Sterling B2B Integrator

Using Sterling B2B Integrator with National Institute of Standards and Technology (NIST) 800-131a Security Compliance

Version 5.2.4.2

Sterling B2B Integrator

Using Sterling B2B Integrator with National Institute of Standards and Technology (NIST) 800-131a Security Compliance

Version 5.2.4.2

Note

Before using this information and the product it supports, read the information in "Notices" on page 19.

Copyright

This edition applies to Version 5 Release 2 Modification 4 Fix Pack 2 of Sterling B2B Integrator and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

National Institute of Standards and Technology (NIST) security compliance (5.2.4.2 or higher)

To conform to the security requirements for the National Institute of Standards and Technology (NIST) standards as specified in the publication 800-131a, applications must use strengthened security by defining specific algorithms that can be used and what their minimum strengths are.

These standards specify the cryptographic algorithms and key lengths that are required in order to remain compliant with NIST security standards. For more information on NIST security standards, see *http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf*.

Algorithms and key strengths that are not allowed for strict NIST 800-131a compliance include::

- RSA keySize < 2048
- DSA keySize < 2048
- EC keySize < 224
- SHA1
- SHA-1
- MD2
- MD4
- MD5
- RC2
- RC4
- DES

Note: In strict NIST 800-131a compliance mode, only TLS 1.2 can be used for SSL and TLS.

NIST 800-131a compliance with Sterling B2B Integrator

Sterling B2B Integrator works in two security compliance modes:

- Non-NIST 800-131a compliance (default)
- Strict NIST 800-131a compliance

The following applies to all adapters, services and components when working in NIST 800-131a compliance mode:

- If an adapter, service, or component is configured with non-NIST 800-131a compliant information, the configuration summary page for that component will indicate non-NIST compliance. To maintain compliance, you must re-configure the adapter, service, or component with NIST 800-131a compliance information.
- When you re-configure an adapter, service, or component it forces the usage of NIST 800-131a compliance information; therefore, any non-NIST 800-131a compliance information will not be available.
- If an adapter or service is configured with non-NIST 800-131a compliance information, it is disabled; you can not restart it without reconfiguration with information that supports NIST 800-131a compliance.

For more information about NIST 800-131a compliance, please see *http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf*.

Enable NIST 800-131a compliance mode

About this task

Property files contain properties that control the operation of Sterling B2B Integrator. To enable NIST 800-131a compliance mode, you must modify the values of these properties. For more information about changing property files, see *Working with Property Files* documentation for general information about how to work with Property Files.

Procedure

1. Stop the system.
2. For UNIX, navigate to */install_dir/properties/security.properties* directory. For Windows, navigate to \install_dir\properties\security.properties directory.
3. Edit the following parameter in the properties file: **`NIST.800-131a=strict`**
4. Save and exit the file.
5. Start the system.

Disable NIST 800-131a compliance mode

About this task

Property files contain properties that control the operation of Sterling B2B Integrator. To disable NIST 800-131a compliance mode, you must modify the values of these properties. For more information about changing property files, see *Working with Property Files* documentation for general information about how to work with Property Files.

Procedure

1. Stop the system.
2. For UNIX, navigate to */install_dir/properties/security.properties* directory. For Windows, navigate to \install_dir\properties\security.properties directory.
3. Edit the parameter in the property file: **`NIST.800-131a=off`**
4. Save and exit the file.
5. Start the system.

Verifying NIST 800-131a compliance with digital certificates

Sterling B2B Integrator contains seven system certificates: OpsDrv, OpsKey, B2BHttp, UIKey, ASISslCert, DefDBCrypt, and doccrypto. All seven RSA certificates have been upgraded from 1024 key strength and SHA1withRSA signature algorithm to 2048 key strength and SHA256withRSA signature algorithm with exception to doccrypto; a new certificate named doccrypto2 with 2048 key strength and SHA256withRSA signature algorithm was added for NIST 800-131a compliance in strict mode and deployed with Sterling B2B Integrator, version 5.2.4.2. All the new documents in the system will be encrypted with these new certificates after NIST 800-131a patch upgrade.

About this task

To ensure you have the correct encryption for your selected certificate to ensure NIST 800-131a compliance, you can verify that the correct certificate was used by locating the key strength of the certificate.

Procedure

1. From the Trading Partner menu, select Digital Certificates > System > List All. A list of System Certificates is displayed.
2. Locate and select the certificate name you want to review. The Certificate Summary displays a detailed list of the certificate properties.
3. Locate the Public Key Length. To ensure NIST 800-131a compliance in strict mode, the Public Key Length is: 2048; if the Public Key Length indicates 1024 for strict mode and an old certificate is being used, the certificate needs to be updated or no longer used.
4. If the certificate is non-NIST compliant, when selected, the following message appears, *Not NIST 800-131a compliant*.

Disabled Adapters in NIST 800-131a compliance mode

An Adapter will be disabled as a result of NIST 800-131a compliance when adapters are configured in "off" mode using noncompliant data, such as noncompliant certificates and cipher strength, and are switched to strict mode.

If a non-NIST 800-131a compliant system certificate, CA certificate, or cipher strength are used when in strict mode, the server adapter is disabled and messages are logged into the log file for the adapter. You must re-configure the non-NIST 800-131a compliant adapter by using a NIST 800-131a compliance certificate and cipher strength to enable the adapter.

If an adapter is disabled as a result of non-NIST 800-131a compliant certificate or cipher strength, a message appears on the Adapter details page, *Not NIST 800-131a compliant*. If you receive an error, you must re-configure the adapter for NIST 800-131a compliance.

Client Adapters

If a client adapter is configured with a non-NIST 800-131a compliance system certificate, trusted certificate, CA certificate, or cipher strength in strict mode, the communication with the server will fail. If you receive a failure, you must re-configure the client adapter for NIST 800-131a compliance.

Re-configure components for NIST 800-131a compliance

If an error appears because a certificate or cipher strength utilized is not strong enough for NIST 800-131a compliance, you will need to re-configure it.

For example, if you are using certificates, you can replace the old, non-NIST 800-131a compliance certificate with a NIST 800-131a compliance certificate by navigating to the area of the system where the certificate is configured for that system component.

Once you re-configure the component with the new certificate or NIST 800-131a compliance information, the adapter, service or system component will be re-enabled.

Using adapters with SSL in NIST 800-131a compliance mode

For adapters using SSL, only Strong cipher strength is an available selection during configuration. When running in NIST 800-131a strict mode, these cipher suites are supported:

SSL_RSA_WITH_AES_128_CBC_SHA256

SSL_RSA_WITH_AES_256_CBC_SHA256

NIST 800-131a compliant cipher suites

Only NIST 800-131a compliant cipher suites are used when running in NIST 800-131a compliance mode. Strong cipher suites can also be configured in off mode; however, only strong cipher suites can be used in strict mode.

Use the parameter NISTCompliantCipherSuite in security.properties to view a list of NIST 800-131a compliant cipher suites.

Note: Do not modify the NISTCompliantCipherSuite entry.

Client adapters with SSL

If a client adapter is configured with a non-NIST 800-131a compliant system certificate, CA certificate, or cipher strength in strict mode, the communication to the server will fail.

If you receive an error, you must re-configure the adapter for NIST 800-131a compliance.

TLS Version

In strict mode, the parameter SSLHelloProtocolForNISTStrict in security.properties controls TLS versions used. It is set to TLS1.2-ONLY. If you are using NIST 800-131a strict compliance, you should not change this value.

If NIST 800-131a is off, the parameter *SSLHelloProtocol=TLS1-TLS1.2* in security.properties controls TLS versions used and is set to TLS1.0, TLS1.1, and TLS1.2.

If you use TLS 1.2 in communication with your trading partner and client authentication for SSL is specified, the key length of the certificate used for client authentication must be at least 1024; otherwise, you will get “intended enc. msg. too short” error during the beginning of an SSL session with your trading partner. In this case, you have to upgrade certificate with the key length at least 1024.

TLS 1.2 is supported in Sterling B2B Integrator default mode, when not in NIST 800-131a compliance mode.

Mail Servers not supporting TLS 1.2

SMTP and B2B mail client adapters use the mail server for communication. If you are using a mail server that does not support TLS 1.2, when you run in NIST 800-131a strict mode, all the communications over SSL with this mail server will fail with a handshake error.

Import and export certificate considerations

Import

When using Sterling B2B Integrator in strict mode, non-NIST 800-131a compliance certificates are not imported into the system, even when using a command line script, import.sh.

When a non-NIST 800-131a compliance certificate is used, the import report will indicate that a failure occurred with the non-NIST 800-131a compliance certificate listed.

If you are using the Sterling B2B Integrator user interface to import a non-NIST 800.131a compliant certificate, an error message appears indicating that the certificate is not compliant.

Export

You can export all certificates regardless of NIST 800-131a compliance.

System certificates with 2048 key strength for NIST 800-131a compliance

Sterling B2B Integrator includes updated certificates from 1024 key strength and SHA1withRSA signature algorithm to 2048 key strength and SHA256withRSA signature algorithm for these system certificates:

- OpsDrv
- OpsKey
- B2BHttp
- UIKey
- ASISsICert
- DEfDBCrypt
- doccrypto2

  Note:
  doccrypto2 is an updated name for NIST 800-131a compliance. doccrypto will remain in the system to allow decryption of legacy documents that are encrypted by it; however, any new documents encrypted with this new certificate after the patch upgrade will be decrypted with doccrypto2.

SHA256 is supported in Sterling B2B Integrator default mode, when not in NIST 800-131a compliance mode.

Certificate Validation in Auth Chain for NIST 800-131a compliance mode

If you are running Sterling B2B Integrator in NIST 800-131a strict mode and if any certificate has the *Auth Chain* flag enabled, then all certificates in its chain (root certificates) must be NIST 800-131a compliant for successful validation.

If one or more certificates in the auth chain are not NIST 800-131a compliant, an error message appears on the summary page of the certificate indicating they are not NIST 800-131a compliant and you will be unable to use this certificate in NIST 800-131a compliance mode.

Note: The *Auth Chain* flag should not be enabled for self-signed certificates.

Using Web Services in NIST 800-131a compliance mode

To accommodate for NIST 800-131a compliance, SHA256withRSA was added to the SigningAlgorithm list.

Web Services uses SOAOutboundSecurityService and SOAInboundSecurityService to sign, encrypt, decrypt, and verify signature over an HTTP or HTTPS. If you are using NIST 800-131a compliance when you configure these services over HTTP or HTTPS, only NIST 800-131a compliant certificates are available for selection.

If a non-NIST 800-131a compliant certificate, signature, or algorithm is used for SOAOutboundSecurityService or SOAInboundSecurityService, the business process fails, indicating in the status report that the *Encryption certificate is not NIST compliant*. If you receive an error, you must re-configure for NIST 800-131a compliance.

Note:
When indicating the **KeyEncodingAlgorithm** on the ResponseSecurityEncryption Settings page, use **RSAOEP.**

Using ebXML in NIST 800-131a compliance mode

When you are in strict mode, the following changes need to be made to the Collaboration Protocol Agreement (CPA) to maintain a successful transaction:

- Verify that all certificates using the ebxml transaction are NIST 800-131a compliant. To verify compliance, refer to Verifying NIST 800-131a Compliance with Digital Certificates.
- Change the tp:HasFunction from: http://www.w3.org/2000/09/xmldsig#sha1 to http://www.w3.org/2001/04/xmlenc#sha256
- Change the tp:SignatureAlgorithm from: http://www.w3.org/2000/09/xmldsig#rsa-sha1 to http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
- If the ebxml transaction uses a server adapter with SSL, that adapter must be configured with a NIST 800-131a compliant certificate and other applicable security details.

  Note: The signing algorithm dsa-sha256 is not supported..

Using SFTP in NIST 800-131a compliance mode

Using Secure File Transfer Protocol (SFTP) ensures that data is transferred securely using a private and safe data stream. SFTP is the standard data transmission protocol for using with SSH2 protocol.

Before establishing a connection, the SFTP server sends an encrypted fingerprint of its public host keys to ensure that the SFTP connection will be exchanging data with the correct server. When the connection is first established, the key is not yet known to the client program and must be confirmed by the user before data is exchanged. Upon connection to an SFTP server and verification that the correct server is being used, the fingerprint information should be saved locally. This allows you to check the fingerprint information against the data you save when you establish a new connection and ensures that no one is between you and the server. Different servers issue fingerprints only once and they are generated by a server's private key. As per the NIST 800-131a SP 800-131a standards, Sterling B2B Integrator supports a certain key length in the different security modes.

As part of the SFTP Client NIST 800-131a compliance, a validation occurs at the SFTP Client Begin session level for any security-related configurable parameter for NIST 800-131a restrictions. If a non-compliant parameter is found, the communication fails and an error is logged in the SFTP client as well as the process status about the non-NIST 800-131a compliance.

Compliance is validated for these areas:

- Ciphers
- Macs
- Known host keys
- User Identity keys

You can use these key lengths for NIST 800-131a mode to establish client-server communication:

Table 1.

Key Length	NIST 800-131a Compliant
SSH1-RSA	768, 1024, 1536 (Non-compliant), 2048 (Strict)
SSH2-DSA	768, 1024, 1536 (Non-compliant), 2048 (Strict)
SSH2-RSA	768, 1024, 1536 (Non-compliant), 2048 (Strict)

If you are running in NIST 800-131a compliance mode and your SFTP server adapters are configured in noncompliant mode, you can view the Advanced State from the Services Configuration page. A state of Start failed appears and the Adapter will be disabled.

SFTP Client GPM

If you are running in NIST 800-131a compliance mode, the SFTP Begin Session Service configuration in the GPM shows only the values that are compliant with NIST 800-131a strict mode.

SSH Remote Profile

The SFTP Client Begin session can be configured using the Profile Id for the SSH Remote profile. This configuration maintains all the information about the remote server that the client can use for connection. If running in NIST 800-131a compliance mode, only compliant information is available during the profile configuration and existing profiles configured with non-compliant information are highlighted in red with a message *Not NIST SP800-131a compliant*.

Known Host Key

All keys must match the NIST SP 800-131a standard. Only the compliant keys are enabled for SSH Known Host Key. All others are disabled.

If a non-compliant key is attempted to be checked in, an error occurs indicating that the key is NOT NIST SP800-131a compliant, check in fails, and a message is logged in the ui.log file. Only keys that are compliant to the NIST SP 800-131a standard can be used when running in NIST 800-131a strict or compliance modes.

If a non-compliant key is attempted to be enabled, an error occurs and this message appears: *Unable to enable the selected key. Not NIST SP800-131a compliant*.

If a Fetch Key is attempted and the key(s) do not meet the NIST 800-131a standard, check-in fails.

Authorized User Key

If noncompliant keys are attempted to be checked-in, check-in fails and the non-compliant key is disabled.

User Identity Key

During key creation, only compliant keys are listed. All other keys at check-in are not allowed.

Host Identity Key

Key length is restricted to NIST 800-131a mode for key creation and only NIST 800-131a compliant keys are shown as enabled. All other keys at check-in are not allowed.

If a non-compliant key is attempted to be enabled, an error occurs and this message appears, *Not NIST SP800-131a compliant*.

Client and Server Communication

When the client and server communicate to negotiate the ciphers and macs, only NIST 800-131a compliant ciphers and macs are used for NIST 800-131a compliance mode.

Limitation of Third Party Communications When in Strict Mode for SFTP

For Sterling B2B Integrator versions 05020402 and higher, public and private SSH keys generated by Sterling B2B Integrator have Q values of 256 bits. This is the default behavior and it impacts some communications when utilized with 2048-bit DSA keys. When using Sterling B2B Integrator to Sterling B2B Integrator SFTP communication, there is no impact. When using Sterling B2B Integrator with Third Party communications with DSA keys, there is no impact for the keys generated externally since they have Q values of 160 bits; however, if the keys are generated through Sterling B2B Integrator, it may impact communication where the Third Party application is not able to process DSA keys with Q values of 256 bits. In this case, communication fails for the client or server at the key verification step with a failure to process 2048 DSA keys. To resolve this issue, you can create keys with an external tool, such as PuttyGen to create 2048 DSA keys that have a Q value of 160 bits.

Using FTP in NIST 800-131a compliance mode

During the configuration of adapters for System and CA certificates with SSL, only NIST 800-131a compliant certificates are available.

Also, during configuration for adapters with SSL, only Strong Cipher strength is compliant when running in strict mode. A list of strong Cipher suites are defined in the property NIST 800-131aCompliantCipherSuite in security.properties.

Non-compliant FTP Adapters

If a non-compliant system certificate, CA certificate, or cipher strength are used, the server adapter is disabled and a message is logged. You must re-configure the adapter using a NIST 800-131a compliant certificate and cipher strength to enable the adapter. View the adapter settings to review the potential violations; if it is non-compliant, a message, *Not NIST SP800-131a compliant* appears. If you receive an error, you must re-configure for NIST 800-131a compliance.

Using MSMQ in NIST 800-131a compliance mode

NIST 800-131a strict compliance modes are not compatible with MSMQ server versions 1.0, 2.0, and 3.0. If you are using one of these server versions, you will need to upgrade for NIST 800-131a compliance.

The MSMQ Adapter and MSMQ Send Service support two encryption althorithms:

- CALG_RC2 (default) - Non-compliant
- CALG_RC4 - Non-compliant

If you are using MSMQ Server 4.0 or MSMQ server 5.0, you can use CALG_AES to support AES encryption for NIST 800-131a compliance.

Privacy level for encryption

These privacy levels are used to request encryption:

- Non (default); non-compliant
- Base (40-bit); non-compliant
- Enhanced (128-bit, supported in MSMQ version 2.0 and later); compliant

GPM Configuration for MSMQ Adapter

When running in NIST 800-131a strict mode, the only values that appear for encryption parameters are those that are compliant with NIST 800-131a strict mode.

Communication Failures

When the MWMQ adapter communicates with non-compliant parameters in NIST 800-131a mode, the communication fails and the failure message is logged. If you receive an error, you must re-configure for NIST 800-131a compliance.

Using AS1 in NIST 800-131a compliance mode

SHA256 signing algorithm was added to AS1 configuration to support NIST 800-131a compliance. When configuring an AS1 trading partner, only NIST 800-131a compliant certificates are used.

If a certificate with non-NIST 800-131a compliance exists in the system prior to upgrading to NIST 800-131a mode, the following message appears, *Not NIST SP800-131a compliant*. You must create a new NIST 800-131a compliant certificate and re-configure AS1 to use the new certificate.

If a non-NIST 800-131a compliance certificate, signature, or algorithm is used, the business process will fail, indicating in the status report that the certificate is *Not NIST SP800-131a compliant*.

Using AS2 in NIST 800-131a compliance mode

SHA256, SHA318, and SHA512 signing algorithms are added to AS2 configuration for signing messages and MDN's to support NIST 800-131a compliance. When configuring an AS2 trading partner, or organization profiles, only NIST 800-131a compliant certificates/algorithms are available for use. If you receive an error, you must go back to the configuration page and re-configure for NIST 800-131a compliance.

If a certificate with non-NIST 800-131a compliance exists in the system prior to upgrading to NIST 800-131a mode, the following message appears, *Not NIST SP800-131a compliant.* You must create a new NIST 800-131a compliant certificate and re-configure AS2 to use the new certificate.

If a non-NIST 800-131a compliance certificate, signature, or algorithm is used, the business process will fail, indicating in the status report that the certificate is *Not NIST SP800-131a compliant*.

Using AS3 in NIST 800-131a compliance mode

SHA2 SHA256, SHA384, and SHA512 signing algorithms are added to AS3 configuration for signing messages and MDN's to support NIST 800-131a compliance.

If a certificate with non-NIST 800-131a compliance exists in the system prior to upgrading to NIST 800-131a mode, the following message appears, *Not NIST SP800-131a compliant*. You must create a new NIST 800-131a compliant certificate and re-configure AS3 to use the new certificate.

If a non-NIST 800-131a compliant certificate, signature, or algorithm is used, the business process will fail, indicating in the status report that the certificate is *Not NIST SP800-131a compliant*.

Using OCSP in NIST 800-131a compliance mode

The Online Certificate Status Protocol (OCSP) is a set of ASN.1 defined data structures for requesting and receiving information about certificate revocation status. These data structures can be sent and received by many transport protocols. If HTTP is used and an OCSP client sends questions and processes responses, the OCSP responder answers questions and generates responses. For NIST 800-131a compliance, only a NIST 800-131a compliant certificate can be used for creating an OCSP request. If a non-compliant certificate is used, the communication fails and no OCSP request is created.

Using EBICS client in NIST 800-131a compliance mode

An EBICS Client non-technical user can be configured with X509 certificates and RSA keys to support NIST 800-131a compliance for signature, encryption, and authentication. Only NIST 800-131a compliant certificates and signing algorithms are available when running with NIST 800-131a compliance enabled.

If only signing is required, a Hardware Security Module can be used in place of X509 certificates and RSA keys; however, only NIST 800-131a compliant certificates can be used. RSA keys must be located or uploaded to the keyfile from the local filesystem. If the selected key is not NIST 800-131a compliant in the selected mode, the process will error. If you receive an error, you must go back to the configuration page and re-configure for NIST 800-131a compliance and only NIST 800-131a compliance certificates and signing algorithms are available when running with NIST 800-131a compliance enabled.

If running in NIST 800-131a compliance mode, only CA certificates that are NIST 800-131a compliant are available on the Bank Configuration page for TLS.

RSA Keys

When an RSA key is retrieved, it is validated for NIST 800-131a compliance based on the selected compliance mode, if it is non-compliant, an error is logged.

Signatures

The signature processes will error out when the keys being used for signature calculation are non-compliant.

Import and Export

SCI_TRUSTED_CERTS and SCI_CA_CERTS are internally imported as part of HOST import dependencies. SCI_PRIVATE_KEY_CERTS and SCI_TRUSTED_CERTS are internally imported as part of USER import dependencies. NIST 800-131a 800-131a compliance imports these dependencies. A USER / HOST can also use RSA keys instead of X509 certificates. If running in NIST 800-131a strict mode, the import report will indicate failures for those USERs / HOSTs with keys where keylengths are not NIST 800-131a compliant.

SCI_TRUSTED_CERTS and SCI_CA_CERTS are exported as part of HOST export. SCI_PRIVATE_KEY_CERTS and SCI_TRUSTED_CERTS export as part of USER export. A USER / HOST can use RSA keys instead of X509 certificates. If the system is running in NIST 800-131a strict mode, export will throw this error to indicate the noncompliance of the RSA keys: *Not NIST 800-130a Compliant*. The keys can still be exported.

HSM Signature (3S Key)

For signing, a Hardware Security Module can be used in place of system certificates and RSA keys; however, only NIST 800-131a compliant certificates can be used.

Using EBICS server in NIST 800-131a compliance mode

The cryptographic functions in EBICS Server including digital signature, encryption, and XML signature are all supported algorithms that are NIST 800-131a compliant.

Only NIST 800-131a compliant certificates, encryption, and signing algorithms are available when running with NIST 800-131a compliance enabled.

Using Connect:Direct in NIST 800-131a compliance mode

The Connect:Dircect Protocol is a session oriented protocol supporting file transfer for remote (business) process execution and submission. Sessions may be secured using Secure+ server (and optional client) authentication and data encryption. Security may be enforced globally by requiring all sessions to use the same security definition. To do this, disable Netmap Node Override to configure one policy for all sessions. Security may also be enforced individually according to specific trading partner requirements. Enable Netmap Node Override to allow different policies for each trading partner.

The Admin User Interface makes available only NIST 800-131a compliant certificates and ciphers when Sterling B2B Integrator is operating in NIST 800-131a compliance mode.

Verifying NIST 800-131a Compliance

There are two ways to verify NIST 800-131a compliance:

- Verify that all adapters are started successfully and are enabled.
- Verify that the business process session status is error free.

Verify Adapters

The Services Configuration page displays an adapter's Advanced State. If Sterling B2B Integrator is running in NIST 800-131a compliant mode and your Connect:Direct Server Adapters is configured in non-compliant mode, the Advanced State will display Start failed and the adapter will be disabled. For additional detail, select the link corresponding to the adapter to view its configuration.

All non-compliant service settings appear with an error in red, NIST 800-131a SP800-131a compliant

The following table illustrates the Connect:Direct Server Adapter's enablement policy with respect to the NIST 800-131a compliance mode used with Sterling B2B Integrator.

Table 2. Connect:Direct Server Adapter Enablement Policy

Connect:Direct Server Adapter Enablement Policy			
Configuration		**Sterling B2B Integrator Security Policy**	
		None	Strict
Global: Adapter defines the security policy for all sessions		Adapter enabled and all sessions allowed.	Adapter is enabled only if the Adapter's configuration meet strict-level site policy.
Local: Individual Nodes define a node-specific security policy for their respective sessions.	Every Node in the Adapter's netmap specifies a secure policy	Adapter enabled and all sessions allowed.	Adapter is Enabled only if every Node's Secure+ configuration meets strict-level site policy.
	At least 1 Node in the Adapter's netmap does not specify a secure policy.	Adapter enabled and all sessions allowed.	Adapter is Enabled. Session only allowed if Node's Secure+ configuration meets strict-level site policy.

Verify Business Processes

The Connect:Direct Begin Session Service Status Report displays service status. If Sterling B2B Integrator is running in NIST 800-131a compliance mode and either your Connect:Direct Server Adapter or the remote node in the adapter's netmap is configured in noncompliant mode, the Begin Session will fail and its Status Report will display "*Secure+ configuration is incompatible with the site security policy.*"

Using PGP in NIST 800-131a compliance mode

Only NIST 800-131a compliant ciphers are used when configuring a PGP Sponsor manager. If a non-NIST 800-131a compliant cipher is used, the system will indicate the noncompliance: *Not NIST 800-130a compliant*. If a non NIST 800-131a compliance cipher algorithm is used during runtime, the business process will fail, indicating in the status report that the algorithm is *Not NIST 800-130a compliant*.

If you receive an error, you must re-configure for NIST 800-131a compliance.

Using MQFTE in NIST 800-131a compliance mode

Sterling B2B Integrator can be configured to transfer files in and out of WebSphere MQ File Transfer Edition Network using WMQFTE AgentAdapter and WMQFTE CreatTransferService.

Sterling File Gateway can also be integrated with Websphere MQFTE network with the configuration in File Gateway.

When performing Services configuration for MQFTE for NIST 800-131A compliance, only the ciphers that are NIST 800-131a compliant are available to select on the configuration page.

Note: Only TLS 1.2 is supported for NIST 800-131a compliance in strict mode. TLS level used is tied to the selected Cipher Suite and since there is no Cipher Suite to support TLS 1.2, it is not supported for NIST 800-131a compliance.

Before saving the configuration of your MQFTE adapter or MQFTE transfer service, verify that the certificate used in Key Store or SSL Cipher is NIST 800-131a compliant. If it is not compliant, a message appears, "*Not NIST SP800-131a compliant*" appears behind the non-compliant information.

If configured MQFTE adapter is non-NIST 800-131a compliant, the adapter is disabled.

If the configured MQFTE service is non-NIST 800-131a compliant, the service is disabled.

During runtime, the Cipher used in the MQFTE adapter and the MQFTE transfer service is verified for NIST 800-131a compliance. The Trust Store and the Key Store used for communicating the MQFTE network and FTP server are verified as well. If any certificate in the store is not NIST 800-131a compliant, the runtime will locate the non-compliance and the MQFTE agent adapter will fail to start and the MQFTE create transfer will fail.

Using SFG in NIST 800-131a compliance mode

During the configuration of a consumer partner, only encryption strength and CA certificates that are NIST 800-131a compliant are available.

Only SSH Remote Profiles that are NIST 800-131a compliant are available.

On the FTPS Settings page, the Encryption strength has all options (STRONG, WEAK, and ALL) if NIST mode is turned off; however, if NIST mode is turned on, only STRONG is an available selection.

If the SSH Remote Profile is not NIST compliant, a message is displayed to indicate it is Not NIST SP800-131a compliant. If you receive an error, you must re-configure for NIST 800-131a compliance.

Using RosettaNet in NIST 800-131a compliance mode

If an identity or trading partner for RosettaNet is configured with non-NIST 800-131a compliant information, an error appears to indicate that it is *Not NIST SP800-131a compliant*. If you receive an error, you must re-configure for NIST 800-131a compliance.

SHA256 signing algorithm has been added for signing messages to support NIST 800-131a compliance.

Using CLA2 in NIST 800-131a compliance mode

CLA2 supports NIST 800-131a compliance when used in compliance for NIST 800-131a mode.

Sterling B2B Integrator V5.2.4, interim fix 2 considerations

- When installing Sterling B2B Integrator V5.2.4, interim fix 2, new certificates are created to support CLA2 for NIST 800-131a compliance.
- If you are upgrading from Sterling B2B Integrator V5.2.4, interim fix 1, or earlier, any certificates that are non-compliant with NIST 800-131a are replaced with new, compliant certificates when interim fix 2 is applied.
- If you are upgrading from a fix pack that doesn't have CLA2 SSL implemented, such as 5241 or earlier, new certificates are created.

Certificate Changes

In order to maintain compliance, the cla2ssl, private key certificate for SSL and the cla2auth, public certificate for command signature verification were changed to include a key length of 2048 bits and a default signing algorithm name for server authentication to: SHA256withRSA.

TLS Version

The default version of TLS protocol used is TLS 1.0; however, if you are using NIST 800-131a strict mode, you must use the TLS protocol version TLS 1.2.

CLA2 Server Changes

An additional property was added for NIST 800-131a compliance for CLA2:

```
CmdLine2server.properties – "NIST.800-131a = off | strict"
```

When used, the remote client is started in the configured mode and the security parameters are loaded automatically and used for communication.

CLA2 Communication

If you are in strict mode, the communication should only be configured with IBM NIST 800-131a compliant JDK. Both the client and server should be on the same mode (whether NIST 800-131a compliance is on or off), and any mismatch will cause a communication failure. The certificates used for authentication and the SSL setup must be NIST 800-131a compliant.

Runtime

When using CLA2 communication, security parameters, such as certificates and underlying JDK must be configured correctly. If the adapter used is configured with non-NIST 800-131a compliant certificates, an error appears on the information page highlighted in red with a message *Not NIST SP800-131a compliant*.

Using OFTP in NIST 800-131a compliance mode

OFTP protocol is supported in Sterling B2B Integrator in OFTP 1.2, OFTP 1.3, OFTP 1.4, and OFTP 2.0; however, only OFTP 2.0 supports secure communications.

TLS Support

The OFTP 2 RFC enforces the usage of TLS and previous versions of SSL are not supported; therefore, only TLS1, TLS 1.1 and TLS 1.2 are supported. This is defined by using the property OFTP.Global.HelloProtocol in OdetteFTP.properties. The default value is OFTP.Global.HelloProtocol=TLS1-TLS1.2.

Ciphers Supported

The following Ciphers supported by OFTP2 are below:

Table 3. Supported Ciphers with OFTP2

Cipher	Suite Symmetric	Asymmetric	Hashing
01	3DES_EDE_CBC_3KEY	RSA_PKCS1_15	SHA-1
02	AEO_256_CBC	RSA_PKCS1_15	SHA-1

TLS Certificate Download

The TLS certificate functionality of OFTP is NOT functional in strict mode. The xml file on the ODETTE site is signed by a non-NIST 800-131a compliant certificate algorithm which is not permitted in strict mode.

Certificate Exchange

When using automatic certificate exchange, the root certificate and/or the auth chain must be present at the receiver's end. The automatic certificate exchange fails if the root or auth chain is not NIST 800-131a complaint.

Adapter and Profile Configuration Considerations:

- When configuring a new adapter or profile, only NIST 800-131a compliant certificates and Cipher strength are available.
- If any non-compliant adapter, certificate, or profile configuration is found, the adapter will not be enabled, the communication fails, and a status message about the non-NIST 800-131a compliance appears.

Using JMS in NIST 800-131a compliance mode

When using JMS 11 for NIST 800-131a compliance, there is no option to control the selection of Cipher suites while configuring the Adapter or Service for Sterling B2B Integrator which does not allow NIST 800-131a compliance for Cipher suite and SSL/TLS version for JMS 11 to be enforced because some providers do not provide an API that allows the control of Cipher suites or TLS version.

Only NIST 800-131a compliant certificates are available for section when working in NIST 800-131a compliance with the JMS adapter and although you can use any JMS provider, there are limitations with some providers:

Table 4. Provider Limitations

Provider	Limitations
Weblogic	Does not work with IBM JDK over SSL
TIBCO	Does not work with IBM JDK over SSL
Active MQ	There is no API to control the Cipher Suite and TLS version
WebSphere MQ	There is no API to control the TLS version

Runtime

Only NIST 800-131a compliance system and CA certificates are available on the Services Configuration page. If a non-NIST 800-131a compliant system or CA certificate are configured, the business process will fail and you must re-configure the adapter with a NIST 800-131a compliant certificate; however if a non-NIST 800-131a compliant Cipher is present the communication will NOT fail because there is no API to control it.

Using Websphere MQ Adapter in NIST 800-131a compliance mode

The WebSphere MQ adapter communicates with WebSphere MQ to send and receive messages. Only compliant ciphers are supported in NIST 800-131a strict mode.

In strict mode, the following ciphers are supported:

- SSL_RSA_WITH_AES_128_CBC_SHA256
- SSL_RSA_WITH_AES_256_CBC_SHA256

Using Websphere MQ Suite Adapter in NIST 800-131a compliance mode

The WebSphere MQ Suite adapter is a set of services used to send and receive messages to WebSphereMQ. When used in the GPM, only the NIST 800-131a compliant Cipher, key certificates, and CA certificates are available for selection.

The WebSphere MQ adapter communicates with WebSphere MQ to send and receive messages. Only compliant ciphers are supported in NIST 800-131a strict mode.

In strict mode, the following ciphers are supported:

- SSL_RSA_WITH_AES_128_CBC_SHA256
- SSL_RSA_WITH_AES_256_CBC_SHA256

Runtime

If a non-NIST 800-131a compliant Cipher, key certificate, or CA certificate are configured, the business process will fail and you must re-configure the adapter with a NIST 800-131a compliant Cipher or certificate.

Using Websphere MQ Suite Async Receive Adapter in NIST 800-131a compliance mode

The WebSphere MQ adapter communicates with WebSphere MQ to send and receive messages. Only compliant ciphers are supported in NIST 800-131a strict mode.

In strict mode, the following ciphers are supported:

- SSL_RSA_WITH_AES_128_CBC_SHA256
- SSL_RSA_WITH_AES_256_CBC_SHA256

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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 and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as shown in the next column.

Trademarks

IBM, the IBM logo, and ibm.com 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 IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

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

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Product Number:

Printed in USA