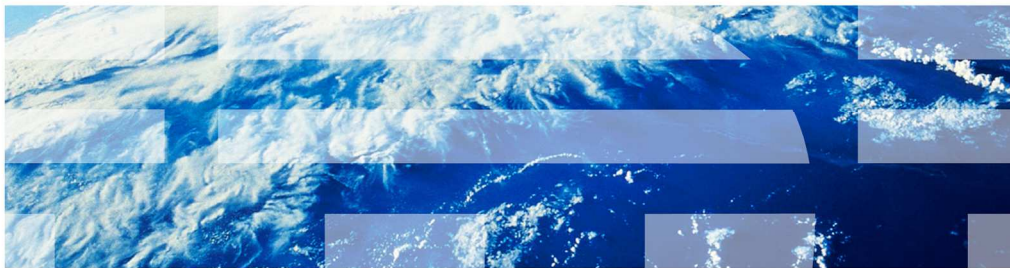


IBM WebSphere Application Server V8.0.0.3

Support for NIST SP 800-131 and NSA Suite B



© 2012 IBM Corporation

This presentation describes Support for NIST SP 800-131 and NSA Suite B that is included in IBM WebSphere® Application Server V8.0.0.3.



WebSphere support for NIST SP800-131 and NSA Suite B

- The National Institute of Standards and Technology (NIST) developed a new standard, SP800-131 to extend the current FIPS standards.
- The National Security Agency (NSA) developed a new standard Suite B.

WebSphere Application Server can be configured to work with various security standards to meet security requirements required by the US government. Government agencies and financial institutions use these standards to ensure that their products conform to specified security requirements.

Recently, new security standards have become available. The National Institute of Standards and Technology (NIST) developed a new standard, Special Publications 800-131 (or SP 800-131). The National Security Agency (NSA) developed a new standard, Suite B.

WebSphere Application Server now works with these new security standards.

What is SP800-131 and Suite B support?

- WebSphere Application Server currently supports Federal Information Processing Standards (FIPS140-2)
- The new standard SP800-131 created by NIST requires longer key lengths and stronger cryptographic algorithms than those required by the FIPS 140-2 standards.
- NIST places requirements on when products move to SP800-131. One requirement is to provide a transition configuration to the new standard. And NIST places a required date for when products must move to the new standard in the strict mode.
- The Suite B standard was created by the NSA to specify cryptographic interoperability. It places some tighter requirements on SP800-131, requiring specific cryptographic algorithms.
- The requirements of the standards take place in the Java Cryptography Extension (JCE) and Java Secure Socket Extension (JSSE) parts of the IBM SDK. The standards are supported in these levels of the IBM SDK.
 - SDK 6.0 SR10
 - SDK 6.26 SR1
 - SDK 7.0 SR1
- With this feature, WebSphere Application Server now supports both of the standards.

WebSphere Application Server supports Federal Information Processing Standards that specify requirements on cryptographic modules placed by the National Institute of Standards and Technology.

SP800-131 strengthens the algorithms and increases the key lengths in order to increase security. SP800-131 provides both transition mode and strict mode. NIST requires a date for when products must comply with the SP 800-131 strict mode. The time between the present date and the required date is known as the transition time. The transition time is a grace period given to customers and products to migrate to the strict mode.

Separate from NIST, the National Security Agency developed a new standard Suite B. Suite B imposes tight requirements using specific cryptographic algorithms and keys.

The requirements of both security standards are available in the IBM SDK. To use this feature, an SDK upgrade is necessary.

Usage scenarios

The following scenarios illustrate where you might use this feature.

Scenario 1 - Enabling SP800-131

Scenario: A system administrator wants to enable SP 800-131 in Strict Mode, first going through Transition Mode

Steps:

1. On deployment manager, **confirm current FIPS status.**
2. On deployment manager, configure **SP 800-131 transition mode**
3. Propagate the change to the nodes
4. On deployment manager, **update SSL protocol** to TLSv1.2 which is SP 800-131 compliant level
5. Make sure other programs such as browser, LDAP, and other programs communicate using TLSv1.2
6. **Update ssl.client.props** to communicate with nodes
7. Propagate the change to the nodes
8. On deployment manager, **configure SP 800-131 strict mode.**
9. **Convert certificates** with signature algorithm that comply with SP800-131

One of the typical scenarios is going to SP 800-131 strict mode.

Scenario 1 looks into this closely. For this example, the SSL dynamic configuration update feature was turned on so that you can see how SP 800-131 configuration affects communication between WebSphere and other programs. It will help you see what to expect when the security standard is enforced.

Scenario 2 - Configure system to SP800-131 mode

Scenario: A system administrator wants to configure WebSphere to be compliant with the SP800-131 standard.

Steps:

1. On a deployment manager convert certificates to comply with the SP800-131 standard.
2. On deployment manager, configure **SP 800-131 strict mode**
3. Propagate the change to the nodes, doing manual sync nodes.
4. Restart the deployment manager and all the nodes and servers in the cell.
5. Make sure other programs such as browser, LDAP, and other programs communicates using TLSv1.2
6. **Update `ssl.client.props`** to communicate with nodes

Another typical scenario is going straight from the state where FIPS is disabled, to SP 800-131 strict mode.

Scenario 2 assumes SSL dynamic update feature is turned off while configuration takes place.

This will help you see the fastest configuration steps for the cell straight to SP 800-131 strict mode.

Scenario 3 - Configure system to Suite B mode

Scenario: A system administrator wants to configure WebSphere to be compliant with the Suite B standard.

Steps:

1. On a deployment manager convert certificates to comply with the Suite B standard.
2. On deployment manager, configure **Suite B mode**
3. Propagate the change to the nodes, doing manual sync nodes.
4. Restart the deployment manager and all the nodes and servers in the cell.
5. Make sure other programs such as browser, LDAP, and other programs communicates using TLSv1.2
6. **Update `ssl.client.props`** to communicate with nodes

The final scenario goes from “FIPS is disabled” to “Suite B”

Just like scenario2, scenario 3 also assumes that the SSL dynamic update feature is turned off while configuration takes place.

This will help you see the fastest configuration steps to go straight to Suite B.

Summary

- This feature supports newly introduced Security Standards.
- This feature provides transition mode for smooth transition to the new Standards.
- Not only WebSphere Application Server but also other programs communicating with it will need to be compliant with the standard.

In Summary, support for NIST SP 800-131 and NSA Suite B enables WebSphere Application Server to comply with new security standards.

Section

Demonstration

This section shows screen captures of Scenarios 1, 2, and 3.

Preparing for configuration (1 of 2)

FIPS configuration includes certificate conversion and SSL protocol update. You can turn off Dynamic SSL update so that the change takes effect after restarting the cell.

In this section, screen captures for scenario 1 shows configuration when dynamic SSL update is on. Screen captures for scenario 2 and 3 shows configuration when dynamic SSL update is off.

SSL certificate and key management

SSL certificate and key management

[SSL configurations](#)

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint. [Rel:](#)

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](#)

[Manage FIPS](#)

Dynamically update the run time when SSL configuration changes occur

10 Support for NIST SP 800-131 and NSA Suite B © 2012 IBM Corporation

Before using this feature, look into the “Dynamically update the runtime when SSL configuration changes occur” option.

With this feature turned on, configuration change takes place immediately. It will help you see how the new configuration affect communication with other programs. However, you might need to make adjustment each time you change configurations.

With this feature turned off, configuration change takes place after the server is restarted. You will not see what configuration affects what area of communication, but you can make configuration changes all at once.

Preparing for configuration (2 of 2)

- Back up the configuration before FIPS configuration because it will affect communication with other programs.

- backupConfig command for V8 (contains URL link to restoreConfig command)

- http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/xml_backupconfig.html

- backupConfig command for V7 (contains URL link to restoreConfig command)

- http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/xml_backupconfig.html

Before you use this feature, back up the configuration.

This feature involves certificate change and an SSL protocol change that affects communication between WebSphere and other programs.

It might be helpful to have original configuration ready to restore.

Demonstration - Scenario 1

This section goes through the steps of scenario 1 with screen captures. Scenario 1 is the migration scenario from FIPS 140-2 to SP 800-131 strict mode with the Dynamic SSL update feature turned on.

Manage FIPS panel

Manage FIPS panel is launched from:

administrative console -> Security -> ssl certificate and key management

SSL certificate and key management

SSL configurations

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

In previous versions of this product, it was necessary to manually configure each endpoint for Secure Sockets Layer (SSL). In this version, you can define a single configuration for the entire application-serving environment. This capability enables you to centrally manage secure communications. In addition, trust zones can be established in multiple node environments by overriding the default, cell-level SSL configuration.

If you have migrated a secured environment to this version using the migration utilities, the old Secure Sockets Layer (SSL) configurations are restored for the various endpoints. However, it is necessary for you to re-configure SSL to take advantage of the centralized management capability.

Configuration settings

[Manage endpoint security configurations](#)

[Manage certificate expiration](#)

Manage FIPS

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](#)
- [Certificate Authority \(CA\) client configurations](#)

This slide shows how to get to new panel to configure new security standard.

Confirm current FIPS Level

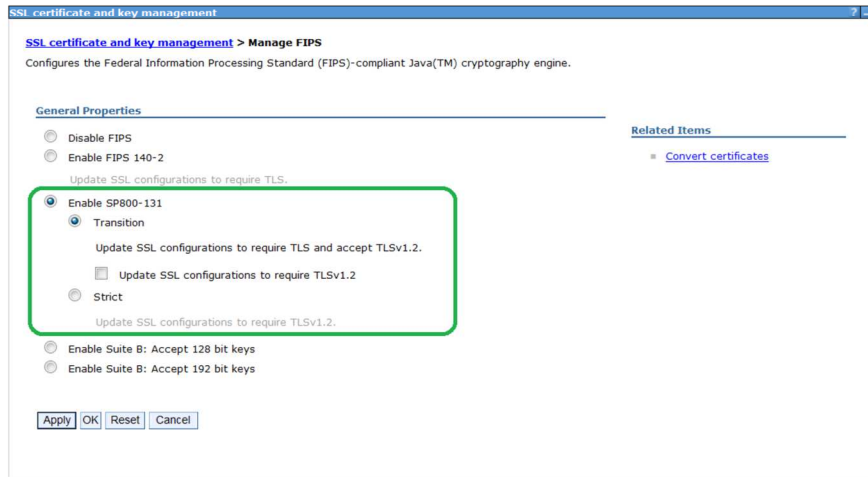
Confirm current FIPS level. In the example below, FIPS140-2 is configured.

The screenshot shows the 'Manage FIPS' configuration page in the IBM SSL certificate and key management console. The page title is 'SSL certificate and key management' and the breadcrumb is 'SSL certificate and key management > Manage FIPS'. The description states: 'Configures the Federal Information Processing Standard (FIPS)-compliant Java(TM) cryptography engine.' The 'General Properties' section contains several radio button options: 'Disable FIPS', 'Enable FIPS 140-2' (which is selected and highlighted with a green box), 'Enable SP800-131', 'Transition', 'Strict', 'Enable Suite B: Accept 128 bit keys', and 'Enable Suite B: Accept 192 bit keys'. Below these options are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'. A 'Related Items' section on the right contains a link for 'Convert certificates'. The footer includes the page number '14', the text 'Support for NIST SP 800-131 and NSA Suite B', and the copyright notice '© 2012 IBM Corporation'.

The current configuration should be displayed on this panel.

Configure SP 800-131 transition mode

Configure SP 800-131 transition mode. Transition mode supports both current algorithm and SSL protocols, and the ones that comply with SP 800-31 strict mode.



First, configure “SP 800-131” transition mode.

Save transition mode

Save transition mode and restart deployment manager. Run syncNode command manually to propagate the change to nodes.

Messages

- Changes have been made to your local configuration. You can:
 - Save directly to the master configuration.
 - Review changes before saving or discarding.
- An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).
- The server may need to be restarted for these changes to take effect.

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](#)

[Manage FIPS](#)

Dynamically update the run time when SSL configuration changes occur

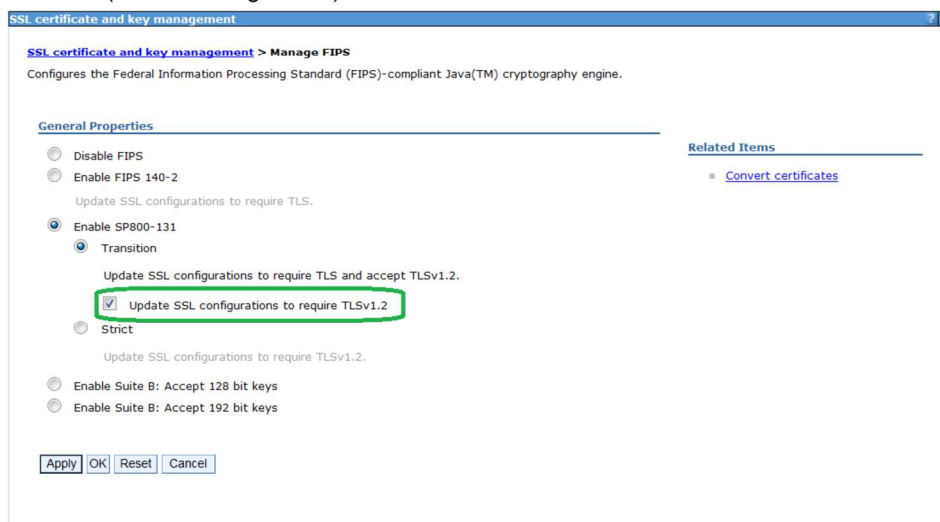
Related Items

- [SSL configurations](#)
- [Dynamic outbound endpoint SSL configurations](#)
- [Key stores and certificates](#)
- [Key sets](#)
- [Key set groups](#)
- [Key managers](#)
- [Trust managers](#)
- [Certificate Authority \(CA\) client configurations](#)

Save the configuration and propagate the changes. The system is now at SP 800-131 transition mode.

Update SSL protocol to require TLSv1.2

Now, on deployment manager, update SSL protocol to require TLSv1.2 to be compliant with SP800-131. This change takes effect immediately if dynamic SSL update feature is enabled (Default configuration)



There is not much impact after going to SP 800-131 transition because it supports all the signature algorithms and protocols.

The next step is to enforce SSL protocols to TLSv1.2 while still in SP 800-131 transition mode.

TLSv1.2 is required for SP 800-131 and both Suite B modes.

Click the "Update SSL configuration to require TLSv1.2". The change will take place immediately when the Dynamic SSL update feature is turned on.

The check box labeled with "Update SSL configuration to require TLSv1.2" is to trigger the action. It does not show current status.

It will update SSL protocols in every SSL configuration.

Check browser configuration

Internet Explorer cannot display the w...



Internet Explorer cannot display the webpage

What you can try:

[Diagnose Connection Problems](#)

[More information](#)



The connection was interrupted

The connection to localhost:9043 was interrupted while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

[Try Again](#)

If administrative console is no longer accessible from browser after changing SSL protocols to TLSv1.2, it is likely that browser is not configured for or supporting the protocol.

Internet Explorer V8 (on Windows 7 and Windows 2008) has option to enable the protocol by going Tools > Internet Options > Advanced (Tab) > Security

Firefox support schedule:

<http://forums.mozillazine.org/viewtopic.php?f=7&t=1831235>

As soon as TLSv1.2 is turned on, if browser does not support TLSv1.2, you can no longer communicate with the administrative console or with applications running on WebSphere Application Server.

This is because WebSphere Application Server now enforces communication with TLSv1.2.

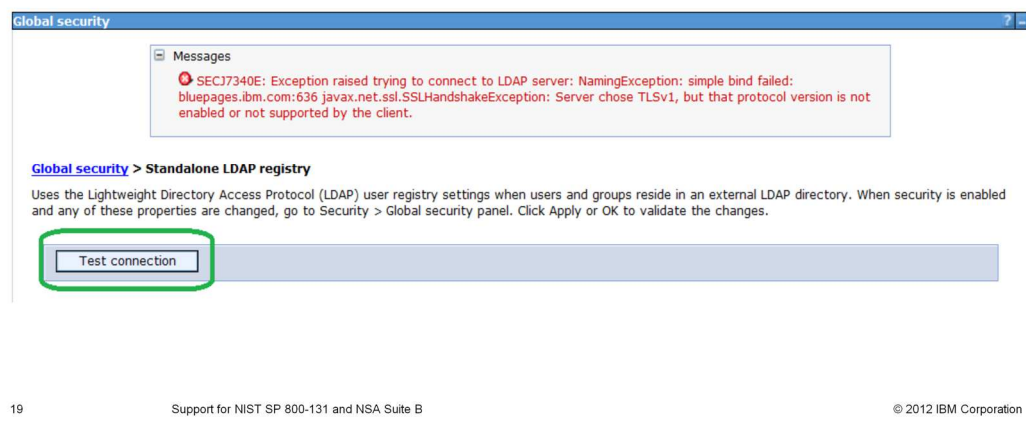
If this happens, turn on TLSv1.2 support in the browser.

Check user registry configuration

Ensure connection between user registry is working after SSL protocol change to TLSv1.2.

Following is an example where LDAP keeps using "TLSv1" and WebSphere requires TLSv1.2. For this case, it is necessary to re-configure LDAP so that it can communicate using TLSv1.2.

Similar connection test is necessary for Federated Repository or custom user registry where SSL connection is used.



The screenshot shows the 'Global security' console. At the top, there is a 'Messages' section with a red error icon and the following text: 'SECJ7340E: Exception raised trying to connect to LDAP server: NamingException: simple bind failed: bluepages.ibm.com:636 javax.net.ssl.SSLHandshakeException: Server chose TLSv1, but that protocol version is not enabled or not supported by the client.' Below the messages, the navigation path 'Global security > Standalone LDAP registry' is shown. Underneath, there is a descriptive paragraph about LDAP user registry settings. At the bottom of the console, a 'Test connection' button is highlighted with a green rectangular box.

The SSL protocol change to TLSv1.2 might affect communication between WebSphere Application Server and the user registry.

In this example, there is an error message for stand-alone LDAP configured using SSL. Just like the example for the browser, the user registry must support TLSv1.2 if an SSL connection is used.

Check nodes

Communication between deployment manager and nodes will also be affected when ssl protocol is changed to TLSv1.2. It is necessary to run nodeSync command manually.

Before running the command, ssl.client.props need to be updated so that syncNode command uses TLSv1.2 to communicate with deployment manager

Nodes

Use this page to manage nodes in the application server environment. A node corresponds to a physical computer system with a distinct IP host address. The following table lists the managed and unmanaged nodes in this cell. The first node is the deployment manager. Add new nodes to the cell and to this list by clicking Add Node.

Preferences

Add Node Remove Node Force Delete Synchronize Full Resynchronize Stop

| Select | Name | Host Name | Version | Discovery Protocol | Status |
|--------------------------|--------------------------------------|-------------------------|------------|--------------------|--------|
| <input type="checkbox"/> | hirokotCellManager01 | hirokot.raleigh.ibm.com | ND 8.0.0.2 | TCP | |
| <input type="checkbox"/> | hirokotNode01 | hirokot.raleigh.ibm.com | ND 8.0.0.2 | TCP | |

Total 2

As the change takes place in the deployment manager, nodes are no longer able to communicate with the deployment manager. In the next slides, you will see how to re-establish the communication.

ssl.client.props file

```
# Sample ssl.client.props
#-----
# Global SSL Properties (applies to entire process)
#-----
com.ibm.ssl.defaultAlias=DefaultSSLSettings
com.ibm.ssl.performURLHostNameVerification=false
com.ibm.ssl.validationEnabled=false
com.ibm.security.useFIPS=true //turn on when FIPS is enabled
com.ibm.websphere.security.FIPSLevel=transition //specify mode
user.root=C:/WAS80ND/AppServer/profiles/Dmgr01
....
#-----
# This SSL configuration is used for all client SSL connections, by default
#-----
com.ibm.ssl.alias=DefaultSSL.Settings
com.ibm.ssl.protocol=TLSv1.2 //ssl protocol
....
```

Following steps will re-establish the communication between deployment manager and nodes.

Before running commands, {profile_root}/properties/ssl.client.props file needs to be updated so WebSphere commands uses TLSv1.2 to communicate with deployment manager

- (1) Stop the deployment manager (require updating ssl.client.props for stopManager command)
- (2) Start the deployment manager
- (3) Stop Node
- (4) Synchronize node with the deployment manager (may require updating ssl.client.props for the syncNode command)
- (5) Start Node

Stop the deployment manager and then run the syncNode command manually to propagate changes in the deployment manager to the nodes.

In order for stopManager and syncNode command to communicate with the deployment manager, the commands need to run in SP 800-131 transition mode and be using TLSv1.2.

SSL configuration for the commands is done by updating the {profile_root}/properties/ssl.client.props file.

Once the ssl.client.props file is updated, the stopManager command should be able to connect to the deployment manager and stop it. Then from each node, run syncNode manually to propagate the changes.

Now system is running at “SP 800-131” transition mode with TLSv1.2 turned on.

Enable SP 800-131 strict mode

Turn on SP 800-131 strict mode to fully comply with SP800-131 requirement. Select these options on the Manage FIPS panel and click Apply or OK.

SSL certificate and key management

SSL certificate and key management > Manage FIPS

Configures the Federal Information Processing Standard (FIPS)-compliant Java(TM) cryptography engine.

General Properties

- Disable FIPS
- Enable FIPS 140-2
- Enable SP800-131**
- Transition

Update SSL configurations to require TLS.

Update SSL configurations to require TLS and accept TLSv1.2.

Update SSL configurations to require TLSv1.2

Strict

Update SSL configurations to require TLSv1.2.

Enable Suite B: Accept 128 bit keys

Enable Suite B: Accept 192 bit keys

Apply OK Reset Cancel

22 Support for NIST SP 800-131 and NSA Suite B © 2012 IBM Corporation

Now you are ready to configure SP 800-131 strict mode. In addition to TLSv1.2, SP 800-131 requires WebSphere Application Server to use a certain set of signature algorithms and key length.

Convert certificates

If there are certificates that does not comply with SP 800-131 requirement, following message is shown. Click “Convert certificates” link to perform the conversion.

The screenshot displays the 'SSL certificate and key management' console window. At the top, a message box states: 'Could not enable FIPS Level=SP 800-131 - Strict Non-compliant certificate(s) is found.' Below this, the page title is 'SSL certificate and key management > Manage FIPS'. The description reads: 'Configures the Federal Information Processing Standard (FIPS)-compliant Java(TM) cryptography engine.' The 'General Properties' section includes radio buttons for 'Disable FIPS', 'Enable FIPS 140-2', 'Enable SP800-131', and 'Transition'. Under 'Enable SP800-131', there are sub-options for 'Transition' and 'Strict'. The 'Strict' option is selected. Below these are checkboxes for 'Update SSL configurations to require TLS', 'Update SSL configurations to require TLSv1.2', and 'Update SSL configurations to require TLSv1.2'. At the bottom of the configuration area are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'. In the 'Related Items' section, a link labeled 'Convert certificates' is highlighted with a green box.

23 Support for NIST SP 800-131 and NSA Suite B © 2012 IBM Corporation

If you try to turn on SP 800-131 strict mode, a message is displayed. This tells you that WebSphere is not currently using the signature algorithm or key size that SP 800-131 strict mode requires.

Click the “Convert certificate” link to convert the certificates.

Select signature algorithm and key size

For the security mode, available signature algorithms and key sizes are shown. Select from list box and click Apply or OK. Certificate conversion can take a while.

SSL certificate and key management

SSL certificate and key management > Manage FIPS > Convert certificates

Convert certificates that can be converted to the selected security standard. All certificates in keystores associated with an SSL configuration will be converted.

General Properties

Algorithm

Strict SHA384withECDSA

Suite B with 128 bit keys SHA256withECDSA

Suite B with 192 bit keys SHA384withECDSA

New certificate key size

384 bits

Certificates that can not be converted

The following certificates are not compliant with the specified security standard and can not be converted.

Apply OK Reset Cancel

When the required security mode is selected, in this case “Strict” for SP 800-131 strict mode, the supported signature algorithm and corresponding key size are displayed in the list box.

Select the signature algorithm and key size from the list box and click Apply or OK.

Certificate conversion will begin.

Save certificates

After successful certificate conversion, this panel opens.

Click Save to replace the certificates with the converted ones, then select "Strict" mode and click Apply or OK to enable SP 800-131 strict mode.

Messages

Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Revert changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

The server may need to be restarted for these changes to take effect.

SSL certificate and key management > Manage FIPS

Configures the Federal Information Processing Standard (FIPS)-compliant Java(TM) cryptography engine.

General Properties

Disable FIPS
 Enable FIPS 140-2
 Update SSL configurations to require TLS.
 Enable SP800-131
 Transition
 Update SSL configurations to require TLS and accept TLSv1.2.
 Update SSL configurations to require TLSv1.2
 Strict
 Update SSL configurations to require TLSv1.2.
 Enable Suite B: Accept 128 bit keys
 Enable Suite B: Accept 192 bit keys

Related Items

- Convert certificates

Apply OK Reset Cancel

25 Support for NIST SP 800-131 and NSA Suite B © 2012 IBM Corporation

When certificates are converted, a Save link is displayed. Click Save to save the converted certificates.

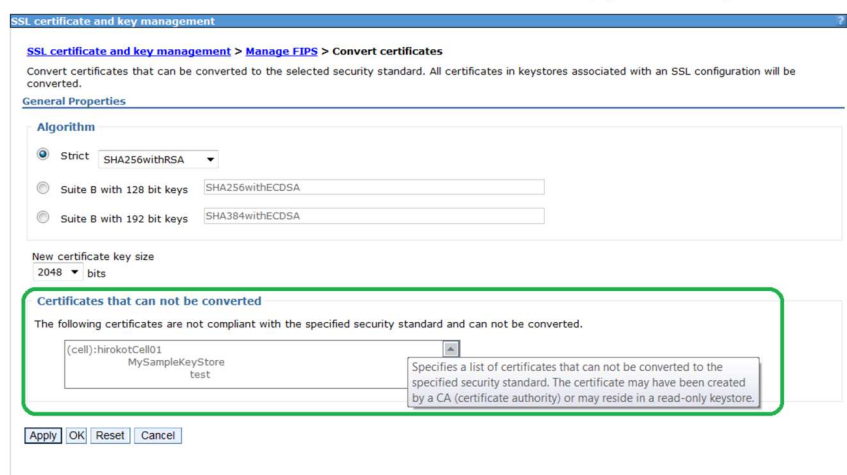
As soon as the certificates are saved, WebSphere Application Server starts using these new certificates and it might cause the communication outage similar to what was seen in previous slides.

Certificates from certificate authority

Certificates issued by certificate authority cannot be converted by this feature. Certificates in read-only keystore cannot be converted also.

These certificates will show in the box below. It is system administrator's responsibility to update these certificates to comply with SP 800-131 (see "How to replace certificate" information center link in reference section)

SP 800-131 strict mode will not be turned on until all certificates comply with the requirement.



In the Convert Certificates panel, there might be messages that show certificates that cannot be converted by WebSphere Application Server.

Due to space limitations, the administrative console does not show the reason for not being able to convert; however the `listCertificateForSecurityStandard` command and trace will display them.

The command output will require parsing certificate information. The trace output is formatted.

WebSphere Application Server is not able to convert RACF® certificates, certificates created by a Certificate Authority, or certificates in a read-only key store. However, read-only key stores can be updated from the administrative console. Go to the SSL certificate and then Key management > Key stores and certificates > {the read-only key store}, and clear the Read only check box.

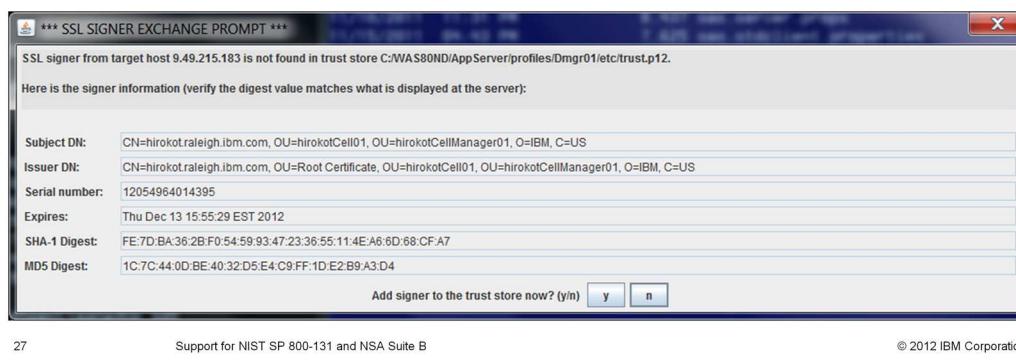
Change to SP 800-131 strict mode

After SP 800-131 strict mode is enabled, check the communication between WebSphere and other programs, just like when TLSv1.2 was turned on.

To restore communication between deployment manager and nodes, run `syncNode` manually with another update in `ssl.client.props`. Expect this prompt asking update in trust store when issuing WebSphere commands and `wsadmin` commands.

Exchanging certificates with other programs might be required in order to restore communication.

Once all the communications are found successful, the system is compliant with SP 800-131



As seen in slide 19-22, you must check communication between other programs including browser, nodes, and other programs.

It is necessary to update `ssl.client.props` again to perform `stopManager` and `syncNode` commands. Exchanging certificates is also necessary to restore communication.

The first time you run WebSphere Application Server's command or `wsadmin` script, a popup in the panel might appear for your approval to exchange signers.

Demonstration for scenario 2 and 3

This section goes through the steps of scenario 2 and 3 with screen captures.

Scenario 2 and 3 is about going from the state where no security standard is configured to SP800-131 strict (Scenario 2) , or to Suite B (Scenario 3).

In these sample steps, Dynamic SSL update is turned OFF so that you can make multiple steps all at once - including node synchronization.

After the cell restarts, the system is compliant with new security standard.

Manage FIPS panel

Manage FIPS panel is launched from:

administrative console -> Security -> ssl certificate and key management

SSL certificate and key management

SSL configurations

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

In previous versions of this product, it was necessary to manually configure each endpoint for Secure Sockets Layer (SSL). In this version, you can define a single configuration for the entire application-serving environment. This capability enables you to centrally manage secure communications. In addition, trust zones can be established in multiple node environments by overriding the default, cell-level SSL configuration.

If you have migrated a secured environment to this version using the migration utilities, the old Secure Sockets Layer (SSL) configurations are restored for the various endpoints. However, it is necessary for you to re-configure SSL to take advantage of the centralized management capability.

Configuration settings

[Manage endpoint security configurations](#)

[Manage certificate expiration](#)

[Manage FIPS](#)

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
- Certificate Authority (CA) client configurations

This slide shows how to get to new panel to configure new security standard.

Going to convert certificates panel

On Manage FIPS panel, click "Convert certificates"

Cell=hirokotCell01, Profile=Dmgr01

SSL certificate and key management

SSL certificate and key management > Manage FIPS

Configures the Federal Information Processing Standard (FIPS)-compliant Java(TM) cryptography engine.

General Properties

- Disable FIPS**
- Enable FIPS 140-2
Update SSL configurations to require TLS.
- Enable SP800-131
 - Transition
Update SSL configurations to require TLS and accept TLSv1.2.
 - Update SSL configurations to require TLSv1.2
 - Strict
Update SSL configurations to require TLSv1.2.
- Enable Suite B: Accept 128 bit keys
- Enable Suite B: Accept 192 bit keys

Related Items

- [Convert certificates](#)

30 Support for NIST SP 800-131 and NSA Suite B © 2012 IBM Corporation

Select the security mode and click Apply or OK to see if certificates are already compliant. If not, click Convert Certificates to convert certificates.

Convert certificates

Convert certificates according to the required FIPS mode.

Cell=hirokotCell01, Profile=Dmgrp01

SSL certificate and key management

SSL certificate and key management > Manage FIPS > Convert certificates

Convert certificates that can be converted to the selected security standard. All certificates in keystores associated with an SSL configuration will be converted.

General Properties

Algorithm

Strict SHA256withRSA *Select this option and choose signature algorithm and keysize for certificates to comply with SP 800-131*

Suite B with 128 bit keys SHA256withECDSA *Select one of these options to comply with Suite B. Signature algorithm and key size are determined according to the Suite B mode (128 bit or 192 bit)*

Suite B with 192 bit keys SHA384withECDSA

New certificate key size
256 bits

Certificates that can not be converted

The following certificates are not compliant with the specified security standard and can not be converted.

31

Support for NIST SP 800-131 and NSA Suite B

© 2012 IBM Corporation

Select your security mode if it is not already selected. The supported signature algorithm and corresponding key size are displayed.

Select the signature algorithm and key size and click Apply or OK, and certificate conversion will begin.

Enable FIPS mode

After converting certificates, the panel comes back to Manage FIPS panel. Enable required FIPS mode.

Cell=hirokotCell01, Profile=Dmgr01

SSL certificate and key management

SSL certificate and key management > Manage FIPS
Configures the Federal Information Processing Standard (FIPS)-compliant Java(TM) cryptography engine.

General Properties

Disable FIPS

Enable FIPS 140-2

Update SSL configurations to require TLS.

Enable SP800-131

Transition

Update SSL configurations to require TLS and accept TLSv1.2.

Update SSL configurations to require TLSv1.2

Strict

Update SSL configurations to require TLSv1.2.

Related Items

[Convert certificates](#)

Enable Suite B: Accept 128 bit keys

Enable Suite B: Accept 192 bit keys

Apply OK Reset Cancel

32 Support for NIST SP 800-131 and NSA Suite B © 2012 IBM Corporation

Select Strict mode to comply with SP 800-131

Select one of these Suite B option according to the choice of certificate conversion.

Once the certificates are converted, save the changes to the configuration and then enable the required security mode.

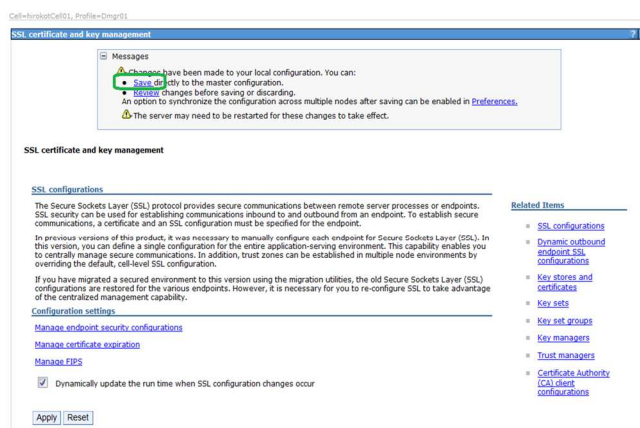
Save the configuration and propagate

Once FIPS mode is saved, propagate the change to the nodes by doing manual sync nodes.

Restart the deployment manager and all the nodes and servers in the cell.

Make sure other programs such as browser, LDAP, and other programs communicates using TLSv1.2 and newly converted certificates.

Update ssl.client.props to communicate with nodes. Now the system is compliant with the required FIPS level.



Save the configuration in the deployment manager and propagate the change by running the syncNode command manually.

The administrative console might still be able to synchronize nodes when dynamic SSL update is disabled. You can take advantage of this instead of using the syncNode command manually.

After restarting the cell, the new security mode is in effect. Ensure that communication with other programs is successful. Also you will need to update the ssl.client.props file.

Properties in `ssl.client.props`

Following table shows the properties to configure in `{profile_root}/properties/ssl.client.props` for each FIPS mode.

| FIPS Security mode | Properties to add to <code>ssl.client.props</code> |
|--|---|
| FIPS not enabled | <pre>com.ibm.security.useFIPS=false #Do not define - com.ibm.websphere.security.FIPSLevel= #Do not define - com.ibm.websphere.security.suitesb= com.ibm.ssl.protocol=(what is configured)</pre> |
| FIPS140-2 | <pre>com.ibm.security.useFIPS=true com.ibm.ssl.protocol=SSL_TLS</pre> |
| <i>SP800-131 transition (no TLSv1.2)</i> | <pre>com.ibm.security.useFIPS=true com.ibm.websphere.security.FIPSLevel=transition #Do not define - com.ibm.websphere.security.suitesb= com.ibm.ssl.protocol=SSL_TLS</pre> |
| <i>SP800-131 transition with TLSv1.2</i> | <pre>com.ibm.security.useFIPS=true com.ibm.websphere.security.FIPSLevel=transition #com.ibm.websphere.security.suitesb= com.ibm.ssl.protocol=TLSv1.2</pre> |
| <i>SP800-131 strict</i> | <pre>com.ibm.security.useFIPS=true com.ibm.websphere.security.FIPSLevel=SP800-131 #Do not define - com.ibm.websphere.security.suitesb= com.ibm.ssl.protocol=TLSv1.2</pre> |
| <i>Suite B 128</i> | <pre>com.ibm.security.useFIPS=true #Do not define - com.ibm.websphere.security.FIPSLevel= com.ibm.websphere.security.suitesb=128 com.ibm.ssl.protocol=TLSv1.2</pre> |
| <i>Suite B 192</i> | <pre>com.ibm.security.useFIPS=true #Do not define -- com.ibm.websphere.security.FIPSLevel= com.ibm.websphere.security.suitesb=192 com.ibm.ssl.protocol=TLSv1.2</pre> |

This slide shows required properties in `{profile_root}/properties/ssl.client.props` file for each security mode.

wsadmin commands

Newly introduced commands for this feature :

FIPSCommands command group

- enableFips
- getFipsInfo
- listCertStatusForSecurityStandard
- convertCertForSecurityStandard

KeyStoreCommand group

- listSignatureAlgorithms

SSLConfigCommand group

- listSSLProtocolTypes

Updated commands with -signatureAlgorithm parameter (optional parameter)

PersonalCertificateCommands group

- createSelfSignedCertificate

CertificateRequestCommads group

- createCertificateRequest

Output from listCertificateStatusForSecurityStandard and convertCerForSecurityStandard will require parsing each certificate's information. For more information, see the information center command reference.

References – Security standards

- FIPS Publications on National Institute of Standards and Technology (NIST)
 - <http://csrc.nist.gov/publications/PubsFIPS.html>
- SP800-131a
 - <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>
- National Security Agency - NSA Suite B Cryptography
 - http://www.nsa.gov/ia/programs/suiteb_cryptography/
- Suite B
 - <http://tools.ietf.org/rfc/rfc6460.txt>

This slide shows links to security standards.

References – Information center links

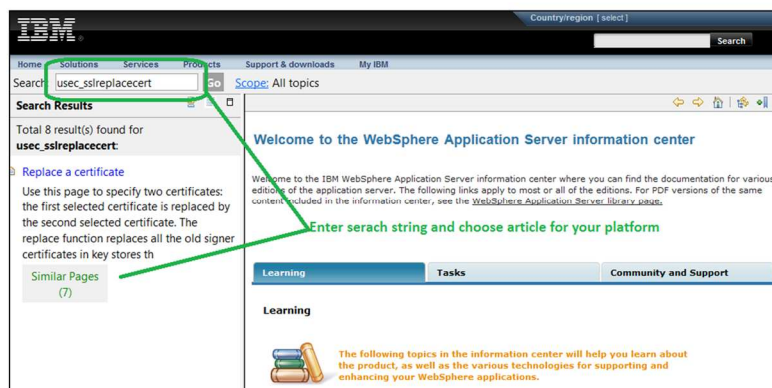
Information center V7 page

- <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>

Information center V8 page

- <http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp>

See the next slides for keywords that take you to related articles.



This slide shows links to the information centers.



Information center keywords for security standards

| Information center article | Search keyword |
|--|-------------------------|
| Configuring Federal Information Processing Standard Java Secure Socket Extension files | tsec_fips |
| Configuring WebSphere Application Server for SP800-131 standard strict mode | tsec_config_strictsp300 |
| Transitioning WebSphere Application Server to the SP800-131 security standard | tsec_transition_sp300 |
| WebSphere Application Server security standards configurations | csec_security_standards |
| Configuring WebSphere Application Server for the Suite B security standard | tsec_config_suiteb |

To search the information center for security standards, use these keywords.

Information center keywords for general information

| Information center article | Search keyword |
|---|-------------------------|
| SSL configurations | csec_sslconfigs |
| Creating a Secure Sockets Layer configuration | tsec_sslconfiguration |
| ssl.client.props client configuration file | rsec_sslclientpropsfile |
| Replace a certificate | usec_sslreplacecert |

To search the information center for general security information, use these keywords.



Information center keywords for related commands

| Information center article | Search keyword |
|--|---------------------|
| PersonalCertificateCommands command group for the AdminTask object | rxml_atpersonalcert |
| CertificateRequestCommands command group of the AdminTask object | rxml_atcertrequests |
| KeyStoreCommands command group for the AdminTask object | rxml_atkeystore |
| SSLConfigCommands command group | rxml_atsslconfig |
| FIPS Commands command group | rxml_fipscommands |

To search the information center for related commands, use these keywords.

References - 3

- Java Secure Socket Extension (JSSE) IBMJSSE2 Provider Reference Guide for the IBM Virtual Machine for Java Platforms
<http://www.ibm.com/developerworks/java/jdk/security/60/secguides/jsse2Docs/JSSE2RefGuide.html>
- JDK policy files
<http://www.ibm.com/developerworks/java/jdk/security/index.html>
- URL for browser

Internet Explorer: SSL protocols configuration steps and supported version:
<http://technet.microsoft.com/en-us/library/dd560644%28WS.10%29.aspx>

Firefox: TLS support discussion
<http://forums.mozillazine.org/viewtopic.php?f=7&t=1831235>

This slide links to JDK and browser information.



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_WASV8003_SecurityCryptoSignatureAlgorithm.ppt

This module is also available in PDF format at: [../WASV8003_SecurityCryptoSignatureAlgorithm.pdf](..\\WASV8003_SecurityCryptoSignatureAlgorithm.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, RACF, 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](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
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.

© Copyright International Business Machines Corporation 2012. All rights reserved.