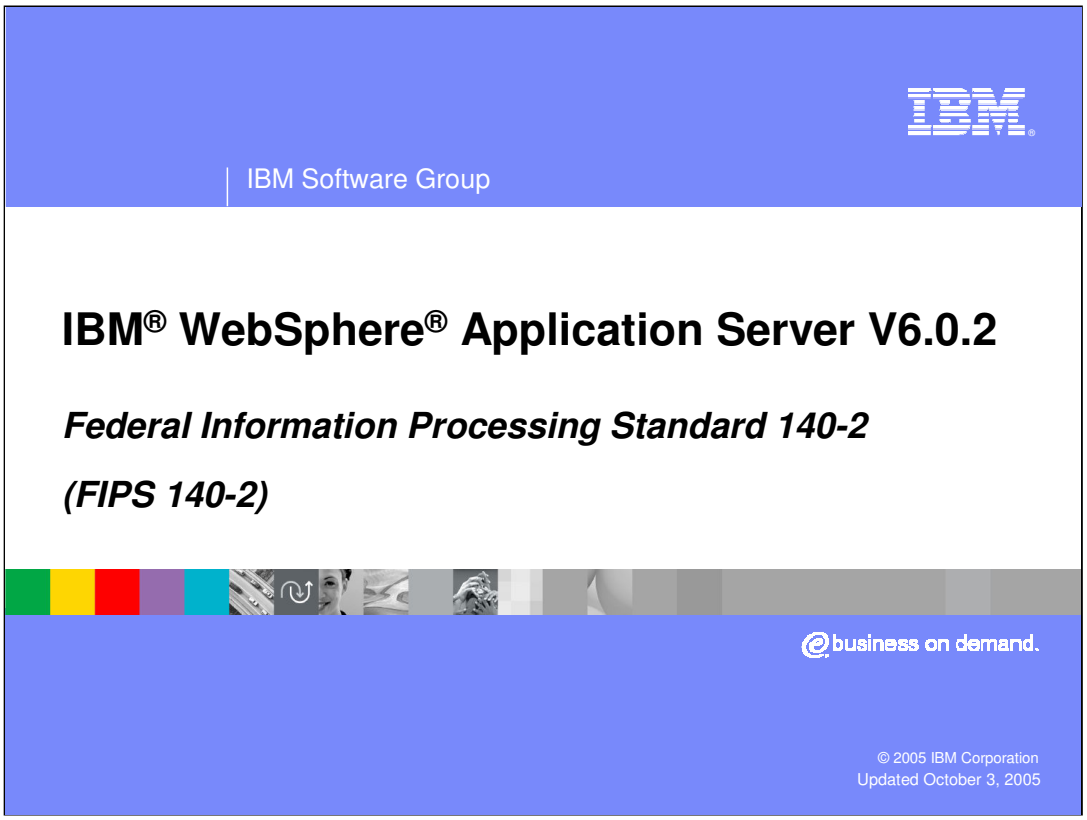


This presentation will provide an overview of the new support for the Federal Information Processing Standard 140-2 in WebSphere Application Server V6.0.2.

Goals

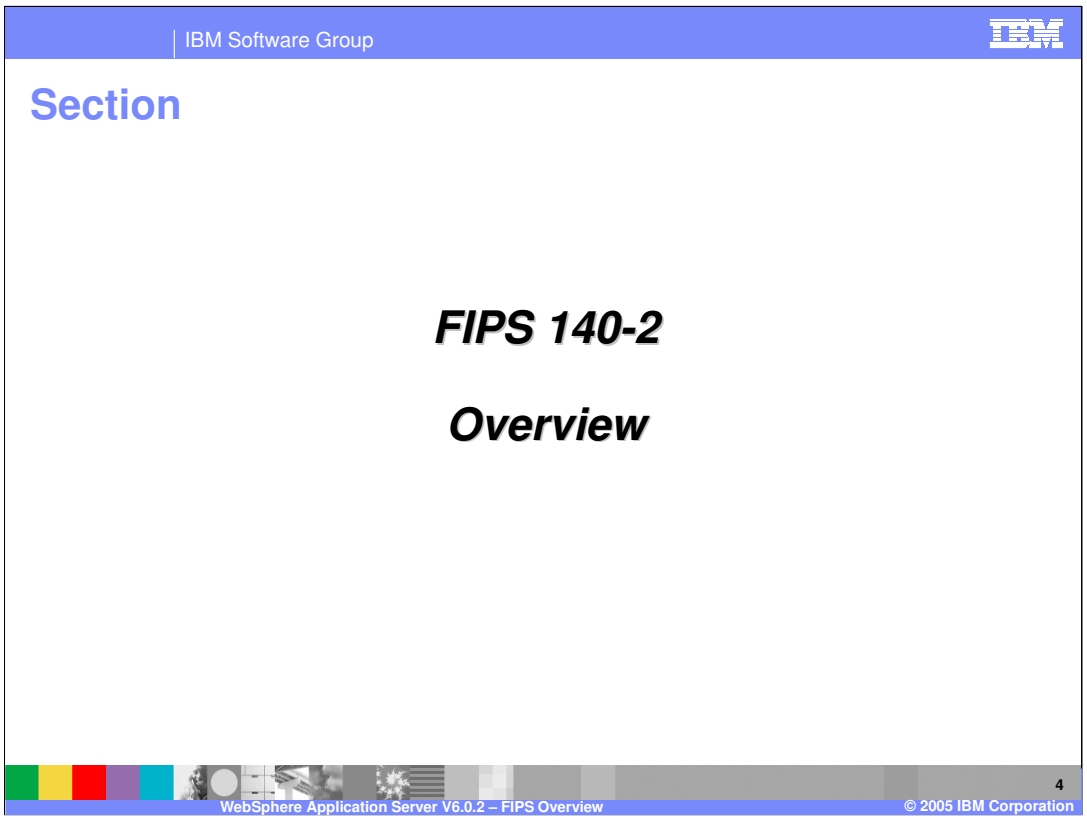
- Provide an overview of the Federal Information Processing Standard 140-2 (FIPS 140-2)
- Discuss FIPS enablement in WebSphere Application Server
- Discuss setup and Configuration tasks needed to enable FIPS for WebSphere Application Server

The goal of this presentation is to provide an overview of FIPS 140-2 and discuss FIPS enablement in WebSphere Application Server V6.0.2.

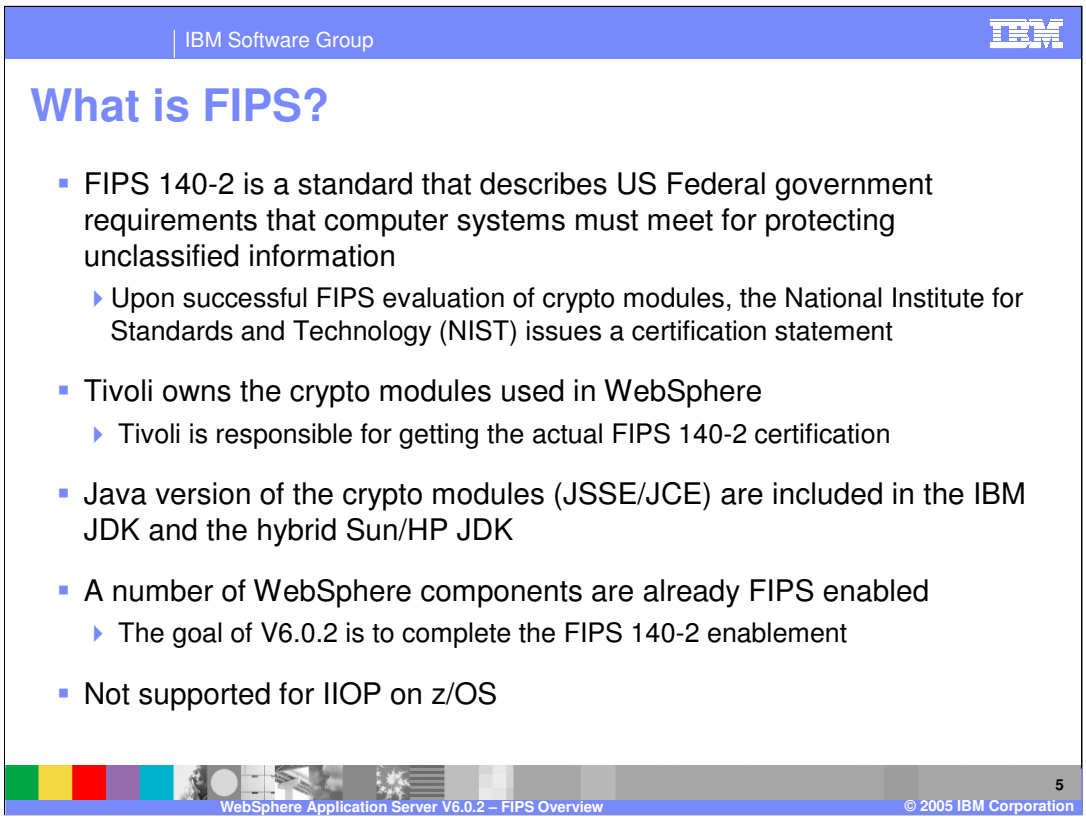
Agenda

- FIPS 140-2 Overview
  - FIPS background information
  - FIPS enablement status on WebSphere Application Server supported products
- Setup and Administration
- Reference

The agenda for this presentation is to first provide an overview of FIPS certification, then go into the details on how to configure WebSphere Application Server to be FIPS compliant, and finally to offer additional information about FIPS compliance in other IBM products.

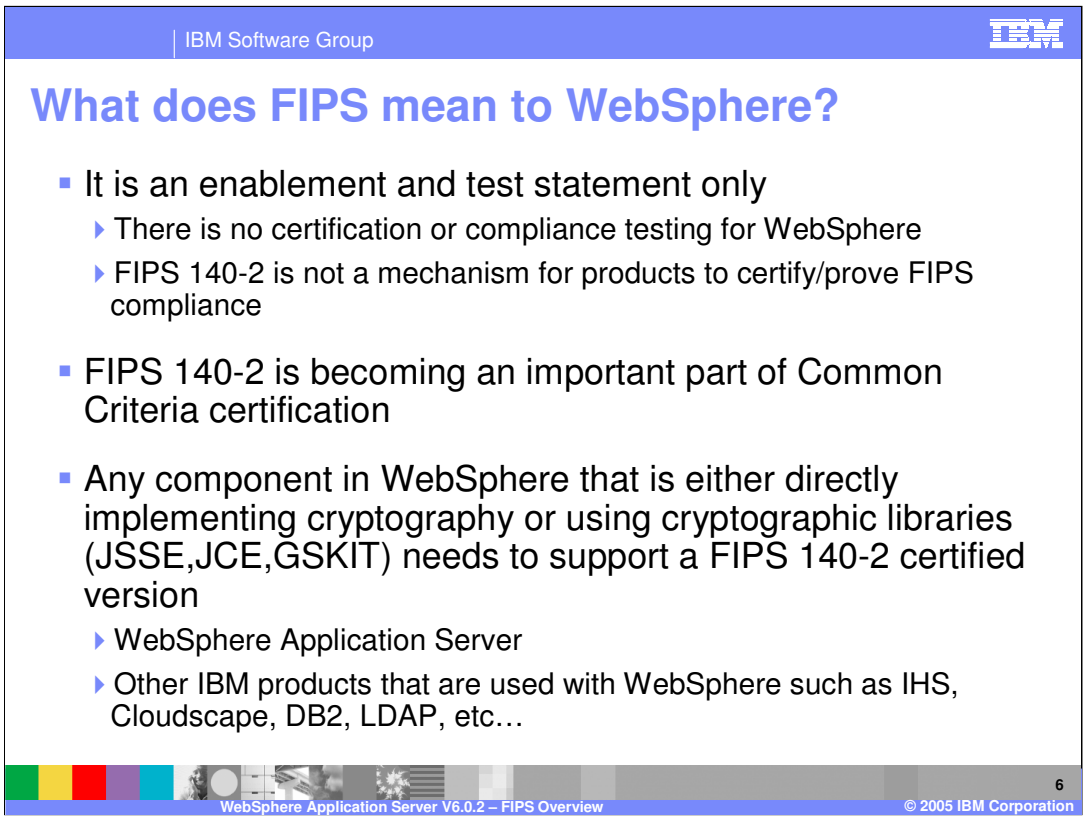


This section will cover the basic concepts of Federal Information Processing Standard 140-2.

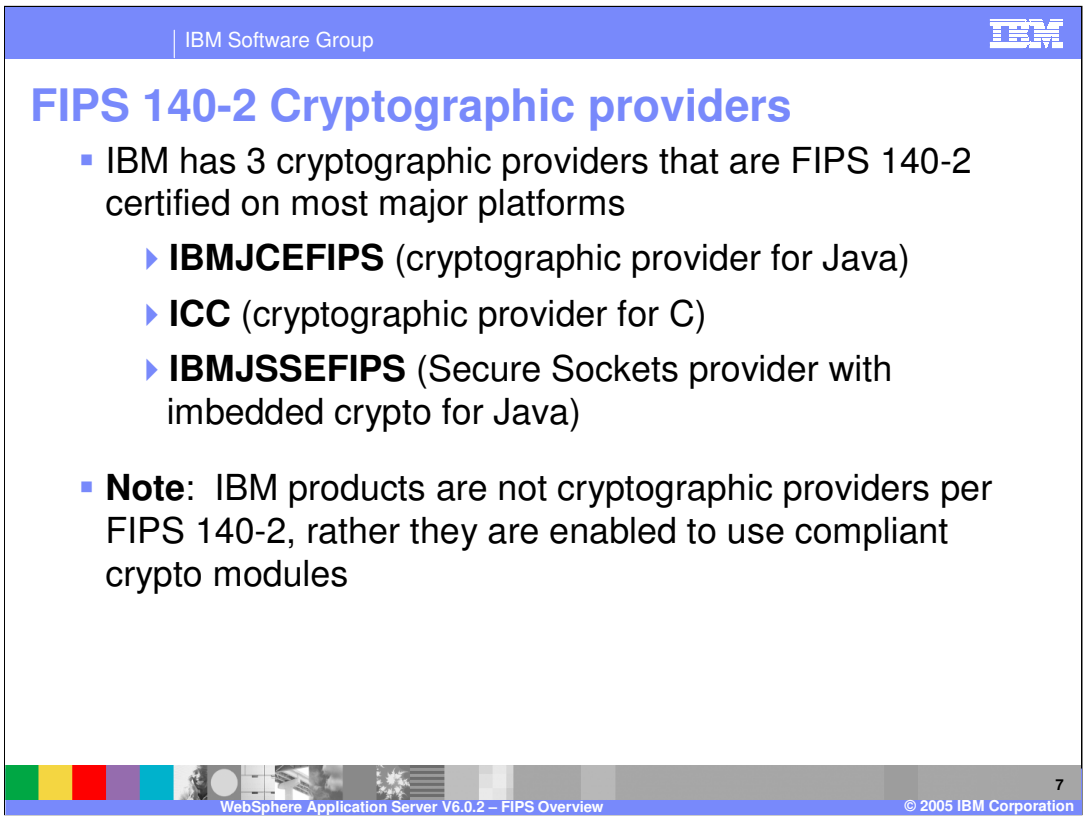


FIPS 140-2 is part of a number of government standards defining government security requirements. In particular, this FIPS standard specifies how computers and software must encrypt data to protect unclassified information, so it affects the cryptographic modules used to encrypt data. Tivoli group owns and is responsible for the FIPS compliance of the cryptographic modules used by WebSphere Application Server. Therefore, the Tivoli group is responsible for getting these modules certified compliant with the FIPS standard. A number of WebSphere components have already been enabled for FIPS support, and the V6.0.2 release is focused on completing this support.

With IIOP on z/OS, system SSL is used which has not been FIPS certified. Currently only the JSSE crypto modules have obtained FIPS certification.



WebSphere Application Server support for the FIPS standard is an enablement and test statement only. What this means is that WebSphere is able to use the Tivoli provided cryptographic modules and has been tested to utilize those modules appropriately. The FIPS standard has become an important part of the Common Criteria certification, which is also supported in WebSphere Application Server V6.0.2. Any WebSphere component capable of performing cryptographic work must support these FIPS compliant modules. This includes other products that are often used with WebSphere such as LDAP, DB2, and IHS.



There are three cryptographic modules that comprise IBM support of FIPS140-2. There is one module addressing each of the following areas:

•Java components

•C components

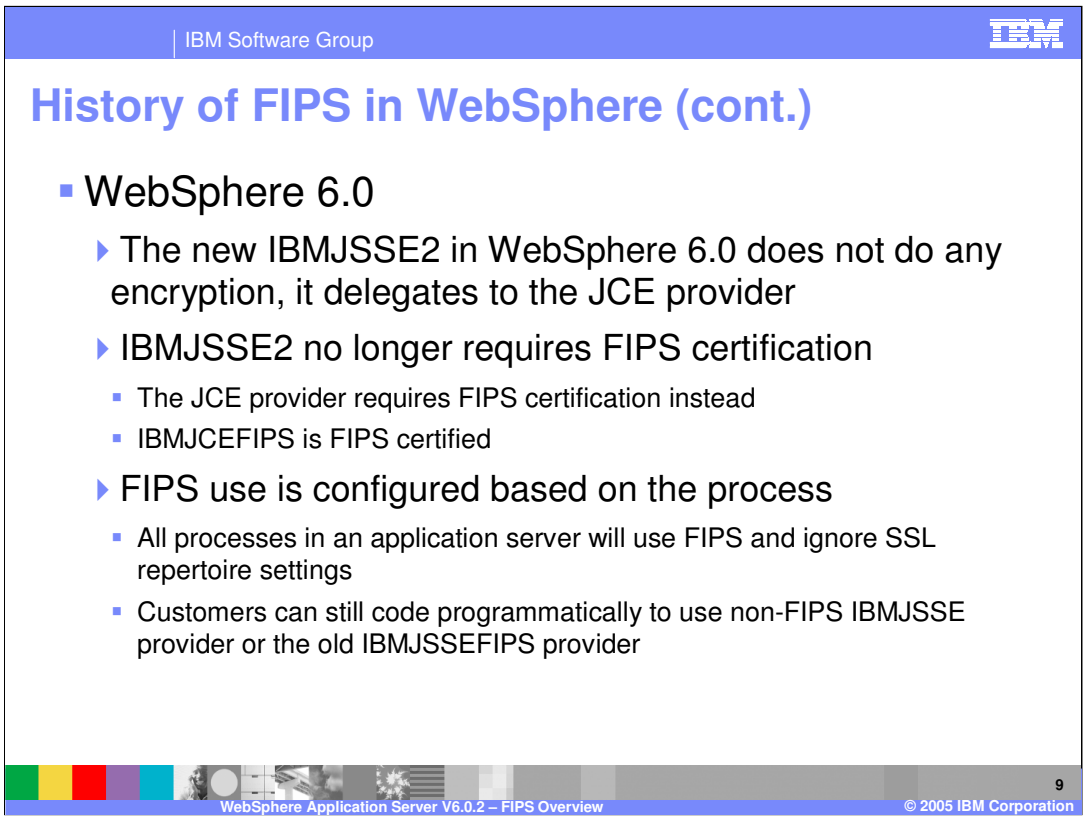
•SSL

IBM products are not considered cryptographic providers for the FIPS 140-2 standard, but are enabled to use compliant cryptographic modules.

History of FIPS in WebSphere

- WebSphere 5.0.2
  - The 5.0.2 release of WebSphere Distributed introduced the ability to use the FIPS 140-2 certified version of Tivoli's Java Secure Socket Extension (JSSE) and Java Cryptography Extension (JCE) packages
    - The non-FIPS JSSE and JCE are used by default
  - FIPS use is configured on a per SSL repertoire basis
    - Each SSL repertoire that needs to use FIPS is configured with the appropriate FIPS provider, ciphers, and protocol

Support for the FIPS 140-2 standard began in WebSphere Application Server for Distributed V5.0.2, which first provided the capability to configure WebSphere to use FIPS compliant modules. It is important to understand that by default WebSphere uses non FIPS compliant modules. FIPS compliance must also be configured for each SSL repertoire configured on an Application Server.



Support for FIPS compliance continued in WebSphere Application Server for Distributed V6.0 and was introduced for z/OS. In particular, there was a change to how WebSphere Application Server performed encryption, having the IBMJSSE2 component delegate to the JCE cryptographic provider instead. This meant that the IBMJSSE2 component no longer required FIPS certification since it no longer performed encryption work, bringing the Application Server to the current state of compliance.

Current WAS Component FIPS enablement

WAS Component	Type of crypto used	FIPS support in v6.0	FIPS support in v6.0.2
LTPA Keys	JCE	Yes	Yes
SSL Channel - HTTP/SSL - JMS/SSL	JCE	Yes	Yes
WS-Security runtime	JCE	No	Yes
LDAP/SSL	JCE	as a client to a FIPS tolerable LDAP server	Yes
WS Plugins	GSKit/ICC	No	Yes
Embedded TAM client AMJRTE 5.1.x	JSSE	No	Yes
XSS4J XML digital signature/XML encryption	JCE	No	Yes
JMX/SSL	JCE	Yes	Yes
DRS	JCE	Yes	Yes
Web Services	JSSE	Yes	Yes
IIOP/SSL (Distributed)	JCE	Yes	Yes

This chart shows the support for FIPS in a number of other WebSphere components.

FIPS state of Products supported with WAS

Product & version	Crypto Used (JSSE/JCE/ICC)	FIPS enabled with v6.0	FIPS enabled with 6.0.2
IIOP/SSL (z/OS)	System SSL	No	No
Cloudscape v5.1.60.17	JSSE/JCE	Yes	Yes
DB2 8.2	GSKIT/ICC	Yes	Yes
DB2 z/OS	NA	No	No
IHS (Apache -- Distributed) V2.0.47.1	GSKIT/ICC	Yes	Yes
IHS (Domino – z/OS)	System SSL	No	No
TAM 5.1	JSSE/JCE	No	Yes, if TAM is upgraded to v6.0.
LDAP – ITDS v5.2	GSKIT/ICC	No	Yes, if ITDS is upgraded to ITDS v6.0

This chart shows the support for FIPS in a number of other WebSphere components.

FIPS state of Products supported with WAS

Product & version	Crypto Used (JSSE/JCE/ICC)	FIPS enabled with v6.0	FIPS enabled with 6.0.2
LDAP z/OS	System SSL	No	No
Caching proxy server	GSKIT/ICC	No	yes
Load Balancer	N/A	N/A	N/A
WebSphere MQ 5.3	GSKIT/ICC	No	MQ 6.0 will support FIPS

There is no FIPS enablement for the Load balancer as it does not use GSKit and does not terminate SSL connections.

Section

Install and Configuration

This section discusses the installation and configuration steps for enabling FIPS compliance.

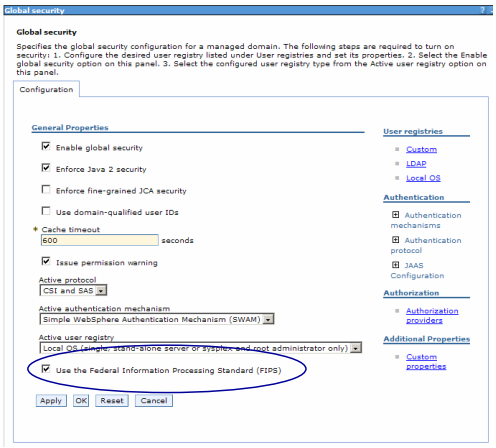
Install

- No installation impact to WebSphere Application Server
- FIPS versions of JSSE/JCE are shipped as part of the SDK
- The Global Security Kit (GSKIT) includes IBM Crypto for C (ICC) which is FIPS 140-2 certified
  - GSKIT is included with products like IHS, LDAP, etc..

No extra installation steps are required to enable the WebSphere Application Server for FIPS compliance. The FIPS compliant cryptographic modules are shipped as part of the standard SDK. The Global Security Kit that is also used by other components that work with WebSphere such as IHS and LDAP servers, includes a cryptographic module that is FIPS compliant as well.

Enabling FIPS Compliance

- FIPS is not turned on by default when global security is enabled
- Enable Federal Information Processing Standard using the Administrative Console
  - Select **Security > Global Security**
  - Select the option to Use FIPS and click OK
  - IBMJSSE2 and IBMJCEFIPS will be enabled



FIPS compliance is not the default setting in WebSphere Application Server. An extra checkbox for FIPS compliance must be selected. When the useFIPS property is set to true from the Administrative Console the SSL repertoires should be visited to reflect the FIPS ciphers, provider, and protocol.

Configuring Clients for FIPS

- Java clients that access enterprise beans
  - modify install_dir/profiles/profile_name/properties/sas.client.props file and set the following property:

    #com.ibm.security.useFIPS=false

    com.ibm.security.useFIPS=true
- Administrative clients (WS Admin) using the Simple Object Access Protocol (SOAP) connector
  - modify the following property in install_dir/profiles/profile_name/properties/soap.client.props file

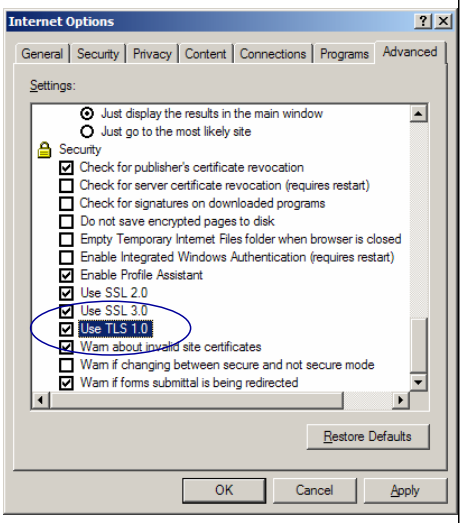
    #com.ibm.ssl.contextProvider=IBMJSSE2

    com.ibm.ssl.contextProvider=IBMJSSEFIPS

There are some extra steps required for clients accessing a FIPS compliant server, these are detailed on this slide. When you select the Use the Federal Information Processing Standard (FIPS) option on the Global Security panel, the Lightweight Third-Party Authentication (LTPA) token format is not backwards-compatible with previous releases of WebSphere Application Server. However, you can continue to use the LTPA keys configured using a previous version of WebSphere Application Server.

Web Browser setting

- Transport Layer Security (TLS) should be enabled for Web Browsers to access Applications on FIPS enabled servers
- Internet Explorer browser
  - TLS is not enabled by default.
  - Select **Tools > Internet Options**
  - On the Advanced tab, select “Use TLS 1.0” option
- Mozilla 1.7 is enabled for TLS by default
- Netscape Version 4.7.x and earlier may not support TLS



After configuring WebSphere Application Servers for FIPS compliance, browsers that access applications on that server should have their Transport Layer Security or TLS enabled. Some browsers may not be enabled for Transport Layer Security and you may see 505 error when attempting to access a secured server.

By default, Microsoft Internet Explorer Version 5.5 might not have Transport Layer Security (TLS) enabled. To enable TLS, open the Internet Explorer browser and click **Tools > Internet Options**. On the Advanced tab, select the Use TLS 1.0 option. **Note:** Netscape Version 4.7.x and earlier versions might not support TLS.

Section

Summary

This section will summarize the topics discussed in this lecture.

Summary

- This presentation explained the concepts behind the FIPS 140-2 certification
- Showed how to configure WebSphere Application Server to be FIPS 140-2 compliant

This presentation explained the FIPS compliance enabled with WebSphere Application Server. It showed hot to enable a WebSphere Application Server to support FIPS compliance and other components that would need to be configured in the environment such as client and web browsers.

Glossary

- FIPS – Federal Information Processing Standard
- NIST – National Institute of Standards and Technology
- JSSE – Java Secure Socket Extension
- JCE – Java Cryptography Extension
- GSKit - IBM Global Security Kit
- ICC – IBM Crypto for C

References/Resources

- NIST Computer Security Division home page: http://csrc.nist.gov/
- FIPS PUB 140-2 Security Requirements for Cryptographic Modules: http://csrc.nist.gov/cryptval/140-2.htm
- Security Evaluations of IBM Products: http://www-3.ibm.com/security/standards/st_evaluations.shtml

Section

Appendix

API support

- JSSE has an API that returns getDefaultCipherSuites which will return just FIPS ciphers when FIPS is enabled.
- Three new java.security.Security objects have been added to check for FIPS enablement and return FIPS JCE and JSSE providers.
  - Com.ibm.websphere.security.fips.enabled – will be set to true when FIPS is enabled false otherwise. This property should be used to determine if FIPS is enabled in WebSphere.
  - Com.ibm.websphere.security.fips.jceProviders – will return a '|' separated list of FIPS JCE providers. IBMJCEFIPS is the only provider in the list at this time.
  - Com.ibm.websphere.security.fips.jsseProviders – will return a '|' separated list of FIPS JSSE providers. IBMJSSE2 is the only provider in the list at this time.

Functional Description - Some FIPS details

- IBMJCEFIPS is FIPS certified.
- FIPS requires the SSL protocol to be TLS.
- IBMJSSE2 in a FIPS mode supports the following ciphers:
  - SSL_RSA_WITH_AES_128_CBC_SHA
  - SSL_RSA_WITH_3DES_EDE_CBC_SHA
  - SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
  - SSL_DHE_RSA_WITH_AES_128_CBC_SHA
  - SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  - SSL_DHE_DSS_WITH_AES_128_CBC_SHA
  - SSL_DHE_DSS_WITH_3DES_ECE_CBC_SHA
  - SSL_DH_anon_WITH_AES_128_CBC_SHA
  - SSL_DH_anon_WITH_3DES_EDE_CBC_SHA

Trademarks, Copyrights, and Disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	CICS	IMS	MQSeries	Tivoli
IBM(logo)	Cloudscape	Informix	OS/390	WebSphere
e(logo)business	DB2	iSeries	OS/400	xSeries
AIX	DB2 Universal Database	Lotus	pSeries	zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

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

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

