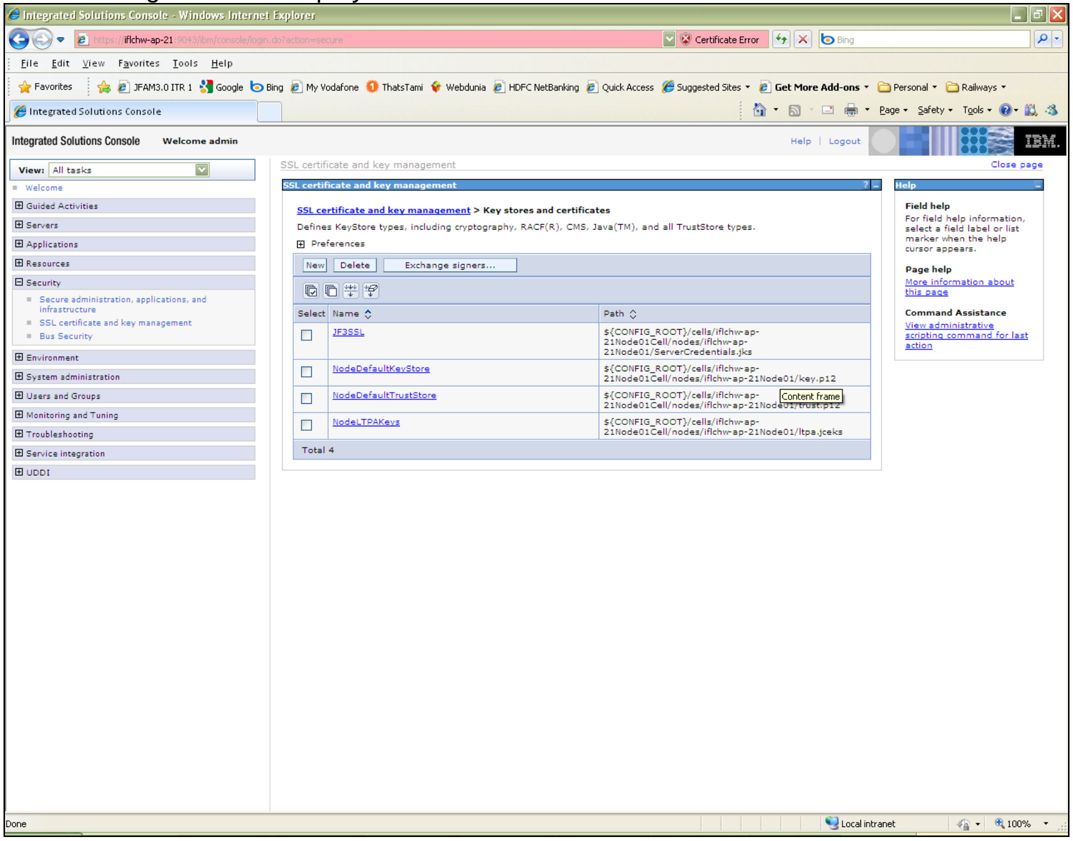
Page help

More information about this page

On the left pane, expand ‘Security’ and click ‘SSL certificate and key management’. The screen displays the details of SSL.

Under ‘Related items’ on the right side, click ‘Key stores and certificates’.

The following screen is displayed:



SSL certificate and key management

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.

⊞ Preferences

New | Delete | Exchange signers...

Select	Name	Path
□	JF3SSL	${CONFIG_ROOT}/cells/iflchw-ap-21Node01Cell/nodes/iflchw-ap-21Node01/ServerCredentials.jks
□	NodeDefaultKeyStore	${CONFIG_ROOT}/cells/iflchw-ap-21Node01Cell/nodes/iflchw-ap-21Node01/key.p12
□	NodeDefaultTrustStore	${CONFIG_ROOT}/cells/iflchw-ap-21Node01Cell/nodes/iflchw-ap-21Node01/trust.p12
□	NodeLTPAKeys	${CONFIG_ROOT}/cells/iflchw-ap-21Node01Cell/nodes/iflchw-ap-21Node01/ltpa.jceks
Total 4		

Help

Field help

For field help information, select a field label or list marker when the help cursor appears.

Page help

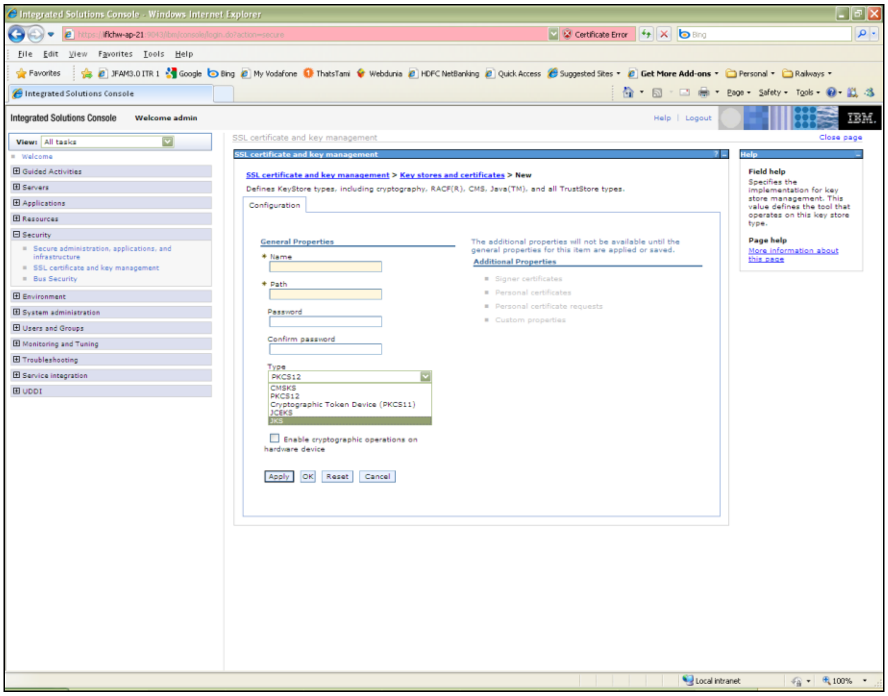
More information about this page

Command Assistance

View administrative scripting command for last action

This screen is used for attaching the key store to the application server.

Click ‘New’ button to add a new key to store.



SSL certificate and key management

SSL certificate and key management

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

Defines KeyStore types, including cryptography, RACF(R), CMS, Java(TM), and all TrustStore types.

Configuration

General Properties

* Name

* Path

Password

Confirm password

Type

PKCS12

CMSKS
PKCS12
Cryptographic Token Device (PKCS11)
JCEKS
JKS

□ Enable cryptographic operations on hardware device

Apply | OK | Reset | Cancel

The additional properties will not be available until the general properties for this item are applied or saved.

Additional Properties

- Signer certificates
- Personal certificates
- Personal certificate requests
- Custom properties

Help

Field help

Specifies the implementation for key store management. This value defines the tool that operates on this key store type.

Page help

More information about this page

Specify the following details:

Name

Specify the key store name.

Path

Specify the location of the key store generated.

This has to be a relative path.

Example

${CONFIG_ROOT}/cells/ips014dorCell01/nodes/ips014dorNode02/jf3sslstore.jks

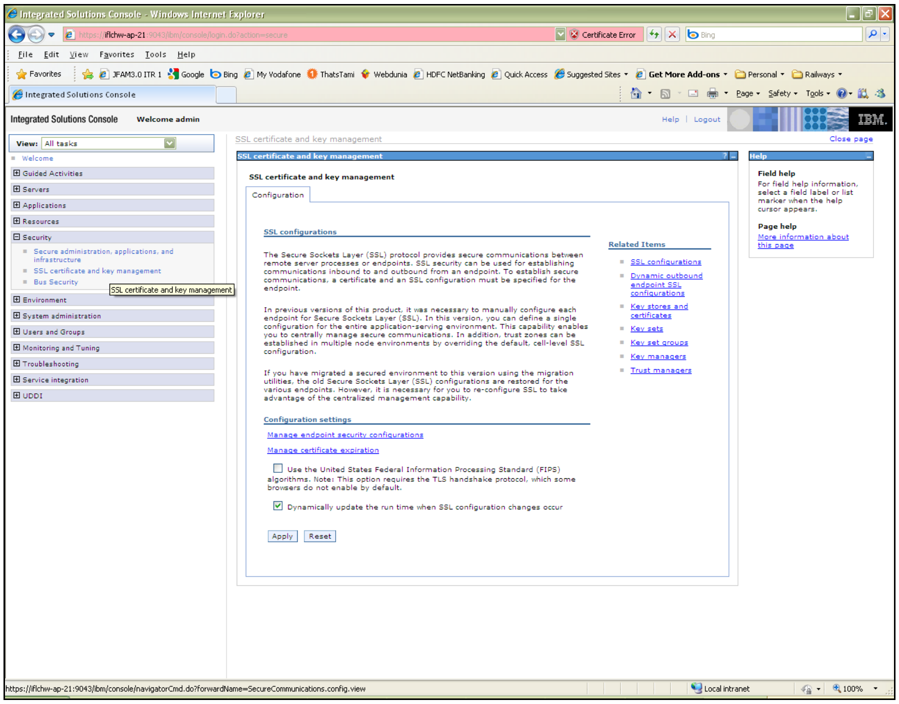
Password

Specify the password given in the 'store pass' parameter during key store generation.

Click 'Apply' and save the changes.

1.4 Creating SSL Configuration

To create SSL configuration, on the left pane, click 'SSL certificate and key management'.



SSL certificate and key management

SSL certificate and key management

Configuration

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

Field help

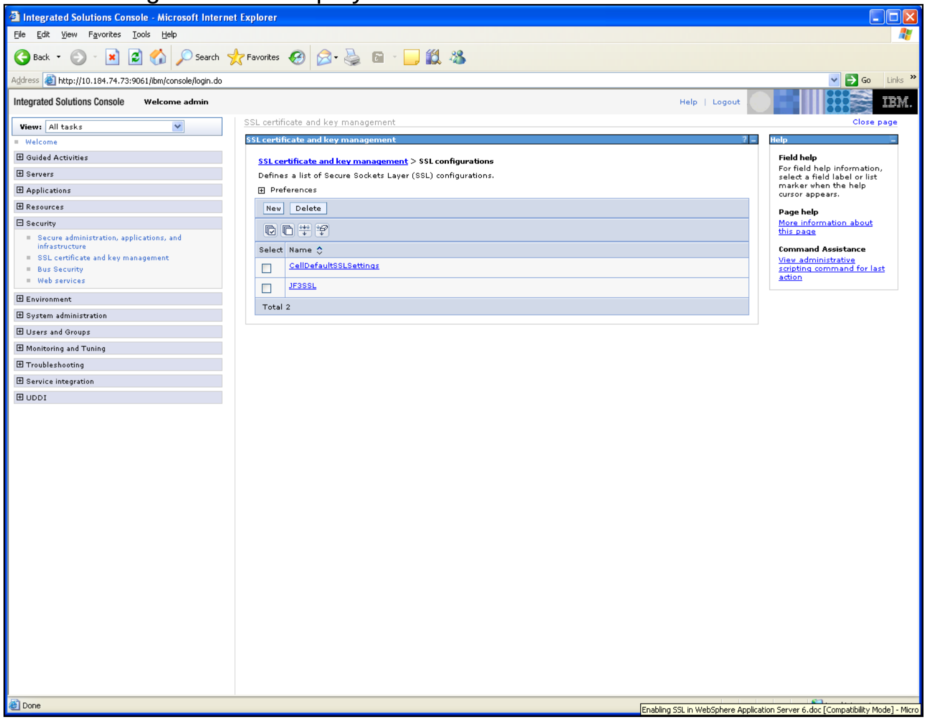
For field help information, select a field label or list marker when the help cursor appears.

Page help

More information about this page

Under the section 'Related items', click 'SSL configurations'.

The following screen is displayed:


Integrated Solutions Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.184.74.73:9061/ibm/console/login.do
Go Links
Integrated Solutions Console Welcome admin
Help | Logout
View: All tasks
Welcome
Guided Activities
Servers
Applications
Resources
Security
Secure administration, applications, and infrastructure
SSL certificate and key management
Bus Security
Web services
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Close page
Done
Enabling SSL in WebSphere Application Server 6.doc [Compatibility Mode] - Micro

SSL certificate and key management

SSL certificate and key management > SSL configurations

Defines a list of Secure Sockets Layer (SSL) configurations.

⊞ Preferences

New Delete

Select	Name
□	CellDefaultSSLSettings
□	JF3SSL
Total 2	

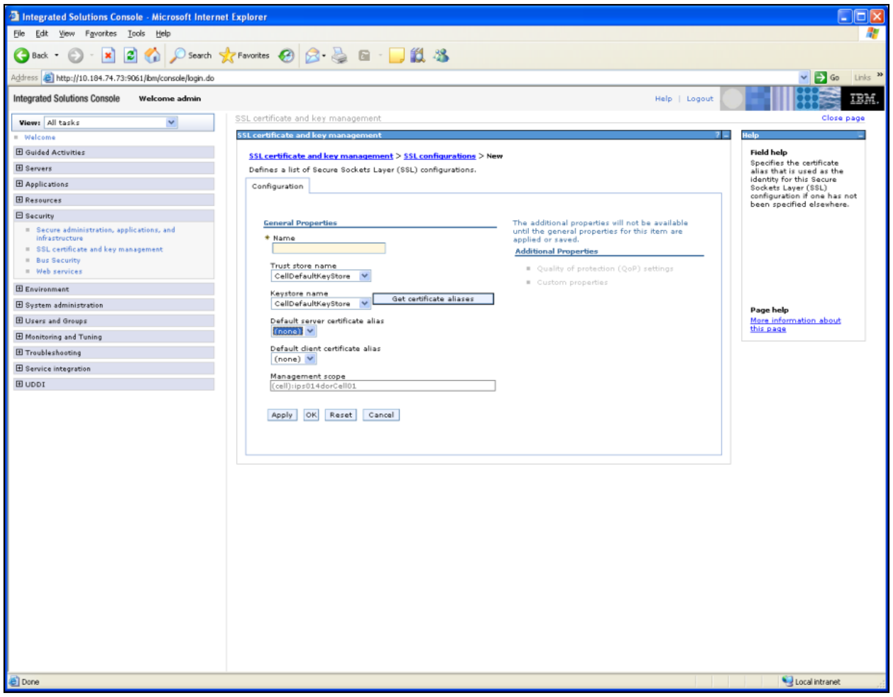
Help

Field help
For field help information, select a field label or list marker when the help cursor appears.

Page help
More information about this page

Command Assistance
View administrative scripting command for last action

Click ‘New’ button. The following screen is displayed.


Integrated Solutions Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.184.74.73:9061/ibm/console/login.do
Go Links
Integrated Solutions Console Welcome admin
Help | Logout
View: All tasks
Welcome
Guided Activities
Servers
Applications
Resources
Security
Secure administration, applications, and infrastructure
SSL certificate and key management
Bus Security
Web services
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Close page
Done
Local intranet

SSL certificate and key management

SSL certificate and key management > SSL configurations > New

Defines a list of Secure Sockets Layer (SSL) configurations.

Configuration

General Properties

* Name

Trust store name: CellDefaultKeyStore

Keystore name: CellDefaultKeyStore Get certificate aliases

Default server certificate alias: (none)

Default client certificate alias: (none)

Management scope: (cell):ips014dorCell01

Apply OK Reset Cancel

The additional properties will not be available until the general properties for this item are applied or saved.

Additional Properties
- Quality of protection (QoP) settings
- Custom properties

Help

Field help
Specifies the certificate alias that is used as the identity for this Secure Sockets Layer (SSL) configuration if one has not been specified elsewhere.

Page help
More information about this page

Specify the following details:

Name

Specify the name of the SSL configuration.

Trusted Store Name

Select the added key store.

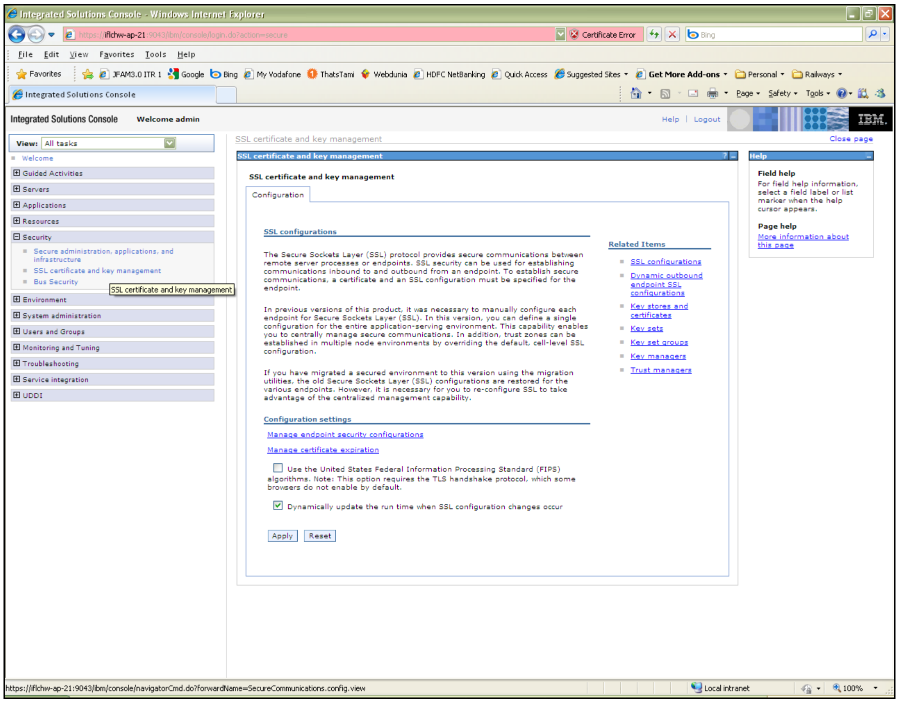
Key Store Name

Select the added key store.

Click the button ‘Get Certificate aliases’. Further, click ‘Apply’ and save the changes.

1.5 Managing Endpoint Security Configurations

This section explains the process of managing endpoint security configurations.


Integrated Solutions Console - Windows Internet Explorer
https://iflchw-ap-21:9043/ibm/console/login.do?action=secure
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
JFAM3.0 ITR 1
Google
Bing
My Vodafone
ThatsTami
Webdunia
HDFC NetBanking
Quick Access
Suggested Sites
Get More Add-ons
Personal
Railways
Integrated Solutions Console
Page
Safety
Tools
Integrated Solutions Console
Welcome admin
Help | Logout
IBM.
View: All tasks
Welcome
Guided Activities
Servers
Applications
Resources
Security
Secure administration, applications, and infrastructure
SSL certificate and key management
Bus Security
SSL certificate and key management
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
SSL certificate and key management
Close page
Help
https://iflchw-ap-21:9043/ibm/console/navigatorCmd.do?forwardName=SecureCommunications.config.view
Local intranet
100%

SSL certificate and key management

SSL certificate and key management

Configuration

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

Apply Reset

Related Items

- SSL configurations
- Dynamic outbound endpoint SSL configurations
- Key stores and certificates
- Key sets
- Key set groups
- Key managers
- Trust managers

Field help

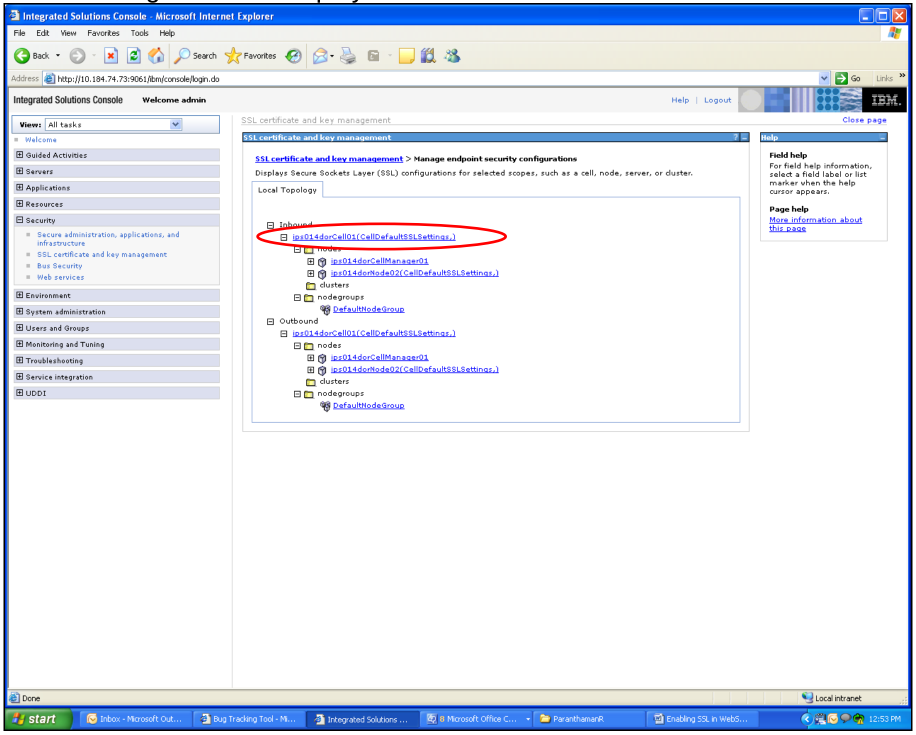
For field help information, select a field label or list marker when the help cursor appears.

Page help

More information about this page

On the left pane, expand ‘Security’ and click ‘SSL certificate and key management’. Under ‘Configuration settings’, click ‘Manage endpoint security configurations’.

The following screen is displayed:



SSL certificate and key management

SSL certificate and key management > Manage endpoint security configurations

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

Local Topology

```
⊟ Inbound
  ⊟ ips014dorCell01(CellDefaultSSLSettings,)
    ⊟ nodes
      ⊞ ips014dorCellManager01
      ⊞ ips014dorNode02(CellDefaultSSLSettings,)
      clusters
    ⊟ nodegroups
        DefaultNodeGroup
⊟ Outbound
  ⊟ ips014dorCell01(CellDefaultSSLSettings,)
    ⊟ nodes
      ⊞ ips014dorCellManager01
      ⊞ ips014dorNode02(CellDefaultSSLSettings,)
      clusters
    ⊟ nodegroups
        DefaultNodeGroup
```

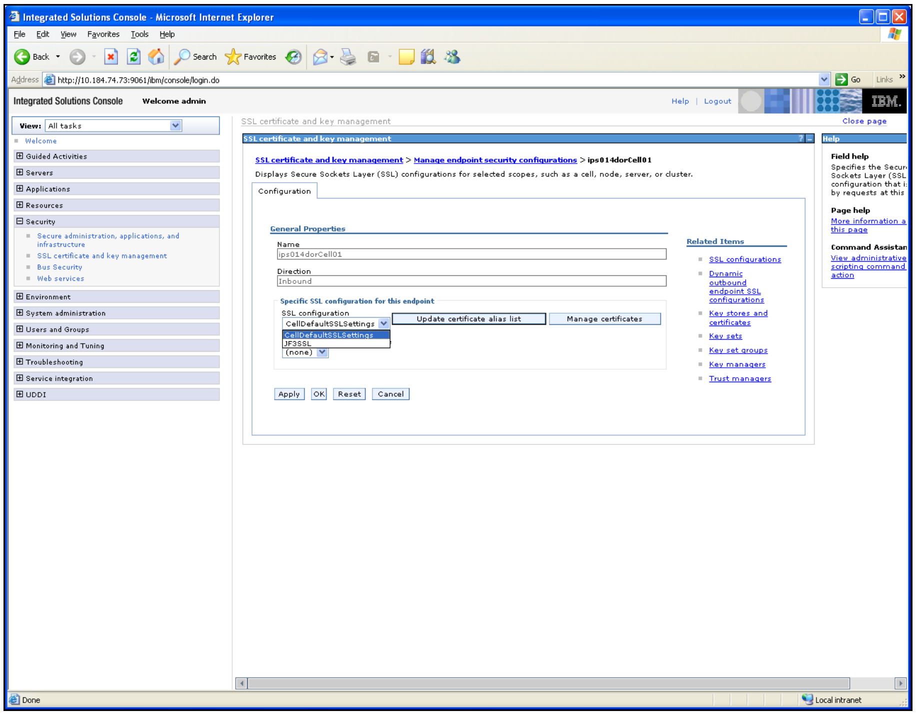
Field help

For field help information, select a field label or list marker when the help cursor appears.

Page help

More information about this page

Click the first link under ‘Inbound tree’. The following screen is displayed:



SSL certificate and key management

SSL certificate and key management > Manage endpoint security configurations > ips014dorCell01

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

Configuration

General Properties

Name: ips014dorCell01

Direction: Inbound

Specific SSL configuration for this endpoint

SSL configuration: CellDefaultSSLSettings

- CellDefaultSSLSettings
- JF3SSL

(none)

Related Items

- SSL configurations
- Dynamic outbound endpoint SSL configurations
- Key stores and certificates
- Key sets
- Key set groups
- Key managers
- Trust managers

Field help

Specifies the Secur Sockets Layer (SSL configuration that i by requests at this

Page help

More information a this page

Command Assistan

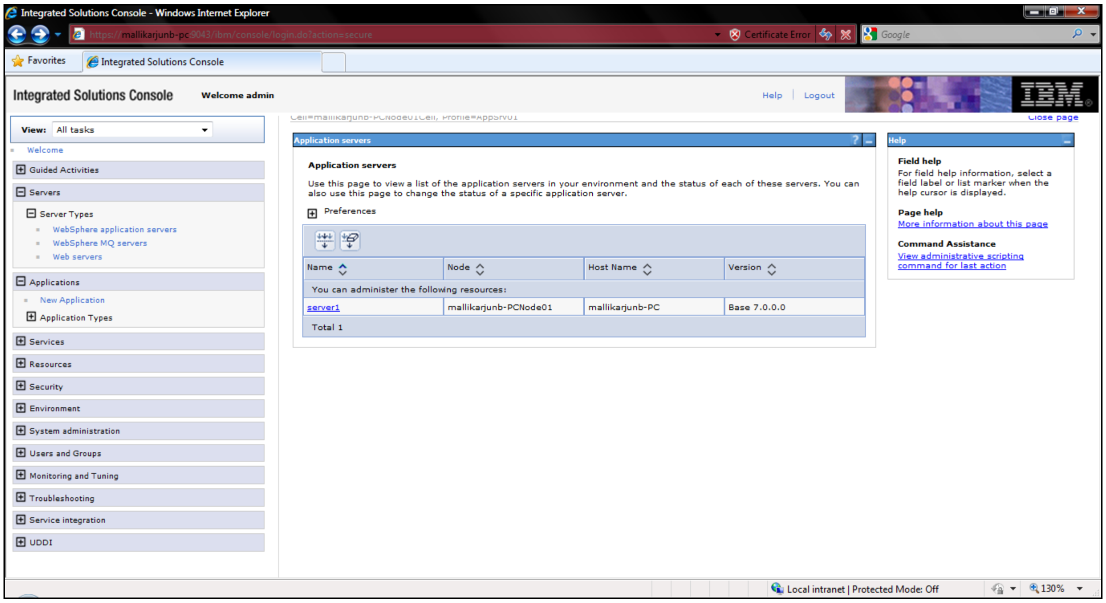
View administrative scripting command action

Under SSL configurations, select the configured SSL from the drop-down list.

Click the button ‘Update certificate alias list’. Click ‘Apply’ and save the changes.

1.6 SSL Settings at Application server level

Go to the servers available on the left and click the application servers link which will refresh the window on the right side to display the details pertaining to application servers



Cell=mallikarjunb-PCNode01Cell, Profile=AppSrv01

Application servers

Application servers

Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page to change the status of a specific application server.

⊞ Preferences

Name	Node	Host Name	Version
You can administer the following resources:			
server1	mallikarjunb-PCNode01	mallikarjunb-PC	Base 7.0.0.0
Total 1			

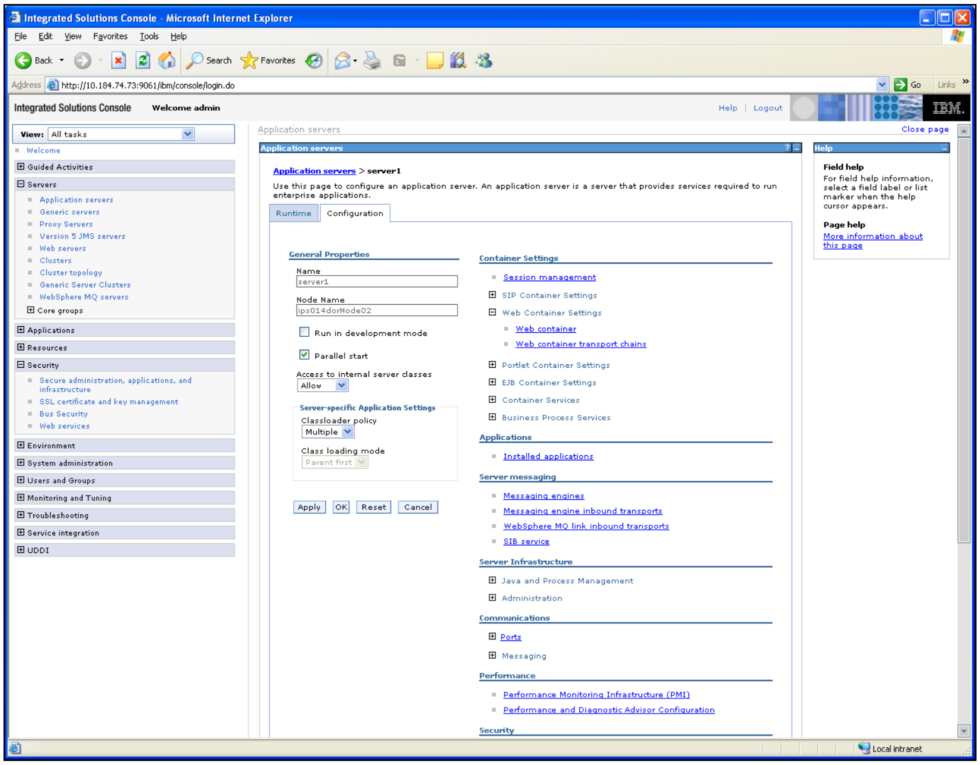
Help

Field help
For field help information, select a field label or list marker when the help cursor is displayed.

Page help
More information about this page

Command Assistance
View administrative scripting command for last action

Click the server to which SSL configuration has to be applied. The following screen is displayed.



Application servers

Application servers > server1

Use this page to configure an application server. An application server is a server that provides services required to run enterprise applications.

Runtime | Configuration

General Properties

Name
server1

Node Name
ips014dorNode02

☐ Run in development mode

☑ Parallel start

Access to internal server classes
Allow

Server-specific Application Settings

Classloader policy
Multiple

Class loading mode
Parent first

Apply | OK | Reset | Cancel

Container Settings
- Session management
- ⊞ SIP Container Settings
- ⊟ Web Container Settings
  - Web container
  - Web container transport chains
- ⊞ Portlet Container Settings
- ⊞ EJB Container Settings
- ⊞ Container Services
- ⊞ Business Process Services

Applications
- Installed applications

Server messaging
- Messaging engines
- Messaging engine inbound transports
- WebSphere MQ link inbound transports
- SIB service

Server Infrastructure
- ⊞ Java and Process Management
- ⊞ Administration

Communications
- ⊞ Ports
- ⊞ Messaging

Performance
- Performance Monitoring Infrastructure (PMI)
- Performance and Diagnostic Advisor Configuration

Security

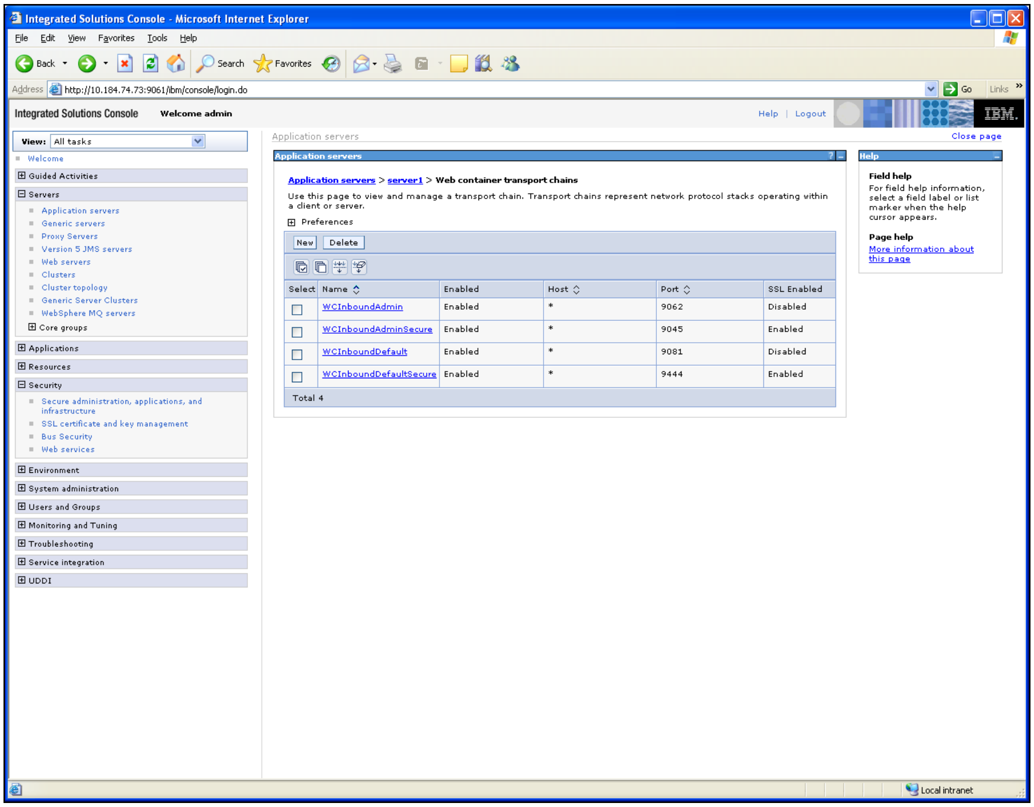
Help

Field help
For field help information, select a field label or list marker when the help cursor appears.

Page help
More information about this page

Go to Configuration tab and click 'Web container transport chains' under 'Container settings'.

The following screen is displayed.



Application servers > server1 > Web container transport chains

Use this page to view and manage a transport chain. Transport chains represent network protocol stacks operating within a client or server.

⊞ Preferences

Select	Name	Enabled	Host	Port	SSL Enabled
□	WCInboundAdmin	Enabled	*	9062	Disabled
□	WCInboundAdminSecure	Enabled	*	9045	Enabled
□	WCInboundDefault	Enabled	*	9081	Disabled
□	WCInboundDefaultSecure	Enabled	*	9444	Enabled
Total 4					

Field help

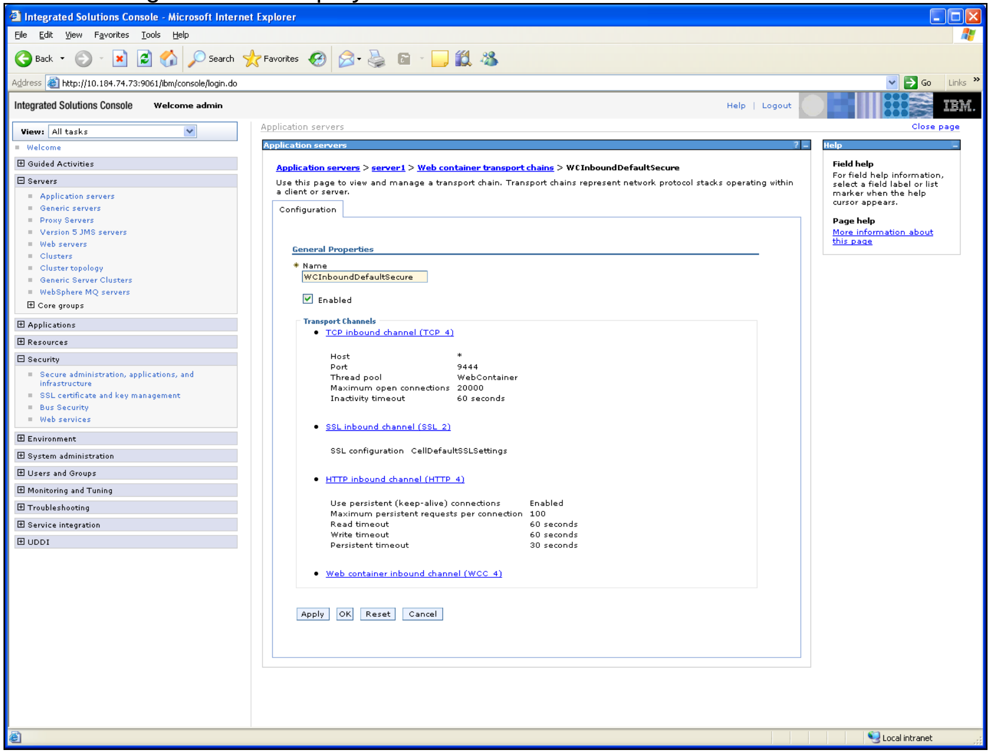
For field help information, select a field label or list marker when the help cursor appears.

Page help

More information about this page

Against their respective names, the secured connection is available under the column ‘SSL Enabled’. Click ‘WCInboundDefaultSecure’.

The following screen is displayed:



Application servers

Application servers > **server1** > **Web container transport chains** > **WCInboundDefaultSecure**

Use this page to view and manage a transport chain. Transport chains represent network protocol stacks operating within a client or server.

Configuration

General Properties

* Name
WCInboundDefaultSecure

☑ Enabled

Transport Channels

- TCP inbound channel (TCP 4)

```
Host                       *
Port                       9444
Thread pool                WebContainer
Maximum open connections   20000
Inactivity timeout         60 seconds
```

- SSL inbound channel (SSL 2)

```
SSL configuration   CellDefaultSSLSettings
```

- HTTP inbound channel (HTTP 4)

```
Use persistent (keep-alive) connections        Enabled
Maximum persistent requests per connection     100
Read timeout                                   60 seconds
Write timeout                                  60 seconds
Persistent timeout                             30 seconds
```

- Web container inbound channel (WCC 4)

Apply OK Reset Cancel

Help

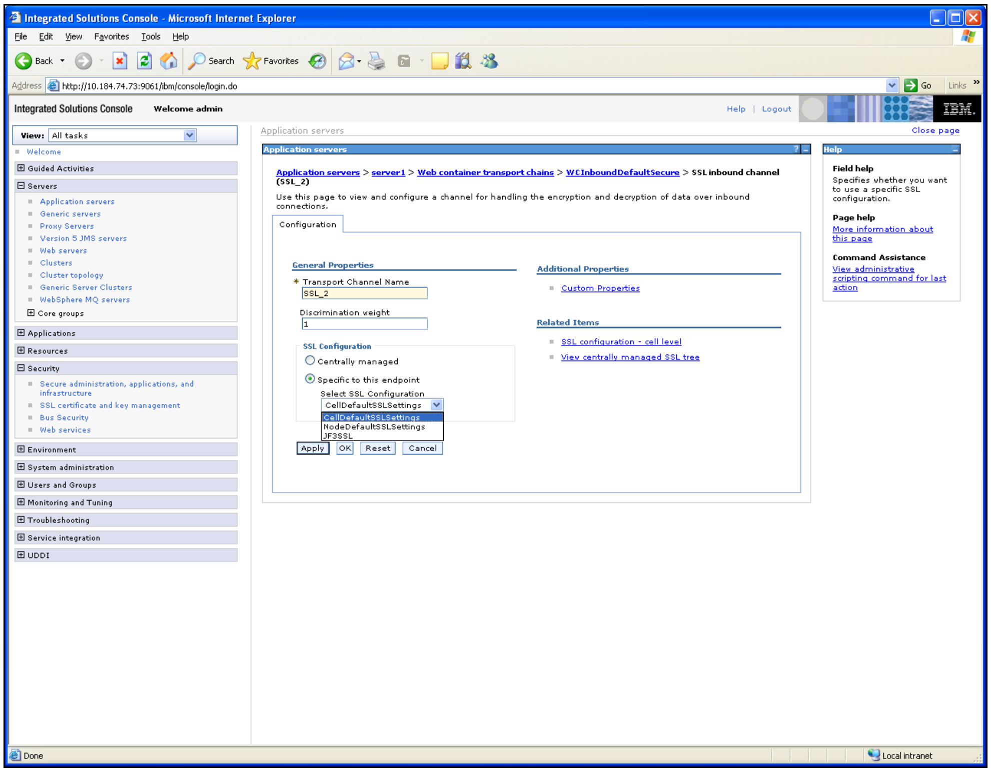
Field help

For field help information, select a field label or list marker when the help cursor appears.

Page help

More information about this page

Click ‘SSL Inbound channel (SSL 2).



Application servers

Application servers > **server1** > **Web container transport chains** > **WCInboundDefaultSecure** > **SSL inbound channel (SSL_2)**

Use this page to view and configure a channel for handling the encryption and decryption of data over inbound connections.

Configuration

General Properties

* Transport Channel Name
SSL_2

Discrimination weight
1

SSL Configuration

○ Centrally managed

● Specific to this endpoint

Select SSL Configuration
CellDefaultSSLSettings
CellDefaultSSLSettings
NodeDefaultSSLSettings
JF3SSL

Apply OK Reset Cancel

Additional Properties

- Custom Properties

Related Items

- SSL configuration - cell level
- View centrally managed SSL tree

Help

Field help

Specifies whether you want to use a specific SSL configuration.

Page help

More information about this page

Command Assistance

View administrative scripting command for last action

Select the configured SSL from the list of SSL configurations. Click ‘Apply’ and save the changes.

1.7 Running Application with SSL

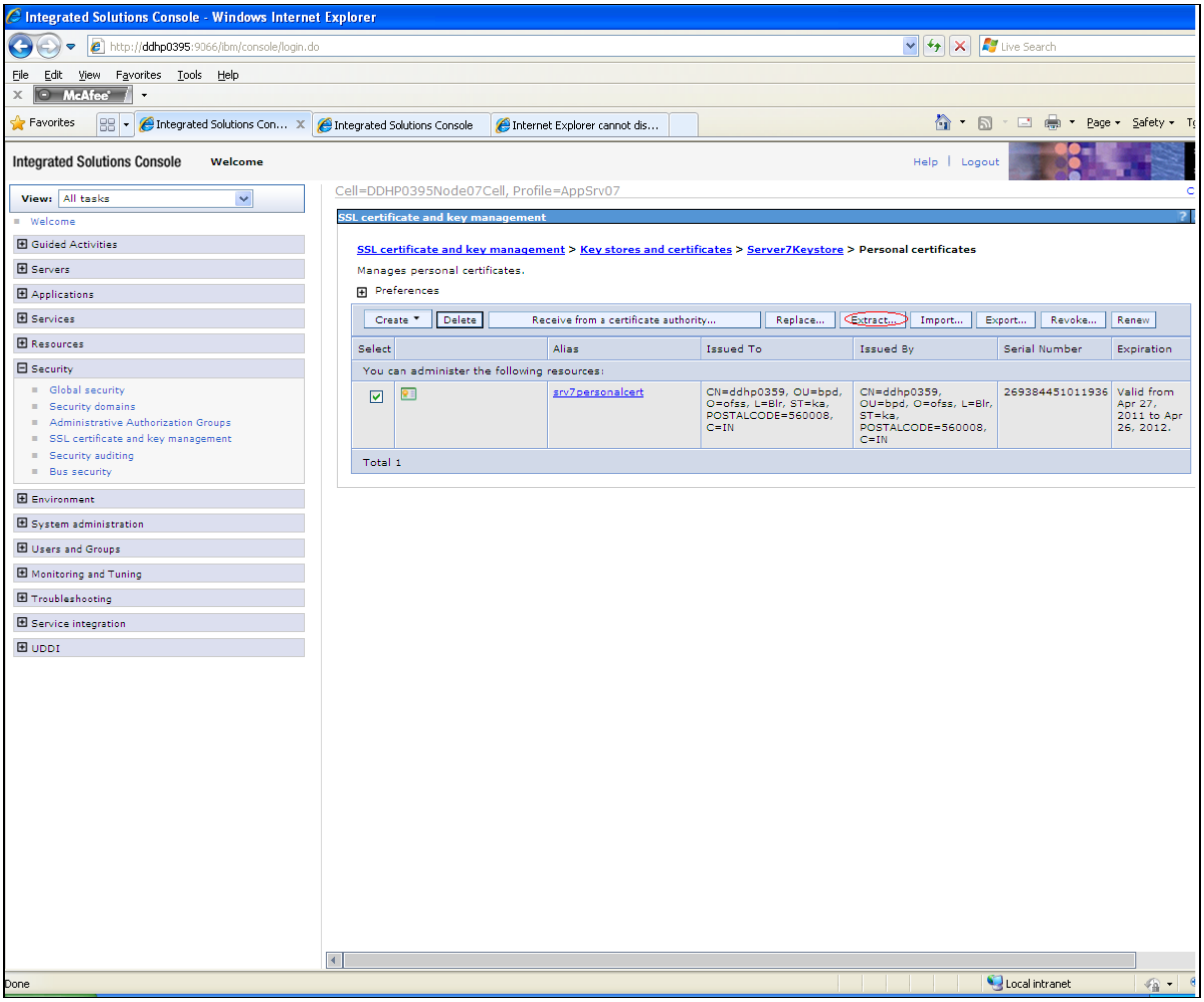
To run the application with SSL, use the following syntax:

https://<<ip address or host name>>:<<port number>>/<<context>>>

1.8 Certificate Exchange for Two Ways SSL

1.8.1 Extracting Certificate for Server1

The process of extracting certificate for Server 1 is described below.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > Server7Keystore > Personal certificates

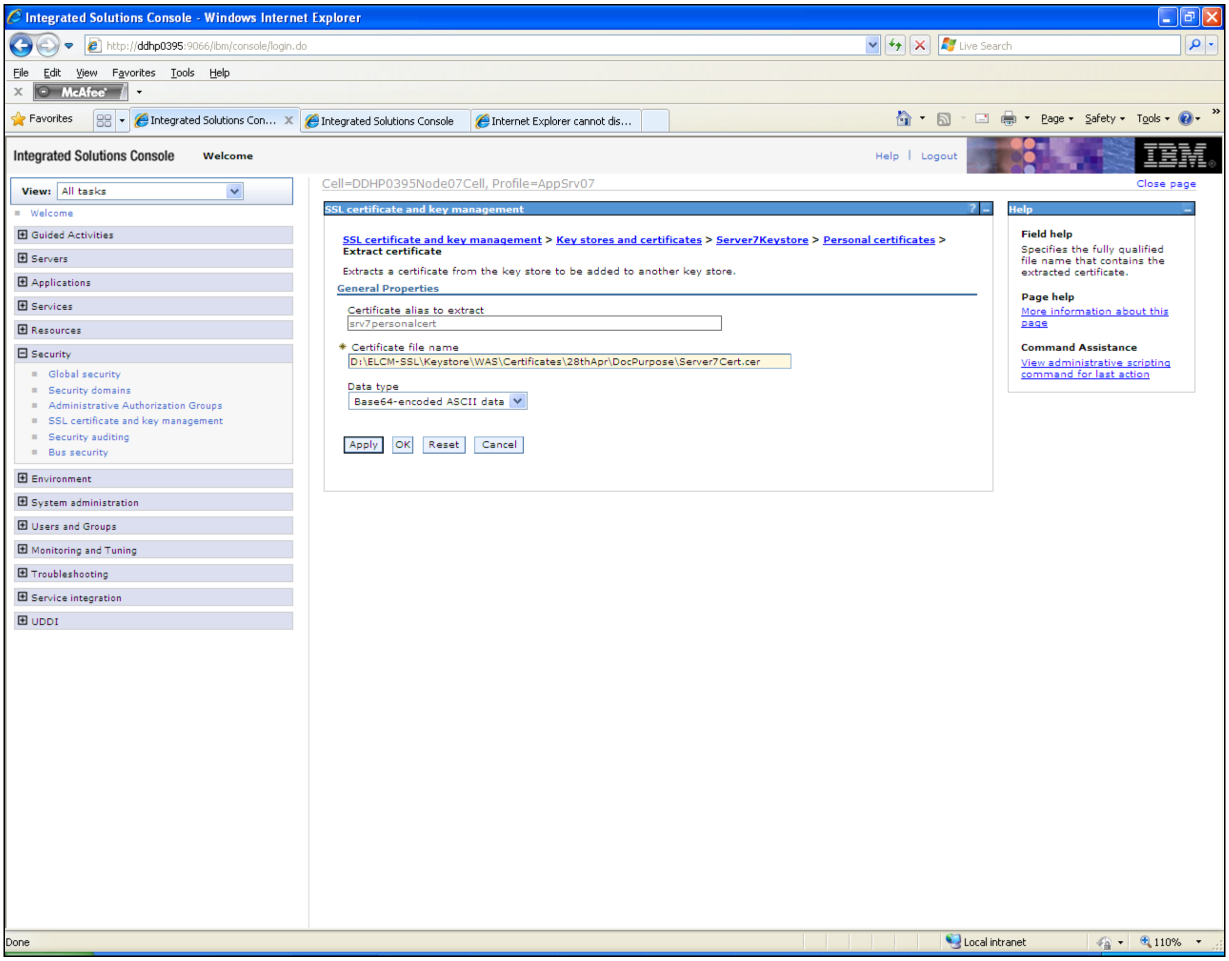
Manages personal certificates.

⊞ Preferences

Select		Alias	Issued To	Issued By	Serial Number	Expiration
You can administer the following resources:						
☑		srv7personalcert	CN=ddhp0359, OU=bpd, O=ofss, L=Blr, ST=ka, POSTALCODE=560008, C=IN	CN=ddhp0359, OU=bpd, O=ofss, L=Blr, ST=ka, POSTALCODE=560008, C=IN	269384451011936	Valid from Apr 27, 2011 to Apr 26, 2012.
Total 1						

On the left pane of the screen, expand ‘Security’. Go to ‘SSL certificate and key management > Key stores and certificates > ELCMKeyStore > Personal certificates.

Select the installed certificate and click ‘Extract’ button.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > Server7Keystore > Personal certificates >
Extract certificate

Extracts a certificate from the key store to be added to another key store.

General Properties

Certificate alias to extract: srv7personalcert

* Certificate file name: D:\ELCM-SSL\Keystore\WAS\Certificates\28thApr\DocPurpose\Server7Cert.cer

Data type: Base64-encoded ASCII data

Apply OK Reset Cancel

Field help
Specifies the fully qualified file name that contains the extracted certificate.

Page help
More information about this page

Command Assistance
View administrative scripting command for last action

Specify the location to save the certificate. This will be used to add in the other server. Ensure that the file has been created in the location.

Eg: \<localfolder>\<server1.cer>

Similarly extract the certificate for the second server.

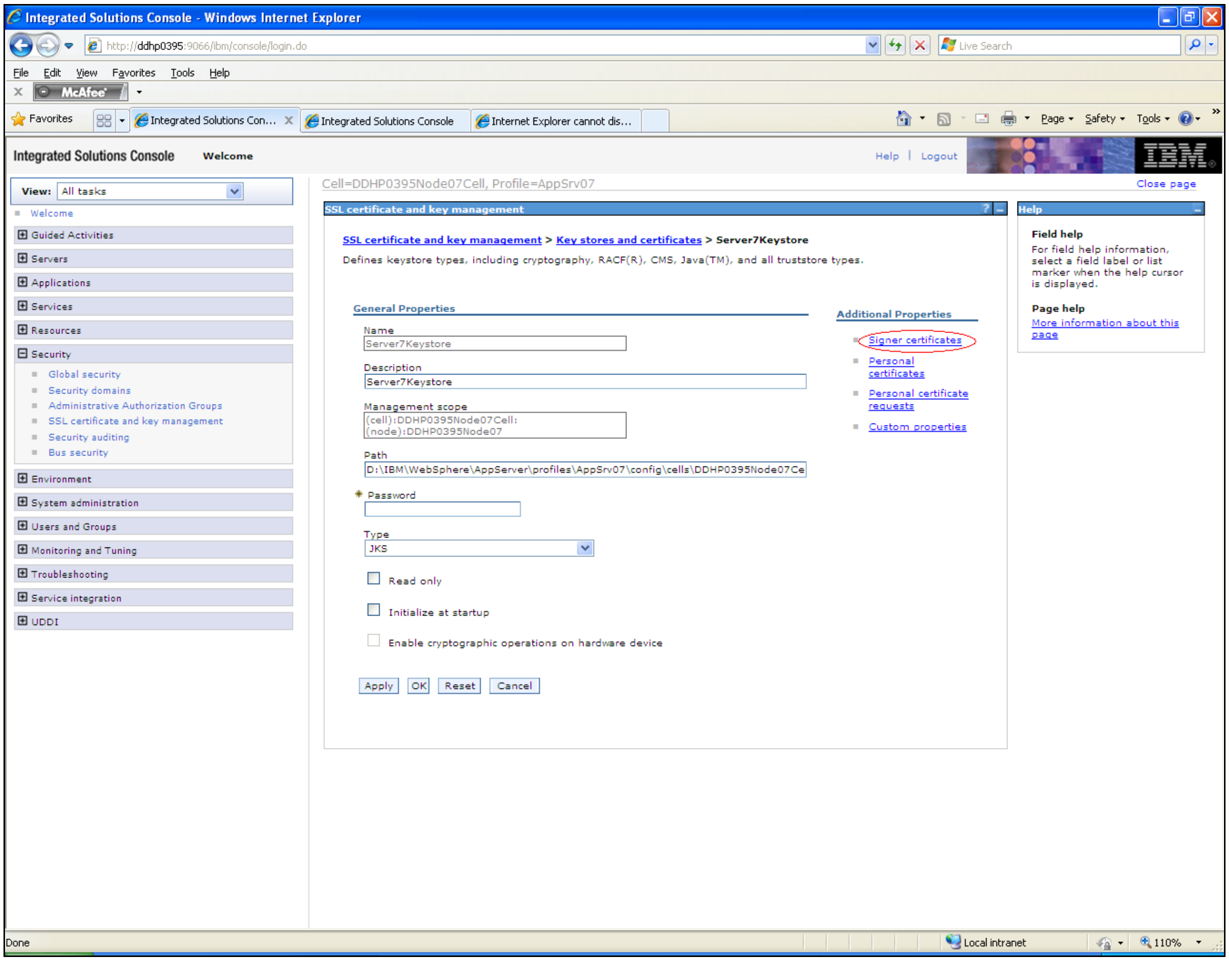
Eg: \<localfolder>\<server2.cer>

1.8.2 Extracting Certificate for Server2

You can follow the steps for server 1 described under ‘Extracting Certificate for Server1’ to extract the certificate for Server2.

1.8.3 Importing Certificate into Keystore for Server1

Go to the other server. Expand ‘Security > SSL certificate and key management > Key stores and certificates > Server7Keystore (which is created now).



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > Server7Keystore

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

General Properties

Name
Server7Keystore

Description
Server7Keystore

Management scope
(cell):DDHP0395Node07Cell:(node):DDHP0395Node07

Path
D:\IBM\WebSphere\AppServer\profiles\AppSrv07\config\cells\DDHP0395Node07Ce

* Password

Type
JKS

□ Read only

□ Initialize at startup

□ Enable cryptographic operations on hardware device

Apply OK Reset Cancel

Additional Properties

- Signer certificates
- Personal certificates
- Personal certificate requests
- Custom properties

Field help

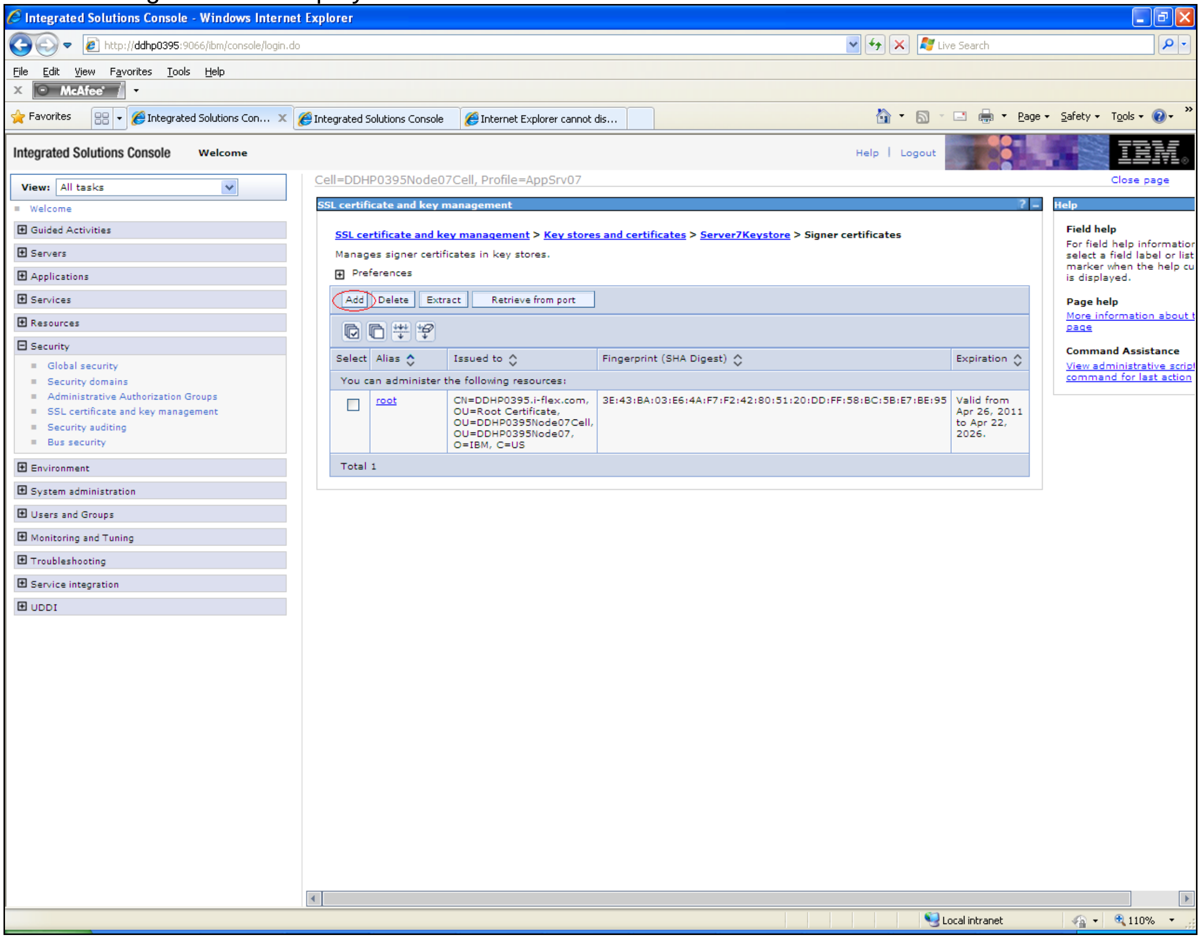
For field help information, select a field label or list marker when the help cursor is displayed.

Page help

More information about this page

Click ‘Signer certificates’.

The following screen is displayed:



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > Server7Keystore > Signer certificates

Manages signer certificates in key stores.

Preferences

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
You can administer the following resources:				
□	root	CN=DDHP0395.i-flex.com, OU=Root Certificate, OU=DDHP0395Node07Cell, OU=DDHP0395Node07, O=IBM, C=US	3E:43:BA:03:E6:4A:F7:F2:42:80:51:20:DD:FF:58:BC:5B:E7:BE:95	Valid from Apr 26, 2011 to Apr 22, 2026.
Total 1				

Help

Field help

For field help information select a field label or list marker when the help cu is displayed.

Page help

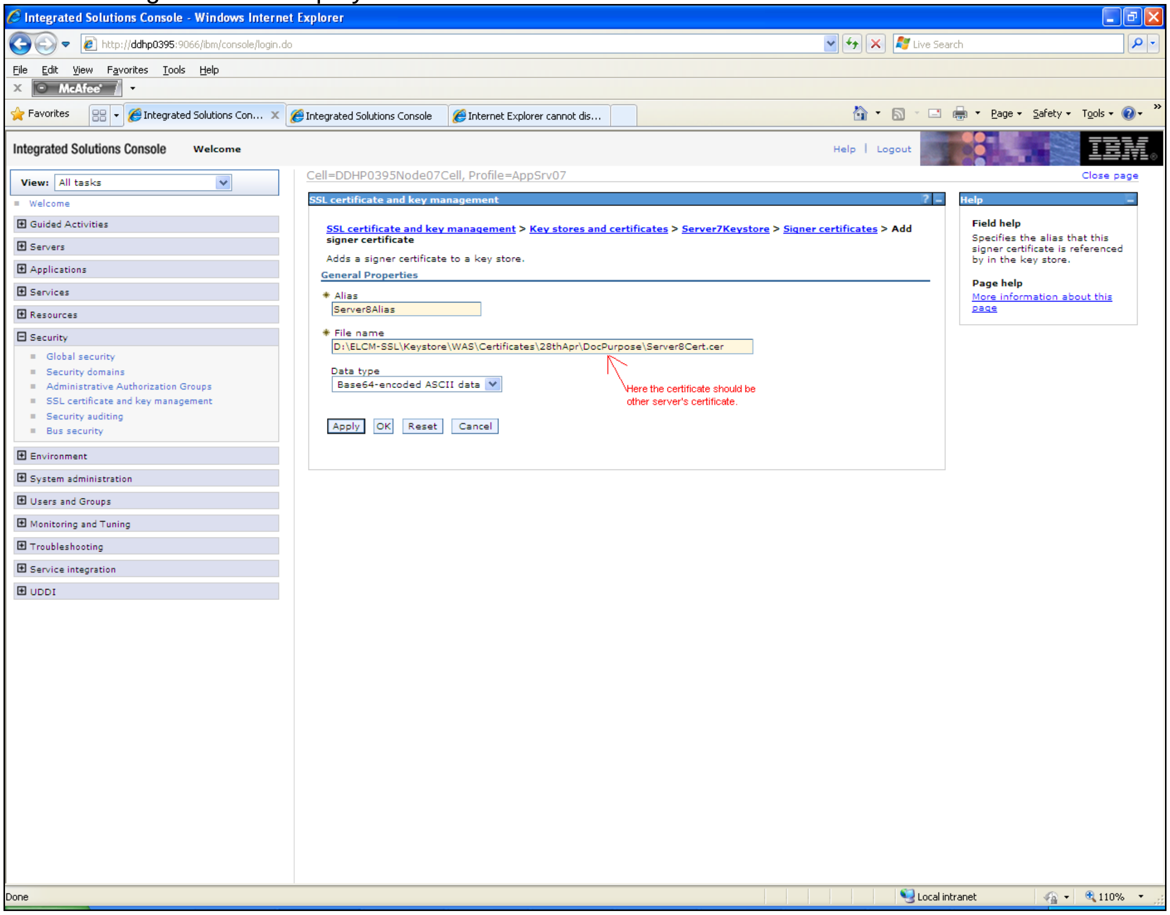
More information about t page

Command Assistance

View administrative script command for last action

Click ‘Add’ button to add the certificate of the other server.

The following screen is displayed:



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > Server7Keystore > Signer certificates > Add signer certificate

Adds a signer certificate to a key store.

General Properties

* Alias: Server8Alias

* File name: D:\ELCM-SSL\Keystore\WAS\Certificates\28thApr\DocPurpose\Server8Cert.cer

Data type: Base64-encoded ASCII data

Apply | OK | Reset | Cancel

Here the certificate should be other server's certificate.

Help

Field help

Specifies the alias that this signer certificate is referenced by in the key store.

Page help

More information about this page

The extracted certificate of the second server has to be imported to the key-store and trust-store of first server. This has to be done using the same local path where the extract certificate was generated for the first server.

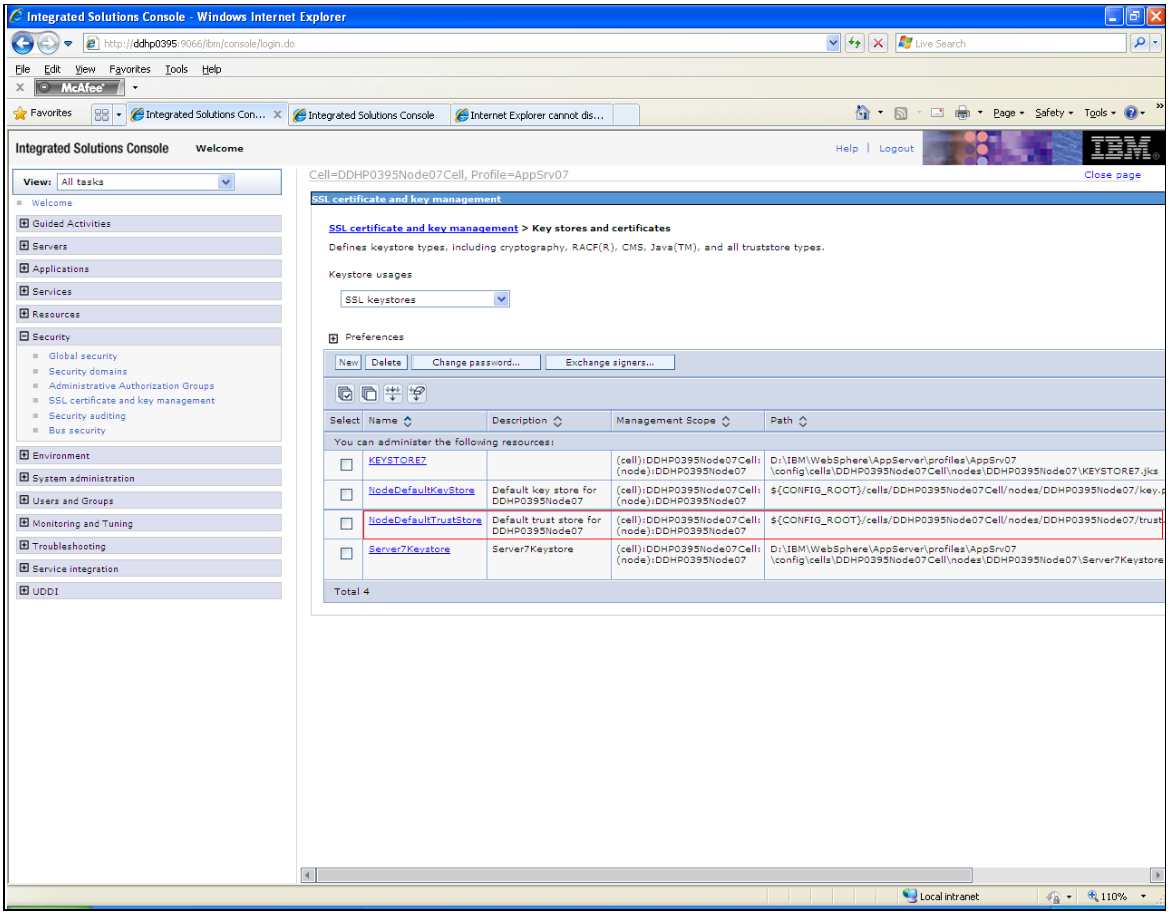
Eg: \<localfolder>\<server1.cer>

1.8.4 Importing Certificate into Keystore for Server2

You can follow the steps for server 1 described under ‘Importing Certificate into Keystore for Server1’ to import the certificate into keystore for Server2.

1.8.5 Importing Certificate into Truststore for Server1

Expand ‘SSL certificate and key management > Key stores and certificates and click ‘NodeDefaultTrustStore’.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

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

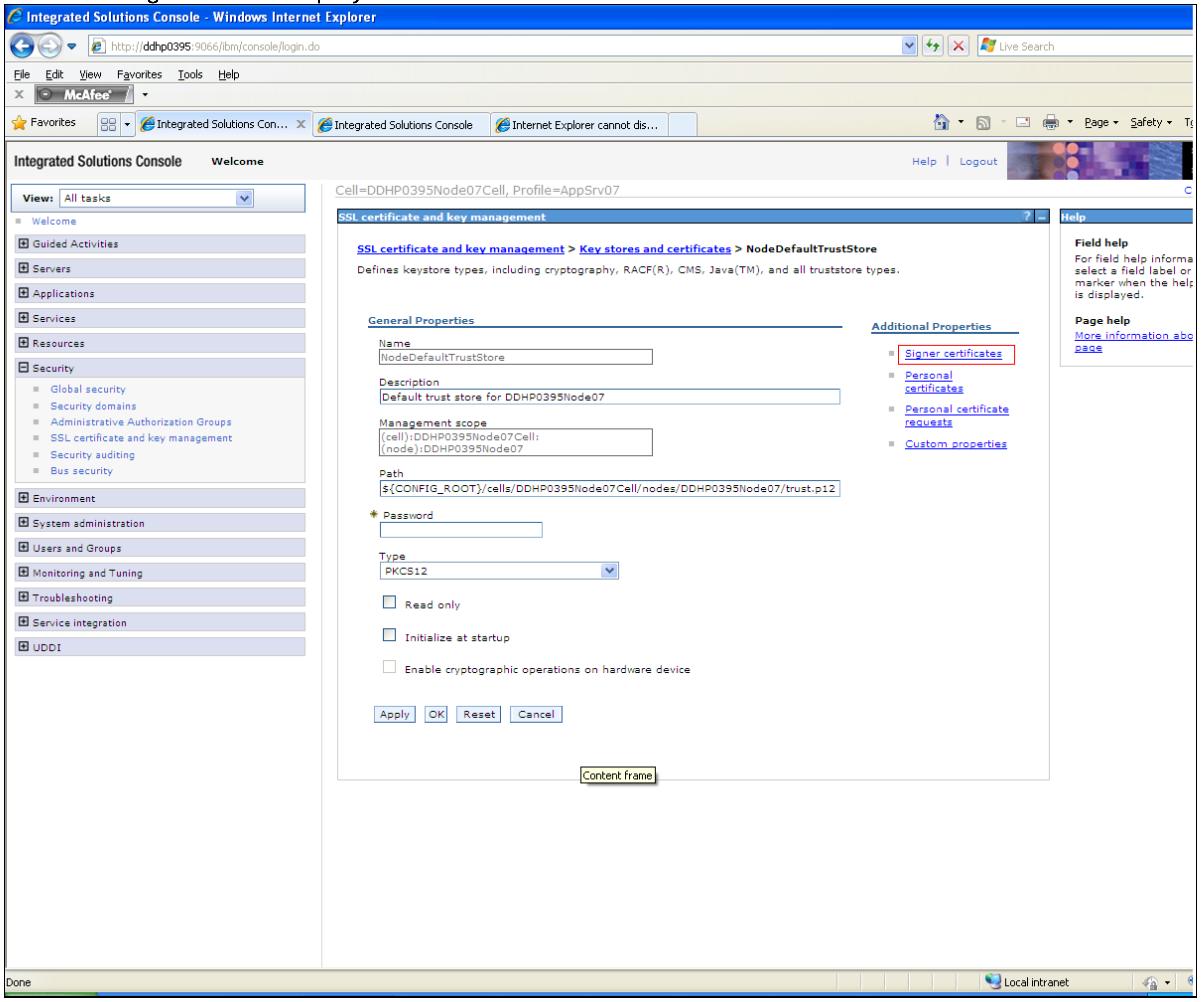
Preferences

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

Select	Name	Description	Management Scope	Path
You can administer the following resources:				
□	KEYSTORE7		(cell):DDHP0395Node07Cell:(node):DDHP0395Node07	D:\IBM\WebSphere\AppServer\profiles\AppSrv07\config\cells\DDHP0395Node07Cell\nodes\DDHP0395Node07\KEYSTORE7.jks
□	NodeDefaultKeyStore	Default key store for DDHP0395Node07	(cell):DDHP0395Node07Cell:(node):DDHP0395Node07	${CONFIG_ROOT}/cells/DDHP0395Node07Cell/nodes/DDHP0395Node07/key.p
□	NodeDefaultTrustStore	Default trust store for DDHP0395Node07	(cell):DDHP0395Node07Cell:(node):DDHP0395Node07	${CONFIG_ROOT}/cells/DDHP0395Node07Cell/nodes/DDHP0395Node07/trust
□	Server7Keystore	Server7Keystore	(cell):DDHP0395Node07Cell:(node):DDHP0395Node07	D:\IBM\WebSphere\AppServer\profiles\AppSrv07\config\cells\DDHP0395Node07Cell\nodes\DDHP0395Node07\Server7Keystore

Total 4

The following screen is displayed.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

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

Name: NodeDefaultTrustStore

Description: Default trust store for DDHP0395Node07

Management scope: (cell):DDHP0395Node07Cell:(node):DDHP0395Node07

Path: ${CONFIG_ROOT}/cells/DDHP0395Node07Cell/nodes/DDHP0395Node07/trust.p12

* Password:

Type: PKCS12

□ Read only

□ Initialize at startup

□ Enable cryptographic operations on hardware device

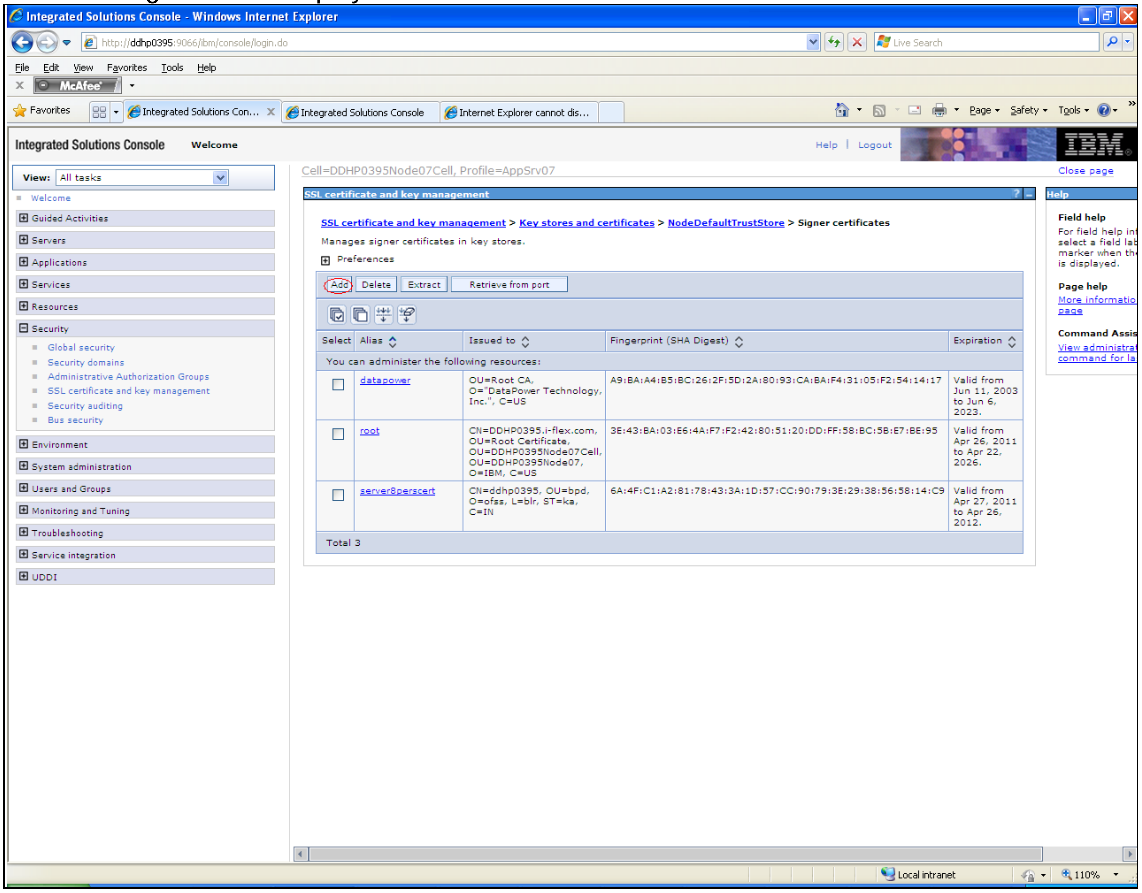
Apply | OK | Reset | Cancel

Additional Properties

- Signer certificates
- Personal certificates
- Personal certificate requests
- Custom properties

Click ‘Signer certificates’.

The following screen is displayed.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates

Manages signer certificates in key stores.

⊞ Preferences

Add | Delete | Extract | Retrieve from port

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
You can administer the following resources:				
□	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.
□	root	CN=DDHP0395.i-flex.com, OU=Root Certificate, OU=DDHP0395Node07Cell, OU=DDHP0395Node07, O=IBM, C=US	3E:43:BA:03:E6:4A:F7:F2:42:80:51:20:DD:FF:58:BC:5B:E7:BE:95	Valid from Apr 26, 2011 to Apr 22, 2026.
□	server8perscert	CN=ddhp0395, OU=bpd, O=ofss, L=blr, ST=ka, C=IN	6A:4F:C1:A2:81:78:43:3A:1D:57:CC:90:79:3E:29:38:56:58:14:C9	Valid from Apr 27, 2011 to Apr 26, 2012.
Total 3				

Field help

For field help in select a field lab marker when th is displayed.

Page help

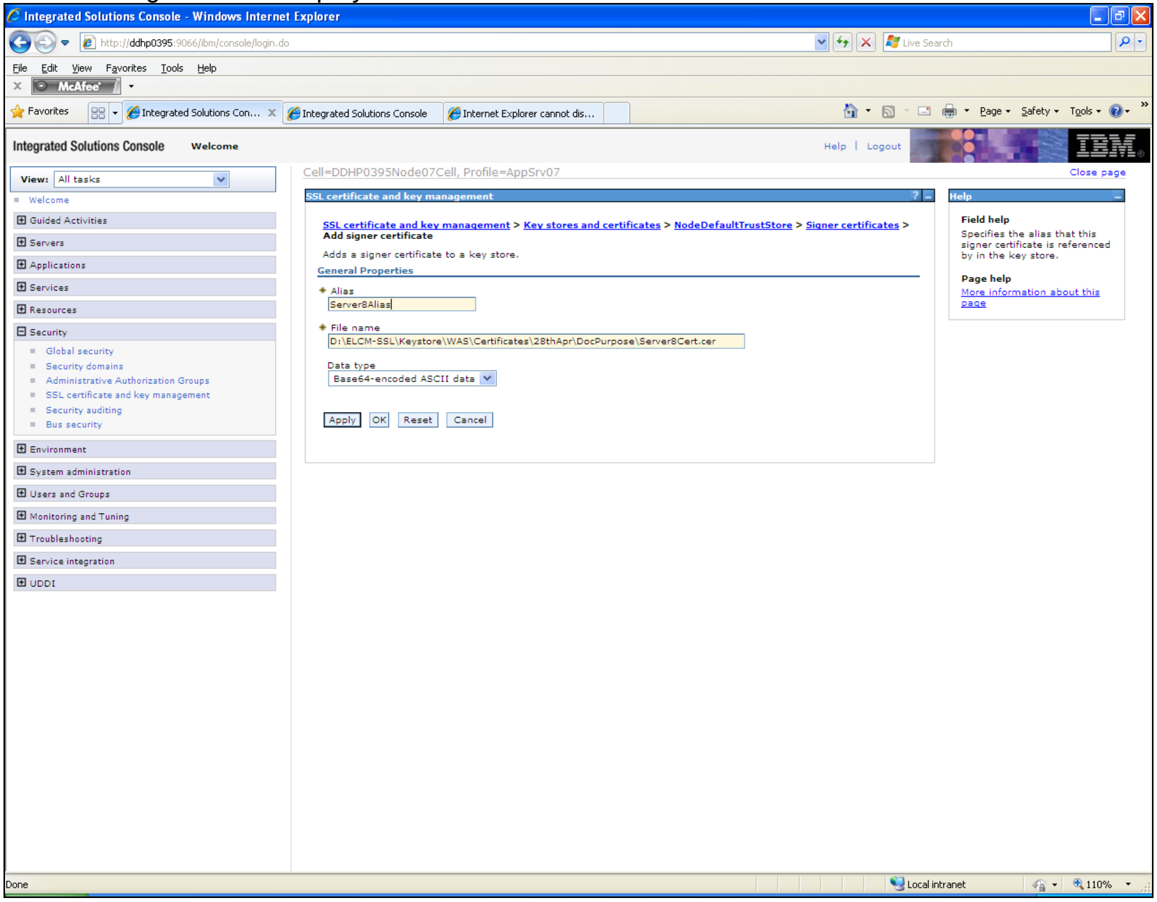
More informatio page

Command Assis

View administrat command for la

Click ‘Add’ button to add the extracted certificate of the second server.

The following screen is displayed.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates > Add signer certificate

Adds a signer certificate to a key store.

General Properties

* Alias: Server8Alias

* File name: D:\ELCM-SSL\Keystore\WAS\Certificates\28thApr\DocPurpose\Server8Cert.cer

Data type: Base64-encoded ASCII data

Apply OK Reset Cancel

Field help

Specifies the alias that this signer certificate is referenced by in the key store.

Page help

More information about this page

Specify the ‘alias’ name to identify the other server.

Eg: For server1, you can give the alias name ‘*server2Alias*’.

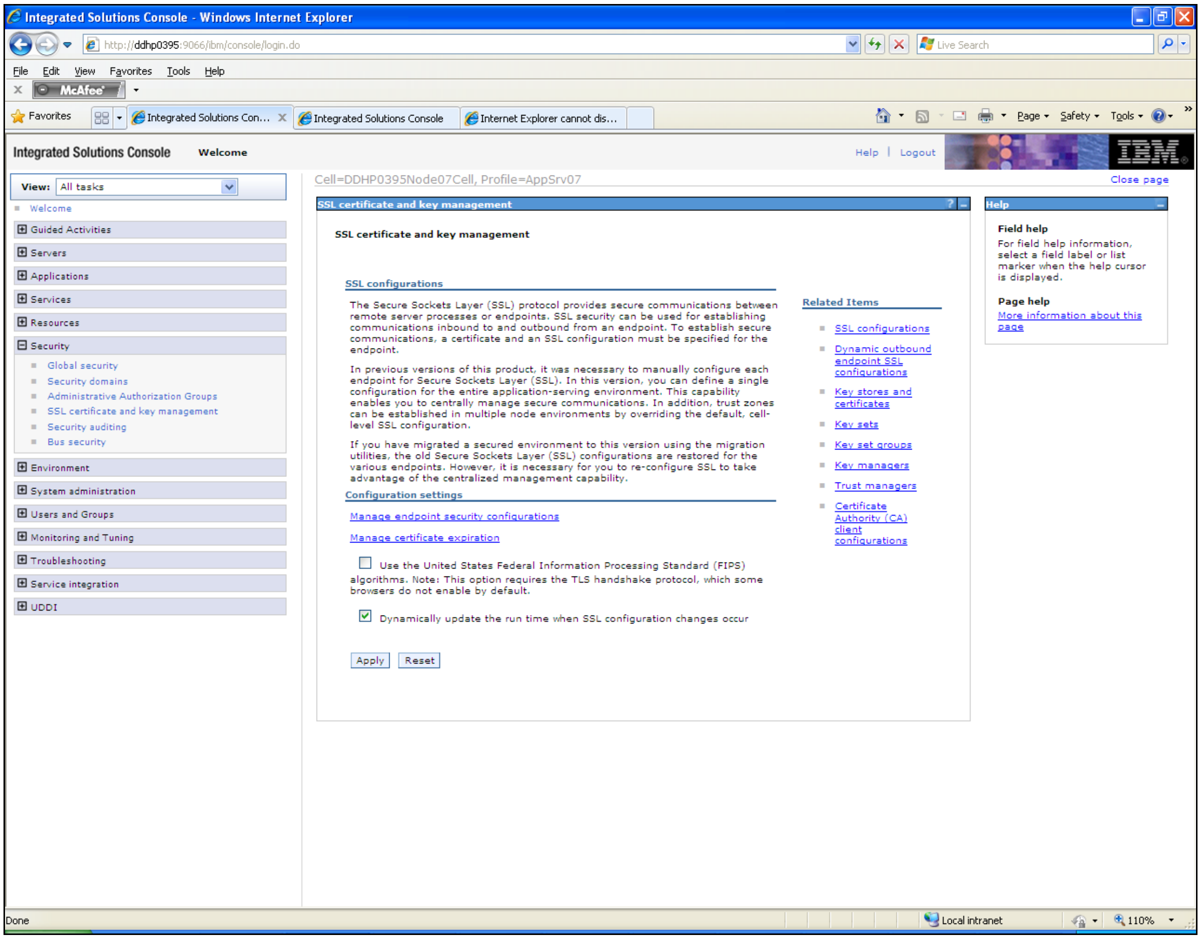
Further, specify the location of the extracted certificate.

1.8.6 Importing Certificate into Truststore for Server2

You can follow the steps for server 1 described under ‘Importing Certificate into Truststore for Server2’ to import the certificate into Truststore for Server2.

1.9 Managing Endpoint Security Configurations

To manage the endpoint security configurations, follow the instructions given below.


Integrated Solutions Console - Windows Internet Explorer
http://ddhp0395:9066/ibm/console/login.do
Live Search
File Edit View Favorites Tools Help
McAfee
Favorites
Integrated Solutions Con…
Integrated Solutions Console
Internet Explorer cannot dis…
Page Safety Tools
Integrated Solutions Console
Welcome
Help | Logout
IBM
View: All tasks
Welcome
Guided Activities
Servers
Applications
Services
Resources
Security
Global security
Security domains
Administrative Authorization Groups
SSL certificate and key management
Security auditing
Bus security
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Close page
SSL certificate and key management
Help
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
Apply
Reset
Done
Local intranet
110%

Cell=DDHP0395Node07Cell, Profile=AppSrv07

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

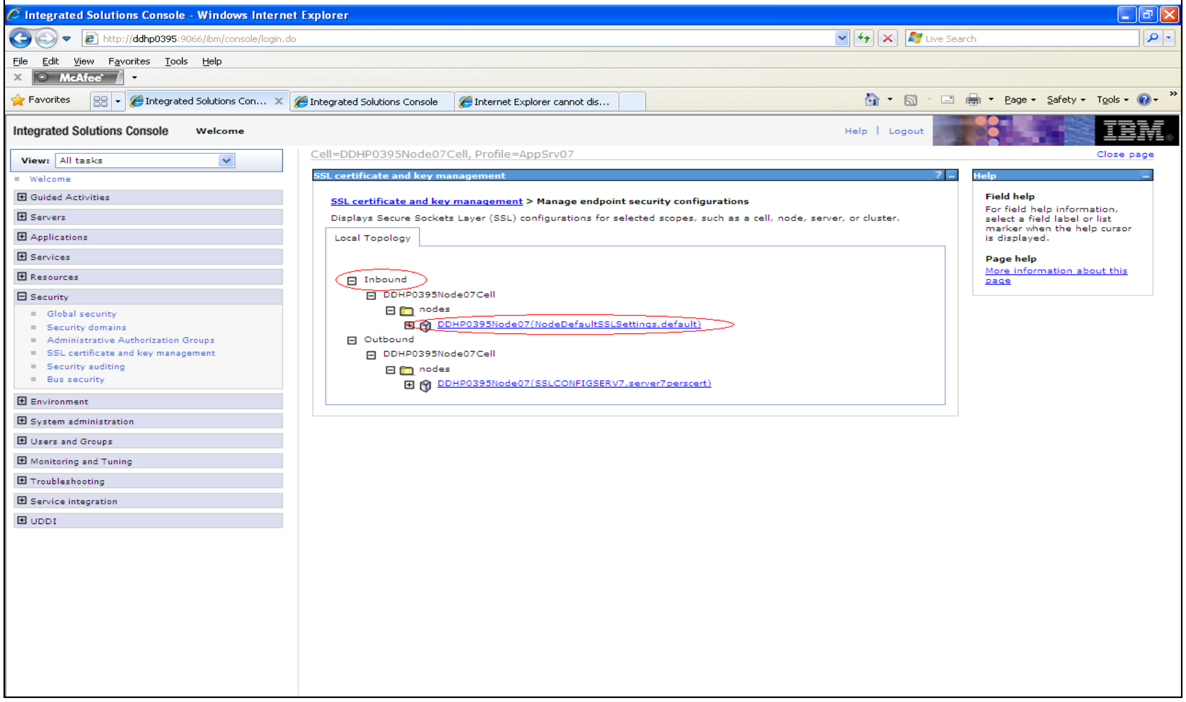
Field help

For field help information, select a field label or list marker when the help cursor is displayed.

Page help

More information about this page

Expand ‘Security > SSL certificate and key management’ and click ‘Manage endpoint security configurations’.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Manage endpoint security configurations

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

Local Topology

```
⊟ Inbound
    ⊟ DDHP0395Node07Cell
        ⊟ nodes
            ⊞ DDHP0395Node07(NodeDefaultSSLSettings,default)
⊟ Outbound
    ⊟ DDHP0395Node07Cell
        ⊟ nodes
            ⊞ DDHP0395Node07(SSLCONFIGSERV7,server7perscert)
```

Help

Field help

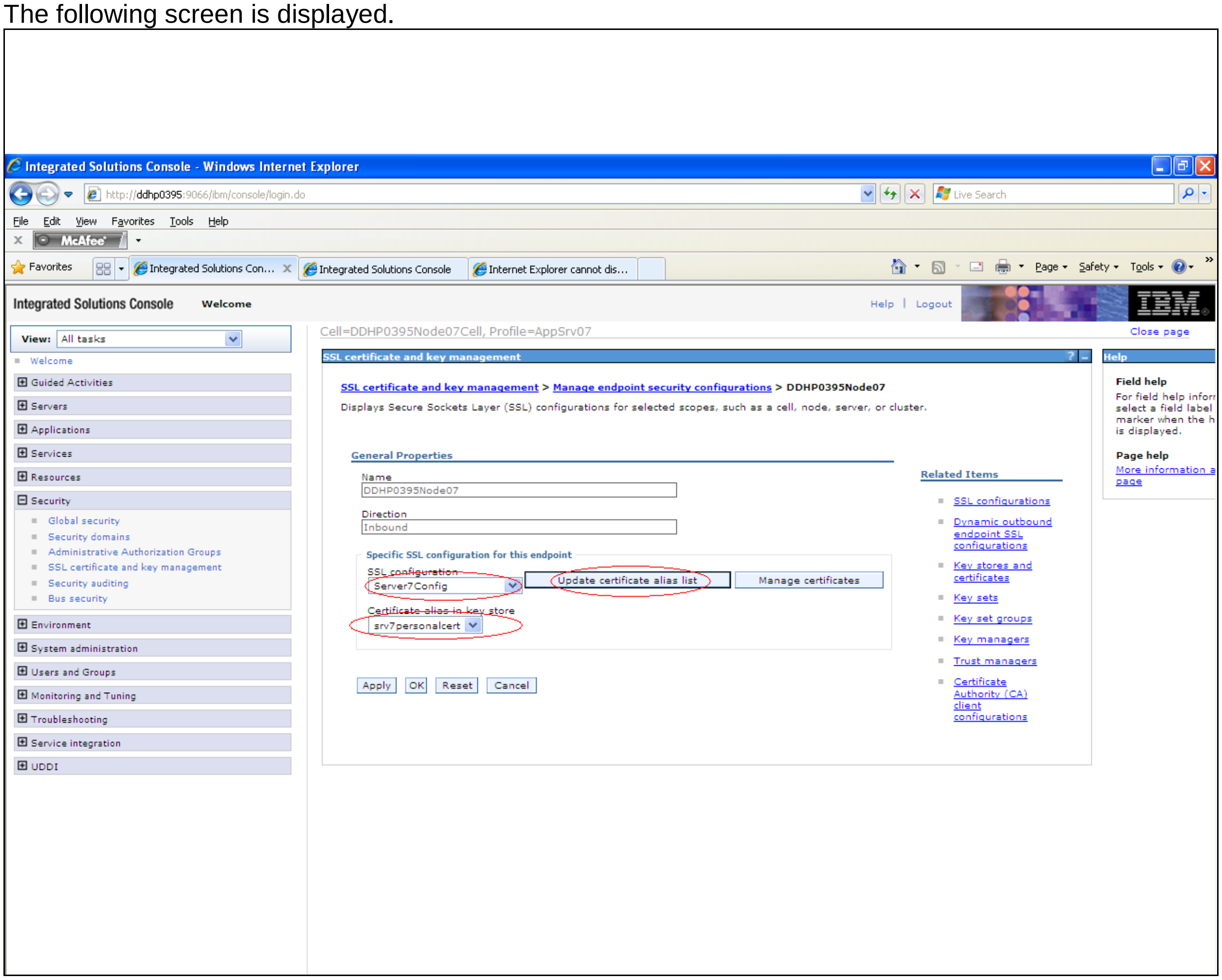
For field help information, select a field label or list marker when the help cursor is displayed.

Page help

More information about this page

Change the inbound node settings. Expand ‘Inbound’ and click ‘DDHP0395Node07(NodeDefaultSSLSettings,default)’.

The following screen is displayed.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > Manage endpoint security configurations > DDHP0395Node07

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

General Properties

Name: DDHP0395Node07

Direction: Inbound

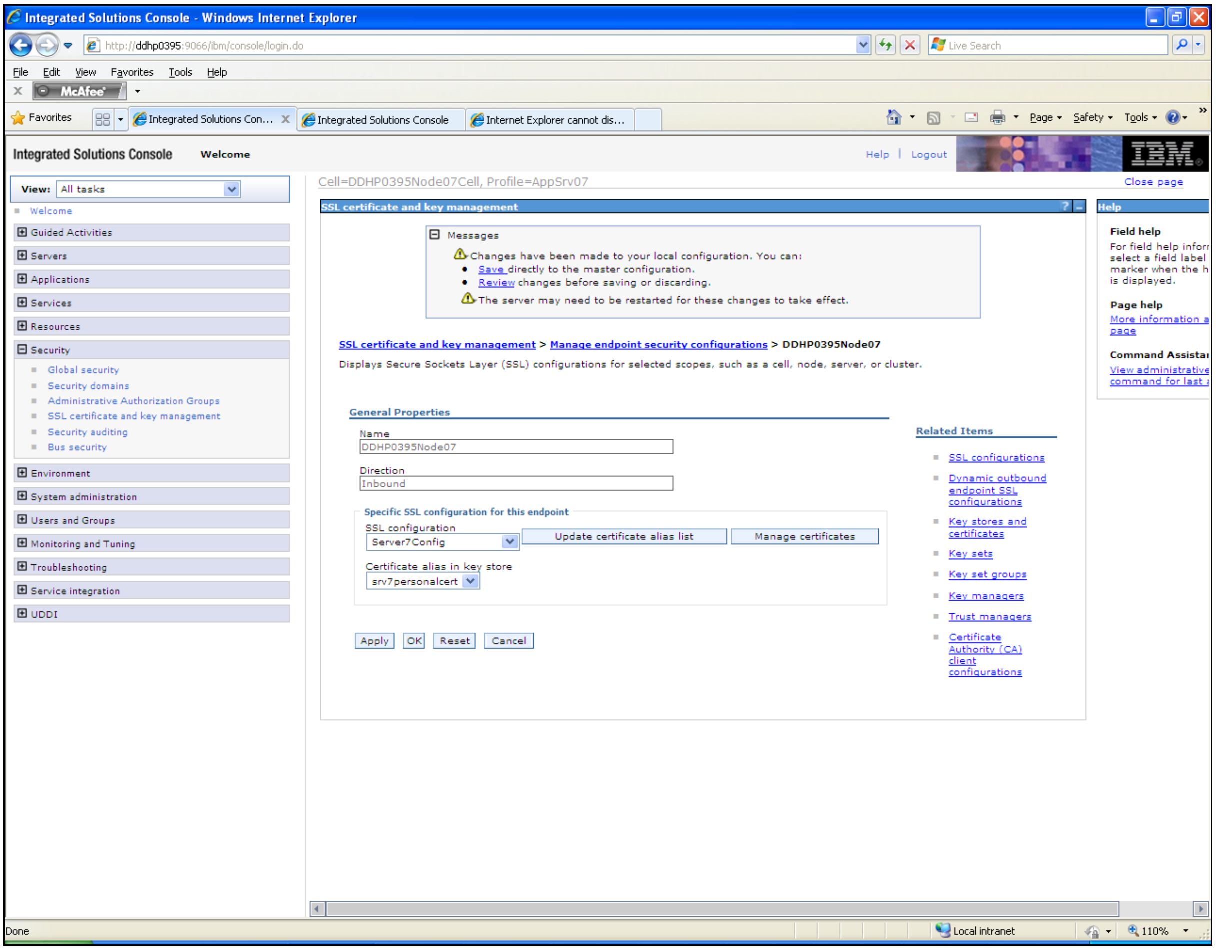
Specific SSL configuration for this endpoint

SSL configuration: Server7Config

Certificate alias in key store: srv7personalcert

Select the ‘SSL Configuration’ created which you just created. Click ‘Update certificate alias list ‘ button.

Ensure that the proper certificate and SSL configuration are selected. Further, click ‘Apply’ and save the settings.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

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 > Manage endpoint security configurations > DDHP0395Node07

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

General Properties

Name: DDHP0395Node07

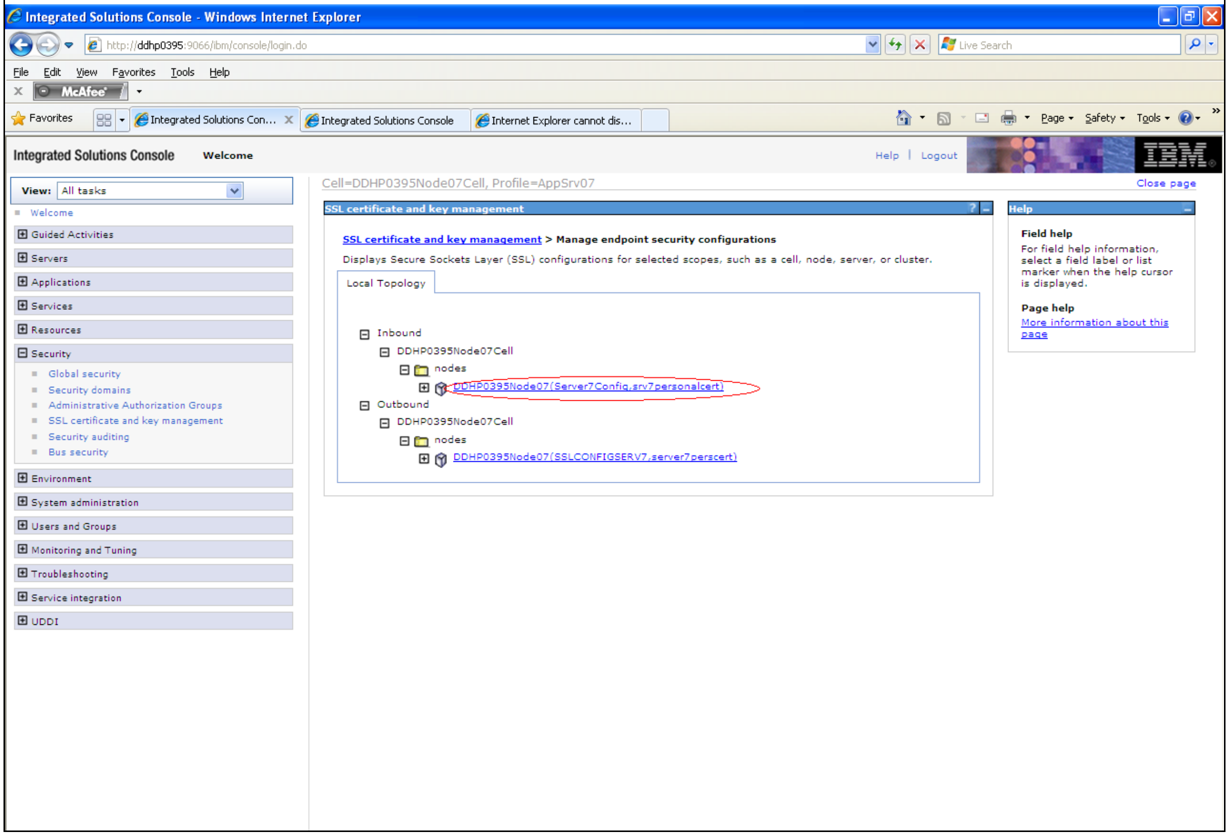
Direction: Inbound

Specific SSL configuration for this endpoint

SSL configuration: Server7Config

Certificate alias in key store: srv7personalcert

You can view the settings under 'Inbound'.


Integrated Solutions Console - Windows Internet Explorer
http://ddhp0395:9066/ibm/console/login.do
Live Search
File Edit View Favorites Tools Help
McAfee
Favorites
Integrated Solutions Con...
Integrated Solutions Console
Internet Explorer cannot dis...
Page Safety Tools
Integrated Solutions Console
Welcome
Help | Logout
IBM
View: All tasks
Welcome
Guided Activities
Servers
Applications
Services
Resources
Security
Global security
Security domains
Administrative Authorization Groups
SSL certificate and key management
Security auditing
Bus security
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Close page
Help
Field help
For field help information, select a field label or list marker when the help cursor is displayed.
Page help
More information about this page

Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

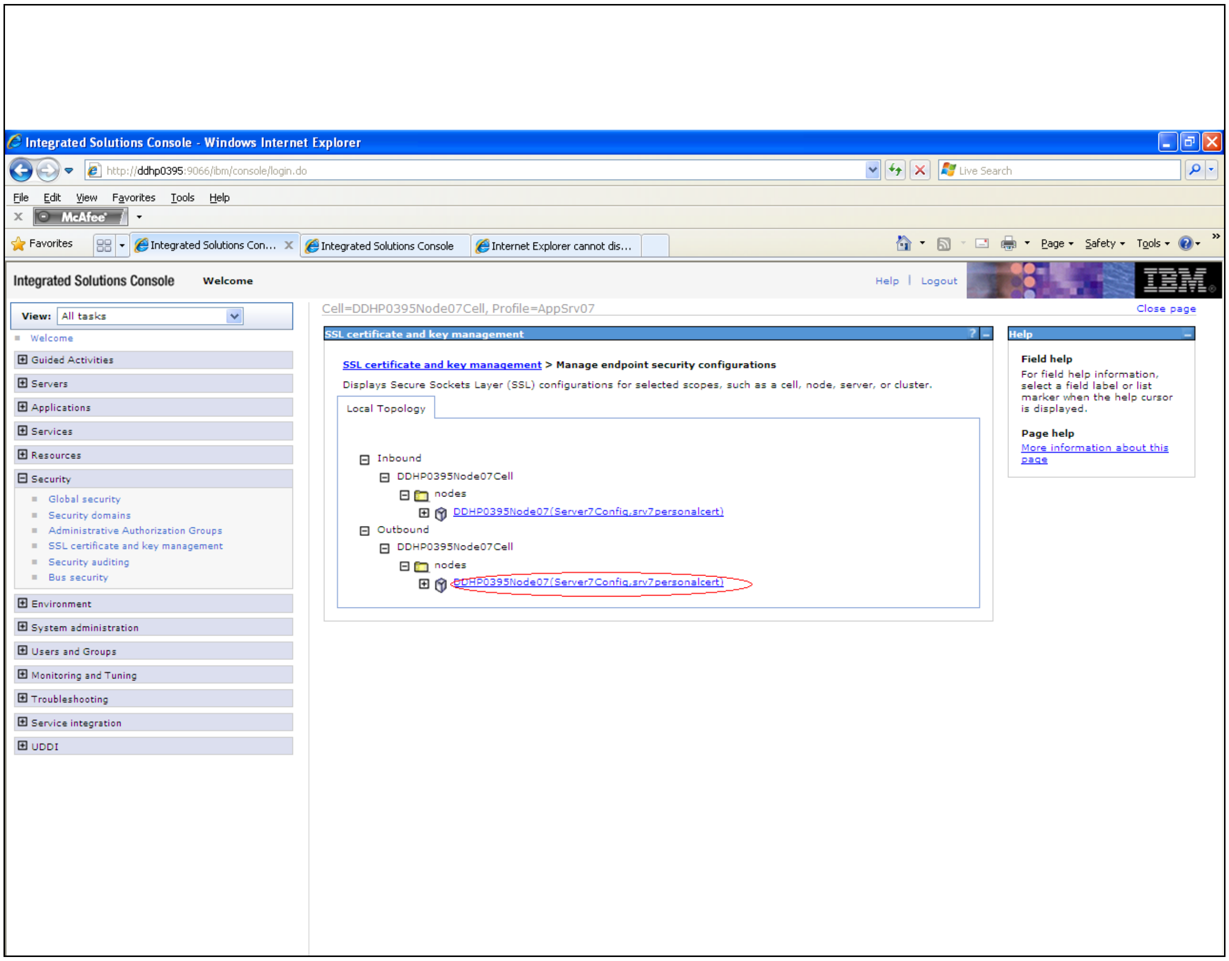
SSL certificate and key management > Manage endpoint security configurations

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

Local Topology

```
⊟ Inbound
   ⊟ DDHP0395Node07Cell
      ⊟ nodes
         ⊞ DDHP0395Node07(Server7Config,srv7personalcert)
⊟ Outbound
   ⊟ DDHP0395Node07Cell
      ⊟ nodes
         ⊞ DDHP0395Node07(SSLCONFIGSERV7,server7perscert)
```

Repeat the above steps for ‘Outbound’ as well.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > **Manage endpoint security configurations**

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

Local Topology

```
⊟ Inbound
    ⊟ DDHP0395Node07Cell
        ⊟ nodes
            ⊞ DDHP0395Node07(Server7Config,srv7personalcert)
⊟ Outbound
    ⊟ DDHP0395Node07Cell
        ⊟ nodes
            ⊞ DDHP0395Node07(Server7Config,srv7personalcert)
```

Help

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

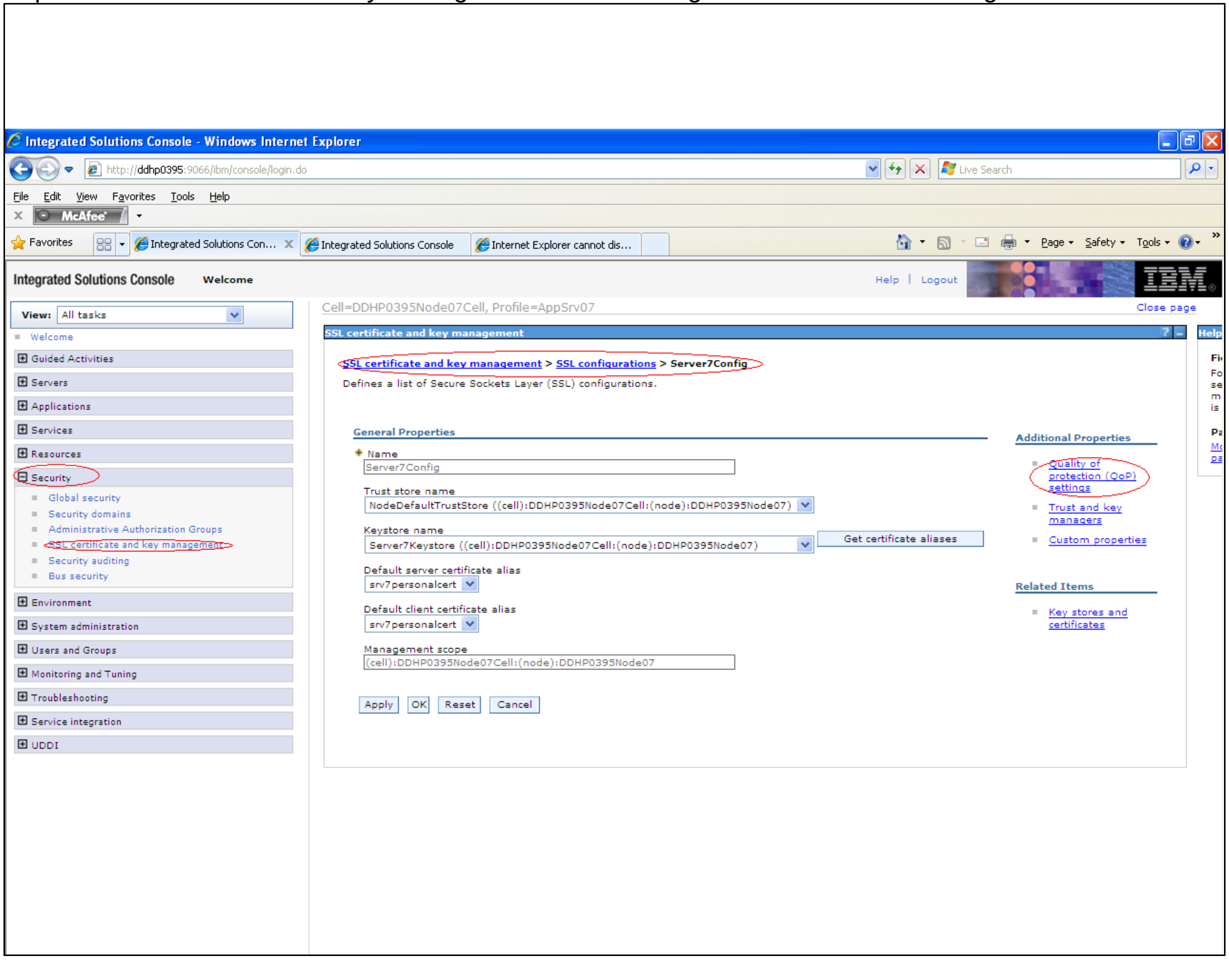
Page help

More information about this page

You need to repeat the above steps for server2 also.

1.10 Protection Quality

Expand ‘SSL certificate and key management > SSL configurations > Server7Config’.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > SSL configurations > Server7Config

Defines a list of Secure Sockets Layer (SSL) configurations.

General Properties

* Name
Server7Config

Trust store name
NodeDefaultTrustStore ((cell):DDHP0395Node07Cell:(node):DDHP0395Node07)

Keystore name
Server7Keystore ((cell):DDHP0395Node07Cell:(node):DDHP0395Node07)

Get certificate aliases

Default server certificate alias
srv7personalcert

Default client certificate alias
srv7personalcert

Management scope
(cell):DDHP0395Node07Cell:(node):DDHP0395Node07

Apply OK Reset Cancel

Additional Properties

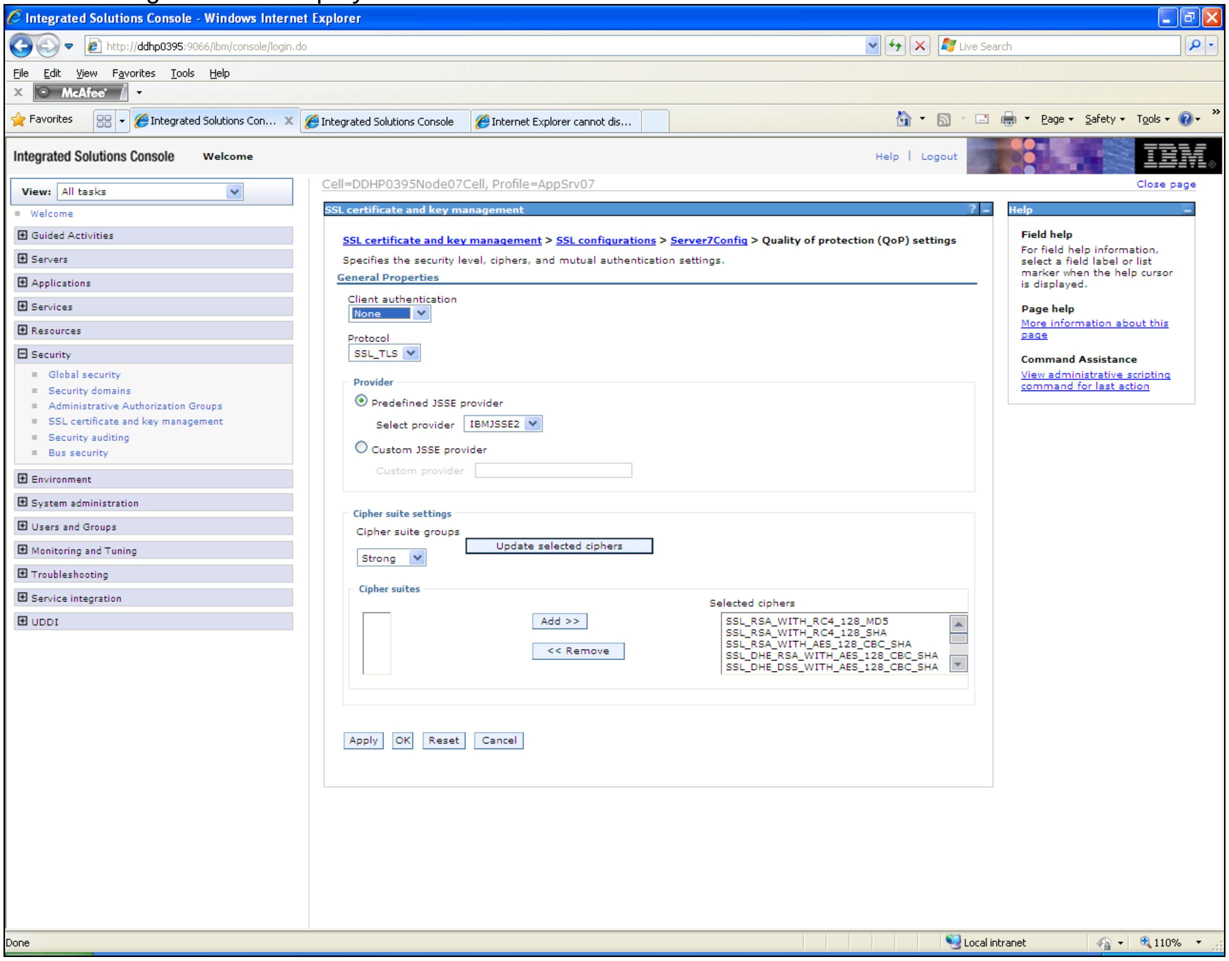
- Quality of protection (QoP) settings
- Trust and key managers
- Custom properties

Related Items

- Key stores and certificates

On the right side, click ‘Quality of protection (QoP) settings’.

The following screen is displayed.


Integrated Solutions Console - Windows Internet Explorer
http://ddhp0395:9066/ibm/console/login.do
Live Search
File Edit View Favorites Tools Help
McAfee
Favorites
Integrated Solutions Con...
Integrated Solutions Console
Internet Explorer cannot dis...
Page Safety Tools
Integrated Solutions Console
Welcome
Help | Logout
IBM
View: All tasks
Welcome
Guided Activities
Servers
Applications
Services
Resources
Security
Global security
Security domains
Administrative Authorization Groups
SSL certificate and key management
Security auditing
Bus security
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Close page
Help
Field help
For field help information, select a field label or list marker when the help cursor is displayed.
Page help
More information about this page
Command Assistance
View administrative scripting command for last action
Done
Local intranet
110%

Cell=DDHP0395Node07Cell, Profile=AppSrv07

SSL certificate and key management

SSL certificate and key management > SSL configurations > Server7Config > Quality of protection (QoP) settings

Specifies the security level, ciphers, and mutual authentication settings.

General Properties

Client authentication: None

Protocol: SSL_TLS

Provider

● Predefined JSSE provider

Select provider: IBMJSSE2

○ Custom JSSE provider

Custom provider

Cipher suite settings

Cipher suite groups: Strong

Update selected ciphers

Cipher suites

Add >>

<< Remove

Selected ciphers

SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_DSS_WITH_AES_128_CBC_SHA

Apply OK Reset Cancel

Under ‘Client authentication’ choose ‘Supported’ from the drop-down list.

Click ‘Apply’ and save the changes.

You need to repeat these steps for the second server. Once you have made the changes to both the servers, restart the servers. It is recommended to restart the servers after making the changes.

// New Changes

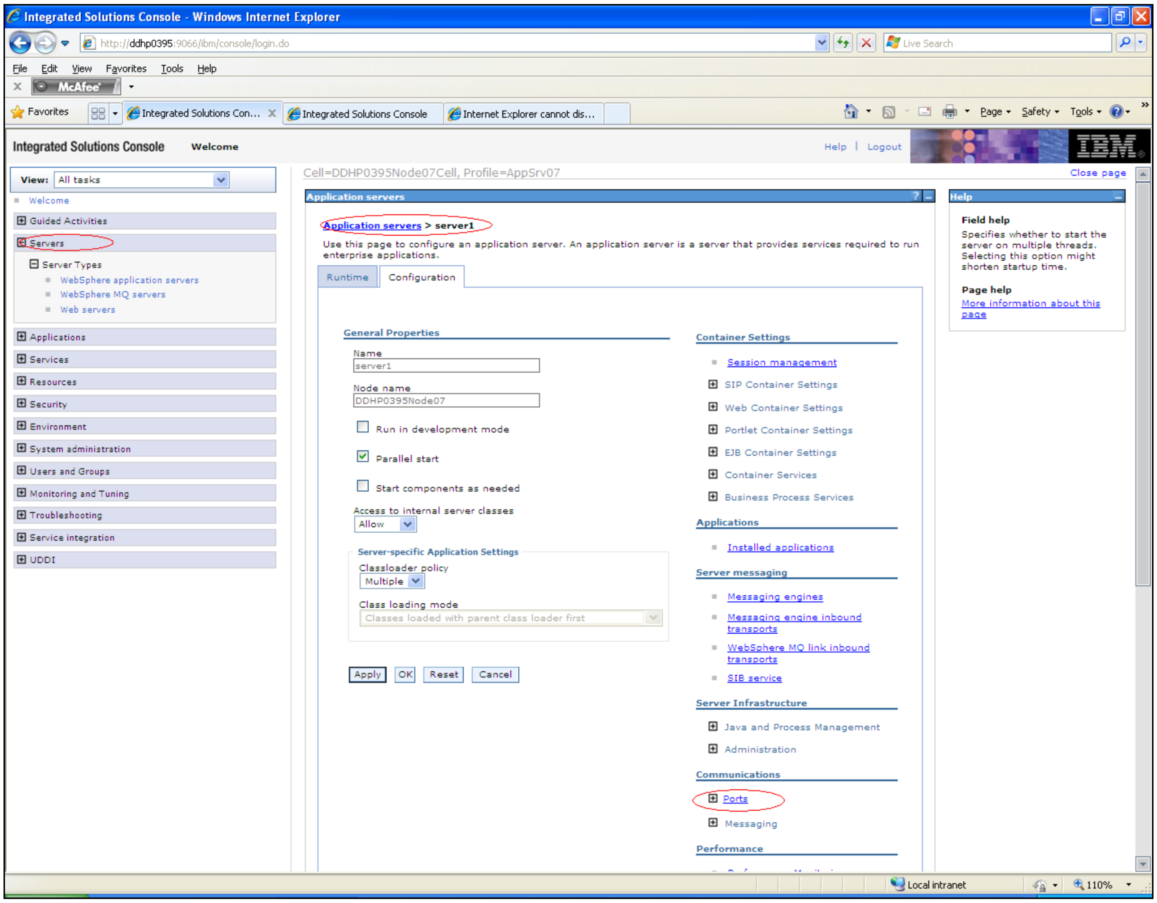
1.11 Importing or Adding Server Certificates using Batch

Alternatively, you can import or add the server certificates using *ikeyman.bat*. This batch is available at the following location:

<InstalledLocatio>\IBM\WebSphere\AppServer\bin

For security reasons, change the password for ‘defaultTruststore’ (trust.p12). The default password is ‘WebAS’.

SSL port information are available in the following screens.



Cell=DDHP0395Node07Cell, Profile=AppSrv07

Application servers

Application servers > server1

Use this page to configure an application server. An application server is a server that provides services required to run enterprise applications.

General Properties

Name: server1

Node name: DDHP0395Node07

☐ Run in development mode

☑ Parallel start

☐ Start components as needed

Access to internal server classes: Allow

Server-specific Application Settings

Classloader policy: Multiple

Class loading mode: Classes loaded with parent class loader first

Container Settings

- Session management
- SIP Container Settings
- Web Container Settings
- Portlet Container Settings
- EJB Container Settings
- Container Services
- Business Process Services

Applications

- Installed applications

Server messaging

- Messaging engines
- Messaging engine inbound transports
- WebSphere MQ link inbound transports
- SIB service

Server Infrastructure

- Java and Process Management
- Administration

Communications

- Ports
- Messaging

Performance

Help

Field help

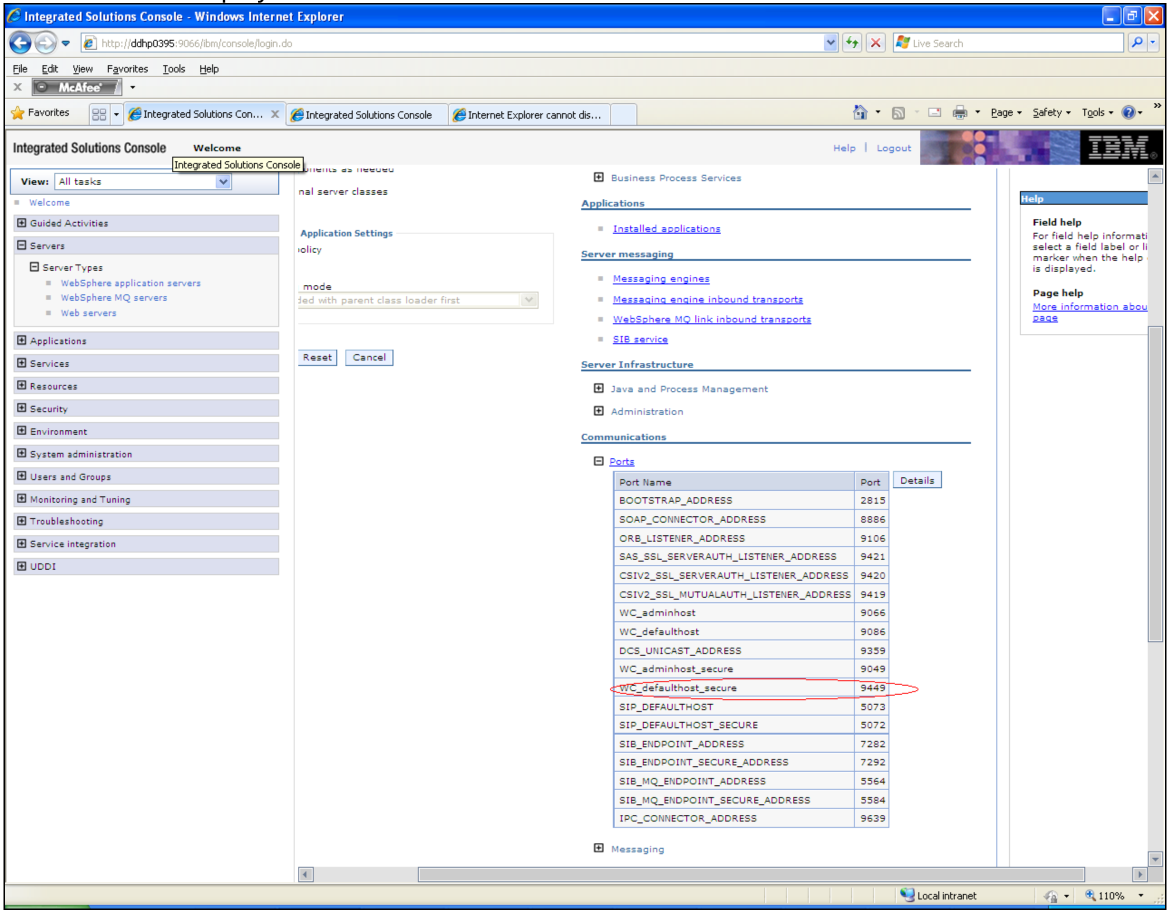
Specifies whether to start the server on multiple threads. Selecting this option might shorten startup time.

Page help

More information about this page

Click ‘Ports’.

The details are displayed as follows.



Port Name	Port
BOOTSTRAP_ADDRESS	2815
SOAP_CONNECTOR_ADDRESS	8886
ORB_LISTENER_ADDRESS	9106
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS	9421
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS	9420
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS	9419
WC_adminhost	9066
WC_defaulthost	9086
DCS_UNICAST_ADDRESS	9359
WC_adminhost_secure	9049
WC_defaulthost_secure	9449
SIP_DEFAULTHOST	5073
SIP_DEFAULTHOST_SECURE	5072
SIB_ENDPOINT_ADDRESS	7282
SIB_ENDPOINT_SECURE_ADDRESS	7292
SIB_MQ_ENDPOINT_ADDRESS	5564
SIB_MQ_ENDPOINT_SECURE_ADDRESS	5584
IPC_CONNECTOR_ADDRESS	9639

SSL Configuration on WebSphere
[November] [2016]
Version 11.83.03.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax:+91 22 6718 3001
www.oracle.com/financialservices/