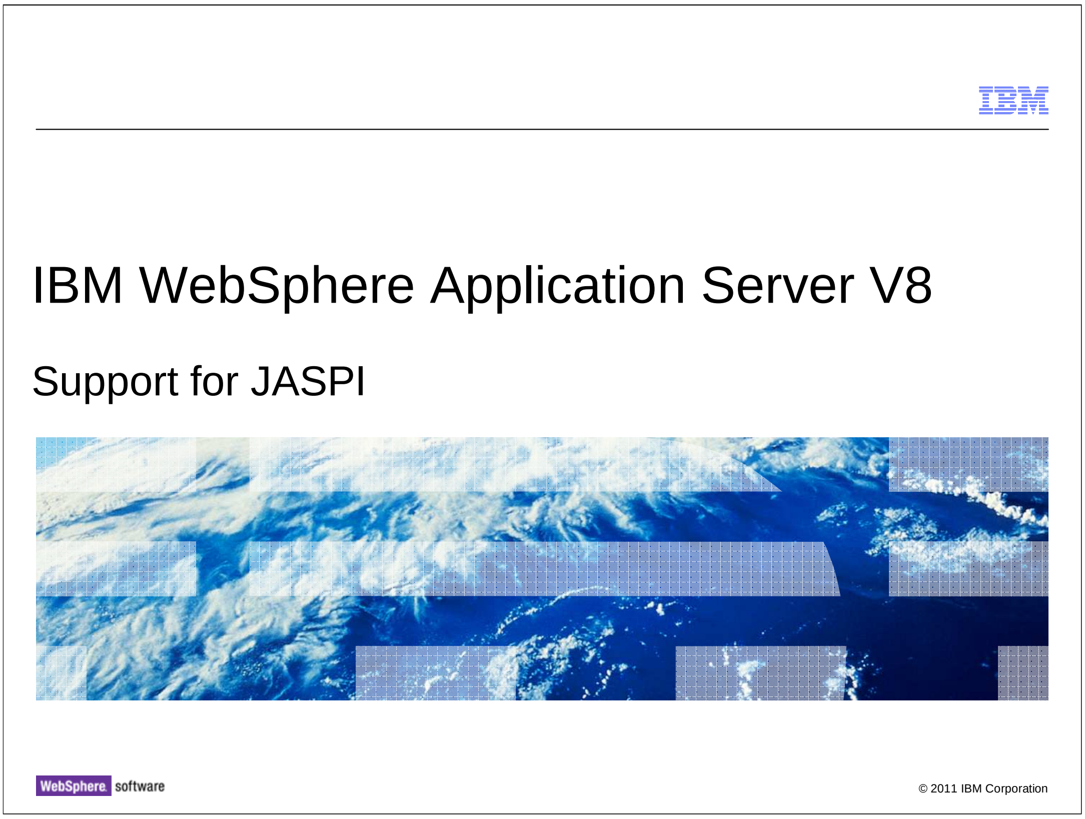


IBM WebSphere Application Server V8

Support for JASPI

WebSphere software

This presentation describes support in WebSphere Application Server version 8 for JSR 196 Java Authentication Service Provider Interface for Containers, abbreviated JASPI.

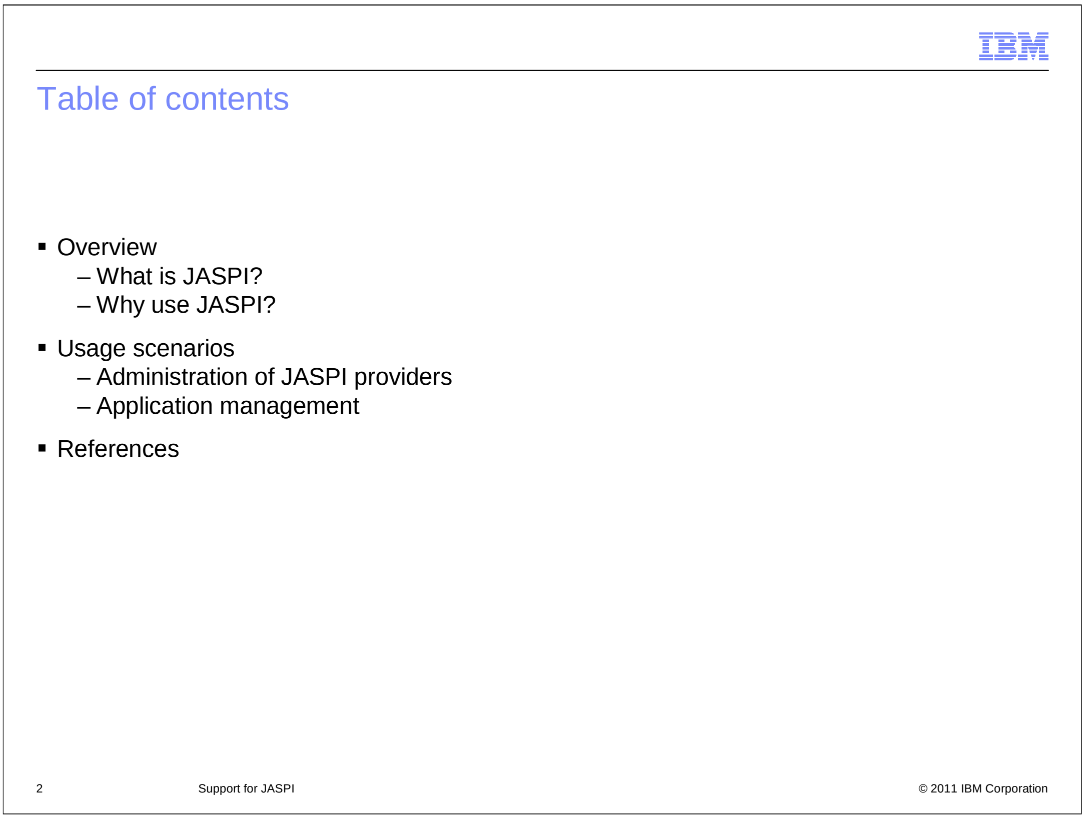


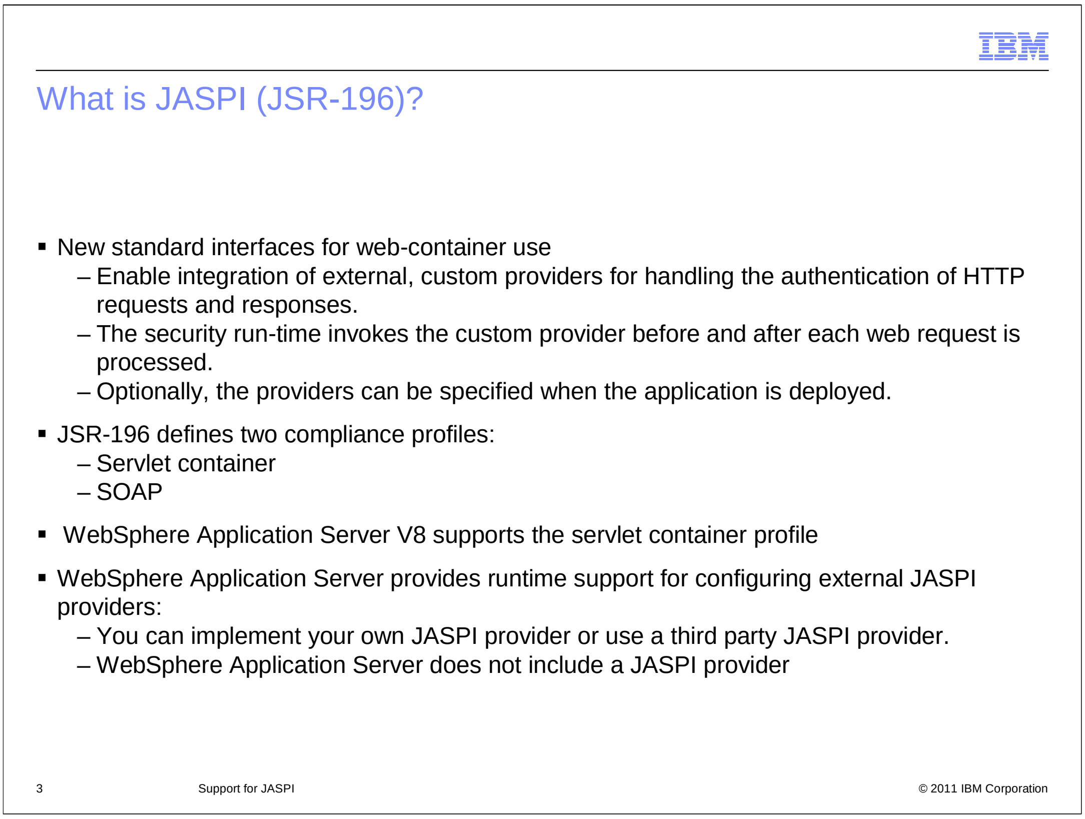
Table of contents

- Overview
  - What is JASPI?
  - Why use JASPI?
- Usage scenarios
  - Administration of JASPI providers
  - Application management
- References

2 Support for JASPI © 2011 IBM Corporation

This presentation covers what JASPI is and why you might want to use it, and common usage scenarios, such as administration of JASPI providers and application management with respect to JASPI.

A collection of resources is also provided at the end of the material.



What is JASPI (JSR-196)?

- New standard interfaces for web-container use
  - Enable integration of external, custom providers for handling the authentication of HTTP requests and responses.
  - The security run-time invokes the custom provider before and after each web request is processed.
  - Optionally, the providers can be specified when the application is deployed.
- JSR-196 defines two compliance profiles:
  - Servlet container
  - SOAP
- WebSphere Application Server V8 supports the servlet container profile
- WebSphere Application Server provides runtime support for configuring external JASPI providers:
  - You can implement your own JASPI provider or use a third party JASPI provider.
  - WebSphere Application Server does not include a JASPI provider

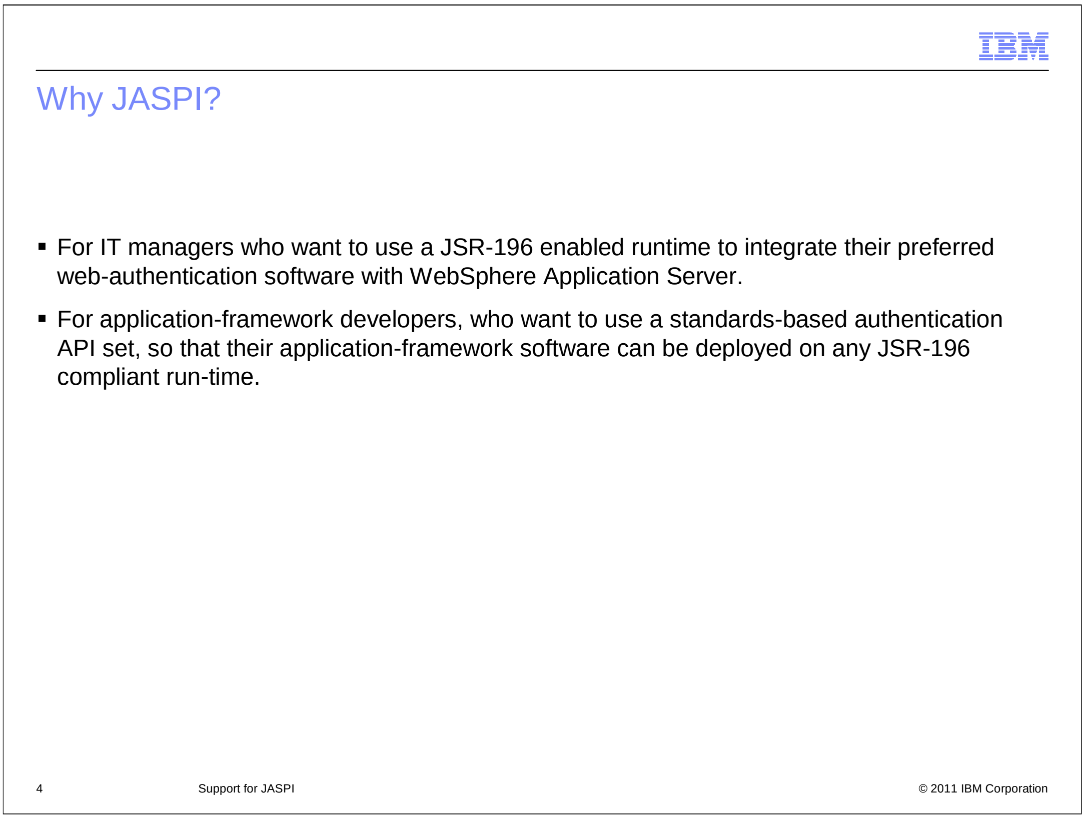
3 Support for JASPI © 2011 IBM Corporation

WebSphere Application Server version 8 supports the JSR 196: Java Authentication SPI for Containers specification, which enables third-party security providers to handle the Java Platform, Enterprise Edition (Java EE) authentication of HTTP request and response messages destined for web applications. The JASPI specification extends the pluggable authentication concepts of the Java Authentication and Authorization Service (JAAS) to the authentication of HTTP request and response messages. When application security is enabled, and a protected web resource is accessed, the web container and the security runtime collaborate to make an authentication decision for the caller.

The JASPI specification defines standard system programming interfaces that enable developers to write a pluggable custom authentication provider that can handle Java EE web authentication mechanisms. The WebSphere Application Server runtime uses these standard system programming interfaces to invoke the JASPI authentication provider. The WebSphere Application Server runtime only supports the Servlet Container Profile section in the JSR 196: Java Authentication Service Provider Interface for Containers specification. The SOAP profile is not supported.

If application security is enabled with JASPI authentication, when the web resource (such as a servlet or a JavaServer Pages (JSP) file) is accessed, the security runtime checks if the web resource is mapped to a JASPI provider defined in the security configuration. If so, the runtime invokes the JASPI authentication provider to perform authentication for the HTTP request and response messages.

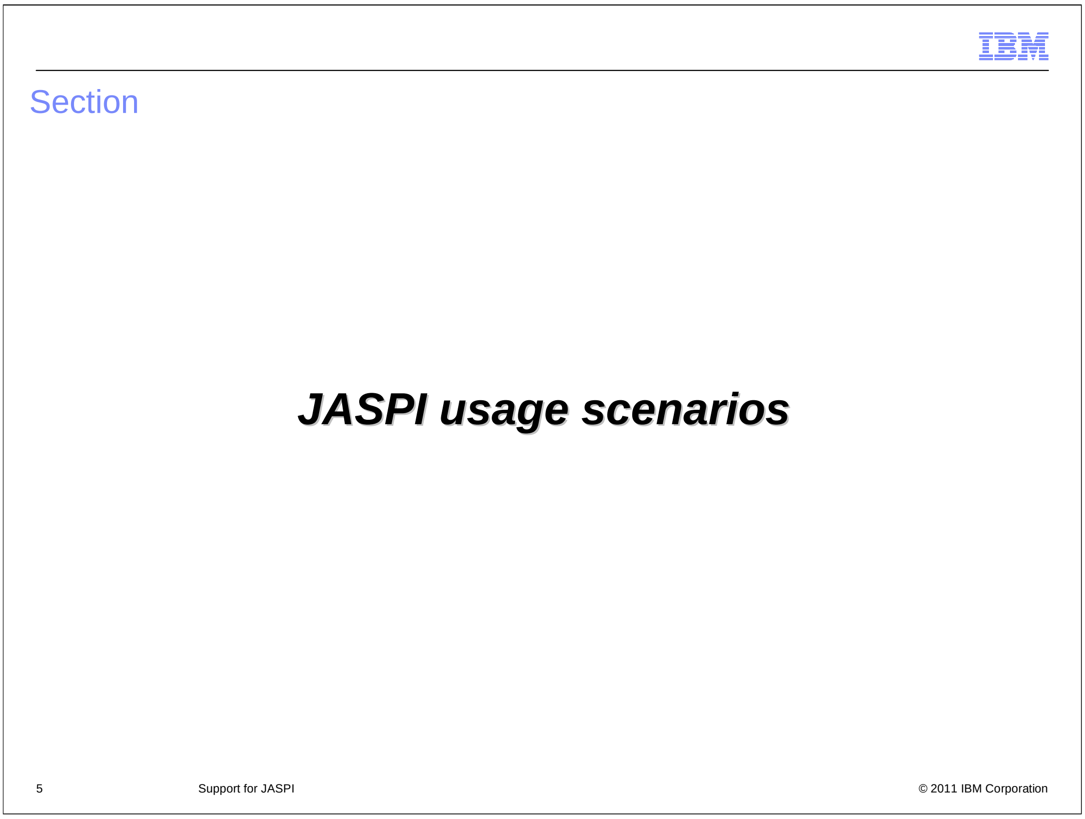
Note that WebSphere Application Server does not ship a default JASPI provider. One has to implement the provider as per the JSR196 specification and configure it in the WebSphere Application Server environment for the security runtime to use it.



Why JASPI?

- For IT managers who want to use a JSR-196 enabled runtime to integrate their preferred web-authentication software with WebSphere Application Server.
- For application-framework developers, who want to use a standards-based authentication API set, so that their application-framework software can be deployed on any JSR-196 compliant run-time.

Since JASPI enables third-party security providers to handle web authentication, JASPI is useful for IT managers who want to use a JSR-196 enabled WebSphere Application Server runtime to integrate their preferred JSR-196 compliant web-authentication software with WebSphere Application Server. It is also useful for application-framework developers who want to use a standards-based authentication API set, so that their application-framework software can be deployed on any JSR-196 compliant run-time.



Section

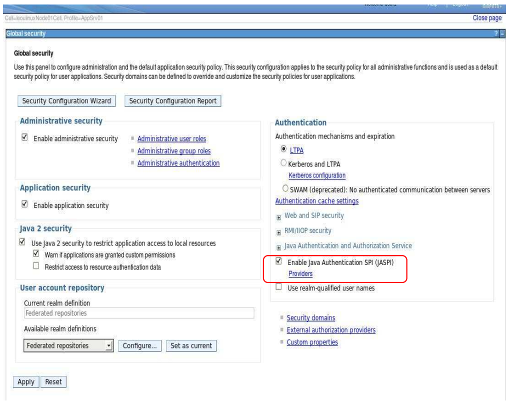
JASPI usage scenarios

5 Support for JASPI © 2011 IBM Corporation

This section covers JASPI configuration scenarios.

A) Scenario: Administering JASPI authentication providers (1 of 3)

- As an administrator, I want to manage the registry of JASPI authentication providers using the administrative console or using wsadmin commands. Additionally, I would like to be able to specify whether JASPI providers are enabled for selected security domains or for the cell.



Cell=leoulinuxNode01Cell, Profile=AppSrv01 Close page

Global security

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard | Security Configuration Report

Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

☑ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

User account repository

Current realm definition: Federated repositories

Available realm definitions: Federated repositories | Configure... | Set as current

Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

Kerberos configuration

○ SWAM (deprecated): No authenticated communication between servers

Authentication cache settings

⊞ Web and SIP security

⊞ RMI/IIOP security

⊞ Java Authentication and Authorization Service

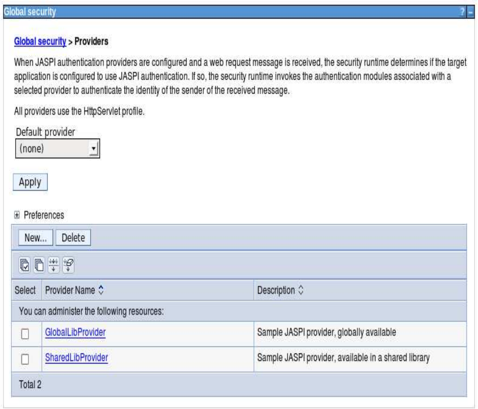
☑ Enable Java Authentication SPI (JASPI)

Providers

☐ Use realm-qualified user names

- Security domains
- External authorization providers
- Custom properties

Apply | Reset



Global security

Global security > Providers

When JASPI authentication providers are configured and a web request message is received, the security runtime determines if the target application is configured to use JASPI authentication. If so, the security runtime invokes the authentication modules associated with a selected provider to authenticate the identity of the sender of the received message.

All providers use the HttpServlet profile.

Default provider: (none)

Apply

⊞ Preferences

New... | Delete

Select	Provider Name	Description
You can administer the following resources:		
☐	GlobalLibProvider	Sample JASPI provider, globally available
☐	SharedLibProvider	Sample JASPI provider, available in a shared library
Total 2		

The JASPI feature can be enabled or disabled for both the cell and for security domains by the WebSphere Application Server Administrator.

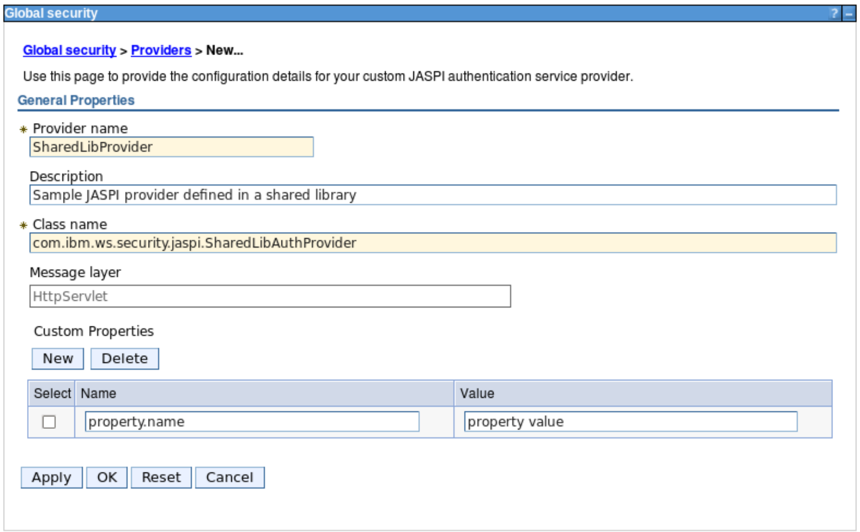
In order to use JASPI, JASPI must be enabled and at least one JASPI provider must be defined.

These actions can be done in the administrative console or with scripting.

An optional default provider can be selected from the list of defined providers. The default configuration for the default provider is none.

The default provider which will handle http servlet request and response message authentication if JASPI is enabled and no JASPI provider is mapped to the web module handling the requests.

A) Scenario: Administering JASPI authentication providers (2 of 3)



Global security > Providers > New...

Use this page to provide the configuration details for your custom JASPI authentication service provider.

General Properties

* Provider name
SharedLibProvider

Description
Sample JASPI provider defined in a shared library

* Class name
com.ibm.ws.security.jaspi.SharedLibAuthProvider

Message layer
HttpServlet

Custom Properties

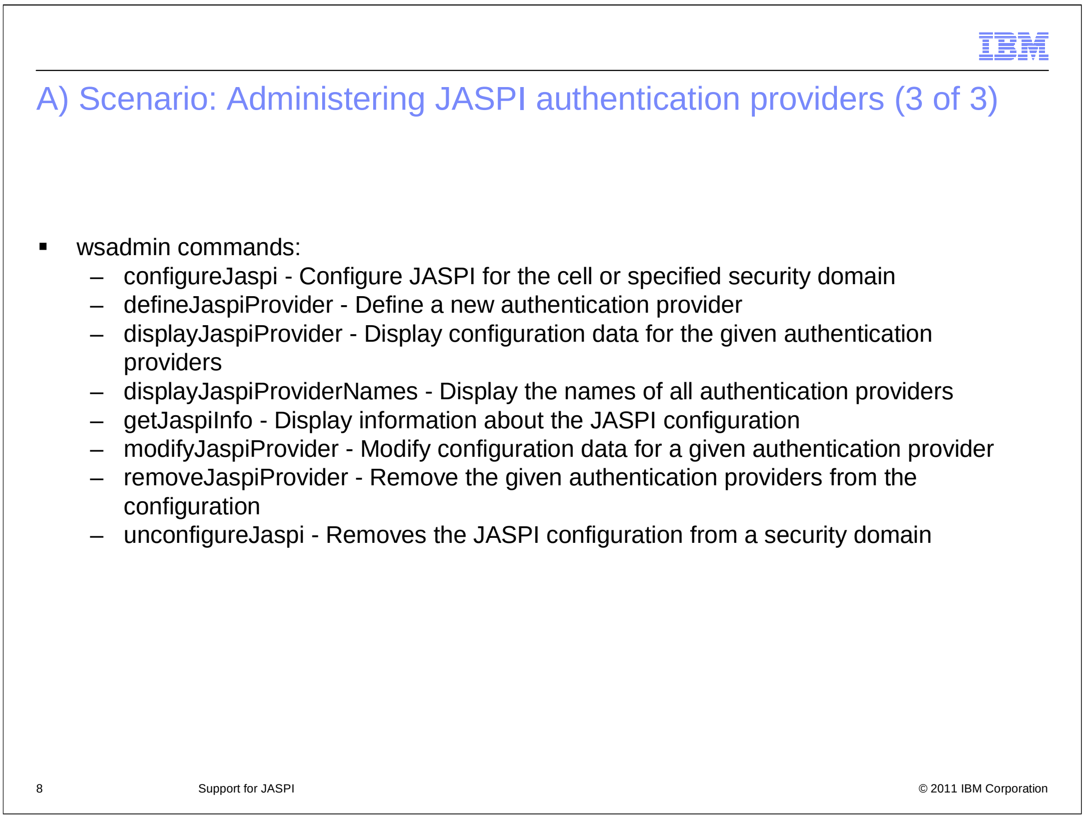
Select	Name	Value
□	property.name	property value

JASPI providers can be defined through the administrative console or scripting.

Each JASPI provider must define a name and implementation class, and might optionally define a description.

Optional custom properties are also supported, and are passed into the JASPI provider implementation at run-time.

Details on JASPI provider implementations are available through the Information Center.



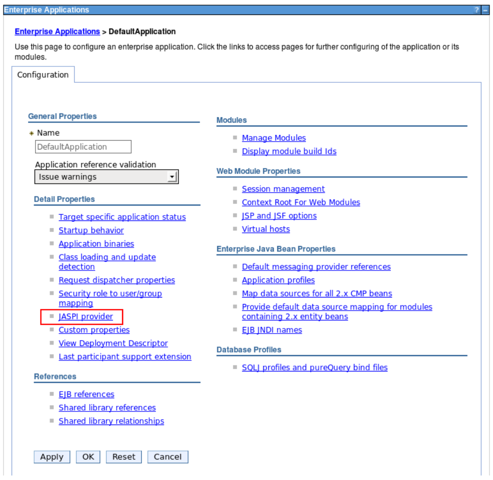
A) Scenario: Administering JASPI authentication providers (3 of 3)

- wsadmin commands:
  - configureJaspi - Configure JASPI for the cell or specified security domain
  - defineJaspiProvider - Define a new authentication provider
  - displayJaspiProvider - Display configuration data for the given authentication providers
  - displayJaspiProviderNames - Display the names of all authentication providers
  - getJaspiInfo - Display information about the JASPI configuration
  - modifyJaspiProvider - Modify configuration data for a given authentication provider
  - removeJaspiProvider - Remove the given authentication providers from the configuration
  - unconfigureJaspi - Removes the JASPI configuration from a security domain

This page lists the available wsadmin tasks for JASPI configuration. See the information center for complete details.

B) Scenario: Application management and JASPI (1 of 2)

- An application deployer wants:
  - to configure and enable JASPI authentication when applications are installed or edited
  - to enable or disable JASPI for selected web modules in the application



Enterprise Applications > DefaultApplication

Use this page to configure an enterprise application. Click the links to access pages for further configuring of the application or its modules.

Configuration

General Properties

* Name: DefaultApplication

Application reference validation: Issue warnings

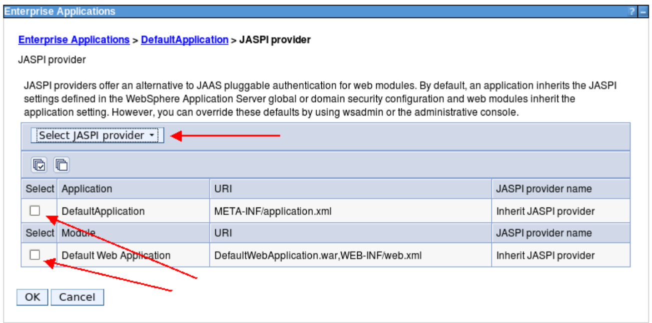
Enterprise Applications
Detail Properties
Target specific application status
Startup behavior
Application binaries
Class loading and update detection
Request dispatcher properties
Security role to user/group mapping
JASPI provider
Custom properties
View Deployment Descriptor
Last participant support extension
References
EJB references
Shared library references
Shared library relationships
Apply
OK
Reset
Cancel
Modules
Manage Modules
Display module build Ids
Web Module Properties
Session management
Context Root For Web Modules
JSP and JSF options
Virtual hosts
Enterprise Java Bean Properties
Default messaging provider references
Application profiles
Map data sources for all 2.x CMP beans
Provide default data source mapping for modules containing 2.x entity beans
EJB JNDI names
Database Profiles
SQLJ profiles and pureQuery bind files

JASPI providers can be mapped to applications and the web modules within an application.

This mapping can be established during application deployment, or after the application has been installed.

You can also disable JASPI for specific applications or web modules within the application.

B) Scenario: Application management and JASPI (2 of 2)



Enterprise Applications

Enterprise Applications > DefaultApplication > JASPI provider

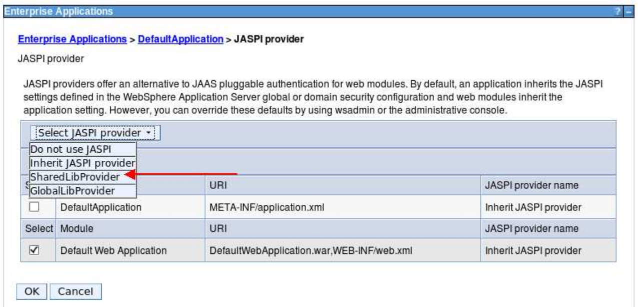
JASPI provider

JASPI providers offer an alternative to JAAS pluggable authentication for web modules. By default, an application inherits the JASPI settings defined in the WebSphere Application Server global or domain security configuration and web modules inherit the application setting. However, you can override these defaults by using wsadmin or the administrative console.

Select JASPI provider ▾

Select	Application	URI	JASPI provider name
□	DefaultApplication	META-INF/application.xml	Inherit JASPI provider

Select	Module	URI	JASPI provider name
□	Default Web Application	DefaultWebApplication.war,WEB-INF/web.xml	Inherit JASPI provider



Enterprise Applications

Enterprise Applications > DefaultApplication > JASPI provider

JASPI provider

JASPI providers offer an alternative to JAAS pluggable authentication for web modules. By default, an application inherits the JASPI settings defined in the WebSphere Application Server global or domain security configuration and web modules inherit the application setting. However, you can override these defaults by using wsadmin or the administrative console.

Select JASPI provider ▾

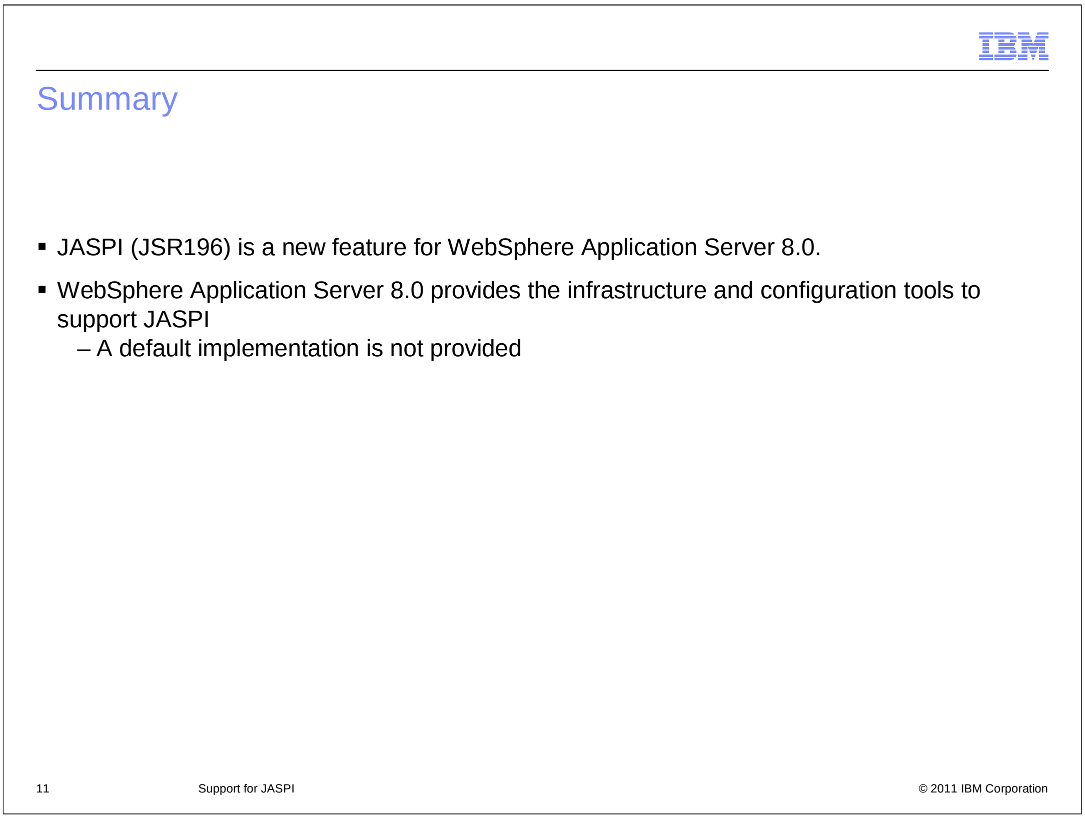
Select	Application	URI	JASPI provider name
□	DefaultApplication	META-INF/application.xml	Inherit JASPI provider

Select	Module	URI	JASPI provider name
☑	Default Web Application	DefaultWebApplication.war,WEB-INF/web.xml	Inherit JASPI provider

By default, installed applications will inherit their JASPI provider from the cell or security domain level configuration.

Applications inherit their JASPI provider from the default JASPI provider defined in the global or domain security configuration, and web modules inherit the application’s JASPI provider.

The JASPI provider mapping configuration can be changed for either the application or web module by selecting either: Do not use JASPI, Inherit JASPI provider, or a JASPI provider defined in the security configuration.

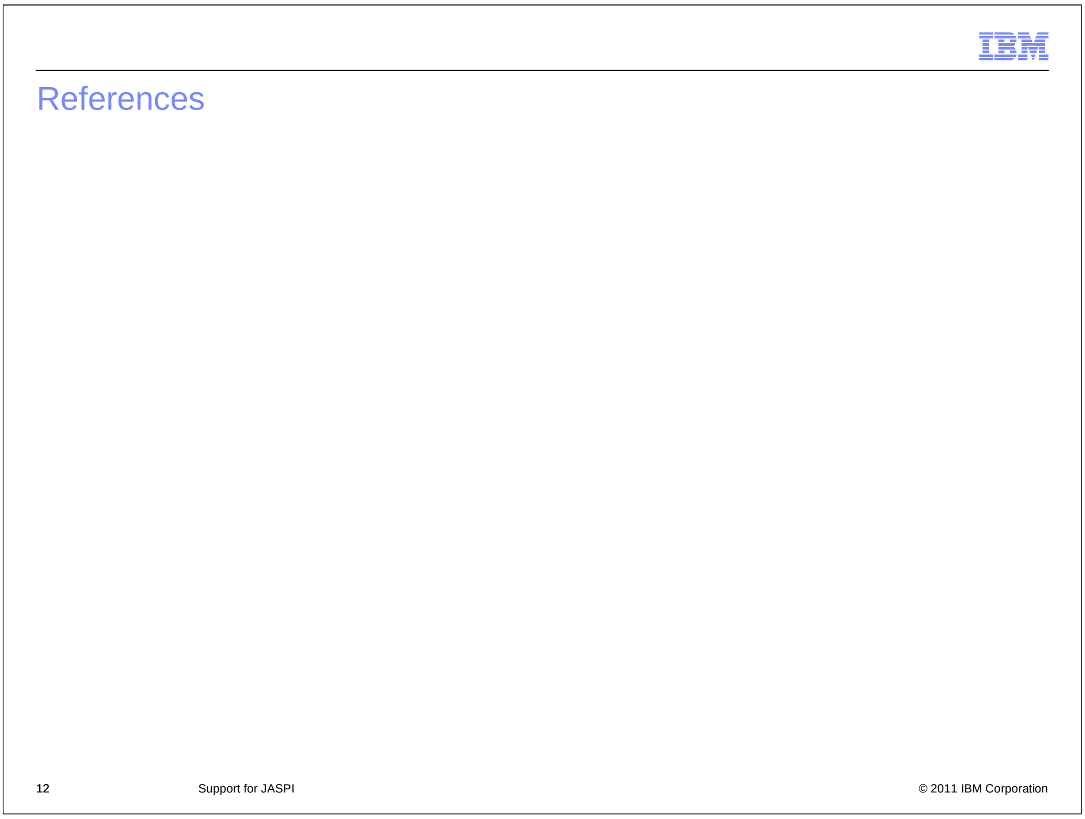


Summary

- JASPI (JSR196) is a new feature for WebSphere Application Server 8.0.
- WebSphere Application Server 8.0 provides the infrastructure and configuration tools to support JASPI
  - A default implementation is not provided

11 Support for JASPI © 2011 IBM Corporation

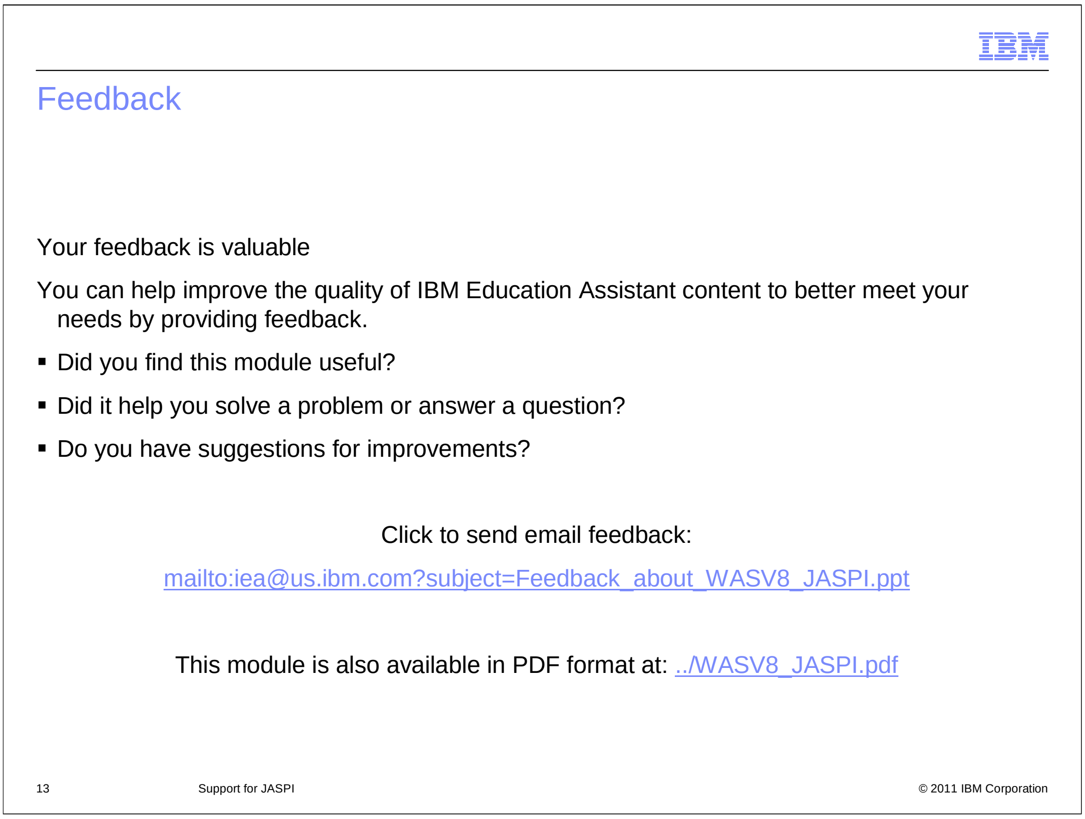
In summary, WebSphere Application Server version 8 supports the JSR 196: Java Authentication SPI for Containers specification, which enables third-party security providers to handle the Java Platform, Enterprise Edition (Java EE) authentication of HTTP request and response messages destined for web applications. This new feature provides the infrastructure and the configuration tools to use JASPI specification compliant providers. Note that WebSphere Application Server version 8 does not include a JASPI provider.



References

12 Support for JASPI

The following are a list of useful references related to the JASPI feature.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

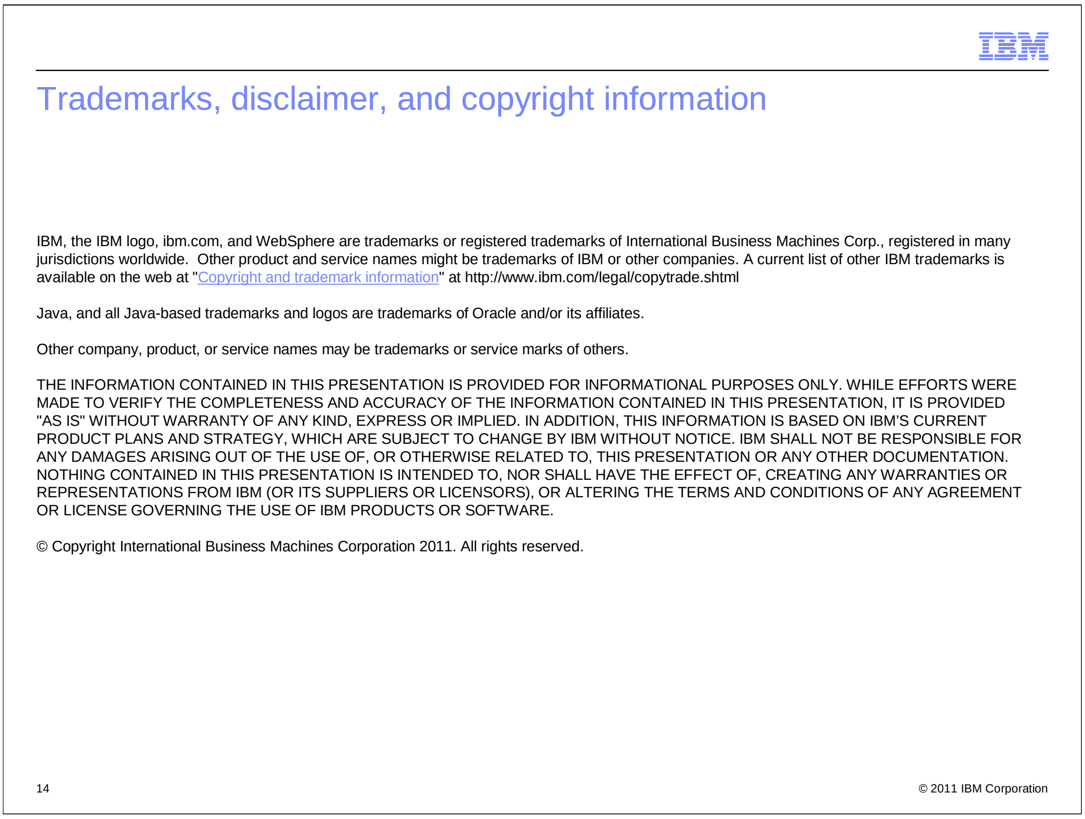
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WASV8_JASPI.ppt

This module is also available in PDF format at: ../WASV8_JASPI.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, 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" at http://www.ibm.com/legal/copytrade.shtml

Java, and all Java-based trademarks and logos are trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.

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.