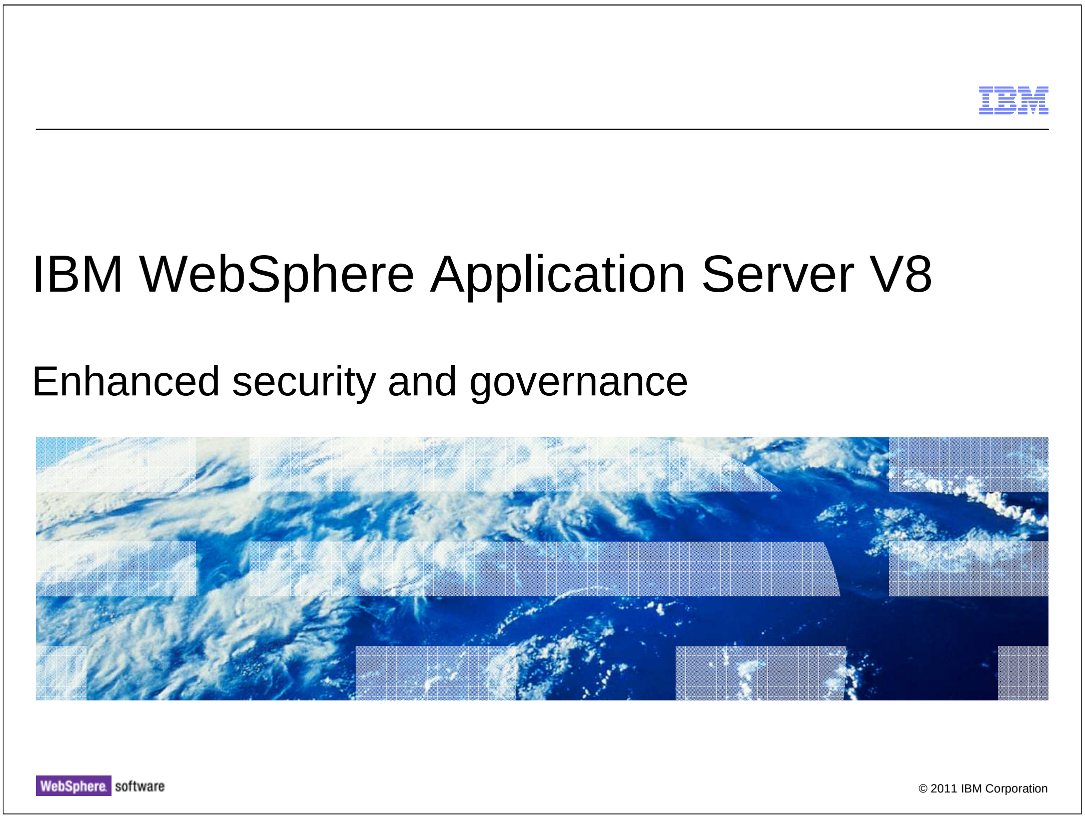


IBM WebSphere Application Server V8

Enhanced security and governance

This presentation describes security enhancements in IBM WebSphere Application Server V8.

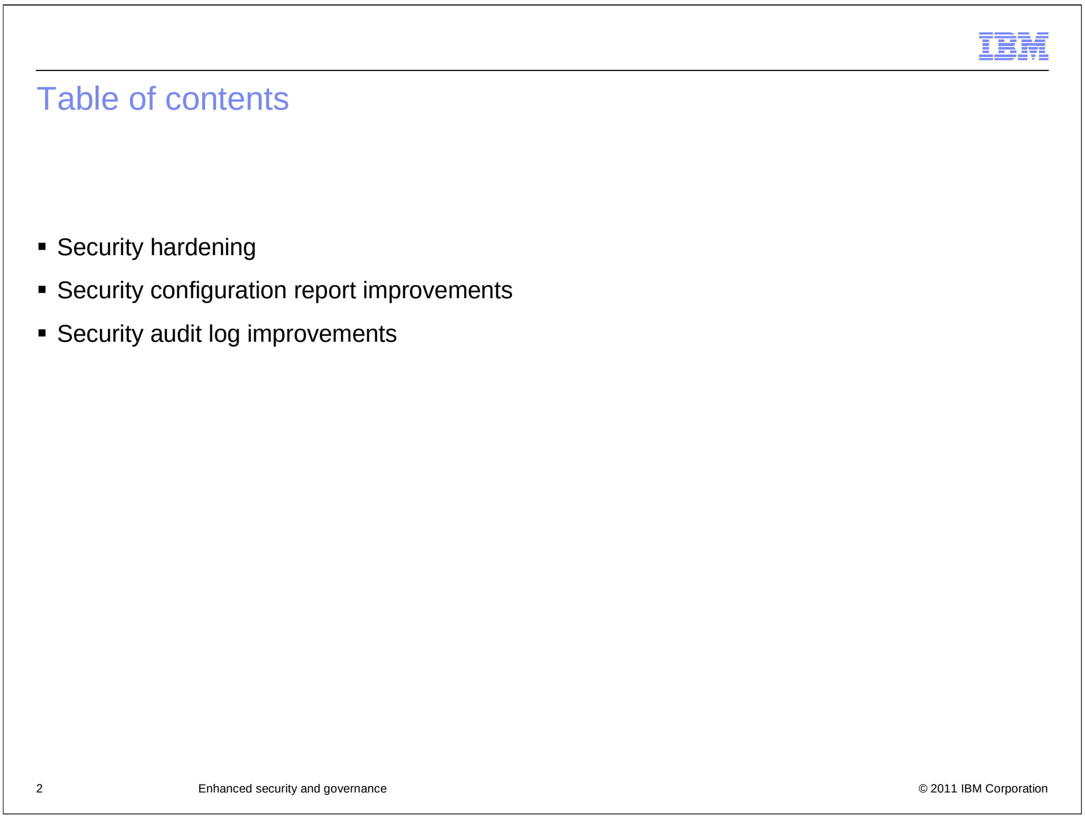


Table of contents

- Security hardening
- Security configuration report improvements
- Security audit log improvements

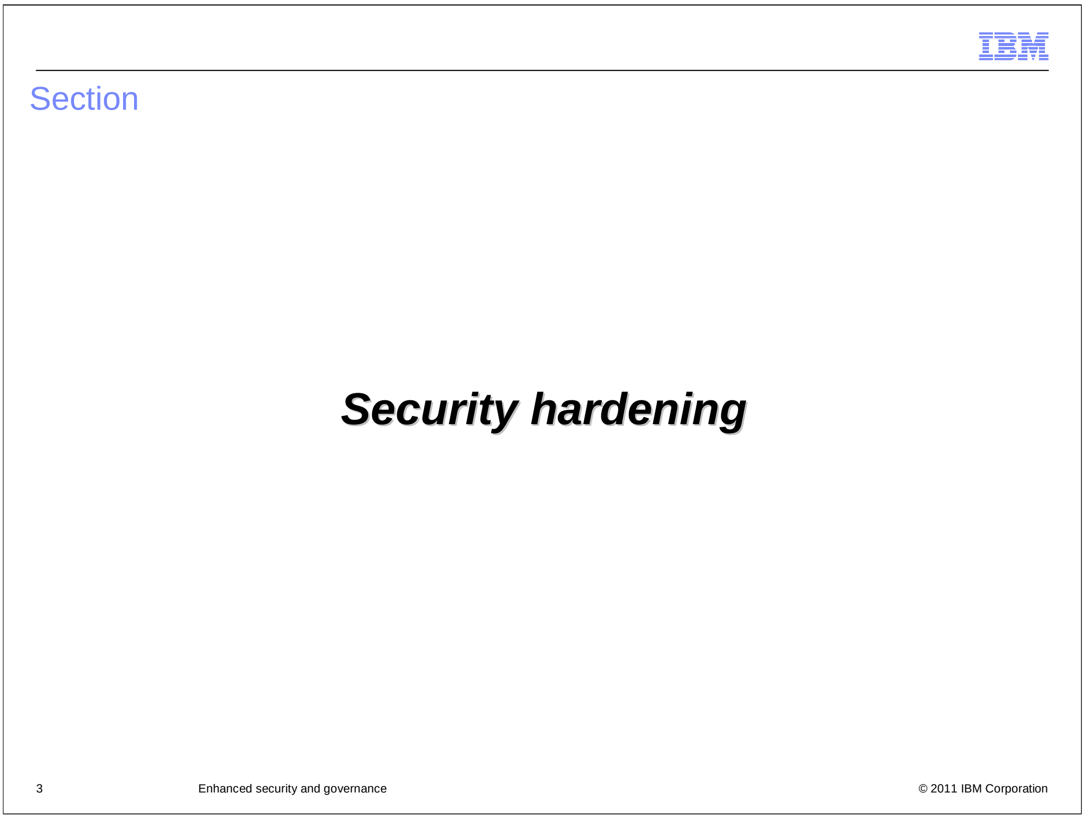
2 Enhanced security and governance

This presentation covers three new features in WebSphere Application Server that enhance the security of your WebSphere environment.

The first topic covers improved default settings that harden your application server environment without the need to modify your security configuration.

The next topic describes new information provided in the security configuration report.

Finally, you will see improvements to security audit log management behaviors.

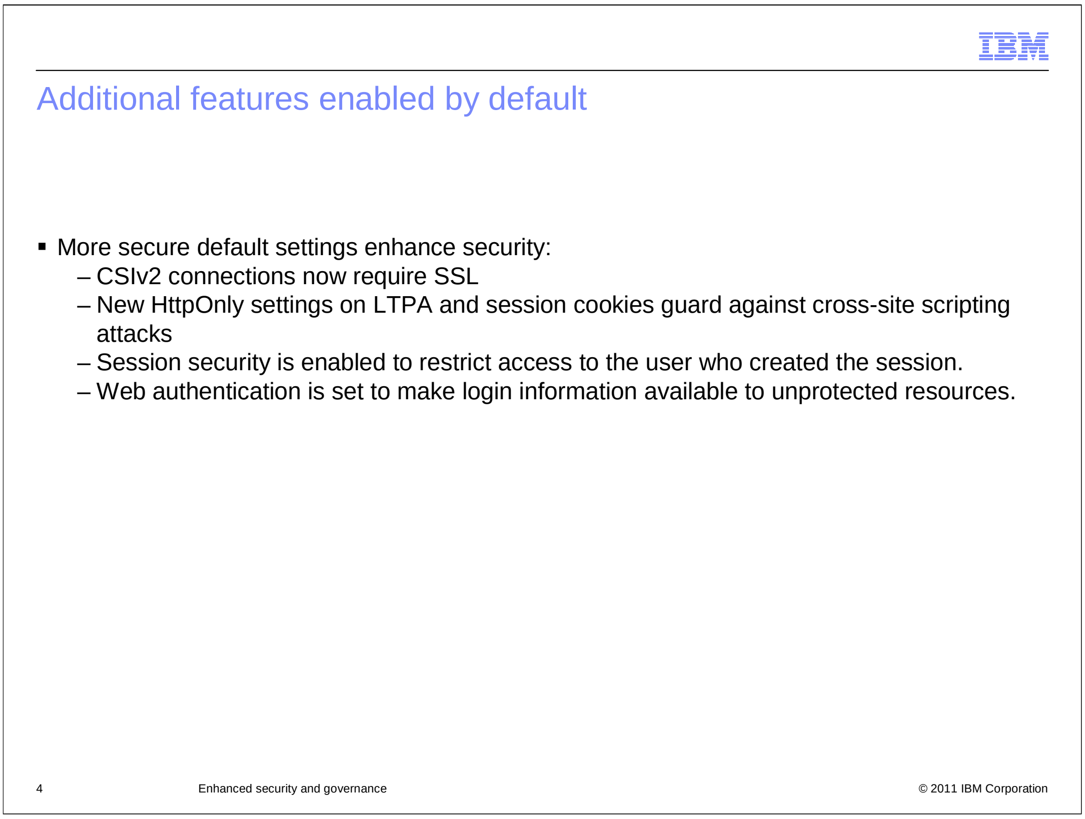


Section

Security hardening

3 Enhanced security and governance © 2011 IBM Corporation

This section covers security hardening.



Additional features enabled by default

- More secure default settings enhance security:
  - CSIv2 connections now require SSL
  - New HttpOnly settings on LTPA and session cookies guard against cross-site scripting attacks
  - Session security is enabled to restrict access to the user who created the session.
  - Web authentication is set to make login information available to unprotected resources.

4 Enhanced security and governance © 2011 IBM Corporation

To provide stronger security, new installations of WebSphere Application Server Version 8.0 are configured with stronger default settings.

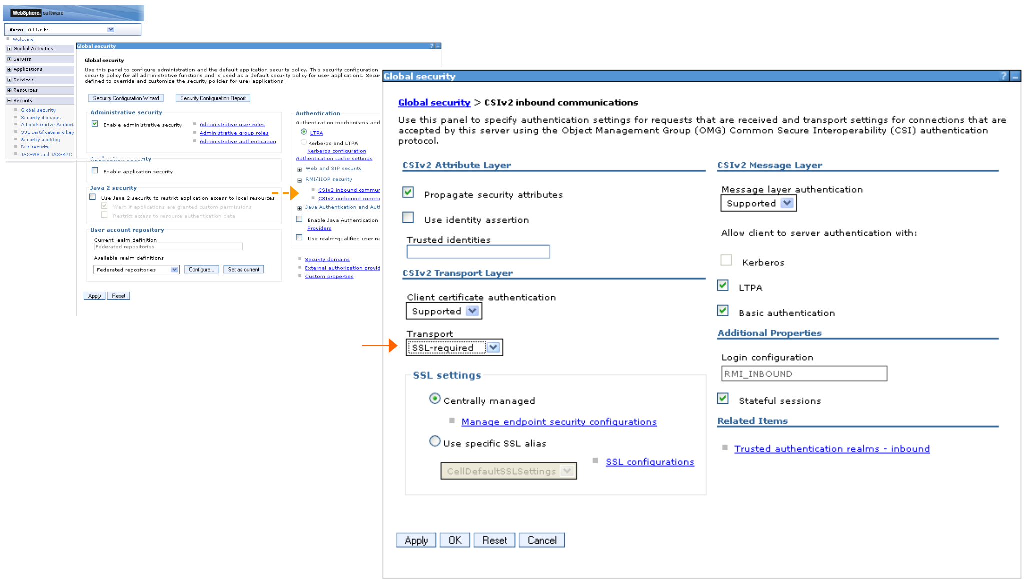
CSIv2 (or Common Security Interoperability Version 2) inbound and outbound connections to WebSphere Application Server are set to require SSL to provide stronger transport level security.

Web security is made more secure by new HttpOnly settings on LTPA cookies and session cookies. The HttpOnly attribute on these cookies will mitigate the possibility of cross-site scripting vulnerability attacks, the HttpOnly attribute is enabled on the LTPA cookie and the WASReqURL cookies by default.

Session security is enabled by default. This ensures that when a session is created for a user, only that user can access the session.

Finally, by default, web authentication is configured so that authentication information is available to unprotected resources. This enables those resources to access information in a secure session without failing and can also be used to determine the login under which unprotected resources were accessed.

CSIV2 SSL required default



WebSphere. software

Views: All tasks

- Welcome
- ⊞ Guided Activities
- ⊞ Servers
- ⊞ Applications
- ⊞ Services
- ⊞ Resources
- ⊟ Security
  - Global security
  - Security domains
  - Administrative Authori
  - SSL certificate and key
  - Security auditing
  - Bus security
  - JAX-WS and JAX-RPC

Global security

Global security

Use this panel to configure administration and the default application security policy. This security configuration security policy for all administrative functions and is used as a default security policy for user applications. Secur 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]

[Apply] [Reset]

Authentication

Authentication mechanisms and

● LTPA

○ Kerberos and LTPA

Kerberos configuration

Authentication cache settings

⊞ Web and SIP security

⊟ RMI/IIOP security

- CSIv2 inbound commur
- CSIv2 outbound comm

⊞ Java Authentication and Aut

☐ Enable Java Authentication Providers

☐ Use realm-qualified user n

- Security domains
- External authorization provid
- Custom properties

Global security

Global security > **CSIv2 inbound communications**

Use this panel to specify authentication settings for requests that are received and transport settings for connections that are accepted by this server using the Object Management Group (OMG) Common Secure Interoperability (CSI) authentication protocol.

CSIv2 Attribute Layer

☑ Propagate security attributes

☐ Use identity assertion

Trusted identities

CSIv2 Transport Layer

Client certificate authentication: Supported

Transport: SSL-required

SSL settings

● Centrally managed

- Manage endpoint security configurations

○ Use specific SSL alias

CellDefaultSSLSettings

- SSL configurations

CSIv2 Message Layer

Message layer authentication: Supported

Allow client to server authentication with:

☐ Kerberos

☑ LTPA

☑ Basic authentication

Additional Properties

Login configuration: RMI_INBOUND

☑ Stateful sessions

Related Items

- Trusted authentication realms - inbound

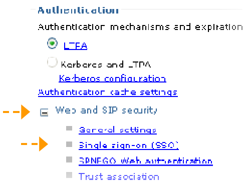
[Apply] [OK] [Reset] [Cancel]

To locate the CSIv2 transport setting in the left navigation area of the console, open “Security” and select “Global security”.

On the “Global security page, Under Authentication, expand RMI/IIOP and select either inbound or outbound CSIv2 communications.

The transport security setting is under CSIv2 Transport Layer.

HttpOnly configuration for web security single-sign on



Authentication

Authentication mechanisms and expiration

● LTPA

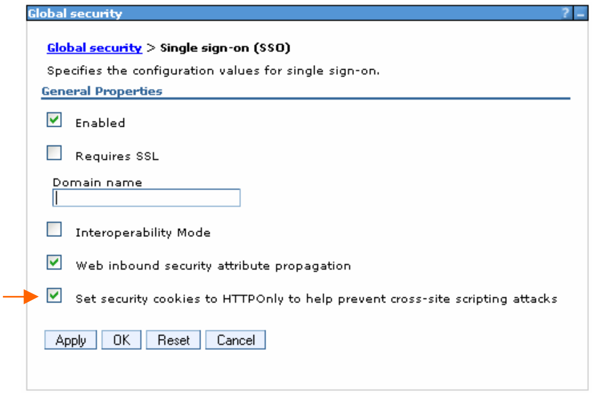
○ Kerberos and LTPA

Kerberos configuration

Authentication cache settings

⊟ Web and SIP security

- General settings
- Single sign-on (SSO)
- SPNEGO Web authentication
- Trust association



Global security > Single sign-on (SSO)

Specifies the configuration values for single sign-on.

General Properties

☑ Enabled

□ Requires SSL

Domain name

□ Interoperability Mode

☑ Web inbound security attribute propagation

☑ Set security cookies to HTTPOnly to help prevent cross-site scripting attacks

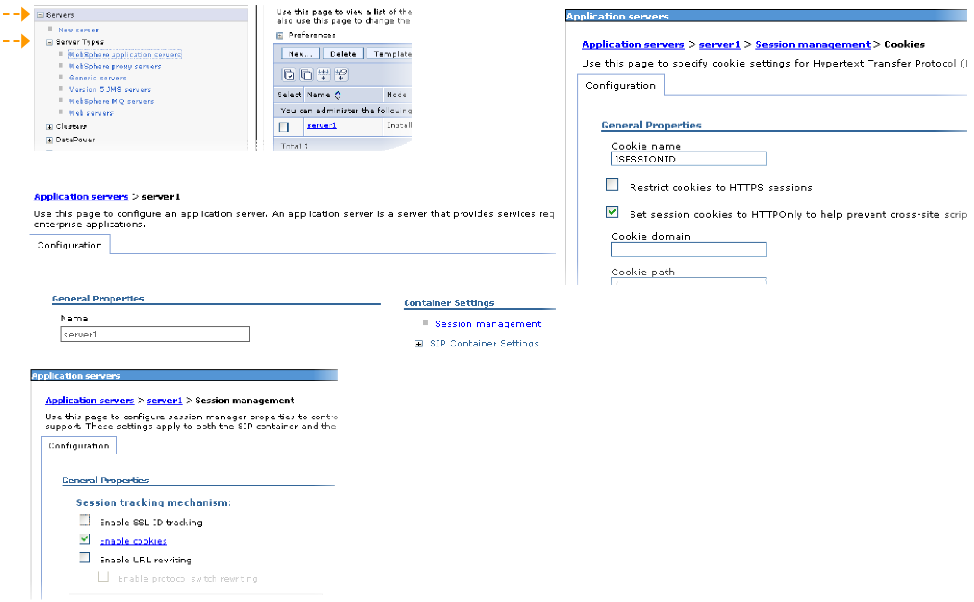
The new HttpOnly attribute controls whether scripts can be included in cookies.

When HttpOnly settings are enabled, cross-site scripting attacks are mitigated by permitting only HTTP elements in cookies.

To locate the HttpOnly setting for LTPA cookies, first go to the “Global security” panel, expand the “Web and SIP security” section and click the “Single sign-on (SSO)” link.

The HttpOnly option is the last setting on the panel.

HttpOnly configuration for session security



Use this page to view a list of the
also use this page to change the

You can administer the following

☐ server1

Application servers > server1

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

General Properties

Name
server1

Application servers > server1 > Session management

Use this page to configure session manager properties to contro
support. These settings apply to both the SIP container and the

General Properties

Session tracking mechanism:

☐ Enable SSL ID tracking

☑ Enable cookies

☐ Enable URL rewriting

☐ Enable protocol switch rewriting

Application servers > server1 > Session management > Cookies

Use this page to specify cookie settings for Hypertext Transfer Protocol (

General Properties

Cookie name
JSESSIONID

☐ Restrict cookies to HTTPS sessions

☑ Set session cookies to HTTPOnly to help prevent cross-site scrip

Cookie domain

Cookie path
/

Session cookie attributes are separately configurable for each application server. Therefore the HttpOnly setting is provided in each application server’s configuration.

To locate the HttpOnly setting for session cookies, expand the “Servers section”, then “Server types” and click the “WebSphere application servers” link.

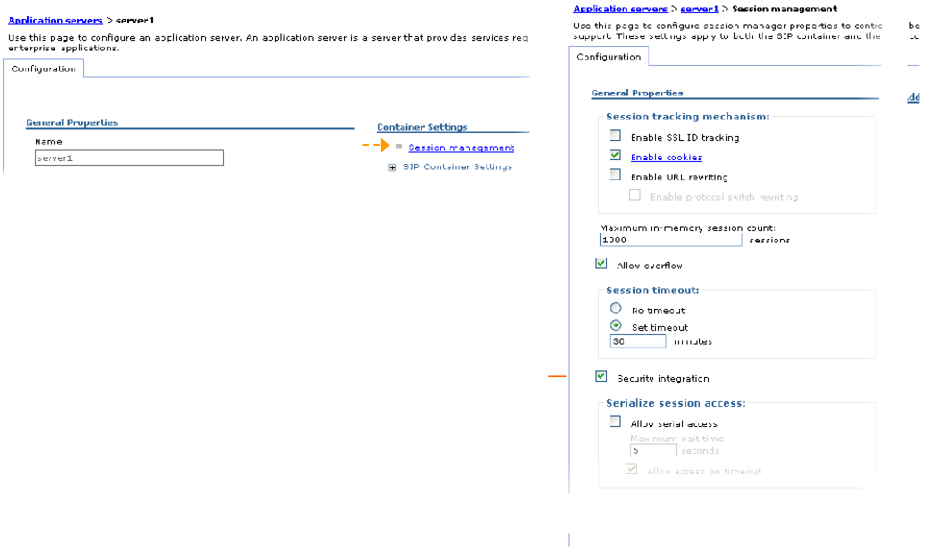
On the “Application servers” panel click a server link.

On the server properties panel, click the “Session management” link.

On the “Session management” panel click the “Enable cookies” link.

The HttpOnly attribute is the third setting on the panel.

Session management security integration



Application servers > server1

Use this page to configure an application server. An application server is a server that prov des services req enterprise applications.

Configuration

General Properties

Name
server1

Container Settings

- Session management
- ⊞ SIP Container Settings

Application servers > server1 > Session management

Use this page to configure session manager properties to contro be support. These settings apply to both the SIP container and the

Configuration

General Properties

Session tracking mechanism:

□ Enable SSL ID tracking
☑ Enable cookies
□ Enable URL rewriting
□ Enable protocol switch rewriting

Maximum in-memory session count:
1000 sessions

☑ Allow overflow

Session timeout:

○ No timeout
● Set timeout
30 minutes

☑ Security integration

Serialize session access:

□ Allow serial access
Maximum wait time
5 seconds
☑ Allow access on timeout

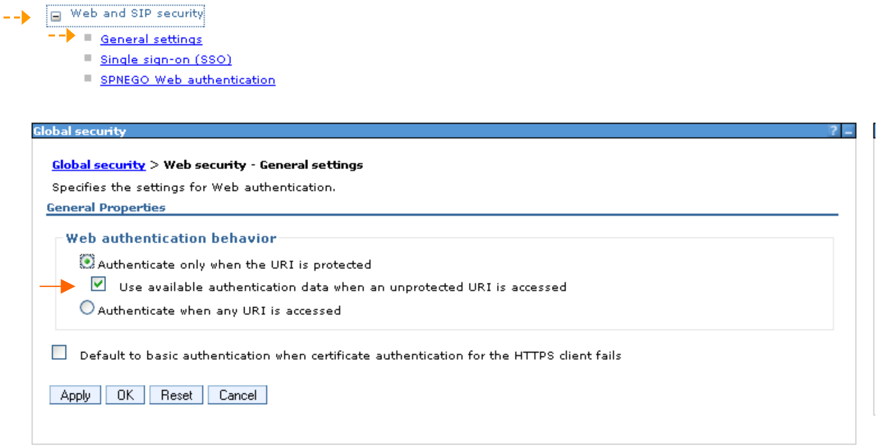
Session security is now enabled by default so that only the user for whom a session was created can access the session.

This setting is provided for each application server.

To locate the setting, select a server and click the “Session management” link.

The setting labeled “security integration” enables session security.

Web authentication behavior



⊟ Web and SIP security
- General settings
- Single sign-on (SSO)
- SPNEGO Web authentication

Global security

Global security > Web security - General settings

Specifies the settings for Web authentication.

General Properties

Web authentication behavior

● Authenticate only when the URI is protected

☑ Use available authentication data when an unprotected URI is accessed

○ Authenticate when any URI is accessed

□ Default to basic authentication when certificate authentication for the HTTPS client fails

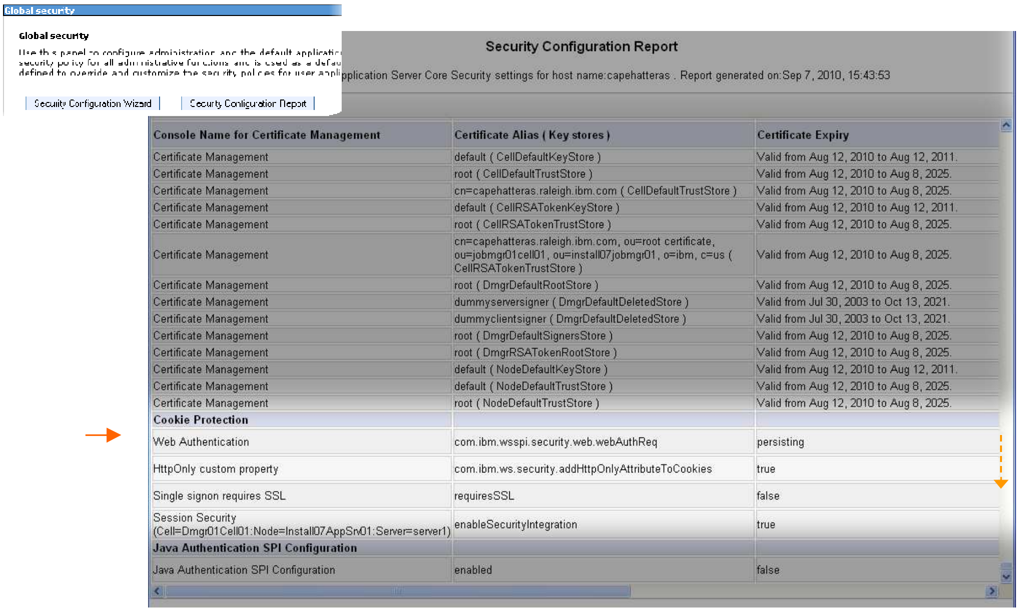
By default, the web authentication behavior is configured to make authentication data available to unprotected web resources.

This enables those resources to access information in a secure session without failing and can also be used to determine the login under which those unprotected resources were accessed.

To locate this setting, on the “Global security” panel, open the web and SIP security area and click “General settings”

The option labeled, “Use available authentication data when an unprotected URI is accessed” controls this behavior.

Updated security configuration report



Global security
Global security
Use th s panel to configure administration and the default applicati
security po icy for all administrative functions and is used as a defau
defined to override and customize the security pol cies for user appli
Security Configuration Wizard
Security Configuration Report

Security Configuration Report

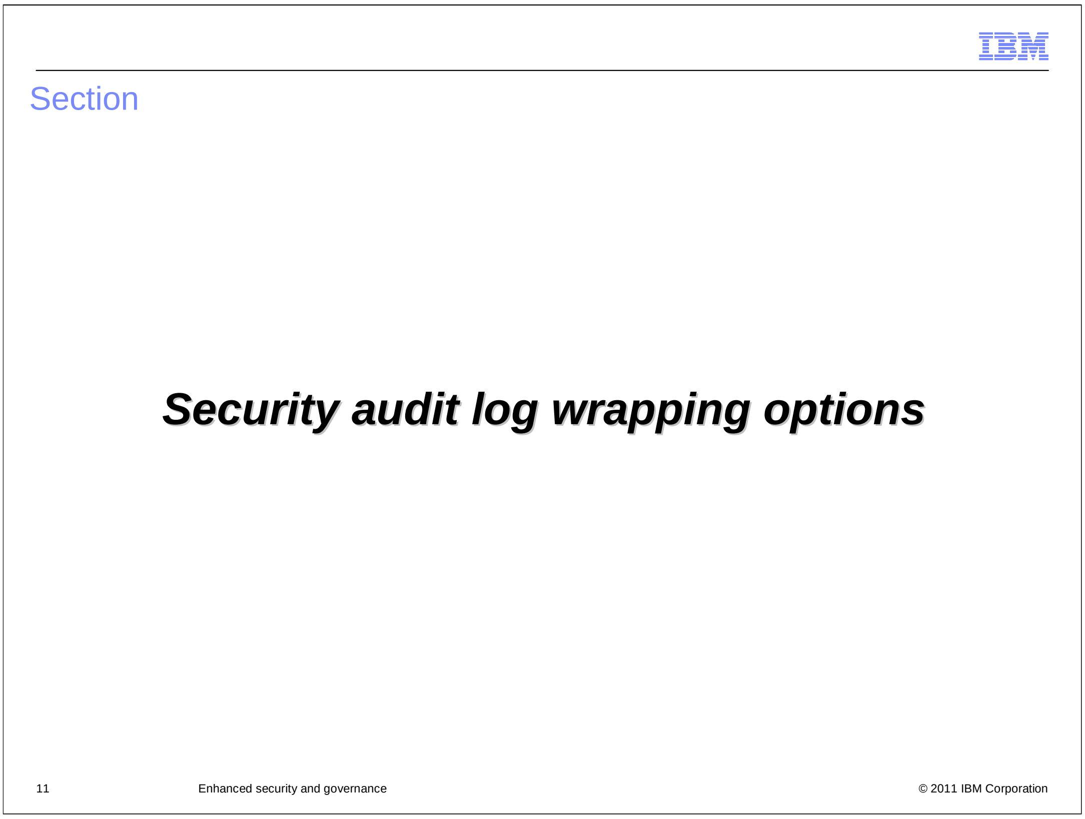
pplication Server Core Security settings for host name:capehatteras . Report generated on:Sep 7, 2010, 15:43:53

Console Name for Certificate Management	Certificate Alias (Key stores)	Certificate Expiry
Certificate Management	default (CellDefaultKeyStore)	Valid from Aug 12, 2010 to Aug 12, 2011.
Certificate Management	root (CellDefaultTrustStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Certificate Management	cn=capehatteras.raleigh.ibm.com (CellDefaultTrustStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Certificate Management	default (CellRSATokenKeyStore)	Valid from Aug 12, 2010 to Aug 12, 2011.
Certificate Management	root (CellRSATokenTrustStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Certificate Management	cn=capehatteras.raleigh.ibm.com, ou=root certificate, ou=jobmgr01cell01, ou=install07jobmgr01, o=ibm, c=us (CellRSATokenTrustStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Certificate Management	root (DmgrDefaultRootStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Certificate Management	dummyserversigner (DmgrDefaultDeletedStore)	Valid from Jul 30, 2003 to Oct 13, 2021.
Certificate Management	dummyclientsigner (DmgrDefaultDeletedStore)	Valid from Jul 30, 2003 to Oct 13, 2021.
Certificate Management	root (DmgrDefaultSignersStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Certificate Management	root (DmgrRSATokenRootStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Certificate Management	default (NodeDefaultKeyStore)	Valid from Aug 12, 2010 to Aug 12, 2011.
Certificate Management	default (NodeDefaultTrustStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Certificate Management	root (NodeDefaultTrustStore)	Valid from Aug 12, 2010 to Aug 8, 2025.
Cookie Protection		
Web Authentication	com.ibm.wsspi.security.web.webAuthReq	persisting
HttpOnly custom property	com.ibm.ws.security.addHttpOnlyAttributeToCookies	true
Single signon requires SSL	requiresSSL	false
Session Security (Cell=Dmgr01Cell01:Node=Install07AppSrv01:Server=server1)	enableSecurityIntegration	true
Java Authentication SPI Configuration		
Java Authentication SPI Configuration	enabled	false

The security configuration report, available from Version 6.1 on, is launched from a button at the top of the “Global security“ panel.

In Version 8, the report includes a new section called “Cookie Protection”. It contains the security configuration setting for HttpOnly, web Authentication settings, Single Sign-on SSL setting, and the session security integration setting for each server in the configuration.

Scroll to the bottom of the report to locate the “Cookie Protection” section.

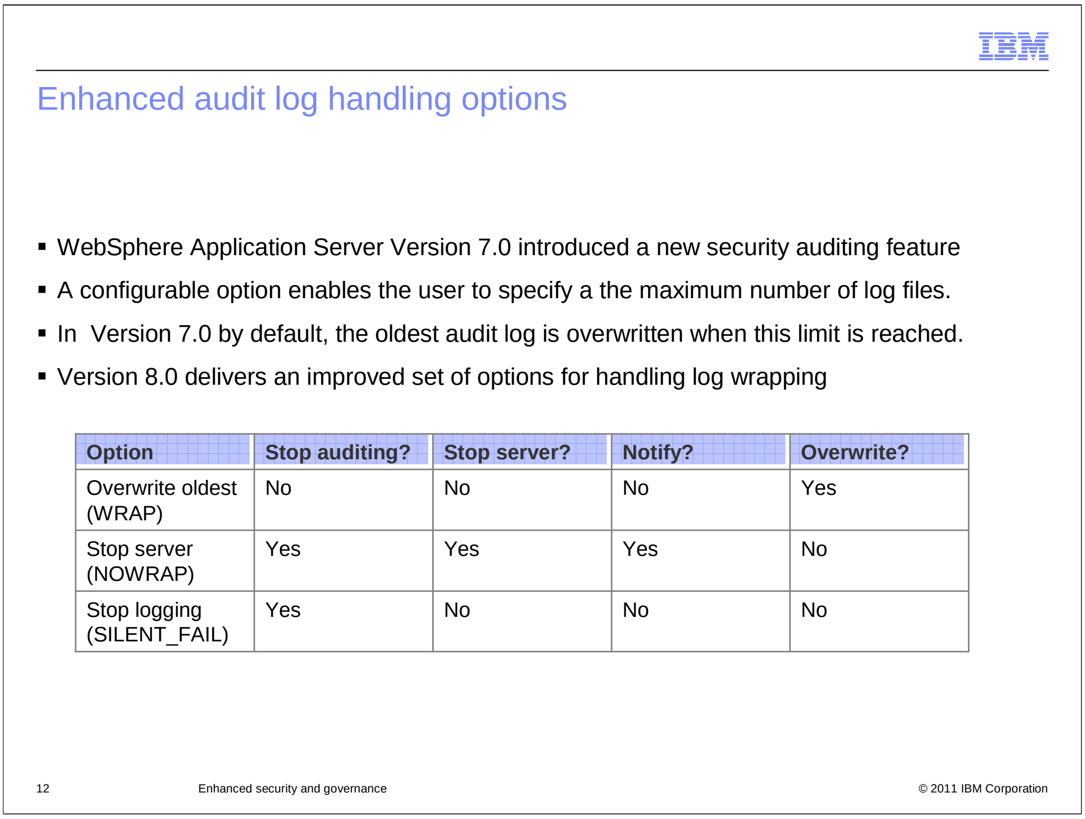


Section

Security audit log wrapping options

11 Enhanced security and governance © 2011 IBM Corporation

The next topic to cover is enhancements to security audit log management in WebSphere Application Server Version 8.



Enhanced audit log handling options

- WebSphere Application Server Version 7.0 introduced a new security auditing feature
- A configurable option enables the user to specify a the maximum number of log files.
- In Version 7.0 by default, the oldest audit log is overwritten when this limit is reached.
- Version 8.0 delivers an improved set of options for handling log wrapping

Option	Stop auditing?	Stop server?	Notify?	Overwrite?
Overwrite oldest (WRAP)	No	No	No	Yes
Stop server (NOWRAP)	Yes	Yes	Yes	No
Stop logging (SILENT_FAIL)	Yes	No	No	No

12 Enhanced security and governance © 2011 IBM Corporation

WebSphere Application Server Version 7.0 introduced a new security auditing capability.

This auditing system includes basic log management features for limiting the size and number of files generated. When the maximum number of files has been generated, the system must respond either by discontinuing logging or by overwriting, or “wrapping” the log files.

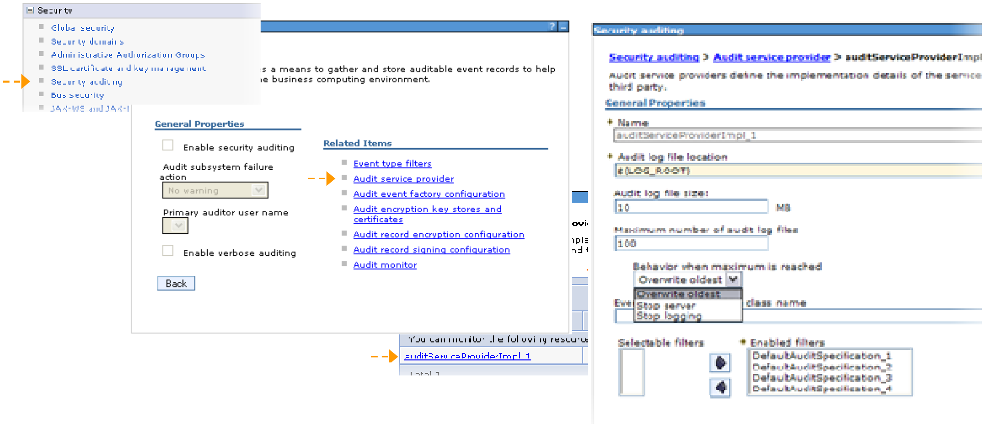
In version 7.0, the default behavior is to overwrite log files, beginning with the oldest, when the limit is reached. Therefore, unless an archiving or offloading capability has been implemented, the audit information in the oldest file is lost.

Version 8.0 provides improved options for handling log wrapping scenarios. The version 7 behavior is called “overwrite oldest” and remains the default.
A second option, “stop server” discontinues the auditing and quiesces the WebSphere server process then issues a notification. No log files are overwritten.
A third option, “stop logging” discontinues auditing, allowing the WebSphere server process to continue but does not issues a notification. Again, no log files are overwritten.

Note that “notification” can mean posting failure messages to the message log file or to sending an email to one or more recipients depending on how the audit monitor service is configured.

You should choose the option that is most aligned with your priorities. If server availability has the highest priority, choose Overwrite oldest or Stop logging. If continuity of logging has the highest priority then choose Stop server or Overwrite oldest. Use Stop server when continuous and complete logging information is more critical than server availability.

New options for handling maximum number of log file conditions



Security
- Global security
- Security domains
- Administrative Authorization Groups
- SSL certificate and key management
- Security auditing
- Bus security
- JAX-WS and JAX-I

s a means to gather and store auditable event records to help
e business computing environment.

General Properties

□ Enable security auditing

Audit subsystem failure action: No warning

Primary auditor user name

□ Enable verbose auditing

Back

Related Items
- Event type filters
- Audit service provider
- Audit event factory configuration
- Audit encryption key stores and certificates
- Audit record encryption configuration
- Audit record signing configuration
- Audit monitor

You can monitor the following resource

auditServiceProviderImpl_1

Total 1

Security auditing

Security auditing > Audit service provider > auditServiceProviderImpl

Audit service providers define the implementation details of the service
third party.

General Properties

* Name: auditServiceProviderImpl_1

* Audit log file location: ${LOG_ROOT}

Audit log file size: 10 MB

Maximum number of audit log files: 100

Behavior when maximum is reached: Overwrite oldest
- Overwrite oldest
- Stop server
- Stop logging

Eve... class name

Selectable filters

* Enabled filters
- DefaultAuditSpecification_1
- DefaultAuditSpecification_2
- DefaultAuditSpecification_3
- DefaultAuditSpecification_4

To locate the audit log wrapping settings expand the “Security” section of the navigation area and click the “Security auditing” link.

On the “security auditing” panel click the “audit service provider” link,

In the “audit service providers” table, click the link of the service provider that you are using,

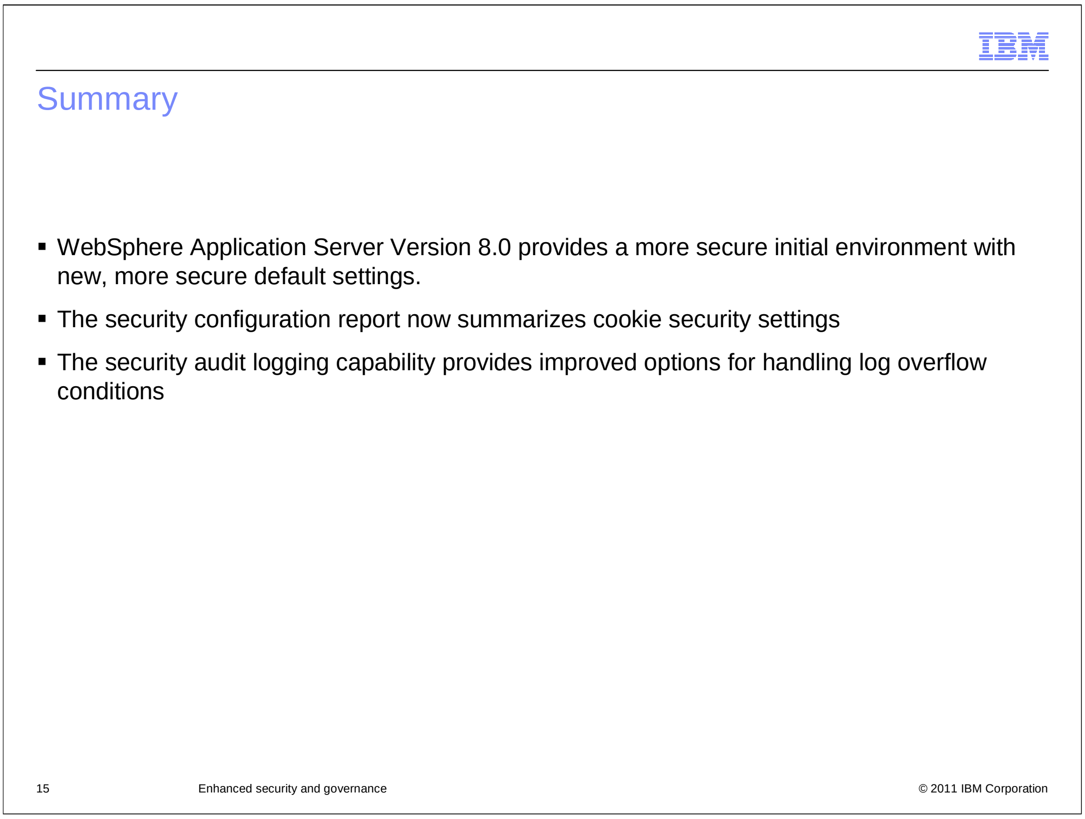
On the properties panel for the audit service provider, the log wrapping options are labeled, “Behavior when maximum is reached.”

Section

Summary

14 Enhanced security and governance © 2011 IBM Corporation

A brief summary of this presentation is discussed.

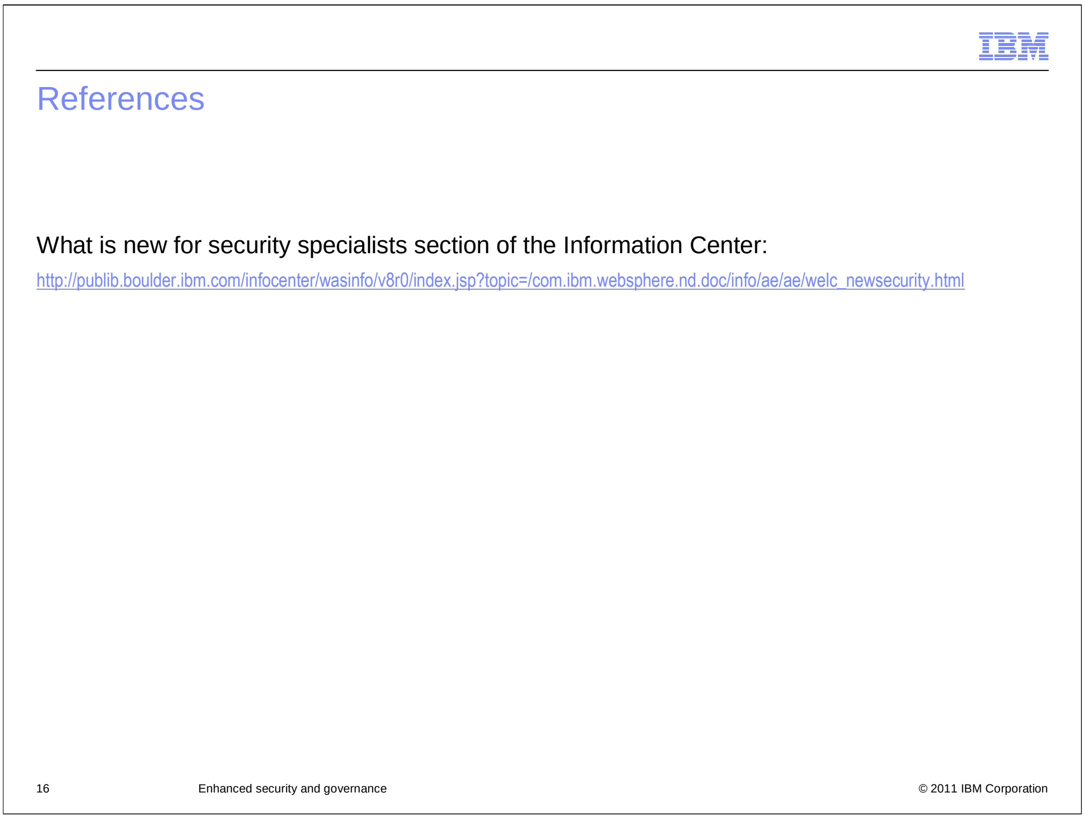


Summary

- WebSphere Application Server Version 8.0 provides a more secure initial environment with new, more secure default settings.
- The security configuration report now summarizes cookie security settings
- The security audit logging capability provides improved options for handling log overflow conditions

15 Enhanced security and governance © 2011 IBM Corporation

WebSphere Application Server Version 8.0 improves the security of your application serving environment by providing new, stronger default settings; A new summary of cookie security settings in the security configuration report; and improved options for handling log overflow conditions with the security auditing feature.

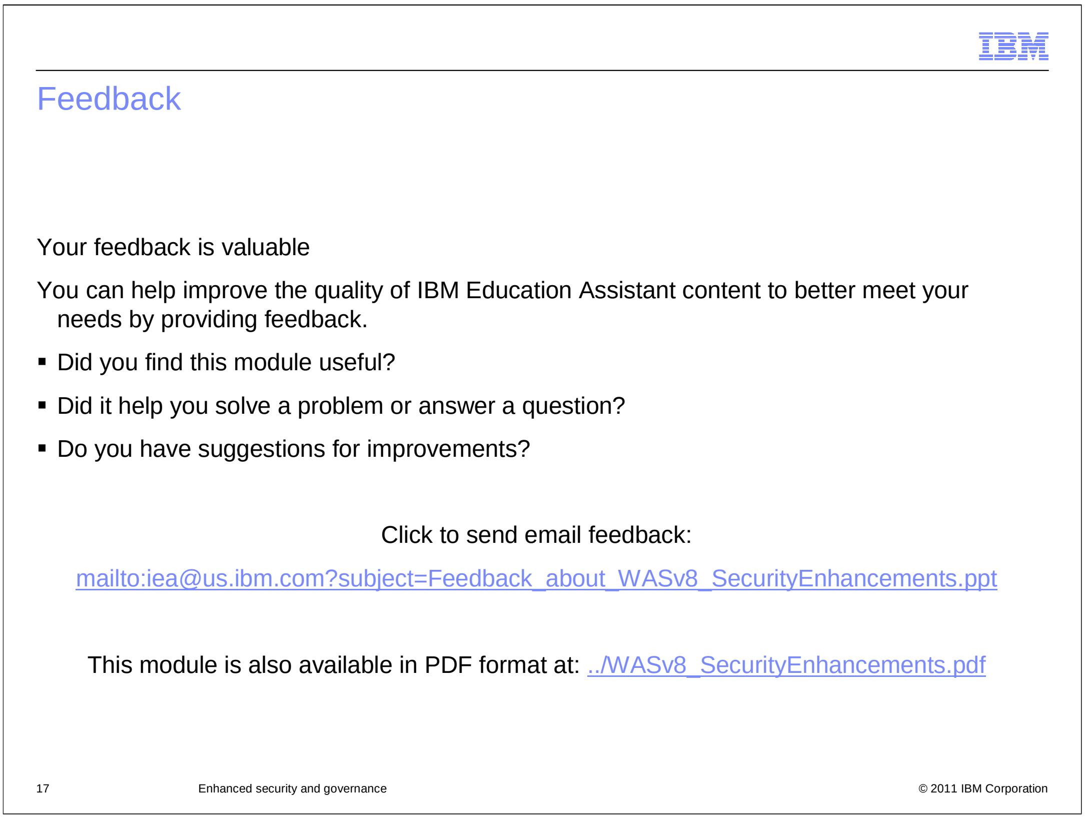


References

What is new for security specialists section of the Information Center:

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc_newsecurity.html

See the information center link shown here for additional information on security enhancements in WebSphere Application Server Version 8.0.



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?

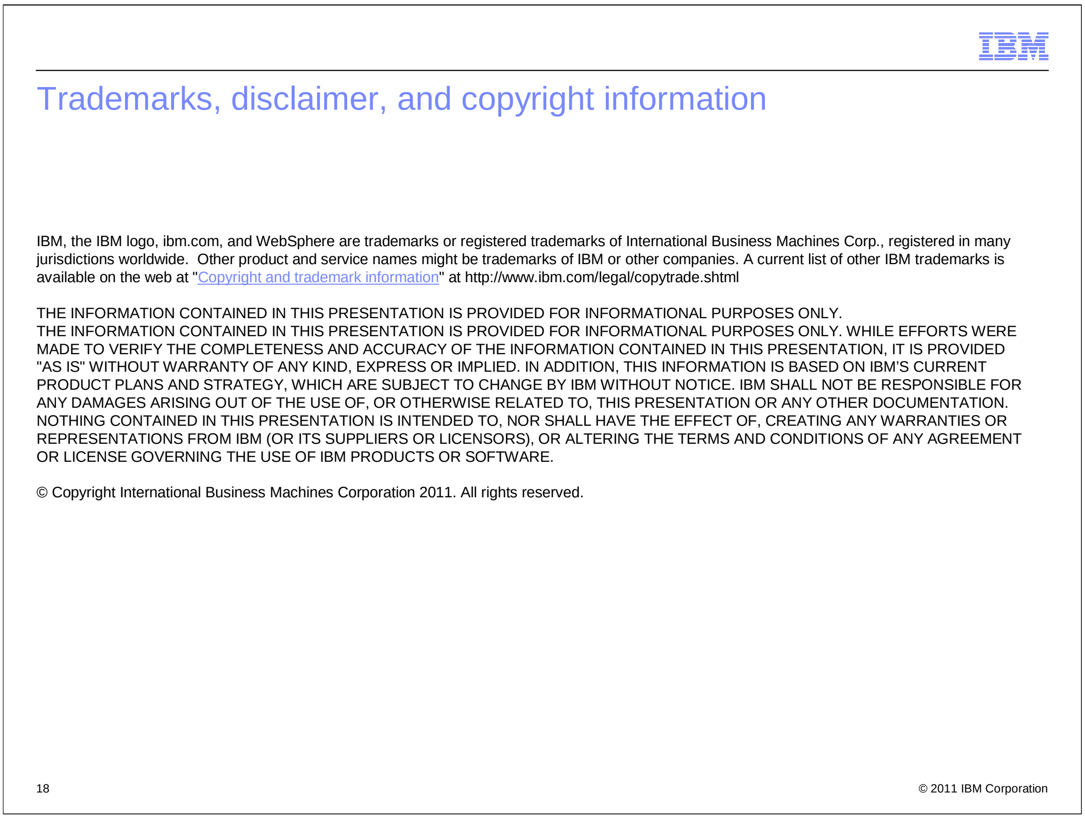
Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WASv8_SecurityEnhancements.ppt

This module is also available in PDF format at: ../WASv8_SecurityEnhancements.pdf

17 Enhanced security and governance © 2011 IBM Corporation

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



Trademarks, disclaimer, and copyright information

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 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.