



# **Hitachi HiCommand™ Device Manager Server Security Guide**



**© 2002 Hitachi Data Systems Corporation, ALL RIGHTS RESERVED**

**Notice:** No part of this publication may be reproduced or transmitted in any form or by any electronic or mechanical means, including photocopying and recording, or stored in a database or retrieval system for any purpose, without the express written permission of Hitachi Data Systems Corporation.

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi Data Systems products or services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements, including license agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

## **Trademarks**

Hitachi Data Systems and the Hitachi Data Systems design mark are registered trademarks service marks of Hitachi, Ltd.

HiCommand is a trademark of Hitachi Data Systems Corporation.

Windows and Windows NT are registered trademarks of Microsoft Corporation.

Solaris, Java, Java2, Java Web Start, and Java Runtime Environment (JRE) are trademarks or registered trademarks of Sun Microsystems, Inc.

VERITAS and SanPoint Control are trademarks or registered trademarks of VERITAS Software Corporation.

All other brand or product names are or may be registered trademarks, trademarks or service marks of and are used to identify products or services of their respective owners.

## Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Data Systems Legal Department for any export compliance questions.

## Document Revision Level

Revision	Date	Description
MK-91HC003-0	November 2001	Initial Release
MK-91HC003-1	January 2002	Revision 1, supersedes and replaces MK-91HC003-0
MK-91HC003-2	June 2002	Revision 2, supersedes and replaces MK-91HC003-1
MK-91HC003-3	November 2002	Revision 3, supersedes and replaces MK-91HC003-2

## Software Revision Level

This document is written to support version 2.2 of the HiCommand™ Device Manager server software.

## Changes in This Revision

- Added new chapter on network configuration for server security (Chapter 2)
- Deleted option of PKI Client Authentication (section 4.2.1).
- Changed Figure 4.6 and Figure 4.7.

# Preface

This Installation Guide provides instructions for configuring the security for the HiCommand™ Device Manager server.

This user's guide assumes that:

- the user has a background in data processing and understands direct-access storage device subsystems and their basic functions,
- the user is familiar with the Hitachi Lightning 9900 and 9900 V Series array subsystems and/or the Thunder 9200 subsystem, and/or the Sun® StorEdge™ T3 subsystem.
- the user is familiar with the Solaris®, Windows NT® or Windows® 2000 operating systems.

You may also contact your Hitachi Data Systems account team or refer to the Hitachi Data Systems worldwide web site (<http://www.hds.com>) for additional information on the Lightning 9900 or 9900 V Series subsystem, the 9200 subsystem, and their features and functions.

## COMMENTS

**Please send us your comments on this document: [doc.comments@hds.com](mailto:doc.comments@hds.com).**

**Make sure to include the document title, number, and revision.**

**Please refer to specific page(s) and paragraph(s) whenever possible.**

(All comments become the property of Hitachi Data Systems Corporation.)

**Thank you!**



# Contents

<b>Chapter 1</b>	<b>Introduction to HiCommand™ Device Manager .....</b>	<b>1</b>
1.1	Overview of HiCommand™ Device Manager .....	1
1.2	HiCommand™ Device Manager Software Components.....	2
<b>Chapter 2</b>	<b>HiCommand™ Device Manager Network Configuration Guide .....</b>	<b>3</b>
2.1.1	Overview of Network Configuration .....	3
2.2	Common Security Risks .....	5
2.3	Server Network Configurations .....	6
2.3.1	Most Secure Configuration: Separate Management LAN Plus Firewall .....	6
2.3.2	Second-Most Secure Configuration: Separate Management LAN Plus Firewalled Devices Under Management .....	8
2.3.3	Third-Most Secure Configuration: Dual-Homed Management Servers Plus Separate Management LAN.....	9
2.3.4	Fourth-Most Secure Configuration: Flat Network.....	10
<b>Chapter 3</b>	<b>HiCommand™ Device Manager Security Properties .....</b>	<b>11</b>
3.1	Summary of HiCommand™ Device Manager Server Security Properties .....	11
3.2	HiCommand™ Device Manager Server Security Properties .....	12
3.2.1	server.http.secure.....	12
3.2.2	server.http.security.realm .....	12
3.2.3	server.http.security.clientIP.....	13
3.2.4	server.https.security.keystore .....	13
3.2.5	server.https.keystore.passphrase .....	13
3.2.6	server.https.keystore.keypass.....	14
3.2.7	server.http.security.unprotected .....	14
3.2.8	server.https.security.truststore .....	14
3.2.9	server.https.truststore.....	15
3.2.10	server.security.logonID.caseSensitive .....	15
<b>Chapter 4</b>	<b>Implementing HiCommand™ Device Manager Server Security.....</b>	<b>17</b>
4.1	Overview of HiCommand™ Device Manager Security .....	17
4.1.1	Introduction to HiCommand™ Device Manager Server Security .....	18
4.2	Using the HiKeytool Script File to Modify Security Properties.....	20
4.2.1	Creating a Keypair .....	20
4.2.2	Enabling TLS/SSL Server Security .....	25
4.2.3	Creating and Importing A Digitally-Signed Certificate .....	27
4.2.3.1	Creating a Certificate Signing Request (CSR).....	27
4.2.3.2	Importing a Signed and Trusted Certificate .....	29
4.2.4	Displaying the Contents of the HiCommand™ Device Manager Keystore.....	32
4.2.4.1	Regular Mode .....	32
4.2.4.2	Verbose Mode.....	33
4.2.5	Deleting an Entry from the HiCommand™ Device Manager Server Keystore .....	34
4.2.6	Changing the HiCommand™ Device Manager Server Keypass .....	36
4.2.7	Change the HiCommand™ Device Manager Server Keystore Password .....	38
4.2.8	Display Contents of the HiCommand™ Device Manager Server Truststore....	40

4.2.9	Displaying the Verbose Contents of the HiCommand™ Device Manager Server Truststore .....	41
4.2.10	Deleting an Entry from the HiCommand™ Device Manager Server Truststore	42
4.2.11	Changing the HiCommand™ Device Manager Server Truststore Password .....	44
<b>Chapter 5</b>	<b>Troubleshooting .....</b>	<b>45</b>
5.1	Contacting the Hitachi Data Systems Technical Support Center .....	45
<b>Glossary, Acronyms, and Abbreviations .....</b>		<b>47</b>
<b>Index .....</b>		<b>49</b>



## List of Figures

Figure 2.1	Incorrect 9900 and 9900V LAN Connection .....	4
Figure 2.2	Most Secure Configuration: Separate Management LAN Plus Firewall .....	7
Figure 2.3	Second-Most Secure Configuration: Separate Management LAN Plus Firewalled Devices .....	8
Figure 2.4	Third-Most Secure Configuration: Dual-Homed Management Servers Plus Separate Management LAN.....	9
Figure 2.5	Fourth-Most Secure Configuration: Flat Network.....	10
Figure 4.1	HiKeytool Main Panel .....	22
Figure 4.2	Creating a Keypair (Windows® Illustration 1).....	22
Figure 4.3	Creating a Keypair (Solaris® Illustration 1) .....	23
Figure 4.4	Creating a Keypair (Windows® Illustration 2).....	23
Figure 4.5	Creating a Keypair (Solaris® Illustration 2) .....	24
Figure 4.6	Default HiCommand™ Device Manager Server Security Level .....	25
Figure 4.7	Selecting and Confirming the HiCommand™ Device Manager Security Level Change .....	26
Figure 4.8	Completed CSR.....	28
Figure 4.9	Sample Certificate Request.....	28
Figure 4.10	Sample Digitally-Signed Certificate.....	30
Figure 4.11	Entering the Location of the Digitally-Signed Certificate (Windows®) .....	30
Figure 4.12	Entering the Location of the Digitally-Signed Certificate (Solaris®).....	31
Figure 4.13	Notification of Successful Import of Digitally-Signed Certificate .....	31
Figure 4.14	Sample Contents of the HiCommand™ Device Manager Server Keystore .....	32
Figure 4.15	Sample Verbose Contents of the HiCommand™ Device Manager Server Keystore .....	33
Figure 4.16	Entering the Number of the Alias to be Deleted .....	34
Figure 4.17	Confirming the Deletion of an Alias .....	35
Figure 4.18	Entering the Current Password .....	36
Figure 4.19	Entering the Old Keypass.....	37
Figure 4.20	Entering and Confirming the New Keypass .....	37
Figure 4.21	Entering Existing Password.....	38
Figure 4.22	Entering Existing Keypass .....	39
Figure 4.23	Entering and Confirming New Keypass .....	39
Figure 4.24	Contents of HiCommand™ Device Manager Server Truststore .....	40
Figure 4.25	Displaying Verbose Information for the HiCommand™ Device Manager Truststore.....	41
Figure 4.26	Entering the Alias to be Deleted from the Truststore .....	42
Figure 4.27	Confirming the Alias to be Deleted from the Truststore .....	43
Figure 4.28	Entering Old Server Truststore Password .....	44
Figure 4.29	Entering and Confirming New Password .....	44

## List of Tables

Table 2.1	Summary of HiCommand™ Device Manager Security Properties .....	11
-----------	--	----



# Chapter 1 Introduction to HiCommand™ Device Manager

## 1.1 Overview of HiCommand™ Device Manager

HiCommand™ Device Manager provides a consistent, easy to use, and easy to configure set of interfaces for managing Hitachi Data Systems storage products. These interfaces allow the HiCommand™ Device Manager system to be controlled by commercial enterprise network management products (e.g., CA Unicenter TNG®) and storage area network (SAN) products (e.g., VERITAS™ SanPoint Control™). HiCommand™ Device Manager provides a web interface for real-time interaction with the storage arrays being managed as well as a command line interface (CLI) for scripting. HiCommand™ Device Manager will manage other vendors' storage area network (SAN) gear as well as direct and network-attached equipment.

HiCommand™ Device Manager gives storage administrators GUI access to the configuration, monitoring, and management features that are already implemented in existing Hitachi Data Systems software products such as LUN Manager, TrueCopy, ShadowImage, and Graph-Track™.

HiCommand™ Device Manager allows you to view the configuration of the storage arrays added to the HiCommand™ Device Manager system, perform configuration operations such as adding and deleting volume paths and securing LUs, and manage data replication features.

HiCommand™ Device Manager provides:

- Storage subsystem discovery and configuration display
- Hierarchical group management for storage
- Alert presentation
- Volume path assignment
- Management of LU groups
- Management of hosts and WWNs

HiCommand™ Device Manager provides several levels of access and functionality for end users, including Access Control, Storage Management and System Support. Access Control handles support for the system administrator, storage administrator, maintenance user and guest user. Storage Management functions include storage configuration and manipulation. System support functions include web client support, user administration, host agent activity and security.

**Note:** The use of the HiCommand™ Device Manager product and all Hitachi Data Systems products is governed by the terms of your license agreement(s) with Hitachi Data Systems.

## 1.2 HiCommand™ Device Manager Software Components

The HiCommand™ Device Manager software product consists of the following basic components:

- **Server Security.** This document covers the topic of server security.
- **Server Installation and Configuration.** The HiCommand™ Device Manager server communicates with the HiCommand™ Device Manager Web Client(s) and the HiCommand™ Device Manager Host Agent(s). For further information on installing and configuring the HiCommand™ Device Manager server, please see *HiCommand™ Device Manager Server Installation and Configuration Guide* (MK-91HC002).
- **Web Client.** The HiCommand™ Device Manager Web Client is a web-based user interface for monitoring and managing Hitachi storage subsystems. The Web Client is a stand-alone Java™-based application that is deployed using the Java Web Start™ software, and communicates with and runs as a client of the HiCommand™ Device Manager server. For further information on the HiCommand™ Device Manager Web Client, please refer to the *HiCommand™ Device Manager Web Client Installation and Configuration Guide* (MK-91HC001).
- **Command Line Interface.** The HiCommand™ Device Manager command line interface enables you to perform Web Client operations by issuing commands from the system command line prompt. For further information on the command line interface, please see the *HiCommand™ Device Manager Command Line Interface Application User's Guide* (MK-91HC007).
- **Host Agent.** The HiCommand™ Device Manager Host Agent runs on the host computer that is attached to the Hitachi storage subsystem(s). The Host Agent collects data on the configuration and utilization of the attached storage and sends this information to the HiCommand™ Device Manager server. For further information on the HiCommand™ Device Manager Host Agent, please refer to the *HiCommand™ Device Manager Agent Installation and Configuration Guide* (MK-92HC019).

## Chapter 2    HiCommand™ Device Manager Network Configuration Guide

### 2.1.1    Overview of Network Configuration

The 9900 and 9900V come equipped with a service processor, which is known as the SVP. The SVP has two Ethernet adapters. The first adapter is for a private (internal) Ethernet LAN, which is intended for intra-array communications only. There are only two user-accessible devices that can access the internal LAN: the Service Processor (SVP), and the 9900 Remote Console. The second adapter is used for other applications to talk to the SVP. This LAN is referred to as the public LAN, because it is visible to other computers outside the array. HiCommand™ Device Manager, Enterprise Resource Manager and Enterprise Storage Resource Manager applications use the public LAN to communicate with the SVP about the array and configuration changes.

While the 9900 and 9900V are managed through their SVP interface, other manageable storage (e.g. Hitachi Thunder arrays and Sun T3 arrays) do not use a private LAN for engineering functions. Instead both the Thunder and the T3 have Ethernet network interfaces that are intended to be directly attached to a public LAN. Once attached to the LAN each has its own remote management API, which can be accessed by a variety of management applications.

**Warning:** Do not under any circumstances attach the 9900 or 9900V private LAN to an external network. Improper or incorrect connectivity to the private LAN can cause serious problems on the array. Private LANs may only be connected to for purposes of HiTrack™, 9900 Remote Console™, and GraphTrack™, but you must follow the instructions in the appropriate installation manuals.

Figure 2.1 illustrates an improper LAN connection.

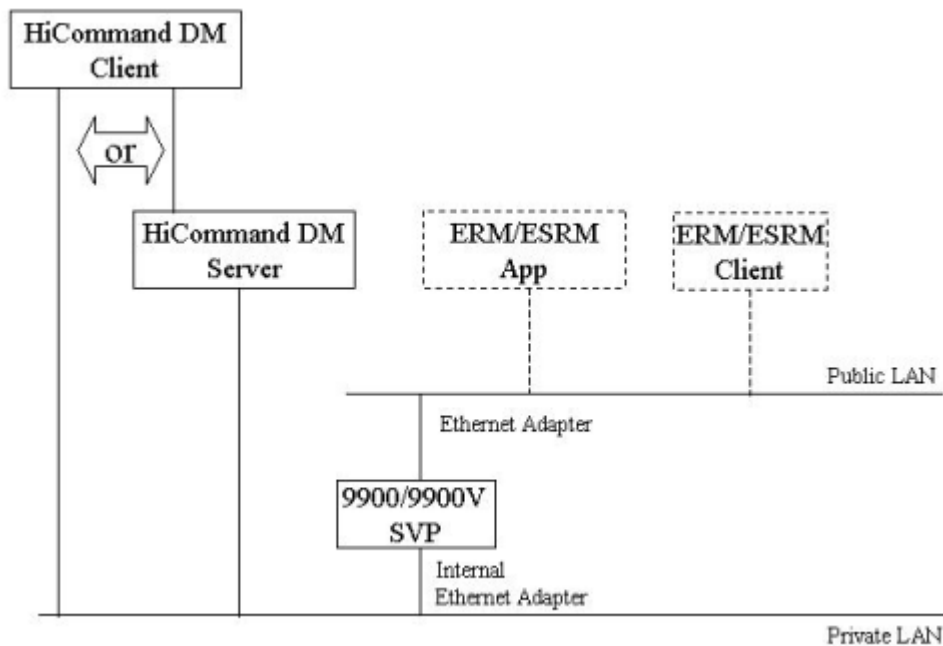


Figure 2.1 Incorrect 9900 and 9900V LAN Connection

## 2.2 Common Security Risks

Because the Thunder™ and Sun T3 arrays are intended to be connected to a public LAN, you must pay particular attention to security risks if you are attaching either array to a public network.

System administrators frequently separate production LANs from management LANs. In such cases, management LANs act as a separate network, which isolates management traffic from a production network and reduces the risk of security-related threats. If a management controller such as the SVP coexists on a production LAN, it is left open for any entity on the IP network to access. Whether the access is intentional or not, the resulting security risks can lead to actual outages characterized as Denial of Storage Service, DoSS. DoSS attacks may lead to a management session being hijacked for malignant purposes, such as unbinding a storage extent from a port during an I/O operation.

The following are guidelines for constructing management LANs:

- Traffic from the production LAN should not flow through, or be routed to the management LAN.
- If possible, all hosts with management interfaces or controllers on the management LAN should be hardened to their maximum level to reduce the potential that software other than the management interface will not lead to an exploit of the entire station or device. (In this case hardening should include removal of unnecessary software, shutting down nonessential services, and updating to the latest patches.)
- The management LAN should only intersect a production LAN on those hosts acting as an interface between the management LAN and the production LAN (e.g. HiCommand DM Server).
- If possible, those hosts intersecting both private LAN and management LAN should be behind a firewall of some kind, further inhibiting unintended access.

## 2.3 Server Network Configurations

### 2.3.1 Most Secure Configuration: Separate Management LAN Plus Firewall

In this case, the server hosting HiCommand Device Manager must either be dual homed or have two NICs, and every other management application must be of similar configuration. The first NIC for each host is attached to a LAN dedicated to management traffic between management host and device under management, which for HiCommand™ Device Manager includes any 9900s, 9900Vs, 9200s, or T3s. A second NIC is attached to a LAN where access is governed by a firewall. As shown in Figure 2.2, each server could also be connected to a different LAN with a different firewall. The firewall contains strict access rules that allow access to the management servers only to HiCommand™ Device Manager or specified management application clients.

This configuration is the most secure but least flexible implementation, as it requires overhead to manage all of the various network components, the servers, and the devices under management. Adding further security to this configuration requires that the underlying management application OS be hardened to the maximum possible limit. This might include disabling services such as Telnet, FTP, SMTP, or IIS. Additionally, if possible all unnecessary packages should be removed.

For an exhaustive study of what is required to harden a server, see <http://ist.uwaterloo.ca/security/howto/>.



Figure 2.2 illustrates a separate management LAN plus a firewall.

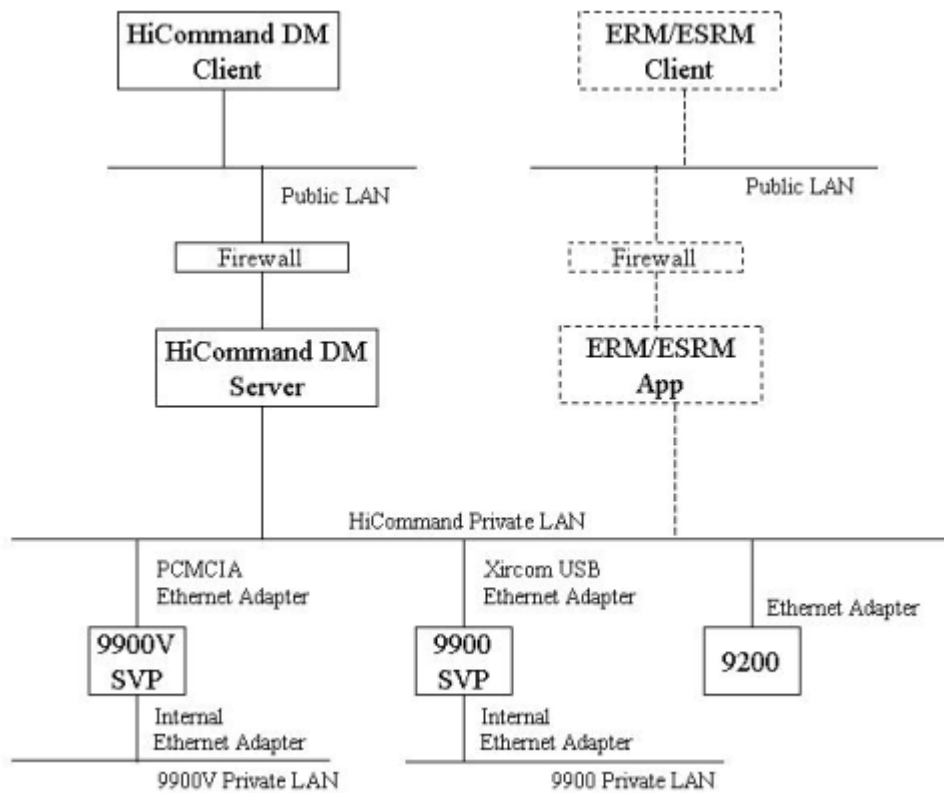


Figure 2.2 Most Secure Configuration: Separate Management LAN Plus Firewall

### 2.3.2 Second-Most Secure Configuration: Separate Management LAN Plus Firewalled Devices Under Management

In this configuration, the server hosting HiCommand™ Device Manager and all other management servers may be single homed, and the actual devices under management are separated from HiCommand™ Device Manager by a firewall. The firewall's rules restrict access to the arrays to HiCommand™ Device Manager and any other required management application. Management clients accessing HiCommand™ Device Manager are not allowed to pass traffic through the firewall to directly talk to the managed arrays, but can participate in management operations directly with HiCommand™ Device Manager or the management application.

This configuration is the second most secure, and is more flexible than the previous option. While this configuration protects the devices under management, it does not protect the management application servers themselves. Therefore all management application servers should be hardened to the maximum possible extent.

Figure 2.3 illustrates a separate management LAN plus firewalled devices under management.

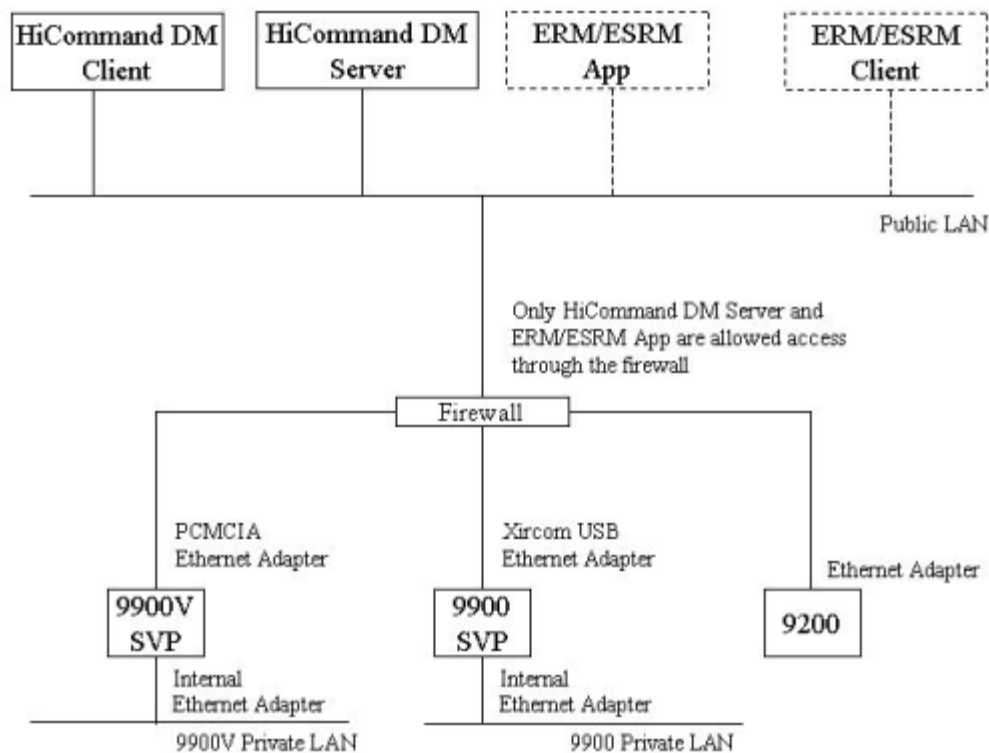


Figure 2.3 Second-Most Secure Configuration: Separate Management LAN Plus Firewalled Devices

### 2.3.3 Third-Most Secure Configuration: Dual-Homed Management Servers Plus Separate Management LAN

In this configuration, the management servers themselves act as the intersection point between the management LAN and a production LAN. The server running HiCommand™ Device Manager or management applications is dual-homed. One NIC is attached to the management LAN along with the devices under management, and the second NIC is attached to a production LAN along with the management clients (e.g., the HiCommand™ Device Manager GUI). Because the management application servers actually act as the gateway between the production LAN and the management LAN, and there is no additional firewall, you must be very sure that the server itself will not route traffic between the two networks.

This configuration is the third most secure, and is more flexible than either of the previously-described configurations. While it protects the devices under management, it does not protect the management application servers themselves. Therefore, all management application servers should be hardened to the maximum possible extent. Additionally, because the management application servers themselves act as gateways between the two LANs, OS hardening is more important.

Figure 2.4 illustrates dual-homed management servers plus a separate management LAN.

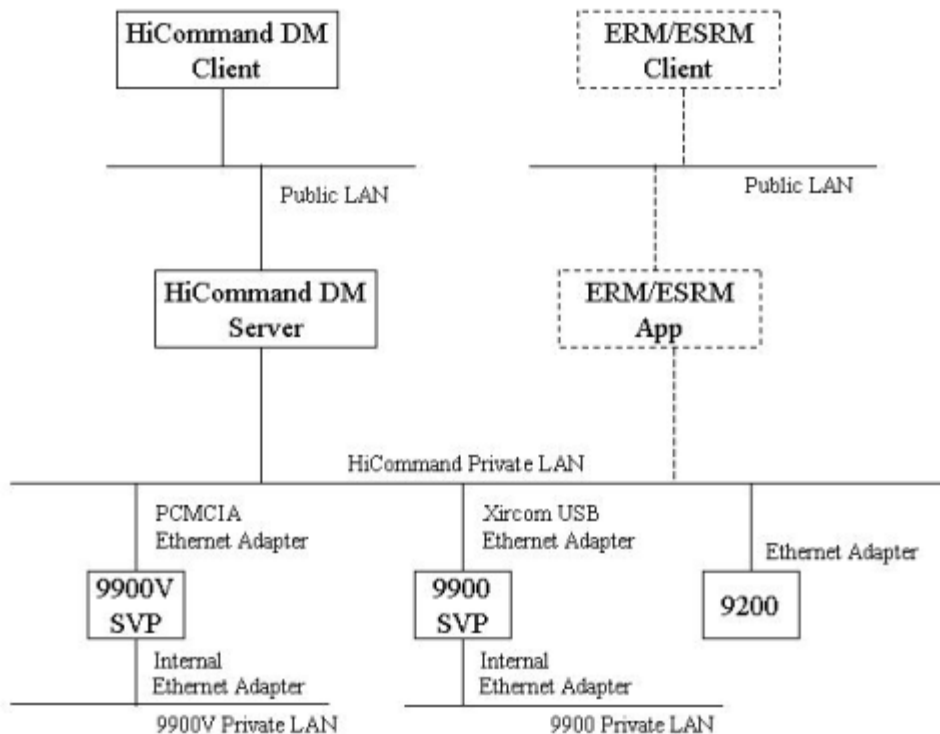


Figure 2.4 Third-Most Secure Configuration: Dual-Homed Management Servers Plus Separate Management LAN

### 2.3.4 Fourth-Most Secure Configuration: Flat Network

Here, the management application servers, managed devices, and managed clients all coexist on the same network.

This configuration is the least secure, though it is the most flexible. It affords no protection to any of the components required for storage management operations, so management application server hardening is paramount. Additionally, you should consider microcode updates to any of the devices under management, especially if they are related in any way to security for the device management controllers themselves. Note: This configuration may be a requirement if the implementation cannot accommodate a management LAN.

Figure 2.5 illustrates a flat network.

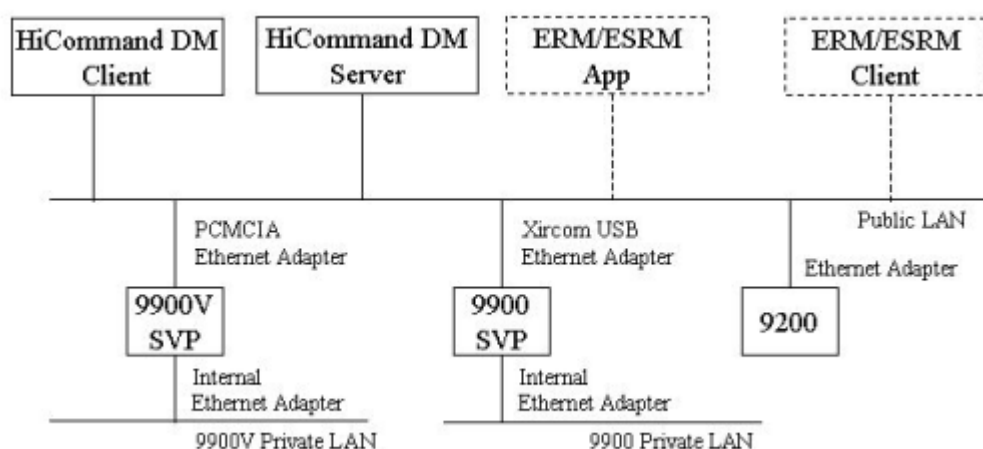


Figure 2.5 Fourth-Most Secure Configuration: Flat Network

## Chapter 3 HiCommand™ Device Manager Security Properties

### 3.1 Summary of HiCommand™ Device Manager Server Security Properties

**Table 3.1 Summary of HiCommand™ Device Manager Security Properties**

server.http.secure	Sets the security level of the HiCommand™ Device Manager server.	Section 3.2.1
server.http.security.realm	Sets the security realm message for the HiCommand™ Device Manager server's authentication challenge.	Section 3.2.2
server.http.security.clientIP	Implements an IP address filter.	Section 3.2.3
server.https.security.keystore	Assigns the name of the keystore file that contains a Server Certificate used for establishing an encrypted communication via Secure Sockets Layer (SSL) and Transport Layer Security (TLS).	Section 3.2.4
server.https.keystore.passphrase	Contains the logon password for the keystore file that contains a keypair and associated Server Certificate used for SSL/TLS connections.	Section 3.2.5
server.https.keystore.keypass	Contains the password for recovering the keypair and associated Server Certificate used for encrypting SSL/TLS connections from the HiCommand™ Device Manager server's keystore.	Section 3.2.6
server.http.security.unprotected	Designates a comma-delimited list of any non-protected file resources under the server's document root.	Section 3.2.7
server.https.security.truststore	Assigns the name and location of the truststore file that contains the Server Certificates.	Section 3.2.8
server.https.truststore	Contains the password used to access the default truststore distributed with the Java Runtime Environment™.	Section 3.2.9
server.security.logonID.caseSensitive	Sets whether a user's logonID is case-sensitive.	Section 3.2.10

## 3.2 HiCommand™ Device Manager Server Security Properties

### 3.2.1 server.http.secure

This property sets the security level of the HiCommand™ Device Manager server. See section 4.2.2 for instructions on how to use HiKeytool to set the security level, as follows:

- **0 = Unsecure.** Any client application can obtain access to the server. No logon authentication is required from the client. This setting is intended for use only on highly secure LANs and/or private networks, and even in those environments more robust server security is highly recommended.
- **1 = Basic Authentication.** This is the default setting, in which the HiCommand™ Device Manager server is operating in protected mode, and client applications attempting to connect with the server must submit an authorized user's logon ID and password and be authenticated against the Access Control List (ACL). **Note:** These requirements do not apply to requests for files that are intentionally designated as being excluded from ACL security protection (see the **server.http.security.unprotected** property in section 3.2.7).
- **2 = Secure Socket (TLS/SSL).** In this security mode, the server opens an additional secure HTTP listener on a port designated by the **server.https.port** property. All communications via this port are strongly encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). See section 4.1 for further information on SSL and TLS. In order for a server to use the secure HTTP protocol, a keypair and associated Server Certificate must be present in the HiCommand™ Device Manager server keystore. This setting is strongly recommended if a HiCommand™ Device Manager server is exposed to any public network or Internet.

### 3.2.2 server.http.security.realm

This property sets the security realm message for the HiCommand™ Device Manager server's authentication challenge. This text is usually displayed in a browser's logon dialog, and the recommended (default) setting is **HiCommand Security**.

### 3.2.3 **server.http.security.clientIP**

This property implements an IP address filter, which helps harden a server against malicious attacks. The default value is `*.*.*.*` which means that an HTTP connection from any client IP address will be accepted. You can restrict HiCommand™ Device Manager server access to designated clients and/or to subnets such as a Local Area Network (LAN) or Wide Area Network (WAN), by using asterisks as a wildcard character. For example, a HiCommand™ Device Manager server would only accept connections from the host machine itself and other client users on a LAN if this directive was set as:

**server.http.security.clientIP=127.0.0.1,192.168.\*.\***

Whitespace (the space following the comma delimiter) is ignored, as are any invalid dotted-decimal IP entries, so that no runtime error is raised if an invalid or incorrectly formatted network address is detected in this list.

Client machines that are not on the access list will be denied access to the server. No HTTP response message (stating a reason for the failure to establish a connection) will be returned to the intruder, in order to reduce vulnerability to certain denial of service attacks that attempt to overload a server by flooding it with a large number of simultaneous (bogus) requests.

### 3.2.4 **server.https.security.keystore**

This property assigns the name of the keystore file that contains the keypair and associated Server Certificate used for establishing an encrypted communication via Secure Sockets Layer(SSL) or Transport Layer Security. The default setting is **keystore**, and this file is assumed to be located in the HiCommand™ Device Manager server's installation directory.

The **keystore** file shipped with a HiCommand™ Device Manager server is an empty placeholder file that does not contain the required keypair and associated Server Certificate needed to run the HiCommand™ Device Manager server in secure mode. If you attempt to start the server in secure mode with an empty **keystore** file, the server will log a fatal exception and fail. A keypair and associated self-signed or trusted certificate must first be installed into the keystore before encrypted communications can be started. See section 4.2.3 for more information about Server Certificates.

### 3.2.5 **server.https.keystore.passphrase**

This property contains the logon password for the keystore file that contains a keypair and associated Server Certificate used for SSL/TLS connections. The logon password is used to check the integrity of the keystore data. See section 4.2.6 for instructions on using HiKeytool to change the password.

### 3.2.6 `server.https.keystore.keypass`

This file contains the password for recovering the keypair and associated Server Certificate used for encrypting SSL/TLS connections from the HiCommand™ Device Manager server's keystore (refer also to the `server.https.security.keystore` property in section 3.2.4). For instructions on how to use HiKeytool to change the keypass, see section 4.2.7.

### 3.2.7 `server.http.security.unprotected`

This property designates a comma-delimited list of any non-protected file resources under the server's document root. When files or directories are designated as **unprotected**, they are not subject to Access Control List checks (user authentication), regardless of the security mode setting for the server. Entire directories (including nested sub-directories) can be flagged as unprotected by using an asterisk as a wildcard character. If this directive is empty all resources are protected, so that every request to the HiCommand™ Device Manager server will require user authentication.

This property allows anyone to view the `index.html` front page via a browser, without user authentication being required. More importantly, it allows the Java Web Start™ application to update its JAR file and deploy (via the `HiCommand.jnlp` file) to the end-user's system without raising a series of logon dialogs. Similarly, the GUI's help files (and certain client installation information) can be viewed via a web browser without separate authentication being required at each step. The default entry for this property is `index.html, HiCommand/*, webstart/*, images/*, style/*, docs/*`. This should not require modification under normal circumstances.

### 3.2.8 `server.https.security.truststore`

This property assigns the name and location of the truststore file that contains the Server Certificates. The default is:  
`server.https.security.truststore={java.home}/lib/security/cacerts.`

The HiCommand™ Device Manager server uses the default truststore distributed with the JRE named "cacerts". **Note:** This property cannot be modified with HiKeytool. If you want to change the value, you must do so by editing the value in the `server.properties` file.



### 3.2.9 **server.https.truststore**

This property contains the password used to access the default truststore distributed with the Java Runtime Environment™. The default value is:

**server.https.truststore.passphrase=changeit.**

For instructions on how to use HiKeytool to change the keypass, see section 4.2.11.

### 3.2.10 **server.security.logonID.caseSensitive**

This Boolean property sets whether a user's logon ID is case-sensitive, and the default is **false**. If it is set to **true**, a user's logon ID must be entered in exactly the same case as exists in the HiCommand™ Device Manager Access Control List (ACL).



# Chapter 4    Implementing HiCommand™ Device Manager Server Security

## 4.1    Overview of HiCommand™ Device Manager Security

This section discusses the following security procedures:

- Enabling SSL/TLS server security (see section 4.2.2)
- Obtaining a signed and trusted Server Certificate (see section 4.2.3)
- Displaying the contents of the keystore (see section 4.2.4)
- Deleting an entry from the keystore (see section 4.2.5)
- Changing the server keypass (see section 4.2.6)
- Changing the server password (see section 4.2.7)
- Displaying the contents of the server truststore (see section 4.2.8)
- Displaying the verbose contents of the server truststore (see section 4.2.9)
- Deleting an entry from the server truststore (see section 4.2.10)
- Changing the password for the server truststore (see section 4.2.11)

**Note:** Screen shots in this section are from Windows®, unless otherwise indicated. Where there are content differences between the Windows® and the Solaris® screen shots, both will be displayed.

## 4.1.1 Introduction to HiCommand™ Device Manager Server Security

HiCommand™ Device Manager uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to encrypt network transmissions between the HiCommand™ Device Manager client and the HiCommand™ Device Manager server. SSL and TLS use cryptography, digital signature technology and digital certificates to provide user authentication, data integrity, and privacy. This document includes instructions for configuring the HiCommand™ Device Manager server to securely communicate over the Internet or an Intranet using SSL and TLS. Future releases will take advantage of the Public Key Infrastructure (PKI) capabilities.

**Important:** If you enable security on HiCommand™ Device Manager, you must make sure that the key pair and associated server certificate do not expire. If either the key pair or the server certificate expire, users will be unable to connect to the HiCommand™ Device Manager Server with the HiCommand™ Device Manager Web Client. See section 4.2.1 for instructions.

This chapter includes the following terms:

- <host name> is used to indicate the name of the host that is running the HiCommand™ Device Manager server, unless otherwise indicated.
- <Java Web Start> is used to indicate the default Java Web Start installation directory on a client machine. If a client's Java Web Start directory is not located in the default location, adjust commands or paths accordingly. The default directories are as follows:  
Windows®: c:\Program Files\Java Web Start
- Solaris®: \$HOME/utils/webstart/
- <installation directory> is used to indicate the default HiCommand™ Device Manager server installation directory. If your directory is not located in the default directory, adjust commands or paths accordingly. The default directories are as follows:
  - Windows®: c:\Program Files\HiCommand\HiCommandServer
  - Solaris®: /opt/HiCommand/HiCommandServer
- **Public Key Infrastructure (PKI)** is a cryptographic technology developed under the guidance of the IETF (Internet Technology Engineering Taskforce) to create a secure networking system that can have interoperative characteristics between multiple vendors.
- **Secure Sockets Layer (SSL)** is a protocol first developed by Netscape® to securely transmit data over the Internet. Two SSL-enabled peers use their Private and Public Keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.
- **Transport Layer Security (TLS)** is the successor protocol to SSL. For more information, see *RFC The TLS Protocol (version 1.0)*, located on <ftp://ftp.isi.edu/in-notes/rfc2246.txt>.
- A **keypair** is two mathematically-related cryptographic keys consisting of a Private Key and its associated Public Key.

- A **Server Certificate** (sometimes also called a Digital Certificate) forms an association between an identity (in this case the HiCommand™ Device Manager server) and a specific keypair. A Server Certificate is used to identify the HiCommand™ Device Manager server to a client so that the server and client can communicate using SSL/TLS. Server Certificates come in two basic types:
  - **Self-signed:** (see section 4.2.1). This is the case where you generate your own certificate, so that the subject of the certificate is the same as the issuer of the certificate. For example, when you create a keypair with the HiKeytool batch file, you will have a keypair and an associated a self-signed certificate.
  - **Signed and Trusted:** (see section 4.2.3). When a Certificate Signing Request (CSR) is generated and sent to a well-known and trusted Certificate Authority (CA) for signing, and is then signed and returned by the Certificate Authority, your certificate is considered signed and trusted. A well-known and trusted Certificate Authority meets the following requirements:
    1. A certificate for that Certificate Authority is located inside the HiCommand™ Device Manager server truststore; and
    2. A certificate for that Certificate Authority is located in the database of trusted Certificate Authorities within browsers supported by HiCommand™ Device Manager; and
    3. A certificate for that Certificate Authority is located within the truststore distributed with Java Web Start.

**Note:** The default HiCommand™ Device Manager server truststore is located at `<HiCommand>/jre/lib/security/cacerts`. You can modify the default location using the `server.https.security.truststore` property in the `server.properties` file (refer to section 3.2.9). The default truststore for Java Web Start is located at `<Java Web Start>/cacerts`.

## 4.2 Using the HiKeytool Script File to Modify Security Properties

### 4.2.1 Creating a Keypair

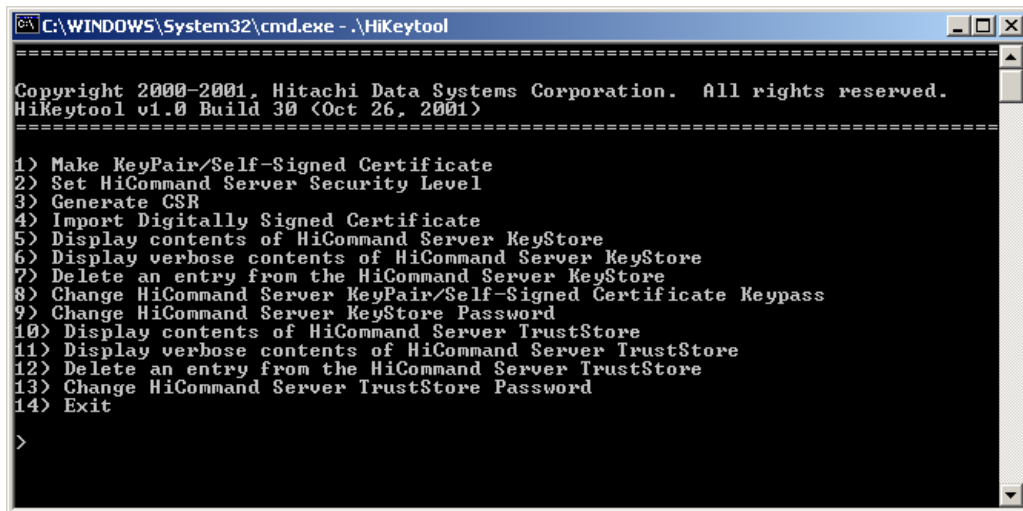
**Note:** If you make a mistake during this process and need to start over, exit by typing **Control+c** and restart HiKeytool.

1. Solaris® users must be logged on as a super-user. Open a command line or terminal window or terminal window, navigate to the <HiCommand Server> directory and launch the HiKeytool script file, as follows:
  - On Windows® type `.\HiKeytool.bat` and select **Enter**.
  - On Solaris® type `./HiKeytool.sh` and select **Enter**.
2. The HiKeytool main panel (see Figure 4.1) will display.
3. From HiKeytool, type **1** (Make Keypair/Self-Signed Certificate). Throughout this section, use the default values presented unless you are either very familiar with the area of cryptography and Java™ security or are otherwise instructed.
4. Enter the server name. The default is **hishark** for Windows® and **sunbox** for Solaris® (see Figure 4.2 and Figure 4.3). Use the default value unless your machine is visible to the LAN or WAN under a different name, in which case you should use the name by which the HiCommand™ Device Manager server is visible.
5. Enter the organizational unit [default=HiCommand Device Manager Administration] (see Figure 4.2). The default value is recommended, but you can use anything meaningful, e.g. Marketing.
6. Enter your organization name. The default is **hishark** for Windows® and **sunbox** for Solaris® (see Figure 4.2 and Figure 4.3). Ordinarily you would use the default value or your host name, but you can use another name, such as the name of your company.
7. Enter your city or locality (see Figure 4.2). There is no default value for this field.
8. Enter your state or province (see Figure 4.2). There is no default value provided, but be sure to spell it out instead of using the two-character state code.
9. Enter your two-character country code [default=US] (see Figure 4.2).
10. Enter your key alias. The default is **hishark** for Windows® and **sunbox** for Solaris® (see Figure 4.2 and Figure 4.3). This should be the local host name of the HiCommand™ Device Manager server. Be sure to use the same value that you used for the server name in step 4, above.

Instructions continued on next page

11. Enter your key password (6 characters minimum) [default=passphrase] (see Figure 4.2). This is the value used to access the keypair entry by the HiCommand™ Device Manager server and the default value is taken from the **server.https.keystore.keypass** property (refer to section 3.2.6). For security reasons, you should change the default value.  
**Important:** If you want to change the default value you should do so by using the process described in section 4.2.7, and should not simply change it directly from the properties file.

12. Enter the key algorithm [default=RSA] (see Figure 4.2). Currently, only RSA is supported.
13. Enter the key size (512, 1024, 2048) [default=2048] (see Figure 4.2). Assuming the RSA key algorithm is used, any Key Size from 512 to 2048 is valid, so long as it is in an increment of 64. Larger key sizes are recommended because that will provide greater data security against brute force and factoring attacks.
14. Enter the signature algorithm [default=MD5withRSA] (see Figure 4.2). Currently, only MD5withRSA is supported.
15. Enter the number of days valid [default=365] (see Figure 4.2). This is the period during which the HiCommand™ Device Manager server keypair will be valid.
  - **If you have your server certificate signed** by a well-known and trusted Certificate Authority, the number of days valid specified by that authority will override the value you place in this field. Be sure to check the web site of your vendor for specific requirements and calendar the need to renew your certificate, because if the key pair and associated server certificate expire, users will be unable to establish a secure connection with the HiCommand™ Device Manager Server via SSL/TLS.
  - **If you elect not to have your server certificate signed**, the value that you place in this field will determine the period during which the keypair and associated server certificate will be valid. The default is 365 days.
16. Enter the keystore password (6 characters minimum) [default=passphrase] (see Figure 4.4 and Figure 4.5). This is the value used to protect and verify the integrity of the keystore, and the default value is taken from the **server.https.keystore.passphrase** property (refer to section 3.2.5). **Important:** If you want to change the default value of the keystore password, you should use the process described in section 4.2.7, and should not simply change it directly from the properties file.
17. Once you have completed these steps, HiCommand™ Device Manager will generate the HiCommand™ Device Manager server keypair and associated certificate. The keypair is placed inside the keystore for the HiCommand™ Device Manager server (see Figure 4.4 and Figure 4.5). **Note:** If you create a keypair with a size of 2048 you might have to wait up to a minute for the keypair to generate.
18. You will need to restart the server for the changes to be effective.



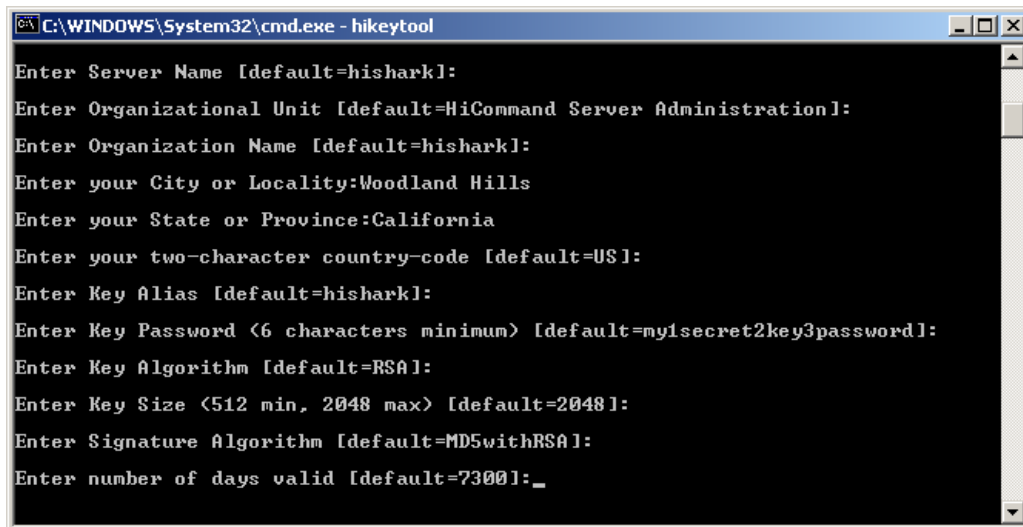
```
C:\WINDOWS\System32\cmd.exe - .\HiKeytool

=====
Copyright 2000-2001, Hitachi Data Systems Corporation. All rights reserved.
HiKeytool v1.0 Build 30 <Oct 26, 2001>
=====

1> Make KeyPair/Self-Signed Certificate
2> Set HiCommand Server Security Level
3> Generate CSR
4> Import Digitally Signed Certificate
5> Display contents of HiCommand Server KeyStore
6> Display verbose contents of HiCommand Server KeyStore
7> Delete an entry from the HiCommand Server KeyStore
8> Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9> Change HiCommand Server KeyStore Password
10> Display contents of HiCommand Server TrustStore
11> Display verbose contents of HiCommand Server TrustStore
12> Delete an entry from the HiCommand Server TrustStore
13> Change HiCommand Server TrustStore Password
14> Exit

>
```

Figure 4.1 HiKeytool Main Panel



```
C:\WINDOWS\System32\cmd.exe - hikeytool

Enter Server Name [default=hishark]:
Enter Organizational Unit [default=HiCommand Server Administration]:
Enter Organization Name [default=hishark]:
Enter your City or Locality:Woodland Hills
Enter your State or Province:California
Enter your two-character country-code [default=US]:
Enter Key Alias [default=hishark]:
Enter Key Password <6 characters minimum> [default=my1secret2key3password]:
Enter Key Algorithm [default=RSA]:
Enter Key Size <512 min, 2048 max> [default=2048]:
Enter Signature Algorithm [default=MD5withRSA]:
Enter number of days valid [default=7300]:_
```

Figure 4.2 Creating a Keypair (Windows® Illustration 1)



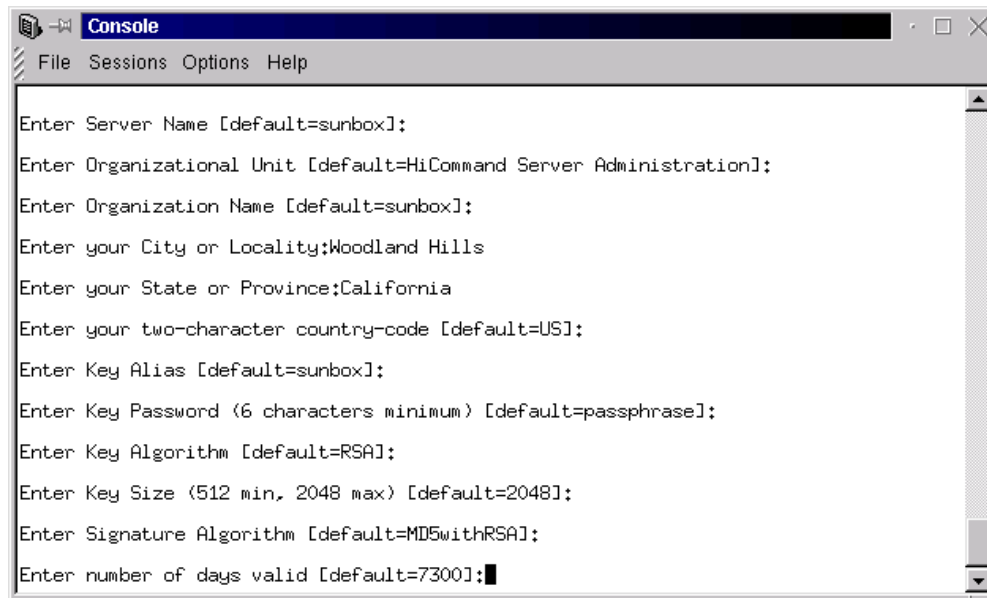


Figure 4.3 Creating a Keypair (Solaris® Illustration 1)

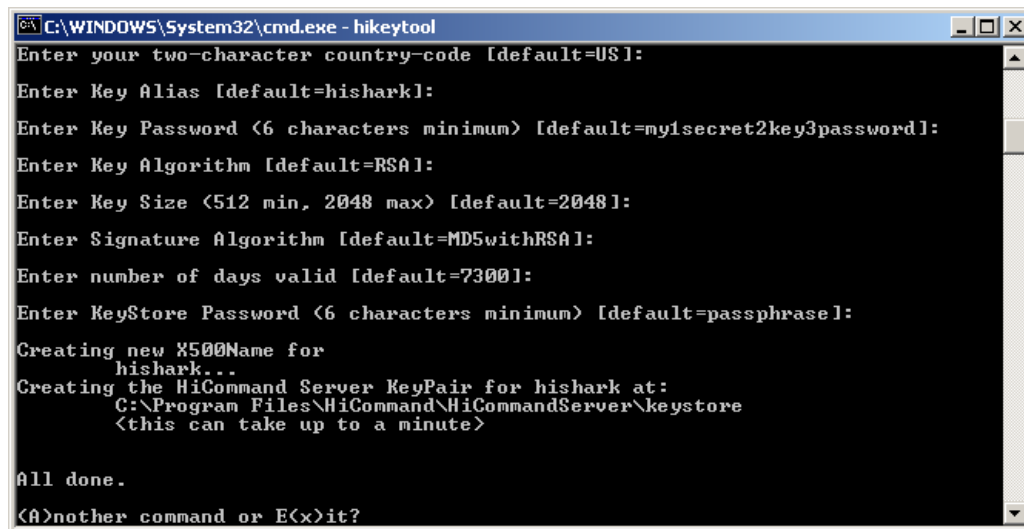
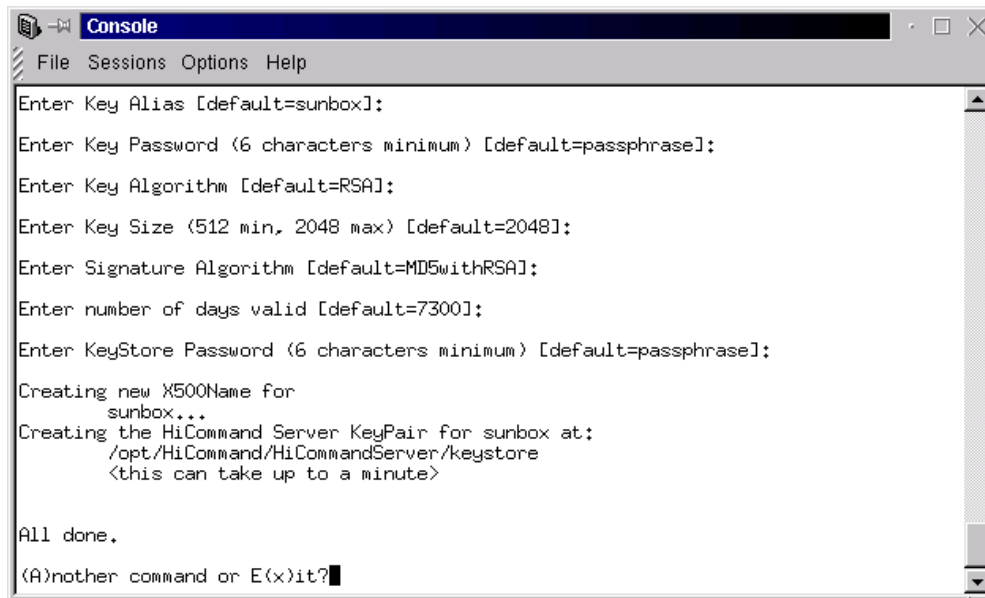


Figure 4.4 Creating a Keypair (Windows® Illustration 2)



```
Console
File Sessions Options Help

Enter Key Alias [default=sunbox]:
Enter Key Password (6 characters minimum) [default=passphrase]:
Enter Key Algorithm [default=RSA]:
Enter Key Size (512 min, 2048 max) [default=2048]:
Enter Signature Algorithm [default=MD5withRSA]:
Enter number of days valid [default=7300]:
Enter KeyStore Password (6 characters minimum) [default=passphrase]:

Creating new X509Name for
sunbox...
Creating the HiCommand Server KeyPair for sunbox at:
/opt/HiCommand/HiCommandServer/keystore
<this can take up to a minute>

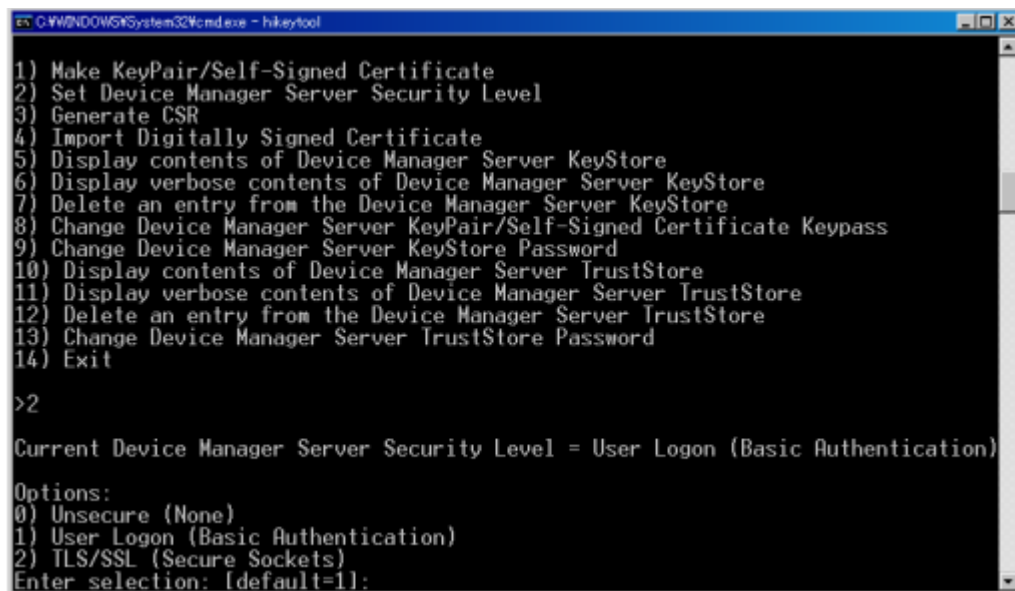
All done.

(A)nother command or E(x)it?
```

**Figure 4.5** Creating a Keypair (Solaris® Illustration 2)

## 4.2.2 Enabling TLS/SSL Server Security

1. **Important:** TLS and SSL require Internet Explorer® 5.5 or Netscape® 4.76 or higher.
2. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
3. From HiKeytool type 2 (Set HiCommand Server Security Level) (see Figure 4.6).
4. HiKeytool will echo the current security level, display the three available levels of security, and prompt the user for an entry (see Figure 4.6), as follows:
  - 0) No authentication required
  - 1) Basic authentication, which will require a user to enter a username and password to be authenticated against the database when accessing the HiCommand™ Device Manager Server. **Note:** This information will be base64 encoded, but it can be easily unencoded and read by anyone listening to the communications being sent on a network.
  - 2) Encrypted using TLS/SSL, which is discussed in this section.
5. To enable TLS/SSL (Secure Sockets), type 2 and select **Enter**. The display will confirm that you have selected TLS/SSL (see Figure 4.7).
6. You will need to restart the HiCommand™ Device Manager server for these changes to take effect.



```
C:\WINDDWS\GSystem32\cmd.exe - hikeytool
1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit
>2
Current Device Manager Server Security Level = User Logon (Basic Authentication)
Options:
0) Unsecure (None)
1) User Logon (Basic Authentication)
2) TLS/SSL (Secure Sockets)
Enter selection: [default=1]:
```

Figure 4.6 Default HiCommand™ Device Manager Server Security Level

```
en C:\WINDOWS\system32\cmd.exe - hikeytool
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

>2

Current Device Manager Server Security Level = User Logon (Basic Authentication)

Options:
0) Unsecure (None)
1) User Logon (Basic Authentication)
2) TLS/SSL (Secure Sockets)
Enter selection: [default=1]:2

Device Manager Server Security level set to: TLS/SSL Secure Socket
You must restart the Device Manager Server for this change to take effect.

(A)nother command or E(x)it?_
```

Figure 4.7 Selecting and Confirming the HiCommand™ Device Manager Security Level Change

## 4.2.3 Creating and Importing A Digitally-Signed Certificate

This section contains instructions for obtaining a digitally-signed certificate from a well known and trusted Certificate Authority. If you want to import an untrusted Server Certificate see <http://<host name>:2001/docs/security/certificates.html> (replace <hostname> with the URL of your HiCommand™ Device Manager server). Refer to section 4.1 for a discussion of the merits of using digitally-signed certificates.

### 4.2.3.1 Creating a Certificate Signing Request (CSR)

To create a Certificate Signing Request:

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool type **3** (Generate CSR) (see Figure 4.8).
3. HiKeytool will inform the user where the Certificate Signing Request has been stored on disk (see Figure 4.8), which will be in a file named <host name>.csr inside the <HiCommand Server> directory. The contents of your CSR will look similar to the example in Figure 4.9. **Important:** Your CSR will contain extra carriage returns and line feeds which *must* be included when it is sent to the Certificate Authority, or it will not be processed correctly.
4. You will then send the CSR to the Certificate Authority of your choice to be digitally signed. The application for digital signing can be done online, and the response is typically returned to you via email from the Certificate Authority.
5. If you intend to have a self-signed certificate digitally signed by a Certificate Authority, you may want to check their web site for specifics. If your Certificate Authority's requirements are sufficiently different, you may want to recreate the HiCommand™ Device Manager server keypair before generating a CSR. To recreate the keypair, first delete the existing keypair (see section 4.2.10 for instructions), and then create a new keypair as described in this section. **Note:** There must be only one entry in the HiCommand™ Device Manager server keystore, or you will likely have problems when you are running the HiCommand™ Device Manager server in secure mode.

```
C:\WINDOWS\System32\cmd.exe - .\HiKeytool.bat
(A)nother command or E(x)it?a

1) Make KeyPair/Self-Signed Certificate
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>3

Generating CSR...
CSR has been written to disk and saved at:
  C:\Program Files\HiCommand\HiCommandServer\hishark.csr
All done!

(A)nother command or E(x)it?_
```

**Figure 4.8 Completed CSR**

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICzDCCABQCAQAwgYYxCzAJBgNVBAYTAiVTMRMwEQYDVQQIEwppDYWxpZm9ybmhlbHRmQWVhZDQ0QW
EwtMb3MgQW5nZWxlczEQAQA4GA1UEChMHhG1zaGFYazEoMCYGA1UECXMfSG1Db21tYW5kIFNlcnZl
ciBBAQZG1pbmlzdHJhZGlvdjEQAQA4GA1UEAxAHhG1zaGFYazCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADBBAQ0CggEBALH9cjGweKgcjqcNEBAJdyduJkVokov5UGrEFQXsVBGgg3F30W5PD83EIWfS0+UJU
BHPE7YI5A/yc8IrTbhnbn+muXHC/+q1KIIzNTAunt0ta2JuhqK5fr22rJh6wCwvzmOweZJAINPNuw
SN7wl0LSz7dpJHAQs4KJBsrG9Gh3+KBU0gFMK080lmHPP9e8vfGfQolYdSQpOddQLyHktQxhmKtTQ
l3adMmXsYxkj4S4CFeaalTuClRaNhg4Q9mPF+YiVmdcqCEXorhQhcMh3iL/AcOrAQ9GBF71xg2Wn
nA8XawVOeScdB0Dr9W9TWakNSAAs5xcfvxkCZ01Z+5itDwdc0CAwEAaAAAMA0GCSqGSIb3DQEB
BAUAA4IBAQBfMblMbLYOZJ2JWJzhGNk1TY8HYvODNIUlanuADS7gc0/iLX5/9amexHePxRhItmhin7
ClCoR+IvNlJxhzqVhgl9noLqbqQhTTFiClGA2COvdFN8VPzeLidch94XaaJfSJ44U29iVgNDSuft
bEk124mimGbDdczRxooDms9pSiI2oCtrWFA7zUXSGO7NquKkPaExO+fM6s5cnTlNew5HE8e6jfoL
e65g9/6hcH7KacbwKzRzU9R4iMrCohW6Hn1V0GDeCyhmAEW0dsHSwaBptEM3gGo+ffXhL54tXX771
tnYJU1QAJfrRqTi9eFL4N2Ooo4An8jXYooBjknolr+X+V4r
-----END NEW CERTIFICATE REQUEST-----
```

**Figure 4.9 Sample Certificate Request**

### 4.2.3.2 Importing a Signed and Trusted Certificate

Once you receive your digitally-signed certificate from the Certificate Authority, you can use HiKeytool to import it. Some Certificate Authorities will return your digitally-signed certificate as an attached file with a **.cer** extension. Others will return the response as text in the body of an email, in which case you should use a text editor such as Notepad or WordPad to save the response in a new file. A digitally-signed certificate looks something like the example in Figure 4.10.

#### To import a digitally-signed certificate:

1. Move the file containing the digitally-signed certificate into the HiCommand™ Device Manager server directory. Name the file **<alias>.cer**, using the alias that you have chosen for the host. In our example the file has been titled **hishark.cer**. **Note:** Be sure to save the response from your Certificate Authority.
2. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
3. From HiKeytool type **4** (Import Digitally Signed Certificate).
4. You will be prompted to enter the location of the digitally-signed certificate. If the certificate is in the default location, select **Enter**. Otherwise, type the complete path and then select **Enter** (see Figure 4.11 and Figure 4.12).
5. You will be notified when the digitally-signed certificate has been imported (see Figure 4.13).
6. You will need to restart the server for the changes to be effective.

```

-----BEGIN CERTIFICATE-----
MIIDMDCCApmgAwIBAgIDOBcYMA0GCSqSIB3DQEBBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGAlUECBMZrk9SIFRFU1RJTkcqUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xZzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
GgYDVQQDExNUaGF3dGUgVGVzdCBBDQSBsb290MB4XDTAxMDkxMTAyMDMzNFoXDTAx
MTAwMjYyMDMzNFowGYYxCzAJBgNVBAYTAlVTMRMwEQYDVQIEwPDYXpZm9ybmlh
MRQwEgYDVQQHEwtMb3MgQW5nZWxlczEQMA4GA1UEChMHAGlzaGFyaZzEOMCYGA1UE
CxMfSGlDb21tYW5kIFNlcnZlciBBZGlpbmlzdHJhdGlvbWJlEQMA4GA1UEAxMHAGlza
aGFyaZCCASIwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALH9c jGweKgc jqcN
EBAJyduJkvOkov5UGrEFQXsVBGgq3F30W5PD83EIWfS0+UJUBHPE7YI5A/yc8Irt
bhn+muXHC/+q1KIIzNTAunt0ta2JuhqK5fR22rJh6wCwvzmOwEZJAINPNUWSN7w
1OLsZ7dEPJHAQs4KJBsrG9Gh3+KBU0gFMK080lmHPP9e8vfGfQolYdSQpOddQLyHK
tQxhMkTQl3adMMsXykjs4SCFea1TuLcLRaNHg4Q9mPF+YiVmdcqCEXorhQhcMh3i
L/AcOrRAQ9GBFZ1xg2WnnA8XawVOeWcdB0Dr9W9TwaKNSAAS5xcF0vxkCZQ01Z+5
iTdWdc0CAwEAAMlMCMwEwYDVR01BAAwCgYIKwYBBQUHAWEdDAYDVR0TAQH/BAIw
ADANBgkqhkiG9w0BAQQFAAOBgQBtzeFG4IfvpPnA7G/khD4rrT1TvjbK4Y1pcROM
cel43uUfKgNYgy35UukoNtd120XOoudLwKvJu5JK7846zWlbeJmCr5BYlmywZuao
MQdXMyPOUnqucgg44/JG2F27xqP4atWEZsNl j5R7XGGXi4RPA05Y0YbbbvMJD0QR
yV00xw==
-----END CERTIFICATE-----

```

Figure 4.10 Sample Digitally-Signed Certificate

```

C:\WINDOWS\System32\cmd.exe - .\HiKeytool.bat
C:\Program Files\HiCommand\HiCommandServer\hishark.csr
All done!

(A>)nother command or E(x)it?a

1) Make KeyPair/Self-Signed Certificate
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

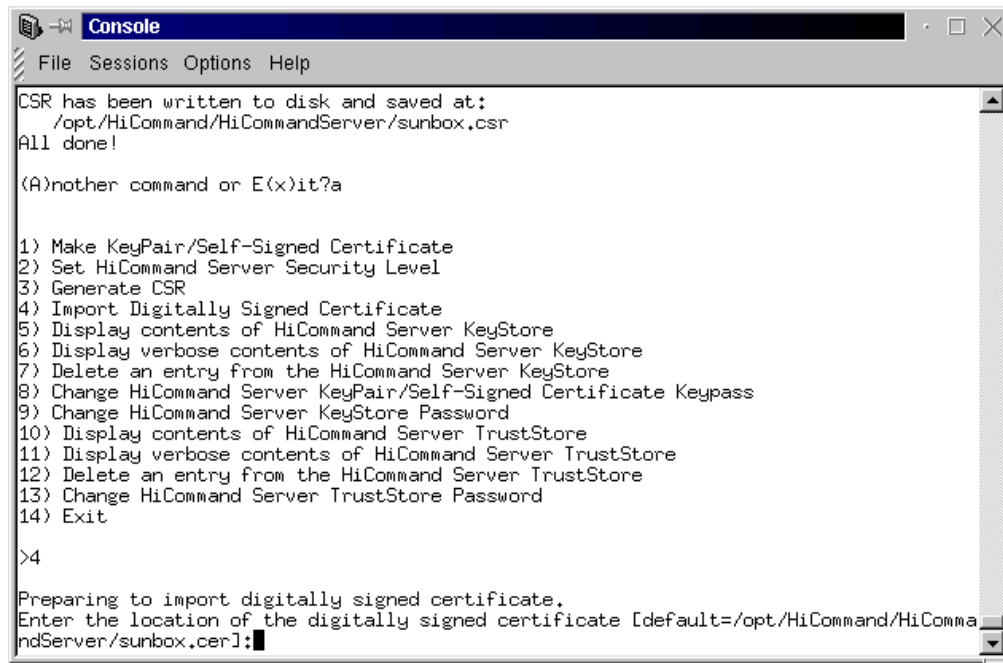
>4

Preparing to import digitally signed certificate.
Enter the location of the digitally signed certificate [default=C:\Program Files
\HiCommand\HiCommandServer\hishark.cer]:_

```

Figure 4.11 Entering the Location of the Digitally-Signed Certificate (Windows®)





```
Console
File Sessions Options Help

CSR has been written to disk and saved at:
/opt/HiCommand/HiCommandServer/sunbox.csr
All done!

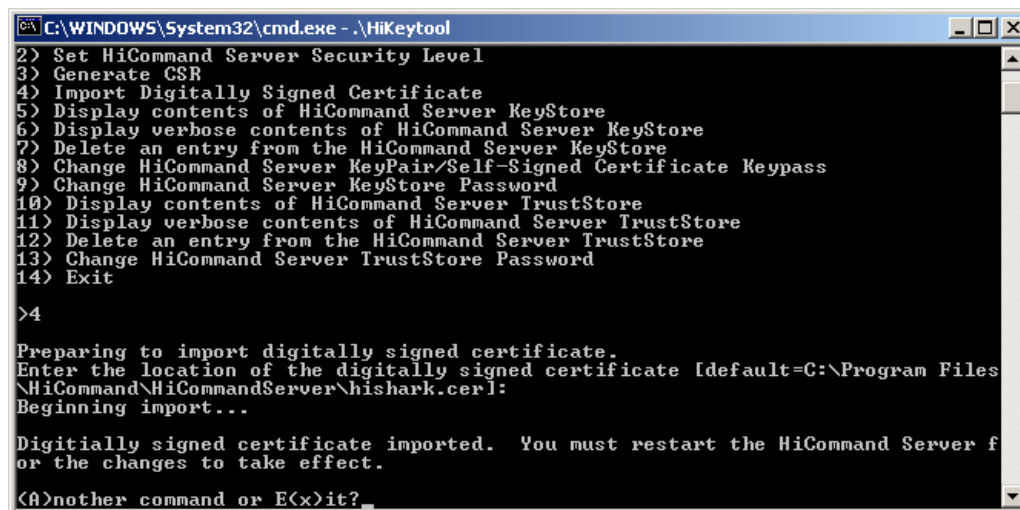
(A)nother command or E(x)it?a

1) Make KeyPair/Self-Signed Certificate
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>4

Preparing to import digitally signed certificate.
Enter the location of the digitally signed certificate [default=/opt/HiCommand/HiCommandServer/sunbox.cer]:
```

Figure 4.12 Entering the Location of the Digitally-Signed Certificate (Solaris®)



```
C:\WINDOWS\System32\cmd.exe - .\HiKeytool

2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>4

Preparing to import digitally signed certificate.
Enter the location of the digitally signed certificate [default=C:\Program Files\HiCommand\HiCommandServer\hishark.cer]:
Beginning import...

Digitally signed certificate imported. You must restart the HiCommand Server for the changes to take effect.

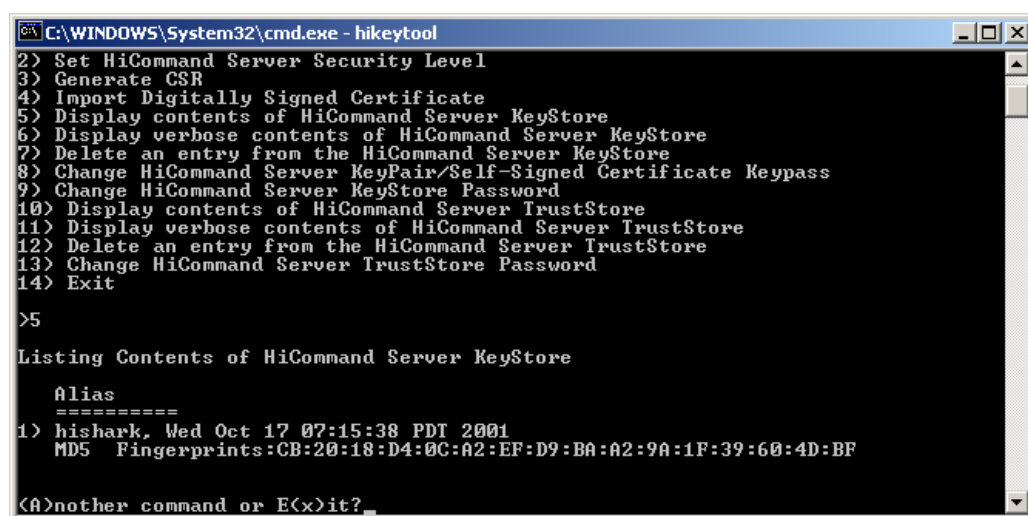
(A)nother command or E(x)it?_
```

Figure 4.13 Notification of Successful Import of Digitally-Signed Certificate

## 4.2.4 Displaying the Contents of the HiCommand™ Device Manager Keystore

### 4.2.4.1 Regular Mode

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool type **5** (Display Contents of HiCommand Server Keystore).
3. HiKeytool will display information similar to that in Figure 4.14, including the alias for the keystore entry, the date the entry was created, and the MD5 Fingerprints for the entry, as follows:



```
C:\WINDOWS\System32\cmd.exe - hikeytool
2> Set HiCommand Server Security Level
3> Generate CSR
4> Import Digitally Signed Certificate
5> Display contents of HiCommand Server Keystore
6> Display verbose contents of HiCommand Server Keystore
7> Delete an entry from the HiCommand Server Keystore
8> Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9> Change HiCommand Server Keystore Password
10> Display contents of HiCommand Server TrustStore
11> Display verbose contents of HiCommand Server TrustStore
12> Delete an entry from the HiCommand Server TrustStore
13> Change HiCommand Server TrustStore Password
14> Exit

>5

Listing Contents of HiCommand Server Keystore

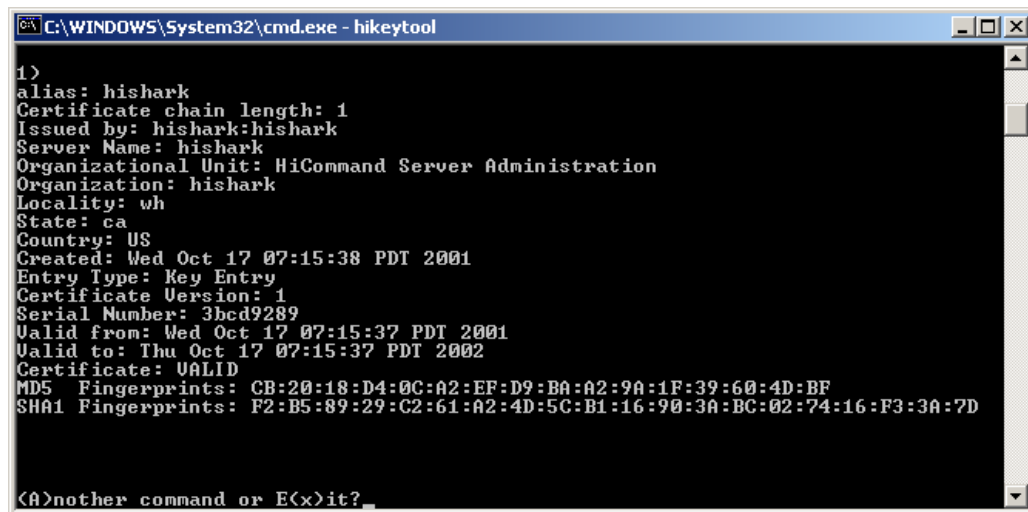
Alias
=====
1> hishark, Wed Oct 17 07:15:38 PDT 2001
MD5 Fingerprints:CB:20:18:D4:0C:A2:EF:D9:BA:A2:9A:1F:39:60:4D:BF

<A>nother command or E<x>it?_
```

Figure 4.14 Sample Contents of the HiCommand™ Device Manager Server Keystore

#### 4.2.4.2 Verbose Mode

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool type **6** (Display Verbose Contents of HiCommand Server Keystore).
3. HiKeytool will display the verbose contents of the HiCommand™ Device Manager server keystore (see Figure 4.15 for a sample).

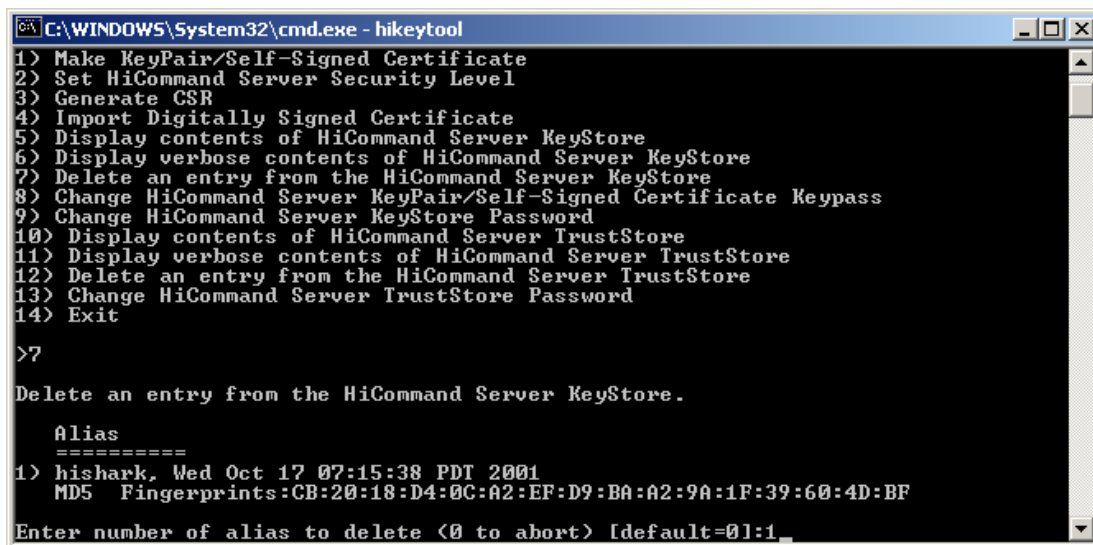


```
C:\WINDOWS\System32\cmd.exe - hikeytool
1>
alias: hishark
Certificate chain length: 1
Issued by: hishark:hishark
Server Name: hishark
Organizational Unit: HiCommand Server Administration
Organization: hishark
Locality: wh
State: ca
Country: US
Created: Wed Oct 17 07:15:38 PDT 2001
Entry Type: Key Entry
Certificate Version: 1
Serial Number: 3bed9289
Valid from: Wed Oct 17 07:15:37 PDT 2001
Valid to: Thu Oct 17 07:15:37 PDT 2002
Certificate: VALID
MD5 Fingerprints: CB:20:18:D4:0C:A2:EF:D9:BA:A2:9A:1F:39:60:4D:BF
SHA1 Fingerprints: F2:B5:89:29:C2:61:A2:4D:5C:B1:16:90:3A:BC:02:74:16:F3:3A:7D
<A>nother command or E<x>it?_
```

Figure 4.15 Sample Verbose Contents of the HiCommand™ Device Manager Server Keystore

#### 4.2.5 Deleting an Entry from the HiCommand™ Device Manager Server Keystore

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool type 7 (Delete an Entry from the HiCommand™ Device Manager Server Keystore).
3. This will display information about the contents of the HiCommand™ Device Manager server keystore, and prompt you to enter the number of the HiCommand™ Device Manager server keypair to be deleted (see Figure 4.16).
4. HiKeytool will request confirmation of the delete (see Figure 4.17). Type Y to confirm the delete.
5. HiKeytool will display the contents of the HiCommand™ Device Manager server keystore after the deletion.



```
C:\WINDOWS\System32\cmd.exe - hikeytool
1> Make KeyPair/Self-Signed Certificate
2> Set HiCommand Server Security Level
3> Generate CSR
4> Import Digitally Signed Certificate
5> Display contents of HiCommand Server KeyStore
6> Display verbose contents of HiCommand Server KeyStore
7> Delete an entry from the HiCommand Server KeyStore
8> Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9> Change HiCommand Server KeyStore Password
10> Display contents of HiCommand Server TrustStore
11> Display verbose contents of HiCommand Server TrustStore
12> Delete an entry from the HiCommand Server TrustStore
13> Change HiCommand Server TrustStore Password
14> Exit

>7

Delete an entry from the HiCommand Server KeyStore.

Alias
=====
1> hishark, Wed Oct 17 07:15:38 PDT 2001
MD5 Fingerprints:CB:20:18:D4:0C:A2:EF:D9:BA:A2:9A:1F:39:60:4D:BF

Enter number of alias to delete (0 to abort) [default=0]:1
```

Figure 4.16 Entering the Number of the Alias to be Deleted

```
C:\WINDOWS\System32\cmd.exe - hikeytool
3> Generate CSR
4> Import Digitally Signed Certificate
5> Display contents of HiCommand Server KeyStore
6> Display verbose contents of HiCommand Server KeyStore
7> Delete an entry from the HiCommand Server KeyStore
8> Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9> Change HiCommand Server KeyStore Password
10> Display contents of HiCommand Server TrustStore
11> Display verbose contents of HiCommand Server TrustStore
12> Delete an entry from the HiCommand Server TrustStore
13> Change HiCommand Server TrustStore Password
14> Exit

>7

Delete an entry from the HiCommand Server KeyStore.

Alias
=====
1) hishark, Wed Oct 17 07:15:38 PDT 2001
MD5 Fingerprints:CB:20:18:D4:0C:A2:EF:D9:BA:A2:9A:1F:39:60:4D:BF

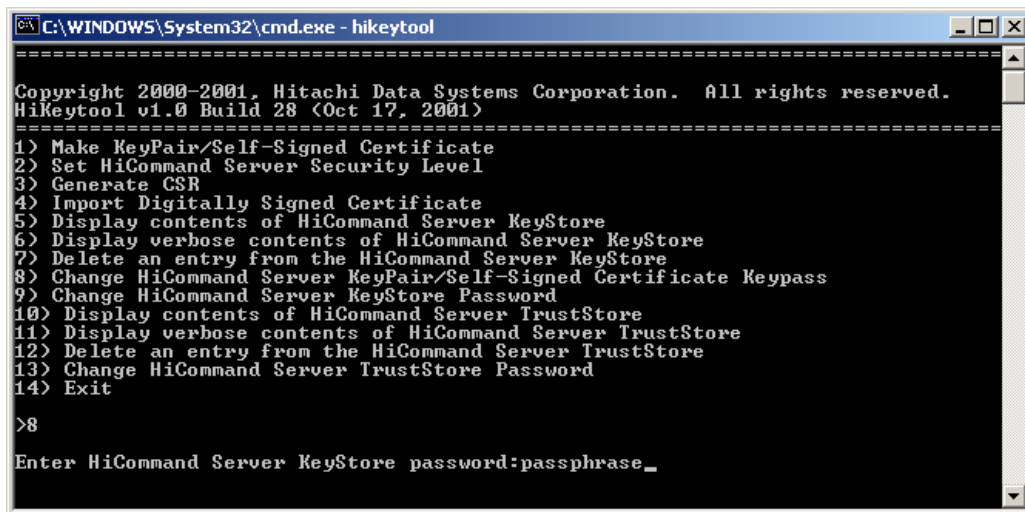
Enter number of alias to delete <0 to abort> [default=0]:1

Delete hishark [1] ? [default=No]:y_
```

Figure 4.17 Confirming the Deletion of an Alias

## 4.2.6 Changing the HiCommand™ Device Manager Server Keypass

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool type **8** (Change HiCommand Server Keypair/Self-Signed Certificate Keypass).
3. Type the existing HiCommand™ Device Manager server password.
4. Type the existing keypass and select **Enter** (see Figure 4.19).
5. Type the new keypass and select **Enter** (see Figure 4.20). This keypass is case sensitive.  
**Warning:** Be sure to enter only characters (A-Z, a-z), numbers (0-9) or whitespace, or you can render your keystore unusable.
6. You will be prompted for a confirmation of the new keypass. Type the new keypass again and select **Enter** (see Figure 4.20).
7. You will need to restart the server for the changes to be effective.



```
C:\WINDOWS\System32\cmd.exe - hikeytool
=====
Copyright 2000-2001, Hitachi Data Systems Corporation. All rights reserved.
HiKeytool v1.0 Build 28 (Oct 17, 2001)
=====
1) Make KeyPair/Self-Signed Certificate
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>8

Enter HiCommand Server KeyStore password:passphrase_
```

Figure 4.18 Entering the Current Password

```
C:\WINDOWS\System32\cmd.exe - hikeytool
=====
1) Make KeyPair/Self-Signed Certificate
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>8

Enter HiCommand Server KeyStore password:passphrase

Passwords must only contain characters <A-Z,a-z>, digits <0-9> and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old keypass:passphrase
```

Figure 4.19 Entering the Old Keypass

```
C:\WINDOWS\System32\cmd.exe - hikeytool
=====
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>8

Enter HiCommand Server KeyStore password:passphrase

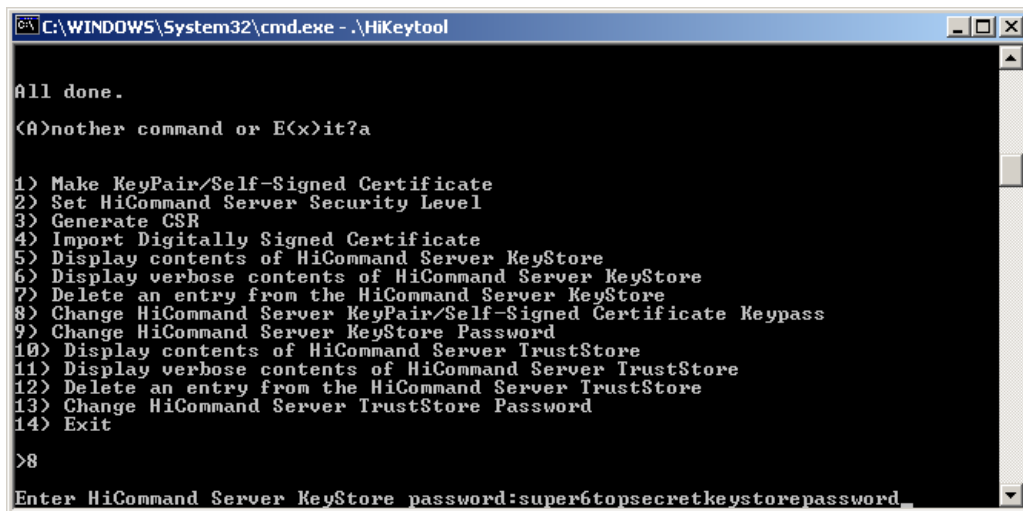
Passwords must only contain characters <A-Z,a-z>, digits <0-9> and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old keypass:passphrase
Enter new keypass:there's a wocket in my pocket
Confirm new keypass:there's a wocket in my pocket
```

Figure 4.20 Entering and Confirming the New Keypass

#### 4.2.7 Change the HiCommand™ Device Manager Server Keystore Password

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool type **9** (Change HiCommand Server Keystore Password).
3. Type the existing password, then select **Enter** (see Figure 4.21).
4. Type the existing keypass, then select **Enter** (see Figure 4.22).
5. You will be prompted for your new password. This password is case-sensitive. **Warning:** Be sure to enter only characters (A-Z, a-z), numbers (0-9) or whitespace, or you can render your keystore unusable. Type the new password and select **Enter** (see Figure 4.23).
6. Confirm the new password (see Figure 4.23).
7. You will have to restart the server for the changes to be effective.



```
C:\WINDOWS\System32\cmd.exe - .\HiKeytool

All done.
<A>nother command or E<x>it?a

1> Make KeyPair/Self-Signed Certificate
2> Set HiCommand Server Security Level
3> Generate CSR
4> Import Digitally Signed Certificate
5> Display contents of HiCommand Server KeyStore
6> Display verbose contents of HiCommand Server KeyStore
7> Delete an entry from the HiCommand Server KeyStore
8> Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9> Change HiCommand Server Keystore Password
10> Display contents of HiCommand Server TrustStore
11> Display verbose contents of HiCommand Server TrustStore
12> Delete an entry from the HiCommand Server TrustStore
13> Change HiCommand Server TrustStore Password
14> Exit

>8

Enter HiCommand Server KeyStore password:super6topsecretkeystorepassword_
```

Figure 4.21 Entering Existing Password



```
C:\WINDOWS\System32\cmd.exe - .\HiKeytool

1) Make KeyPair/Self-Signed Certificate
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>8

Enter HiCommand Server KeyStore password:super6topsecretkeystorepassword

Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old keypass:my1secret2key3password_
```

Figure 4.22 Entering Existing Keypass

```
C:\WINDOWS\System32\cmd.exe - .\HiKeytool

2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>8

Enter HiCommand Server KeyStore password:super6topsecretkeystorepassword

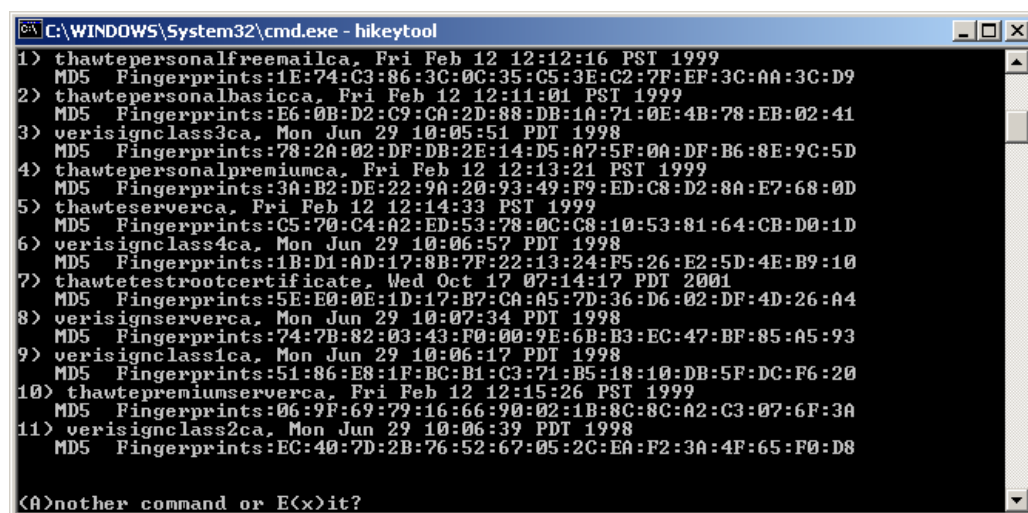
Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old keypass:my1secret2key3password
Enter new keypass:newsupersecretpassword
Confirm new keypass:newsupersecretpassword_
```

Figure 4.23 Entering and Confirming New Keypass

## 4.2.8 Display Contents of the HiCommand™ Device Manager Server Truststore

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool type 10 (Display Contents of HiCommand Server Truststore).
3. The display will include the entry alias, the date the certificate was created, and the MD5 Fingerprints for that entry (see Figure 4.24).



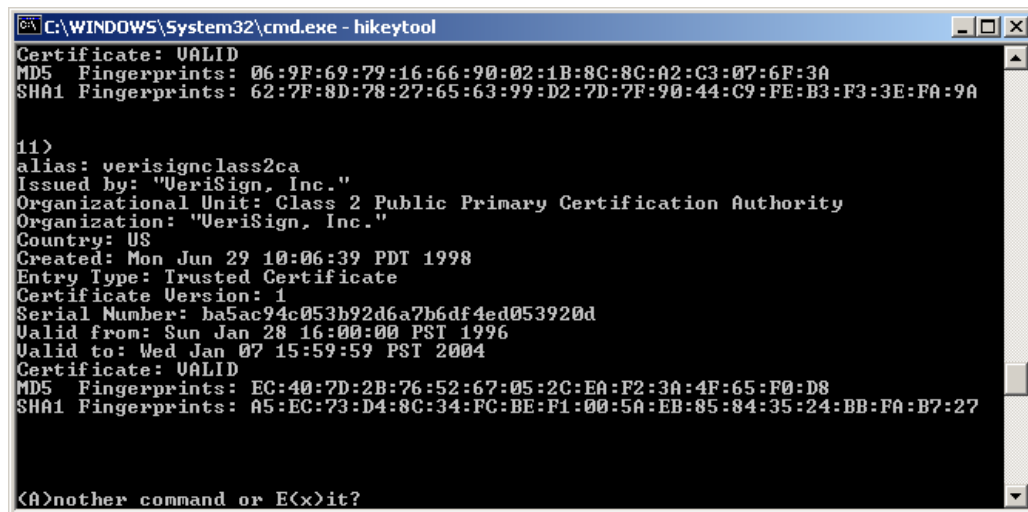
```
C:\WINDOWS\System32\cmd.exe - hikeytool
1> thawtepersonalfreemailca, Fri Feb 12 12:12:16 PST 1999
MD5 Fingerprints:1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
2> thawtepersonalbasicca, Fri Feb 12 12:11:01 PST 1999
MD5 Fingerprints:E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
3> verisignclass3ca, Mon Jun 29 10:05:51 PDT 1998
MD5 Fingerprints:78:2A:02:DF:DB:2E:14:D5:A7:5F:0A:DF:B6:8E:9C:5D
4> thawtepersonalpremiumca, Fri Feb 12 12:13:21 PST 1999
MD5 Fingerprints:3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D
5> thawteserverca, Fri Feb 12 12:14:33 PST 1999
MD5 Fingerprints:C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
6> verisignclass4ca, Mon Jun 29 10:06:57 PDT 1998
MD5 Fingerprints:1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
7> thawtetestrootcertificate, Wed Oct 17 07:14:17 PDT 2001
MD5 Fingerprints:5E:E0:0E:1D:17:B7:CA:A5:7D:36:D6:02:DF:4D:26:A4
8> verisignserverca, Mon Jun 29 10:07:34 PDT 1998
MD5 Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
9> verisignclass1ca, Mon Jun 29 10:06:17 PDT 1998
MD5 Fingerprints:51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20
10> thawtepremiumserverca, Fri Feb 12 12:15:26 PST 1999
MD5 Fingerprints:06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
11> verisignclass2ca, Mon Jun 29 10:06:39 PDT 1998
MD5 Fingerprints:EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8

<A>nother command or E<x>it?
```

Figure 4.24 Contents of HiCommand™ Device Manager Server Truststore

#### 4.2.9 Displaying the Verbose Contents of the HiCommand™ Device Manager Server Truststore

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool type 11 (Display Verbose Contents of HiCommand Server Truststore).
3. This will display the verbose information for each entry in the HiCommand™ Device Manager server truststore (see Figure 4.25).



```
C:\WINDOWS\System32\cmd.exe - hikeytool
Certificate: VALID
MD5 Fingerprints: 06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
SHA1 Fingerprints: 62:7F:8D:78:27:65:63:99:D2:7D:7F:90:44:C9:FE:B3:F3:3E:FA:9A

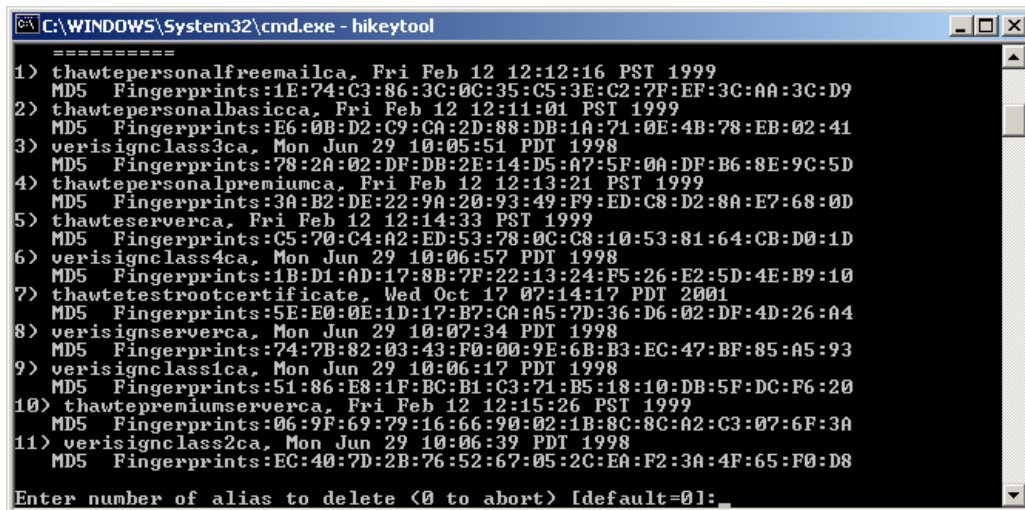
11>
alias: verisignclass2ca
Issued by: "VeriSign, Inc."
Organizational Unit: Class 2 Public Primary Certification Authority
Organization: "VeriSign, Inc."
Country: US
Created: Mon Jun 29 10:06:39 PDT 1998
Entry Type: Trusted Certificate
Certificate Version: 1
Serial Number: ba5ac94c053b92d6a7b6df4ed053920d
Valid from: Sun Jan 28 16:00:00 PST 1996
Valid to: Wed Jan 07 15:59:59 PST 2004
Certificate: VALID
MD5 Fingerprints: EC:40:7D:2B:76:52:67:05:2C:E0:F2:3A:4F:65:F0:D8
SHA1 Fingerprints: A5:EC:73:D4:8C:34:FC:BE:F1:00:5A:EB:85:84:35:24:BB:FA:B7:27

<A>nother command or E<x>it?
```

Figure 4.25 Displaying Verbose Information for the HiCommand™ Device Manager Truststore

#### 4.2.10 Deleting an Entry from the HiCommand™ Device Manager Server Truststore

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. From HiKeytool, type 12 (Delete an Entry from the HiCommand Server Truststore).
3. HiKeytool will display a list of all entries in the HiCommand™ Device Manager server truststore.
4. Type the number of the alias to be deleted from the HiCommand™ Device Manager server truststore, and select **Enter** (see Figure 4.26).
5. HiKeytool will request confirmation from the user to delete the designated entry. Type Y to delete the entry (see Figure 4.27).
6. HiKeytool will delete the nominated entry, re-list the contents of the HiCommand™ Device Manager server truststore, and note that the deletion has been completed.



```
C:\WINDOWS\System32\cmd.exe - hikeytool
=====
1) thawtepersonalfreemailca, Fri Feb 12 12:12:16 PST 1999
MD5 Fingerprints:1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
2) thawtepersonalbasicca, Fri Feb 12 12:11:01 PST 1999
MD5 Fingerprints:E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
3) verisignclass3ca, Mon Jun 29 10:05:51 PDT 1998
MD5 Fingerprints:78:2A:02:DF:DB:2E:14:D5:A7:5F:0A:DF:B6:8E:9C:5D
4) thawtepersonalpremiumca, Fri Feb 12 12:13:21 PST 1999
MD5 Fingerprints:3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D
5) thawteserverca, Fri Feb 12 12:14:33 PST 1999
MD5 Fingerprints:C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
6) verisignclass4ca, Mon Jun 29 10:06:57 PDT 1998
MD5 Fingerprints:1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
7) thawtetestrootcertificate, Wed Oct 17 07:14:17 PDT 2001
MD5 Fingerprints:5E:E0:0E:1D:17:B7:CA:A5:7D:36:D6:02:DF:4D:26:A4
8) verisignserverca, Mon Jun 29 10:07:34 PDT 1998
MD5 Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
9) verisignclass1ca, Mon Jun 29 10:06:17 PDT 1998
MD5 Fingerprints:51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20
10) thawtepremiumserverca, Fri Feb 12 12:15:26 PST 1999
MD5 Fingerprints:06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
11) verisignclass2ca, Mon Jun 29 10:06:39 PDT 1998
MD5 Fingerprints:EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8

Enter number of alias to delete <0 to abort> [default=0]:
```

Figure 4.26 Entering the Alias to be Deleted from the Truststore

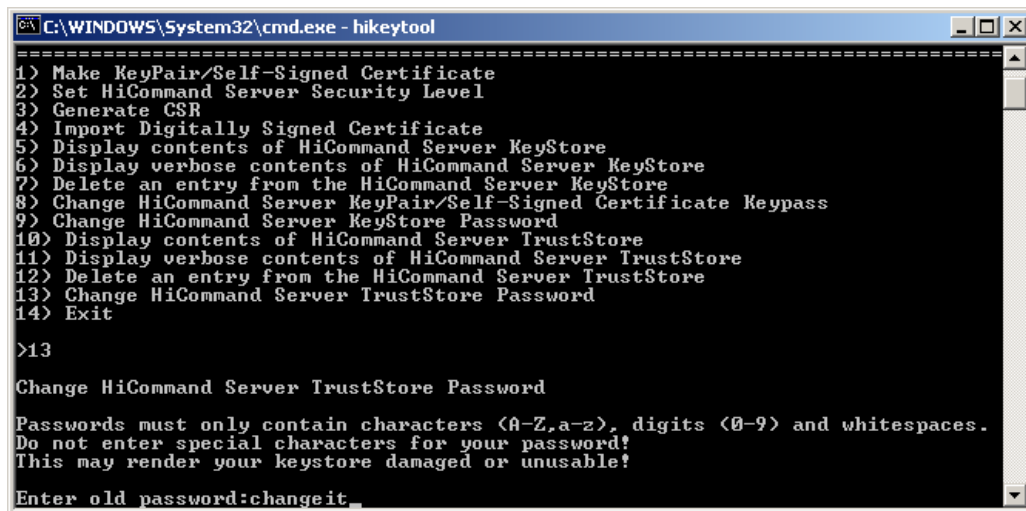
```
C:\WINDOWS\System32\cmd.exe - hikeytool
MD5 Fingerprints:1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
2> thawtpersonalbasicca, Fri Feb 12 12:11:01 PST 1999
MD5 Fingerprints:E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
3> verisignclass3ca, Mon Jun 29 10:05:51 PDT 1998
MD5 Fingerprints:78:2A:02:DF:DB:2E:14:D5:A7:5F:0A:DF:B6:8E:9C:5D
4> thawtpersonalpremiumca, Fri Feb 12 12:13:21 PST 1999
MD5 Fingerprints:3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D
5> thawteserverca, Fri Feb 12 12:14:33 PST 1999
MD5 Fingerprints:C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
6> verisignclass4ca, Mon Jun 29 10:06:57 PDT 1998
MD5 Fingerprints:1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
7> thawtetestrootcertificate, Wed Oct 17 07:14:17 PDT 2001
MD5 Fingerprints:5E:E0:0E:1D:17:B7:CA:A5:7D:36:D6:02:DF:4D:26:A4
8> verisignserverca, Mon Jun 29 10:07:34 PDT 1998
MD5 Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
9> verisignclass1ca, Mon Jun 29 10:06:17 PDT 1998
MD5 Fingerprints:51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20
10> thawtpremiumserverca, Fri Feb 12 12:15:26 PST 1999
MD5 Fingerprints:06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
11> verisignclass2ca, Mon Jun 29 10:06:39 PDT 1998
MD5 Fingerprints:EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8

Enter number of alias to delete (<0 to abort> [default=0]:?
Delete thawtetestrootcertificate [7] ? [default=No]:y
```

Figure 4.27 Confirming the Alias to be Deleted from the Truststore

#### 4.2.11 Changing the HiCommand™ Device Manager Server Truststore Password

1. Open a command line or terminal window and launch HiKeytool (refer to section 4.2.1 for instructions).
2. Select **13** (Change HiCommand Server Truststore Password).
3. Type the existing truststore password and select **Enter** (see Figure 4.28).
4. Type the new truststore password and select **Enter** (see Figure 4.29). This password is case sensitive. **Warning:** Be sure to enter only characters (A-Z, a-z), numbers (0-9) or whitespace, or you can render your keystore unusable.
5. Type the new password in again, and select **Enter** (see Figure 4.29).
6. You will need to restart the server for the changes to take effect.



```
C:\WINDOWS\System32\cmd.exe - hikeytool
=====
1) Make KeyPair/Self-Signed Certificate
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

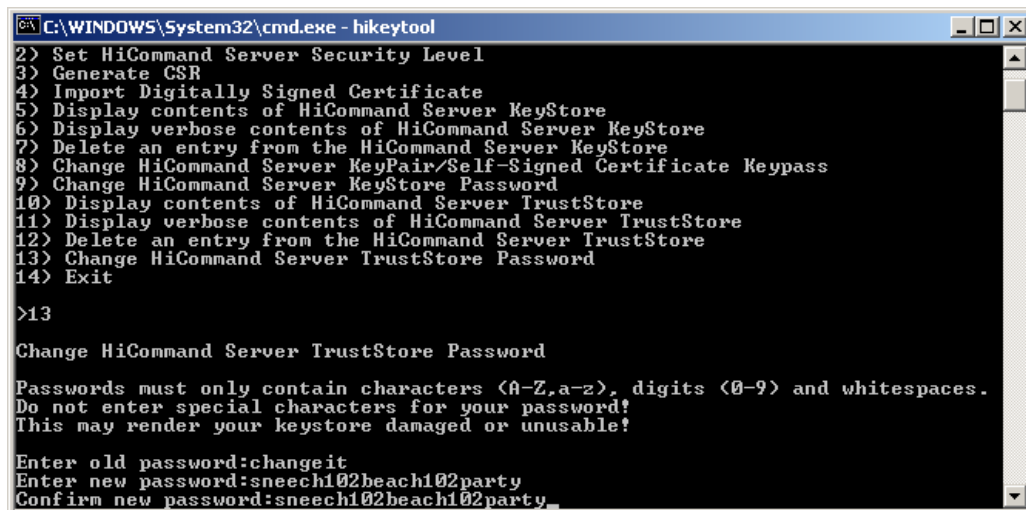
>13

Change HiCommand Server TrustStore Password

Passwords must only contain characters <A-Z,a-z>, digits <0-9> and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old password:changeit_
```

Figure 4.28 Entering Old Server Truststore Password



```
C:\WINDOWS\System32\cmd.exe - hikeytool
=====
2) Set HiCommand Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of HiCommand Server KeyStore
6) Display verbose contents of HiCommand Server KeyStore
7) Delete an entry from the HiCommand Server KeyStore
8) Change HiCommand Server KeyPair/Self-Signed Certificate Keypass
9) Change HiCommand Server KeyStore Password
10) Display contents of HiCommand Server TrustStore
11) Display verbose contents of HiCommand Server TrustStore
12) Delete an entry from the HiCommand Server TrustStore
13) Change HiCommand Server TrustStore Password
14) Exit

>13

Change HiCommand Server TrustStore Password

Passwords must only contain characters <A-Z,a-z>, digits <0-9> and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old password:changeit
Enter new password:sneechi02beach102party
Confirm new password:sneechi02beach102party_
```

Figure 4.29 Entering and Confirming New Password

# Chapter 5 Troubleshooting

## 5.1 Contacting the Hitachi Data Systems Technical Support Center

If you need to call the Hitachi Data Systems Technical Support Center, be sure to provide as much information about the problem as possible, including the circumstances surrounding the error or failure, and the exact content of any error messages.

The worldwide Hitachi Data Systems Technical Support Centers are:

- Hitachi Data Systems North America/Latin America  
San Diego, California, USA  
1-800-348-4357
- Hitachi Data Systems Europe  
Contact Hitachi Data Systems Local Support
- Hitachi Data Systems Asia Pacific  
North Ryde, Australia  
011-61-2-9325-3300





## Glossary, Acronyms, and Abbreviations

DASD	direct access storage device
DKCMAIN	software for the service processor (SVP), which is the notebook computer that is part of the 9900 subsystem
GB	gigabyte(s)
kB	kilobyte(s)
LAN	local-area network
LDEV	logical device
LUN Manager	A Remote Console software option that allows users to add and delete SCSI paths, set host and port modes, configure the fibre-channel topology, and set or release high-speed mode. See the <i>LUN Manager User's Guide</i> (MK-91RD049) for more information.
RMCMAIN	remote console main software
SANTinel™	A Remote Console software option that allows the user to set or change security parameters for one or more ports, set or change LUN group definitions, and set or change WWN or WWN group parameters. See the <i>LUN Manager User's Guide</i> (MK-91RD049) for more information.
SNMP	Simple network management protocol (part of the TCP/IP protocol suite). <b>Note:</b> The Windows® SNMP service is included as part of Windows®. The Hitachi SNMP Agent is a program product that must also be installed on the SVP and on each subsystem. See the <i>Remote Console User's Guide</i> (MK-90RD003) for more information.
TCP/IP	transmission control protocol/internet protocol
WWN	Worldwide name, which is a unique identifier for a particular open-system host bus adapter consisting of a 64-bit physical address (the IEEE 48-bit format with 12-bit extension and 4-bit prefix).



# Index

## C

- changing server keypass
  - entering and confirming new keypass
    - illustration, 35
  - entering current password
    - illustration, 34
  - entering old keypass
    - illustration, 35
  - instructions, 34
- changing server keystore password
  - entering and confirming new keypass
    - illustration, 37
  - entering existing keypass
    - illustration, 37
  - entering existing password
    - illustration, 36
  - instructions, 36
- changing truststore password
  - entering and confirming new password
    - illustration, 42
  - entering old password
    - illustration, 42
  - instructions, 42
- configuring networks, 1-8
  - common security risks, 3
  - dual-homed management servers plus separate management LAN, 7
  - flat network, 8
  - overview, 1
  - separate management LAN plus firewall, 4
  - separate management LAN plus firewalled devices, 6
- creating a keypair
  - instructions, 18
  - Solaris® illustration 1, 21
  - Solaris® illustration 2, 22
  - Windows® illustration 1, 20
  - Windows® illustration 2, 21
- creating CSR
  - illustration, 26
  - instructions, 25
  - sample CSR, 26

## D

- deleting keystore entry
  - confirming deletion
    - illustration, 33
  - entering alias number
    - illustration, 32
  - instructions, 32
- deleting truststore entry

confirming alias

illustration, 41

entering alias

illustration, 40

instructions, 40

Device Manager

overview, 1

overview of software components, 2

displaying keystore contents (regular mode)

illustration, 30

instructions, 30

displaying keystore contents (verbose mode)

illustration, 31

instructions, 31

displaying truststore contents

illustration, 38

instructions, 38

displaying verbose truststore contents

illustration, 39

instructions, 39

dual-homed management servers plus separate management LAN

illustration, 7

## E

enabling TLS/SSL

changing TLS/SSL level

illustration, 24

displaying default level

illustration, 23

instructions, 23

## F

flat network

illustration, 8

## G

glossary, acronyms and abbreviations, 45

## H

HiKeytool main panel

illustration, 20

## I

importing signed certificate

entering certificate location

Solaris® illustration, 29

Windows® illustration, 28

instructions, 27

notification of successful import

illustration, 29

- sample signed certificate, 28
- Incorrect 9900 and 9900V LAN Connection illustration, 2

## O

- overview

- Device Manager, 1
- Device Manager security, 15-17
- Device Manager software components, 2
- security properties
  - description, 10-13
  - table, 9

## S

- security panels

- creating a keypair
  - Solaris® illustration 1, 21
  - Solaris® illustration 2, 22
  - Windows® illustration 1, 20
  - Windows® illustration 2, 21

- creating CSR

- illustration, 26

- creating CSR

- sample CSR, 26

- enabling TLS/SSL

- changing TLS/SSL level
  - illustration, 24

- displaying default level
  - illustration, 23

- HiKeytool main panel, 20

- security procedures

- changing server keypass

- instructions, 34

- changing server keystore password

- instructions, 36

- changing truststore password

- instructions, 42

- configuring networks, 1-8

- common security risks, 3

- dual-homed management servers plus
  - separate management LAN, 7

- flat network, 8

- overview, 1

- separate management LAN plus firewall, 4

- separate management LAN plus firewalled devices, 6

- creating a keypair

- instructions, 18

- creating and importing signed certificate

- instructions, 25-29

- creating CSR

- instructions, 25

- deleting keystore entry

- instructions, 32

- deleting truststore entry

- instructions, 40

- displaying keystore contents (regular mode)

- instructions, 30

- displaying keystore contents (verbose mode)

- instructions, 31

- displaying truststore contents

- instructions, 38

- displaying verbose truststore contents

- instructions, 39

- enabling TLS/SSL

- instructions, 23

- importing signed certificate

- instructions, 27

- security properties

- descriptions

- in general, 10-13

- server.http.secure, 10

- server.http.security.clientIP, 10

- server.http.security.realm, 10

- server.http.security.unprotected, 11

- server.https.keystore.keypass, 11

- server.https.keystore.passphrase, 11

- server.https.security.keystore, 11

- server.https.security.truststore, 12

- server.https.truststore, 13

- server.security.logonID.caseSensitive, 13

- table, 9

- separate management LAN plus firewall

- illustration, 5

- separate management LAN plus firewalled

- devices

- illustration, 6

- signed certificate

- creating and importing

- instructions, 25-29

## T

- troubleshooting

- contacting Hitachi Data Systems, 43