Redpaper

Bert Dufrasne
Andre Candra
Scott Helmick
Peter Kimmel
Abilio de Oliveira
Axel Westphal
Bruce Wilson

IBM DS8870 and NIST SP 800-131a Compliance

The IBM® DS8870, starting with Release 7.2 (Licensed Machine Code (LMC) 7.7.20.xx.xx) or later, enables compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-131a.

With the ever-growing landscape of national, state, and local regulations, industry requirements, and increased security threats, ensuring the protection of an organization’s information is a key part of being a successful business.

Businesses need tools to protect against the known threats, but also guard against as yet unknown threats. Effective threat and vulnerability management must be proactive rather than reactive, preventing problems rather than responding to them.

One of the pillars of information security is cryptography because it addresses the concerns of confidentiality, authentication, and data integrity of the information.

NIST established the Special Publication 800 series in 1990 to specifically address information technology security. In particular, NIST SP 800-131a is intended to provide guidance that is associated with the usage of the cryptography by the Federal Government Agencies for the protection of sensitive, but unclassified information.

The security strength of an algorithm with a particular key length is measured in bits and is, basically, a measure of the difficulty of discovering the key. The appropriate security strength that is used depends on the sensitivity of the data being protected and also depends on the actual vulnerability status of the data that is exposed.

For the United States federal government, a minimum security strength of 80 bits was the recommendation until 2010. By the beginning of 2011, the minimum key strength number increased from 80 bits to 112 bits. However, with the acceptance of a certain amount of risk, the minimum of 80 bits of security strength may be used until the end of 2013.

NIST SP 800-131a requires longer key lengths and stronger cryptography than other standards. The standard requires cryptographic algorithms that have key strengths of at least 112 bits.

Strict enforcement of NIST SP 800-131a imposes the usage of the Transport Layer Security (TLS) 1.2 protocol for the Secure Sockets Layer (SSL) context.

This IBM Redpaper™ publication describes how the DS8870 addresses compliance with NIST SP 800-131a. This publication helps customers tailor and configure their DS8870 environment to enable it for NIST SP 800-131a compliance.

DS8870 environment and NIST SP 800-131a compliance

The first consideration in preparing the environment for NIST SP 800-131a compliance is to make sure that the DS8870 itself supports the requirements for compliance. To that end, you must upgrade your DS8870 (Hardware Management Console and Storage System) to Release 7.2.

Important: The first step towards NIST SP 800-131a compliance in a DS8870 environment is to upgrade the DS8870 to microcode Release 7.2.

As shipped, the DS8870 is not in NIST SP 800-131a compliant mode, and access to the DS8870 is little changed from previous releases, which are intentional and necessary to avoid breaking scripts that some clients might have developed for their environment.

Clients are responsible for enforcing NIST compliance on the various interfaces that access their DS8870 systems. Enforcing NIST compliance on the DS8870 can be done incrementally (that is, one interface at a time) by using various DS CLI controls. Each control specifies an input or output access point that can be maintained in legacy mode or placed in “800131a” mode.

Table 1 summarizes the different interface controls, whether they can act as input, output, or both, from the DS8870 standpoint, and what products communicate over that interface (access source). The various controls and settings are explained in the sections that follow.

Table 1 Interface controls

Interface control	Input/Output	Access source
CIM	Input	SMI-S client
DS GUI	Input	HTML browser
DSNI	Input	DS CLI, HMTU, and IBM Tivoli® Storage Productivity Center
	Output	Directory Services and encryption key servers
WUI	Input	HTML browser

It is important to understand that enabling NIST compliance for a specific interface on the DS8870 implies that the products communicating with the DS8870 through that interface must also be NIST SP 800-131a compliant.

Important: Before activating controls on the DS8870 and disabling other protocols, make sure that all other external systems (hardware and software) communicating with the DS8870 in your environment can support the TLS 1.2 protocol. Otherwise, access to those systems is lost.

Such products consist of the hardware and software for all external systems that directly or indirectly attach to the DS8870, including key management servers, DS Graphical User Interface (DS GUI) and DS Command Line Interface (DS CLI) clients, monitoring servers, such as Tivoli Productivity Center, Storage Management Initiative Specification (SMI-S) clients and listeners, and the IP network.

The focus for compliance is on how the different components can securely communicate with the DS8870, so the focus is on the network and the communication protocols that are used.

On network interfaces that attach to the DS8870, the user is responsible for first upgrading external software to versions that support TLS 1.2 and then activating “800131a” communication mode for the different interfaces and protocols that are used to communicate with the DS8870.

Figure 1 shows, for a typical DS8870 environment, some of the typical hardware and software elements that communicate with the DS8870.

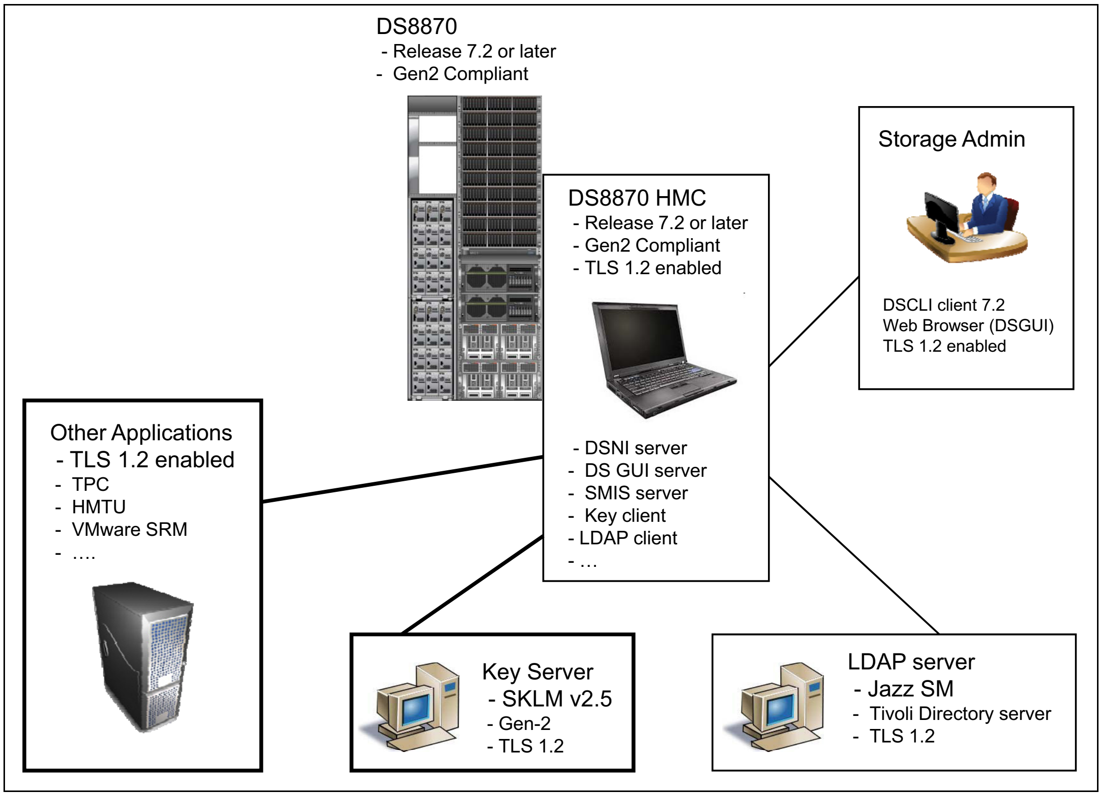


Figure 1 Typical DS8870 compliant environment with NIST SP 800-131a

NIST SP 800-131a requires communication between the DS8870 and other entities that use the Transport Layer Security (TLS) 1.2 protocol.

Another aspect of the NIST SP 800-131a compliance pertains to encryption. IBM initially introduced disk encryption on the IBM DS8000® with 80-bit security strength; IBM calls this the Gen-1 certificate. For the DS8000, digital certificates are created and set by manufacturing for each Storage Facility.

DS8870 Release 7.2 offers 112-bit security strength; IBM calls this the Gen-2 certificate. DS8870 Release 7.2 is the first model to support the 112-bit security strength certificates in support of NIST SP 800-131a.

The encryption and key servers setup for NIST SP 800-131a compliance is described in "Encryption and key server compliance" on page 33.

DS Network Interface

Most applications that communicate with the DS8870 do so through the DS Network Interface (DSNI). For NIST SP 800-131a compliance, such applications must be customized to use the DSNI client R 7.2.

It is not possible to address all of the possible client applications that can access the DS8870 through the DSNI, but this section covers the most commonly used applications.

DSNI, formerly known as IBM Enterprise Storage Server® Network Interface (ESSNI), is based on a logical client/server model. As shown in Figure 2, the DSNI server component is in the Hardware Management Console and interacts with the two DS8870 internal servers. The DSNI server handles all network-based requests for DS8000 configuration and copy services.

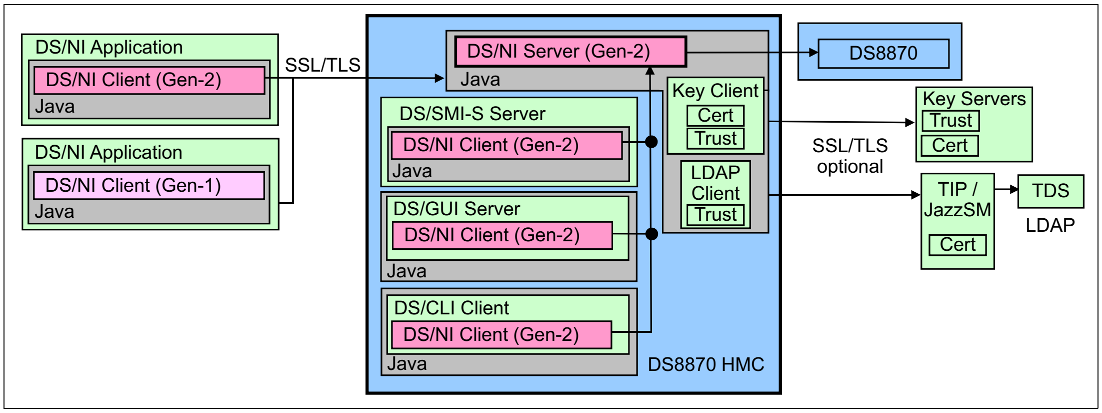


Figure 2 DSNI connection

The DSNI client is in the client application that needs to communicate with the DS8870. Consider the following items:

- The DSNI client can also be found in external applications that communicate with the DS8870. Examples of such external applications include Tivoli Storage Productivity Center, Tivoli Storage Productivity Center for Replication, and the IBM Heat Map Transfer Utility.
- The DSNI client can be embedded in various entities that are on the HMC, such as the DS GUI server, DS CLI client, and SMI-S Server.
- Additionally, DSNI also enables the DS8870 to support LDAP authentication and disk encryption with usage of an external key server.

DSNI clients earlier than Licensed Machine Code (LMC) 7.7.20.xx contain a legacy certificate with an MD5 digital signature (shown in Figure 2 as DS/NI Client Gen-1 certificate). DSNI communication with the DSNI client uses port 1750. These earlier DSNI clients attempt to connect on port 1750 by using the SSLv3 protocol and the legacy certificate.

DSNI clients that support LMC 7.7.20.xx and later contain both the certificate that is used in earlier versions of DS8000 and a newer certificate that has a stronger NIST SP 800-131a-approved digital signature (shown in Figure 2 on page 4 as DS/NI Gen-2 Certificate). However, to support compatibility with earlier versions of the DSNI agents, port 1751 is used for communication with the NIST SP 800-131a certificate. The DSNI client first attempts to connect on port 1751 by using the TLS 1.2 protocol and a NIST SP 800-131a-compliant certificate. If that attempt fails, the DSNI client uses the prior DSNI client algorithm and tries port 1750. This algorithm ensures that the DSNI client can connect to a DS8870 or previous DS8000 model machine automatically with the highest level of security possible. For more information, see “DSNI server and port 1750” on page 8.

Important: All applications that use the DS Network Interface server to connect to the DS8870 must be updated to NIST SP 800-131a security conformance before you update the DS Network Interface server, or connectivity to these applications is lost.

Upgrading client applications for NIST SP 800-131a compliance

Several IBM software products that can be used in a DS8870 environment come with embedded DSNI client code. The following sections provide information that is related to NIST SP 800-131a compliance for the most commonly used applications that include an embedded DSNI client.

IBM Tivoli Storage Productivity Center

IBM Tivoli Storage Productivity Center is a resource management application that provides comprehensive visibility, control, and automation for managing heterogeneous software, system, and storage infrastructures through a centralized, web-based management console.

The IBM Tivoli Storage Productivity Center application has an embedded DSNI client that communicates with a DSNI server on one or more Hardware Management Consoles. A user must configure the Tivoli Storage Productivity Center server with IP addresses of one or more DS8000 HMCs, and an appropriate DSNI user ID and password. The user account is authenticated by the DSNI server.

At the time of writing, a version of the IBM Tivoli Storage Productivity Center that was NIST SP 800-131a-compliant, and that thus supported the TLS v1.2 protocol, was not available.

IBM Easy Tier Heat Map Transfer Utility

IBM Easy Tier® Heat Map Transfer provides a data placement algorithm at a mirrored primary site, and can reapply it at the mirrored secondary site through the Easy Tier Heat Map Transfer Utility (HMTU).

HMTU communicates with a DS8870 through the DS Network Interface (DSNI). NIST SP 800-131a requires communication through DSNI to be secure. To enable HMTU to work with a DS8870 in NIST SP 800-131a-compliant security setting, complete the following steps:

1. Upgrade HMTU to Version 7.2. Previous versions do not support a DS8870 with the NIST SP 800-131a-compliant security setting.
2. Update servers that are running the HMTU to a version of Java that is NIST SP 800-131a-compliant, such as IBM Java 6 SP10 and later.
3. For NIST SP 800-131a security compliance, all Java-based external applications that connect to the DS8870 must use a version of Java that meets the requirements of NIST SP 800-131a, such as IBM Java 6 SP10 and later.

4. Set the Network Interface security level of all DS8870 systems that are listed in the HMTU to NIST SP 800-131a compliant. For more information, see “DSNI server and port 1750” on page 8.

5. Restart the HMTU server daemon. After you upgrade HMTU and the Java version, the former HMTU server is still running and therefore cannot communicate with a DS8870 with NIST SP 800-131a-compliant security settings (see Example 1).

Example 1   Check connection to DS8870

```
hmtu>lsdev -checkconn
Date/Time: 2013-11-05 11:56:09 IBM HMTU Version: 7.7.20.555
DevId               HMC1                 HMC2                 User
ConnStatus
===============================================================================
===================
IBM.2107-75ZA571    9.155.70.13                               itso_admin
Cannot connect
IBM.2107-75ZA181    9.155.54.49                               itso_admin
Cannot connect
```

Restarting the HMTU server, as shown in Example 2, makes the HMTU server daemon run using a compliant HMTU and Java version, so the HMTU server can communicate with the DS8870 by using NIST SP 800-131a-compliant security settings (see Example 3).

Example 2   Restart HMTU server

```
hmtu>manageserver -action stop
Date/Time: 2013-11-05 11:56:27 IBM HMTU Version: 7.7.20.555
GUSS00040I The Easy Tier heat map transfer server was stopped successfully.
hmtu>manageserver -action start
Date/Time: 2013-11-05 11:56:37 IBM HMTU Version: 7.7.20.555
GUSS00039I The Easy Tier heat map transfer server was started successfully.
Tip: Refer the command lsdev -checkconn to check the status of the storage
systems. Issue the lshmt command to check the data transfer results
```

Example 3   Check connection to DS8870 after a server restart

```
hmtu>lsdev -checkconn
Date/Time: 2013-11-05 11:56:55 IBM HMTU Version: 7.7.20.555
DevId               HMC1                 HMC2                 User
ConnStatus
==================================================================================
================
IBM.2107-75ZA571    9.155.70.13                               itso_admin
Running
IBM.2107-75ZA181    9.155.54.49                               itso_admin
Running
```

IBM DS8000 Adapter for VMware vCenter Site Recovery Manager

The IBM DS8000 Adapter for VMware vCenter Site Recovery Manager (SRM) is a software add-on that is used as a Storage Replication Adapter (SRA) that integrates with a VMware vCenter Site Recovery Manager (SRM) solution.

The DS8000 SRA enables VMware vCenter SRM to perform a failover between DS8000 storage systems. The DS8000 SRA extends SRM capabilities and allows it to employ

DS8000 replication and mirroring as part of the SRM comprehensive Disaster Recovery Planning (DRP) solution.

The DS8000 Adapter for SRM has an embedded DSNI client that communicates with a DSNI server on one or more HMCs. You must configure the DS8000 SRM plug-in with a DSNI user ID and password and the IP addresses of one or more DS8000 management servers. The user account is authenticated by the DSNI server.

To achieve NIST SP 800-131a compliance in a DS8870 that is connected to VMware SRM, complete the following steps:

1. Update the DS8000 for VMware vCenter Site Recovery Manager software that connects to a DS8870 with R7.2 or later to a version that is NIST SP 800-131a compliant, such as DS8000 for VMware vCenter Site Recovery Manager 5.x Version 2.2.1. You can check for the latest version of the DS8000 SRM add-on software at the following website:

   http://www.vmware.com/go/download-srm

2. Ensure that you have a NIST SP 800-131a-compliant Java version that is installed for VMware SRM and the DS8000 plug-in. All Java-based external applications that connect to the DS8870 must use a version of Java that meets the requirements of NIST SP 800-131a, such as IBM Java 6 SP10 and later.
3. Set the SSL protocol for the DS8000 for VMware vCenter Site Recovery Manager software to enable TLS 1.2.

DS CLI client

DS CLI communicates with a DS8870 through the DSNI protocol. NIST SP 800-131a requires communication through DSNI to support TLS 1.2. To get DS CLI to work with a DS8870 in NIST SP 800-131a-compliant security setting, complete the following steps:

1. Upgrade DS CLI to Version 7.7.20.xx.xx or later. Previous versions do not support a DS8870 with the NIST SP 800-131a-compliant security setting. Previous versions also do not include the **manageaccess** command that is required to change the security setting on DS8870. You can download the latest DS CLI code level at the following website:

   http://www-01.ibm.com/support/docview.wss?uid=ssg1S4001056

2. For NIST SP 800-131a security compliance, all Java-based external applications that connect to the DS8870 must use a version of Java that meets the requirements of NIST SP 800-131a, such as IBM Java 6 SP10 and later.
3. Set the Network Interface security level of all DS8870 systems that are listed in HMTU to be NIST SP 800-131a compliant. For more information, see “DSNI server and port 1750” on page 8.

DSNI server and port 1750

To change the security level for the DSNI server on the HMC to be NIST SP 800-131a compliant, use the DS CLI **manageaccess** command with the **-ni** flag, as shown in Example 4.

Example 4 Setting the DSNI security level

```
dscli> manageaccess -ctrl ni -action setsecurity -level 800131a

CMUC00462W manageaccess: Changing the ESSNI security level will restart the ESSNI
server in order for the change to take effect, and will take a few minutes to
complete. If specifying 800131a, ensure that all ESSNI clients and Java levels are
NIST SP 800-131a compliant before proceeding. Are you sure that you want to
continue? [Y/N]: y
CMUC00212I manageaccess: completed successfully.
```

You can check the result of the security level change by running **showaccess**, as shown in Example 5.

Example 5 Checking the DSNI security level

```
dscli> showaccess hmc1
hmc            hmc1
cmdline        enabled
wui            disabled
modem          disabled
vpn            disabled
port1750       disabled
cim(security) legacy
gui(security) legacy
ni(security)  800131a
wui(security) legacy
```

In Example 5, after you change the security level of the DS Network Interface (DSNI), TLS 1.2 is used for the communication. Changing the DSNI security level also disables port 1750 of the network interface. The DS8870 uses the new 1751 port with the NIST SP 800-131a-compliant certificate. Changing this control restarts the DSNI server, but the DSNI clients usually automatically reconnect in a couple of minutes.

However, it is possible to disable only port 1750 without enabling the NIST SP 800-131a-compliant security setting. This control does not affect connections to Storage Authentication Service through LDAP and Key Lifecycle Manager. Example 6 shows how to use the **manageaccess** command to disable port 1750.

Example 6 Disable port 1750 of DSNI

```
dscli> manageaccess -ctrl port1750 -action disable
CMUC00464W manageaccess: Enabling port 1750 allows clients such as DS CLI to
connect without having the current code level. Disabling the port can ensure that
only those clients that support higher levels of secure communication can connect.
Are you sure that you want to continue? [Y/N]: y
CMUC00470I manageaccess: Port 1750 has been disabled successfully on HMC 1.
dscli> showaccess hmc1
hmc            hmc1
cmdline        enabled
wui            disabled
modem          disabled
```

```
vpn            disabled
port1750       disabled
cim(security)  legacy
gui(security)  legacy
ni(security)   legacy
wui(security)  legacy
```

As you can see in Example 6 on page 8, the usage of port 1750 is disabled, but the DSNI security setting is still the same.

Storage Management Initiative - Specification interface

The Storage Management Initiative - Specification (SMI-S) is a storage standard that is developed by the Storage Networking Industry Association (SNIA). SMI-S is based on the Common Information Model (CIM) and the Web-Based Enterprise Management (WBEM) standards that are defined by the Distributed Management Task Force (DMTF). SMI-S enables broad interoperable management of various storage vendor systems.

Figure 3 shows the SMI-S communication flow in the DS8870.

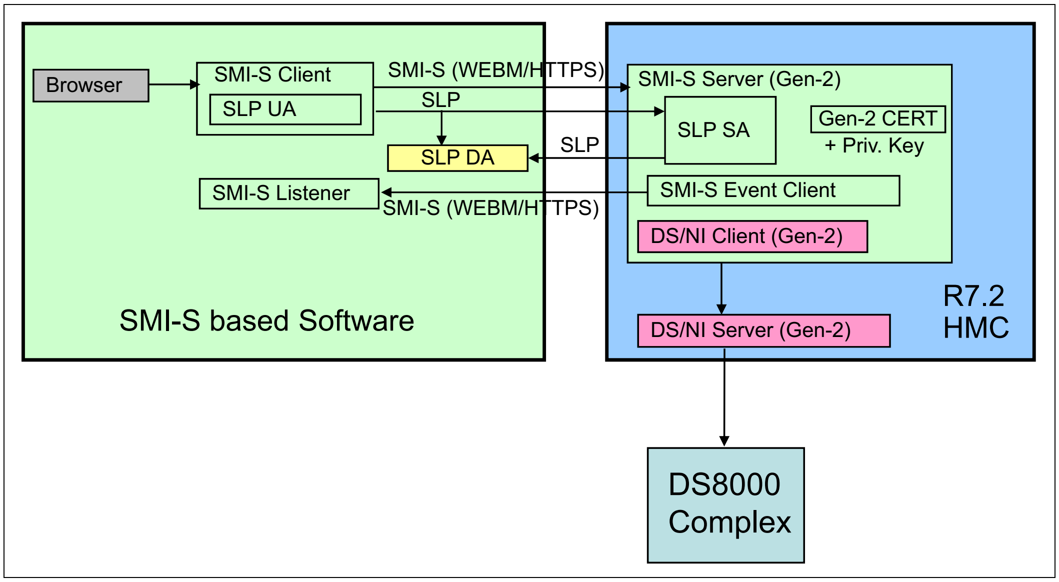


Figure 3   SMI-S communication in a DS8870

The SMI-S protocol ensures that the SMI-S server supports an SLP service agent (SLP SA) to allow SMI-S clients to find SMI-S agents with an SLP user agent (SLP UA). Some applications have an SLP Directory Agent (SLP DA) that registers URL for SLP SA services and provides service URLs to SLP UA. Some storage applications have an embedded SMI-S client that communicates with an SMI-S agent in a DS8870, which in turn sends SMI-S events to a specified URL known as an SMI-S listener. The SMI-S client communicates with an SMI-S agent in the DS8870 that implements the CIM objects that are used to manage DS8870 storage subsystems through a DS Network Interface (DSNI) connection.

Note: The DS8870 uses port 6989 for HTTPS on the SMI-S server that is on the HMC to communicate with various software.

The following IBM software products use SMI-S clients that support the DS8870:

- IBM Tivoli Storage FlashCopy® Manager (FCM) Version 4.1 or later
- IBM Tivoli Storage Manager for Advanced Copy Services
- IBM Tivoli Monitoring (SAN Monitoring)

The following vendor software products have SMI-S plug-ins for IBM devices that are developed by the vendor or by IBM:

- IBM System Storage® Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service
- HP Storage Essentials
- Symantec CommandCentral
- SolarWinds (Tek-Tools) Storage Profiler
- EMC ControlCenter
- IntelliMagic Vision and IntelliMagic Direction

NIST SP 800-131a compliance for an SMI-S agent or listener

To make the application that provides an SMI-S client or listener enabled for NIST SP 800-131a compliance, complete the following steps:

1. Update the SMI-S client or SMI-S listener software to a version that is NIST SP 800-131a-compliant.

   Update servers with SMI-S client or SMI-S listener software that connect to a DS8870 NIST SP 800-131a-compliant system by using NIST SP 800-131a-compliant cryptographic library support (including Java and OpenSSL). In some cases, the application might include its own cryptographic library. For NIST SP 800-131a compliance support, see the applicable application vendor’s documentation.

2. Enable TLS 1.2 on the server and install NIST SP 800-131a-compliant trust anchors

   To be NIST-compliant, you must use TLS 1.2 communication and the TLS cipher suite with a minimum 112-bit security strength. Typically, DS/SMI-S clients and listeners that connect to DS8870 do not have a trust anchor. For information about configuring the software to be NIST SP 800-131a compliant, see the applicable software vendor’s documentation.

NIST SP 800-131a compliance for an SMI-S server on an HMC

NIST SP 800-131a compliance is available in DS8870 with Licensed Machine Code 7.7.20.xx.xx or later.

> **Important:** Before you set the DS8870 security for SMI-S to be NIST SP 800-131a-compliant, ensure that you have upgraded the SMI-S clients and listener to be SMI-S compliant. Otherwise, the SMI-S client loses access to the DS8870.

To make the DS8870 SMI-S NIST SP 800-131a-compliant, complete the following steps:

1. You can check the security level for SMI-S connection by running **showaccess**, as shown in Example 7. In this example, we use the **hmc1** parameter. If your system is a dual-HMC configuration, the **showaccess** command can be run in both HMCs.

   Example 7 Show HMC access

   ```
   dscli> showaccess hmc1
   hmc            hmc1
   cmdline        enabled
   wui            disabled
   modem          disabled
   vpn            disabled
   port1750       enabled
   cim(security) legacy
   gui(security) legacy
   ni(security)  legacy
   wui(security) legacy
   ```

2. To change the security level to NIST SP 800-131a compliant, run **manageaccess** on the DS CLI, as shown in Example 8.

   Example 8 Change the HMC CIM server security level

   ```
   dscli> manageaccess -ctrl cim -action setsecurity -level 800131a
   CMUC00461W manageaccess: Changing the security level of the DS CIM causes a
   required restart of its server. Are you sure that you want to continue? [Y/N]:
   y
   CMUC00212I manageaccess: completed successfully.
   ```

   You can check the change in access by running **showaccess**, as shown in Example 9.

   Example 9 Running the showaccess command

   ```
   dscli> showaccess hmc1
   hmc            hmc1
   cmdline        enabled
   wui            disabled
   modem          disabled
   vpn            disabled
   port1750       enabled
   cim(security) 800131a
   gui(security) legacy
   ni(security)  legacy
   wui(security) legacy
   ```

Configuring the DS GUI

The DS GUI code is on the HMC and users access it remotely through a supported web browser.

As is the case with other interfaces that are described in this paper, setting the security level to be NIST SP 800-131a compliant requires specific settings on both the DS8870 HMC (where the DS GUI is) and the remote workstation where the browser that is used to access the DS GUI is.

Because the GUI server is accessed through a web browser, there is a web server that runs in the HMC. This server handles all browser-based access to the DS GUI server on the HMC, as shown in Figure 4.

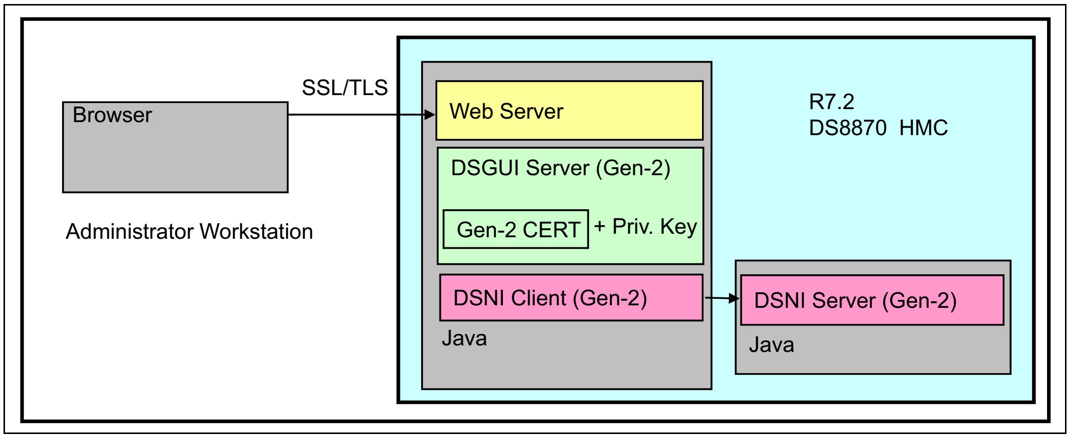


Figure 4 DS GUI server and web browser

Changing the DS GUI security level on the HMC

To implement NIST SP 800-131a security compliance for DS SM, you must set the DS GUI security level to ‘800131a’. The security level is set by running specific DS CLI commands. These commands are available starting with Version 7.7.20.xx.

Example 10 shows the output of a new DS CLI command, **`showaccess`**, which displays the current security level settings in the HMC. (This command is not available with DS CLI Versions 7.7.1x.xxx and earlier). The specific setting that relates to the GUI is the `gui (security)` level, which is set to `legacy`. This level allows for non-compliant NIST SP 800-131a browser access to the GUI.

Example 10 Displaying the current security settings

```
dscli> showaccess hmc1

hmc           hmc1
cmdline       enabled
wui           disabled
modem         disabled
vpn           disabled
port1750      disabled
cim(security) legacy
gui(security) legacy
ni(security)  legacy
wui(security) legacy
```

To change the security level, run **`manageaccess`**. With this command, the security level can be set to either `legacy` or `800131a`.

When set to `legacy`, non-NIST SP 800-131a-compliant security is in place for that particular server. In the case of GUI usage, this means that access to the GUI server using a browser without TLS 1.2 support enabled remains possible.

Example 11 on page 13 shows the **`manageaccess`** command that is being used to change the GUI security level to `800131a`.

Example 11 Changing the DS GUI security settings

```
dscli> manageaccess -ctrl gui -action setsecurity -level 800131a
CMUC00460W manageaccess: Changing the security level of the DS GUI causes a
required restart of its server. If the level is set to 800131a, only browsers that
support this level will be able to connect to the GUI. Are you sure that you want
to continue? [Y/N]: y
CMUC00212I manageaccess: completed successfully.
dscli>
```

When the command is submitted correctly, there is a warning that is displayed indicating that the GUI server will be restarted. This restart disconnects all users that are currently using the GUI through a browser. There is also a warning that all clients must be compliant to access the GUI. Finally, a confirmation for this change is requested. Enter `y` to continue the request. After a few seconds, the `completed successfully` message is displayed.

With this level set, the GUI is now NIST SP 800-131a compliant. The setting can be confirmed by running **`showaccess`**, as shown in Example 12.

Example 12 Confirming the current security settings

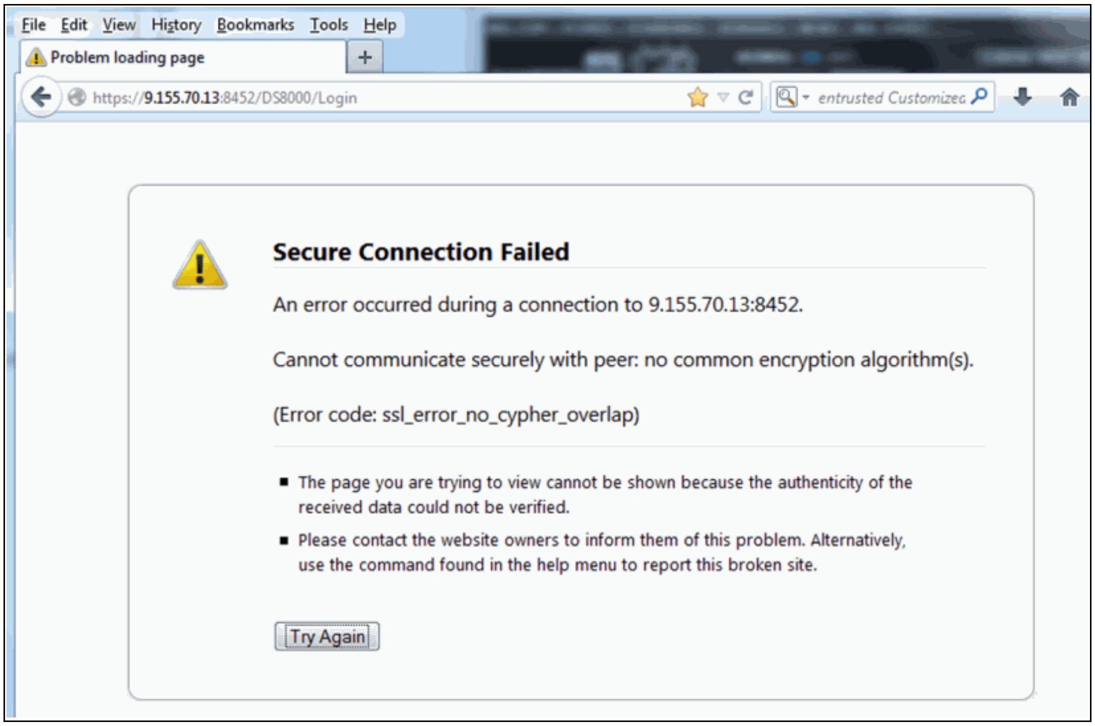
```
dscli> showaccess hmc1

hmc            hmc1
cmdline        enabled
wui            enabled
modem          enabled
vpn            disabled
port1750       enabled
cim(security)  legacy
gui(security)  800131a
ni(security)   legacy
wui(security)  legacy
dscli>
```

After the security level is set, it can be changed to the alternative value at any time, but when you return it to `legacy` level, it is no longer NIST SP 800-131a compliant.

Web browser security setup

Now that the HMC GUI is NIST SP 800-131a compliant, it is necessary to make sure that the browser being used to access it is compliant. If you attempt to access the GUI with a browser that is not compliant, the browser returns a failure message, as shown in Figure 5.


File Edit View History Bookmarks Tools Help
Problem loading page
https://9.155.70.13:8452/DS8000/Login
entrusted Customizec

Secure Connection Failed

An error occurred during a connection to 9.155.70.13:8452.

Cannot communicate securely with peer: no common encryption algorithm(s).

(Error code: ssl_error_no_cypher_overlap)

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem. Alternatively, use the command found in the help menu to report this broken site.

Figure 5 Browser not compliant

The browsers that are used to access the DS Storage Manager and DS Service GUI also must be compliant with the NIST SP 800-131a security standard. Your browser must be enabled to support TLS 1.2 to have access to a NIST SP 800-131A-compliant cryptographic library.

The following browsers support TLS 1.2 protocols:

- Opera 10 with Presto 2.2 (TLS 1.2 is disabled by default)
- Safari 5 with iOS 5.0
- Internet Explorer 8 with Windows 7 (TLS 1.2 is disabled by default on IE8-IE10)

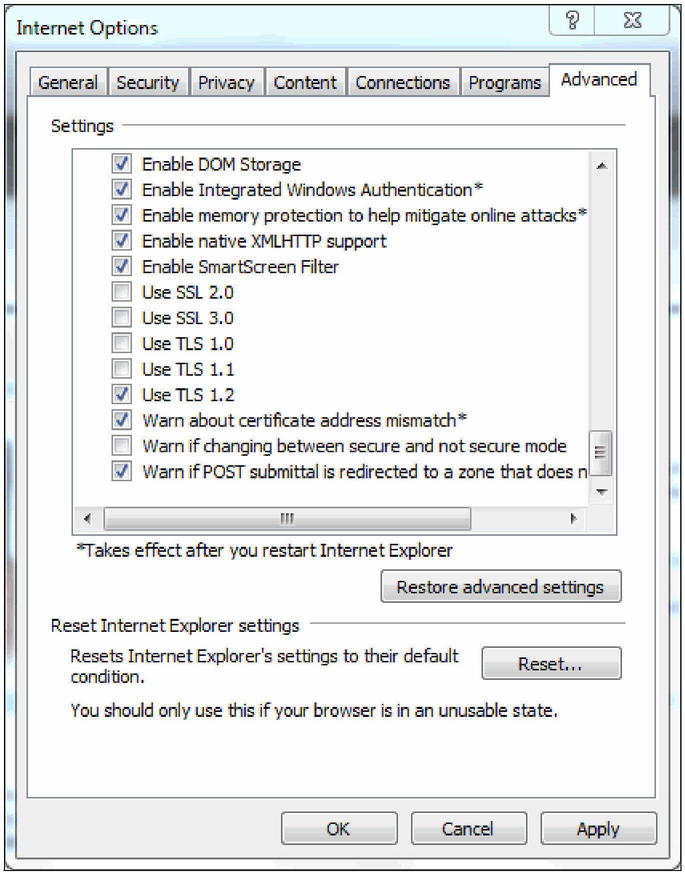
Browser setup example

To configure your browser for TLS 1.2, see the documentation for your browser. For example, in Microsoft Internet Explorer, complete the following steps:

1. Click **Tools** → **Internet Options**.

2. On the Advanced tab, under Settings, select **Use TLS 1.2**.

   The Internet Options window that is shown in Figure 6 opens. By default, the TLS 1.2 setting is disabled. Select it by selecting the corresponding check box.



☑ Enable DOM Storage
☑ Enable Integrated Windows Authentication*
☑ Enable memory protection to help mitigate online attacks*
☑ Enable native XMLHTTP support
☑ Enable SmartScreen Filter
☐ Use SSL 2.0
☐ Use SSL 3.0
☐ Use TLS 1.0
☐ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
☐ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart Internet Explorer

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Figure 6 Enabling MS Internet Explorer to use TLS 1.2

> **Important:** Ensure that all external browsers that access the DS Storage Manager and the DS Service GUI are configured for TLS 1.2. Otherwise, connections to these systems are lost.

Browser plug-in

The Storage Manager GUI server is running Java based software and is accessed by a browser. As a result, the browser that is used to access it must contain a Java plug-in to support the communication to the GUI in the HMC. This plug-in is separate from the Java software that might be running on the browser workstation. There are various versions of Java plug-ins that are available that support various security protocols.

When you set up the browser for TLS 1.2 protocol support, it is also necessary to ensure that you have a version of the Java plug-in that also supports TLS 1.2. The Java software that is installed on the workstation that supports TLS 1.2 includes the Java plug-in that supports TLS 1.2. But, you still must make sure that the browser that you are using has the TLS 1.2 supported plug-in installed and enabled. Currently, the known Java plug-ins that support TLS 1.2 are IBM Java Version 1.6 and Version 1.7, and Oracle Java Version 1.7.

Configuring the Web User Interface on the HMC

To make the DS8870 HMC Web User Interface (WUI) NIST SP 800-131a compliant, complete the following steps:

1. Check the current security level for your Web User Interface connection by running **showaccess**, as shown in Example 13. In this example, we use the **hmc1** parameter. If your system is a dual-HMC configuration, you can run **showaccess** in both HMCs.

   Example 13 Showing the security level of the WUI connection

   ```
   dscli> showaccess hmc1
   hmc           hmc1
   cmdline       enabled
   wui           disabled
   modem         disabled
   vpn           disabled
   port1750      enabled
   cim(security) legacy
   gui(security) legacy
   ni(security)  legacy
   wui(security) legacy
   ```

2. To change the security level of the HMC WUI to be NIST SP 800-131a compliant, run **manageaccess**, as shown in Example 14.

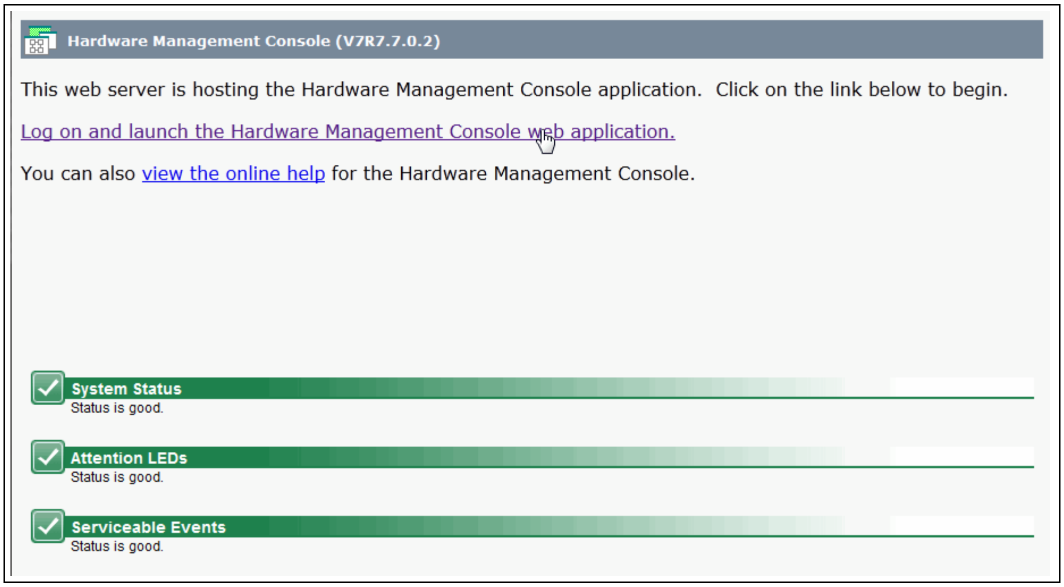
   Example 14 Changing the security level of the WUI

   ```
   dscli> manageaccess -ctrl wui -action setsecurity -level 800131a
   CMUC00463W manageaccess: Changing the security level of the DS WUI. If
   successfully, you must reboot the HMC in order for the change to take effect.
   Are you sure that you want to continue? [Y/N]: Y
   CMUC00212I manageaccess: completed successfully.
   dscli>
   ```

Important: After you run **manageaccess**, you must restart the HMC in order for the NIST SP 800-131A security setting to take effect.

To restart the HMC, complete the following steps:

1. Log in at the HMC, as shown in Figure 7. Click **Log on and launch the Hardware Management Console web application** to open the login window and log in. The default user ID is customer and the default password is cust0mer.



Hardware Management Console (V7R7.7.0.2)

This web server is hosting the Hardware Management Console application. Click on the link below to begin.

Log on and launch the Hardware Management Console web application.

You can also view the online help for the Hardware Management Console.

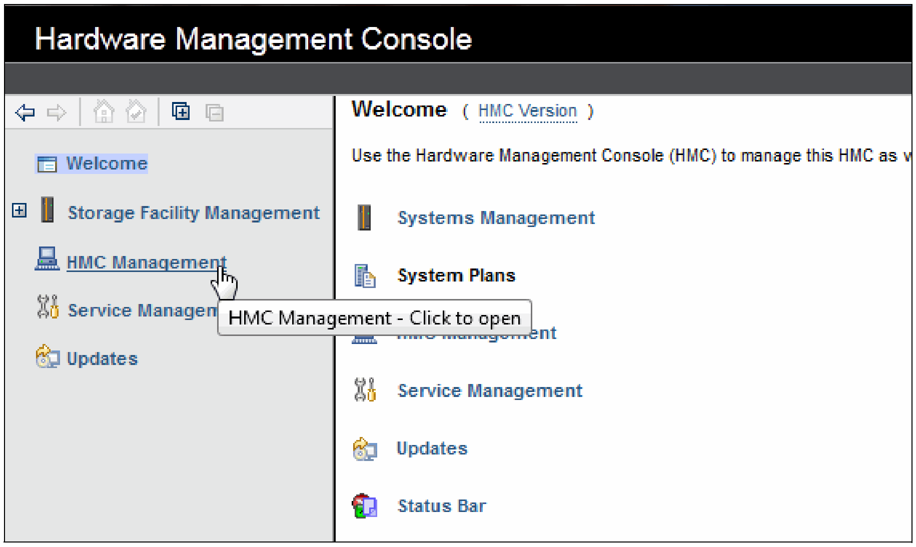
System Status
Status is good.

Attention LEDs
Status is good.

Serviceable Events
Status is good.

Figure 7 Hardware Management Console

2. If you log in successfully, you can see the HMC window. Click **HMC Management**, as shown in Figure 8.



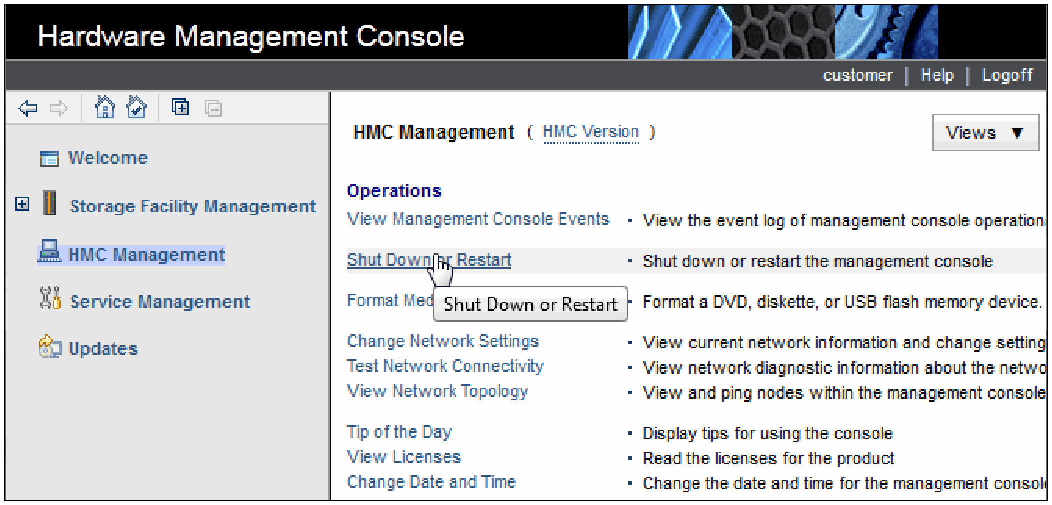
Hardware Management Console

Welcome (HMC Version)

Use the Hardware Management Console (HMC) to manage this HMC as v

Figure 8 Open HMC Management

3. In the HMC Management area, click **Shutdown or Restart**, as shown in Figure 9. Select **Restart HMC** and click **OK**.



Operations

View Management Console Events	View the event log of management console operation
Shut Down or Restart	Shut down or restart the management console
Format Med	Format a DVD, diskette, or USB flash memory device.
Change Network Settings	View current network information and change setting
Test Network Connectivity	View network diagnostic information about the netwo
View Network Topology	View and ping nodes within the management console
Tip of the Day	Display tips for using the console
View Licenses	Read the licenses for the product
Change Date and Time	Change the date and time for the management consol

Figure 9 Restart HMC

4. After you restart the HMC, you can check whether the security setting for WUI changed by running **`showaccess`**, as shown in Example 15.

Example 15 Checking the security level for WUI

```
dscli> showaccess hmc1
hmc           hmc1
cmdline       enabled
wui           disabled
modem         disabled
vpn           disabled
port1750      enabled
cim(security) legacy
gui(security) legacy
ni(security)  legacy
wui(security) 800131a
```

Important: If you have not changed the setting on your internet browser, you cannot access WUI remotely. Change the internet browser setting to support TLS 1.2.

For information about the internet browser setting, see “Web browser security setup” on page 14.

Configuring DS8870 remote access for NIST SP 800-131a

The DS8000 series can use Directory Services-based user authentication. This capability relies on the Lightweight Directory Access Protocol (LDAP). The benefits of a centralized user management approach can be substantial when you are faced with a large and complex overall IT environment. Maintaining local user management for each device is simple when the IT environment consists of a few users and a few DS8000 systems and other systems. For more information about LDAP Authentication with the DS8000, see *IBM System Storage DS8000: LDAP Authentication*, REDP-4505.

This section explains the steps to perform to make DS8000 remote access NIST SP 800-131a compliant.

If you access the DS8870 through the IBM Tivoli Productivity Center and want to use remote access login, you must install IBM Jazz™ for Service Management (Jazz SM) and IBM WebSphere® Application Server. Although the installation of WebSphere Application Server and Jazz SM is optional during the Tivoli Storage Productivity Center V5.2 installation, it is required for remote DS8000 security services.

For more information about installing Jazz SM and WebSphere Application Server, see the following website:

`http://pic.dhe.ibm.com/infocenter/tivihelp/v59r1/index.jsp`

The implementation of DS8870 remote access compliance with NIST SP 800-131A involves the following high-level tasks:

1. Configuring NIST SP 800-131A support for Jazz SM and WebSphere Application Server.
2. Creating a NIST SP 800-131A compliant truststore file for LDAP server.
3. Configuring the DS8870 security setting to be NIST SP 800-131A compliant.

Configuring NIST SP 800-131A support for Jazz SM and WebSphere Application Server

Jazz SM runs on top of WebSphere Application Server. To make Jazz SM NIST SP 800-131A compliant, you must configure the WebSphere Application Server to be NIST-compliant.

To configure the WebSphere Application Server for an LDAP connection, complete the following steps:

1. Log in to the WebSphere Application Server Integrated Solutions Console from a web browser. Use the following link to access the console:

   `https://yourserver.com:16316/ibm/console/logon.jsp`

You can define the Jazz for Service Management and WebSphere Application Server port in the `portdef.props` file in the Jazz SM installation directory. The default `portdef.props` file location for Windows Server is `C:\Program Files\IBM\ JazzSM\Profile\properties`, as shown in Figure 10.

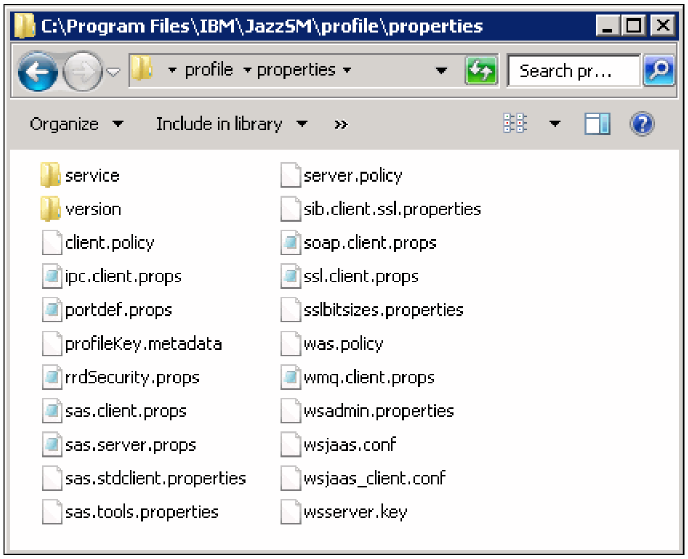


Figure 10 The portdef.port file location

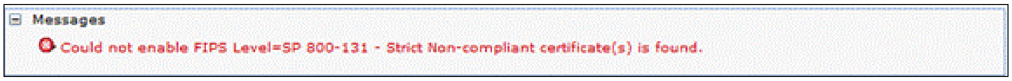
Example 16 shows the content of the `portdef.props` file, which lists port numbers that are used by the Jazz SM server. The default WebSphere Application Server Management console port is defined as `WC_adminhost_secure` with port number 16316.

Example 16 Portdef file content

```
WC_defaulthost_secure=16311
WC_defaulthost=16310
WC_adminhost_secure=16316
WC_adminhost=16315
BOOTSTRAP_ADDRESS=16312
SOAP_CONNECTOR_ADDRESS=16313
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=16319
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=16321
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=16320
ORB_LISTENER_ADDRESS=16318
DCS_UNICAST_ADDRESS=16317
IPC_CONNECTOR_ADDRESS=16314
REST_NOTIFICATION_PORT=16322
```

2. From the console, click **Security** → **SSL certificate and key management**, and under Related Items, click **SSL configurations**.
3. Click the **Node default SSL settings** link to open it, and under **Additional Properties**, click **Quality of protection (QoP) settings**.
4. For the protocol**,** ensure that **TLSv1.2** is selected; for the cipher suite groups, ensure that **Strong** is selected. Click **Update selected ciphers**.
5. Click **OK** and save directly to the master configuration.
6. Click the **SSL certificate and key management** link and then click **Manage FIPS**.
7. In the Manage FIPS window, click **Enable SP800-131** and then select **Strict**.

8. Click **OK**. If you see the non-compliant certificate error that is shown in Figure 11, complete the following steps:
   a. Under Related Items, click **Convert certificates**.
   b. Ensure that the Algorithm setting is Strict.
   c. For the New certificate key size, select **2048 bits**.
   d. Click **OK** and save directly to the master configuration.

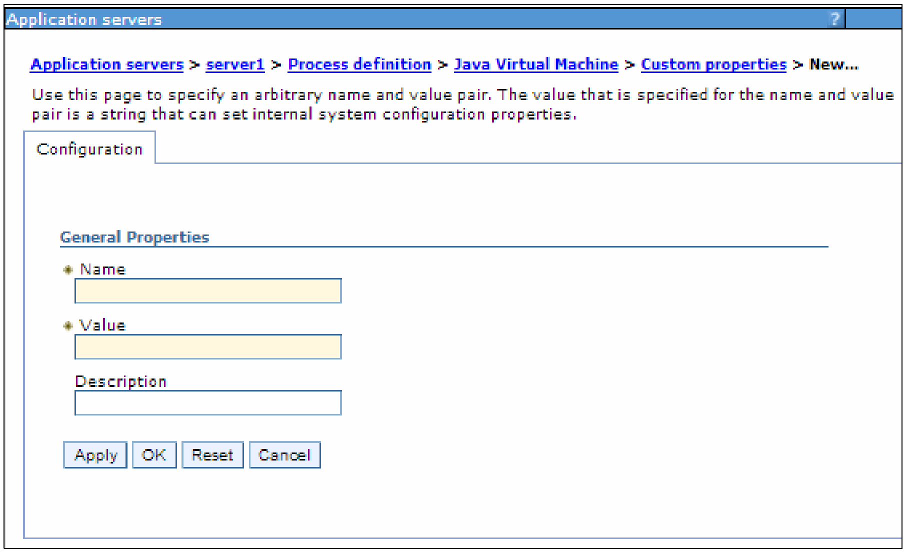


Messages

Could not enable FIPS Level=SP 800-131 - Strict Non-compliant certificate(s) is found.

Figure 11 Non-compliant certificate NIST SP 800-131a

9. In the Jazz SM installation directory, which is shown in Figure 10 on page 20, edit the `ssl.client.props` file with the following changes:
   a. Search for `com.ibm.security.useFIPS` and change the property to `true`.
   b. Search for `com.ibm.websphere.security.FIPSLevel` and if the line does not exist, add it, and then set the property to `SP800-131`.
   c. Search for `com.ibm.ssl.protocol` and change the property to `TLSv1.2`.
10. In the WebSphere Application Server management web window, click **Server** → **Server Types** → **WebSphere application servers** and then click **server1** to open it.
11. Under Server Infrastructure, click **Java and Process Management** → **Process definition**.
12. Under Additional Properties, click **Java Virtual Machine** and then click **Custom properties**.
13. Click **New**, and add the following three custom properties, one at a time (see Figure 12):
    - com.ibm.team.repository.transport.client.protocol with a value of TLSv1.2
    - com.ibm.jsse2.sp800-131 with a value of strict
    - com.ibm.rational.rpe.tls12only with a value of true



Application servers

Application servers > server1 > Process definition > Java Virtual Machine > Custom properties > New...

Use this page to specify an arbitrary name and value pair. The value that is specified for the name and value pair is a string that can set internal system configuration properties.

Configuration

General Properties

* Name

* Value

Description

Figure 12 New Java Virtual Machine Custom properties

14. Restart the application server by completing the following steps:

   a. In the command prompt window, change your directory to `JazzSM_install_directory\profile\bin`.

   b. Stop the Jazz for Service Management by running the following command, where **`server1`** is the default Jazz SM profile name, and **`user_name`** and **`password`** is the server administrator user ID and password combination:

```
stopServer.bat server1 -username user_name -password password
```

   c. Start the Jazz for Service Management server by running the following command, where **`server1`** is the default Jazz SM profile name:

```
startServer.bat server1
```

Creating a NIST SP 800-131A-compliant truststore file for an LDAP server

The certificate and the truststore file from the Jazz SM server are required for Secure Sockets Layer (SSL) communication between the DS8000 HMC and the Tivoli Storage Productivity Center server. NIST SP 800-131A compliance requires at least a 2048-bit strength truststore file.

Extracting the certificate from WebSphere Integrated Solutions Console

To accomplish this task, complete the following steps:

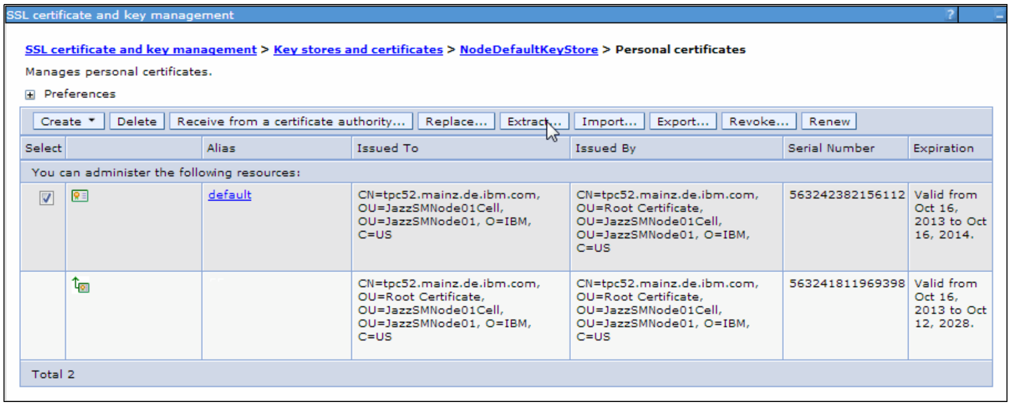
1. Open a web browser and enter the following address in to the Address field to access the WebSphere Integrated Solutions Console:

   `https://`*`yourserver.com`*`:16316/ibm/console`

2. Export the certificate:

   a. Log in to the WebSphere Integrated Solutions console.

   b. In the WebSphere Integrated Solutions Console navigation tree, click **Security** → **SSL certificate and key management** → **Key stores and certificates** → **NodeDefaultKeyStore** → **Personal Certificates**. Select the default certificate and click **Extract**, as shown in Figure 13.



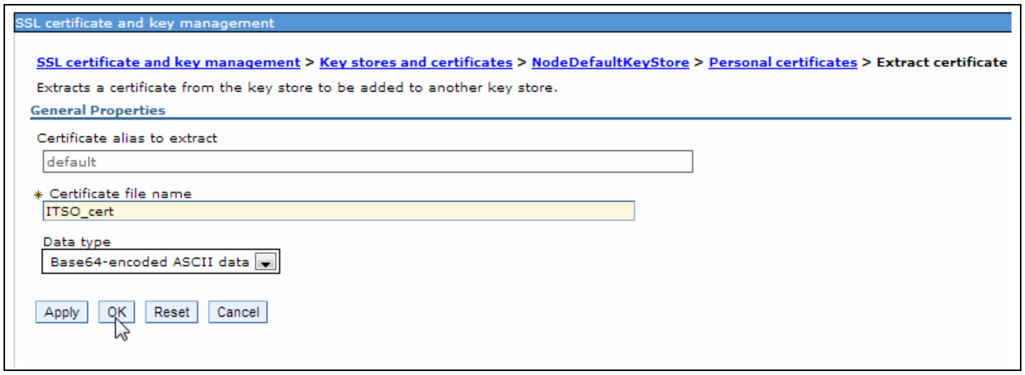
SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates

Manages personal certificates.

Select		Alias	Issued To	Issued By	Serial Number	Expiration
You can administer the following resources:						
☑		default	CN=tpc52.mainz.de.ibm.com, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	CN=tpc52.mainz.de.ibm.com, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	563242382156112	Valid from Oct 16, 2013 to Oct 16, 2014.
			CN=tpc52.mainz.de.ibm.com, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	CN=tpc52.mainz.de.ibm.com, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	563241811969398	Valid from Oct 16, 2013 to Oct 12, 2028.
Total 2						

Figure 13 Certificate extraction from WebSphere Integrated Solutions Console

c. Enter a file name for the extracted certificate, as shown in Figure 14. The file automatically is created in the `Jazz SM_Directory/profile/etc/` directory. In the Windows operating system, the default directory is `C:\JazzSM_Directory\profile\etc\`. Accept and select the default data type and click **OK**.


SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates > Extract certificate

Extracts a certificate from the key store to be added to another key store.

General Properties

Certificate alias to extract: default

* Certificate file name: ITSO_cert

Data type: Base64-encoded ASCII data

Figure 14 Insert certificate extraction name

Creating a NIST SP 800-131A-compliant truststore file

Create the truststore file and import the certificate into the truststore file by using the iKeyman tool. Complete the following steps:

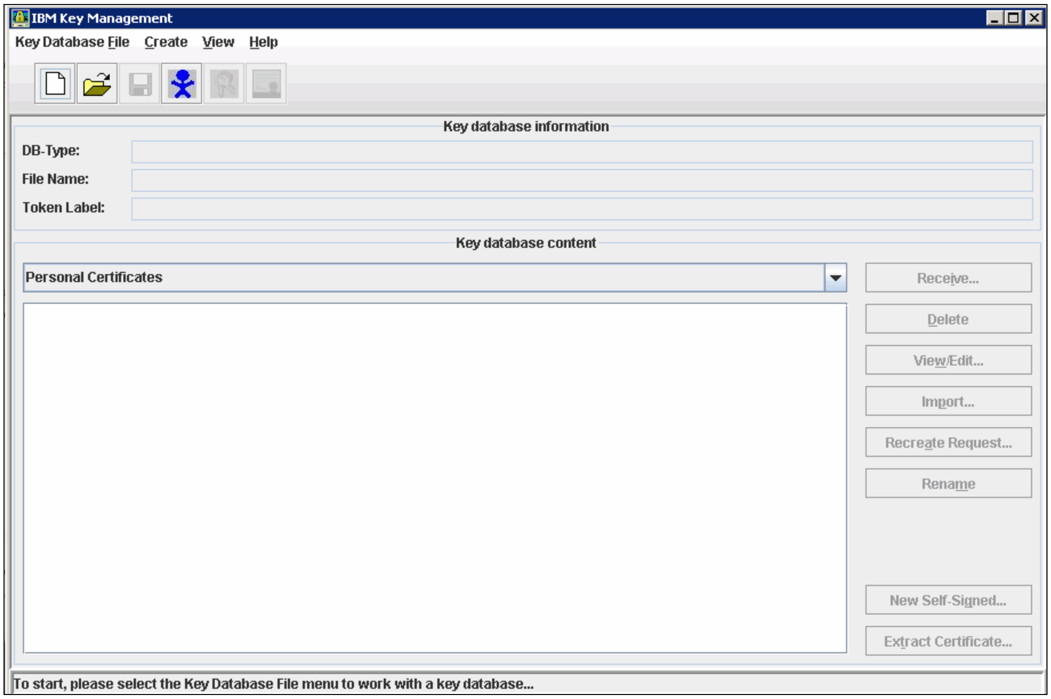
1. For example, in Windows Server 2008, open a command prompt window and enter the following command to open the IBM Key Management window:

   ```
   JazzSM_install_dir\profile\bin\ikeyman.bat
   ```

   The iKeyman utility is a GUI-based tool that you can use to manage your digital certificates. With iKeyman, you can create a key database or test a digital certificate, add certificate authority (CA) roots to your database, copy certificates from one database to another, request and receive a digital certificate from a CA, set default keys, and change passwords.

   A *certificate authority* is a trusted central administrative entity that can issue digital certificates to users and servers. The trust in the CA is the foundation of trust in the certificate as a valid credential. A CA uses its private key to create a digital signature on the certificate that it issues to validate the certificate's origin. Others can use the CA certificate's public key to verify the authenticity of the certificates that the CA issues and signs. The term *truststore* refers to a special designation that is given to a CA certificate. This truststore designation allows a browser or other application to authenticate and accept certificates that the CA issues.

2. In the IBM Key Management window (Figure 15), click **Key Database File** → **New**.

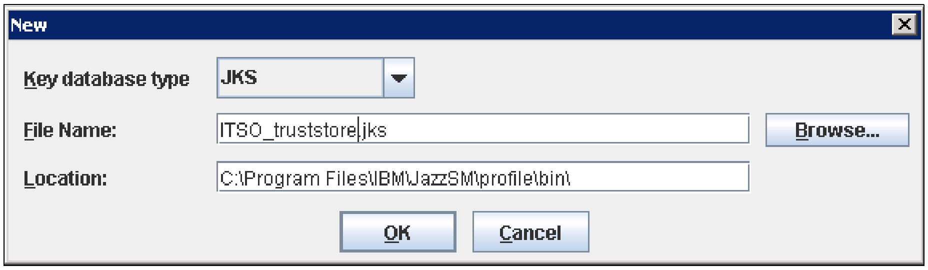


Personal Certificates

To start, please select the Key Database File menu to work with a key database...

Figure 15 iKeyman window

3. In the New window (Figure 16), for Key database type, select a type or leave the default of JKS, and for File Name, enter a truststore file name. For example, enter itso_key.jks.



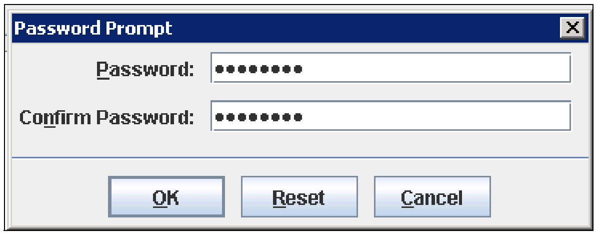
Key database type: JKS

File Name: ITSO_truststore.jks

Location: C:\Program Files\IBM\JazzSM\profile\bin\

Figure 16 Setting the truststore location and file name

4. In the Password Prompt window that is shown in Figure 17, specify a password for the truststore file, reconfirm the password, and click **OK**. The truststore file is created, and you return to the IBM Key Management window.

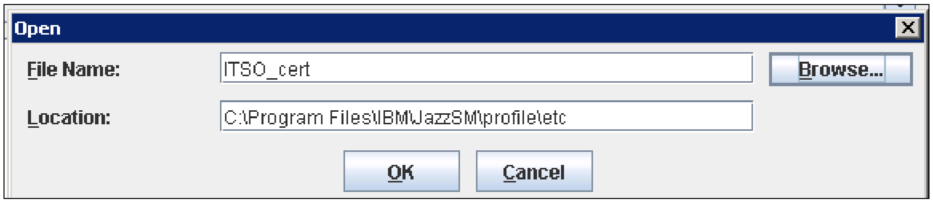


Password: ••••••••

Confirm Password: ••••••••

Figure 17 Confirm truststore password

5. Import the certificate into the truststore file by running the following steps:
   a. Add the exported certificate file from the Jazz SM to the truststore file.
   b. From the IBM Key Management window (see Figure 18), click **Add**.



File Name: ITSO_cert

Location: C:\Program Files\IBM\JazzSM\profile\etc

Figure 18 Select certificate authority

   c. In the Add CA certificate from a file window, click **Browse**.
   d. Select the certificate file that you previously created and click **OK**.
   e. In the Enter a Label window, enter any label (any character string of your choice). For example, we enter itso_cert_label. Click **OK**.

      The certificate is successfully stored in the truststore file.
   f. Exit the iKeyman tool and find the truststore file. In our example, the file is in the following location:

      ```
      c:\Program Files\IBM\tivoli\tip\bin\itso_trust_store.jks
      ```

You need this truststore file and password while configuring the LDAP-based policy on the DS8000 server.

Configuring a DS8870 for LDAP authentication for a NIST SP 800-131a-compliant environment

To configure LDAP authentication, you can use either the DS GUI or the DS CLI.

> **Important:** You must make sure that your DS8870 is configured to be NIST SP 800-131A-compliant before you configure remote authentication.

Configuring DS8000 authentication using DS CLI

Complete the following steps:

1. Go to the DS CLI installation directory and open the DS CLI command window.
2. In the DS CLI command window, enter the HMC IP Address, User Name, and Password.
3. To check the existing Authentication policies, run `lsauthpol`, as shown in Example 17. The default initialPolicy is set for basic (non-LDAP) authentication.

Example 17 Checking the authentication policy

```
dscli> lsauthpol
name          type  state
==========================
initialPolicy Basic active
```

4. Create an empty policy where the **`-type sas`** parameter specifies the authentication policy type. To accomplish this, run **`mkauthpol -type sas ITSOPol`**, as shown in Example 18. Currently, `sas` (Storage Authentication Service) is the only valid value for this parameter, and it is required. ITSOPol defines the name of the new policy.

Example 18 Creating an authentication policy

```
dscli> mkauthpol -type sas ITSOPol
CMUC00365I mkauthpol: The authentication policy ITSOPol has been created.
```

5. Add a policy server or policy servers to the policy, as shown in Example 19, by running the **`setauthpol`** command with the **`-action setauthserver`** and **`-loc`** parameters, where the **`-loc`** parameter is the URL for the Jazz SM server.

Example 19 Setting the policy server

```
dscli> setauthpol -action setauthserver -loc
https://9.155.50.162:16311/TokenSer
vice/services/Trust ITSOPol
CMUC00366I setauthpol: The authentication policy ITSOPol has been modified.
```

> **Default port:** The default port number that is used by Jazz SM is 16311. You can check the default port of your Jazz SM server by checking the **`WC_defaulthost_secure`** parameter in the `portdef.props` file. To learn more about checking the port number that you use, see “Configuring NIST SP 800-131A support for Jazz SM and WebSphere Application Server” on page 19. The Authentication Service URL is the following one:
>
> `https://yourserver.com:13611/TokenService/services/Trust`

6. Add the keystore file to the policy. Run **`setauthpol`** with the **`-action settruststore`** and **`-loc`** parameters, where the value is the location of the truststore file (see “Creating a NIST SP 800-131A-compliant truststore file for an LDAP server” on page 22), and with the **`-pw`** parameter for the truststore file password. Example 20 shows the running of this command and its output.

Example 20 Setting the truststore file

```
dscli> setauthpol -action settruststore -loc C:\ITSO_truststore.jks -pw
passw0rd
 ITSOPol
CMUC00366I setauthpol: The authentication policy ITSOPol has been modified.
```

7. Add the user of the policy by running **`setauthpol`** with the **`-action setsasuser`** parameter, as shown in Example 21.

Example 21 Setting a user

```
dscli> setauthpol -action setsasuser -username itsouser -pw passw0rd ITSOPol
CMUC00366I setauthpol: The authentication policy ITSOPol has been modified.
```

8. Map existing users and user groups from the LDAP server to user groups on the DS8000 by running setauthpol with the **`-action setmap`** and **`-groupmap User:Group`** parameters, as shown in Example 22.

Example 22 Mapping a user to a group

```
dscli> setauthpol -action setmap -groupmap admin:Administrators ITSOPol
CMUC00366I setauthpol: The authentication policy ITSOPol has been modified.
```

9. Now that the policy is set up, check it by running the command that is shown in Example 23. The policy is now in the inactive state.

Example 23 Listing the available authentication policy

```
dscli> lsauthpol
name          type  state
============================
ITSOPol       SAS   inactive
initialPolicy Basic active
```

10. To view the authentication policy configuration, run **showauthpol**, as shown in Example 24.

Example 24 Showing the authentication policy configuration

```
dscli> showauthpol ITSOPol
name     ITSOPol
type     SAS
state    inactive
location https://9.155.50.162:16311/TokenService/services/Trust
truststore ITSOPol_trustStore.jks
sasuser    itsouser
```

11. Test the configuration by running **testauthpol**, as shown in Example 25.

Example 25 Testing the authentication policy

```
dscli> testauthpol -username itsouser -pw passw0rd ITSOPol
CMUC00371I testauthpol: The authentication policy ITSOPol has been
authenticated
 on location https://9.155.50.162:16311/TokenService/services/Trust
```

12. If the test completes successfully, active the policy by running **chauthpol** with the **-activate** parameter, as shown in Example 26.

Example 26 Activating the authentication policy

```
dscli> chauthpol -quiet -activate -username itsouser -pw passw0rd ITSOPol
CMUC00369I chauthpol: The authentication policy ITSOPol has been modified.
```

13. Check the state of the policy by running l**sauthpol**, as shown in Example 27.

Example 27 Listing the policy

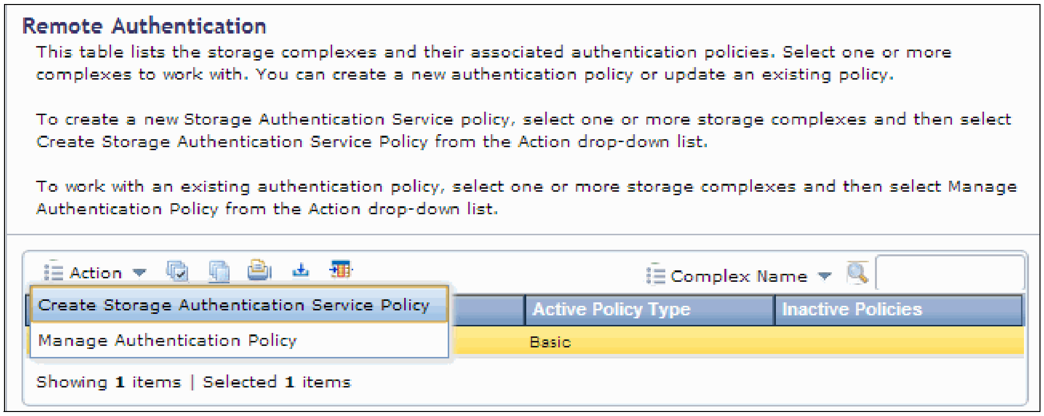
```
dscli> lsauthpol
name          type  state
============================
ITSOPol       SAS   active
initialPolicy Basic inactive
```

Configuring DS8000 authentication by using the DS GUI

To configure DS8000 LDAP authentication by using the DS GUI, complete the following steps:

1. Open the DS GUI with the administrative user ID and password. Enter the User Name and Password and click **OK**.

2. In the DS8000 Storage Manager menu (left pane), hover over the **Access** menu, and select **Remote Authentication**. Select **IbmStoragePlex**, click **Action**, and select **Create Storage Authentication Service Policy**, as shown in Figure 19.



Remote Authentication

This table lists the storage complexes and their associated authentication policies. Select one or more complexes to work with. You can create a new authentication policy or update an existing policy.

To create a new Storage Authentication Service policy, select one or more storage complexes and then select Create Storage Authentication Service Policy from the Action drop-down list.

To work with an existing authentication policy, select one or more storage complexes and then select Manage Authentication Policy from the Action drop-down list.

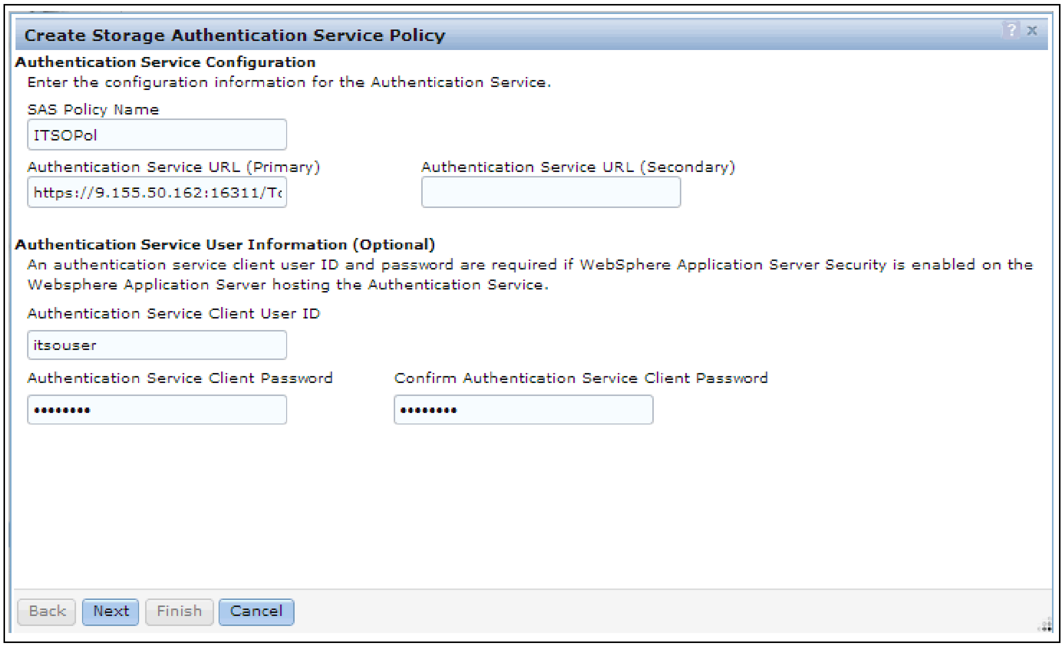
Action
Complex Name
Create Storage Authentication Service Policy
Manage Authentication Policy
Active Policy Type
Inactive Policies

Active Policy Type	Inactive Policies
Basic	

Showing 1 items | Selected 1 items

Figure 19 Select Create Storage Authentication Service policy

3. In the Create Storage Authentication Service Policy window (Figure 20), complete the following steps.



Create Storage Authentication Service Policy

Authentication Service Configuration

Enter the configuration information for the Authentication Service.

SAS Policy Name: ITSOPol

Authentication Service URL (Primary): https://9.155.50.162:16311/Tc

Authentication Service URL (Secondary):

Authentication Service User Information (Optional)

An authentication service client user ID and password are required if WebSphere Application Server Security is enabled on the Websphere Application Server hosting the Authentication Service.

Authentication Service Client User ID: itsouser

Authentication Service Client Password: ••••••••

Confirm Authentication Service Client Password: ••••••••

Figure 20 Create Storage Authentication Service Policy window

a. For Policy Name, enter any name. You can define more than one policy, but only one can be active. You can also switch freely between the different policies.

b. For Authentication Service URL (Primary), enter the URL to the Jazz SM. The following URL is the default to the truststore:

```
https://yourserver.com:16311/TokenService/services/Trust
```

c. For Authentication Service URL (Secondary), enter the backup URL that points to your secondary Jazz SM. Although this is not necessary, it is preferable to have redundant Jazz SM servers and LDAP servers for DS8000 authentication to LDAP. If the remote authentication is not available, you cannot log on to a DS8000 that has remote authentication enabled to perform administrative tasks.

d. For Authentication Service Client User ID, enter the user ID from the Jazz SM that is set up by installation.

e. For Authentication Service Client Password, enter the password from the Jazz SM user.

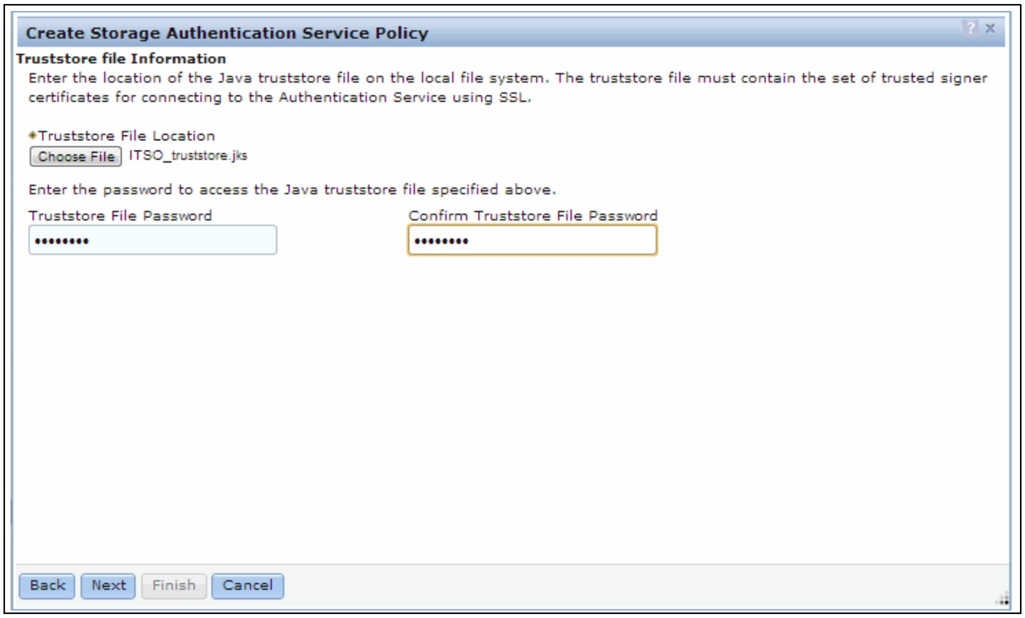
f. For Confirm Authentication Service Client Password, enter the password again, and then click **Next**.

4. In the Truststore file Information window (Figure 21):

a. For Truststore File Location, enter the NIST SP 800-131A-compliant truststore directory that you created. For more information, see “Creating a NIST SP 800-131A-compliant truststore file” on page 23.

b. For Truststore File Password, enter the password that was entered when the truststore was created.

c. For Confirm Truststore File Password, enter the password again, and then click **Next**.



Create Storage Authentication Service Policy

Truststore file Information

Enter the location of the Java truststore file on the local file system. The truststore file must contain the set of trusted signer certificates for connecting to the Authentication Service using SSL.

*Truststore File Location

Choose File ITSO_truststore.jks

Enter the password to access the Java truststore file specified above.

Truststore File Password: ••••••••

Confirm Truststore File Password: ••••••••

Figure 21 Truststore file Information window

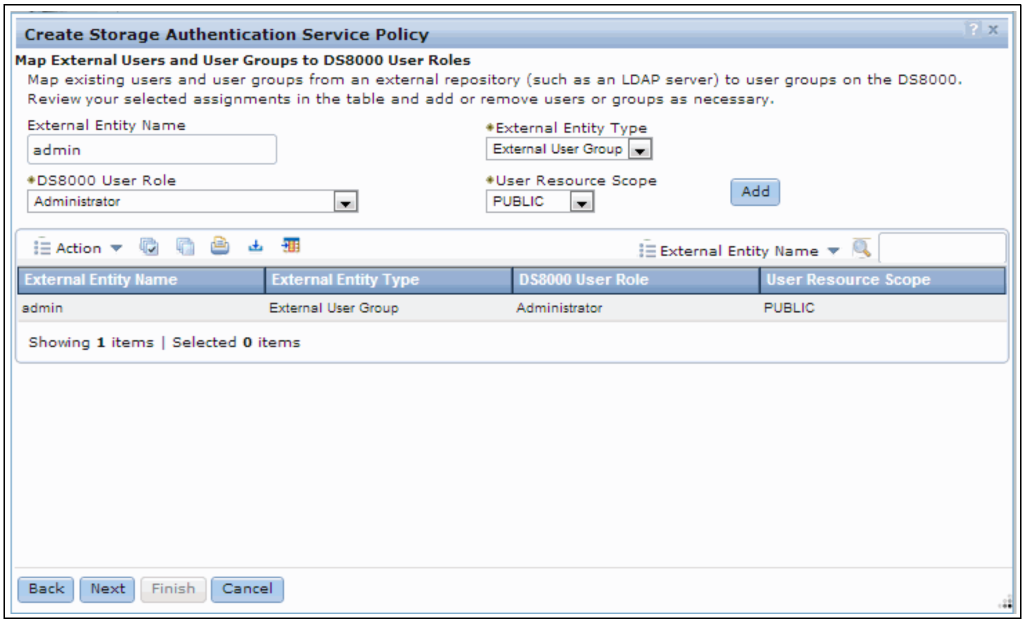
5. In the Map External Users and User Groups to DS8000 User Roles window (Figure 22):

   a. For External Entity Name, enter the name of the user or user group that exists in the LDAP directory.

   b. Select the External Entity Type. The type of entity can be External User Group or External User Name.

   c. For DS8000 User Role, select a role from the list, and then click **Add**.

   d. To map more than one user or group, repeat these steps. Click **Next**.



Create Storage Authentication Service Policy

Map External Users and User Groups to DS8000 User Roles

Map existing users and user groups from an external repository (such as an LDAP server) to user groups on the DS8000. Review your selected assignments in the table and add or remove users or groups as necessary.

External Entity Name: admin

*External Entity Type: External User Group

*DS8000 User Role: Administrator

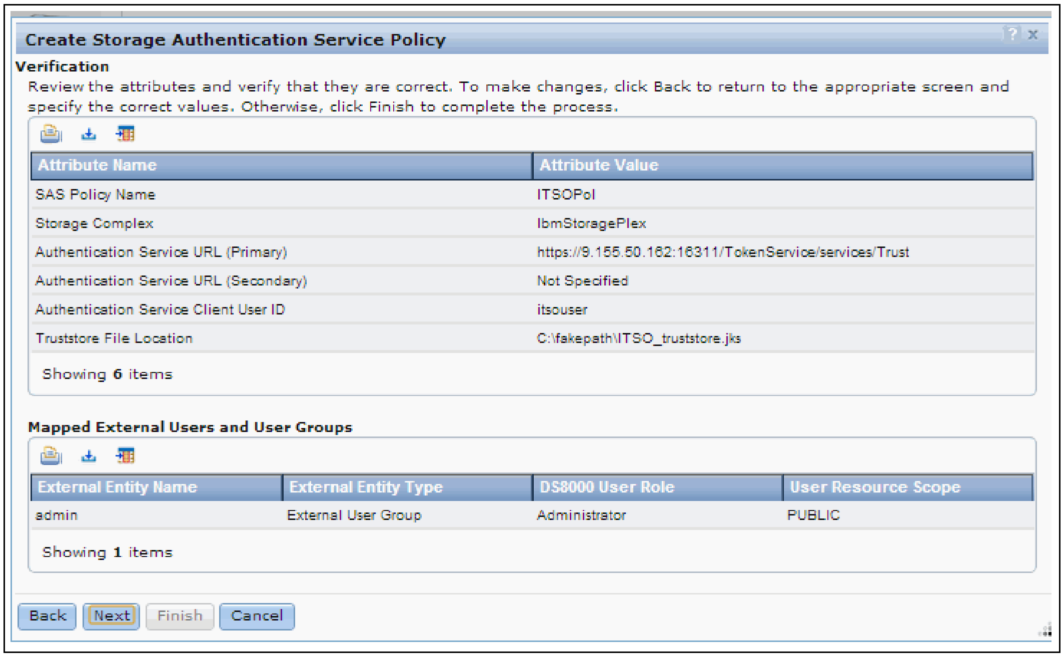
*User Resource Scope: PUBLIC

External Entity Name	External Entity Type	DS8000 User Role	User Resource Scope
admin	External User Group	Administrator	PUBLIC

Showing **1** items | Selected **0** items

Figure 22 Map External Users and User Groups to DS8000 User Rules window

6. In the Verification window (Figure 23), you can see the settings that will be stored. Verify the information and click **Next** to continue or click **Back** to make changes.



Create Storage Authentication Service Policy

Verification

Review the attributes and verify that they are correct. To make changes, click Back to return to the appropriate screen and specify the correct values. Otherwise, click Finish to complete the process.

Attribute Name	Attribute Value
SAS Policy Name	ITSOPol
Storage Complex	IbmStoragePlex
Authentication Service URL (Primary)	https://9.155.50.162:16311/TokenService/services/Trust
Authentication Service URL (Secondary)	Not Specified
Authentication Service Client User ID	itsouser
Truststore File Location	C:\fakepath\ITSO_truststore.jks

Showing 6 items

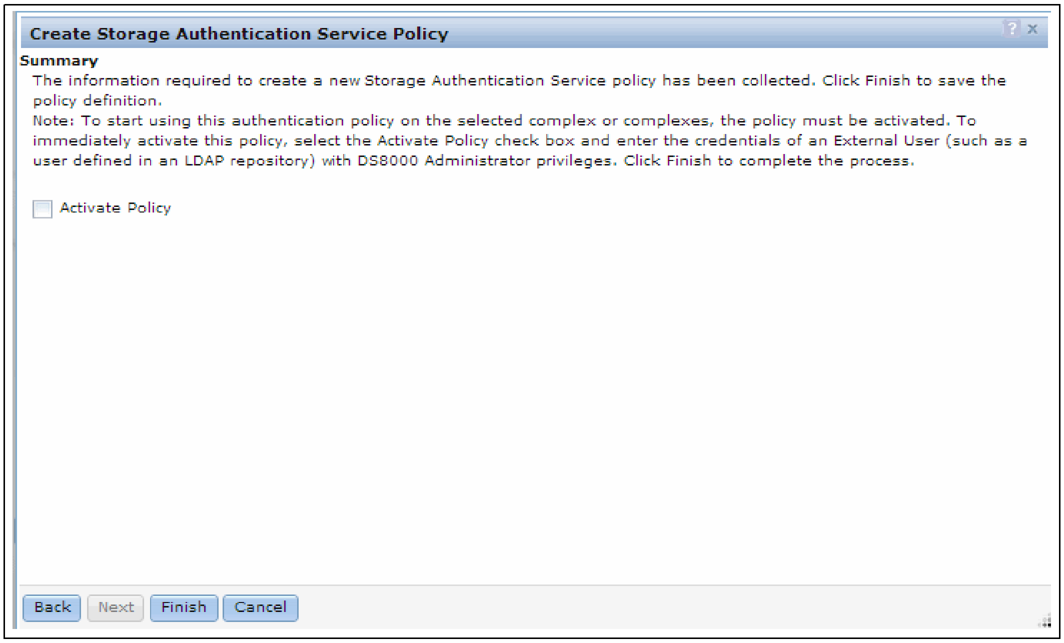
Mapped External Users and User Groups

External Entity Name	External Entity Type	DS8000 User Role	User Resource Scope
admin	External User Group	Administrator	PUBLIC

Showing 1 items

Figure 23 Verification window

7. In the Summary window (Figure 24), leave the Activate the Policy check box cleared. In the next step, you test the policy before you activate it. Click **Finish** to create the policy.



Create Storage Authentication Service Policy

Summary

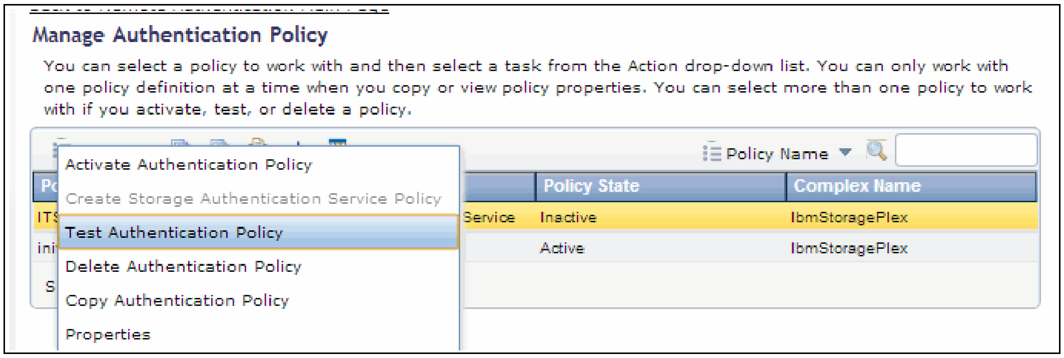
The information required to create a new Storage Authentication Service policy has been collected. Click Finish to save the policy definition.

Note: To start using this authentication policy on the selected complex or complexes, the policy must be activated. To immediately activate this policy, select the Activate Policy check box and enter the credentials of an External User (such as a user defined in an LDAP repository) with DS8000 Administrator privileges. Click Finish to complete the process.

□ Activate Policy

Figure 24 Summary window

8. On the Manage Authorization Policy window (Figure 25), select a policy. Under the Action menu, click **Test Authentication Policy**.



Manage Authentication Policy

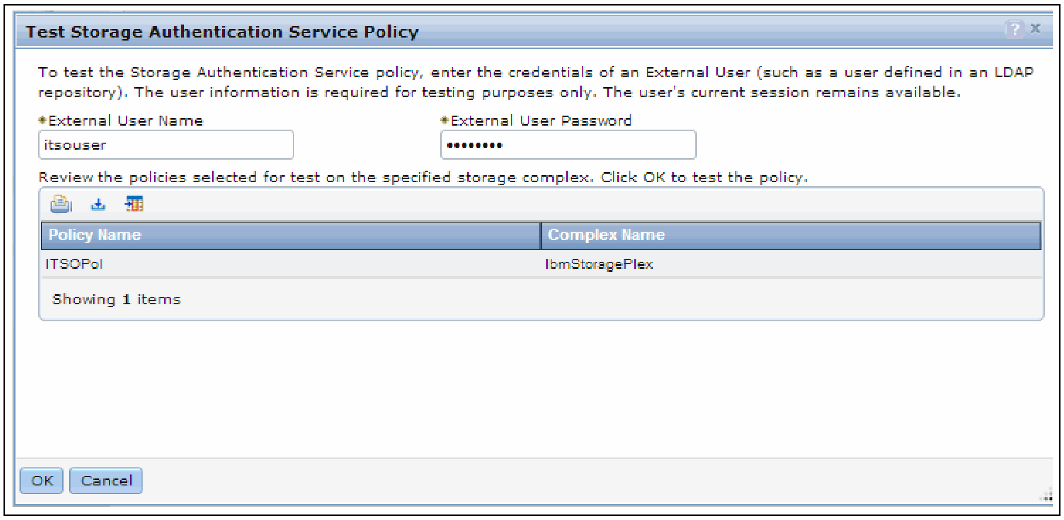
You can select a policy to work with and then select a task from the Action drop-down list. You can only work with one policy definition at a time when you copy or view policy properties. You can select more than one policy to work with if you activate, test, or delete a policy.

Policy Name
Activate Authentication Policy
Create Storage Authentication Service Policy
Test Authentication Policy
Delete Authentication Policy
Copy Authentication Policy
Properties
Po
Policy State
Complex Name
ITS
Service
Inactive
IbmStoragePlex
ini
Active
IbmStoragePlex
S

Figure 25 Test Authentication Policy

9. In the Test Storage Authentication Service Policy window (Figure 26), enter values for the External User Name and External User Password fields. The user must be an existing user from the LDAP Directory and mapped to a local DS8000 role. Click **OK**.

   The test takes a few seconds to complete. When complete, the Test summary window opens only if there is something wrong; the Result Status cell is red and the error messages are displayed in the Result details box. In that case, go back to the configuration and check the settings.



Test Storage Authentication Service Policy

To test the Storage Authentication Service policy, enter the credentials of an External User (such as a user defined in an LDAP repository). The user information is required for testing purposes only. The user's current session remains available.

*External User Name: itsouser

*External User Password: ••••••••

Review the policies selected for test on the specified storage complex. Click OK to test the policy.

Policy Name	Complex Name
ITSOPol	IbmStoragePlex

Showing 1 items

Figure 26 Test Storage Authentication Service Policy

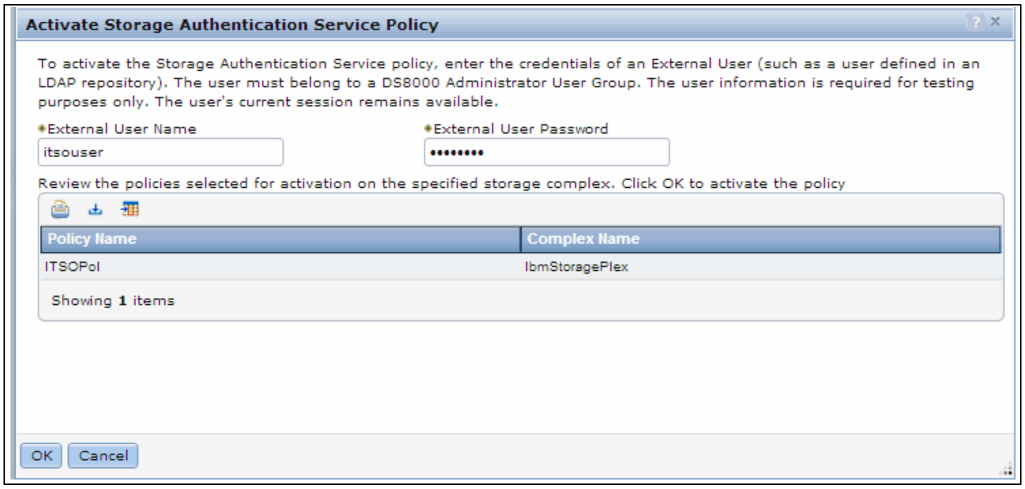
10. Activate the configuration. Select a policy. Under the Action menu, click **Activate**.

11. In the Activate Storage Authentication Service Policy window (Figure 27), complete the following steps:

    a. For External User Name, enter a name that exists and is valid user name from the LDAP Directory.

    b. Enter the External User password.

    c. Click **OK** to activate the policy.



Activate Storage Authentication Service Policy

To activate the Storage Authentication Service policy, enter the credentials of an External User (such as a user defined in an LDAP repository). The user must belong to a DS8000 Administrator User Group. The user information is required for testing purposes only. The user's current session remains available.

*External User Name: itsouser

*External User Password: ••••••••

Review the policies selected for activation on the specified storage complex. Click OK to activate the policy

Policy Name	Complex Name
ITSOPol	IbmStoragePlex

Showing 1 items

Figure 27 Activate Storage Authentication Service Policy window

Encryption and key server compliance

Enabling disk encryption on the DS8870 requires an external key server that is implemented by the IBM Security Key Lifecycle Manager.

This section describes the steps to configure the key servers and achieve NIST SP 800-131a compliance and security objectives.

There are two aspects of the configuration that need to change to enable compliance with NIST SP 800-131a:

- The IBM Security Key Lifecycle Manager (SKLM) Version 2.5 uses an IBM proprietary protocol (IPP), which is NIST SP 800-131a compliant, to communicate with the Hardware Management Console (HMC). However, it is a preferred practice to use TLS 1.2 for HMC network communications.
- The second change is to use the Gen-2 certificate on the DS8870 that is running Release 7.2 microcode. DS8000 has used a Gen-1 certificate since the introduction of disk encryption in March 2009. The Gen-1 certificate provides 80-bit encryption strength. The Gen-2 certificate provides 112-bit encryption strength and is required for NIST SP 800-131a compliance.

NIST SP 800-131a requirements for key servers

The DS8870 uses key servers to manage certificates and data keys that are associated with data encryption. If one or more key servers are configured on the DS8870, the HMC initiates periodic connections to the key servers to monitor whether the key servers are accessible. When an encryption group or recovery key is configured on the DS8870, the HMC initiates connections to the key servers to request key services and periodically verifies that any active data keys are valid on all configured key servers.

The DS8870 supports the following key servers:

- IBM Security Key Lifecycle Manager
- IBM Security Key Lifecycle Manager for z/OS®

Encryption key servers use a secure connection with the Hardware Management Console (HMC) using, by default, an IBM Proprietary Protocol (IPP). IPP uses a digital certificate to authenticate the key client with the key server and has data security for the data keys that are passed between the key client and server. However, TLS 1.2 also can be enabled. IBM Security Key Lifecycle Manager V2.5 also ships with an NIST SP 800-131a-compliant Java level to meet compliance requirements. Using TLS 1.2 is preferred even if NIST SP 800-131a compliance is not required in your environment.

The periodic key server accessibility monitoring is implemented in DSNI server on the HMC. The key services requests and periodic data key validation are implemented in the key client in the storage facility image. The key client also communicates through the DSNI server.

For more information about the IBM distributed key servers, go to the following website:

https://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.sklm.doc_2.5/welcome.htm

Configuring SKLM V2.5 to use TLS 1.2

The SKLM V2.5 key servers and DS8870 are not configured by default to use TLS 1.2 for SKLM to HMC communication. The SSL certificate on the SKLM must be exported and configuration changes for security access level on the DS8870 are required.

The DS GUI does not support making these changes; The SKLM command line and DS CLI must be used to make the changes.

First, export the IBM SKLM SSL certificate, and then investigate the security access level on the DS8870. If needed, change the security access level on the DS8870 and redefine the key servers to use TLS 1.2.

Complete the following steps:

1. Initiate a command-line interface (CLI) session on the SKLM server. Modify the configuration file to enable TLS 1.2 communication with the HMC. Example 28 shows the commands to run and shows the changes that are required in the configuration file.

   Example 28 Changing the SKLM configuration properties file

   ```
   1. cd /opt/IBM/WebSphere/AppServer/products/sklm/config
   2. vi SKLMConfig.properties
   3. change following line:
      TransportListener.ssl.protocols=SSL_TLSv2  ----> add v2
   4. Add following line at the end of the file.
      requireSHA2Signatures=true
   ```

```
Step 3 will configure the SKLM to support TLS 1.2.

Step 4 will configure SKLM to take connections from a client that is in NIST SP
800-131a compliance mode.

If you are not ready to implement TLS 1.2 communication, do not perform Step 4
to add requireSHA2Signatures=true to the last line of SKLMConfig.properties.
```

2. Log in to the SKLM GUI to create an SSL certificate. Only one SSL certificate can be active; if an SSL certificate exists, it becomes inactive.
3. Log in to the SKLM CLI to identify the active SSL certificate. This certificate must be exported to a file for use when defining key servers on the DS8870. Example 29 shows the steps that are required to identify the active SSL certificate.

Example 29 Identify the active SSL certificate on the SKLM

```
1. cd /opt/IBM/WebSphere/AppServer/bin
2. ./wsadmin.sh -username SKLMAdmin -password passw0rd -lang jython
3. wsadmin> print AdminTask.tklmCertList('[-usage SSLSERVER -v y]')
CTGKM0001I Command succeeded.
CTGKM0661I  Found 1 certificates.

uuid
CERTIFICATE-51e37703-e625-41ac-a050-2c76c68c875a
alias                               ssl_tklm6
information                         null
key store name                      defaultKeyStore
key store uuid                      DUMMY-KEYSTORE-1
owner                               null
key state                           ACTIVE
issuer name                         CN=ssl_tklm6
subject name                        CN=ssl_tklm6
activation date                    10/23/13 7:49:34 PM Central European Summer
Time
archive date                        null
compromise date                     null
creation date                      10/23/13 7:49:34 PM Central European Summer
Time
expiration date                    10/21/23 7:49:34 PM Central European Summer
Time
destroy date                        null
trusted                             1
has private key                     TRUE
serial number                       800958824665661
...

This example shows the default user name and password for the SKLM, change to
user name and password as needed for your configuration.
The uuid shows the certificate that needs to be exported and the key state
shows the active certificate.
```

4. Export the certificate to a file. Example 30 shows the commands that are required to export the SSL certificate.

Example 30   Export the SSL certificate from the SKLM

```
1. cd /opt/IBM/WebSphere/AppServer/bin
2. ./wsadmin.sh -username SKLMadmin -password passw0rd -lang jython
3. wsadmin> print AdminTask.tklmCertExport('[-uuid
CERTIFICATE-a74a853c-4421-4af9-ad29-50062d8dad6d -fileName
/tmp/tklm6_ssl_certificate.crt]')

This creates a file in /tmp with the exported certificate. This file will need
to be added to the file system where DS CLI is running, it will be used when
the key servers are defined to the DS8870.
```

5. Log out of the SKLM. Log in to the DS8870 with DS CLI with *storage administrator* authority. If the key servers already are defined to the DS8870, then continue with this step. If no key servers are defined, then continue with step 6 to install the new certificate that was exported from the SKLM in 4. Example 31 shows how to remove one of the key servers; perform steps 5 and 6 for only one key server.

Example 31   Commands to remove a key server

```
dscli> lskeymgr -l
Date/Time: October 23, 2013 9:40:33 AM MST IBM ...
ID  state   status addr         port
====================================
1   active  normal 9.155.115.59 3801
2   active  normal 9.155.115.60 3801
dscli> rmkeymgr 2
dscli> lskeymgr -l
Date/Time: October 23, 2013 9:40:33 AM MST IBM ...
ID  state   status addr         port
====================================
1   active  normal 9.155.115.59 3801
dscli>
```

Note: Do not delete all working key servers before activating one with the new certificate and TLS 1.2 communication first. If less than four key servers are defined, then create another one using same address with the TLS port (the default port is port 441).

Delete only one key server, then create it again with the new certificate and port if four key servers are already defined.

6. Now you are ready to install a certificate. Example 32 shows the `mkkeymgr` command that you run to define the key servers. Install the SKLM certificate that was exported in step 4, and use the SKLM SSL port (port 441 is the default). The location of the certificate is the location that was chosen in step 4; the location must be in the file system where DS CLI is running. In Example 32, we create the key server that was deleted in step 5. You must customize these commands to match your environment.

Example 32   Installing a NIST SP 800-131a certificate

```
dscli> mkkeymgr -port 441 -addr 9.155.115.60 -cert
/tmp/tklm6_ssl_certificate.crt 2
dscli> lskeymgr -l
```

```
Date/Time: October 23, 2013 9:40:33 AM MST IBM ...
ID  state   status addr         port
====================================
1   active  normal 9.155.115.59 3801
2   active  normal 9.155.115.60 441
dscli>

Only key server 2 is using SSL port 441, key server one is using TPC port 3801.
```

Note: You must set the encryption key server SSL port (441 is the default) for TLS 1.2 for network communication. Tivoli Storage Productivity Center port 3801 should be used if TLS 1.2 is not being enabled for network communication.

Note: The key server ID is a decimal number 1 - 4. Four is the maximum number of key servers that the DS8000 can support.

Repeat these steps for each encryption key server until all of them are updated. Now, the DS8870 has the new certificate and all key servers are created to use the new SSL certificate that was created on the key server and SSL port (441 by default) to use TLS 1.2 for HMC to key server communication.

Migrating from the Gen-1 to the Gen-2 certificate

Migrating from the Gen-1 to the Gen-2 certificate is a one-time irreversible change. Careful consideration and planning are required because of the irreversible nature of the change. Also, using the Gen-2 certificate does not necessarily require TLS 1.2 be enabled; these two changes are separate.

To use the Gen-2 certificate on the DS8870 for data encryption, complete the following steps:

1. Verify the version of certificate that is being used for data encryption. Example 33 shows how to verify which certificate, Gen-1, or Gen-2, is being used by the DS8870 for data encryption.

Example 33   Determine which certificate the DS8000 is using for data encryption

```
dscli> showkeygrp 1
Date/Time: October 23, 2013 7:01:33 PM MST IBM …
ID          1
numranks    1
numpools    1
state       accessible
reckeystate configured
reckeydate  07/17/2013 23:27:20 MST
datakeydate 04/18/2012 16:27:35 MST
label       ds8k_tuc_02
label2      -
certificate GEN1
dscli>
```

2. Run **managekeygrp** to change from the Gen-1 certificate to the Gen-2 certificate for data encryption on the DS8870 with Release 7.2 microcode or later, as shown in Example 34.

Example 34 Update the certificate from Gen-1 to Gen-2 on the DS8870

```
dscli> managekeygrp -action updatecert -key data -label ds8k_tuc_02 1
Date/Time: October 23, 2013 7:40:23 PM CET IBM ...
CMUC00472I managekeygrp: The certificate for encryption group 1 has been updated

If you have secondary certificate label then the -label2 flag must also be
used.
```

Besides the DS8870, previous models of the DS8000 series do not support the Gen-2 certificate.

3. Verify that the Gen-2 certificate is now being used for data encryption, as shown in Example 35.

Example 35 Verify that the certificate was updated from Gen-1 to Gen-2

```
dscli> showkeygrp 1
Date/Time: October 23, 2013 7:01:33 PM MST IBM …
ID          1
numranks    1
numpools    1
state       accessible
reckeystate configured
reckeydate  07/17/2013 23:27:20 MST
datakeydate 04/18/2012 16:27:35 MST
label       ds8k_tuc_02
label2      -
certificate GEN2
dscli>
```

If the SSL certificate was updated from the key server and the data encryption certificate was updated to Gen-2, the DS8870 encryption configuration is NIST SP 800-131a compliant.

Authors

This paper was produced at the IBM European Storage Competence Center in Mainz, Germany by a team of specialists from around the world working for the International Technical Support Organization, San Jose Center.

Bert Dufrasne is an IBM Certified IT Specialist and Project Leader for System Storage disk products at the ITSO, San Jose Center. He has worked at IBM in various IT areas. He has written many IBM Redbooks® publications and has developed and taught technical workshops. Before joining the ITSO, he worked for IBM Global Services as an Application Architect. He holds a Master’s degree in Electrical Engineering.

Andre Candra is an IBM IT Specialist for Storage solutions, working for Global Technology Service (GTS) at IBM Indonesia. He provides support to customers with IBM disk solutions, such as the DS8000 series, IBM XIV®, Storwize® V7000, IBM TS3500, and the SAN switch. His areas of expertise include planning, implementing, and supporting storage solutions for Open System servers and IBM mainframes. Andre holds a degree in electrical engineering from the Institut Teknologi Bandung in Indonesia.

Scott Helmick is a Product Field Engineer (PFE) working at IBM in Tucson, Arizona. He provides support to IBM Clients and IBM Service Representatives to resolve complex and critical problems with hardware, microcode, operating systems, and applications. He has been with IBM for about 30 years in various technical support roles. Scott holds a degree from the DeVry Institute of Technology.

Peter Kimmel is an IT Specialist and ATS team lead of the Enterprise Disk Solutions team at the European Storage Competence Center (ESCC) in Mainz, Germany. He joined IBM Storage in 1999 and since then has worked with all the various Enterprise Storage Server (ESS) and DS8000 generations, with a focus on architecture and performance. He has been involved in the Early Shipment Programs (ESP) of these early and all current installations, and co-authored several IBM Redbooks publications about the DS8000 series. Peter holds a Diploma (MSc) degree in Physics from the University of Kaiserslautern.

Abilio de Oliveira is an IBM Certified IT Specialist Expert and works as a Client Technical Specialist in Storage Technical Sales, Brazil. He has 18 years of experience in IT. He holds a degree in Computer Sciences and specializes in Information Security. He currently works as a Regional Designated Specialist designing storage solutions for customers in Latin America and supporting IBM Business Partner sales activities.

Axel Westphal works as an IT Specialist at the European Storage Competence Center (ESCC) in Mainz, Germany. He joined IBM in 1996 working for Global Services as a System Engineer. His areas of expertise include setup and demonstration of IBM System Storage products and solutions in various environments. He has been an author and contributor to several white papers and IBM Redbooks publications about the DS8000 series.

Bruce Wilson is a Senior Education Specialist with ITS at IBM Canada. He has worked with IBM for 32 years, with the first 10 years in the field servicing mainframe servers and various storage products. For the last 22 years, he has been instructing IBM Service Representatives about the IBM System z® server, IBM Parallel Sysplex®, and disk and tape hardware. Bruce has co-authored two previous IBM Redbooks publications dealing with HCD and SAN products.

Thanks to the following people for their contributions to this project:

Rick Ripberger and Dale H. Anderson
IBM US

Kerstin Blum, Peter Klee, Eugen Poljakow, Bjoern Wesselbaum, Jens Wissenbach
IBM Germany

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

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 grant 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.

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 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 supply in any way it believes appropriate without incurring any obligation to you.

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 measurements 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.

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.

This document REDP-5069-00 was created or updated on April 8, 2014.

Send us your comments in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an email to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

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

DS8000®
Easy Tier®
Enterprise Storage Server®
FlashCopy®
IBM®
Jazz™
Parallel Sysplex®
Redbooks®
Redpaper™
Redbooks (logo) ®
Storwize®
System Storage®
System z®
Tivoli®
WebSphere®
XIV®
z/OS®

The following terms are trademarks of other companies:

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

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

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