

*IBM Tivoli Directory Integrator
Compliance for NIST SP800-131A
Specifications*



Contents

About this publication 1

Access to publications and terminology 1

Accessibility 2

Technical training. 2

Support information. 2

NIST SP 800-131A specifications 5

Support for NIST SP 800-131A 5

Modifications to properties files 5

Creating NIST-compliant self-signed certificates. . . . 6

AMC and new certificates 8

Upgrading JRE 9

Verification of NIST configuration 9

Notices 11

About this publication

IBM Tivoli Directory Integrator is an open-architecture, integration solution. You can use this solution to synchronize and exchange information across multiple applications and platforms for providing a consistent enterprise-level view of identity or generic data.

IBM Tivoli Directory Integrator Compliance for NIST SP800-131A Specifications document describes how to configure Tivoli Directory Integrator components to comply with the requirements as defined by National Institute of Standards and Technology (NIST) Special Publications 800-131A.

Access to publications and terminology

This section provides:

- A list of publications in the “IBM Tivoli Directory Integrator library.”
- Links to “Online publications” on page 2.
- A link to the “IBM Terminology website” on page 2.

IBM Tivoli Directory Integrator library

Use these short descriptions of publications and of external sources that can help you understand methodology and components.

IBM Tivoli Directory Integrator V7.1.1 Getting Started

Contains a brief tutorial and introduction to Tivoli Directory Integrator. Includes examples to create interaction and hands-on learning of Tivoli Directory Integrator.

IBM Tivoli Directory Integrator V7.1.1 Installation and Administrator Guide

Includes complete information about installation, migration from a previous version, configuration the logging functionality, and the security model underlying the Remote Server API of Tivoli Directory Integrator. Contains information about how to deploy and manage solutions.

IBM Tivoli Directory Integrator V7.1.1 Users Guide

Contains information about using Tivoli Directory Integrator. Contains instructions for designing solutions with the Directory Integrator designer tool (the Configuration Editor) or running the ready-made solutions from the command line. Also, provides information about interfaces, concepts, and AssemblyLine creation.

IBM Tivoli Directory Integrator V7.1.1 Reference Guide

Contains detailed information about the individual components of Tivoli Directory Integrator such as Connectors, Function Components, Parsers, Objects, and so on. These components are the building blocks of the AssemblyLine.

IBM Tivoli Directory Integrator V7.1.1 Problem Determination Guide

Provides information about Tivoli Directory Integrator tools, resources, and techniques that can aid in the identification and resolution of problems.

IBM Tivoli Directory Integrator V7.1.1 Messages Guide

Provides a list of all informational, warning, and error messages that are associated with the Tivoli Directory Integrator.

IBM Tivoli Directory Integrator V7.1.1 Password Synchronization Plug-ins Guide

Includes complete information for installing and configuring each of the five IBM® Password Synchronization Plug-ins: Windows Password Synchronizer, Sun Directory Server Password Synchronizer, IBM Tivoli Directory Server Password Synchronizer, Domino® Password Synchronizer, and Password Synchronizer for UNIX and Linux. Also, provides configuration instructions for the LDAP Password Store and JMS Password Store.

IBM Tivoli Directory Integrator V7.1.1 Release Notes

Describes new features and late-breaking information about Tivoli Directory Integrator that did not get included in the documentation.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Tivoli Directory Integrator Information Center

The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDI.doc_7.1.1/welcome.htm site displays the information center welcome page for this product.

IBM Security Information Center

The <http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp> site displays an alphabetical list of and general information about all IBM Security product documentation.

IBM Publications Center

The <http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss> site offers customized search functions to help you find all the IBM publications that you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

NIST SP 800-131A specifications

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-131A guidelines provide cryptographic key management guidance.

NIST SP 800-131A specification mandates changes to the rules for cryptography. These specifications enforce major changes to algorithm strength rules and use of secure sockets (TLS 1.2). NIST SP 800-131A specification mandates:

- SHA1 is not allowed for digital signatures
- RSA 1024 keys are not allowed
- RSA keys with minimum of 2048 bits are allowed
- DES keys are not allowed
- AES keys of any length are allowed
- TLS 1.2 protocol must be enabled

For more information about NIST SP 800-131A, see *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths* at: <http://csrc.nist.gov/publications/PubsSPs.html>

Support for NIST SP 800-131A

You must upgrade Tivoli Directory Integrator to support NIST SP 800-131A requirements.

Make the following modifications to Tivoli Directory Integrator to comply with NIST SP 800-131A requirements to strengthen the security.

- Encrypt and decrypt data files as per the requirements.
- Enable TLS 1.2 protocol.
- Use NIST-compliant digital signatures.

Note: For IBM Tivoli Directory Integrator V7.1 and V7.1.1, verify that the minimum JRE is IBM JRE 1.6 SR10. See “Upgrading JRE” on page 9 for more details.

Modifications to properties files

You must configure the `solution.properties` and `global.properties` files to support the NIST requirements.

Add the following property to the `global.properties` and `solution.properties` files.

```
com.ibm.di.server.NIST.on=true
```

The default value of this property is false. When you set the value to true, Tivoli Directory Integrator uses TLS 1.2 protocol to establish the SSL connections.

Modify the `com.ibm.di.securityTransformation` property to use AES/ECB/NOPadding.

The following example shows the new `global.properties` file when **`com.ibm.di.securityTransformation`** is set to its default value:

```
com.ibm.di.securityTransformation=DES/ECB/NoPadding

## NIST Setting
#com.ibm.di.server.NIST.on=true
#com.ibm.di.securityTransformation=AES/ECB/NoPadding
```

The **`com.ibm.di.securityTransformation`** property in the `global.properties` and `solution.properties` files determines the cipher for the encryption or decryption of Tivoli Directory Integrator configurations. The default value is set to `DES/ECB/NoPadding`.

Note: You must migrate the existing encrypted files, if there is any change of the key or the cipher that the Tivoli Directory Integrator Server uses for encryption. To migrate an encrypted file, you must decrypt it with the old encryption key or old cipher, and encrypt it with the new one.

Files that are encrypted or contain encrypted parts are:

- Tivoli Directory Integrator configuration files
- Server API User registry file
- Tivoli Directory Integrator properties files

Note: Tivoli Directory Integrator properties files can contain encrypted properties, even if the files are not encrypted as a whole.

By default, all sensitive properties, such as passwords, in the `global.properties` file or the `solution.properties` file are encrypted. You must migrate `global.properties` and `solution.properties` files when you change the server encryption key. For more information about encryption and decryption of data in Tivoli Directory Integrator, see: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDI.doc_7.1.1%2Fadminguide57.htm&path%3D7_4_11_3

When Tivoli Directory Integrator supports NIST, the following connectors can communicate over TLS 1.2 protocol:

- HTTP Server Connector
- DSMLv2SOAPServer Connector
- LDAP Server Connector
- TCP Server Connector

Creating NIST-compliant self-signed certificates

To create NIST-compliant self-signed certificates, you must use minimum of SHA2 for digital signatures and cryptographic with a minimum key strength of 112 bits.

About this task

This task describes how to create NIST-compliant self-signed certificates with the `keyman` tool. For Tivoli Directory Integrator installation instructions, see the Installation instructions for IBM Tivoli Directory Integrator topic in http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDI.doc_7.1.1/welcome.htm.

Procedure

1. Start the `ikeyman.exe` tool present in the `<TDI_install_dir>\jvm\jre\bin\ikeyman.exe` directory.
2. Select **Key Database File > New**.
3. In the **File Name** field, type an appropriate file name, for example, `nist_testserver.jks`.
4. Click **OK**.
5. In the **Password** field, type the password.
6. Click **OK**.
7. Click **New Self_Signed**.
8. Type the appropriate values in the data fields as shown:

Option	Description
Key Label	admin
Version	X509 V3
Key Size	2048
Signature Algorithm	SHA2WithRSA

9. Click **OK**.
10. Extract the resultant certificate in a der file. For example: `nist_testserver.der`
11. Create the `nist_testadmin.jks` and `nist_testadmin.der` files by following the steps 1 - 9.
12. Import the `nist_testserver.der` file into Signer certificates of `nist_testadmin.jks` with the label as `server`.
13. Import the `nist_testadmin.der` into Signer certificates of `nist_testserver.jks` with the label as `admin`.

Results

Tivoli Directory Integrator Version 7.1, Fix Pack 7 and Tivoli Directory Integrator Version 7.1.1, Fix Pack 2 onwards, sample NIST certificates are shipped. You can find these certificates in the `<fix_pack_install_dir>\NIST\Sample Certificates` directory. The keystore passwords for these jks files are as follows:

Key Store	Password
<code>nist_testserver.jks</code>	<code>server</code>
<code>nist_testadmin.jks</code>	<code>administrator</code>

Example

You might need to edit the following example `solution.properties` or `global.properties` file when NIST is enabled.

```
com.ibm.di.server.NIST.on=true
```

```
## server authentication
javax.net.ssl.trustStore=serverapi/nist_testadmin.jks
{protect}-javax.net.ssl.trustStorePassword=administrator
```

```
## client authentication
javax.net.ssl.keyStore=serverapi/nist_testadmin.jks
{protect}-javax.net.ssl.keyStorePassword=administrator
```

```

api.keystore=nist_testserver.jks
api.key.alias=server
{protect}-api.keystore.password=server

api.truststore=nist_testserver.jks
{protect}-api.truststore.pass=server

com.ibm.di.server.encryption.keystore=nist_testserver.jks

## Server API client properties
api.client.ssl.custom.properties.on=true
api.client.keystore=serverapi/nist_testadmin.jks
{protect}-api.client.keystore.pass=

{protect}-api.client.key.pass=administrator
api.client.truststore=serverapi/nist_testadmin.jks
{protect}-api.client.truststore.pass=administrator

```

Note: The truststore and keystore values shown in this example are based on the sample certificates that are shipped with the Tivoli Directory Integrator Fix Pack.

AMC and new certificates

You must configure Administration and Monitoring Console (AMC) if you start the Tivoli Directory Integrator server with the `com.ibm.di.server.NIST` property set to `true`.

For more information about AMC, see the “AMC and Action Manager security” topic at: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDI.doc_7.1.1/welcome.htm

To monitor the Tivoli Directory Integrator server through AMC, make the following changes:

1. Run the following script file to stop AMC.
 - `stop_tdiamc.bat` for Windows
 - `stop_tdiamc.sh` for Linux
2. Update the AMC keystores to use the new NIST-compliant certificates. Copy the `nist_testadmin.jks` file into the AMC deployment directory. The default AMC deployment directory is `<TDI_Install_dir>\lwi\runtime\isc\eclipse\plugins\AMC_7.X.X`.
3. In the `<TDI_Install_dir>\lwi\runtime\isc\eclipse\plugins\AMC_7.X.X\amc.properties` file, update the following properties to point to the new certificates:


```

api.truststore=nist_testadmin.jks
api.truststore.pass=administrator
api.truststore.type=jks
api.client.keystore=nist_testadmin.jks
api.client.keystore.pass=administrator
api.client.keystore.type=jks

```
4. Run the following script file to start AMC.
 - `start_tdiamc.bat` for Windows
 - `start_tdiamc.sh` for Linux

Upgrading JRE

You must verify that the minimum JRE is IBM JRE 1.6 SR10 or higher for IBM Tivoli Directory Integrator V7.1 and V7.1.1.

About this task

Use the following command to determine the current JRE version:

```
<tdi-install-dir>\jvm\jre\bin>java -version
```

Note: JRE upgrade is required only for Tivoli Directory Integrator Version 7.1.

Procedure

1. Stop all components such as Tivoli Directory Integrator Server, Configuration Editor, Administration and Monitoring Console, and **tdisrvctl** utility.
2. Contact L2 support for the fix with latest JRE fixes. See <http://www-01.ibm.com/support/docview.wss?uid=swg21621588>
3. Extract the fix package to a temporary directory.
4. Back up the older <TDI_Install_dir>\jvm folder from the system where Tivoli Directory Integrator is installed.
5. Extract the jvm.tar.gz or jvm.zip file.
6. Replace the older jvm folder with the jvm folder extracted from the jvm.tar.gz or jvm.zip file.

Verification of NIST configuration

You can verify the NIST configuration by confirming whether the new cipher suites are used.

1. Modify the solution.properties file by adding:
javax.net.debug=ssl
2. Start the Tivoli Directory Integrator server in daemon mode.
3. Run the following command:
tdisrvctl.bat -T "..\nist_testserver.jks" -W server -K "..\nist_testadmin.jks"
-P administrator -op srvinfo

Note: The syntax is based on the sample jks files. The files are placed in the installation directory.

Successful configuration of NIST shows the following SSL cipher data in the Tivoli Directory Integrator server log file:

JsseJCE: Using cipher AES/GCM/NoPadding from provider

Notices

This information was developed for products and services offered in the U.S.A. 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 give you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte (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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

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 states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply 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 Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All 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 the names and addresses used by an actual business enterprise 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. 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 IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

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, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

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 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.

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