



# Sun StorageTek™ Crypto Key Management System (KMS)

## Administration Guide

Part Number: 316195102

Revision: A

Version: 2.1





# Crypto Key Management System (KMS)

---

## Administration Guide

Version 2.1  
Revision A

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part No. 316195102

Submit comments about this document at:  
<http://www.sun.com/hwdocs/feedback>

Copyright © 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

Use is subject to license terms.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, Jiro, Solaris and Sun StorEdge are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

This product is covered and controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

---

Copyright © 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

L'utilisation est soumise aux termes de la Licence.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, Jiro, Solaris et Sun StorEdge sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Ce produit est soumis à la législation américaine en matière de contrôle des exportations et peut être soumis à la réglementation en vigueur dans d'autres pays dans le domaine des exportations et importations. Les utilisations, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers les pays sous embargo américain, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exhaustive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

We welcome your feedback. Use the OpinionLab [+] feedback system on the documentation Web site or Send your comments to:

Storage Technical Publications  
Sun Microsystems, Inc.  
500 Eldorado Blvd.  
Mailstop: UBRM06-307  
Broomfield, CO 80021-6307  
USA

Please include the publication name, part number, and edition number in your correspondence if they are available.  
This will expedite our response.



# Revision History

---

| EC       | Date          | Revision | Description  |
|----------|---------------|----------|--|
| EC000826 | January, 2009 | A        | <i>Crypto Key Management System 2.1 Administration Guide</i> |



# Contents

---

**Revision History**   iii

**Contents**   v

**Figures**   xv

**Tables**   xvii

**What's New?**   xix

**Preface**   xxi

**1. Introduction**   1

Overview   1

KMS Concepts   2

    KMS Clusters   2

    Agents   2

    Network Connections   2

    Initial Setup - Direct Connection or Remote Console   3

    Initial Setup - QuickStart Program   4

    Key Lifecycle   4

    State Transition   5

    KMS States and Transitions   6

        Pre-activation   6

        Active   6

        Deactivated   7

        Compromised   7

|  |           |
|--|-----------|
| Destroyed/Destroyed Compromised                      | 7         |
| Users and Role-based Access Control                  | 9         |
| Allowed Operations for Each Role                     | 9         |
| Quorum Protection                                    | 9         |
| Data Units, Keys, Key Groups, and Key Policies       | 10        |
| TCP/IP Connections and the KMA                       | 11        |
| KMS in the Network                                   | 12        |
| KMS Manager Software Requirements                    | 13        |
| Using Online Help                                    | 13        |
| Role-Based Access Control                            | 13        |
| Role-Based Operations                                | 14        |
| Setting Up and Managing the Key Management Appliance | 18        |
| <b>2. Getting Started</b>                            | <b>19</b> |
| Starting the Embedded Light Out Manager              | 20        |
| Connecting to the KMA                                | 20        |
| Using a Network Connection                           | 21        |
| Running the QuickStart Program                       | 25        |
| Starting QuickStart                                  | 26        |
| Specifying the Network Configuration                 | 27        |
| Initializing the KMA                                 | 32        |
| Configuring the Cluster                              | 33        |
| Entering Key Split Credentials                       | 34        |
| Entering Initial Security Officer User Credentials   | 36        |
| Specifying the Autonomous Unlocking Preference       | 37        |
| Setting the Key Pool Size                            | 38        |
| Synchronizing KMA Time                               | 39        |
| Joining an Existing Cluster                          | 40        |
| Restoring a Cluster From a Backup                    | 43        |
| Adding Agents and Enrolling Tape Drives              | 50        |
| <b>3. Using the KMS Manager</b>                      | <b>51</b> |
| What is the KMS Manager?                             | 51        |
| Installing the KMS Manager Software                  | 52        |



|   |           |
|---|-----------|
| SDM Download                                | 56        |
| Direct Download                             | 60        |
| Starting the KMS Installation               | 61        |
| Invoking the KMS Manager                    | 68        |
| Starting the KMS Manager with Windows       | 68        |
| Starting the KMS Manager with Solaris       | 68        |
| KMS Manager GUI Overview                    | 69        |
| System Menu                                 | 70        |
| View Menu                                   | 71        |
| Help Menu                                   | 72        |
| Toolbar Buttons                             | 74        |
| Shortcut Keys                               | 74        |
| Menu Accelerator Keys                       | 74        |
| Using Online Help                           | 75        |
| KMS Manager GUI Panes                       | 76        |
| KMS Management Operations Tree Pane         | 76        |
| KMS Management Operation Details Pane       | 77        |
| Session Audit Log Pane                      | 78        |
| Status Bar                                  | 79        |
| Panels                                      | 80        |
| Uninstalling the KMS Manager Software       | 82        |
| Invoking the Executable File                | 82        |
| Invoking Add/Remove Programs (Windows Only) | 82        |
| Completing the Uninstall Process            | 83        |
| <b>4. Using the System Menu</b>             | <b>85</b> |
| Connecting to the Cluster                   | 85        |
| Creating a Cluster Profile                  | 85        |
| Deleting a Cluster Profile                  | 89        |
| Disconnecting from the KMA                  | 89        |
| Changing the Passphrase                     | 90        |
| Specifying the Configuration Settings       | 91        |
| Exiting from the KMS Manager                | 93        |

|   |           |
|---|-----------|
| <b>5. Security Officer Operations</b>       | <b>95</b> |
| Security Officer Role                       | 96        |
| KMA List Menu                               | 97        |
| Viewing KMAs                                | 98        |
| Creating a KMA                              | 102       |
| Viewing/Modifying a KMA's Details           | 105       |
| Setting a KMA Passphrase                    | 107       |
| Deleting a KMA                              | 108       |
| User List Menu                              | 109       |
| Viewing Users                               | 110       |
| Creating a User                             | 113       |
| Viewing/Modifying a User's Details          | 115       |
| Setting a User's Passphrase                 | 117       |
| Deleting Users                              | 119       |
| Role List Menu                              | 120       |
| Viewing Roles                               | 120       |
| Viewing Operations for a Role               | 122       |
| Site List Menu                              | 123       |
| Viewing Sites                               | 124       |
| Creating a Site                             | 127       |
| Viewing/Modifying a Site's Details          | 129       |
| Deleting a Site                             | 130       |
| SNMP Manager List Menu                      | 131       |
| Viewing a KMA's SNMP Managers               | 131       |
| Creating a New SNMP Manager                 | 134       |
| Viewing/Modifying an SNMP Manager's Details | 136       |
| Deleting an SNMP Manager                    | 137       |
| Key Transfer                                | 138       |
| Overview                                    | 138       |
| Key Transfer Partners Feature               | 138       |
| Key Transfer Process                        | 139       |
| Configuring Key Transfer Partners           | 139       |
| Exporting/Importing Keys                    | 141       |

|   |     |
|---|-----|
| Transfer Partners Menu                      | 142 |
| Transfer Partner List Menu                  | 143 |
| Creating a Transfer Partner                 | 147 |
| Viewing/Modifying Transfer Partner Details  | 150 |
| Deleting a Transfer Partner                 | 153 |
| Key Transfer Public Key List Menu           | 154 |
| Viewing the Key Transfer Public Key List    | 154 |
| Viewing the Key Transfer Public Key Details | 157 |
| Creating a Key Transfer Public Key          | 158 |
| Backup List Menu                            | 159 |
| Viewing Backup Files History                | 160 |
| Viewing Backup Details                      | 163 |
| Restoring a Backup                          | 165 |
| System Dump Menu                            | 168 |
| Creating a System Dump                      | 168 |
| Security Parameters Menu                    | 170 |
| Retrieving the Security Parameters          | 170 |
| Modifying the Security Parameters           | 172 |
| Core Security                               | 173 |
| Core Security Management Menu               | 174 |
| Backup Core Security                        | 175 |
| Creating a Core Security Backup             | 175 |
| Key Split Configuration                     | 177 |
| Viewing the Key Split Configuration         | 177 |
| Modifying the Key Split Configuration       | 178 |
| Autonomous Unlock Option                    | 180 |
| Local Configuration Menu                    | 182 |
| Lock/Unlock KMA                             | 183 |
| Locking the KMA                             | 183 |
| Unlocking the KMA                           | 184 |
| Network Configuration Information           | 187 |
| Displaying the Network Configuration        | 187 |
| System Time Menu                            | 189 |

|  |            |
|--|------------|
| Retrieving the Local Clock Information         | 189        |
| Adjusting the KMA's Local Clock                | 191        |
| <b>6. Compliance Officer Operations</b>        | <b>193</b> |
| Compliance Officer Role                        | 193        |
| Key Policies                                   | 194        |
| Key Policy List Menu                           | 194        |
| Viewing Key Policies                           | 194        |
| Creating a Key Policy                          | 198        |
| Viewing/Modifying a Key Policy                 | 200        |
| Deleting a Key Policy                          | 201        |
| Key Groups                                     | 202        |
| Key Groups Menu                                | 204        |
| Key Group List Menu                            | 204        |
| Viewing Key Groups                             | 205        |
| Creating a Key Group                           | 208        |
| Viewing/Modifying a Key Group's Details        | 210        |
| Deleting a Key Group                           | 211        |
| Agent Assignment to Key Groups Menu            | 212        |
| Assigning an Agent to a Key Group              | 214        |
| Removing an Agent from a Key Group             | 216        |
| Key Group Assignment to Agents Menu            | 218        |
| Assigning a Key Group to an Agent              | 221        |
| Removing a Key Group from an Agent             | 223        |
| Key Group Assignment to Transfer Partners Menu | 225        |
| Viewing Key Group Assignments                  | 226        |
| Adding a Key Group to a Transfer Partner       | 227        |
| Removing a Key Group from a Transfer Partner   | 228        |
| Transfer Partner Assignment to Key Groups Menu | 229        |
| Viewing Transfer Group Assignments             | 230        |
| Adding a Transfer Partner to a Key Group       | 231        |
| Removing a Transfer Partner from a Key Group   | 232        |
| Importing a KMS 1.0 Key Export File            | 233        |
| Audit Event List Menu                          | 235        |

|   |            |
|---|------------|
| Viewing Audit Logs                          | 235        |
| Viewing Audit Log Details                   | 239        |
| Exporting an Audit Log                      | 240        |
| Data Units Menu                             | 241        |
| Other Functions                             | 242        |
| <b>7. Operator Operations</b>               | <b>243</b> |
| Operator Role                               | 243        |
| Key Groups Menu                             | 244        |
| Key Group List                              | 244        |
| Agent Assignment to Key Groups              | 244        |
| Transfer Partner Assignment to Key Groups   | 244        |
| Agent List Menu                             | 245        |
| Viewing the Agent List                      | 246        |
| Creating an Agent                           | 249        |
| Viewing/Modifying an Agent                  | 252        |
| Setting an Agent's Passphrase               | 253        |
| Deleting Agents                             | 254        |
| Key Group Assignment to Agents Menu         | 255        |
| Import Keys Menu                            | 256        |
| Data Units                                  | 258        |
| Data Unit List Menu                         | 258        |
| Viewing Data Units                          | 259        |
| Viewing/Modifying Data Unit Details         | 262        |
| Destroying Post-operational Keys            | 268        |
| Software Upgrade Menu                       | 269        |
| Guidelines for Performing Software Upgrades | 269        |
| Uploading and Applying Software Upgrades    | 270        |
| Backup List Menu                            | 272        |
| Audit Event List Menu                       | 272        |
| KMA List Menu                               | 272        |
| Site List Menu                              | 272        |
| SNMP Manager List Menu                      | 272        |
| System Time Menu                            | 272        |

|            |  |            |
|------------|--|------------|
|            | Lock/Unlock KMA Menu                   | 272        |
| <b>8.</b>  | <b>Backup Operator Operations</b>      | <b>273</b> |
|            | Backup Operator Role                   | 273        |
|            | Backup List Menu                       | 273        |
|            | Viewing Backup Files History           | 274        |
|            | Viewing Backup Details                 | 275        |
|            | Creating a Backup                      | 277        |
|            | Confirming a Backup's Destruction      | 278        |
|            | Backup Command Line Utility            | 279        |
|            | Solaris Syntax                         | 279        |
|            | Windows Syntax                         | 279        |
|            | Parameter Descriptions                 | 279        |
|            | Example                                | 280        |
|            | IPv6 Addresses with Zone IDs           | 280        |
|            | KMA List Menu                          | 282        |
|            | Modifying a Key Pool Size              | 282        |
|            | Other Functions                        | 284        |
| <b>9.</b>  | <b>Auditor Operations</b>              | <b>285</b> |
|            | Auditor Role                           | 285        |
|            | Audit List Menu                        | 285        |
|            | Security Parameters Menu               | 285        |
|            | Other Functions                        | 286        |
| <b>10.</b> | <b>Using the KMS Console</b>           | <b>287</b> |
|            | What is the KMS Console?               | 287        |
|            | Logging into the KMA                   | 288        |
|            | Operator                               | 289        |
|            | Security Officer                       | 290        |
|            | Other Roles                            | 291        |
|            | Operator Role Functions                | 292        |
|            | Rebooting the KMA                      | 293        |
|            | Shutting Down the KMA                  | 293        |
|            | Enabling the Technical Support Account | 294        |

|   |            |
|---|------------|
| Disabling the Technical Support Account               | 295        |
| Disabling the Primary Administrator                   | 296        |
| Setting the Keyboard Layout                           | 297        |
| Logging Out   | 298        |
| Security Officer Role Functions                       | 299        |
| Logging the KMA Back into the Cluster                 | 300        |
| Setting a User's Passphrase                           | 302        |
| Setting the KMA Management IP Address                 | 303        |
| Setting the KMA Service IP Addresses                  | 305        |
| Viewing/Adding/Deleting Gateways                      | 307        |
| Specifying the DNS Settings                           | 309        |
| Resetting the KMA to the Factory Default              | 310        |
| Enabling the Technical Support Account                | 312        |
| Disabling the Technical Support Account               | 314        |
| Enabling the Primary Administrator                    | 315        |
| Disabling the Primary Administrator                   | 316        |
| Setting the Keyboard Layout                           | 317        |
| Logging Out   | 318        |
| Other Role Functions                                  | 319        |
| Setting the Keyboard Layout                           | 320        |
| Logging Out   | 321        |
| <b>A. SNMP Management Information Base (MIB) Data</b> | <b>323</b> |
| <b>Glossary</b>                                       | <b>325</b> |
| <b>Index</b>  | <b>333</b> |





# Figures

---

|            |  |     |
|------------|--|-----|
| FIGURE 1-1 | Connections to the KMA                                       | 3   |
| FIGURE 1-2 | Key Lifecycle Periods  | 4   |
| FIGURE 1-3 | State Transition Diagram                                     | 5   |
| FIGURE 1-4 | Typical Deployment of KMS Solution                           | 12  |
| FIGURE 2-1 | Embedded Lights Out Manager Login Screen                     | 21  |
| FIGURE 2-2 | Power Control  | 22  |
| FIGURE 6-1 | Key Group Relationship with Key Policies, Agents, Data Units | 203 |



# Tables

---

|           |  |     |
|-----------|--|-----|
| TABLE 1-1 | KMA Port Connections                     | 11  |
| TABLE 1-2 | Other Services                           | 11  |
| TABLE 1-3 | System Operations/User Roles             | 14  |
| TABLE 2-1 | Compatible Web Browser and Java Versions | 20  |
| TABLE P-1 | KMA Object Identifiers                   | 323 |



# What's New?

KMS Release 2.1 includes the following enhancements:

## **Revision A:**

| Enhancement  | Primary Location  |
|--|---|
| A table has been added that lists KMA and unused port connections.   | <a href="#">“TCP/IP Connections and the KMA” on page 11</a>   |
| In the QuickStart program, the “Setting the IP Address” function has been split into four separate processes: <ul style="list-style-type: none"><li>■ Set KMA Management IP Addresses</li><li>■ Set KMA Service IP Addresses</li><li>■ Modify Gateway Settings</li><li>■ Set DNS Configuration</li></ul> | <ul style="list-style-type: none"><li>■ <a href="#">“Setting the KMA Management IP Addresses” on page 27</a></li><li>■ <a href="#">“Setting the KMA Service IP Addresses” on page 28</a></li><li>■ <a href="#">“Viewing/Adding/Deleting Gateways” on page 29</a></li><li>■ <a href="#">“Specifying the DNS Settings” on page 31</a></li></ul> |
| A procedure describing how to add agents and enroll tape drives appears under the “Running the QuickStart Program” topic.  | <a href="#">“Adding Agents and Enrolling Tape Drives” on page 50</a>  |
| Separate procedures, one for Windows and the other for Solaris, describe how to start the KMS installer.   | <a href="#">“Starting the KMS Installation” on page 61</a>  |
| The KMA List menu and KMA details dialog box include Management Network Address (IPv6) and Service Network Address (IPv6) columns.   | <ul style="list-style-type: none"><li>■ <a href="#">“Viewing KMAs” on page 98</a></li><li>■ <a href="#">“Viewing/Modifying a KMA’s Details” on page 105</a></li></ul>   |
| The Key Split Quorum Authentication dialog displays when you change a User’s roles or passphrase in the User Details dialog and when you change a KMA’s passphrase in the KMA Details dialog.  | <ul style="list-style-type: none"><li>■ <a href="#">“Viewing/Modifying a KMA’s Details” on page 105</a></li><li>■ <a href="#">“Viewing/Modifying a User’s Details” on page 115</a></li></ul>  |
| The Transfer Partner List menu and Transfer Partners Details dialog contains an Export Format column. This indicates whether keys can be wrapped (wrap keys encrypt the media key on the LAN and the token.)   | <a href="#">“Transfer Partner List Menu” on page 143</a>  |
| The Security Parameters menu and Modify dialog box display a FIPS Mode Only field, which determines whether the KMA can import 1.0 keys or import/export v2.x (FIPS) format transfer files.  | <ul style="list-style-type: none"><li>■ <a href="#">“Retrieving the Security Parameters” on page 170</a></li><li>■ <a href="#">“Modifying the Security Parameters” on page 172</a></li></ul>  |
| The Network Configuration menu shows network configuration settings for the KMA to which you are currently connected.  | <a href="#">“Network Configuration Information” on page 187</a>   |

---

**Revision A:**

| Enhancement   | Primary Location  |
|---|---|
| The Audit Event Details dialog displays Previous and Next buttons. These buttons display the previous or next Audit Event currently displayed in the Audit Event List panel.  | <a href="#">“Viewing Audit Log Details” on page 239</a>   |
| For Windows system users, the Backup Command Line utility allows you to enter link-local IPv6 addresses.  | <a href="#">“IPv6 Addresses with Zone IDs” on page 280</a>  |
| In the KMS Console, the “Log KMA into Cluster” menu selection has been changed to “Log KMA Back into Cluster.”  | <a href="#">“Security Officer Role Functions” on page 299</a>   |
| In the KMS Console, the “Set KMA IP Addresses” screen has been divided into four separate screens: <ul style="list-style-type: none"><li>■ Set KMA Management IP Addresses</li><li>■ Set KMA Service IP Addresses</li><li>■ Modify Gateway Settings</li><li>■ Set DNS Configuration</li></ul> | <ul style="list-style-type: none"><li>■ <a href="#">“Setting the KMA Management IP Address” on page 303</a></li><li>■ <a href="#">“Setting the KMA Service IP Addresses” on page 305</a></li><li>■ <a href="#">“Viewing/Adding/Deleting Gateways” on page 307</a></li><li>■ <a href="#">“Specifying the DNS Settings” on page 309</a></li></ul> |
| The <i>SNMP Management Information Base (MIB) Data</i> appendix describes SNMP information for users who have configured an SNMP Agent in their network and have defined SNMP Managers in the KMS Manager GUI.  | <a href="#">“SNMP Management Information Base (MIB) Data” on page 323</a>   |

---

# Preface

---

---

## Audience

This guide provides configuration and administration information for Sun Microsystems StorageTek™ Crypto Key Management System (KMS) software. It is intended for storage administrators, system programmers and operators responsible for configuring and maintaining the KMS software at their site.

---

## Organization of This Guide

This guide contains the following chapters:

- Introduction
- Getting Started
- Using the KMS Manager
- Using the System Menu
- Security Officer Operations
- Compliance Officer Operations
- Operator Operations
- Backup Operator Operations
- Auditor Operations
- Using the KMS Console

An index and glossary are also included.

## Additional Information

Sun Microsystems, Inc. (Sun) offers several methods for you to obtain additional information.

### Sun's External Web Site

Sun's external Web site provides marketing, product, event, corporate, and service information. The external Web site is accessible to anyone with a Web browser and an Internet connection.

The URL for the Sun external Web site is: <http://www.sun.com>

The URL for Sun StorageTek™ brand-specific information is:  
<http://www.sun.com/storagetek/index.jsp?intcmp=1902>

### Customer-Accessible Documents and Software Downloads

Customers can download Sun StorageTek documents by going to the Sun Microsystems Documentation website.

The URL for the CRC is <http://docs.sun.com/app/docs>

Software downloads are available at

<http://www.sun.com/download/>

### Partners Site

The Sun StorageTek Partners site is a Web site for partners with a Sun StorageTek Partner Agreement. This site provides information about products, services, customer support, upcoming events, training programs, and sales tools to support Sun StorageTek Partners. Access to this site, beyond the Partners Login page, is restricted. On the Partners Login page, Sun employees and current partners who do not have access can request a login ID and password and prospective partners can apply to become Sun StorageTek resellers.

The URL for partners with a Sun Partner Agreement is:  
<http://www.sun.com/partners/>



## Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

## Hardcopy Publications

Contact a Sun sales or marketing representative to order additional paper copies of this publication or to order other StorageTek brand product customer publications in paper format.

## Customer Support

Customer support is available 24 hours a day, seven days a week, to customers with Sun or StorageTek maintenance contracts and to Sun employees. You can find additional information about customer support on the Customer Resource Center (CRC) Web site at:

<http://www.sun.com/storagetek/support/index.jsp>

## Customer-initiated Maintenance

Customer-initiated maintenance begins with a telephone call from you to Sun Microsystems StorageTek Support. You receive immediate attention from qualified Sun personnel, who record problem information and respond with the appropriate level of support.

To contact Sun Microsystems StorageTek Support about a problem:

1. Use the telephone and call:

**☎ 800.872.4786 (1.800.USA.4SUN)** (inside the United States)

**☎ 800.722.4786** (Canada)

For international locations, go to

<http://www.sun.com/service/contacting/solution.html>

for the appropriate telephone number

2. Describe the problem to the call taker. The call taker will ask several questions and will either route your call to or dispatch a support representative.

If you have the following information when you place a service call, the process will be much easier:

|                                 |       |
|---------------------------------|-------|
| Account name                    | <hr/> |
| Site location number            | <hr/> |
| Contact name                    | <hr/> |
| Telephone number                | <hr/> |
| Equipment model number          | <hr/> |
| Device address                  | <hr/> |
| Device serial number (if known) | <hr/> |
| Urgency of problem              | <hr/> |
| Fault Symptom Code (FSC)        | <hr/> |
| Problem description             | <hr/> |
|                                 | <hr/> |
|                                 | <hr/> |
|                                 | <hr/> |

## Sun's Worldwide Offices

You may contact any of Sun's worldwide offices to discuss complete storage, service, and support solutions for your organization. You can find address and telephone number information on Sun's external Web site at:

<http://www.sun.com/worldwide/>

---

## Related Publications

The following publications provide additional information about specific topics relating to the use of the Key Management System (KMS):

- *Key Management System (KMS) 2.1 Installation and Service Manual*
- *Key Management System (KMS) 2.1 Systems Assurance Guide.*

---

# Conventions for Reader Usability

## Product Names

KMS refers to the 2.1 implementation of the Sun StorageTek™ Crypto Key Management System.

## Typographic

Some examples in this guide include *italic* type. Italic type is used to indicate a variable. You must substitute an actual value for these variables.

The use of mixed upper and lower case characters for commands, control statements, and parameters indicates that lower case letters may be omitted to form abbreviations. For example, you may simply enter POL when executing the POLicy command.

## Alert Messages

Alert messages call your attention to information that is especially important or that has a unique relationship to the main text or graphic.

---

**Warning** – Information necessary to keep you from damaging your hardware or software.

---

---

**Caution** – Information necessary to keep you from corrupting your data.

---

---

**Tip** – Information that can be used to shorten or simplify your task or they may simply be used as a reminder.

---

---

**Note** – Information that may be of special interest to you. Notes are also used to point out exceptions to rules or procedures.

---

# Introduction

---

---

## Overview

The Crypto Key Management System (KMS) creates, stores, and manages encryption keys. It consists of the following components:

- **Key Management Appliance (KMA)** – A security-hardened box that delivers policy-based Lifecycle Key Management, authentication, access control, and key provisioning services. As a trust authority for storage networks, the KMA ensures that all storage devices are registered and authenticated, and that all encryption key creation, provisioning and deletion is in accordance with prescribed policies.
- **KMS Manager GUI** – A Graphical User Interface that is executed on a workstation and communicates with the KMA over an IP network to configure and manage the KMS. The KMS Manager GUI must be installed on a customer-provided workstation.
- **KMS Cluster** – The full set of KMAs in the system. All of these KMAs are aware of each other and replicate information to each other.
- **Agent** – A device or software that performs encryption, using keys managed by the KMS Cluster. These are the Sun StorageTek encrypting tape drives. Agents communicate with KMAs via the Agent API. The Agent API is a set of software interfaces that are incorporated into the agent hardware or software.

---

# KMS Concepts

## KMS Clusters

KMS supports clustering of multiple KMAs, which provides load balancing and failover. All KMAs in a KMS Cluster act in an active/active manner. All KMAs can provide all capabilities to any agent. Actions performed on one KMA are quickly replicated to all other KMAs in the Cluster.

## Agents

Agents perform cryptographic operations, specifically, encrypting data as it is written and decrypting data as it is read. Agents contact the KMS Cluster in order to create and retrieve keys used to perform the cryptography.

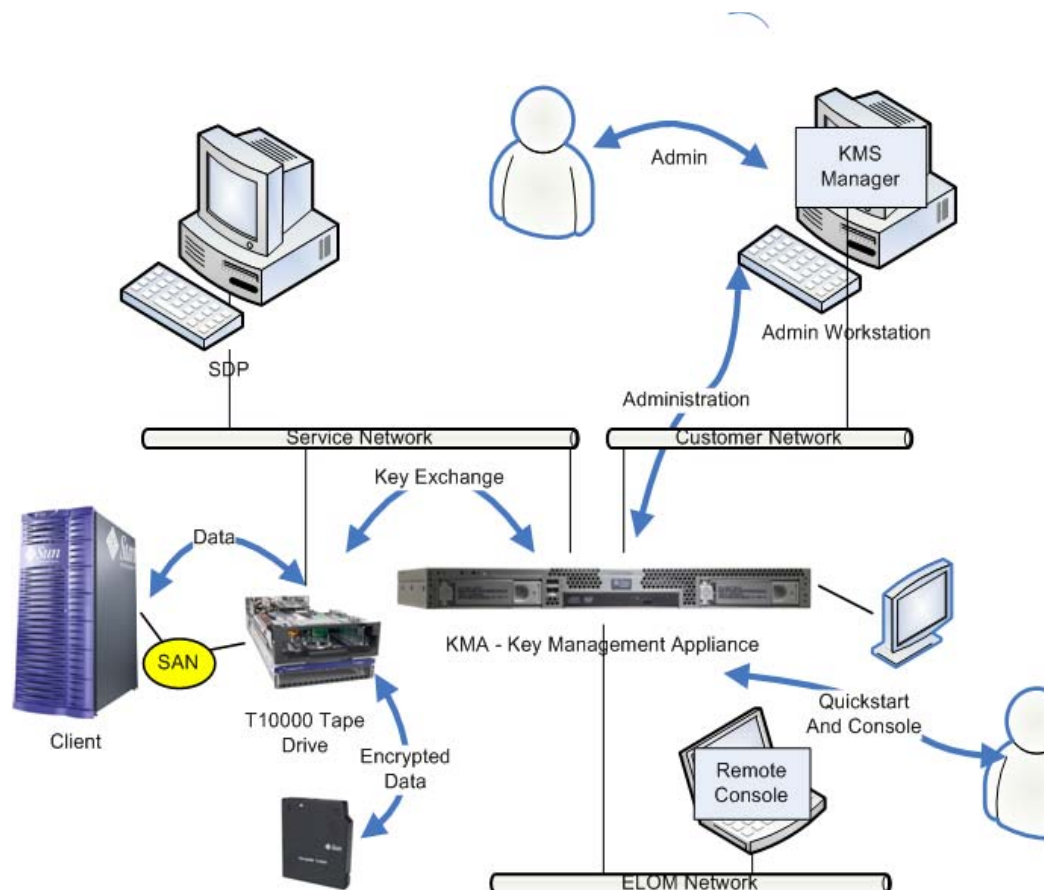
## Network Connections

The KMS uses TCP/IP networking for the connections between KMAs, Agents, and machines where the KMS Manager GUI is running. In order to provide flexible network connections, two interfaces are provided for network connections on the KMA:

- The management connection, intended for connection to the customer network
- The service connection, intended for connection to the tape drives.

With production KMA installation, library-specific accessory kits are available that include switches and cables for connecting to the drives and the KMA. This is shown in [FIGURE 1-1](#).

**FIGURE 1-1** Connections to the KMA



## Initial Setup - Direct Connection or Remote Console

KMA initial setup is performed through the console connection. This can be done by using a monitor and keyboard connected directly to the KMA or by the remote console function in the Embedded Lights Out Manager (ELOM). The ELOM provides a remote connection to the console allowing you to perform server functions.

The ELOM remote console function requires a third network connection, labeled the "ELOM Network" in [FIGURE 1-1](#). The ELOM's IP address must be configured as described later in this document in order to use the remote console function.

---

**Note** – Most commonly, the ELOM Network will actually be the same network as the customer network.

---

## Initial Setup - QuickStart Program

When a KMA in the factory default state is powered on, a wizard function called QuickStart will run on the console to perform the initial setup. Once complete, most other functions can be done from the KMS manager GUI. A limited function console interface remains active for a small set of functions.

## Key Lifecycle

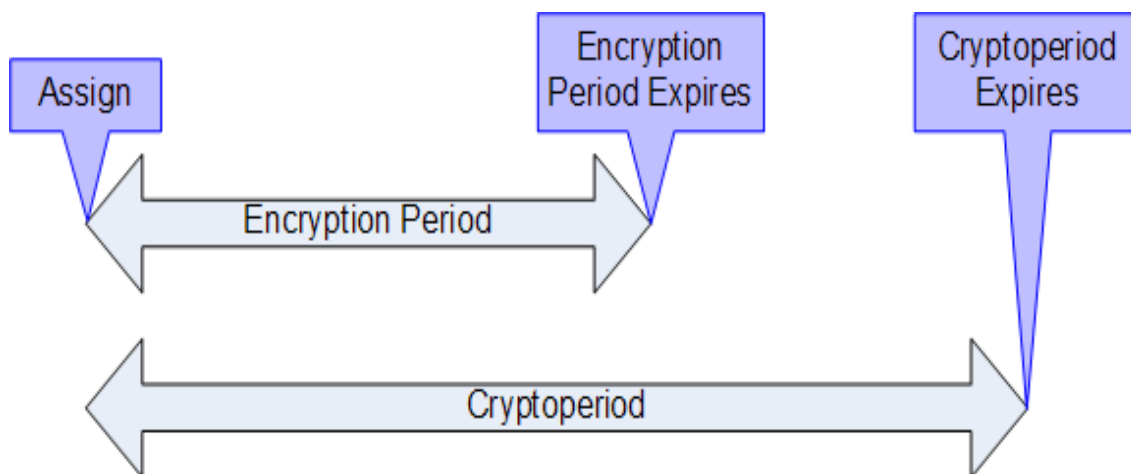
Keys undergo a lifecycle based on the key policy. The lifecycle imposed by the KMS is based on the NIST 800-57 guidelines. A few additional states are added to deal with nuances of the KMS.

The key lifecycle is based on two time periods (see [FIGURE 1-2](#)) defined in the key policies:

- Encryption period
- Cryptoperiod

The encryption period is the period after a key is assigned that can be used to encrypt data. The cryptoperiod is the period that can be used for decryption. The two periods start at the same time when the key is assigned.

**FIGURE 1-2** Key Lifecycle Periods

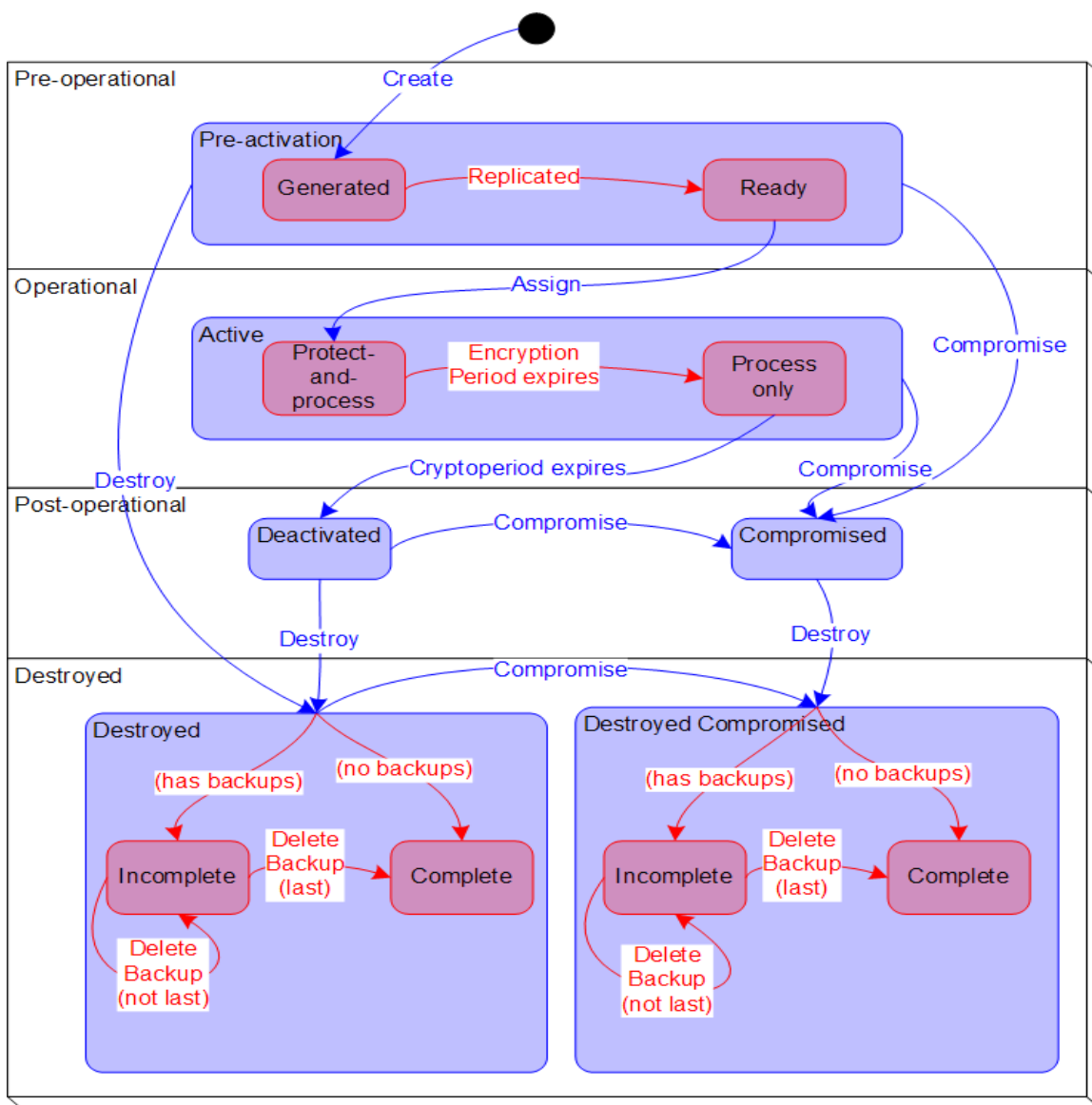




## State Transition

These encryption period and cryptoperiod, combined with other functions of the KMS, define a state transition for keys as shown in [FIGURE 1-3](#). In this diagram, states and transitions shown in blue are defined by NIST 800-57.

**FIGURE 1-3** State Transition Diagram



## KMS States and Transitions

In [FIGURE 1-3](#), states and transitions shown in red are added by the KMS. When examining keys in the KMS Manager, only the innermost state is listed. KMS states are listed below.

### Pre-activation

This state indicates that the key has generated but is not yet available for use. Within the pre-activation state, the key can take two further states, generated and ready.

#### *Generated*

A generated state indicates a key that has been created on one KMA in a KMS Cluster. It remains generated until it has been replicated to at least one other KMA in a multi-KMS Cluster. In a Cluster with only a single KMA, a key must be recorded in at least one backup to transition out of the generated state.

#### *Ready*

A ready state indicates that the key has been protected against loss by replication or a backup. A ready key is available for assignment. The “replicated” transition occurs when the key is replicated or (for a single KMS Cluster) backed up.

### Active

This state indicates that the key may be used to protect information (encrypt) or to process previously protected information (decrypt). NIST states that an active key may be designated to protect only, process only, or protect and process. Further, it specifically states that for symmetric data encryption keys, a key may be used for some time period to protect and process information and once this time period expires, the key may continue to be used for processing only.

Within the active state, the KMS adds two substates. These states are described in NIST, but are not specifically identified as states.

#### *Protect-and-process*

A key in this state can be used for both encryption and decryption. A key is placed into this state when it is assigned. The assignment is done when an encryption agent requests a new key to be created.

*Process only*

A key in this state can be used for decryption but not encryption. When an agent determines that none of the keys available to it for a specific data unit that is being read or written are in the protect-and-process state, it should create a new key.

Keys move from the protect-and-process state to the process only state when the encryption period for the key expires.

**Deactivated**

This state indicates that the key has passed its cryptoperiod but may still be needed to process (decrypt) information. NIST specifically states that keys in this state may be used to process data.

The NIST guidelines state that if post-operational keys, including deactivated and compromised keys, need to remain accessible, they should be archived. This is a key recovery process that allows keys to be recalled from an archive and made available for use.

The KMS provides archives in the form of KMA backups but cannot recall a single key from a backup. Therefore, the KMS retains post-operational phase keys in the KMS Cluster and delivers them upon request from an agent.

**Compromised**

Keys are in the compromised state when they are released to or discovered by an unauthorized entity. Compromised keys should not be used to protect information, but may be used to process information.

**Destroyed/Destroyed Compromised**

Destroyed and Destroyed Compromised keys (keys that are compromised before or after destruction) no longer exist. However, information about the key may be retained. Key material from destroyed keys is removed from the KMS Cluster. Destroyed keys will not be delivered to an agent.

---

**Note** – The only way to destroy a key is through the GUI or the management API.

---

The NIST guidelines do not provide any basis for destroying keys based on time.

Within the Destroyed and Destroyed Compromised states, the KMS defines two substates, incomplete and complete. These states are created because the KMS does not control the backups that it creates. A customer administrator must inform the KMS when a backup has been destroyed. Only after all backups have been destroyed can a key be considered truly destroyed.

### *Incomplete*

This substate indicates that at least one backup still exists that contains the destroyed key. In this substate, the key does not exist in any KMA in the KMS Cluster. Keys in this state cannot be delivered to agents.

### *Complete*

This substate indicates that all backups containing the key have been destroyed. The key does not exist in any KMA, nor in any backup. Strictly speaking, backups that contain the key may well still exist. Although the KMS identifies the backups as destroyed, it is the responsibility of the user to ensure these backups have actually been destroyed.

It is worth noting again that the “destroyed” transition occurs only as the result of an administrative command. Further, keys may still be delivered to an encryption agent when the key is in the post-operational phase (Deactivated and Compromised states.) This interpretation is consistent with NIST’s descriptions for the post-operational phase. The NIST guidelines specify that a post-operational key should be destroyed when it is “no longer needed.” We believe that only a user can determine when a key is “no longer needed,” so only an external entity can initiate the destroyed transition.

## Users and Role-based Access Control

The KMS provides the ability to define multiple users, each with a user ID and passphrase. Each user is given one or more pre-defined roles. These roles are:

- **Security Officer** – performs KMS setup and management
- **Operator** – performs agent setup and day-to-day operations
- **Compliance Officer** – defines key groups and controls agent access to key groups
- **Backup Operator** – performs backup operations
- **Auditor** – can view system audit trails

A Security Officer is defined during the QuickStart process. Additional users may be defined using the KMS Manager GUI after QuickStart is complete.

### Allowed Operations for Each Role

[TABLE 1-3 on page 14](#) lists the functions for each role. It displays only the allowed operations for the GUI and the console. Although you may see an operation, it may fail when you attempt it. This can occur if roles are removed from a user between the time of display and when the operation is attempted.

All roles except the Auditor's must create a functioning encryption system. A user can have one or multiple roles.

### Quorum Protection

The KMS also provides quorum protection for certain operations. You can define a quorum of up to 10 users and a threshold from one to the number of quorum users. This information is called the *Key Split Credentials* (see [“Entering Key Split Credentials” on page 34](#)).

The user IDs and passphrases are different from the user IDs and passphrases used to log into the system. When you attempt an operation that requires quorum approval, a screen is displayed that allows all quorum users to input their userid and passphrase. At a minimum, you must supply the specified threshold of userids and passphrases for the operation to be allowed.

## Data Units, Keys, Key Groups, and Key Policies

Data units are used to represent data that is encrypted by agents. For tape drives, a data unit is a tape cartridge, and data units are always present. This is not a fundamental requirement, and future agents may operate without defining data units.

Keys are the actual key values (key material) and their associated metadata.

Key policies define parameters that govern keys. This includes lifecycle parameters (such as encryption period and cryptoperiod) and export/import parameters (for example, import allowed, export allowed.)

Key groups associate keys and key policies. Key groups have a specific key policy and are assigned to agents. Each agent has a list of allowed key groups. Agents are allowed to retrieve only the keys that are assigned to one of the agent's allowed key groups. Agents also have a default key group. When an agent creates a key (more specifically, assigns it to a data unit), the key is placed into the agent's default key group. There is functionality in place to allow more sophisticated control of key groups by agents. However, existing agents cannot leverage this functionality.

In order for the system to function, at least one key policy and one key group must be defined. That key group must be assigned as the default key group for all agents.

## TCP/IP Connections and the KMA

If a firewall exists between the entities (KMS Manager, Agents, and other KMAs in the same Cluster) and the KMA, the firewall must allow the entity to establish TCP/IP connections with the KMA on the following ports:

- KMS Manager-to-KMA communication requires ports 3331, 3332, 3333, 3335.
- Agent-to-KMA communication requires ports 3331, 3332, 3334, 3335.
- KMA-to-KMA communication requires ports 3331, 3332, 3336.

[TABLE 1-1](#) lists ports KMAs explicitly used or ports at which KMAs provide services.

**TABLE 1-1** KMA Port Connections

| Port Number | Protocol | Direction  | Description                                  |
|-------------|----------|------------|--|
| 22          | TCP      | Listening  | SSH (only when Technical Support is enabled) |
| 123         | TCP/UDP  | Listening  | NTP  |
| 161         | UDP      | Connecting | SNMP   |
| 3331        | TCP      | Listening  | KMS CA Service                               |
| 3332        | TCP      | Listening  | KMS Certificate Service                      |
| 3333        | TCP      | Listening  | KMS Management Service                       |
| 3334        | TCP      | Listening  | KMS Agent Service                            |
| 3335        | TCP      | Listening  | KMS Discovery Service                        |
| 3336        | TCP      | Listening  | KMS Replication Service                      |

[TABLE 1-2](#) shows other services listening at ports that might not be used.

**TABLE 1-2** Other Services

| Port Number | Protocol | Direction  | Description                           |
|-------------|----------|------------|---------------------------------------|
| 53          | TCP/UDP  | Connecting | DNS                                   |
| 111         | TCP/UDP  | Listening  | RPC (KMAs respond to rpcinfo queries) |
| 4045        | TCP/UDP  | Listening  | NFS lock daemon                       |
| 7100        | TCP      | Listening  | Font server                           |

# KMS in the Network

FIGURE 1-4 shows a typical deployment of the KMS solution.

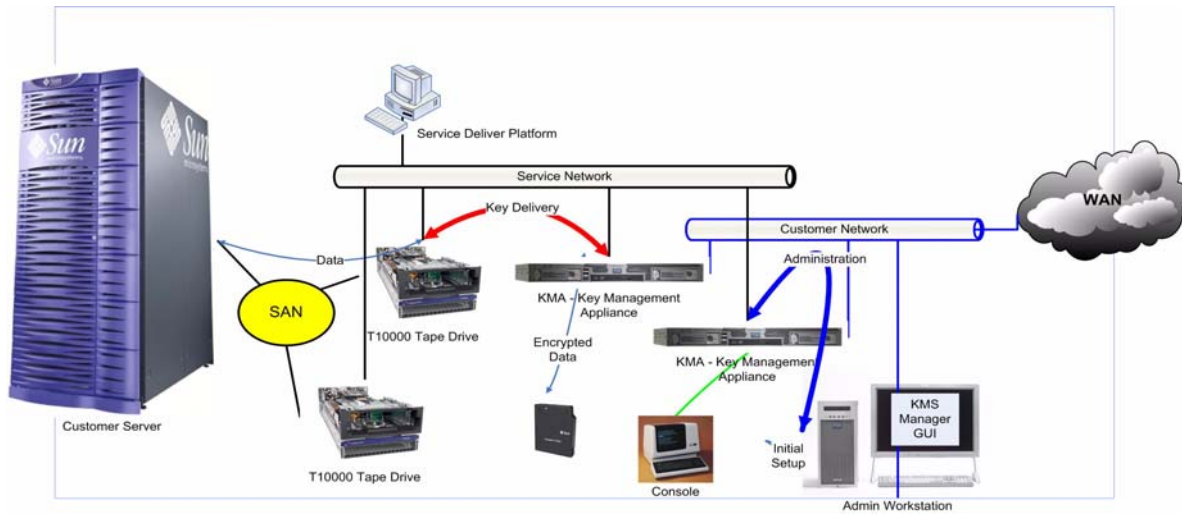


FIGURE 1-4 Typical Deployment of KMS Solution



---

# KMS Manager Software Requirements

To run the KMS Manager, you need a workstation that is running Microsoft® Windows XP, Solaris 10 x86 update 3, or Solaris 10 x86 update 4.

---

## Using Online Help

The KMS Manager includes comprehensive online help. To display help on any KMS Manager screen,

- Click the **Help** button that is located at the top of the panel for general help.

or

- Navigate to a panel by either pressing the **Tab** key or by clicking somewhere within the panel. Then, click **F1** to view context-sensitive help.

---

## Role-Based Access Control

KMS defines the following roles:

- **Security Officer** – manages security settings, users, sites, and transfer partners
- **Compliance Officer** – manages key policies and key groups and determines which agents and transfer partners can use key groups
- **Operator** – manages agents, data units, and keys
- **Backup Operator** – performs backups
- **Auditor** – views information about the KMS Cluster.

A single KMA user account may be assigned membership to one or more roles. The KMA verifies that the requesting user entity has permission to execute an operation based on the user's role(s). For more information on the roles, refer to "[Logging into the KMA](#)" on page 288.

## Role-Based Operations

TABLE 1-3 shows the system operations that each user role can perform. In the “Roles” columns,

- **Yes** – the role is allowed to perform the operation.
- **Quorum** – the role is allowed to perform the operation but must also provide a quorum.
- A blank means the role is not allowed to perform the operation.

**TABLE 1-3** System Operations/User Roles

| Entity                | Operation                     | Roles            |                    |          |                 |         |
|-----------------------|-------------------------------|------------------|--------------------|----------|-----------------|---------|
|                       |                               | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor |
| Console               |                               |                  |                    |          |                 |         |
|                       | Log In                        | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | Set KMA Locale                | Yes              |                    |          |                 |         |
|                       | Set KMA IP Address            | Yes              |                    |          |                 |         |
|                       | Enable Tech Support           | Yes              |                    |          |                 |         |
|                       | Disable Tech Support          | Yes              |                    | Yes      |                 |         |
|                       | Enable Primary Administrator  | Yes              |                    |          |                 |         |
|                       | Disable Primary Administrator | Yes              |                    | Yes      |                 |         |
|                       | Restart KMA                   |                  |                    | Yes      |                 |         |
|                       | Shutdown KMA                  |                  |                    | Yes      |                 |         |
|                       | Log KMS into Cluster          | Quorum           |                    |          |                 |         |
|                       | Set User's Passphrase         | Yes              |                    |          |                 |         |
|                       | Reset KMA                     | Yes              |                    |          |                 |         |
|                       | Zeroize KMA                   | Yes              |                    |          |                 |         |
|                       | Logout                        | Yes              | Yes                | Yes      | Yes             | Yes     |
| Connect               |                               |                  |                    |          |                 |         |
|                       | Log In                        | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | Create Profile                | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | Delete Profile                | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | Set Config Settings           | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | Disconnect                    | Yes              | Yes                | Yes      | Yes             | Yes     |
| Key Split Credentials |                               |                  |                    |          |                 |         |
|                       | List                          | Yes              |                    |          |                 |         |
|                       | Modify                        | Quorum           |                    |          |                 |         |
| Autonomous Unlock     |                               |                  |                    |          |                 |         |

**TABLE 1-3** System Operations/User Roles

| Entity              | Operation         | Roles            |                    |          |                 |         |
|---------------------|-------------------|------------------|--------------------|----------|-----------------|---------|
|                     |                   | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor |
|                     | List              | Yes              |                    |          |                 |         |
|                     | Modify            | Quorum           |                    |          |                 |         |
| Lock/Unlock KMA     |                   |                  |                    |          |                 |         |
|                     | List Status       | Yes              | Yes                | Yes      | Yes             | Yes     |
|                     | Lock              | Yes              |                    |          |                 |         |
|                     | Unlock            | Quorum           |                    |          |                 |         |
| Site                |                   |                  |                    |          |                 |         |
|                     | Create            | Yes              |                    |          |                 |         |
|                     | List              | Yes              |                    | Yes      |                 |         |
|                     | Modify            | Yes              |                    |          |                 |         |
|                     | Delete            | Yes              |                    |          |                 |         |
| Security Parameters |                   |                  |                    |          |                 |         |
|                     | List              | Yes              | Yes                | Yes      | Yes             | Yes     |
|                     | Modify            | Yes              |                    |          |                 |         |
| KMA                 |                   |                  |                    |          |                 |         |
|                     | Create            | Yes              |                    |          |                 |         |
|                     | List              | Yes              |                    | Yes      |                 |         |
|                     | Modify            | Yes              |                    |          |                 |         |
|                     | Delete            | Yes              |                    |          |                 |         |
| User                |                   |                  |                    |          |                 |         |
|                     | Create            | Yes              |                    |          |                 |         |
|                     | List              | Yes              |                    |          |                 |         |
|                     | Modify            | Yes              |                    |          |                 |         |
|                     | Modify Passphrase | Yes              |                    |          |                 |         |
|                     | Delete            | Yes              |                    |          |                 |         |
| Role                |                   |                  |                    |          |                 |         |
|                     | List              | Yes              |                    |          |                 |         |
| Key Policy          |                   |                  |                    |          |                 |         |
|                     | Create            |                  | Yes                |          |                 |         |
|                     | List              |                  | Yes                |          |                 |         |
|                     | Modify            |                  | Yes                |          |                 |         |
|                     | Delete            |                  | Yes                |          |                 |         |
| Key Group           |                   |                  |                    |          |                 |         |
|                     | Create            |                  | Yes                |          |                 |         |
|                     | List              |                  | Yes                | Yes      |                 |         |

**TABLE 1-3** System Operations/User Roles

| Entity                                 | Operation           | Roles            |                    |          |                 |         |
|--|---------------------|------------------|--------------------|----------|-----------------|---------|
|  |                     | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor |
|  | List Data Units     |                  | Yes                | Yes      |                 |         |
|  | List Agents         |                  | Yes                | Yes      |                 |         |
|  | Modify              |                  | Yes                |          |                 |         |
|  | Delete              |                  | Yes                |          |                 |         |
| Agent                                  |                     |                  |                    |          |                 |         |
|  | Create              |                  |                    | Yes      |                 |         |
|  | List                |                  | Yes                | Yes      |                 |         |
|  | Modify              |                  |                    | Yes      |                 |         |
|  | Modify Passphrase   |                  |                    | Yes      |                 |         |
|  | Delete              |                  |                    | Yes      |                 |         |
| Agent/Key Group Assignment             |                     |                  |                    |          |                 |         |
|  | List                |                  | Yes                | Yes      |                 |         |
|  | Modify              |                  | Yes                |          |                 |         |
| Data Unit                              |                     |                  |                    |          |                 |         |
|  | Create              |                  |                    |          |                 |         |
|  | List                |                  | Yes                | Yes      |                 |         |
|  | Modify              |                  |                    | Yes      |                 |         |
|  | Modify Key Group    |                  | Yes                |          |                 |         |
|  | Delete              |                  |                    |          |                 |         |
| Keys                                   |                     |                  |                    |          |                 |         |
|  | List Data Unit Keys |                  | Yes                | Yes      |                 |         |
|  | Destroy             |                  |                    | Yes      |                 |         |
|  | Compromise          |                  | Yes                |          |                 |         |
| Transfer Partners                      |                     |                  |                    |          |                 |         |
|  | Configure           | Quorum           |                    |          |                 |         |
|  | List                | Yes              | Yes                | Yes      |                 |         |
|  | Modify              | Quorum           |                    |          |                 |         |
|  | Delete              | Yes              |                    |          |                 |         |
| Key Transfer Keys                      |                     |                  |                    |          |                 |         |
|  | List                | Yes              |                    |          |                 |         |
|  | Update              | Yes              |                    |          |                 |         |
| Transfer Partner Key Group Assignments |                     |                  |                    |          |                 |         |
|  | List                |                  | Yes                | Yes      |                 |         |
|  | Modify              |                  | Yes                |          |                 |         |
| Backup                                 |                     |                  |                    |          |                 |         |

**TABLE 1-3** System Operations/User Roles

| Entity                | Operation                        | Roles            |                    |          |                 |         |
|-----------------------|----------------------------------|------------------|--------------------|----------|-----------------|---------|
|                       |                                  | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor |
|                       | Create                           |                  |                    |          | Yes             |         |
|                       | List                             | Yes              | Yes                | Yes      | Yes             |         |
|                       | List Backups with Destroyed Keys |                  | Yes                | Yes      |                 |         |
|                       | Restore                          | Quorum           |                    |          |                 |         |
|                       | Confirm Destruction              |                  |                    |          | Yes             |         |
| Core Security Backup  |                                  |                  |                    |          |                 |         |
|                       | Create                           | Yes              |                    |          |                 |         |
| SNMP Manager          |                                  |                  |                    |          |                 |         |
|                       | Create                           | Yes              |                    |          |                 |         |
|                       | List                             | Yes              |                    | Yes      |                 |         |
|                       | Modify                           | Yes              |                    |          |                 |         |
|                       | Delete                           | Yes              |                    |          |                 |         |
| Audit Event           |                                  |                  |                    |          |                 |         |
|                       | View                             | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | View Agent History               |                  | Yes                | Yes      |                 |         |
|                       | View Data Unit History           |                  | Yes                | Yes      |                 |         |
|                       | View Data Unit Key History       |                  | Yes                | Yes      |                 |         |
| System Dump           |                                  |                  |                    |          |                 |         |
|                       | Create                           | Yes              |                    | Yes      |                 |         |
| System Time           |                                  |                  |                    |          |                 |         |
|                       | List                             | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | Modify                           | Yes              |                    |          |                 |         |
| NTP Server            |                                  |                  |                    |          |                 |         |
|                       | List                             | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | Modify                           | Yes              |                    |          |                 |         |
| Software Version      |                                  |                  |                    |          |                 |         |
|                       | List                             | Yes              | Yes                | Yes      | Yes             | Yes     |
|                       | Upgrade                          |                  |                    | Yes      |                 |         |
| Network Configuration |                                  |                  |                    |          |                 |         |
|                       | Display                          | Yes              | Yes                | Yes      | Yes             | Yes     |

# Setting Up and Managing the Key Management Appliance

For procedures on getting your KMS solution installed and configured, refer to the *KMS 2.1 Installation and Service Manual*.

## Getting Started

---

This chapter describes the following topics:

- Starting the Embedded Lights Out Manager (ELOM) – ELOM provides a remote connection to the console (page [20](#))
- Running the QuickStart program – QuickStart is a utility that a customer (Security Officer or qualified representative) can use to configure a new KMA (page [25](#)).

---

**Note** – A service representative can also run QuickStart, however, since this program establishes critical security parameters, customers may prefer to do it themselves, following their corporate security policies.

---

# Starting the Embedded Light Out Manager

The Embedded Lights Out Manager (ELOM) system contains a separate processor from the main server. As soon as power is applied (plugged-in), and after a one or two minute boot period, ELOM provides a remote connection to the console allowing you to perform server functions, such as the *QuickStart* program.

**Note** – Refer to the *KMA Installation and Service Manual* for some basic ELOM commands to configure the server. For more information, see the *Embedded Lights Out Manager Administration Guide*.

## Connecting to the KMA

Connect to the KMA through the Embedded Lights Out Manager using either:

- The network connection, LAN 1 NET MGT ELOM interface (suggested), or
- The keyboard and monitor attached to the KMAs.



**Popup blockers** will prevent Windows from launching in the following procedures. Disable the popup blockers before beginning.

If the window appears, but a console window does not, the Web browser or Java version is incompatible with the ELOM. Upgrade to the latest versions of the browser and Java. See [TABLE 2-1](#) for a list of compatible versions.

**TABLE 2-1** Compatible Web Browser and Java Versions

| Client OS   | Java Runtime Environment<br>Including Java Web Start | Web Browsers   |
|---|--|--|
| ■ Microsoft Windows XP Pro  | JRE 1.5<br>(Java 5.0 Update 7 or later)              | ■ Internet Explorer 6.0 and<br>later Mozilla 1.7.5 or later<br>■ Mozilla Firefox 1.0 |
| ■ Red Hat Linux 3.0 and 4.0   |  | ■ Mozilla 1.7.5 or later<br>■ Mozilla Firefox 1.0                                    |
| ■ Solaris 9<br>■ Solaris 10<br>■ SUSE Linux 9.2   |  | ■ Mozilla 1.7.5  |
| You can download the Java 1.5 runtime environment at: <a href="http://java.com">http://java.com</a><br>The current version of the ELOM guide is located at: <a href="http://dlc.sun.com/">http://dlc.sun.com/</a><br>You can download Sun Fire X2100 M2 Server documentation at:<br><a href="http://docs.sun.com/app/docs/coll/x2100m2">http://docs.sun.com/app/docs/coll/x2100m2</a> |  |  |



## Using a Network Connection

1. Using another workstation on the network, launch a Web browser.
2. Connect to the KMA ELOM using the IP Address or hostname of LAN 1 (NET MGT), which is the address just configured.

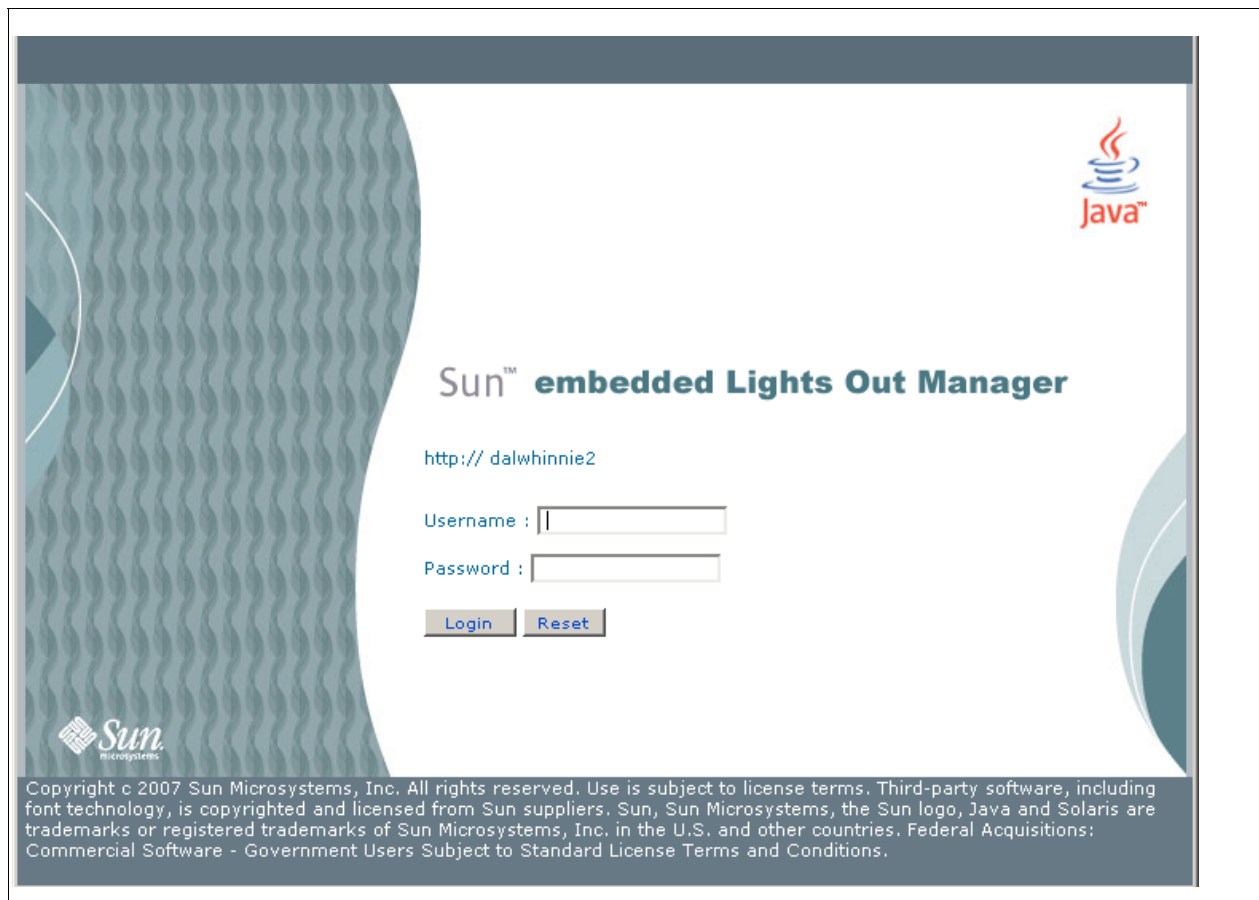
---

**Note** – Because the certificate in the ELOM will not match the assigned name or IP, you will receive one or more warnings from your web browser.

---

3. Click OK or Yes to bypass these warnings.  
Once past the warnings, you will receive the ELOM login prompt.

**FIGURE 2-1** Embedded Lights Out Manager Login Screen



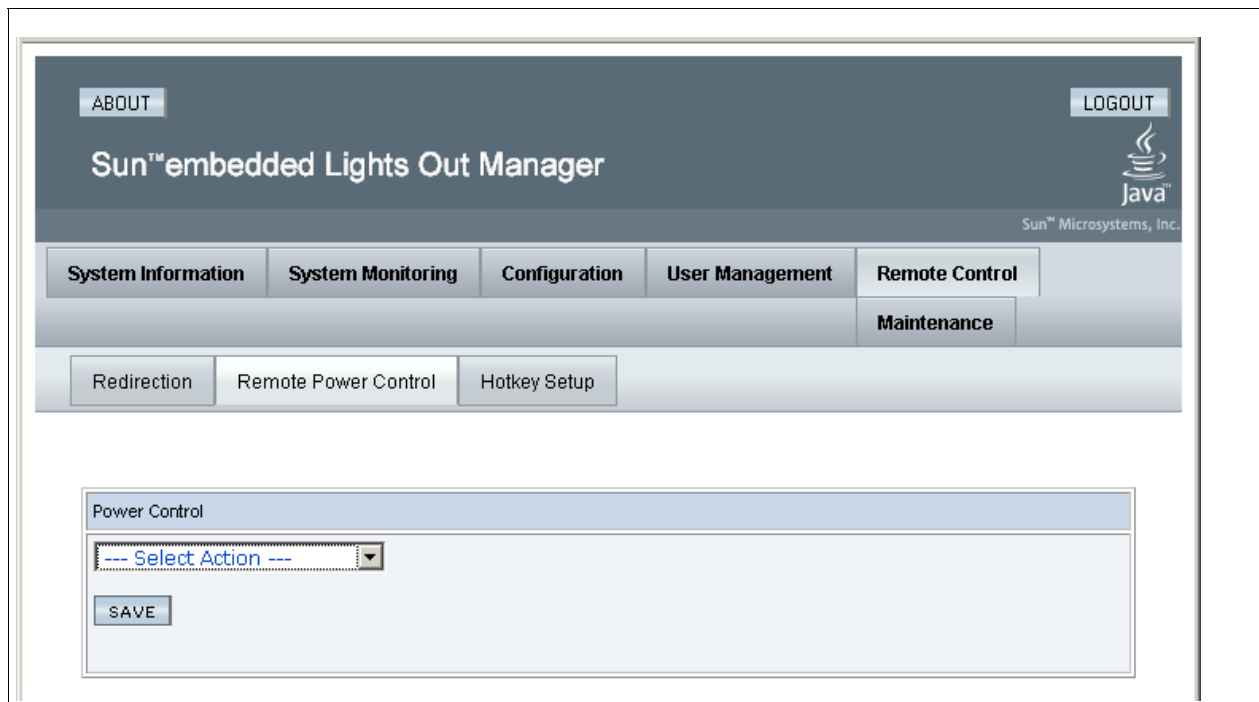
4. Log in using:  
    Userid = root  
    Password = changeme

The next screen is the Manager Screen. If the server has just been connected to power, and it has not been powered on, it will not have completed a system boot.

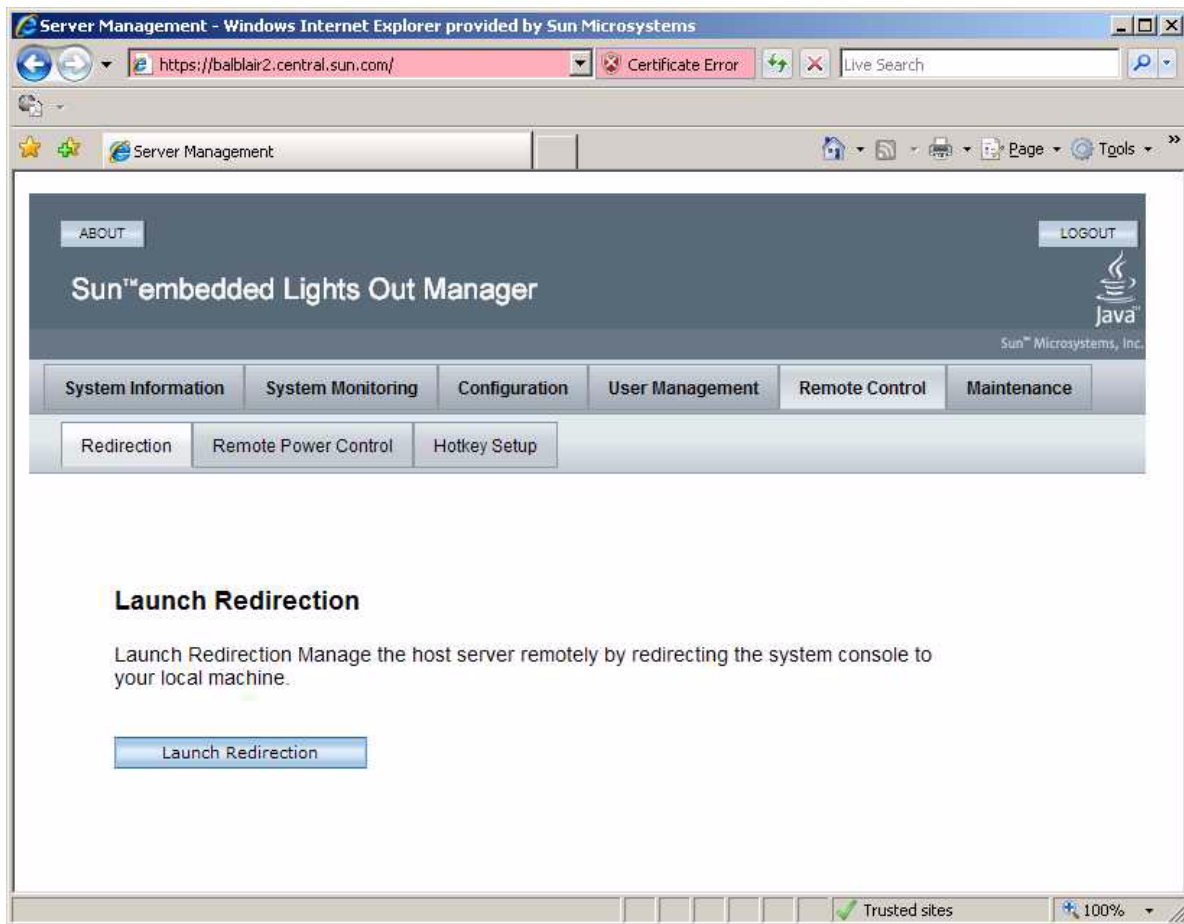
KMAs are configured to boot up automatically when initially powered on and should boot up to the QuickStart prompt within a few minutes of being powered on.

5. Check the power status by clicking on the **System Monitoring** tab.
6. If the Power Status shows “power off,” click the **Remote Control** tab to the far right of the upper row of tabs.
7. Click the **Remote Power Control** tab in the second row of tabs.
8. In the Select Action drop-down, choose **Power On** and click the **Save** button.  
The KMA will begin powering up. This will take a few minutes; however, you can continue with the KMA configuration.

**FIGURE 2-2** Power Control

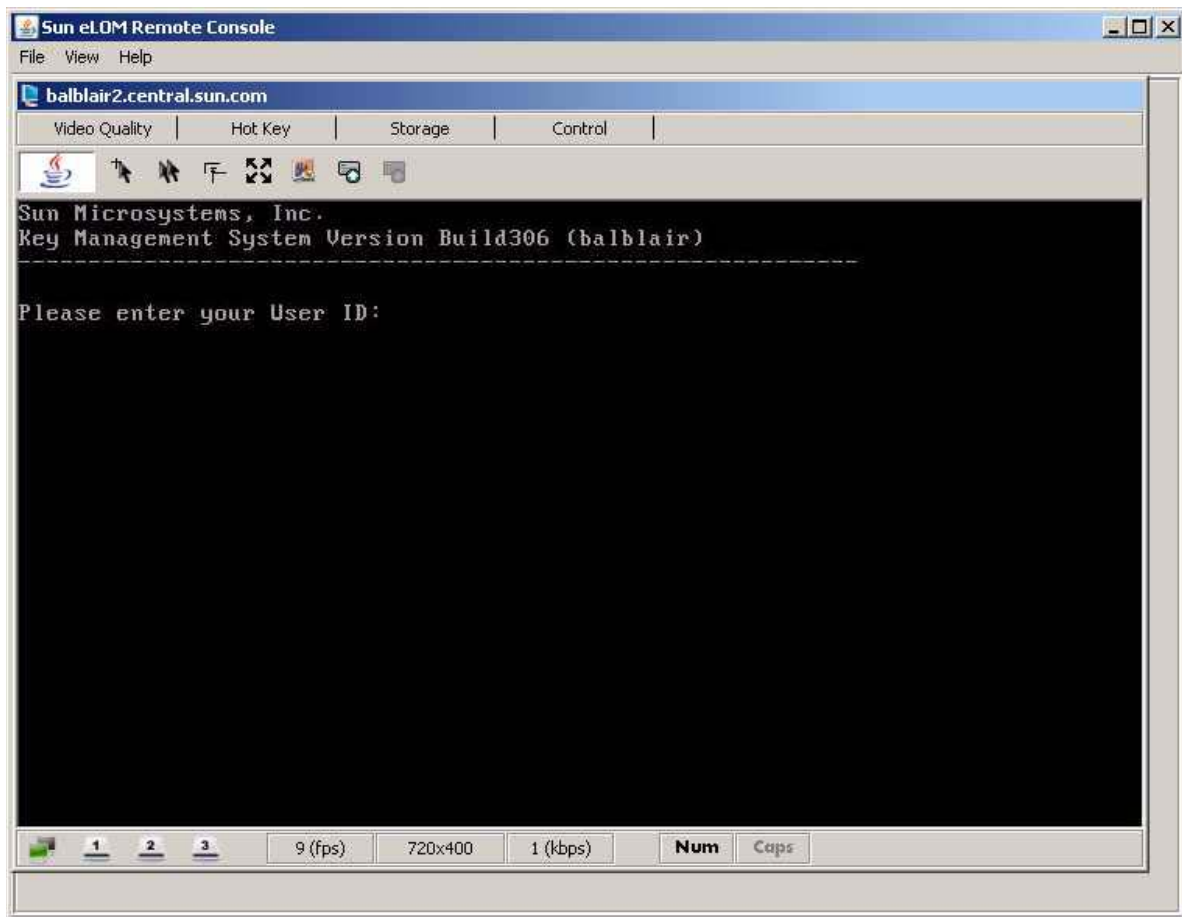


9. Click the **Remote Control** tab in the first row of tabs.
10. Click the **Redirection** tab in the second row of tabs.
11. Click the **Launch Redirection** button.  
A java applet will be downloaded before starting the remote console window.



This launches the remote console screen in a new window.

12. Save the javaRKVM.jnlp file when requested, then open it to start the remote console. Click past any warnings that may be displayed.



---

## Running the QuickStart Program

When a KMA in the factory default state is powered on, a special mode of the KMA Configuration Menu called QuickStart is automatically executed. QuickStart collects the minimal configuration information required for initializing the KMA. Once the QuickStart program has been successfully completed, it cannot be re-executed. The only way to access the QuickStart program again is to reset the KMA to its factory default state (refer to [“Resetting the KMA to the Factory Default” on page 310.](#))

---

**Note** – In the following screen examples, entries in **bold** represent areas where you respond.

---

## Starting QuickStart

To run the QuickStart Program:

Power on the KMA. When you power up the KMA for the first time, QuickStart is executed, and the Welcome to QuickStart! screen is displayed.

```

Sun Microsystems, Inc.
Key Management System Version xxx (Buildxxx)
-----
Welcome to QuickStart!

The QuickStart program will guide you through
the necessary steps for configuring the KMA.

You may enter Ctrl-c at any time to abort; however,
it is necessary to successfully complete all steps in this
initialization program to enable the KMA.

Press Enter to continue:

Set Keyboard Layout
-----

Press Ctrl-c to abort.

You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian           ( 2) Belarusian       ( 3) Belgian
( 4) Bulgarian          ( 5) Croatian         ( 6) Danish
( 7) Dutch              ( 8) Finnish          ( 9) French
(10) German             (11) Icelandic        (12) Italian
(13) Japanese-type6     (14) Japanese         (15) Korean
(16) Malta_UK           (17) Malta_US          (18) Norwegian
(19) Portuguese         (20) Russian           (21) Serbia-And-Montenegro
(22) Slovenian          (23) Slovakian         (24) Spanish
(25) Swedish            (26) Swiss-French      (27) Swiss-German
(28) Taiwanese          (29) TurkishQ          (30) TurkishF
(31) UK-English         (32) US-English

The current layout is US-English.

Please enter the number for the keyboard layout : 32

The keyboard layout has been applied successfully.

Press Enter to continue:

```

---

**Note** – If the user presses Ctrl-c, the QuickStart program resets and the Welcome to QuickStart! screen is redisplayed.

---

## Specifying the Network Configuration

The following procedures allow you to establish the network configuration.

### *Setting the KMA Management IP Addresses*

To set the KMA Management IP addresses:

1. Press <Enter> to continue. The following information is displayed.

```
Set KMA Management IP Addresses
-----

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other KMAs or Users in your system.

Do you want to configure the Management Network interface to have
an IPv6 address? [y/n]:

Do you want to use DHCP to configure the Management Network
interface? [y/n]:

Please enter the Management Network IP Address [10.80.180.39]:

Please enter the Management Network Subnet Mask [255.255.254.0]:
```

2. At the Please enter your choice: prompt on the main menu, type **3** and press <Enter>.
3. Type either **n** or **y** at the Do you want to configure the Management Network interface to have an IPv6 address prompt.
4. Type either **n** or **y** at the Do you want to use DHCP to configure the Management Network interface prompt. If you type **n**, go to [Step 5](#). If you type **y**, you go to the procedure [“Setting the KMA Service IP Addresses” on page 28](#).
5. At the prompt, type the Management Network IP address and press <Enter>.
6. At the Please enter the Management Network Subnet Mask: prompt, type the subnet mask address, (for example **255.255.254.0**) and press <Enter>.

### *Setting the KMA Service IP Addresses*

To set the KMA Service IP addresses:

1. Press <Enter> to continue. The following information is displayed.

```
Set KMA Service IP Addresses
-----

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other Agents in your system.

Do you want to configure the Service Network interface to have an
IPv6 address?
[y/n]: y

Do you want to use DHCP to configure the Service Network interface?
[y/n]: n

Please enter the Service Network IP Address [192.168.1.39]:

Please enter the Service Network Subnet Mask [255.255.255.0]:
```

2. At the Please enter your choice: prompt on the main menu, type **4** and press <Enter>.
3. Type either **n** or **y** at the Do you want to configure the Service Network interface to have an IPv6 address prompt.
4. Type either **n** or **y** at the Do you want to use DHCP to configure the Service Network interface prompt. If you type **n**, go to [Step 5](#). If you type **y**, you go to the procedure [“Viewing/Adding/Deleting Gateways”](#) on page 29.
5. At the prompt, type the Service Network IP address and press <Enter>.
6. At the Please enter the Service Network Subnet Mask: prompt, type the subnet mask address, (for example **255.255.255.0**) and press <Enter>.



### Viewing/Adding/Deleting Gateways

This menu option shows the current gateway settings (five to a page) on the Management (M) and Service (S) interfaces.

1. Press <Enter> to continue. The following information is displayed, indicating that you can add a gateway, remove a gateway, or accept the current gateway configuration.

```

Modify Gateway Settings
-----

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

  # Destination                Gateway                Netmask                IF
  -----
  1 default                    10.80.181.254          0.0.0.0                M
  2 default                    10.80.181.21           0.0.0.0                M
  3 default                    192.168.1.119          0.0.0.0                S
  4 10.0.0.0                   10.80.180.25           255.255.254.0          M
*  5 10.80.180.0               10.80.180.39           255.255.254.0          M

Press Enter to continue:

Modify Gateway Settings
-----

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

  # Destination                Gateway                Netmask                IF
  -----
*  6 192.168.1.0               192.168.1.39           255.255.255.0          S
  7 192.168.25.0               10.80.180.25           255.255.255.0          M
  8 192.168.26.0               10.80.180.25           255.255.255.0          M
*  9 127.0.0.1                 127.0.0.1              255.255.255.255
* 10 fe80::                     fe80::216:36ff:feca:15b6 10                      M

(1) Continue
(2) Back
1

```

# Modify Gateway Settings

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are indicated with an asterisk (\*). Management routes are indicated with an 'M', and service routes with an 'S'.

| #    | Destination | Gateway                  | Netmask | IF |
|------|-------------|--------------------------|---------|----|
| * 11 | fe80::      | fe80::216:36ff:feca:15b9 | 10      | S  |

You can add a route, delete a route, or exit the gateway configuration. Please choose one of the following:

- (1) Add a gateway
  - (2) Remove a configured gateway (only if modifiable)
  - (3) Exit gateway configuration
  - (4) Display again
- 3

2. At the Please enter your choice: prompt on the main menu, type **5** and press <Enter>.
3. At the (1) Continue (2) Back prompt, type **1** to display the next gateway setting or **2** to return to the previous gateway setting.
4. At the Please choose one of the following: prompt, type **1, 2, 3, or 4** and press <Enter>.

---

**Note** – If at any time the user presses Ctrl+c, no changes are saved and the user is returned to the main menu.

---

### *Specifying the DNS Settings*

This menu option shows the DNS settings, and prompts the user for a new DNS domain (if you want to configure one) and the DNS server IP addresses.

1. Press <Enter> to continue. The following information is displayed.

```
Set DNS Configuration
-----

Press Ctrl-c to abort.

DNS configuration is optional, but necessary if this KMA
will be configured using hostnames instead of IP addresses.

Current DNS configuration:

Domain:
Nameservers:

Please enter the DNS Domain (blank to unconfigure DNS):
central.sun.com

Up to 3 DNS Name Servers can be entered. Enter each name
server separately, and enter a blank name to finish.

Please enter DNS Server IP Address #1: 10.80.0.5

Please enter DNS Server IP Address #2:
```

2. At the Please enter your choice: prompt on the main menu, type 6 and press <Enter>.
3. Enter the DNS domain name at the Please enter the DNS Domain (blank to unconfigure DNS): prompt.
4. Enter the DNS server IP address at the Please enter DNS Server IP address prompt. You can enter up to three IP addresses.
5. Press <Enter>, without specifying an IP address, to finish.

## Initializing the KMA

1. Press <Enter> to continue. The following information is displayed.

The KMA Name is a unique identifier for your KMA. This name should not be the same as the KMA Name for any other KMA in your cluster. It also should not be the same as any User Names or Agent IDs in your system.

Please enter the KMA Name: **KMA-1**

Press Enter to continue:

Set Root Passphrase (Technical Support)

---

The 'root' account can only be used by Support personnel to administer support under extreme circumstances. You must set the 'root' account Passphrase to a secure value.

This Passphrase can be reset at a later date by a Security Officer User.

Passphrases must be at least 8 characters and at most 64 characters in length.

Passphrases must not contain the User's User Name.  
Passphrases must contain characters from 3 of 4 character classes (uppercase, lowercase, numeric, other).

Please enter a new Passphrase for the operating system  
'root' account: **\*\*\*\*\***

Please re-enter the 'root' Passphrase: **\*\*\*\*\***

Press Enter to continue:

Press Ctrl-c to abort.

2. At the prompt, type a unique identifier for the KMA.

---

**Note** – A KMA Name cannot be altered once it is set using the QuickStart program. It can only be changed by resetting the KMA to the factory default and running QuickStart again.

---

3. At the prompt, type a value for the root passphrase, ensuring that it satisfies the rules above.
4. At the Please re-enter the 'root' Passphrase: prompt, type the same passphrase you entered in [Step 3](#) and press <Enter>.

## Configuring the Cluster

1. At the prompt, press <Enter>. The following information is displayed, indicating that you can use this KMA to create a new Cluster, join an existing Cluster, or restore a Cluster from a backup of this KMA.

```
You can now use this KMA to create a new Cluster, or you can have  
this KMA join an existing Cluster. You can also restore a backup  
to this KMA or change the KMA Version.
```

```
Please choose one of the following:
```

- (1) **Create New Cluster**
- (2) Join Existing Cluster
- (3) Restore Cluster from Backup

```
Please enter your choice: 1
```

```
Create New Cluster
```

2. At the prompt, type 1, 2, or 3 and press <Enter>.

If you type 1, go to [“Entering Key Split Credentials”](#) on page 34.

If you type 2, go to [“Joining an Existing Cluster”](#) on page 40.

If you type 3, go to [“Restoring a Cluster From a Backup”](#) on page 43.

## Entering Key Split Credentials

Key Split Credentials user IDs and passphrases should be entered by the individual who owns that user ID and passphrase. Using one person to collect and enter this information defeats the purpose of having the Key Split Credentials.

If it is impractical for all members of the Key Split Credentials to enter this information at this time, enter a simple set of credentials now, and then enter the full credentials later in the KMS Manager.

However, doing this creates a security risk. If a Core Security backup is created with simple Key Split Credentials, it can then be used to restore a backup.

1. At the Please enter your choice: prompt, type 1. The following information is displayed.

The Key Split credentials are used to wrap splits of the Core Security Key Material which protects Data Unit Keys.

When Autonomous Unlocking is not enabled, a quorum of Key Splits must be entered in order to unlock the KMA and allow access to Data Unit Keys.

A Key Split credential, consisting of a unique User Name and Passphrase, is required for each Key Split.

The Key Split Size is the total number of splits that will be generated.

This number must be greater than 0 and can be at most 10.

Please enter the Key Split Size: **1**

The Key Split Threshold is the number of Key Splits required to obtain a **quorum**.

Please enter the Key Split Threshold: **2**

Please enter the Key Split User Name #1: **user1**

Passphrases must be at least 8 characters and at most 64 characters in length.

Passphrases must not contain the User's User Name.

Passphrases must contain characters from 3 of 4 character classes (uppercase, lowercase, numeric, other).

Please enter Key Split Passphrase #1: **\*\*\*\*\***

Please re-enter Key Split Passphrase #1: **\*\*\*\*\***

Press Enter to continue:

Press Ctrl-c to abort.

**Notes:**

- The Key Split Size and Key Split Threshold can be changed at a later time using the KMS Manager.
  - User IDs and passphrases should be entered only by an authorized user to keep them secure. These items also can be changed after running the QuickStart program.
2. At the Please enter the Key Split Size: prompt, type the number of key splits that will be generated and press <Enter>.
  3. At the Please enter the Key Split Threshold: prompt, type the number of required keys splits to obtain a quorum and press <Enter>.
  4. At the Please enter the Key Split User Name #1: prompt, type the username for the first Key Split user and press <Enter>.
  5. At the Please enter Key Split Passphrase #1: prompt, type the passphrase for the first Key Split user and press <Enter>.
  6. At the Please re-enter Key Split Passphrase #1: prompt, type the same passphrase that you previously entered and press <Enter>.
  7. Repeat [Step 4](#) through [Step 6](#) until all user names and passphrases have been entered for the selected Key Split size.

---

**Note** – The Key Split user names and passphrases are independent of other user accounts that are established for KMA administration.

---

## Entering Initial Security Officer User Credentials

1. At the `Press Enter to continue:` prompt, press `<Enter>`. The following information is displayed.

```
The Initial Security Officer User is the first User that can
connect to the KMA via the KMS Manager. This User can subsequently
create additional Users and administer the system.
```

```
Please enter a Security Officer User Name: SecOfficer
```

```
A Passphrase is used to authenticate to the KMA when a connection
is made via the KMS Manager.
```

```
Passphrases must be at least 8 characters and at most 64 characters
in length.
```

```
Passphrases must not contain the User's User Name.
```

```
Passphrases must contain characters from 3 of 4 character classes
(uppercase, lowercase, numeric, other).
```

```
Please enter the Security Officer Passphrase: *****
```

```
Please re-enter the Security Officer Passphrase: *****
```

```
Press Enter to continue:
```

```
Press Ctrl-c to abort.
```

---

**Note** – This initial Security Officer user account will be used to logon to the KMA using the KMS Manager.

---

2. At the prompt, type the Security Officer's user name and press `<Enter>`. The following information is displayed.
3. At the prompt, type the Security Officer's passphrase and press `<Enter>`.
4. At the `Please re-enter the Security Officer Passphrase:` prompt, re-type the same passphrase and press `<Enter>`.

---

**Important** – All KMAs have their own passphrases that are independent of passphrases assigned to users and Agents. The first KMA in a Cluster is assigned a random passphrase. If this KMA's certificate expires, and you want to retrieve its entity certificate from another KMA in the Cluster, you would have to use the KMS Manager to set the passphrase to a known value. For procedures, refer to [“Setting a KMA Passphrase” on page 107](#).

---



## Specifying the Autonomous Unlocking Preference

---

**Caution** – While it is more convenient and increases the availability of the KMS Cluster, enabling autonomous unlocking creates security risks. When autonomous unlocking is enabled, a powered-off KMA must retain sufficient information to boot up fully and begin decrypting stored keys.

This means a stolen KMA can be powered up, and an attacker can begin extracting keys for the KMA. While it is not easy to extract keys, a knowledgeable attacker will be able to dump all keys off the KMA. No cryptographic attacks will be needed.

If autonomous unlocking is disabled, cryptographic attacks will be required to extract keys from a stolen KMA.

You should carefully consider potential attacks and security concerns before choosing to enable autonomous unlocking.

---

1. At the Press Enter to continue: prompt, press <Enter>. The following information is displayed.

```
When Autonomous Unlocking is DISABLED, it is necessary to
UNLOCK the KMA using a quorum of Key Split Credentials
EACH TIME the KMA starts before normal operation of the
system can continue. Agents may NOT register Data Units
with or retrieve Data Unit Keys from a locked KMA.

When Autonomous Unlocking is ENABLED, the KMA will
automatically enter the UNLOCKED state each time the
KMA starts, allowing it to immediately service Agent requests.

Do you wish to enable Autonomous Unlocking? [y/n]: y
```

---

**Note** – The Autonomous Unlocking feature allows the KMA to enter a fully operational state after a hard or soft reset without requiring the entry of a quorum of passphrases using the KMS Manager. You can change this option from the KMS Manager at a later time.

---

2. At the prompt, type **y** or **n** and press <Enter>.

## Setting the Key Pool Size

1. At the `Press Enter to continue:` prompt, press `<Enter>`. The following information is displayed.

```
Enter Key Pool Size
-----

Press Ctrl-c to abort.

Each KMA pre-generates and maintains a pool of keys. These
pre-operational keys must be backed up or replicated before
a KMA will provide them to an Agent for use in protecting
data. This helps to ensure that a key will never be
permanently lost, even in disaster scenarios.

A smaller key pool size prevents unnecessary initial
database (and backup) size, but requires frequent backups
or a reliable network to ensure that activation-ready keys
are always available. Conversely, a large key pool size is
more tolerant of infrequent backups or unreliable network
connections between KMAs, but the large number of pre-
generated keys causes the database (and backups) to be
quite large.

Please select the key pool size (1000 - 200000):
```

2. At the prompt, enter the key pool size. The value entered determines the initial size that the new KMA generates and maintains.

## Synchronizing KMA Time

KMAs in a Cluster **must** keep their clocks synchronized. Internally, all KMAs use UTC time (coordinated universal time).

You can also use the KMS Manager to adjust date and time settings to local time.

```
KMAs in a Cluster must keep their clocks synchronized. Specify an
NTP server if one is available in your network. Otherwise, specify
the date and time to which the local clock should be set.
```

```
Please enter the NTP Server Hostname or IP Address (optional):
```

```
ntp.example.com
```

```
Press Enter to continue:
```

```
Initializing new cluster...
```

```
New KMS cluster has been created.
```

```
Press Enter to continue:
```

```
Key Management System Version Build xyz
```

```
_____
KMA initialization complete!
```

```
You may now connect to the KMA via the KMS Manager in order to
continue with KMS configuration.
```

```
Press Enter to exit:
```

```
Key Management System Version Build xyz (KMA-1)
```

```
_____
Please enter your User Name:
```

1. If an NTP server is available in your network environment, at the Please enter the NTP Server Hostname or IP Address (optional): prompt, enter the NTP server hostname or IP address.
2. If an NTP server is not available, press <Enter>. Then, at the Please enter the date and time for this KMA prompt, enter the date and time in one of the specified formats, or press <Enter> to use the displayed date and time.
3. At the prompt, press <Enter>. KMA initialization is complete.
4. Press <Enter> to exit. The QuickStart program terminates and a login prompt is displayed (refer to [“Logging into the KMA” on page 288](#)). The KMA now has the minimum system configuration that is required to communicate with the KMS Manager.
5. Your next step is to use the KMS Manager to connect to the Cluster. For procedures, refer to [“Connecting to the Cluster” on page 85](#).

## Joining an Existing Cluster

---

**Important** – Before performing this task, the Security Officer must first log into the KMS Cluster using the KMS Manager and create a KMA. See [“Creating a KMA” on page 102](#).

The KMA Name specified in the KMA initialization process (see [“Initializing the KMA” on page 32](#)) must match the KMA name you enter when you create the KMA.

---

To join a new KMA to an existing Cluster

1. When you complete the KMA initialization process (see [“Initializing the KMA” on page 32](#)), at the prompt, press <Enter>.

The following information is displayed, indicating that you can use this KMA to create a new Cluster, join an existing Cluster, or restore a Cluster from a backup of this KMA.

```
You can now use this KMA to create a new Cluster, or you can have
this KMA join an existing Cluster.  You can also restore a backup
to this KMA or change the KMA Version.
```

```
Please choose one of the following:
```

- ```
(1)  Create New Cluster
(2)  Join Existing Cluster
(3)  Restore Cluster from Backup
```

```
Please enter your choice: 2
```

```
Join Existing Cluster
```

2. At the Please enter your choice: prompt, type 2. The following information is displayed.

```

Join Existing Cluster
-----
Press Ctrl-c to abort.

In order to join a Cluster, the KMA must contact
another KMA which is already in the Cluster.

Please enter the Management Network IP Address or Host Name of an
existing KMA in the cluster: 129.80.60.172

Please enter this KMA's Passphrase:*****

Press Enter to continue:

This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #1: user1

Please enter Key Split Passphrase #1: *****

Press Enter to continue:

Joining cluster...

KMA has joined the KMS cluster.

Press Enter to continue:

Key Management System Version xxx
-----

KMA initialization complete!

You may now connect to the KMA via the KMS Manager
in order to continue with KMS configuration.

Press Enter to exit:

```

---

**Note** – Before this new KMA can communicate with an existing KMA in the Cluster, you must use the KMS Manager to create an entry for this KMA in the existing KMA's database. For procedures, refer to [“Creating a KMA” on page 102](#).

---

3. At the prompt, type the network address of one KMA in the existing Cluster and press <Enter>.
4. At the prompt, type the passphrase for the KMA and press <Enter>.
5. Enter the first Key Split user name for the first KMA.

6. Type the passphrase for the Key Split user, and press <Enter>.

---

**Important** – Enter Key Split user names and passphrases carefully. Any errors cause this process to fail with a non-specific error message. To limit information exposed to an attacker, no feedback is given as to which Key Split user name or passphrase is incorrect.

---

7. Repeat [Step 5](#) and [Step 6](#) until you have entered a sufficient number of Key Split user names and passphrases to form a quorum.
8. At the next Please enter Key Split User Name prompt, press <Enter>. Enter a blank name to finish.  
The initialization is complete.
9. Press <Enter> to exit. The QuickStart program terminates and a login prompt is displayed (refer to [“Logging into the KMA” on page 288](#)). The KMA now has the minimum system configuration that is required to communicate with the KMS Manager.
10. Your next step is to use KMS Manager to connect to the Cluster. For procedures, refer to [“Connecting to the Cluster” on page 851](#).

## Restoring a Cluster From a Backup

This option allows you to create a Security Officer account that can be used to restore the Backup image to the KMA using the KMS Manager. You can use a Backup to restore a KMA's configuration in the event a KMA experiences a failure (for example, hard disk damage). This, however, is not typically required since a KMA that is restored to the factory default state can readily join an existing Cluster and build up its database by receiving replication updates from Cluster peers. Restoring a KMA from a Backup is still useful in the event that all KMAs in a Cluster have failed.

---

### Notes –

You first must create a Backup. For procedures on creating Backups using the KMS Manager, refer to [“Creating a Backup” on page 277](#).

**Sun recommends you specify a new Security Officer name that did not exist in the KMS Cluster when the last backup was performed. If you specify an existing Security Officer name and provide a different passphrase, the old passphrase is overwritten.**

**If you specify an existing Security Officer name and other roles were added to that user before the last backup was performed, these other roles will no longer be assigned to this User.**

---

To restore the backup image:

1. When you complete the KMA initialization process (see [“Initializing the KMA” on page 32](#)), at the prompt, press <Enter>.

The following information is displayed, indicating that you can use this KMA to create a new Cluster, join an existing Cluster, or restore a Cluster from a backup of this KMA.

```
You can now use this KMA to create a new Cluster, or you can have
this KMA join an existing Cluster. You can also restore a backup
to this KMA or change the KMA Version.
```

```
Please choose one of the following:
```

- ```
(1) Create New Cluster
(2) Join Existing Cluster
(3) Restore Cluster from Backup
```

```
Please enter your choice: 3
```

```
Restore Cluster from Backup
```

2. At the Please enter your choice: prompt, type 3. The following information is displayed.

```
Initial Restore Cluster From Backup
Enter Initial Security Officer User Credentials
-----
Press Ctrl-c to abort.

The initial Security Officer User is the first User that
can connect to the KMA via the KMS Manager. This User can
subsequently create additional Users and administer
the system.

Please enter a Security Officer User ID: SO1

A Passphrase is used to authenticate to the KMA when
a connection is made via the KMS Manager.

Passphrases must be at least 8 characters and at most 64
characters in length.
```

3. At the prompt, type the Security Officer's user name and press <Enter>.

---

**Best Practice** – Enter a **temporary** restore Security Officer user ID (for example, RestoreSO) instead of the Security Officer user ID that existed prior to the restore.

---

4. At the prompt, type the Security Officer's passphrase and press <Enter>.



5. At the Please re-enter the Security Officer's Passphrase: prompt, retype the passphrase you entered in [Step 4](#) and press <Enter>.

```

Set Time Information
-----

Press Ctrl-c to abort.

KMAs in a Cluster must keep their clocks synchronized.
Specify an NTP server if one is available in your network.
Otherwise, specify the date and time to which the local clock
should be set.

Please enter the NTP Server Hostname or IP Address (optional):

The date and time for this KMA must be specified in ISO 8601 format
including a time zone. Here are some valid ISO 8601 format
patterns:

    YYYY-MM-DDThh:mm:ssZ
    YYYY-MM-DD hh:mm:ssZ
    YYYY-MM-DDThh:mm:ss-0600
    YYYY-MM-DD hh:mm:ss-0600
    YYYY-MM-DDThh:mm:ss+02:00
    YYYY-MM-DD hh:mm:ss+02:00

Please enter the date and time for this KMA [2007-09-17
22:32:53.698Z]: 2007-09-17 22:33:00-0600

Press Enter to continue:

The KMA is now ready to be restored.

Press Enter to continue:

```

6. If an NTP server is available in your network environment, at the Please enter the NTP Server Hostname or IP Address (optional): prompt, enter the NTP server hostname or IP address.
7. If an NTP server is not available, press <Enter>. Then, at the Please enter the date and time for this KMA prompt, enter the date and time in one of the specified formats, or press <Enter> to use the displayed date and time.
- Ensure the date and time are accurate. Key lifecycles are based on time intervals, and the original creation times for the keys are contained in the backup. An accurate time setting on the replacement KMA is essential to preserve the expected key lifecycles.

8. At the prompt, press <Enter>. The following information is displayed, indicating that initialization is complete.

```
KMA Management System Version xxx
-----

KMA initialization complete!

You may now connect to the KMA via the KMS Manager
in order to continue with KMS configuration.

Press Enter to exit:
```

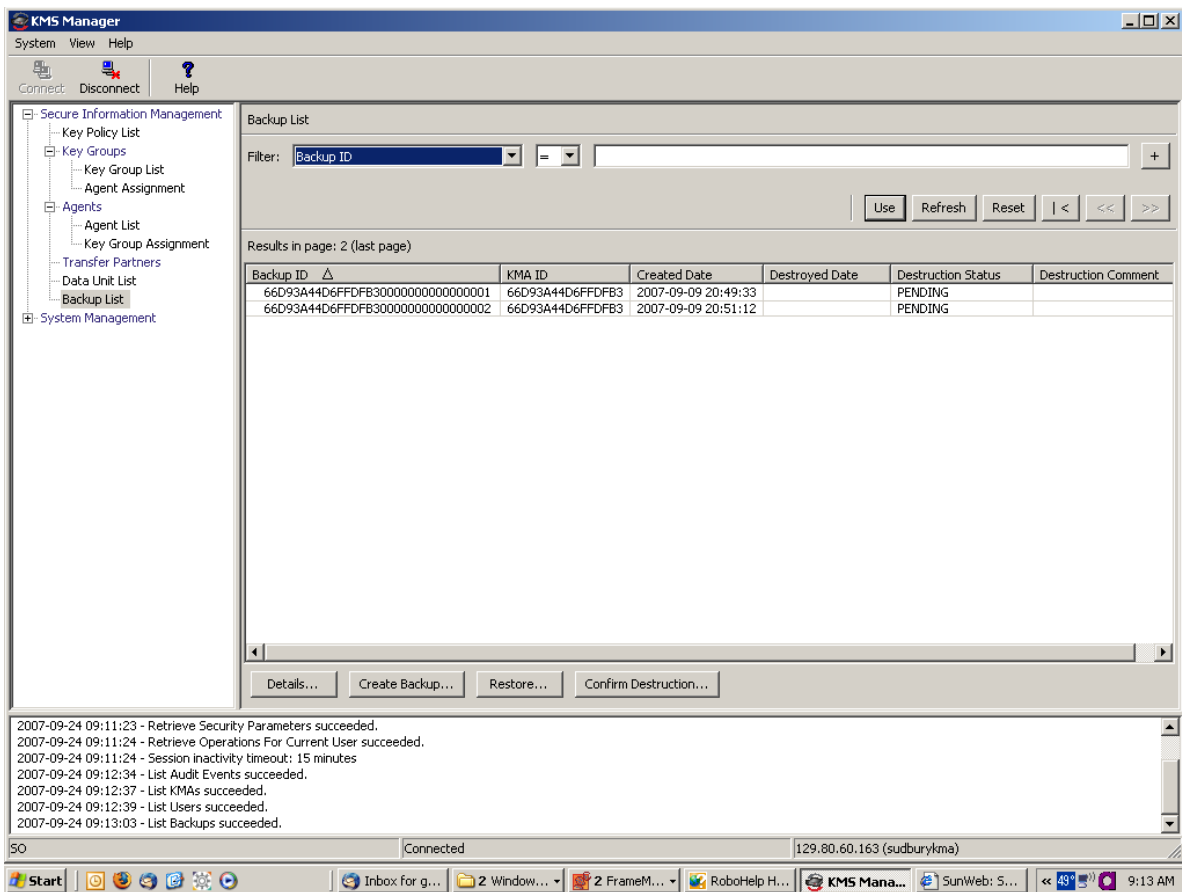
9. Press <Enter> to exit. The QuickStart program terminates and a login prompt is displayed.

---

**Best Practice** – Log in to the KMS Manager GUI as the temporary restore Security Officer user ID you established in [Step 3](#).

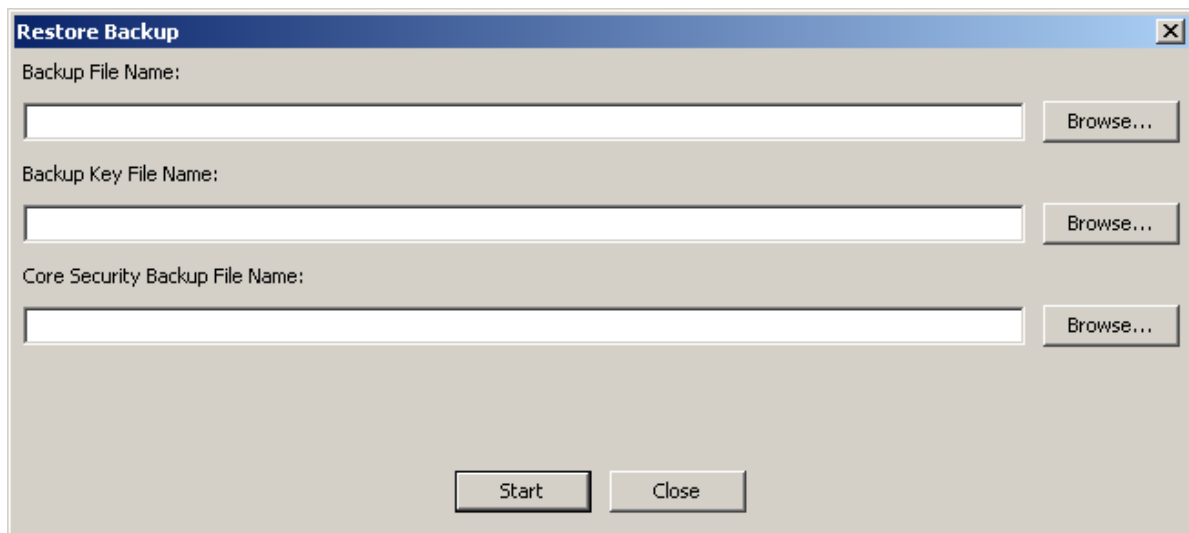
---

10. Login as the Security Officer on the KMS Manager and select **Backup List**. From the Backup List screen, click the **Restore** button to upload and restore the backup to the KMA.



- To complete the restore operation, the KMS Manager prompts for a Backup File that corresponds to the Backup Key file, a Backup Key file, and a Core Security backup file.

The Backup Key file and Backup file must match, but any Core Security Backup file can be used.

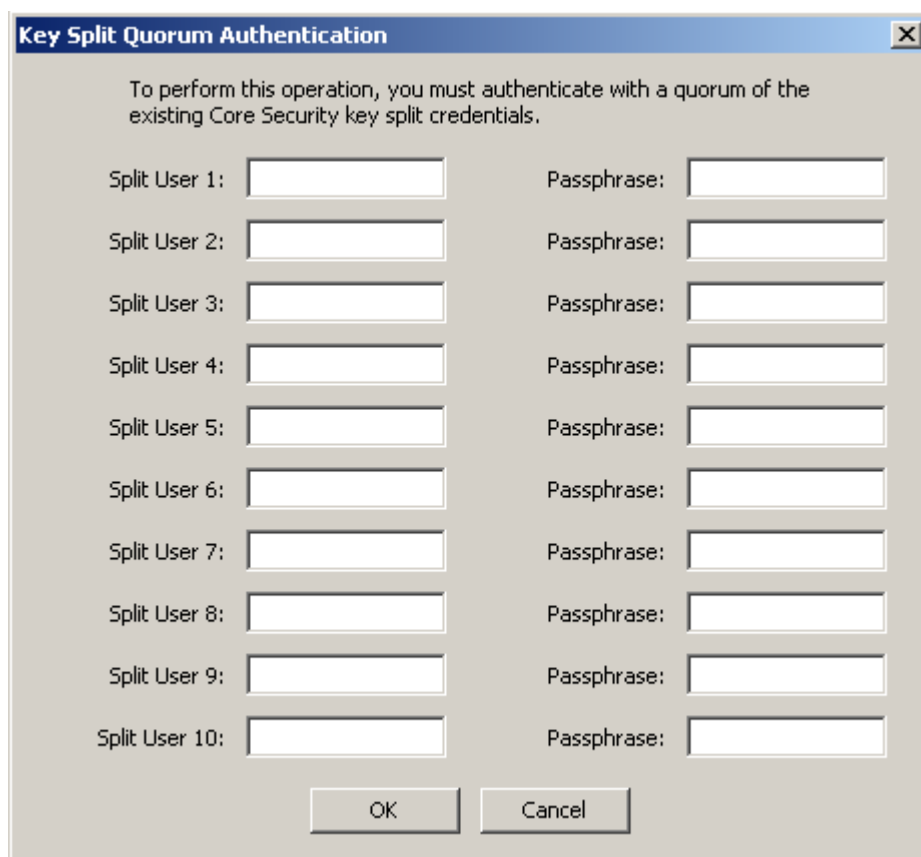


The **Restore Backup** dialog box contains three input fields, each with a **Browse...** button to its right:

- Backup File Name:** [Text Field] **Browse...**
- Backup Key File Name:** [Text Field] **Browse...**
- Core Security Backup File Name:** [Text Field] **Browse...**

At the bottom of the dialog are two buttons: **Start** and **Close**.

12. The KMS Manager then prompts for a quorum of Key Split users. These must be Key Split Credential users that were in effect when the Core Security Backup was performed.



The **Key Split Quorum Authentication** dialog box contains the following text and fields:

To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials.

|                |              |             |              |
|----------------|--------------|-------------|--------------|
| Split User 1:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 2:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 3:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 4:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 5:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 6:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 7:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 8:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 9:  | [Text Field] | Passphrase: | [Text Field] |
| Split User 10: | [Text Field] | Passphrase: | [Text Field] |

At the bottom of the dialog are two buttons: **OK** and **Cancel**.

Once the restore is complete, the Key Split Credentials that were in effect when the backup (not the Core Security Backup) was completed, will be restored.

---

**Important** – Enter Key Split user names and passphrases carefully. Any errors cause the “Joining an Existing Cluster” process to fail with a non-specific error message. To limit information exposed to an attacker, no feedback is given as to which Key Split user name or passphrase is incorrect.

---

13. When the restore process is completed, a new Cluster is created.

---

**Best Practice** – Log in to the KMS Manager GUI using the original Security Officer user ID (the one that existed prior to the restore), and delete the temporary restore Security Officer user ID as a cleanup step. Refer to [“Deleting Users” on page 119](#).

---

## Adding Agents and Enrolling Tape Drives

After the KMA has been set up, you can proceed to add agents and enroll tape drives to use that KMA:

1. Log into the KMS Manager GUI as an Operator and create an agent (refer to [“Creating an Agent” on page 249](#)).
2. Using the Virtual Operator Panel (VOP), perform the following operations. Refer to the VOP documentation if you do not know how to connect to and use the VOP.
  - a. Ask the service representative to license the tape drive(s) (refer to “License the Tape Drives” in chapter 3 of the *KMS Installation and Service Manual*). Use the Virtual Operator Panel (VOP) to perform this function.
  - b. Ask the service representative to enroll the tape drive(s) (refer to “Enroll the Tape Drives” in chapter 3 of the *KMS Installation and Service Manual*).

The customer must supply this information:

    - Is the drive going to use a permanently encrypting tape drive?
    - What is the agent ID, passphrase, and KMS IP address of the appliance?
3. Log into the KMS Manager GUI as a Compliance Officer, create at least one key group (refer to [“Creating a Key Group” on page 208](#)), and assign the tape drives (agents) to this Key Group (refer to [“Assigning a Key Group to an Agent” on page 221](#) and to “Enroll the Tape Drives” in the *KMS Installation and Service Manual*).

## Using the KMS Manager

---

This chapter describes the KMS Manager and explains procedures for:

- Installing the KMS Manager software (page [52](#))
- Invoking the KMS Manager (page [68](#))
- Uninstalling the KMS Manager software (page [82](#)).

The chapter also provides a brief description of the menus and panes.

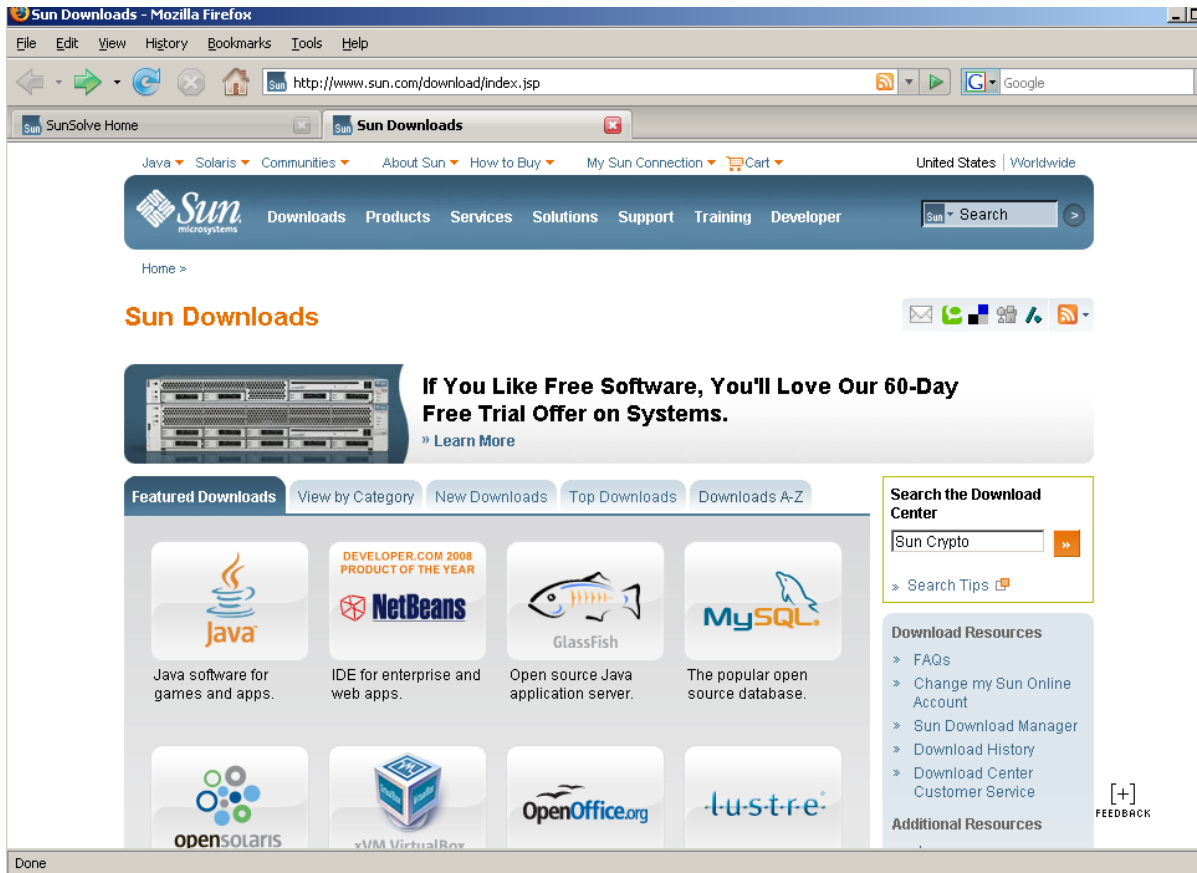
### What is the KMS Manager?

The KMS Manager is an application that serves as a client to the KMA. It can be used to configure, control, and monitor the KMA. Depending on the assigned user roles, users can perform different operations.

# Installing the KMS Manager Software

To download the installer for the KMS Manager software:

1. Go to the Sun Download Center (SDLC) website at the following location:  
<http://www.sun.com/download/index.jsp>



---

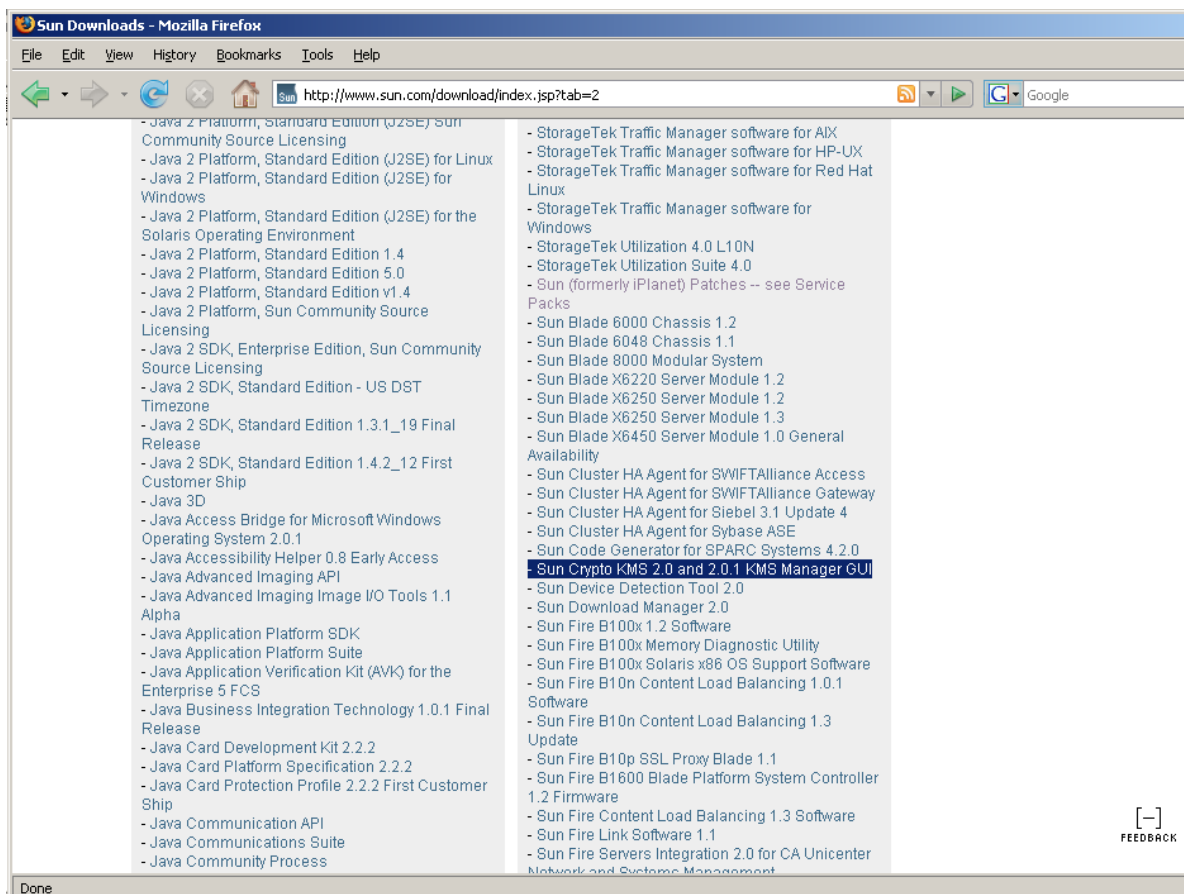
**Note** – There are a number of ways to access the KMS installer. The following procedure describes one method.

---

2. Click the **Downloads A-Z** tab.



3. In the right column, scroll down and click **Sun Crypto KMS 2.0, 2.0.1, and 2.1 KMS Manager GUI**.



4. Provide the following information:

- Platform
- Language
- Your User Name and Password. You can set up the user name and password, if you have not established an account.

---

**Note** – You must also click the box next to the **I agree to the Sun Crypto KMS 2.0, 2.0.1, and 2.1 License Agreement** field to move to the next screen.

---

**Sun Crypto KMS 2.0 and 2.0.1 KMS Manager GUI**

**Provide Information, then Continue to Download**

The KMS Manager GUI software provides the administrative interface to the KMS. The KMS Manager GUI installers also supply the KMS backup utility. Use this download link for the various platform installers.

New features include:

- Critical bug fixes
- Security enhancements

**Select Platform and Language for your download:**

Platform:

Language:

☐ I agree to the Sun Crypto KMS 2.0 and 2.0.1 License Agreement

User Name:

Example: jim23 or jim@company.com

Password:

[» Register Now](#)  
[» Why Register?](#)  
[» Forgot User Name or Password ?](#)

**Log In and Continue »**

**Search the Download Center**

[» Search Tips](#)

**Download Resources**

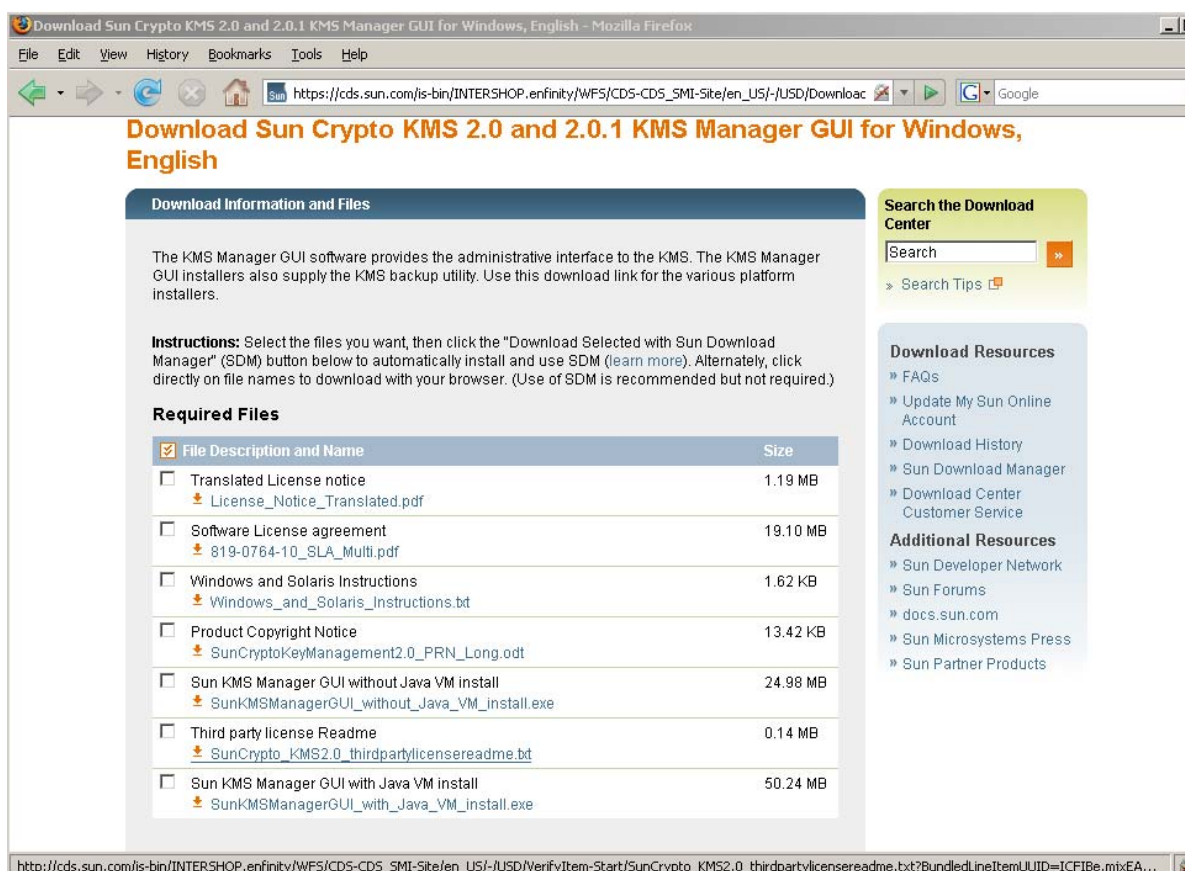
- » FAQs
- » Download History
- » Sun Download Manager
- » Download Center
- » Customer Service

**Additional Resources**

- » Sun Developer Network
- » Sun Forums
- » docs.sun.com
- » Sun Microsystems Press
- » Sun Partner Products

5. Click **Log In and Continue**.

Either the Solaris or Windows download screen is displayed, depending on the platform you selected. The following screen shows the Windows download.



- At this point, you can either continue the installer download by
  - Starting the Sun Download Manager (SDM). Refer to [“SDM Download”](#) on page 56.
  - Clicking directly on the file name. See [“Direct Download”](#) on page 60.

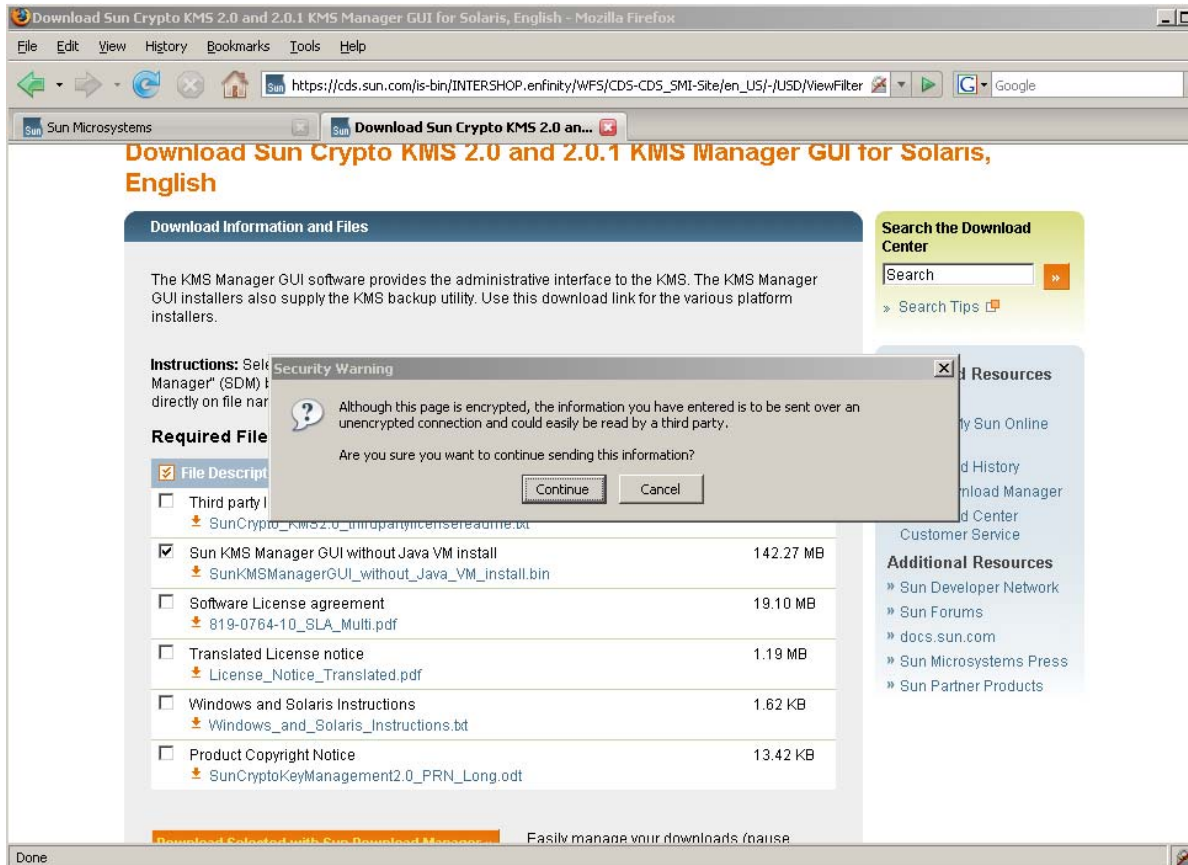
---

**Note** – SDM is recommended but not required. It allows you to pause, resume, restart, and verify the download process.

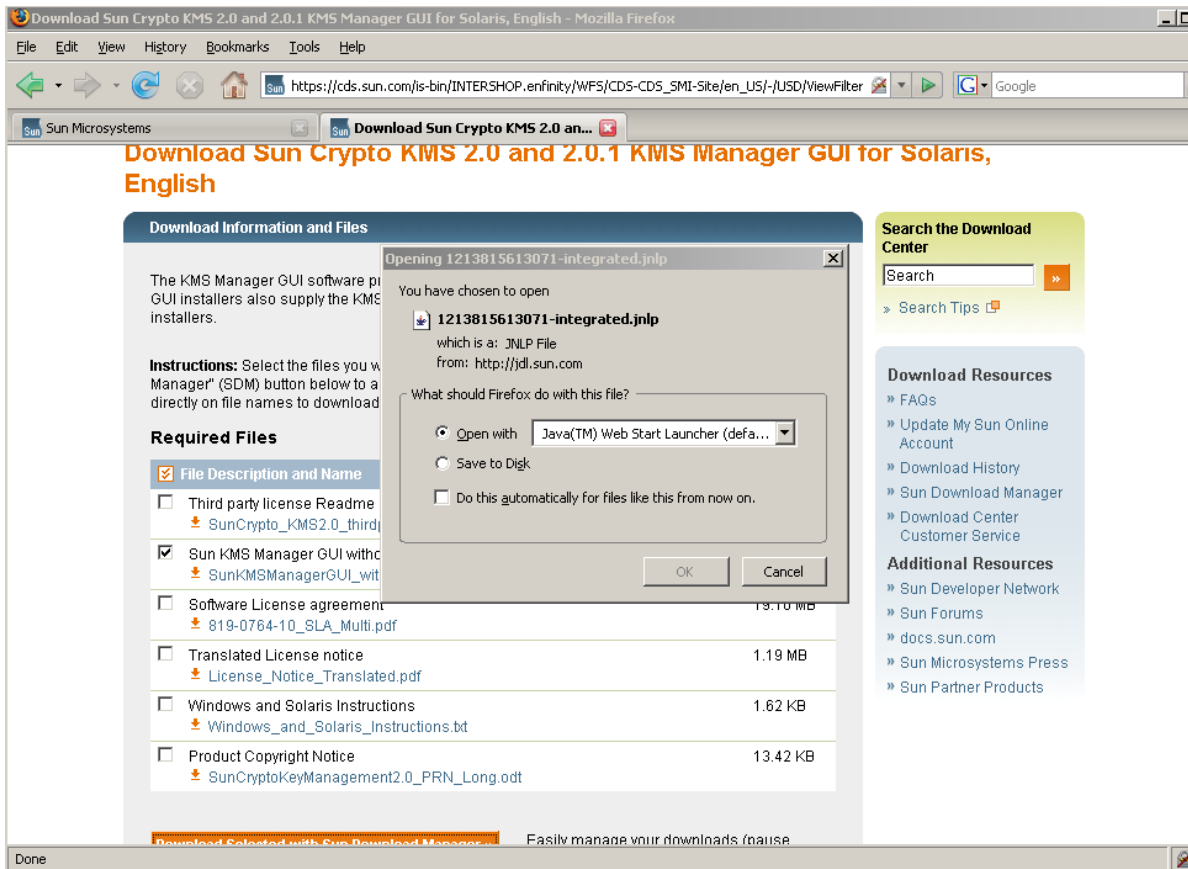
---

## SDM Download

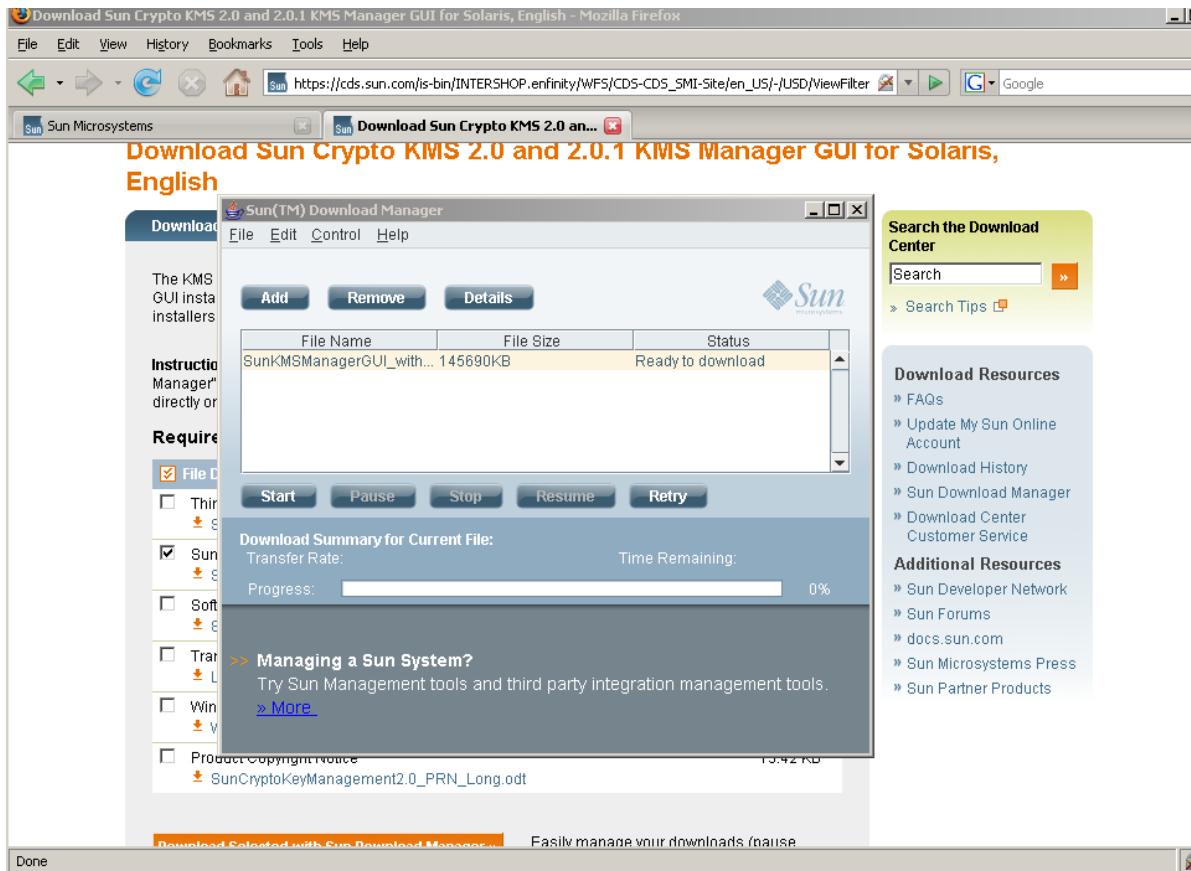
- Click the box next to **Sun KMS Manager GUI without Java**, if Java is installed on your Windows system, or **Sun KMS Manager GUI with Java VM install**, if it is not.
- Click **Download Selected with Sun Download Manager**.
- Click **Continue** when the security warning is displayed.



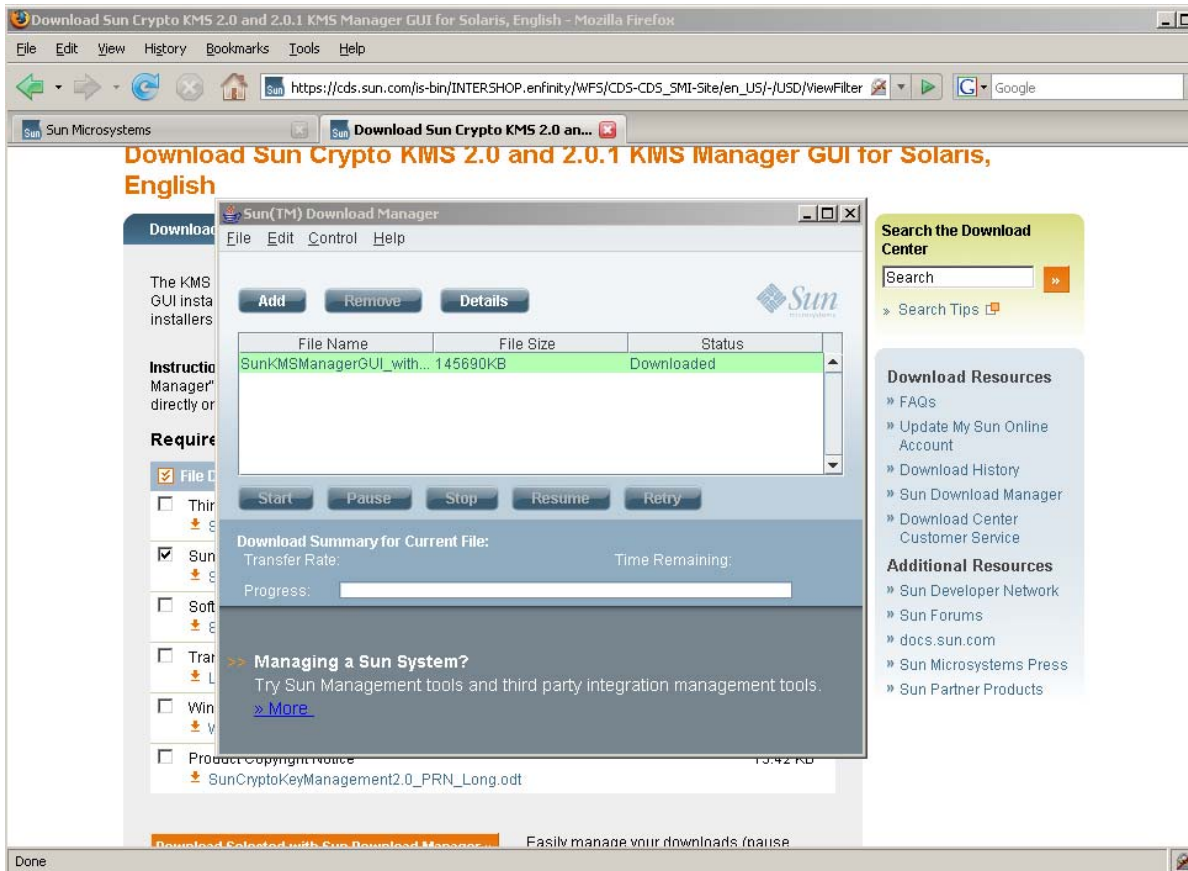
- d. Choose either to start downloading the installer now or to save it to disk to launch it later.



e. Select **Start**.



When the download is complete, this screen displays:

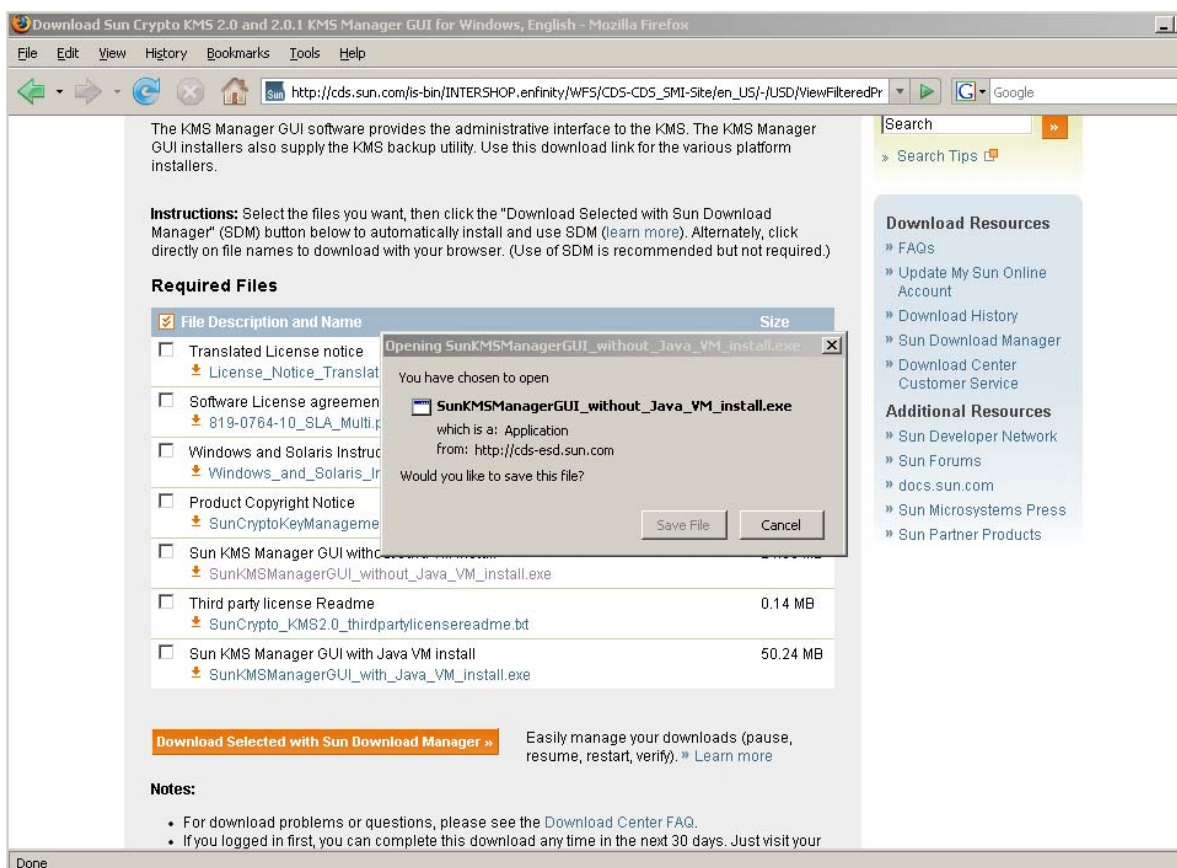


The installer shortcut should now be on your desktop.

See [“Starting the KMS Installation”](#) on page 61 to initialize the installer program.

## Direct Download

Click directly on the file name and click **Save File** to download the installer with your browser. The installer shortcut is installed directly to your desktop.



See [“Starting the KMS Installation”](#) on page 61 to initialize the installer program.



## Starting the KMS Installation

7. Depending on whether you are running a Windows or Solaris system, select the applicable process to invoke the installer program.
    - For Windows, double-click the shortcut to start the installer program.
    - For Solaris,
      - a. Set your DISPLAY environment to identify the system to which this installer should be displayed.
        - i. If you start the installer program on the local Solaris system, set your DISPLAY environment variable to “:0.0.”
        - ii. Navigate to the directory where you downloaded the installer.
        - iii. Invoke the installer.
- For example, if you downloaded the installer to the /tmp directory, and you plan to invoke it on your local Solaris system, you start the installer by entering the following commands at a shell prompt:

```
DISPLAY=:0.0
export DISPLAY
cd /tmp
ls install.bin
sh ./install.bin
```

---

**Note** – If you invoke the installer on one Solaris system and want it to be displayed on another Solaris system, set your DISPLAY environment variable to identify the system on which it should be displayed. On the display system, first run the xhost(1) utility to allow access from the system from which you will invoke the installer.

For example, on the system (named “hosta”) where you wish to display the installer, enter:

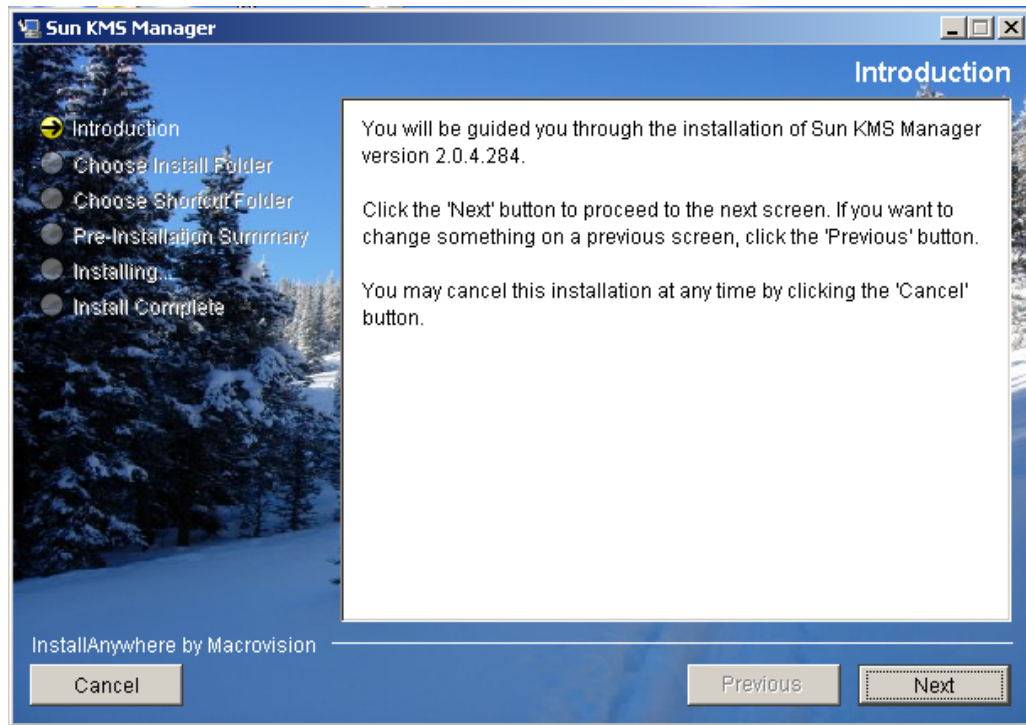
```
xhost +
```

On the system where you start the installer, enter:

```
ping hosta
DISPLAY=hosta:0.0
export DISPLAY
cd /tmp
ls install.bin
sh ./install.bin
```

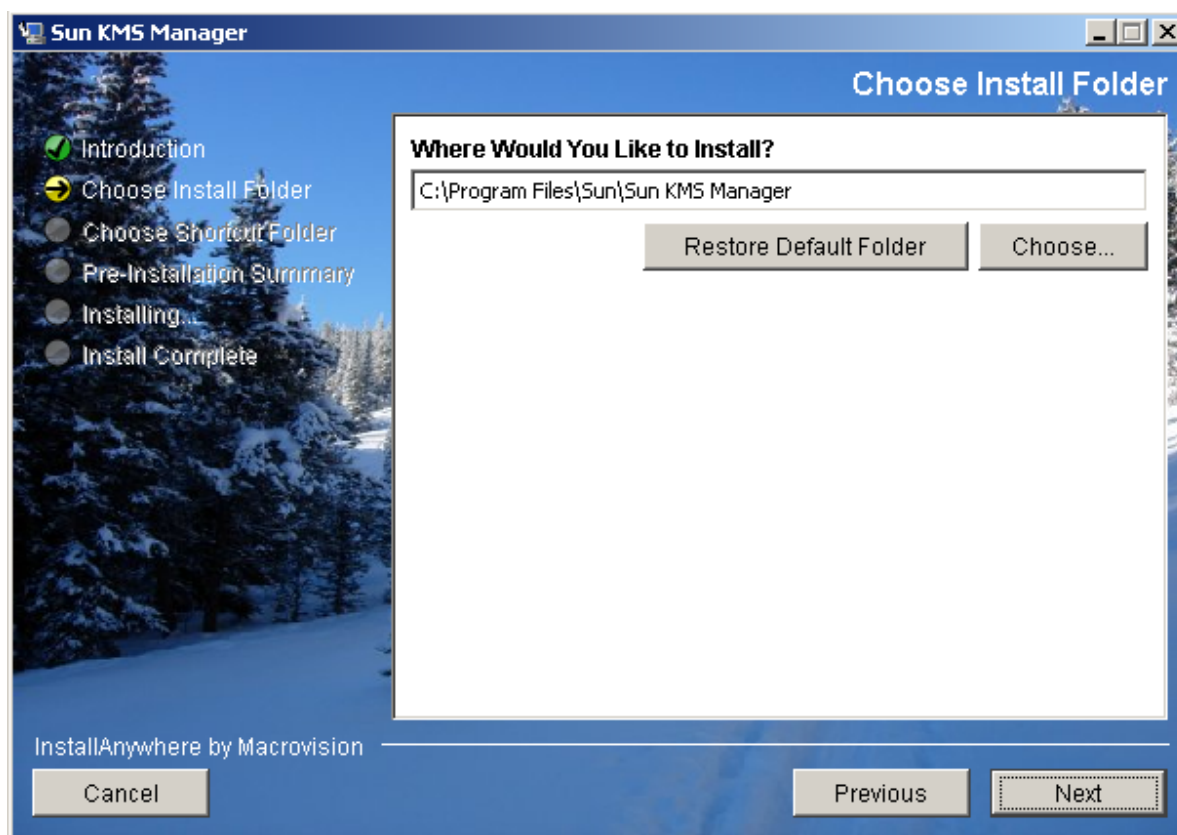
---

The Introduction window is displayed. The following screen examples are for a Windows system.



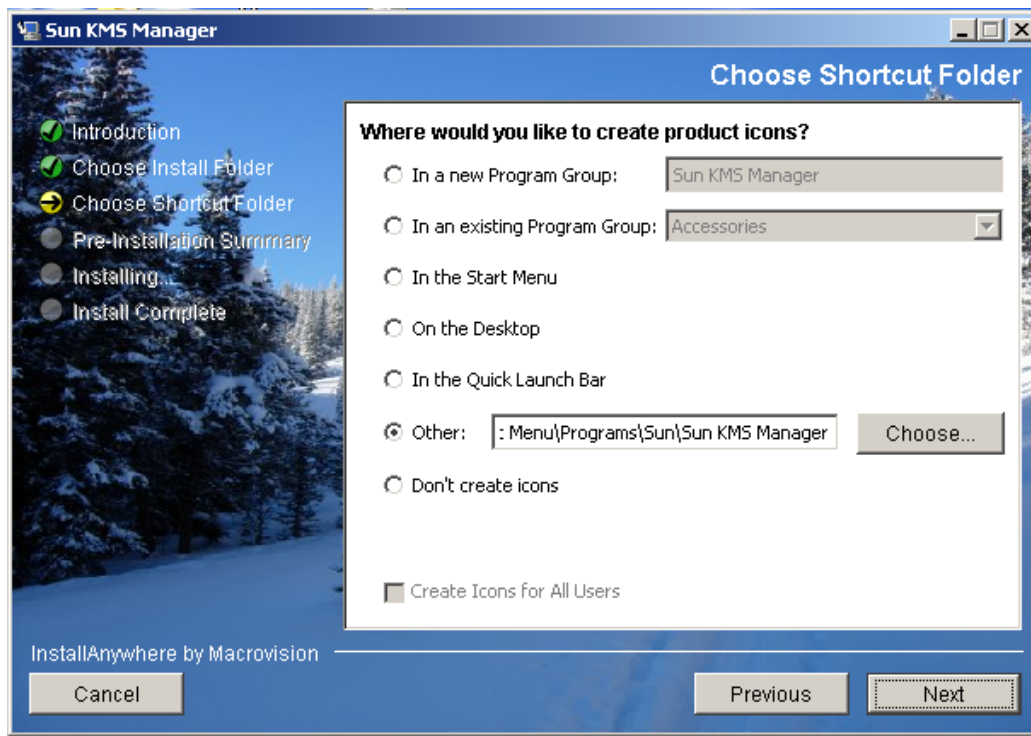
8. Select Next.

9. The Choose Install Folder window is displayed.



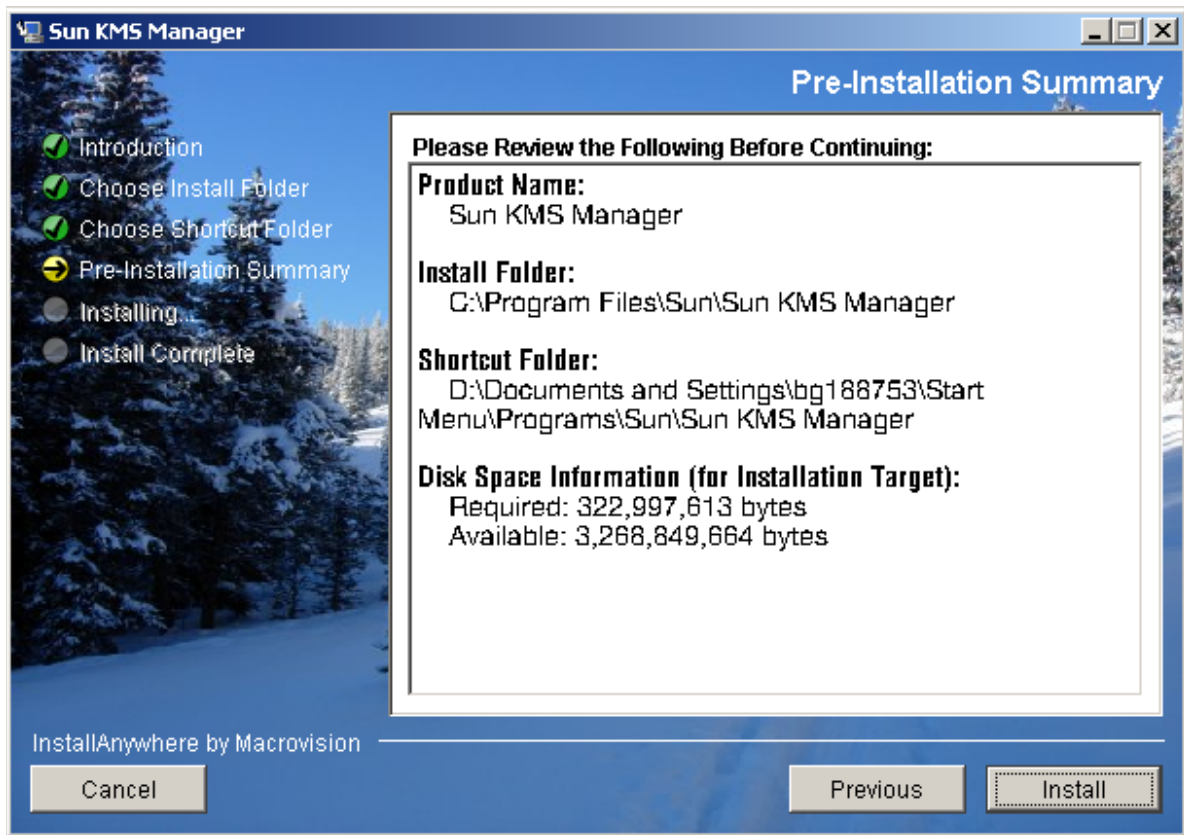
10. To select the default folder, select Next, or supply your own installation folder, and select Next.

11. The Choose Shortcut Folder window is displayed, allowing you to create the product icons where you desire.

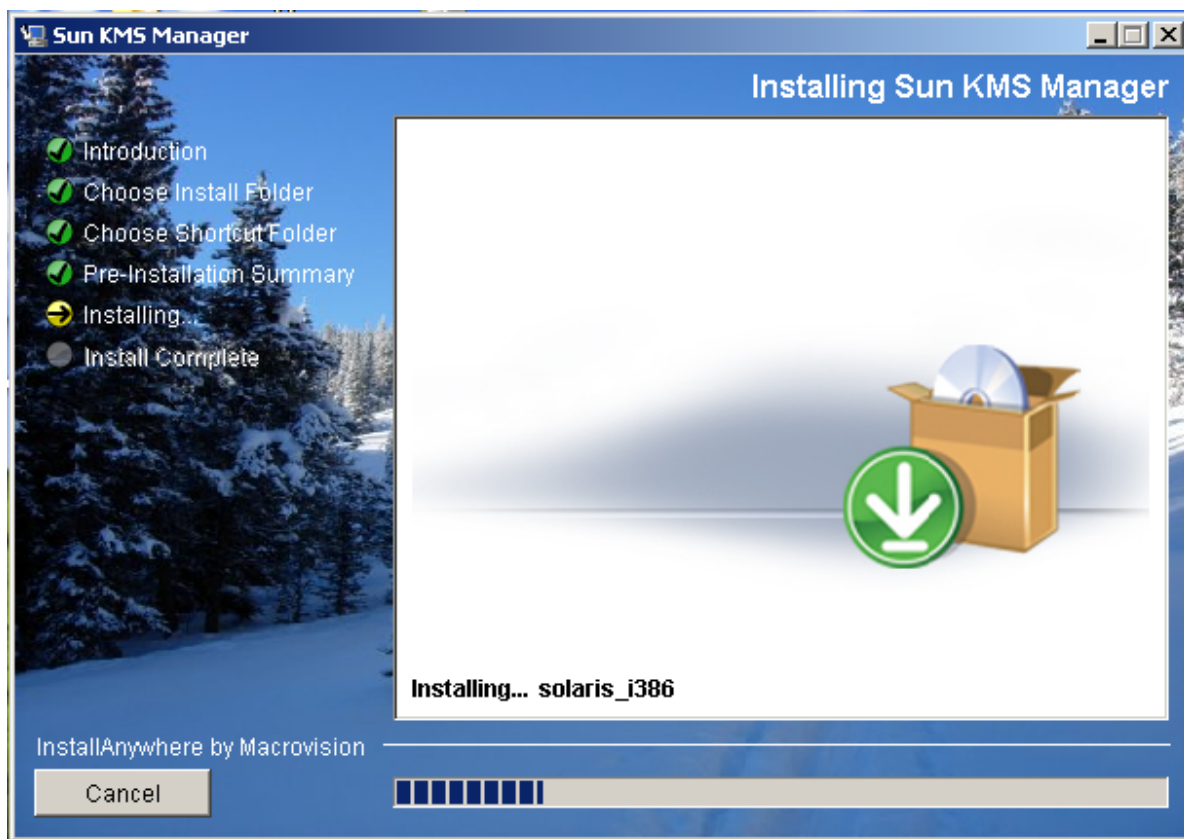


12. Select Next after you make your choice.

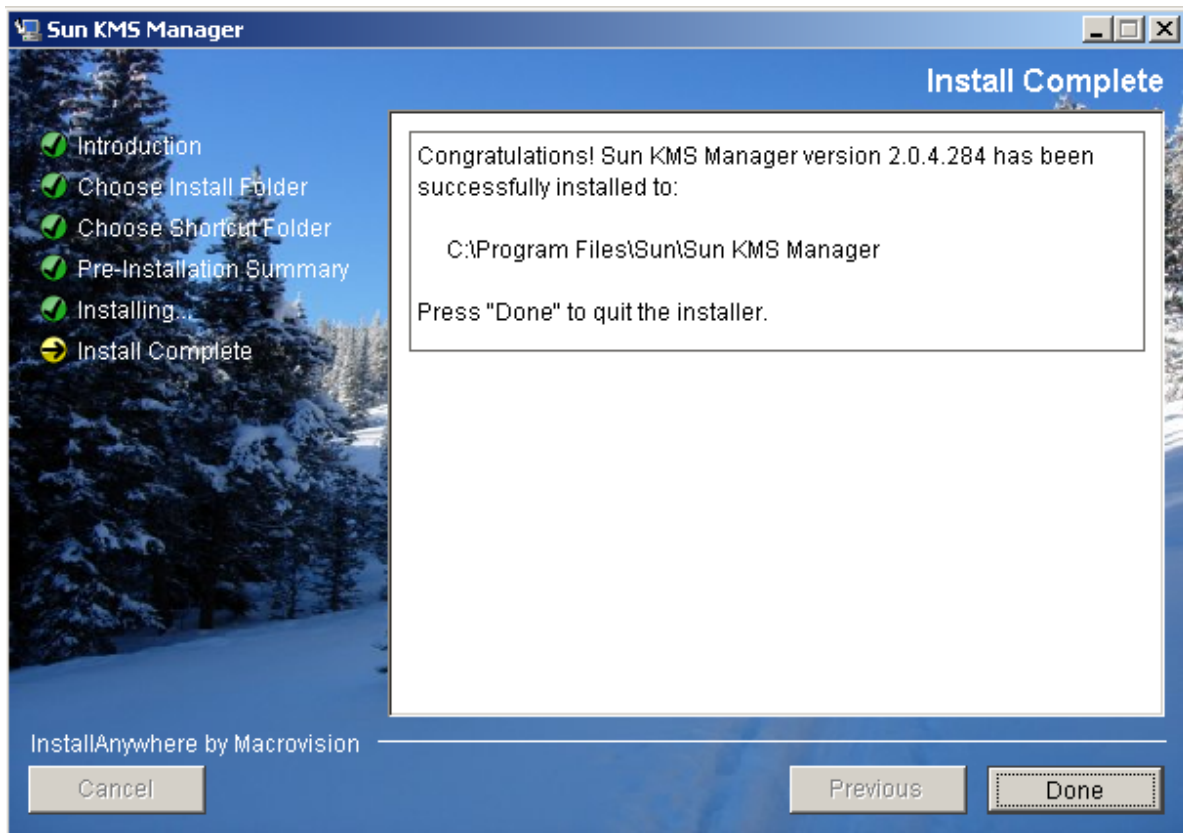
13. The Pre-Installation summary screen is displayed.



14. Select Install to install the KMS Manager, or select Previous to revise your setup.



15. The installation process is now complete. Select Done to exit.



## Invoking the KMS Manager

Two methods can be used to invoke the KMS Manager, depending on your environment:

- Startup with Windows
- Startup with Solaris

### Starting the KMS Manager with Windows

If you instructed the installation program to create a shortcut, double-click it to launch the KMS Manager application.



Otherwise, launch Windows Explorer, navigate to where you installed the KMS Manager, and invoke KMS\_Manager.exe.

### Starting the KMS Manager with Solaris

As with Windows, you can direct the installation program to create a shortcut. For example, if you create the shortcut in your home directory, you can invoke it at a shell prompt by entering:

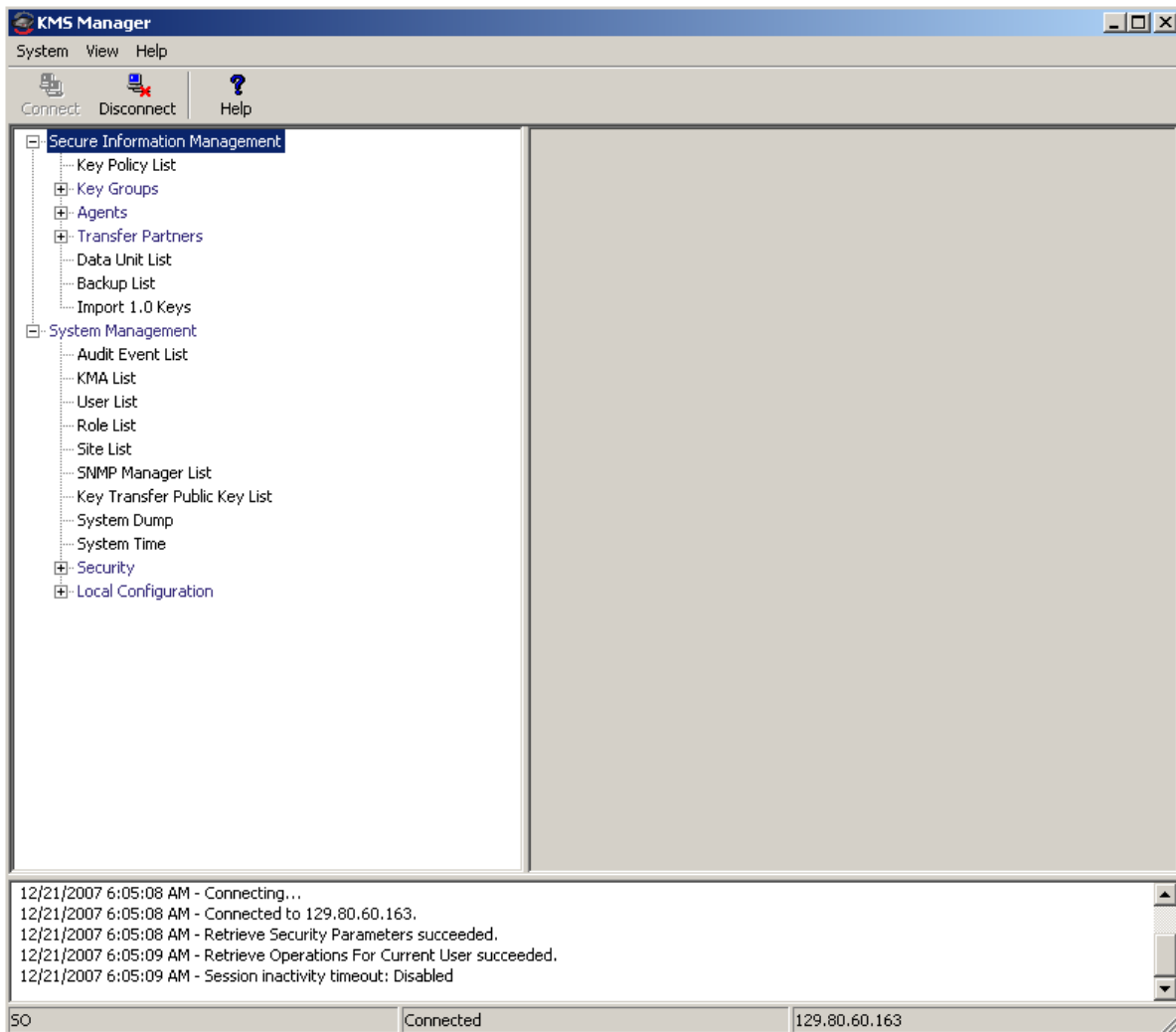
```
~/KMS_Manager
```

Alternatively, you can navigate to where you installed the KMS Manager and invoke KMS\_Manager.exe.



# KMS Manager GUI Overview

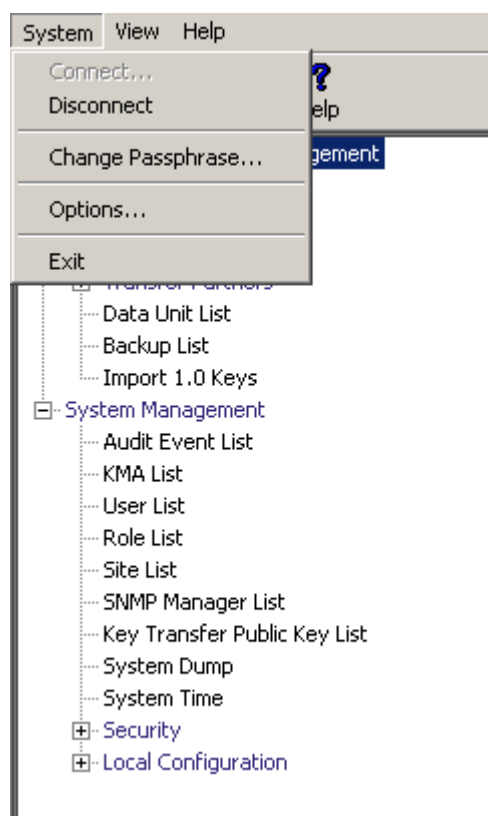
The KMS Manager GUI is shown below with a sample menu.



The KMS Manager GUI contains a System menu, View menu, and Help menu. Click the appropriate action bar item to display a menu and then select a menu item.

Toolbar buttons provide shortcuts to several menu options.

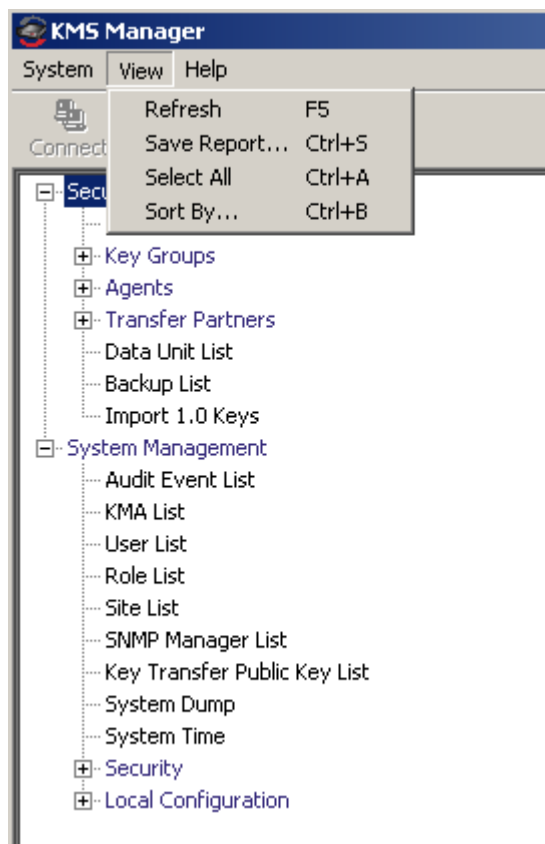
## System Menu



### *System Menu Options*

- **Connect:** Displays the Connect to Cluster dialog box that allows you to connect to a pre-existing Cluster using a Profile or create a new Cluster profile.
- **Disconnect:** Displays the Disconnect from KMA dialog box that allows you to disconnect from the KMA.
- **Change Passphrase:** Displays the Change passphrase dialog box that allows you to modify the passphrase.
- **Options:** Displays the Options dialog box that is used to specify various configuration settings.
- **Exit:** Closes the KMS Manager GUI.

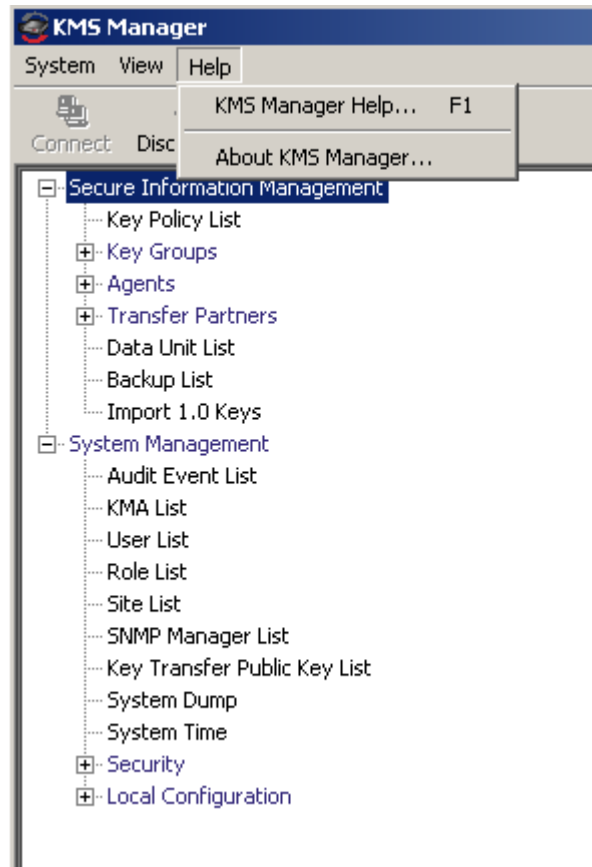
## View Menu



### *View Menu Options*

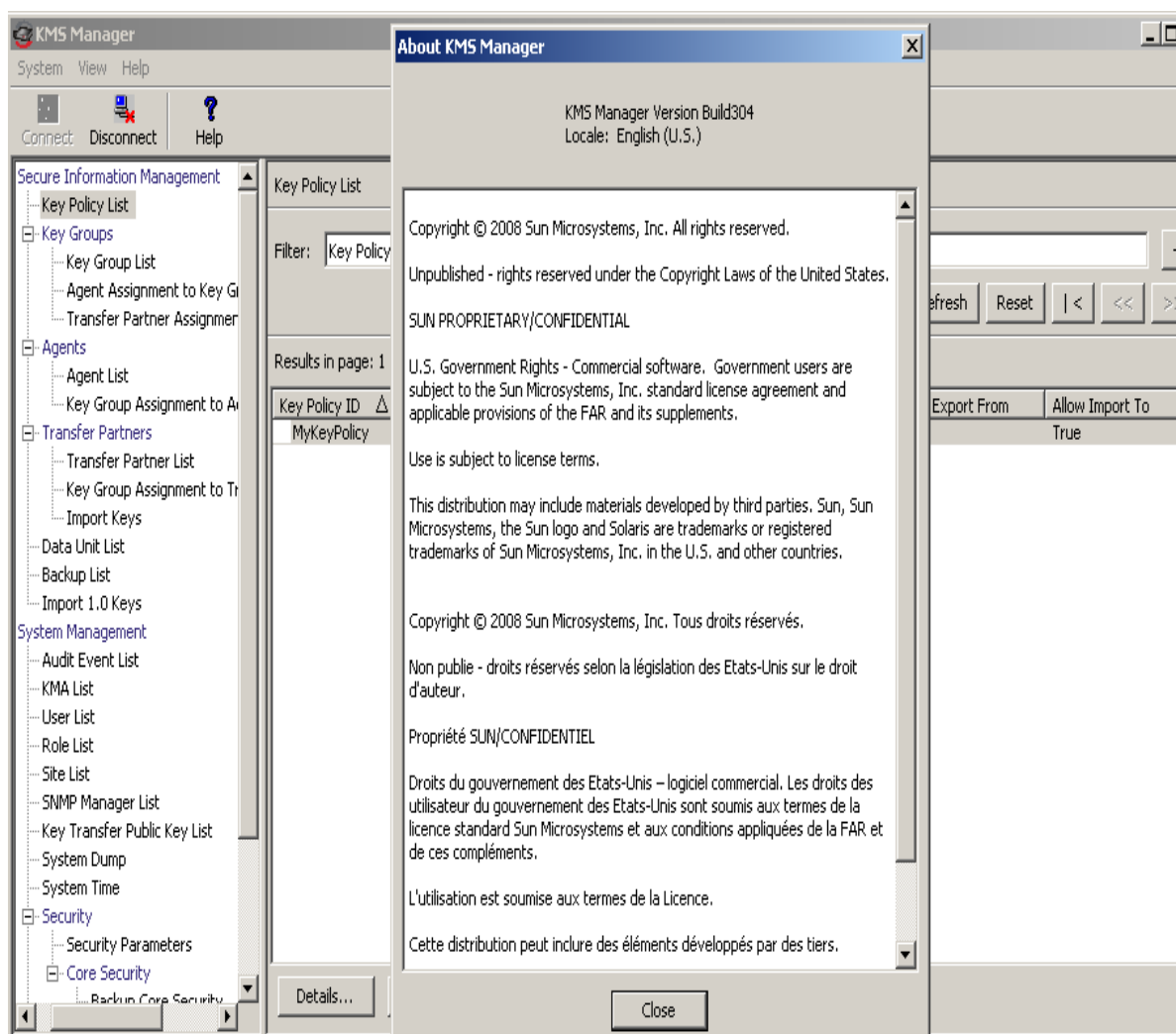
- **Refresh:** Refreshes the screen.
- **Save Report:** Save Report allows you to download the contents of any List screen. to a text file on the system where the KMS Manager is running.
- **Select All:** Select All selects all items on a List screen.
- **Sort By:** Sorts a list of items on a List screen. This is equivalent to clicking on column headings in a list.

## Help Menu





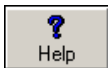
## Help Menu Options

- **KMS Manager Help:** Displays the online help index and table of contents for KMS Manager.
- **About KMS Manager:** Displays the version and copyright information about KMS Manager. Click the Close button to close this dialog box.



## Toolbar Buttons

The table below describes the Toolbar buttons on the KMS.

| Button  | Description   |
|---|---|
|  | Displays the Connect to KMA dialog box that allows the user to connect to a KMA by selecting a profile. |
|  | Displays the Disconnect from KMA dialog box that allows the user to disconnect from the KMA.            |
|  | Displays the online help index and table of contents for KMS.   |

## Shortcut Keys

Shortcut keys allows you to choose commands in a single step. The following shortcut keys are used:

|   |        |
|---|--------|
| Cuts the current selection  | Ctrl+X |
| Copies the current selection  | Ctrl+C |
| Copies the contents from the Clipboard to the current selection point | Ctrl+V |
| Brings up a dialog box to save a report to a local site               | Ctrl+S |

## Menu Accelerator Keys

Menu accelerator keys are supported for all menu items. Hold down the “Alt” key to display the accelerator keys.

## Using Online Help

You can use online help for complete information about the KMS. Online help is easy to use. You are able to view topics in various ways. You can:

- Browse a table of contents
- Search for keywords
- Use an index
- Navigate backward
- Print topics.

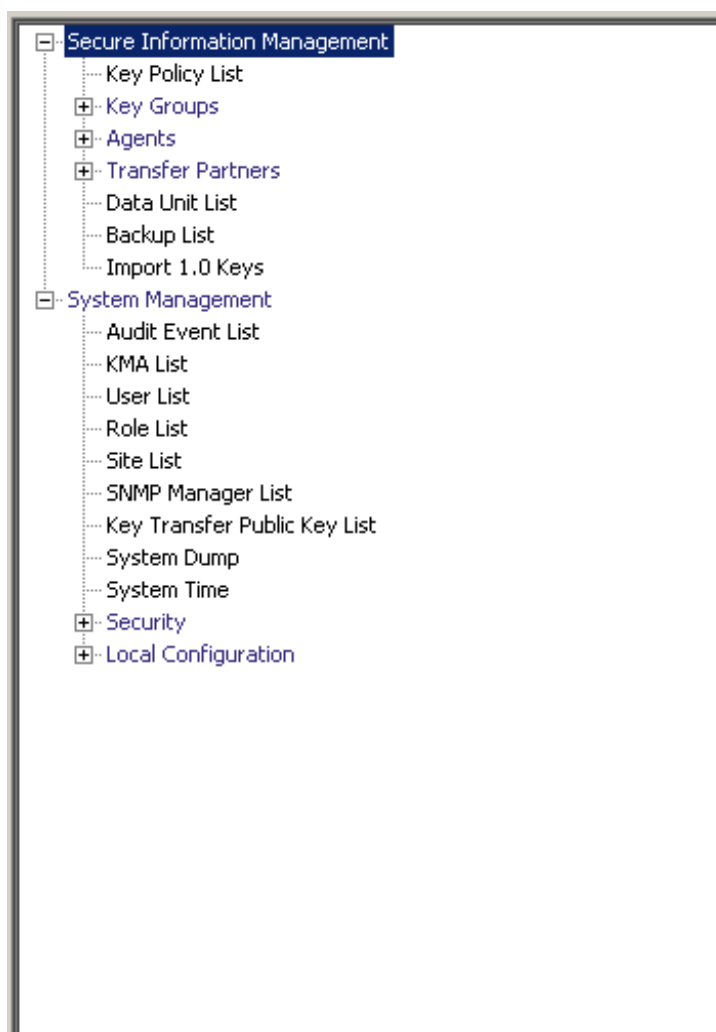
## KMS Manager GUI Panes

The KMS Manager GUI includes three panes:

- KMS Management Operations Tree
- KMS Management Operation Details
- Session Audit Log.

### KMS Management Operations Tree Pane

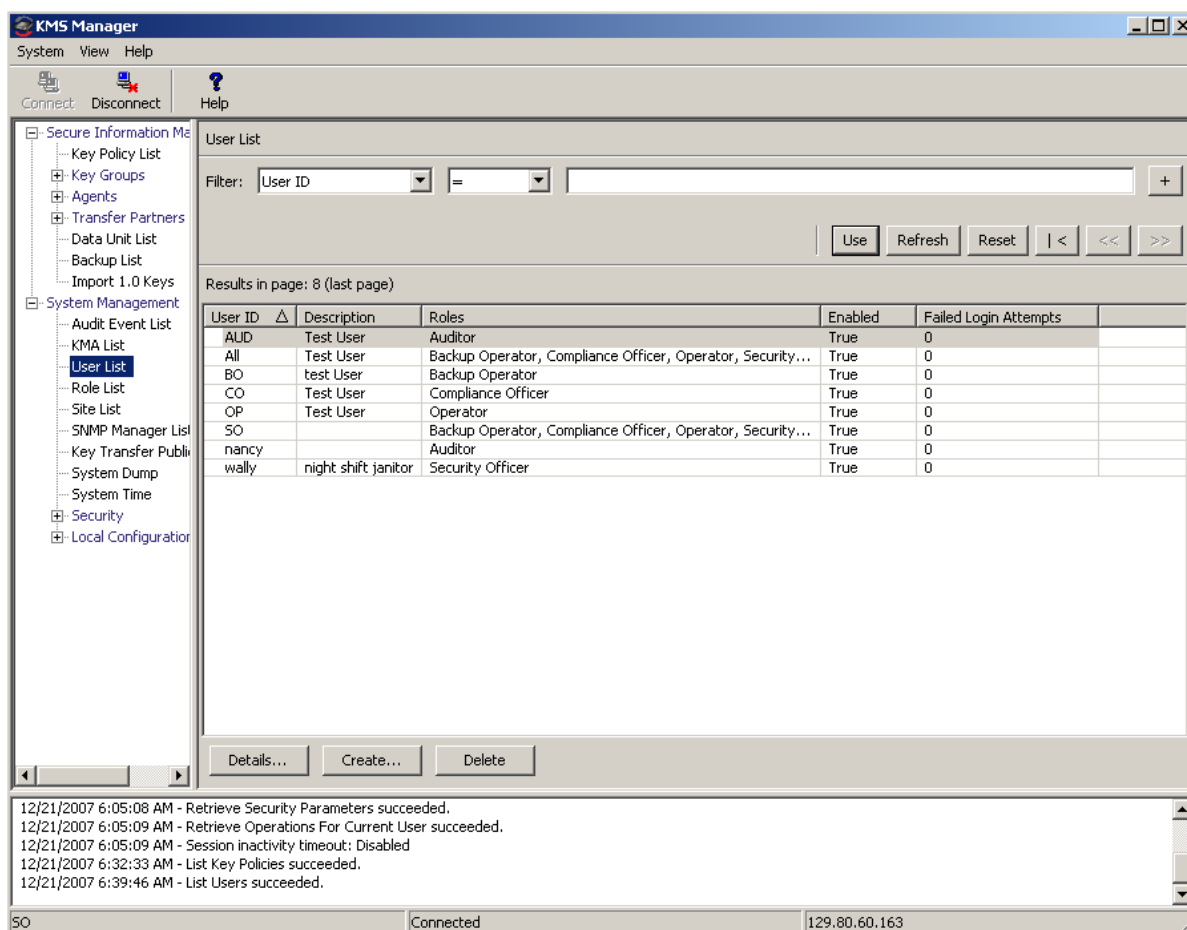
The KMS Management Operations Tree pane, located on the left-side of the screen, displays all operational functions of the KMS. Depending on your assigned role(s), the options on this tree pane differ. The example below shows the operations that a Security Officer can perform.





## KMS Management Operation Details Pane

When an operation is selected, the KMS Manager Operation Details pane, to the right of the Operations Tree Pane, displays the required components for the selected operations. The user can apply filters on the items that are displayed in list panels. The example below shows the User List, when the User List menu option was selected from the System Management menu in the Operations Tree pane.



## Session Audit Log Pane

The Session Audit Log pane, below the Operations Tree Pane and the Operations Details Pane, provides a scrollable list of the most recent session events.

The screenshot shows the KMS Manager application window. The left pane displays a tree view with categories like Secure Information Management and System Management. The 'User List' item under System Management is selected. The main pane shows a 'User List' section with a filter box and a table of users. Below the table are buttons for 'Details...', 'Create...', and 'Delete'. At the bottom, a log pane shows a series of system events with timestamps and descriptions.

**User List**

Filter: User ID = [ ] +

Use Refresh Reset | < << >> >

Results in page: 8 (last page)

| User ID | Description         | Roles  | Enabled | Failed Login Attempts |
|---------|---------------------|--|---------|-----------------------|
| AUD     | Test User           | Auditor  | True    | 0                     |
| All     | Test User           | Backup Operator, Compliance Officer, Operator, Security... | True    | 0                     |
| BO      | test User           | Backup Operator  | True    | 0                     |
| CO      | Test User           | Compliance Officer   | True    | 0                     |
| OP      | Test User           | Operator   | True    | 0                     |
| SO      | Test User           | Backup Operator, Compliance Officer, Operator, Security... | True    | 0                     |
| nancy   |                     | Auditor  | True    | 0                     |
| wally   | night shift janitor | Security Officer   | True    | 0                     |

Details... Create... Delete

12/21/2007 6:05:08 AM - Connecting...  
12/21/2007 6:05:08 AM - Connected to 129.80.60.163.  
12/21/2007 6:05:08 AM - Retrieve Security Parameters succeeded.  
12/21/2007 6:05:09 AM - Retrieve Operations For Current User succeeded.  
12/21/2007 6:05:09 AM - Session inactivity timeout: Disabled  
12/21/2007 6:32:33 AM - List Key Policies succeeded.

SO Connected 129.80.60.163

## Status Bar

The Status Bar, at the bottom of the screen, is comprised of the following fields:

- **User Name:** Displays the username of the currently logged-in user. In the screen below, the Security Officer (SO) is logged in.
- **Connection Status:** Displays the state of the current connection, that is, **Connected**
- **KMA IP Address:** Displays the Management Network IP address and Name of the target KMA.

If there is no connection to the KMA, the Status fields are blank.

The screenshot shows the KMS Manager application window. The title bar is 'KMS Manager'. The menu bar includes 'System', 'View', and 'Help'. Below the menu bar are buttons for 'Connect', 'Disconnect', and 'Help'. The left sidebar contains a tree view with the following items: 'Secure Information Management' (expanded), 'Key Policy List', 'Key Groups', 'Agents', 'Transfer Partners', 'Data Unit List', 'Backup List', 'Import 1.0 Keys', 'System Management' (expanded), 'Audit Event List', 'KMA List', 'User List' (selected), 'Role List', 'Site List', 'SNMP Manager List', 'Key Transfer Public', 'System Dump', 'System Time', 'Security', and 'Local Configuration'. The main area is titled 'User List' and contains a filter box with 'User ID' selected, an equals sign, and a search field. Below the filter are buttons for 'Use', 'Refresh', 'Reset', and navigation arrows. The text 'Results in page: 8 (last page)' is displayed. A table lists users with columns: 'User ID', 'Description', 'Roles', 'Enabled', and 'Failed Login Attempts'. The table contains 8 rows of data. At the bottom of the main area are buttons for 'Details...', 'Create...', and 'Delete'. The status bar at the very bottom shows 'SO' for the user, 'Connected' for the status, and '129.80.60.163' for the IP address. A log window at the bottom of the main area shows several system messages dated 12/21/2007.

| User ID | Description         | Roles  | Enabled | Failed Login Attempts |
|---------|---------------------|--|---------|-----------------------|
| AUD     | Test User           | Auditor  | True    | 0                     |
| All     | Test User           | Backup Operator, Compliance Officer, Operator, Security... | True    | 0                     |
| BO      | test User           | Backup Operator  | True    | 0                     |
| CO      | Test User           | Compliance Officer   | True    | 0                     |
| OP      | Test User           | Operator   | True    | 0                     |
| SO      |                     | Backup Operator, Compliance Officer, Operator, Security... | True    | 0                     |
| nancy   |                     | Auditor  | True    | 0                     |
| wally   | night shift janitor | Security Officer   | True    | 0                     |

12/21/2007 6:05:08 AM - Connected to 129.80.60.163.  
12/21/2007 6:05:08 AM - Retrieve Security Parameters succeeded.  
12/21/2007 6:05:09 AM - Retrieve Operations For Current User succeeded.  
12/21/2007 6:05:09 AM - Session inactivity timeout: Disabled  
12/21/2007 6:32:33 AM - List Key Policies succeeded.  
12/21/2007 6:39:46 AM - List Users succeeded.

## Panels

The are common panel components in the KMS Manager screens. These are described below:

### Title

Displays the title of the screen.

### Filter

Allow you to filter the database by specific keys. It contains the following components:

**Table label:** Specifies the table to which the filtering applies

**Filter Attribute combo box:** Indicates the fields to filter

**Filter Operator 1 combo box:** Provides the filter operators that are applied to Filter Value 1. The filter operations are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not Empty

**Filter Value 1 control:** Used as a single value or the starting value of the filter key range

**Filter Value 2 control:** Used as a single value or the ending value of the filter key range

**Use button:** Applies the filter to the displayed list.

### Refresh:

Click this button to refresh the displayed list. This does not apply filters selected since the last Use or Reset, and does not change the page of the list.

### Reset:

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of items that can be displayed on the current page. Appends "(last page)" if you are at the end of the list. The maximum number of items displayed on a page is defined by the Query Page Size value on the Options dialog.

---

**Note** – If the number of records output is greater than the Query Page Size, multiple pages are displayed. Click the buttons below the filters to move between pages.

---

**Sorting:**

Click a column heading to sort the list by that field. If the output requires multiple pages, the complete set of results is sorted, then the corresponding page is returned.

**Message**

Displays messages that are related to database queries. It works in conjunction with the Database View list. It contains the following components:

- Static text label: Displays error messages, such as:  
`Result limit exceeded. 10,000 results returned. Use a filter to reduce the filter size.`

## Uninstalling the KMS Manager Software

Two options are available to begin to uninstall the KMS software:

- Navigate to the directory where the uninstall program resides and launch the executable file from there
- For Windows users only, launch the Add or Remove Programs process

In both cases, the Preparing Setup window will be displayed after you finish these procedures. See [“Completing the Uninstall Process” on page 83](#).

### Invoking the Executable File

To uninstall the KMS Manager software:

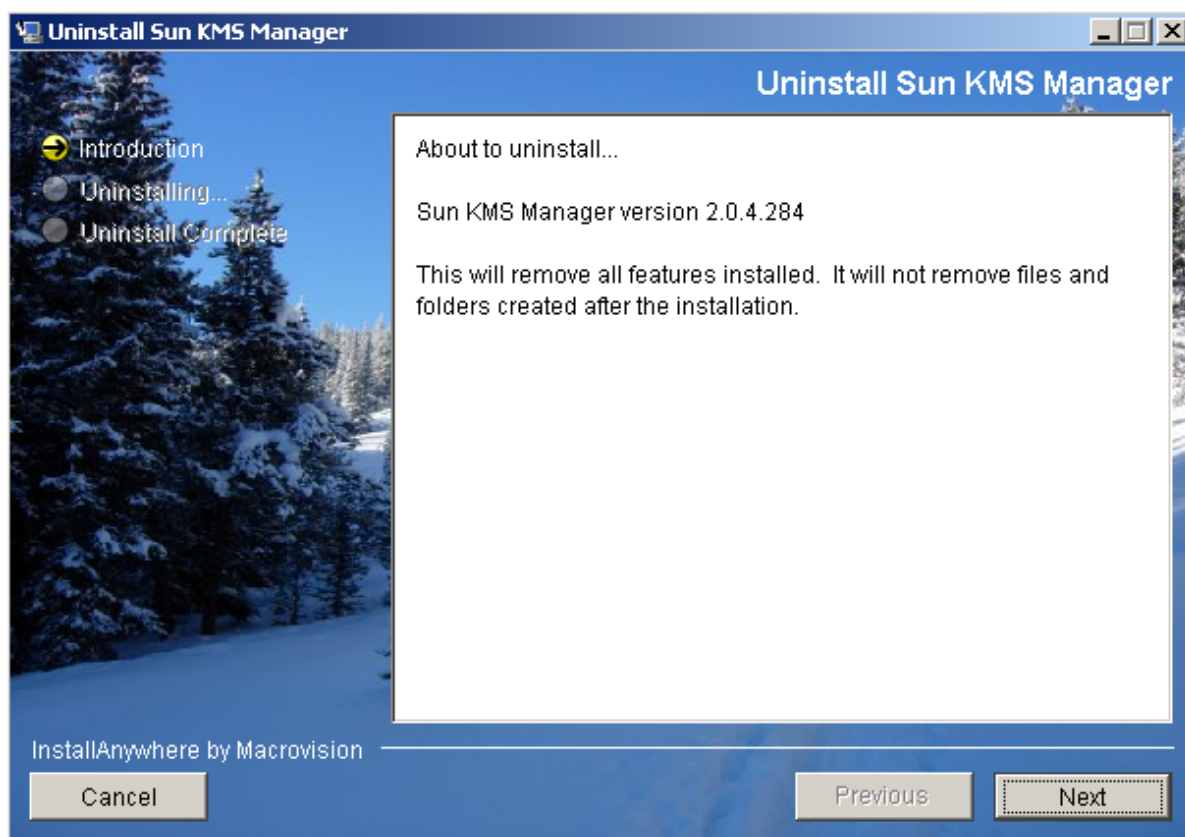
1. Navigate to the “Uninstall\_Sun KMS Manager” directory, which resides under the directory where the KMS Manager was installed.
2. Invoke the “Uninstall Sun KMS Manager” (Windows) or “Uninstall\_Sun\_KMS\_Manager” (Solaris) executable to launch the uninstall process.
3. The Preparing Setup window is displayed, while the install/uninstall program prepares for the uninstall process.

### Invoking Add/Remove Programs (Windows Only)

1. Click **Start**, select **Settings**, **Control Panel**, double-click **Add or Remove Programs**. The Add or Remove Programs window is displayed. Scroll down the list (if the software is not visible), select Sun KMS Manager, then click the Change/Remove button.
2. The Preparing Setup window is displayed, while the install/uninstall program prepares for the uninstall process.

## Completing the Uninstall Process

The KMS uninstall dialog box is displayed, prompting you to confirm that you want to remove the selected application and all its features.



1. Click the Next button to continue or click the Cancel button to stop the process and return to the Add or Remove Program window (Windows) or shell prompt (Solaris).

---

**Note** – Your connection profiles will not be removed.

---

2. When the uninstall process is completed, the Uninstall Complete window is displayed. Click the Finish button to close this window. Close this window to return to the Add or Remove Program window (Windows) or shell prompt (Solaris).





## Using the System Menu

---

This chapter gives detailed instructions for connecting to the KMA using the KMS Manager. It also gives instructions for using the other options on the System menu.

---

### Connecting to the Cluster

---

**Important** – Before connecting to a KMA, at least one Cluster profile must exist and a user must be created and enabled on the KMA.


---

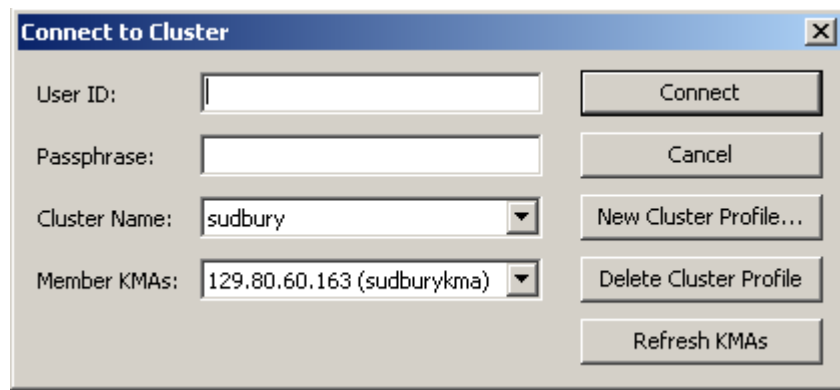
This section gives procedures for connecting to the KMA using the KMS Manager. If this is the first time that you are connecting to the KMA, you must first define a Cluster profile. On subsequent occasions, you will be able to connect to the KMA using the Cluster profile that you created. The KMS Manager uses the Cluster profile information to initiate communications with a Cluster (the KMA IP address).

---

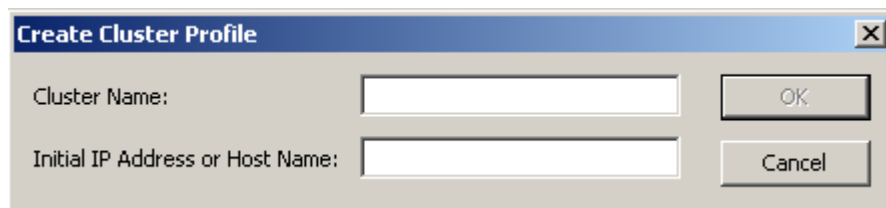
### Creating a Cluster Profile

To create a Cluster profile:

1. From the System menu, select Connect or from the Tool bar, click . The Connect to Cluster dialog box is displayed. If you have pre-existing profile, the Cluster profile name and its IP address will be displayed in the Cluster Name and IP Address fields respectively.



2. Click the New Cluster Profile button. The Create Cluster Profile dialog box is displayed.



3. Complete the following parameters:

**Cluster Name**

Type a value that uniquely identifies the Cluster profile name.

**Initial IP Address or Host Name**

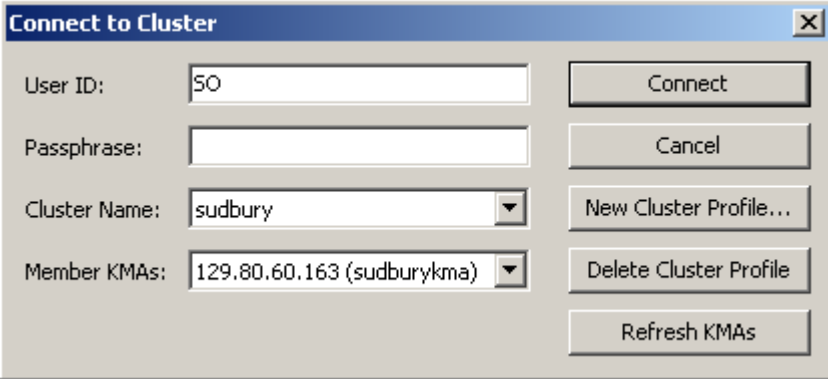
Type the Service Network IP address or Host Name of the initial KMA in this Cluster to connect to. The choice of which network to connect to depends on what network the computer system where the KMS Manager is running is connected to.

---

**Note** – You only have to create a single Cluster profile because covers the entire Cluster and can be used by any user (of the Agent). The only reason that you would want to create another Cluster profile is if you want to establish a second Cluster or you have changed the IP addresses of all KMAs in the current Cluster.

---

4. Click the OK button. The Connect to Cluster dialog box is displayed with the Cluster profile information you created.



The image shows a 'Connect to Cluster' dialog box with the following fields and buttons:

|               |   |   |
|---------------|---|---|
| User ID:      | <input type="text" value="SO"/>                         | <input type="button" value="Connect"/>                |
| Passphrase:   | <input type="password"/>                                | <input type="button" value="Cancel"/>                 |
| Cluster Name: | <input type="text" value="sudbury"/>                    | <input type="button" value="New Cluster Profile..."/> |
| Member KMAs:  | <input type="text" value="129.80.60.163 (sudburykma)"/> | <input type="button" value="Delete Cluster Profile"/> |
|               |   | <input type="button" value="Refresh KMAs"/>           |

5. Complete the following parameters and click the Connect button:

#### User ID

Type the name of the user who will connect to specified KMA, or if this is the first time that you are connecting to the KMA after performing the initial QuickStart process, type the name of the Security Officer created during the QuickStart.

#### Passphrase

Type the passphrase for the selected user.

#### Cluster Name

Select the Cluster to connect to.

#### Member KMAs

Select the KMA to connect to within that Cluster.

---

**Note** – If a KMA has joined the Cluster after the user previously connected to that Cluster, that KMA does not appear in the Member KMAs list. To update the list, enter the user name and passphrase, choose a Cluster profile, and click the Refresh KMAs button.

---

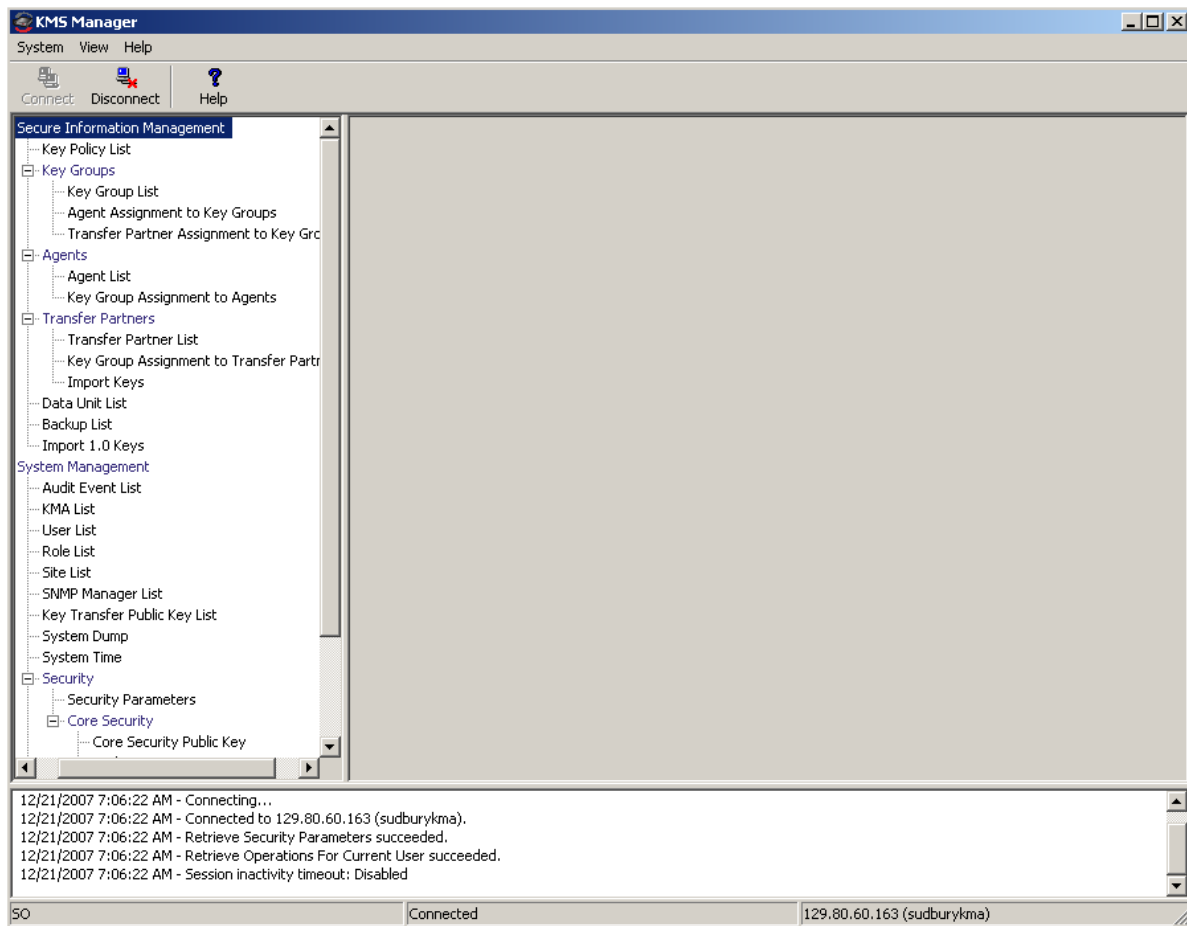


---

**Important** – The KMA authenticates the user ID and passphrase. The returned list of KMA IP addresses is used to populate the Cluster profile and stored on the host. The next time the user connects to the KMA, the user can enter the user name and passphrase, choose a Cluster profile, and select a KMA.

---

6. If the connection is successful, the Status bar of the KMS Manager GUI displays the user name and alias, the KMA's connection status (**Connected**), the KMA's IP address.



7. You can now use the KMS Manager to perform various operations. See [Chapter 5](#) through [Chapter 9](#) for the operations that various user roles can perform.

---

**Note** – Depending on the role assignment, the tasks in the KMA Management Operations Tree pane differ.

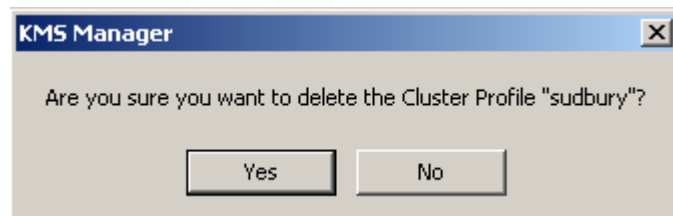
---

---

## Deleting a Cluster Profile

To delete a Cluster profile:

1. From the Connect to Cluster dialog box, click the down-arrow beside the Cluster Name field, highlight the Cluster profile that you want to delete and click the Delete Cluster Profile button. The Delete Cluster Profile dialog box is displayed, prompting you to confirm that you want to delete the selected Cluster profile.




2. Click the Yes button to delete the Profile. The Cluster Profile is deleted and you are returned to the Connect to Cluster dialog box.

---

## Disconnecting from the KMA

To disconnect from the KMA:

1. From the System menu, select **Disconnect** or from the Tool bar, click . You are immediately disconnected from the KMA and the KMS Cluster. The session Audit Log pane indicates the date and time when you disconnected from the KMA.

---

## Changing the Passphrase

---

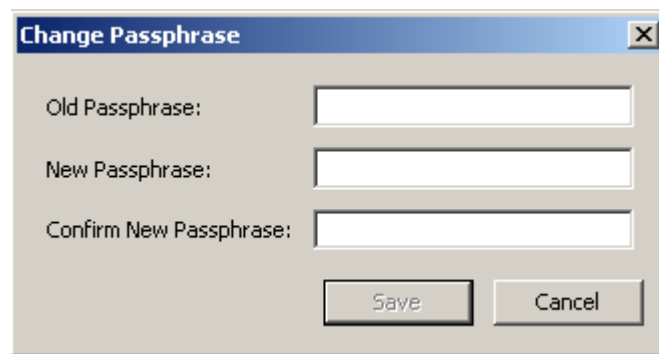
**Note** – This menu option is only enabled if the user is connected to a KMA using a profile.

---

This function allows users to change their own passphrases. This function does not invalidate a user's current certificate.

To change a connected user's passphrase:

1. From the System menu, select **Change Passphrase....** The Change Passphrase dialog box is displayed.

A screenshot of a 'Change Passphrase' dialog box. The dialog has a title bar with the text 'Change Passphrase' and a close button (X). Inside the dialog, there are three text input fields labeled 'Old Passphrase:', 'New Passphrase:', and 'Confirm New Passphrase:'. Below the input fields are two buttons: 'Save' and 'Cancel'.

2. Complete the following parameters and click the OK button:

**Old Passphrase**

Type the user's old passphrase.

**New Passphrase**

Type the user's new passphrase.

**Confirm New Passphrase**

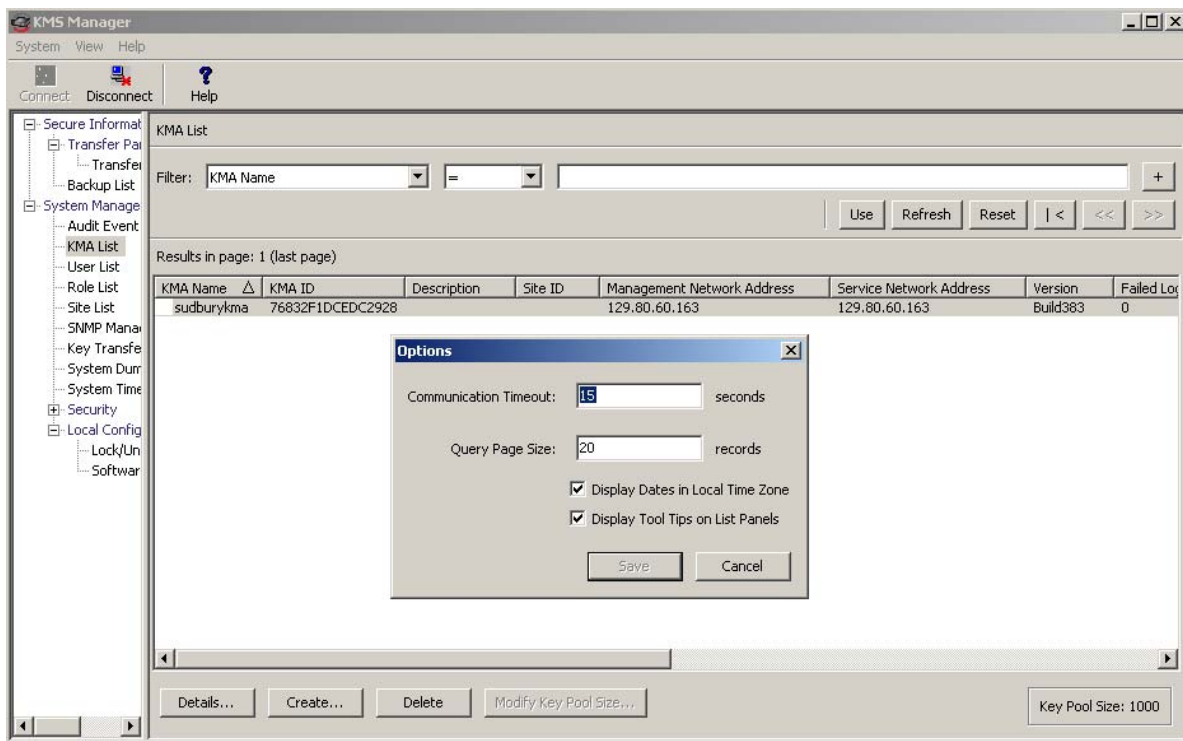
Retype the same passphrase.

3. The following message is displayed in the session Audit Log pane, indicating the date and time when you changed the user's passphrase.

# Specifying the Configuration Settings

To specify the configuration settings:

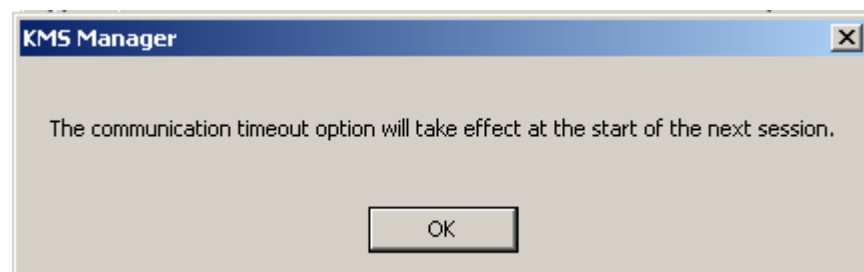
1. From the System menu, select Options.... The Options dialog box is displayed, showing the current configuration settings.



2. Modify the following parameters, as required and click the Save button:

## Communication Timeout

Type a timeout period (in seconds) for communications with the connected KMA. If the KMA does not respond within the timeout value, the KMS Manager will give up on the communication. The minimum value is 1; the maximum value is 60. The default is 15.



**Query Page Size**

Type the maximum number of items to display on a screen, dialog, or tab on a dialog that displays a list of items. Paging can be used to view a list longer than this limit. The minimum value is 1; the maximum value is 1000. The default is 20.

**Display Dates in Local Time Zone**

Select this check box to display all dates and times in the local machine's time zone (i.e., where the KMS Manager is running), rather than UTC. The default is selected. The following confirmation message is displayed.

**Display Tool Tips on List Panels**


Select this check box if you want to see a tool tip when you position the cursor over an item. This is the default.



---

## Exiting from the KMS Manager

To exit from the KMS Manager:

1. From the System menu, select **Exit** or from the Title bar, click  . The KMS Manager closes and you are returned to the Windows desktop.
2. The KMS Manager immediately disconnects if connected and closes.



## Security Officer Operations

---

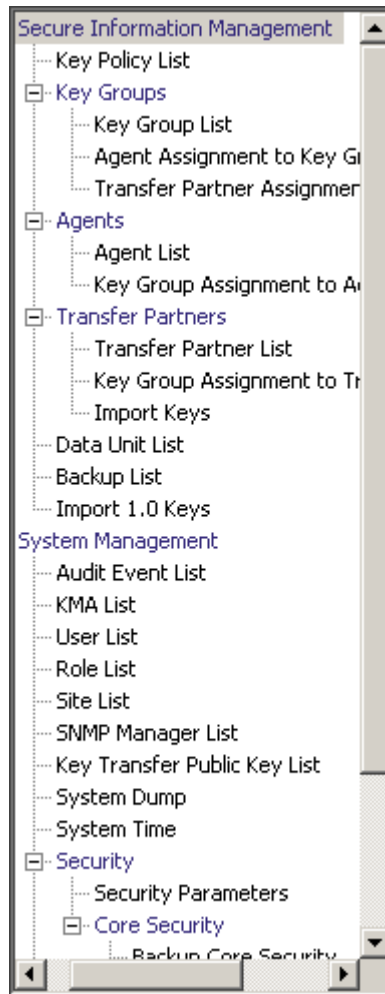
A Security Officer manages security settings, users, sites, and transfer partners. This chapter describes the following:

- Operations that a user who has been given a Security Officer role can perform. If you have been assigned multiple roles, refer to the appropriate chapter for instructions on performing the specific role.
- Procedures for enabling and disabling a technical support account

---

## Security Officer Role

As a Security Officer, you can manage the entities (KMAs, Users, Sites, Transfer Partners) as well as various security aspects of the system.

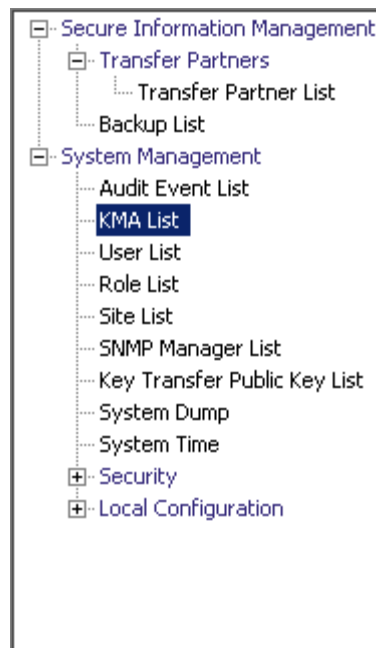


---

## KMA List Menu

The KMA List menu option allows you to:

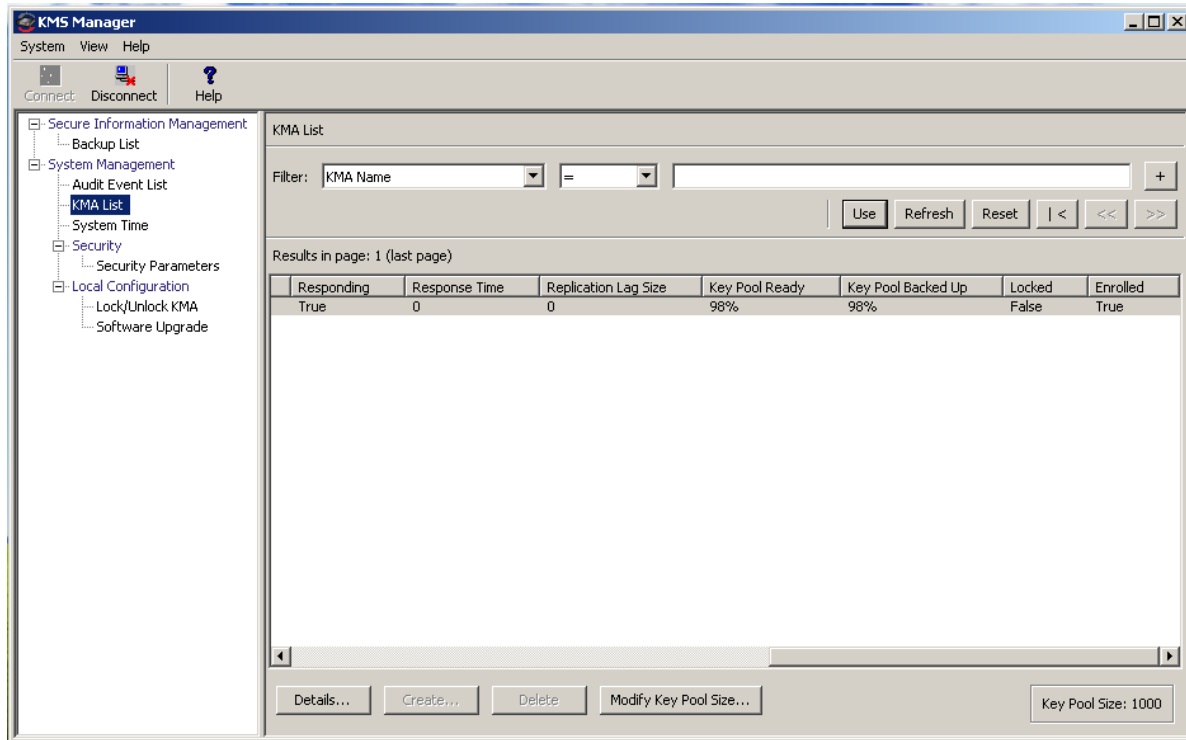
- View KMAs
- Create a KMA
- Modify a KMA's information
- Delete a KMA
- Modify a Key Pool size (refer to [“Modifying a Key Pool Size” on page 282](#)). This is a Backup Operator function.



## Viewing KMAs

To view KMAs:

From the System Management menu, select KMA List. The KMA List screen is displayed.



You can also scroll through the database and filter the KMA list by any of the following keys:

- KMA Name
- KMA ID
- Description
- Site ID
- Management Network Address
- Service Network Address
- Management Network Address (IPv6)
- Service Network Address (IPv6)
- Version

- Failed Login Attempts
- Responding
- Response Time
- Replication Lag Size
- Key Pool Ready
- Key Pool Backed Up
- Locked
- Enrolled.

The **Use** button applies the filter to the displayed list for the KMA.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA.  
Possible values are:

- KMA Name
- Description
- Site ID
- Management Network Address
- Service Network Address
- Management Network Address (IPv6)
- Service Network Address (IPv6)
- Version
- Failed Login Attempts
- Enrolled

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

**Filter Value 1 box:**

Type a value in this field.

**Use:**

Click this button to apply the filter to the displayed list.

**Refresh:**

Click this button to refresh the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

**KMA Name**

Displays the user-supplied identifier that distinguishes each KMA in a Cluster.

**KMA ID**

Displays a system-generated unique identifier that identifies the KMA.

**Description**

Describes the KMA.

**Site ID**

Describes the site to which the KMA belongs.

**Management Network Address**

Displays the IP address of the KMA on the management network.

**Service Network Address**

Displays the IP address of the KMA on the service network.

**Management Network Address (IPv6)**

Displays the IPv6 address (if any) of the KMA on the management network.

**Service Network Address (IPv6)**

Displays the IPv6 address (if any) of the KMA on the service network.

**Version**

Displays the version number of the KMA software.

**Failed Login Attempts**

Displays the number of times that an attempted logon has failed.

**Responding**

Indicates whether the KMA is running. Possible values are True or False.

**Response Time**

Displays the time (in milliseconds) that the KMA takes to respond to a request.



**Replication Lag Size**

Displays the number of updates waiting to be replicated.

**Key Pool Ready**

Displays the percentage of unallocated keys that are ready.

**Key Pool Backed Up**

Displays the percentage of the Key Pool that has been backed up.

**Locked**

Indicates whether or not the KMA is locked.

---

**Note** – The **Key Pool Backed Up** and **Locked** fields show an “N/A” value if that KMA does not support these features.

---

**Enrolled**

Indicates whether the KMA has been added or logged into the Cluster successfully. Possible values are True or False.

If you want to create a KMA, click the Create button. For more information, refer to [“Creating a KMA” on page 102](#) below.

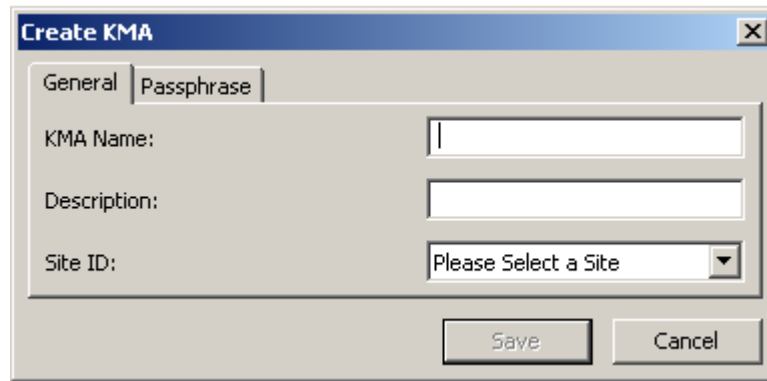
If you want to view / modify a KMA’s details, highlight the KMA and click the Details button. For more information, refer to [“Viewing/Modifying a KMA’s Details” on page 105](#).

If you want to delete a KMA, click the Delete button. For more information, refer to [“Deleting a KMA” on page 108](#).

## Creating a KMA

To create a KMA:

1. From the KMA List screen, click the Create button. The Create KMA dialog box is displayed, with the General tab active.



The image shows the 'Create KMA' dialog box with the 'General' tab selected. The dialog has a title bar with a close button. Inside, there are two tabs: 'General' and 'Passphrase'. The 'General' tab contains three input fields: 'KMA Name:' with a text box, 'Description:' with a text box, and 'Site ID:' with a dropdown menu showing 'Please Select a Site'. At the bottom right are 'Save' and 'Cancel' buttons.

2. Complete the following parameters:

### *General Tab*

#### **KMA Name**

Type a value that uniquely identifies the KMA in a Cluster. This value can be between 1 and 64 (inclusive) characters.

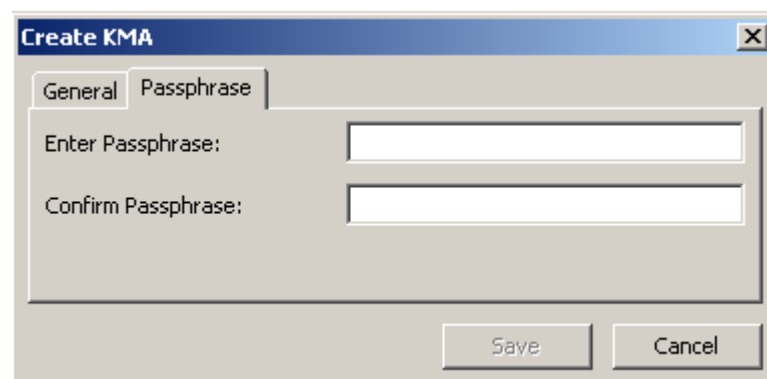
#### **Description**

Type a value that uniquely describes the KMA. This value can be between 1 and 64 (inclusive) characters.

#### **Site ID**

Click the down-arrow and select the site to which the KMA belongs. This field is optional.

3. Open the Passphrase tab.



The image shows the 'Create KMA' dialog box with the 'Passphrase' tab selected. The dialog has a title bar with a close button. Inside, there are two tabs: 'General' and 'Passphrase'. The 'Passphrase' tab contains two input fields: 'Enter Passphrase:' and 'Confirm Passphrase:'. At the bottom right are 'Save' and 'Cancel' buttons.

4. Complete the following parameters and click the Save button.

### Enter Passphrase

Type the passphrase for this user. The minimum value is 8 characters; the maximum value is 64 characters. The default value is 8.

Passphrase requirements:

- A passphrase must not contain the user's KMA Name.
- A passphrase must contain three of the four character classes: uppercase, lowercase, numeric, or special characters.

The following special characters are allowed:

' ~ ! @ # \$ % ^ & \* ( ) - \_ = + [ ] { } \ | ; : ' " < > , . / ?

- Control characters, including tabs and linefeeds, are not allowed.

---

**Note** – To modify the minimum length requirement for passphrases, see [“Modifying the Security Parameters” on page 172](#).

---

### Confirm Passphrase

Type the same value that you entered in the Enter Passphrase field.

5. The KMA record is added to the database and the entry is displayed in the KMA List screen.

The screenshot shows the 'KMA List' application window. At the top, there is a filter section with a dropdown menu set to 'KMA Name', an equals sign, and an empty text field. Below this are buttons for 'Use', 'Refresh', 'Reset', and navigation arrows. The main area displays a table with the following data:

| KMA Name   | KMA ID           | Description | Site ID | Management Network Address | Service Network Address | Version |
|------------|------------------|-------------|---------|----------------------------|-------------------------|---------|
| sudburykms | 372FC5113E67F069 |             |         | 129.80.60.163              | 129.80.60.163           | Build2  |

Overlaid on the table is a 'Create KMA' dialog box. It has two tabs: 'General' and 'Passphrase'. The 'General' tab is active, showing fields for 'KMA Name' (containing 'stkms'), 'Description' (empty), and 'Site ID' (a dropdown menu with 'Louisville' selected). At the bottom of the dialog are 'Save' and 'Cancel' buttons.

6. You must now run the QuickStart program on the KMA(s) you created so that they can join the Cluster. For procedures on joining a Cluster, refer to ["Joining an Existing Cluster" on page 40.](#)

## Viewing/Modifying a KMA's Details

**Note** – If you are not a Security Officer, when you view a KMA's detailed information, all fields, including the Save button are disabled.

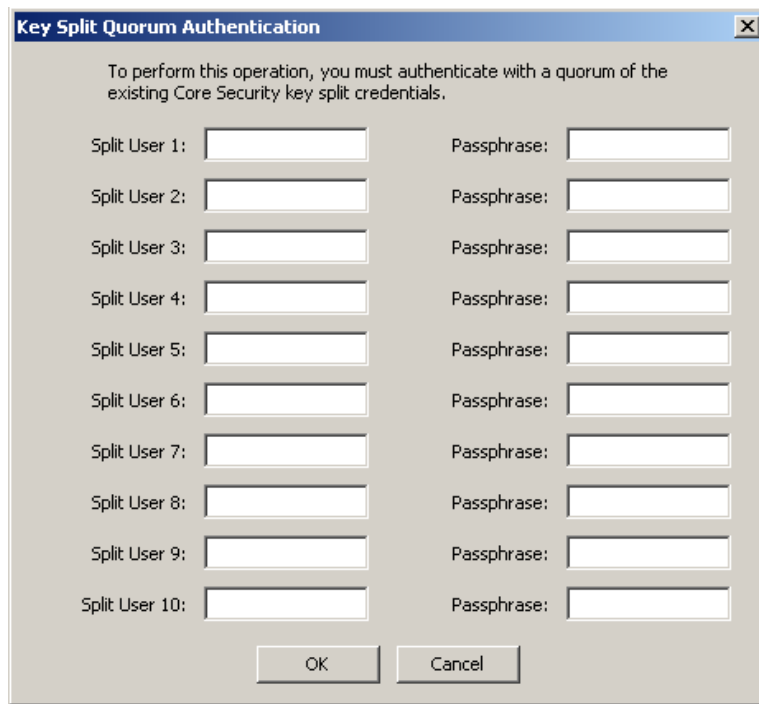
To modify a KMA's details:

1. From the KMAs List screen, double-click a KMA entry for which you want more detailed information or highlight a KMA entry and click the Details button. The KMA Details dialog box is displayed.

| KMA Details                        |                                    |
|------------------------------------|------------------------------------|
| General   Passphrase               |                                    |
| KMA ID:                            | 7E32B6D5206539EB                   |
| KMA Name:                          | glenkinchiekma                     |
| Description:                       |                                    |
| Site ID:                           |                                    |
| Management Network Address:        | 10.80.180.39                       |
| Service Network Address:           | 192.168.1.39                       |
| Management Network Address (IPv6): | 2007::abcd:abcd:efff:216:36ff:feca |
| Service Network Address (IPv6):    | 2006::216:36ff:feca:15b9/64        |
| Version:                           | 2.1 (Build482)                     |
| Failed Login Attempts:             | 0                                  |
| Responding:                        | True                               |
| Response Time:                     | 0 milliseconds                     |
| Replication Lag Size:              | 0                                  |
| Ready Keys:                        | 1001                               |
| Backed-up Ready Keys:              | 1001                               |
| Generated Keys:                    | 0                                  |
| Key Pool Ready:                    | 100 %                              |
| Key Pool Backed Up:                | 100 %                              |
| Locked:                            | False                              |
| Enrolled:                          | True                               |
| <div>Save Cancel</div>             |                                    |

2. On the General tab, change the following fields:
  - Description
  - Site ID.
3. Open the Passphrase tab and modify the following parameters:
  - Passphrase
  - Confirm Passphrase (retype the same passphrase).
4. When you are finished, click the Save button. The KMA record in the database is modified.

5. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



The dialog box is titled "Key Split Quorum Authentication" and contains the following text: "To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials." Below this text are ten rows of input fields. Each row consists of a label (Split User 1 through Split User 10), a text box for the user name, a label (Passphrase:), and a text box for the passphrase. At the bottom of the dialog box are two buttons: "OK" and "Cancel".

| Split User     | Passphrase |
|----------------|------------|
| Split User 1:  |            |
| Split User 2:  |            |
| Split User 3:  |            |
| Split User 4:  |            |
| Split User 5:  |            |
| Split User 6:  |            |
| Split User 7:  |            |
| Split User 8:  |            |
| Split User 9:  |            |
| Split User 10: |            |

OK Cancel

6. Choosing the OK button after the last user name and passphrase is entered, sends the user names and passphrases to the KMA for authentication.
7. If the authentication is successful, the Key Split Quorum Authentication dialog box closes.

## Setting a KMA Passphrase

---

**Note** – You can change a KMA's passphrase, provided you are not connected to it.

---

When you are creating a new Cluster, a random passphrase is automatically assigned to the KMA that is used to create the new Cluster. If the KMA wants to retrieve an entity's certificate from another KMA in the Cluster because its certificate has expired, then you would have to use this function to set the passphrase to a known value.

To set a KMA's passphrase:

1. From the KMA List screen, double-click the KMA entry or highlight a KMA entry and click the Details button. The KMA Details dialog box is displayed, with the General tab active.
2. Open the Passphrase tab and modify the following parameters:
  - Passphrase
  - Confirm Passphrase (retype the same passphrase).
3. Click the Save button to save the changes. The database entry for the KMA is changed.
4. Using the Console, on the KMA where the passphrase has been changed, select the function to log the KMA into the Cluster. The KMA is not able to communicate with the Cluster until it is logged back in.

## Deleting a KMA

---

**Important** – Before you delete a KMA, you should take it off-line using the Console “Shutdown KMA” function. If you fail to do this, the KMA will continue to function outside of the Cluster, and send “stale information” to Agents and users.

Normally, this command will only be used to delete a failed KMA from the Cluster. However, it may also be used to remove a KMA that is being decommissioned. However, in that case, using the Console “Reset KMA” function with the zeroize option is a better choice. This function deletes the KMA from the Cluster and wipes all information from the disk of the KMA that is being decommissioned.

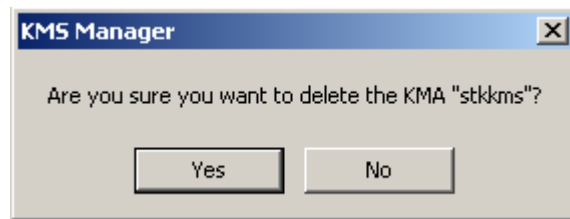
If you want a deleted KMA to rejoin a Cluster, you must reset the KMA to the factory default and select option 2 from the QuickStart program.

---

This option gives the Security Officer the ability to delete a KMA that is no longer in service.

To delete a KMA:

1. From the KMAs List screen, highlight the KMA you want to delete and click the Delete button. The following dialog box is displayed, prompting you to confirm that you want to delete the selected KMA.



2. Click the Yes button to delete the KMA. The currently selected KMA is deleted and you are returned to the KMAs List screen. The system also removes any entries that are associated with the KMA and not used by any other entity.

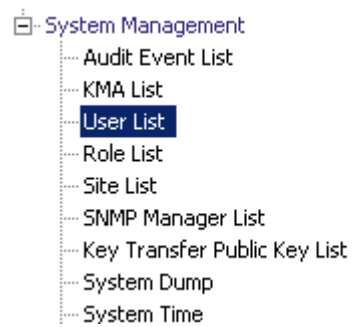


---

## User List Menu

The User List menu option allows you to:

- View users
- Create a user
- Modify existing user information
- Delete an existing user



## Viewing Users

To view users:

From the System Management menu, select **User List**. The User List screen is displayed.

User List

Filter: User ID =  +

Use Refresh Reset | < << >>

Results in page: 8 (last page)

| User ID | Description         | Roles  | Enabled | Failed Login Attempts |
|---------|---------------------|--|---------|-----------------------|
| AUD     | Test User           | Auditor  | True    | 0                     |
| All     | Test User           | Backup Operator, Compliance Officer, Operator, Security... | True    | 0                     |
| BO      | test User           | Backup Operator  | True    | 0                     |
| CO      | Test User           | Compliance Officer   | True    | 0                     |
| OP      | Test User           | Operator   | True    | 0                     |
| SO      |                     | Backup Operator, Compliance Officer, Operator, Security... | True    | 0                     |
| nancy   |                     | Auditor  | True    | 0                     |
| wally   | night shift janitor | Security Officer   | True    | 0                     |

Details... Create... Delete

You can also scroll through the database and filter the User list by any of the following keys:

- User ID
- Description
- Roles
- Enabled
- Failed Login Attempts.

The **Use** button applies the filter to the displayed list for the User.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA.

Possible values are:

- User ID
- Description
- Enabled
- Failed Login Attempts

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not Empty

**Filter Value 1 box:**

Type a value in this field.

**Use:**

Click this button to apply the filter to the displayed list.

**Refresh:**

Click this button to refresh the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

**User ID**

Displays a unique identifier, commonly referred to as “User Name” that distinguishes each user in a Cluster.

**Description**

Describes the user.

**Roles**

Displays the list of security roles for a user. The roles allow the user to perform various operations.

**Enabled**

Indicates the status of the user. Possible values are **True** or **False**.

**Failed Login Attempts**

Indicates the number of failed login attempts.

If you want to create a user, click the Create button. For more information, refer to [“Creating a User” on page 113](#).

If you want to modify a user’s details, highlight the user and click the Details button. For more information, refer to [“Viewing/Modifying a User’s Details” on page 115](#).

If you want to delete a user, click the Delete button. For more information, refer to [“Deleting Users” on page 119](#).

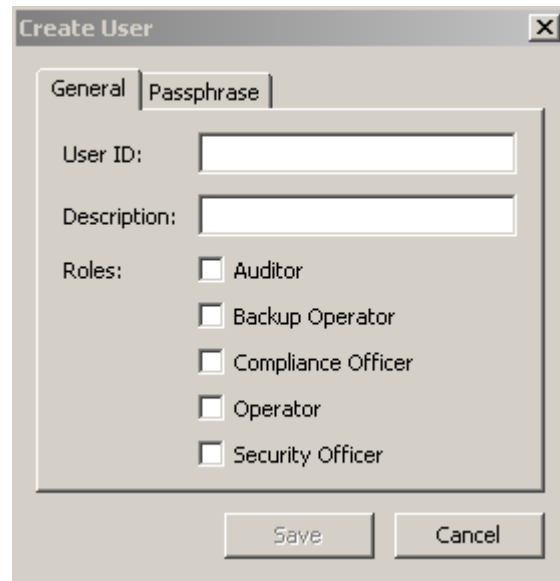
A Security Officer can set a user’s passphrase if the user’s passphrase and/or certificate has been compromised. For procedures on setting a user’s passphrase, refer to [“Setting a User’s Passphrase” on page 117](#).

Users can also change their own passphrase. For procedures, refer to [“Changing the Passphrase” on page 90](#).

## Creating a User

To create a user:

1. From the User List screen, click the Create button. The Create User dialog box is displayed, with the General tab open.

The image shows a 'Create User' dialog box with a title bar containing a close button (X). It has two tabs: 'General' and 'Passphrase'. The 'General' tab is active and contains the following fields and options:

- 'User ID:' followed by a text input field.
- 'Description:' followed by a text input field.
- 'Roles:' followed by a list of five roles, each with an unchecked checkbox:
  - Auditor
  - Backup Operator
  - Compliance Officer
  - Operator
  - Security Officer

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

2. Complete the following parameters:

### *General Tab*

#### **User ID**

Type a value that uniquely identifies the user. This value can be between 1 and 64 (inclusive) characters.

#### **Description**

Type a value that describes the user. This value can be between 1 and 64 (inclusive) characters.

#### **Roles**

Select the check boxes beside the roles you want the user to perform.

*Passphrase Tab*

3. Open the Passphrase tab.

4. Complete the following parameters:

**Passphrase**

Type the passphrase for this user. The minimum value is 8 characters; the maximum value is 64 characters. The default value is 8.

Passphrase requirements:

- A passphrase must not contain the user's User ID.
- A passphrase must contain three of the four character classes: uppercase, lowercase, numeric, or special characters.

The following special characters are allowed:

' ~ ! @ # \$ % ^ & \* ( ) - \_ = + [ ] { } \ | ; : ' " < > , . / ?

- Control characters, including tabs and linefeeds, are not allowed.

---

**Note** – To modify the minimum length requirement for passphrases, see [“Modifying the Security Parameters” on page 172](#).

---

**Confirm Passphrase**

Type the same value that you entered in the Enter Passphrase field.

5. Click the Save button. The user record is added to the database. The new user is displayed in the User List.

## Viewing/Modifying a User's Details

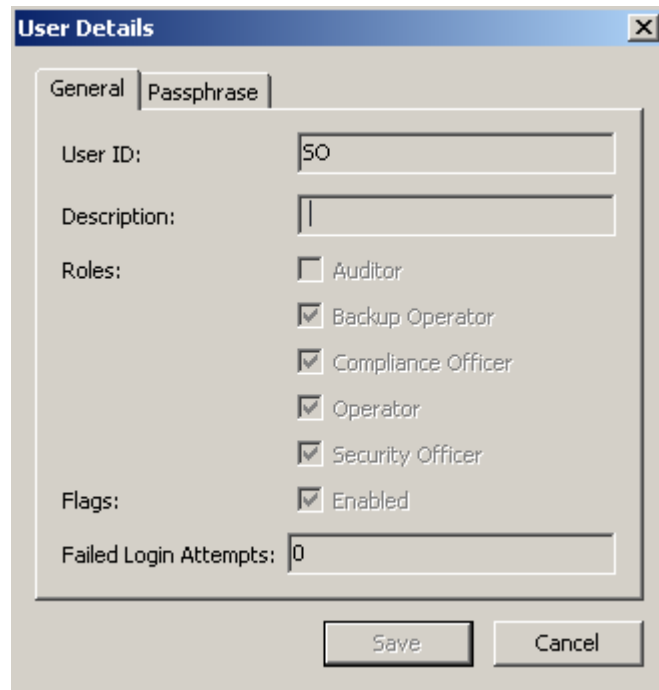
---

**Note** – The currently logged-in Security Officers cannot modify their records.

---

To modify user information:

1. From the Users List screen, double-click a user for which you want more information or highlight a user record and click the Details button. The User Details dialog box is displayed, where all fields, including the Save button are disabled.



The image shows a 'User Details' dialog box with two tabs: 'General' and 'Passphrase'. The 'General' tab is active. It contains the following fields and options:

- User ID: A text box containing 'SO'.
- Description: A text box.
- Roles: A list of roles with checkboxes:
  - ☐ Auditor
  - ☒ Backup Operator
  - ☒ Compliance Officer
  - ☒ Operator
  - ☒ Security Officer
- Flags: A list of flags with checkboxes:
  - ☒ Enabled
- Failed Login Attempts: A text box containing '0'.

At the bottom of the dialog box are two buttons: 'Save' and 'Cancel'.

2. On the General tab, modify the following parameters:

- User ID
- Description
- Roles
- Flags - Enabled
- Failed Login Attempts.

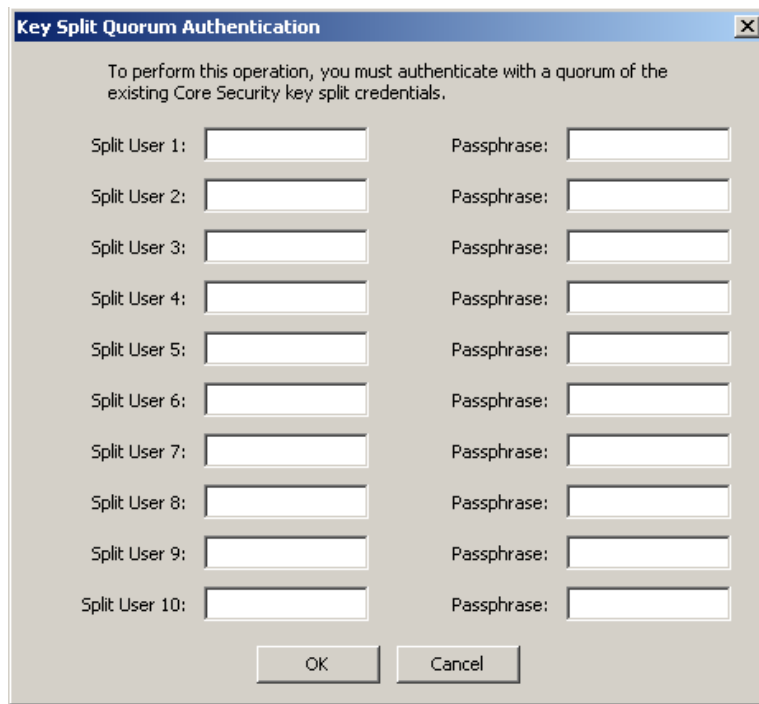
The Failed Login Attempts field displays the number of times that a login attempt has failed.

3. Open the Passphrase tab and modify the following parameters:

- Passphrase
- Confirm Passphrase.

4. When you are finished, click the Save button. The user record in the database is modified.

5. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



The dialog box is titled "Key Split Quorum Authentication" and contains the following text: "To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials." Below this text are ten rows of input fields. Each row consists of a label (e.g., "Split User 1:", "Split User 2:", ..., "Split User 10:") followed by a text box, and then the label "Passphrase:" followed by another text box. At the bottom of the dialog box are two buttons: "OK" and "Cancel".

| User Label     | User Input           | Passphrase Input                 |
|----------------|----------------------|----------------------------------|
| Split User 1:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 2:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 3:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 4:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 5:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 6:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 7:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 8:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 9:  | <input type="text"/> | Passphrase: <input type="text"/> |
| Split User 10: | <input type="text"/> | Passphrase: <input type="text"/> |

OK Cancel

Choosing the OK button after the last user name and passphrase is entered, sends the user names and passphrases to the KMA for authentication.

If the authentication is successful, the Key Split Quorum Authentication dialog box closes.

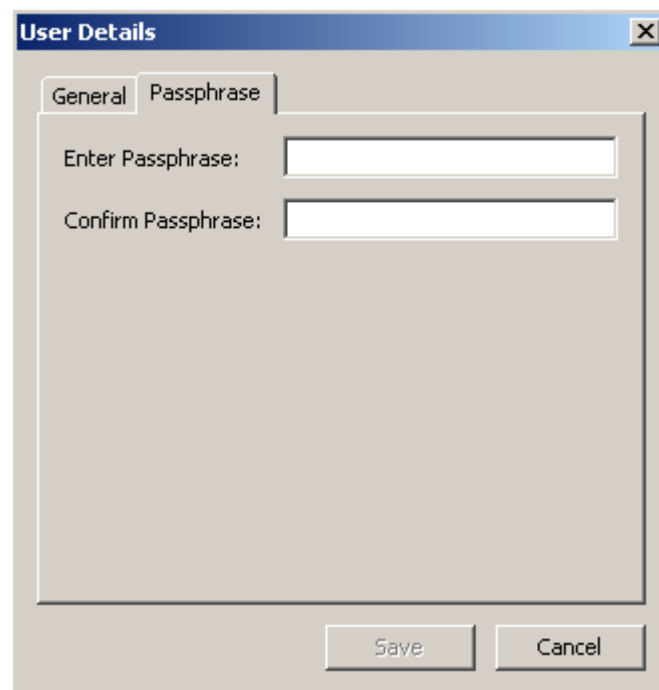


## Setting a User's Passphrase

As the Security Officer, you can set a user's passphrase if you believe that the user's passphrase and/or certificate has been compromised. A new certificate is generated when the user uses the new passphrase to logon to the KMA.

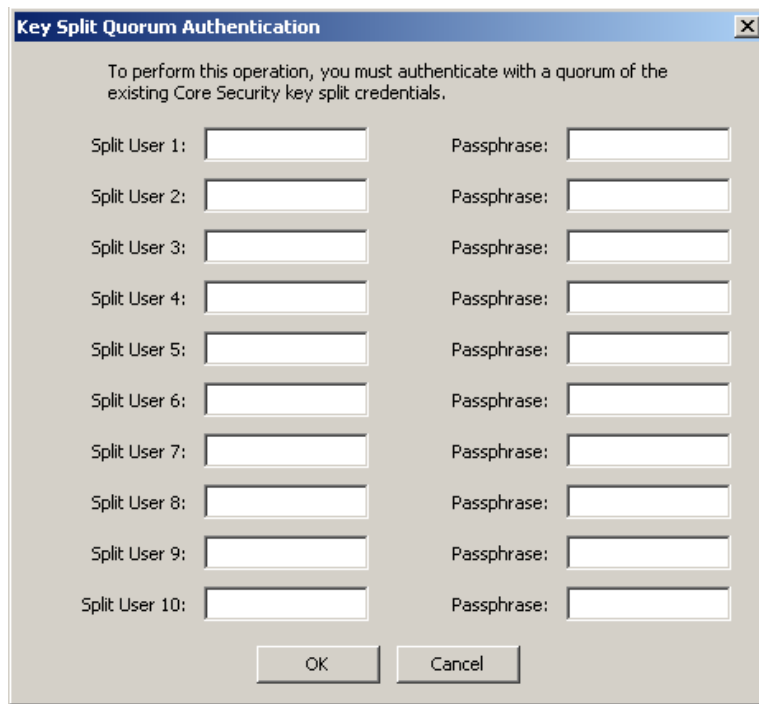
To set a user's passphrase:

1. From the User List screen, double-click the user whose passphrase you want to select or highlight the user and click the Details button.
2. The User Details dialog box is displayed. Open the Passphrase tab.

The image shows a 'User Details' dialog box with a blue title bar and a close button (X) in the top right corner. Inside the dialog, there are two tabs: 'General' and 'Passphrase'. The 'Passphrase' tab is currently selected. Below the tabs, there are two text input fields. The first field is labeled 'Enter Passphrase:' and the second field is labeled 'Confirm Passphrase:'. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

3. In the Enter Passphrase field, type the passphrase that was assigned by the Security Officer when the user account was created.
4. In the Confirm Passphrase field, type the same value you entered in [Step 3](#). The new passphrase for the user record is saved.

5. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



The dialog box is titled "Key Split Quorum Authentication" and contains the following text: "To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials." Below this text are ten rows of input fields. Each row consists of a label (e.g., "Split User 1:", "Split User 2:", ..., "Split User 10:") followed by a text box, and then the label "Passphrase:" followed by another text box. At the bottom of the dialog box are two buttons: "OK" and "Cancel".

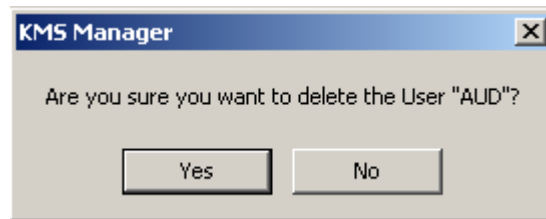
6. Choosing the OK button after the last user name and passphrase is entered, sends the user names and passphrases to the KMA for authentication.
7. If the authentication is successful, the Key Split Quorum Authentication dialog box closes.

## Deleting Users

Users cannot delete themselves.

To delete a user:

1. From the Users List screen, select the user you want to delete and click the Delete button. The following dialog box is displayed, prompting you to confirm that you want to delete the selected user.



2. Click the Yes button to delete the user. The currently selected user is deleted and you are returned to the User List screen, where the deleted user is no longer in the User List.

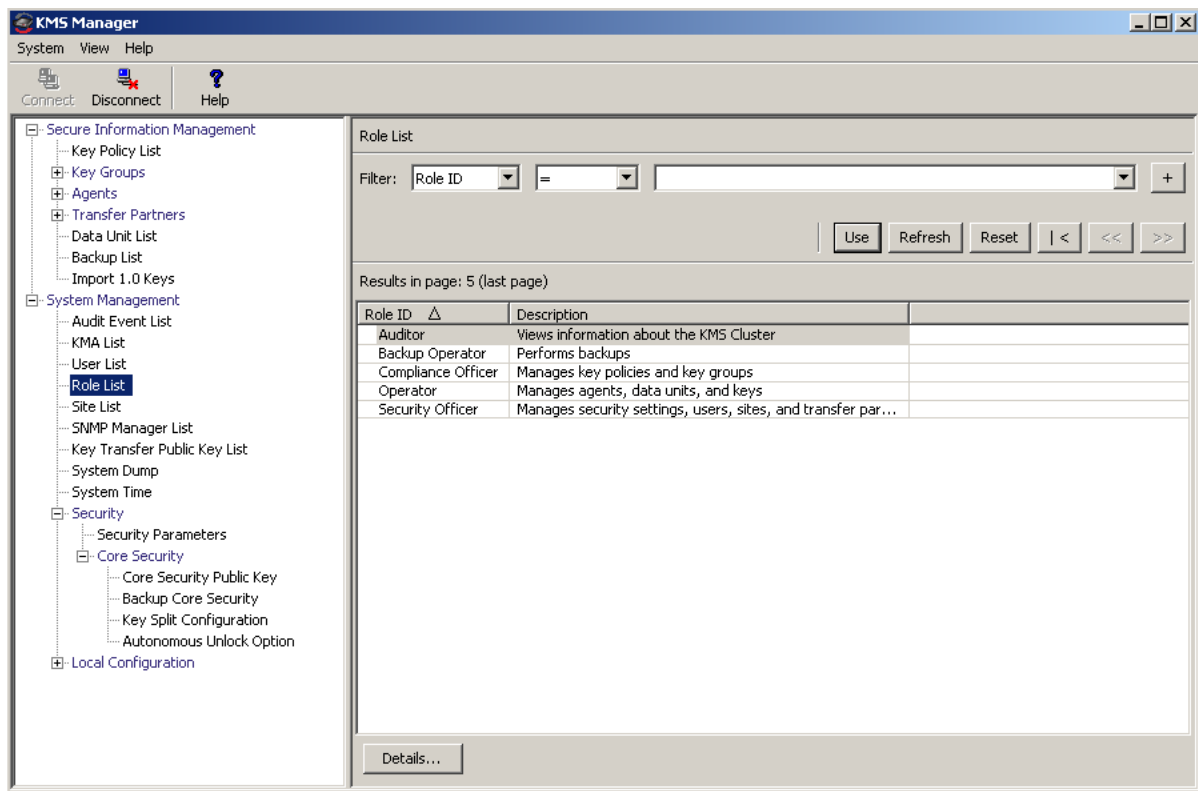
# Role List Menu

The Role List menu option allows gives you the ability to view user roles. Roles are fixed logical groupings of various system operations that a user can perform. A user can have more than one role.

## Viewing Roles

To view roles:

From the System Management menu, select **Role List**. The Role List screen is displayed.



You can also scroll through the database and filter the Roles list by either of the following keys:

- Role ID
- Description.

The **Use** button applies the filter to the displayed list.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA.  
Possible values are:

- Role ID
- Description

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Empty
- Not Empty

**Filter Value 1 box:**

Type a value in this field.

**Refresh:**

Click this button to refresh the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

**Role ID**

Displays the unique identifier that distinguishes each security role.

**Description**

Describes the role.

If you want more detailed information on a role, highlight a role entry and click the Details button. For more information, refer to [“Viewing Operations for a Role” on page 122](#).

## Viewing Operations for a Role

The Role Operations dialog box allows the you to view a role and its permitted operations.

To view the operations for a specific role:

1. From the Role List screen, highlight a role and click the Details button. The Role Operations dialog box is displayed, indicating the operations for the selected role.



2. Click the Close button to close this dialog box. You are returned to the Role List screen.

## Site List Menu

A Site is a physical location with at least one KMA, to which several Agents (Hosts and KMS Cluster) connect. Sites allows Agents to respond to KMA failures or load balancing more effectively by connecting to another KMA in the local Site rather than a remote one

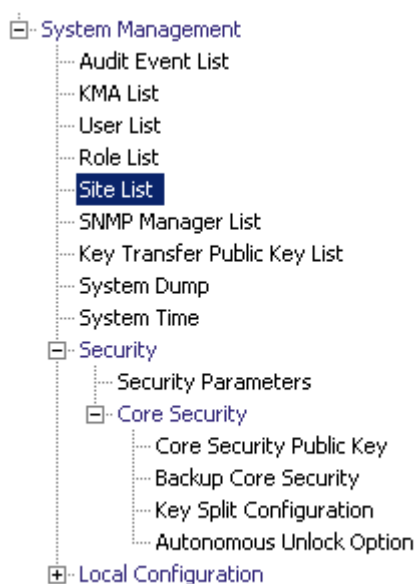
The Site List menu option gives you the ability to:

- View sites
- Create a site
- Modify an site's information
- Delete a site.

---

**Note** – An Operator can view sites only. A Security Officer can manage the sites.

---



## Viewing Sites

To view sites:

From the System Management menu, select Site List. The Site List screen is displayed.

Site List

Filter: Site ID =  +

Use Refresh Reset | < << >> >

Results in page: 4 (last page)

| Site ID    | Description               |
|------------|---------------------------|
| LaBarge    | This is a site in Wyoming |
| Louisville | another site              |
| Sitenumba1 | This is a site            |
| Toronto    | Yada is a site            |

Details... Create... Delete

You can also scroll through the database and filter the Sites list by any of the following keys:

- Site ID
- Description.

The **Use** button applies the filter to the displayed list for the Site.

The fields and their descriptions are given below:

### Filter:

Displays the fields that you can use to filter the results of queries made to the KMA.  
Possible values are:

- Site ID
- Description



**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~

**Filter Value 1 box:**

Type a value in this field.

**Use:**

Click this button to apply the filter to the displayed list.

**Refresh:**

Click this button to refresh the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

**Site ID**

Uniquely identifies the site.

**Description**

Describes the site.

Click the Create button to create a Site. For more information, refer to [“Creating a Site” on page 127](#).

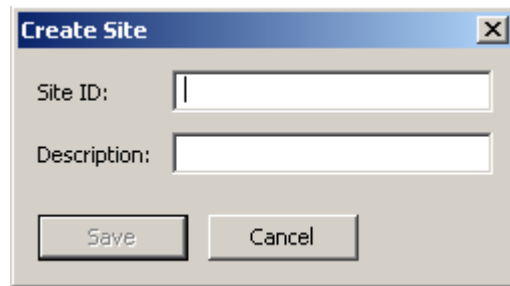
If you want to view / modify a Site’s detailed information, highlight the Site and click the Details button. For more information, refer to [“Viewing/Modifying a Site’s Details” on page 129](#).

Click the Delete button to delete a selected Site. For more information, refer to [“Deleting a Site” on page 130](#).

## Creating a Site

To create a site:

1. From the Site List screen, click the Create button. The Create Site dialog box is displayed.

A screenshot of the 'Create Site' dialog box. It has a title bar with 'Create Site' and a close button. Inside, there are two text input fields: 'Site ID:' and 'Description:'. Below the fields are two buttons: 'Save' and 'Cancel'.

2. Complete the following parameters:

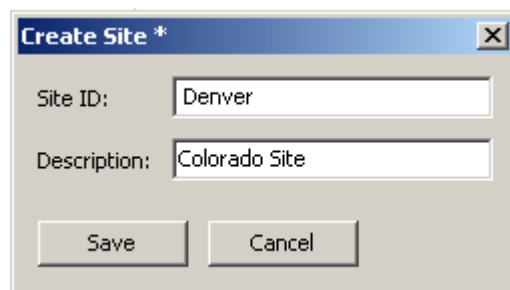
### Site ID

Type a value that uniquely identifies the site. This value can be between 1 and 64 (inclusive) characters.

### Description

Type a value that uniquely describes the site. This value can be between 1 and 64 (inclusive) characters.

An example of a completed dialog box is shown below.

A screenshot of the 'Create Site' dialog box with example data. The title bar says 'Create Site \*'. The 'Site ID:' field contains the text 'Denver'. The 'Description:' field contains the text 'Colorado Site'. The 'Save' and 'Cancel' buttons are at the bottom.

3. Click the Save button. The new Site is saved and stored in the database and is displayed in the Site List.

Site List

Filter:

Site ID

=

+

Use

Refresh

Reset

| <

<<

>>

Results in page: 5 (last page)

| Site ID    | Description               |
|------------|---------------------------|
| Denver     | Colorado Site             |
| LaBarge    | This is a site in Wyoming |
| Louisville | another site              |
| Sitenumba1 | This is a site            |
| Toronto    | Yada is a site            |

Details...

Create...

Delete

## Viewing/Modifying a Site's Details

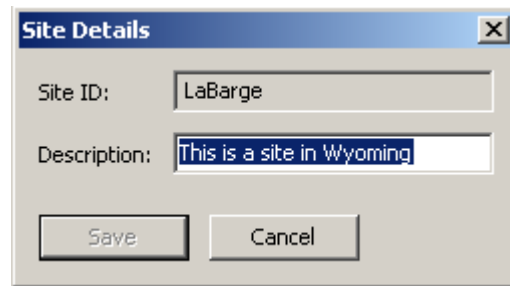
---

**Note** – If you are not a Security Officer, when you view a site's detailed information, all fields, including the Save button are disabled.

---

To modify a Site's details:

1. From the Site List screen, click the Details button. The Site Details dialog box is displayed.



2. Change the Description field and click the Save button. The Site details are modified and stored in the database.

## Deleting a Site

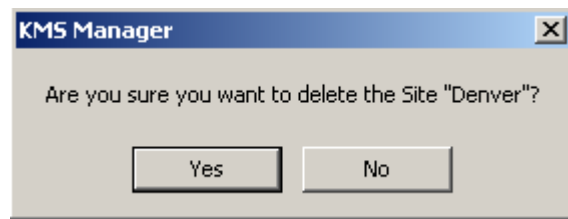
---

**Note** – If the site is in use, that is, agents or KMAs are specified to be at the site, they must first be deleted or changed to a different site before you can delete it.

---

To delete a site:

1. From the Site List screen, highlight the Site you want to delete and click the Delete button. The following dialog box is displayed, prompting you to confirm your actions.



2. Click the Yes button to delete the Site. The currently selected Site is deleted and you are returned to the Site List screen.

# SNMP Manager List Menu

The following menus discuss viewing, creating, and modifying SNMP Managers.

Additionally, SNMP information is generated for users who have configured an SNMP Agent in their network and defined SNMP Managers in the KMS Manager GUI. When at least one SNMP Manager is defined in the KMS Manager GUI, the KMAs will send SNMP Informs to the IP address of that SNMP Manager(s).

Refer to [“SNMP Management Information Base \(MIB\) Data” on page 323](#) for more details about the information that KMAs send in their SNMP Inform packets.

## Viewing a KMA’s SNMP Managers

To view the SNMP Managers:

From the System Management menu, select SNMP Manager List. The SNMP Manager List screen is displayed.

SNMP Manager List

Filter: SNMP Manager ID =

Use

Refresh

Reset

| <

<<

>>

Results in page: 0 (last page)

| SNMP Manager ID | Description | Network Address | Enabled | User Name |
|-----------------|-------------|-----------------|---------|-----------|
|-----------------|-------------|-----------------|---------|-----------|

Details...

Create...

Delete

You can also scroll through the database and filter the SNMP Manager List by any of the following keys:

- SNMP Manager ID
- Description
- Network Address
- Enabled
- User Name.

The **Use** button applies the filter to the displayed list for the SNMP Manager.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA.  
Possible values are:

- SNMP Manager ID
- Description
- Network Address
- Enabled
- User Name.

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

**Filter Value 1 box:**

Type a value in this field.

**Use:**

Click this button to apply the filter to the displayed list.

**Refresh:**

Click this button to refresh the list.



**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

**SNMP Manager ID**

Displays the user-defined unique identifier for the SNMP Manager.

**Description**

Displays a description for the SNMP Manager. This field is optional.

**Network Address**

Displays the network address that will be used when sending an SNMP trap.

**Enabled**

Indicates whether this SNMP Manager is enabled or not.

**User Name**

Displays the user name that was used to establish a secure, trusted SNMPv3 connection to this SNMP Manager.

Click the Create button to create a new SNMP Manager. For more information, refer to [“Creating a New SNMP Manager”](#) below.

If you want to view/modify a SNMP Manager detailed information, highlight the entry and click the Details button. For more information, refer to [“Viewing/Modifying an SNMP Manager’s Details”](#) on page 136.

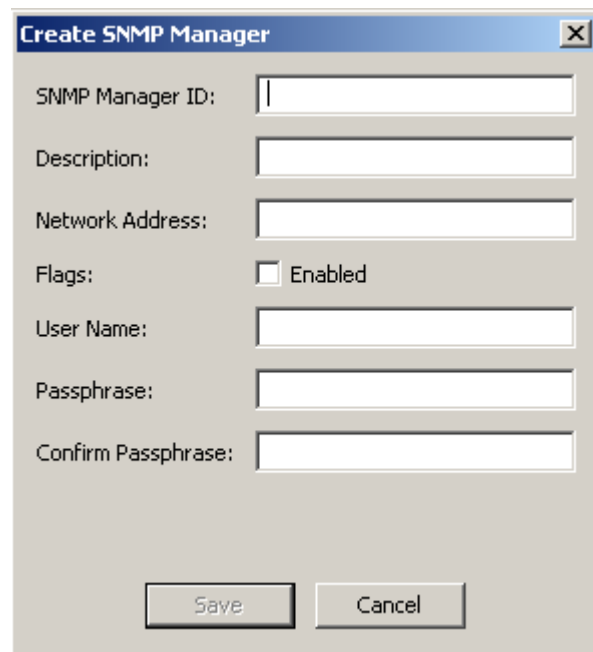
Click the Delete button to delete the selected SNMP Manager. For more information, refer to [“Deleting an SNMP Manager”](#) on page 137.

## Creating a New SNMP Manager

**Note** – Before you can create an SNMP manager, you must ensure that you use SNMP protocol Version 3 and SHA (not MD5) as the authentication protocol. Refer to your SNMP Agent documentation for more information about creating SNMP Version 3 users.

Also, if the SNMP user has a passphrase, then the KMA uses this passphrase for both the Authentication Passphrase and the Encryption Passphrase for that SNMP user. Thus, these passphrases must have the same value for this SNMP user in the SNMP Agent. If the SNMP user does not have a passphrase, then the KMA uses a security level of “noAuthNoPriv” when it sends SNMP informs to the SNMP Agent.

1. From the SNMP Managers List screen, click the Create button.  
The Create SNMP Manager dialog box is displayed.

A screenshot of the 'Create SNMP Manager' dialog box. The dialog has a title bar with the text 'Create SNMP Manager' and a close button (X). Inside the dialog, there are several input fields: 'SNMP Manager ID:' with a text box, 'Description:' with a text box, 'Network Address:' with a text box, 'Flags:' with a checkbox labeled 'Enabled', 'User Name:' with a text box, 'Passphrase:' with a text box, and 'Confirm Passphrase:' with a text box. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

2. Complete the following parameters:

### SNMP Manager ID

Type a value that uniquely identifies the SNMP Manager. This value can be between 1 and 64 (inclusive) characters.

### Description

Type a value that describes the SNMP Manager. This value can be between 1 and 64 (inclusive) characters.

### Network Address

Type the SNMP Manager's network address.

**Flags - Enabled**

Select this check box to indicate whether SNMP is enabled or not.

**User Name**

Type the user name that will be used to authenticate the SNMP Manager.

**Passphrase**

Type the passphrase that will be used to authenticate the SNMP Manager.

**Confirm Passphrase**

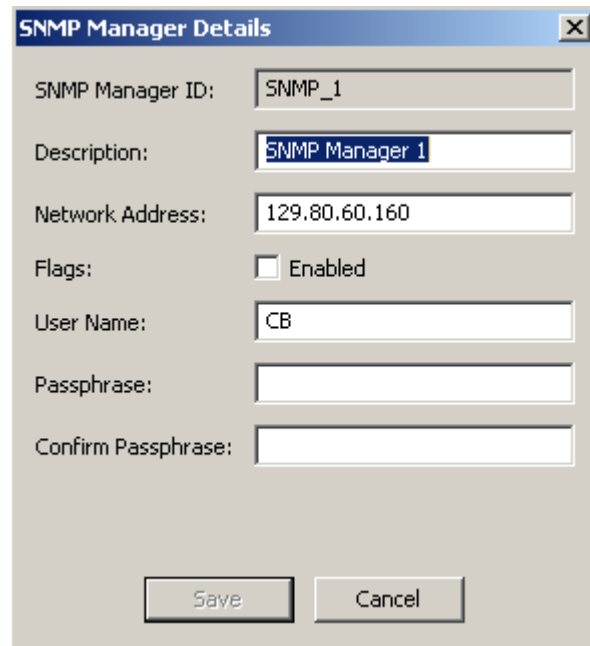
Type the same passphrase that was entered in the Passphrase field.

3. When you are finished, click the Save button to save the information. The new SNMP Manager entry and its associated profile is stored in the database.

## Viewing/Modifying an SNMP Manager's Details

To view/modify an SNMP Manager's details:

1. From the SNMP Managers List screen, double-click an SNMP Manager entry for which you want more information and click the Details button. The SNMP Manager Details dialog box is displayed.



The image shows a dialog box titled "SNMP Manager Details" with a close button (X) in the top right corner. The dialog box contains several input fields and a checkbox. The fields are labeled as follows:

- SNMP Manager ID:
- Description:
- Network Address:
- Flags: ☐ Enabled
- User Name:
- Passphrase:
- Confirm Passphrase:

At the bottom of the dialog box, there are two buttons: "Save" and "Cancel".

2. Change the parameters, as required.
3. When you are finished, click the Save button to save the changes.

---

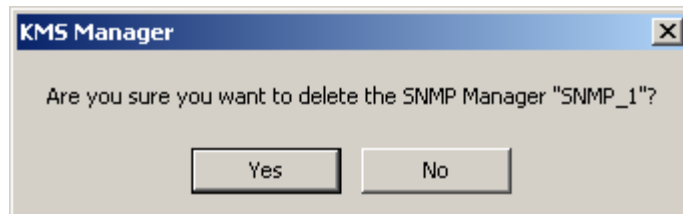
**Note** – Every time you modify a SNMP Manager's details, you have to re-specify the passphrase.

---

## Deleting an SNMP Manager

To delete an SNMP Manager:

1. From the SNMP Managers List screen, highlight the SNMP Manager you want to delete and click the Delete button. The SNMP Manager Confirm Delete dialog box is displayed.



2. Click the Yes button to delete the SNMP Manager. The currently selected SNMP Manager is deleted and you are returned to the SNMP Managers List screen.

---

# Key Transfer

## Overview

Key Transfer, also called Key Sharing, allows keys and associated data units to be securely exchanged between Partners and is required to exchange encrypted media. This process requires each party in the transfer establish a public/private key pair and then provide the public key to the other party.

Each party enters the other party's public key into their own KMS Cluster. Once this initial configuration is complete, the sending party uses Export Keys to generate a transfer file, which is sent from the sending party to the receiving party. The receiving party then uses Import Keys to import the keys and their associated data units into their KMS Cluster.

The transfer file is signed using the sending party's private key and encrypted using the receiving party's public key. This allows only the receiving party to decrypt the transfer file using their own private key. The receiving party can verify the file was in fact produced by the expected sender by using the sender's public key.

## Key Transfer Partners Feature

The Key Transfer Partners feature allows keys to be moved from one KMS Cluster to another. Typically, this feature can be used to exchange tapes between companies or within a company if multiple Clusters are configured to deal with large numbers of sites.

The Key Transfer process involves these steps:

- Each KMS Cluster configures the other Cluster as a Transfer Partner. This is usually done once.
- The user exports keys from one KMS Cluster and imports them into the other. This step can be done many times.

# Key Transfer Process

Within the KMS, you must perform a number of tasks in a specific order. Since these tasks involve more than one user role, the actual procedures reside in different chapters in this document.

## Configuring Key Transfer Partners

To move keys, you must configure a Key Transfer Partner for both KMS Clusters participating in key movement.

**In the following procedure, “C1” refers to the first KMS Cluster, “C2” to the second.**

### C1 Administrator (Security Officer role):

1. Acquire the Public Key information for C1 (your Cluster). To do this, go to the Key Transfer Public Key List Menu. See [“Viewing the Key Transfer Public Key List” on page 154](#) and [“Viewing the Key Transfer Public Key Details” on page 157](#).
2. Cut and paste the Public Key ID and Public Key into an e-mail or other agreed-upon form of communication. Send this information to the C2 administrator.

---

**Note** – The exact communication method should be sufficiently secure that when C2 receives the information, it can be confident it actually came from C1. There is a mechanism, the fingerprint, to prevent modification of this information in transit.

---

### C2 Administrator (Security Officer role):

3. C2 Administrator: Enter the Public Key information from C1 into the KMS Cluster by accessing the Transfer Partner List menu. See [“Transfer Partner List Menu” on page 143](#).
4. Click the Create... button. Fill in a name for the Transfer Partner, a description, and contact information. Determine what you want to do with this Partner. See [“Creating a Transfer Partner” on page 147](#).
5. Select the Public Keys tab. Fill in the Public Key ID and Public Key from the information supplied by C1.

As the Public Key is entered, the system will compute the fingerprint. The C1 and C2 administrators should be communicating with each other using a different mechanism than was used for the transfer of the key itself.

Both administrators should look at their KMS and verify the fingerprint matches. A mismatch indicates the key has been damaged or modified during the transfer.

6. If the fingerprint is correct, click Save. The system will prompt for a quorum. This is because the key export operations that are enabled by this step could be used to extract valid keys from a KMS Cluster. C1 is now configured as a Transfer Partner in the C2 KMS Cluster.

**C2 Administrator (Security Officer role):**

7. Repeat [Step 1](#) and [Step 2](#), this time for the C2 KMS Cluster.


**C1 Administrator (Security Officer role):**

8. Repeat [Step 3](#) through [Step 6](#) to add C2's Public Key to C1.

**C1 Administrator (Compliance Officer Role):**

9. C1 must configure Key Groups that can be sent to C2. See ["Viewing Key Group Assignments" on page 226](#).

**C2 Administrator (Compliance Officer Role):**

10. C2 must configure Key Groups that can receive keys from C1. See ["Viewing Key Group Assignments" on page 226](#).
11. Select the desired Transfer Partner.
12. Select one or more disallowed Key Groups, and click the Move to  button to add them to the Key Group list. See ["Adding a Key Group to a Transfer Partner" on page 227](#).



## Exporting/Importing Keys

The next procedure is used to export keys from one KMS Cluster and import them into another. This can be done many times.

**In the following procedure, “C1” refers to the first KMS Cluster, “C2” to the second. These instructions are written to allow C2 to export keys that are then imported into C1.**

### **C2 Administrator (Operator Role):**

1. To exchange keys, go to the Data Unit List screen. See [“Viewing Data Units” on page 259](#).
2. Select one or more Data Units (tapes) to be sent from C2 to C1. The External Tag is the barcode on the tapes.
3. Click the Export Keys button to display the dialog box.
4. Select the destination Transfer Partner, select the Export Keys file name if necessary, and click Start. The Transfer File will be created.  
Only the Keys belonging to the Key Groups that are allowed to be exported to C1 are exported.
5. Send the Transfer File to the C1 administrator by email or another agreed-upon form of communication or mechanism to move files.

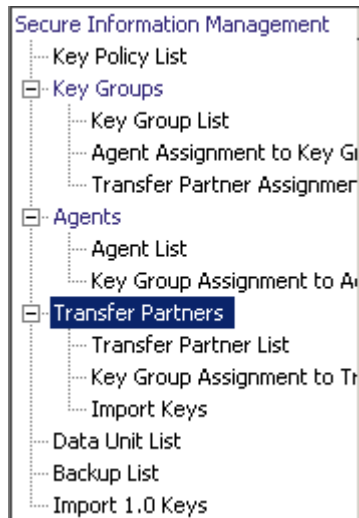
### **C1 Administrator (Operator Role):**

6. Select the Import Keys screen. See [“Import Keys Menu” on page 256](#).
7. Supply the Destination Key Group the keys are to be imported to, the Sending Transfer Partner (C2, in this case) that exported these keys, and the Key Transfer file name. The selected key group must be a key group that is configured to receive keys from C2.
8. Click Start.

---

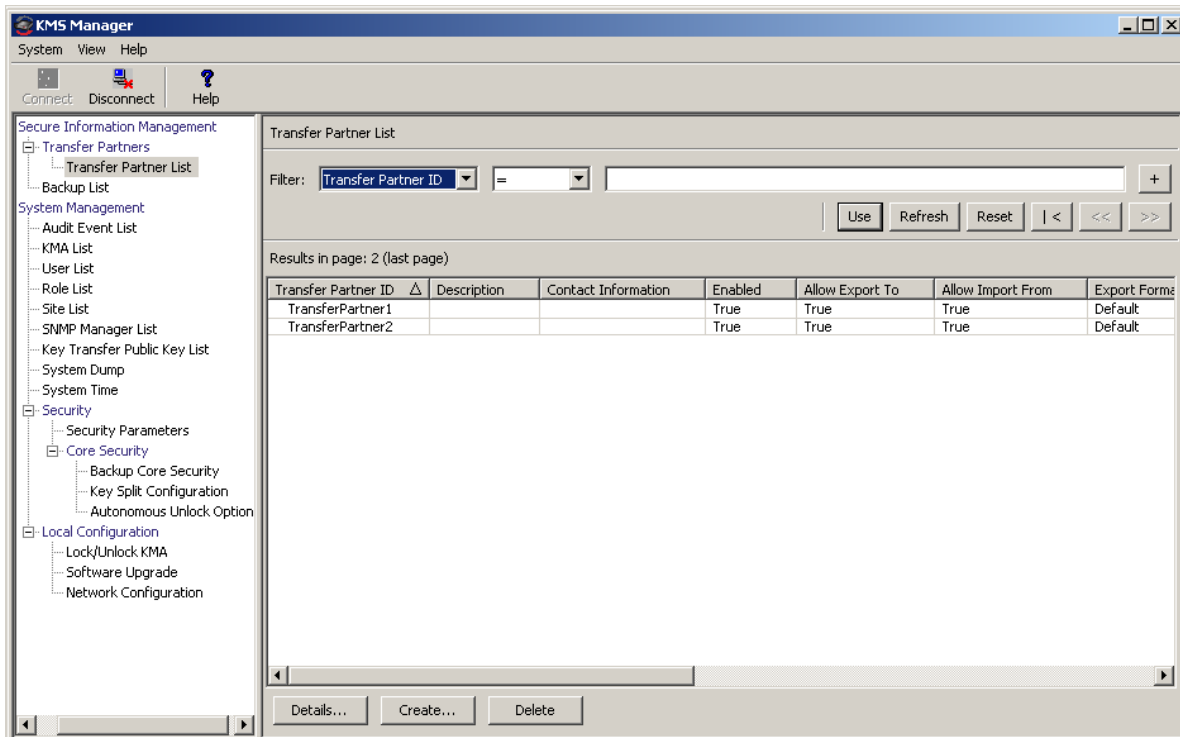
## Transfer Partners Menu

The Key Transfer Partners feature allows keys to be moved from one KMS Cluster to another.



## Transfer Partner List Menu

From the Secure Information Management menu, select **Transfer Partner List**.



You can also scroll through the database and filter the Transfer Partner list by any of the following keys:

- Transfer Partner ID
- Description
- Contact Information
- Enabled
- Allow Export To
- Allow Import From

The **Use** button applies the filter to the displayed list for the Transfer Partner.

The fields and their descriptions are given below:

### Filter:

Select filter options to filter the displayed list of Transfer Partners. Only Transfer Partners that satisfy all filters will be displayed.

**Filter Attribute combo box:**

Click the down-arrow and select an attribute to filter by. Possible values are:

- Transfer Partner ID
- Description
- Contact Information
- Enabled
- Allow Export To
- Allow Import From

**Filter Operator combo box:**

Click the down-arrow and select the filter operation to apply to the selected attribute. This filter option is not displayed for all filter attributes. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

**Filter Value text box:**

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

**Filter Value combo box:**

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.



Click this button to add additional filters.



Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

**Use:**

Click this button to apply the selected filters to the displayed list and go to the first page.

**Refresh:**

Click this button to refresh the displayed list. This does not apply filters selected since the last Use or Reset, and does not change the page of the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of items that can be displayed on the current page. Appends "(last page)" to the number of items if you are at the end of the list. The maximum number of items displayed on a page is defined by the Query Page Size value on the Options dialog.

**Transfer Partner ID:**

Displays the unique identifier that distinguishes each Transfer Partner. This value can be between 1 and 64 (inclusive) characters. Click this Column Name to sort by this attribute.

**Description:**

Describes the Transfer Partner. This value can be between 1 and 64 (inclusive) characters. Click this Column Name to sort by this attribute.

**Contact Information:**

Displays contact information about the Transfer Partner. Click this Column Name to sort by this attribute.

**Enabled:**

Indicates whether the Transfer Partner is allowed to share keys. Possible values are: True or False. If this field is False, the Transfer Partner cannot share keys. Click this Column Name to sort by this attribute.

**Allow Export To:**

Indicates whether the Transfer Partner is allowed to export keys. Possible values are: True or False. If this field is False, the Transfer Partner cannot export keys. Click this Column Name to sort by this attribute.

**Allow Import From:**

Indicates whether keys can be imported from this Transfer Partner. Possible values are: True or False. If this field is False, keys cannot be imported from this Transfer Partner. Click this Column Name to sort by this attribute.

**Export Format:**

Indicates whether keys can be wrapped (wrap keys encrypt the media key on the LAN and the token.) In the Export Format column, a “v2.0” value means that this Transfer Partner does not wrap keys when it exports them. A “v2.1 (FIPS)” value means that this Transfer Partner wraps keys when it exports them. An “N/A” value signifies that the connected KMA runs 2.0.x KMS software, and thus does not allow the user to select this setting.

**Public Key ID**

Displays the unique identifier that distinguishes each Public Key. This value can be between 1 and 64 (inclusive) characters. Click this Column Name to sort by this attribute.

**Public Key Fingerprint**

Shows the fingerprint, or hash value, of the Public Key.

**Entry Date**

Displays the date the Public Key was entered into the KMS Cluster.

## Creating a Transfer Partner

To create a transfer partner:

1. From the Transfer Partner List screen, click the Create button. The Create Transfer Partner dialog box is displayed, with the General tab active.

The screenshot shows a Windows-style dialog box titled "Create Transfer Partner". It has two tabs: "General" and "Public Keys". The "General" tab is active and contains the following elements:

- Transfer Partner ID:** A single-line text input field.
- Description:** A multi-line text area.
- Contact Information:** A large, empty text area.
- Flags:** A section containing three checkboxes:
  - ☒ Enabled
  - ☐ Allow Export To
  - ☐ Allow Import From

At the bottom right of the dialog are two buttons: "Save" and "Cancel".

2. Complete the following parameters:

### *General Tab*

#### **Transfer Partner ID**

Uniquely identifies the Transfer Partner.

#### **Description**

Type a value that uniquely describes the Transfer Partner. This value can be between 1 and 64 (inclusive) characters. This field can be left blank.

**Contact Information**

Type a value that identifies contact information about the Transfer Partner. This field can be left blank.

**Flags - Enabled**

Check this box to allow this Transfer Partner to share keys. If the field is not selected, the Transfer Partner cannot share keys.

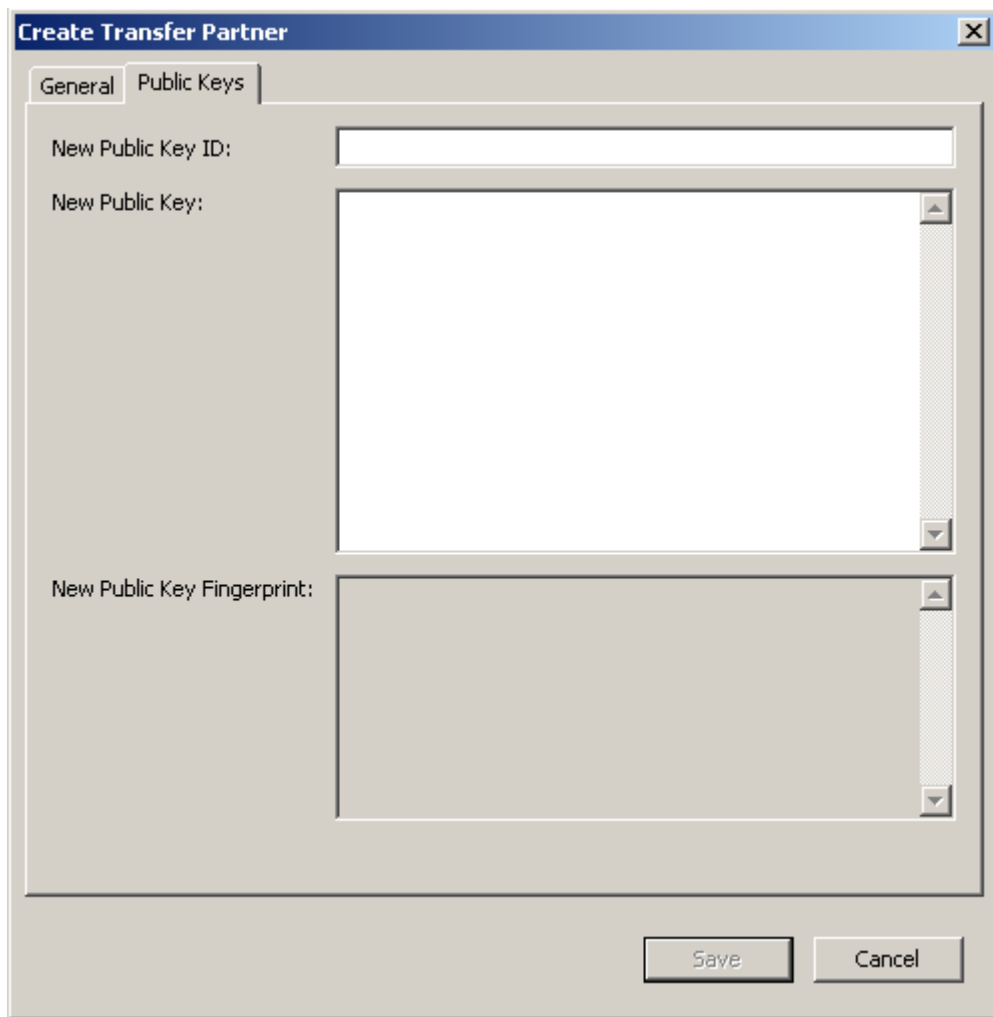
**Allow Export To**

Check this box to allow keys to be exported to the Transfer Partner. If this field is not selected, the Transfer Partner will not be available for the export keys operation.

**Allow Import From**

Check this box to indicate whether keys can be imported from this Transfer Partner. If this field is not selected, keys cannot be imported from this Transfer Partner.

3. Open the Public Keys tab.



The screenshot shows a Windows-style dialog box titled "Create Transfer Partner". It has two tabs: "General" and "Public Keys", with "Public Keys" currently selected. The dialog contains three input fields, each with a label to its left: "New Public Key ID:" followed by a single-line text box; "New Public Key:" followed by a large multi-line text area; and "New Public Key Fingerprint:" followed by another large multi-line text area. At the bottom right of the dialog are two buttons: "Save" and "Cancel".



*Public Keys Tab***New Public Key ID**

Enter the Public Key ID provided to you by the Transfer Partner.

**New Public Key**

Enter the Public Key provided to you by the Transfer Partner.

**New Public Key Fingerprint**

This read-only field shows the fingerprint, or hash value, of the new Public Key. Verify this fingerprint with the Partner to ensure the Public Key has not been tampered with, accidentally or deliberately, during transmission.

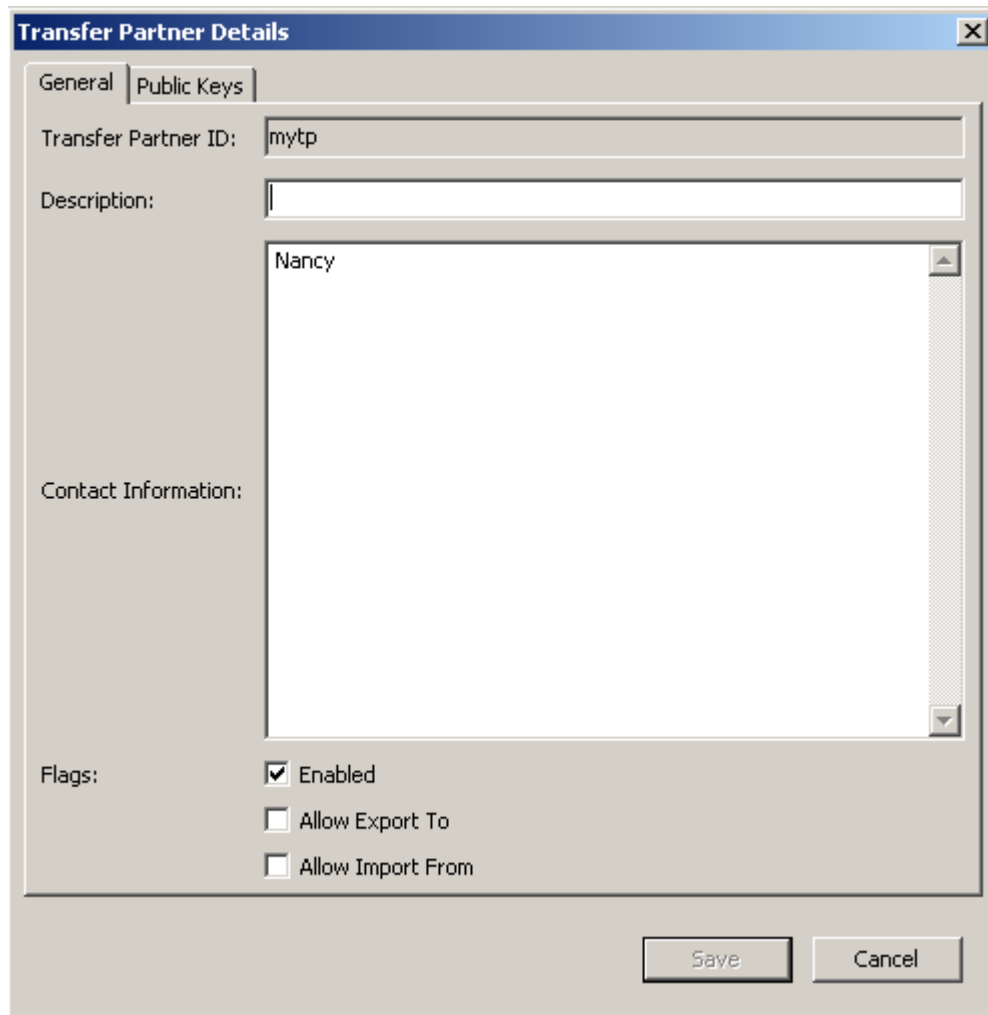
4. When you are finished, click the Save button.

## Viewing/Modifying Transfer Partner Details

The Transfer Partner Details dialog box allows you to view detailed information about a specific Transfer Partner.

To view these details:

1. From the Transfer Partner List screen, highlight a Transfer Partner ID and click the Details button. The Transfer Partner Details dialog box is displayed.



The image shows a screenshot of the 'Transfer Partner Details' dialog box. It has a title bar with the text 'Transfer Partner Details' and a close button. Below the title bar are two tabs: 'General' and 'Public Keys'. The 'General' tab is selected. Inside the dialog, there are several fields: 'Transfer Partner ID:' with the value 'mytp', 'Description:' with an empty text box, and 'Contact Information:' with a large text area containing the name 'Nancy'. At the bottom, there is a 'Flags:' section with three checkboxes: 'Enabled' (checked), 'Allow Export To' (unchecked), and 'Allow Import From' (unchecked). At the very bottom of the dialog are two buttons: 'Save' and 'Cancel'.

### *General Tab*

2. On the General tab, you can change the following fields:

- Description
- Contact Information
- Flags Enabled
- AllowExport To
- Allow Import From

The Transfer Partner ID field is read-only.

3. When you are finished, click the Save button. The Transfer Partners record in the database is modified.
4. Open the Public Keys tab.

**Transfer Partner Details \***

General Public Keys

New Public Key ID:

New Public Key:

New Public Key Fingerprint:

Existing Public Keys:

| Public Key ID                    | Public Key                                |
|----------------------------------|---|
| 23F3156AA4864460DF9FB777F1AD7... | 0201018EFD5E3DBEB972DD357B24815202302FF8f |

Save Cancel

### *Public Keys Tab*

5. On the Public Keys tabs, you can change the following fields:

#### **New Public Key ID**

Enter the new Public Key ID provided to you by the Transfer Partner.

#### **New Public Key**

Enter the new Public Key provided to you by the Transfer Partner.

**New Public Key Fingerprint**

This read-only field shows the fingerprint, or hash value, of the new Public Key. Verify this key with the sending transfer partner.

**Existing Public Keys**

This list displays Public Keys associated with this Transfer Partner.

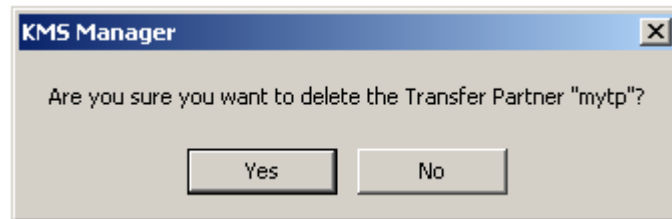
6. When you are finished, click the Save button.

## Deleting a Transfer Partner

This option gives the Security Officer the ability to delete a Transfer Partner.

To delete a Transfer Partner:

1. From the Transfer Partner List screen, highlight the Transfer Partner ID you want to delete and click the Delete button. The Transfer Partner Confirm Delete dialog box is displayed.



2. Click the Yes button to delete the Transfer Partner. The currently selected Transfer Partner is deleted, and you are returned to the Transfer Partner List screen.

# Key Transfer Public Key List Menu

To share keys between Transfer Partners, Security Officers first must access Public Key information for their KMS Cluster. This menu provides public key information. The Public Key and Public Key ID displayed by this command must be sent to the Transfer Partner.

## Viewing the Key Transfer Public Key List

To view the Key Transfer Public Key List:

1. From the System Management menu, select Key Transfer Public Key List.

Key Transfer Public Key List

Filter: Public Key ID =

+

Use

Refresh

Reset

| <

<<

>>

Results in page: 2 (last page)

| Public Key ID                    | Created Date ▾       | Public Key                                       | Public Key Fingerprint  |
|----------------------------------|----------------------|--|-------------------------|
| 9CE46A4BB276A9FB4A22A5AC51A22627 | 1/7/2008 10:44:16 AM | 02010190E4D77B563DB885A7F856BB38F0A69E941D535... | rare tease goofy roc    |
| 9CE46A4BB276A9FB6AE492172EA4C999 | 1/7/2008 10:32:14 AM | 02010183D788368911AE2E18D965152CE3120E39325EC... | jilt equal gallop vinyl |

Details...

Create

You can also scroll through the database and filter the Key Transfer Public Key List by any of the following keys:

- Public Key ID
- Created Date
- Public Key

The **Use** button applies the filter to the displayed list for the Key Transfer Public Key List.

The fields and their descriptions are given below:

**Filter:**

Select filter options to filter the displayed list of Public Keys. Only Public Keys that satisfy all filters will be displayed.

**Filter Attribute combo box:**

Click the down-arrow and select an attribute to filter by. Possible values are:

- Public Key ID
- Created Date
- Public Key

**Filter Operator combo box:**

Click the down-arrow and select the filter operation to apply to the selected attribute. This filter option is not displayed for all filter attributes. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

**Filter Value text box:**

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

**Filter Value combo box:**

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

**Filter Value combo box:**

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.



Click this button to add additional filters.



Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

**Use:**

Click this button to apply the selected filters to the displayed list and go to the first page.

**Refresh:**

Click this button to refresh the displayed list. This does not apply filters selected since the last Use or Reset, and does not change the page of the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of items that can be displayed on the current page. Appends "(last page)" to the number of items if you are at the end of the list. The maximum number of items displayed on a page is defined by the Query Page Size value on the Options dialog.

**Public Key ID:**

Displays the unique identifier that distinguishes each Public Key. This value can be between 1 and 64 (inclusive) characters. Click this Column Name to sort by this attribute.

**Created Date:**

Displays the date and time when this Public Key was created. Click this Column Name to sort by this attribute.

The private key corresponding to the most recently created public key will be used to sign all exported Key Transfer files.

**Public Key:**

Displays the Public Key used to perform key transfers between Transfer partners. This value is shown in base 64. Click this Column Name to sort by this attribute.

**Public Key Fingerprint:**

The hash of the Public Key. This value is used to verify the Public Key is correctly transmitted, and it is shown in base 64.



## Viewing the Key Transfer Public Key Details

To view the Key Transfer Public Key details screen:

1. Select a Public Key and click the Details button.

The Key Transfer Public Key Details dialog box is displayed.



The dialog box titled "Key Transfer Public Key Details" contains the following fields:

- Public Key ID:** 9CE46A4BB276A9FI
- Created Date:** 1/7/2008 10:44:16
- Public Key:** A list box containing the following hexadecimal strings:
  - 02010190E4D7
  - 7B563DB885A7
  - F856BB38F0A6
  - 9E941D535FE9
  - F5B2C9D4BE4E
  - F99431F23FD0
  - 7D258E8C05EC
  - 5F79700A8B0E
- Public Key Fingerprint:** A list box containing the following text strings:
  - rare tease
  - goofy room
  - agent dingy

A "Close" button is located at the bottom center of the dialog box.

# Creating a Key Transfer Public Key

To create a Key Transfer Public Key:

- 1. Click the Create button.
- 2. Provide the new key to all existing Transfer Partners.

Since any Key Transfer files created after the new Key Transfer Public Key is created will be signed with the new Key Transfer Public Key, partners must be provided with the new Key Transfer Public Key before they can import the new Key Transfer files.

Key Transfer Public Key List

Filter: Public Key ID =

+

Use

Refresh

Reset

| <

<<

>>

Results in page: 3 (last page)

| Public Key ID                    | Created Date ▾       | Public Key                                       | Public Key Fingerprir   |
|----------------------------------|----------------------|--|-------------------------|
| 9CE46A4BB276A9FBE8FE99E7C3E203F8 | 1/15/2008 6:11:00 PM | 020101CAD193962581A1DEE0E3EF3319084F2801A63F0... | selma flush equal all   |
| 9CE46A4BB276A9FB4A22A5AC51A22627 | 1/7/2008 10:44:16 AM | 02010190E4D77B563DB885A7F856BB38F0A69E941D535... | rare tease goofy roc    |
| 9CE46A4BB276A9FB6AE492172EA4C999 | 1/7/2008 10:32:14 AM | 02010183D788368911AE2E18D965152CE3120E39325EC... | jilt equal gallop vinyl |

Details...

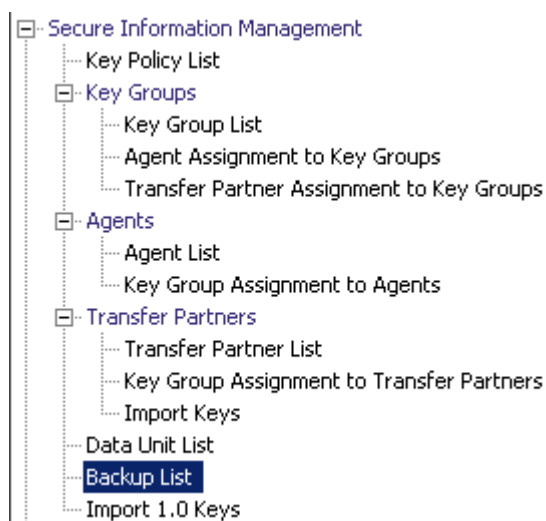
Create

---

# Backup List Menu

The Backups List menu option allows the Security Officer to:

- View the history of the Backups
- View details of a Backup file
- Restore Backups



## Viewing Backup Files History

To view Backup files history:


From the Secure Information Management menu, select Backup List. The Backup List screen is displayed.

Backup List

Filter: Backup ID =  +

Use Refresh Reset | < << >> >

Results in page: 2 (last page)

| Backup ID  | KMA ID           | Created Date         | Destroyed Date | Destruction |
|---|------------------|----------------------|----------------|-------------|
| FDAC7620B1491D50000000000000000001  | FDAC7620B1491D50 | 12/4/2007 8:26:49 AM |                | PENDING     |
| FDAC7620B1491D50000000000000000002  | FDAC7620B1491D50 | 12/4/2007 8:30:18 AM |                | PENDING     |

Details... Create Backup... Restore... Confirm Destruction...

You can also scroll through the database and filter the Backup Files by any of the following keys:

- Backup ID
- KMA ID
- Created Date
- Destroyed Date
- Destruction Status
- Destruction Comment.

The + button applies the filter to the displayed list for the Backup file.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA.  
Possible values are:

- Backup ID
- Created Date
- Destroyed Date
- Destruction Status
- Destruction Comment.

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~

**Filter Value 1 box:**

If you selected a date filter, click Set Date to specify start date and time. The value appears as a starting value of the filter key range. If you selected any other filter, type a value in this field.

**Filter Value 2 box:**

If you selected a date filter, click Set Date to select an end date and time. The value appears as an ending value of the filter key range.

**Use:**

Click this button to apply the filter to the displayed list.

**Refresh:**

Click this button to refresh the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

**Backup ID**

Displays a system-generated unique identifier that distinguishes each Backup file.

**KMA ID**

Displays the KMA for which the Backup file was generated.

**Created Date**

Displays the date when the backup was created.

**Destroyed Date**

Displays the date that the Backup file was marked as being manually destroyed.

**Destruction Status**

Indicates the status of the backup with respect to its destruction. Possible values are:

**NONE**

The Backup file has not been destroyed and does not contain Data Unit keys that have been destroyed.

**PENDING**

The Backup file has not yet been manually destroyed and contains copies of Data Unit keys that have been destroyed.

**DESTROYED**

The Backup file has been manually destroyed.

**Destruction Comment**

Displays user-supplied information on the Backup file's destruction.

**Details:**

Click this button to view more detailed information on a Backup.

**Create Backup:**

Click this button to create a Backup. This button is not enabled if you are a Security Officer.

**Restore:**

Click this button to restore a Backup.

**Confirm Destruction:**

Click this button to confirm the destruction of a Backup. This button is not enabled if you are a Security Officer.

If you want more detailed information on a backup, highlight the backup and click the Details button. For more information, refer to [“Viewing Backup Details” on page 163](#).

Click the Restore button to restore the currently selected backup. For more information, refer to [“Restoring a Backup” on page 165](#).

## Viewing Backup Details

The Backup Details dialog box is used to view the details of a Backup file.

---

**Note** – Backup files are created and restored on the KMA.

---

To view the details of a Backup file:

1. From the Backups List screen, double-click the Backup entry for which you want more information or highlight the Backup entry and click the Details button. The Backup Details dialog box is displayed, with all fields read-only.

|                      |                                  |
|----------------------|----------------------------------|
| Backup ID:           | FDAC7620B1491D500000000000000001 |
| KMA ID:              | FDAC7620B1491D50                 |
| Created Date:        | 12/4/2007 8:26:49 AM             |
| Completed Date:      | 12/4/2007 8:26:52 AM             |
| Downloaded Date:     | 12/4/2007 8:28:13 AM             |
| Destroyed Date:      |                                  |
| Destruction Status:  | PENDING                          |
| Destruction Comment: |                                  |

Close

2. The fields and their descriptions are given below:

### Backup ID

Displays a system-generated unique identifier that distinguishes each Backup file.

### KMA ID

Displays the KMA on which this Backup file is generated.

### Created Date

Displays the date and time when the Backup file was created.

### Completed Date

Displays the date and time when the Backup file was completed.

### Downloaded Date

Displays the date and time when the Backup file was downloaded.

**Destroyed Date**

Displays the date when the Backup file was destroyed.

**Destruction Status**

Indicates the status of the backup with respect to its destruction.

**Destruction Comment**

Displays user-supplied information on the Backup file's destruction.

3. Click the Close button to close this dialog box.



## Restoring a Backup

This function gives the user the ability to upload and restore a backup that consists of a Backup file and a Backup key file to the KMA. Before you restore a Backup file to a KMA, ensure that you have the quorum for authentication.

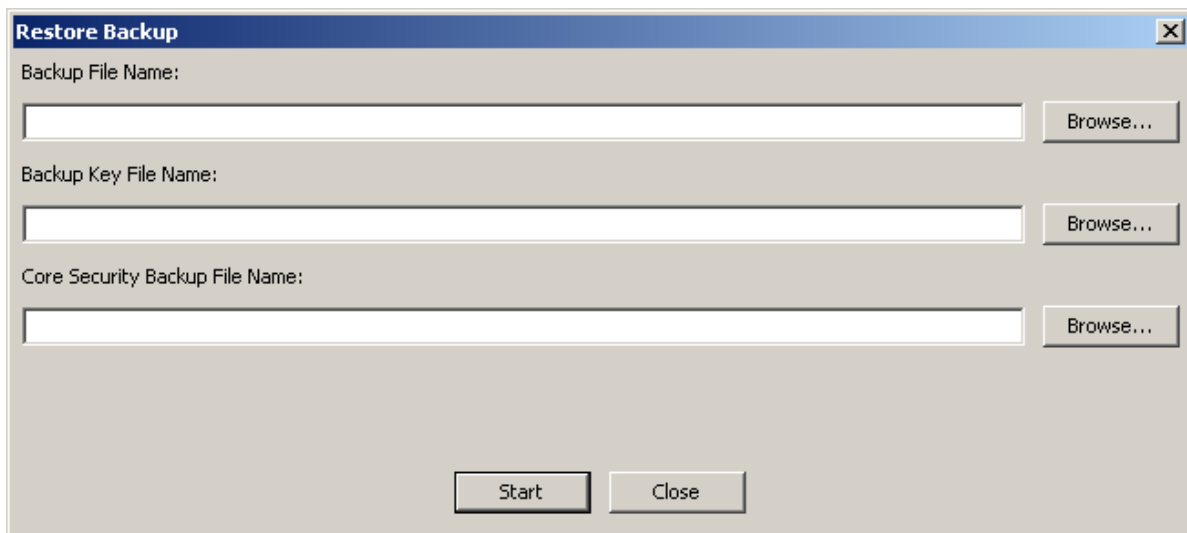
---

**Important** – Before you start this procedure, you must perform the procedure [“Restoring a Cluster From a Backup”](#) on page 43.

---

To restore a backup:

1. From the Backup List screen, highlight the Backup you want to restore and click the Restore button. The Restore Backup dialog box is displayed.
2. Select the desired Core Security backup, backup key file, and backup file. The backup key file and the backup must match, that is, they must have been created at the same time. The Core Security backup can be older or newer than the backup key file and backup file. Any Core Security backup file can be used with any backup key file and backup file.
3. Click the Start button.

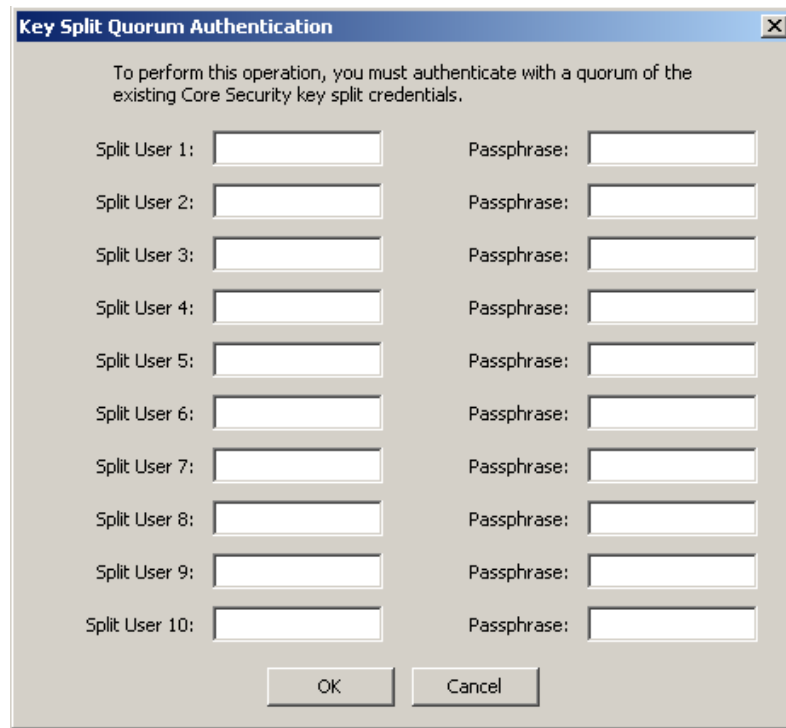


The image shows a 'Restore Backup' dialog box with a blue title bar and a close button (X) in the top right corner. The dialog contains three input fields, each with a 'Browse...' button to its right:

- Backup File Name:** An empty text box with a 'Browse...' button.
- Backup Key File Name:** An empty text box with a 'Browse...' button.
- Core Security Backup File Name:** An empty text box with a 'Browse...' button.

At the bottom of the dialog, there are two buttons: 'Start' and 'Close'.

4. When the upload process is completed, it is indicated on the Restore Backup dialog box and the Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



The dialog box is titled "Key Split Quorum Authentication" and contains the following text: "To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials." Below this text are ten rows of input fields. Each row consists of a label (Split User 1 through Split User 10) followed by a text box for the user name, and then the label "Passphrase:" followed by a text box for the passphrase. At the bottom of the dialog box are two buttons: "OK" and "Cancel".

5. Choosing the OK button after the last user name and passphrase is entered, sends the user names and passphrases to the KMA for authentication. If the authentication is successful, the Key Split Quorum Authentication dialog box closes.

The user IDs and passphrases, and the number required (i.e., the quorum) must match with the Key Split Credentials that were in effect when the Core Security backup was created.

6. The Restore Backup dialog box is displayed, indicating the status of the restore process.
7. The fields and their descriptions are given below:

**Backup File Name**

Name of the backup file.

**Backup Wrapping Key File Name**

Displays the name of the Backup Key File.

**Core Security Backup File Name**

Name of the backup file containing Core Security Key material.

8. When the restore is completed, a message indicating this is displayed. Click the Close button to close this dialog box. The database and the Secure Key Store are restored to the KMA.

---

**Note** – After you successfully restore a backup, you need to update the IP address settings for the KMA. Network settings are not backed up, and thus are not restored. Refer to [“Setting the KMA Management IP Address” on page 303](#) and [“Setting the KMA Service IP Addresses” on page 305](#).

---

---

## System Dump Menu

The System Dump menu creates a system dump for problem resolution and downloads it to a compressed file on the system where the KMS Manager is running. The downloaded file is in a format that can be opened with compression utilities.

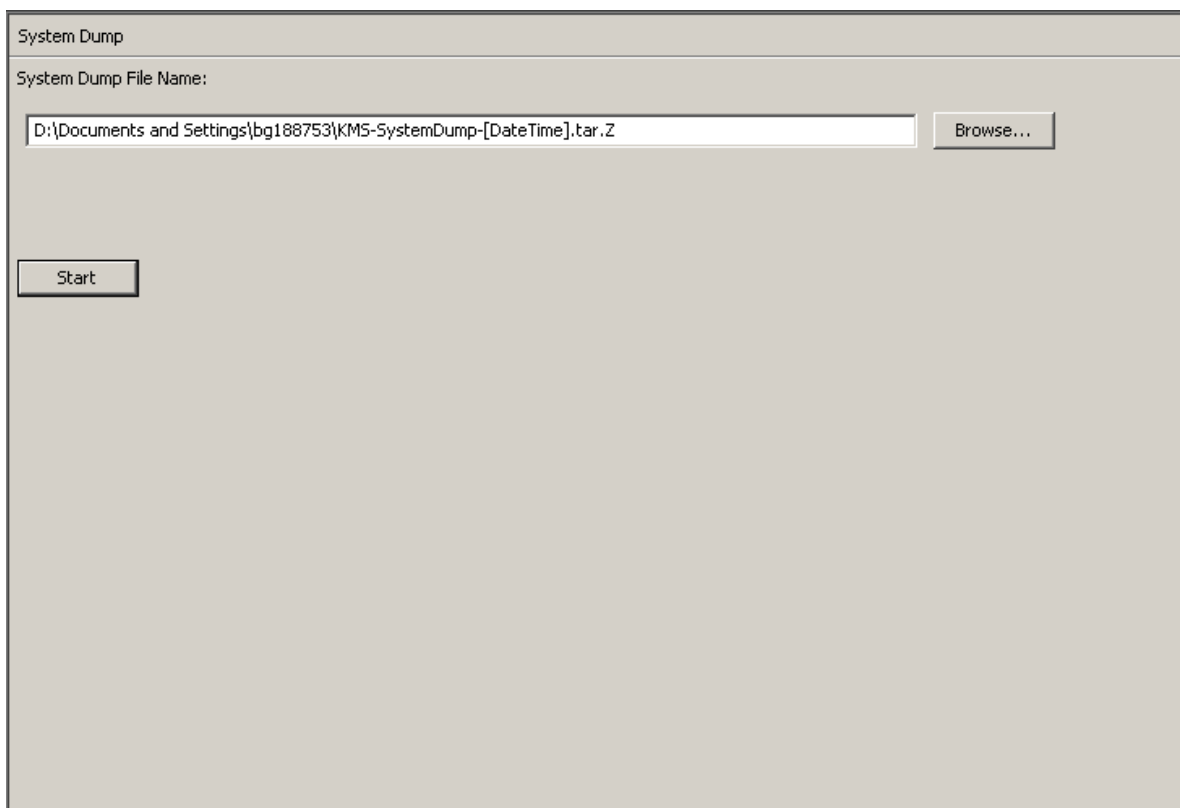
---

**Note** – The dump does not include any key material or information from which keys can be inferred.

---

## Creating a System Dump

1. To create a system dump, from the System Management menu, select System Dump. The screen is displayed and shows an automatically-generated \*.tar.Z file. If desired, you can click Browse to select a destination path.
2. Click the Start button to begin the download. The system displays messages indicating the amount of system dump information that is being downloaded in real-time and tells you when the process is complete.
3. Go to the destination path and open the \*.tar.Z file to view the system dump information.



The fields and their descriptions are given below:

**File Name:**

Displays an automatically-generated \*.tar.gz file.

**Browse:**

Click this button to specify a location for this file.

**Start:**

Click this button to initiate the download process.

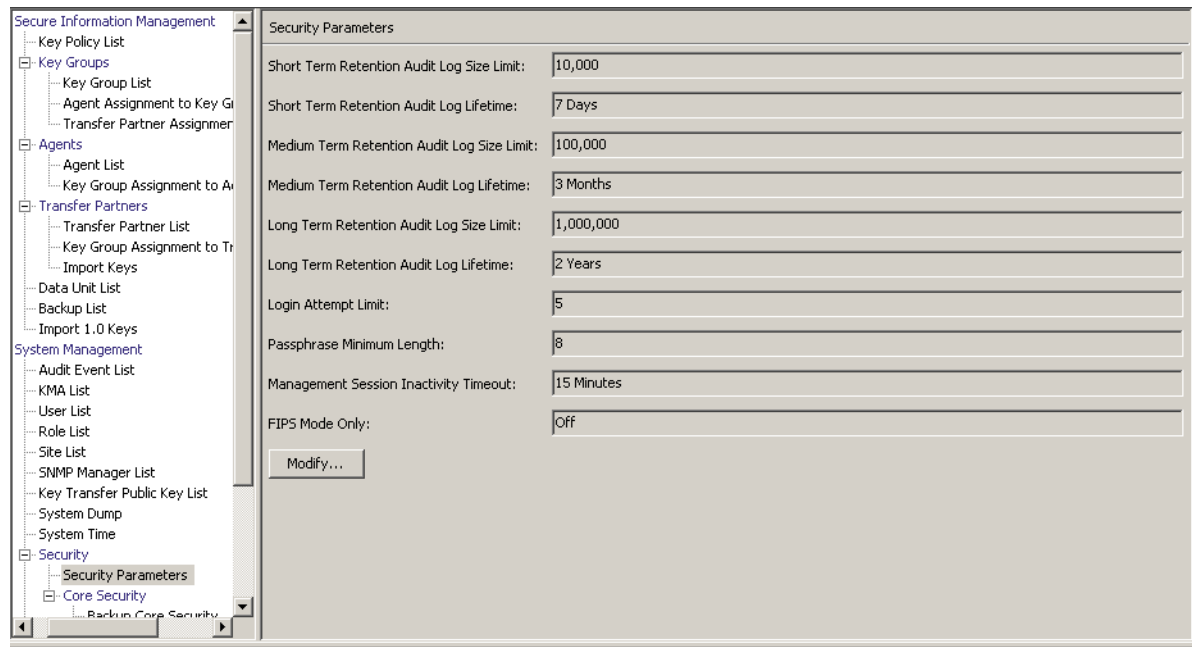
# Security Parameters Menu

The Security menu gives the Security Officer the ability to view and modify the KMA's security parameters.

## Retrieving the Security Parameters

To retrieve the security parameters:

From the Security menu, select Security Parameters. The Security Parameters screen is displayed in read-only mode.



The fields and their descriptions are given below:

### Short Term Retention Audit Log Size Limit

Displays the number of Error event Audit Log entries that are retained before they are truncated. The default is 10,000. The minimum value is 1000; maximum value is 1,000,000.

**Short Term Retention Audit Log Lifetime**

Displays the amount of time (in days) that Short Term Audit Log entries are retained before they are truncated. The default is 7 days. The minimum value is 7 days; maximum value is 25,185 days (approximately 69 years).

**Medium Term Retention Audit Log Size Limit**

Displays the number of Error event Audit Log entries that are retained before they are truncated. The default is 100,000. The minimum value is 1000; maximum value is 1,000,000.

**Medium Term Retention Audit Log Lifetime**

Displays the amount of time (in days) that Short Term Audit Log entries are retained before they are truncated. The default is 90 days. The minimum value is 7 days; maximum value is 24,855 days.

**Long Term Retention Audit Log Size Limit**

Displays the number of long term retention Audit Log entries that are retained before they are truncated. The default is 1,000,000. The minimum value is 1000; maximum value is 1,000,000.

**Long Term Retention Audit Log Lifetime**

Displays the amount of time (in days) that Long Term Audit Log entries are retained before they are truncated. The default is 730 days. The minimum value is 7 days; maximum value is 24,855 days.

**Login Attempt Limit**

Indicates the number of failed login attempts before an entity is disabled. The default is 5. The minimum value is 1; maximum value is 1000.

**Passphrase Minimum Length**

Displays the minimum length of the passphrase. The default is 8 characters. The minimum value is 8 characters; the maximum value is 64 characters.

**Management Session Inactivity Timeout**

Displays the maximum length of time (in minutes) a KMS Manager or Console login session can be left idle before being automatically logged out. Changing this value has no effect on sessions that are already in progress. The default is 15 minutes. The minimum value is 0, meaning no time is used; the maximum value is 60 minutes.

**FIPS Mode Only**

Displays the import key and format transfer file settings.

An **Off** value means the KMA can import 1.0 keys and allows export and import of v2.0 or v2.1 (FIPS) format transfer files. An **On** value means the KMA cannot import 1.0 keys and allows export and import of v2.1 (FIPS) format transfer files only.

The **On** value can be set only if the current Replication Version is at least 10.

If you want to change the Security Parameters, click the Modify button. For more information, refer to [“Modifying the Security Parameters” on page 172](#).

## Modifying the Security Parameters

To modify security parameters:

1. From the Security Parameters List screen, click the Modify button. The Modify Security Parameters screen is displayed.

**Modify Security Parameters**

Short Term Retention Audit Log Size Limit: 10,000

Short Term Retention Audit Log Lifetime: 7 Day(s)

Medium Term Retention Audit Log Size Limit: 100,000

Medium Term Retention Audit Log Lifetime: 3 Month(s)

Long Term Retention Audit Log Size Limit: 1,000,000

Long Term Retention Audit Log Lifetime: 2 Year(s)

Login Attempt Limit: 5

Passphrase Minimum Length: 8

Management Session Inactivity Timeout: 15 Minutes

FIPS Mode Only: Off

Save Cancel

2. Modify the security parameters, as required. When you are finished, click the Save button. The changes are saved in the KMA database.



---

## Core Security

The primary element of the Core Security component is the Root Key Material. It is key material that is generated when a Cluster is initialized. The Root Key Material protects the Master Key. The Master Key is a symmetric key that protects the Data Unit Keys stored on the KMA.

Core Security is protected with a key split scheme that requires a quorum of users defined in the Key Split Credentials to provide their usernames and passphrases to unwrap the Root Key Material.

This security mechanism enables two operational states for the KMA: locked and unlocked.

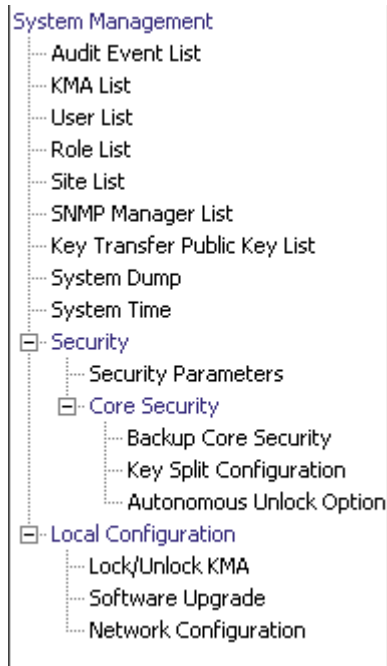
A KMA in the locked state is not able to unwrap the Root Key Material, and thus is unable to access the Data Unit Keys. As a result, the KMA is unable to service Agent requests to register new Data Units or retrieve Data Unit Keys for existing Data Units.

A KMA in the unlocked state is able to use the Root Key Material to access the Data Unit Keys and service Agent requests for Data Unit Keys.

---

# Core Security Management Menu

The Core Security menu contains the following menu options:



It allows the Security Officer to:

- Create a Core Security backup
- View/Modify Key Split Credentials
- Enable/Disable the Autonomous Unlock Option

## Backup Core Security

The Backup Core Security option allows the Security Officer to back up Core Security Key material and download it to a file on the local system.

---

**Caution** – Core security backup files should be carefully protected. Because any Core Security backup file can be used with any backup file/backup key file pair, even old Core Security backup files remain useful.

---

## Creating a Core Security Backup

A new core security backup needs to be performed after the Key Split Credentials are modified.

---

**Important** – The Security Officer must back up Core Security Key material before the Backup Officer can create a backup. See [“Creating a Backup” on page 277](#).

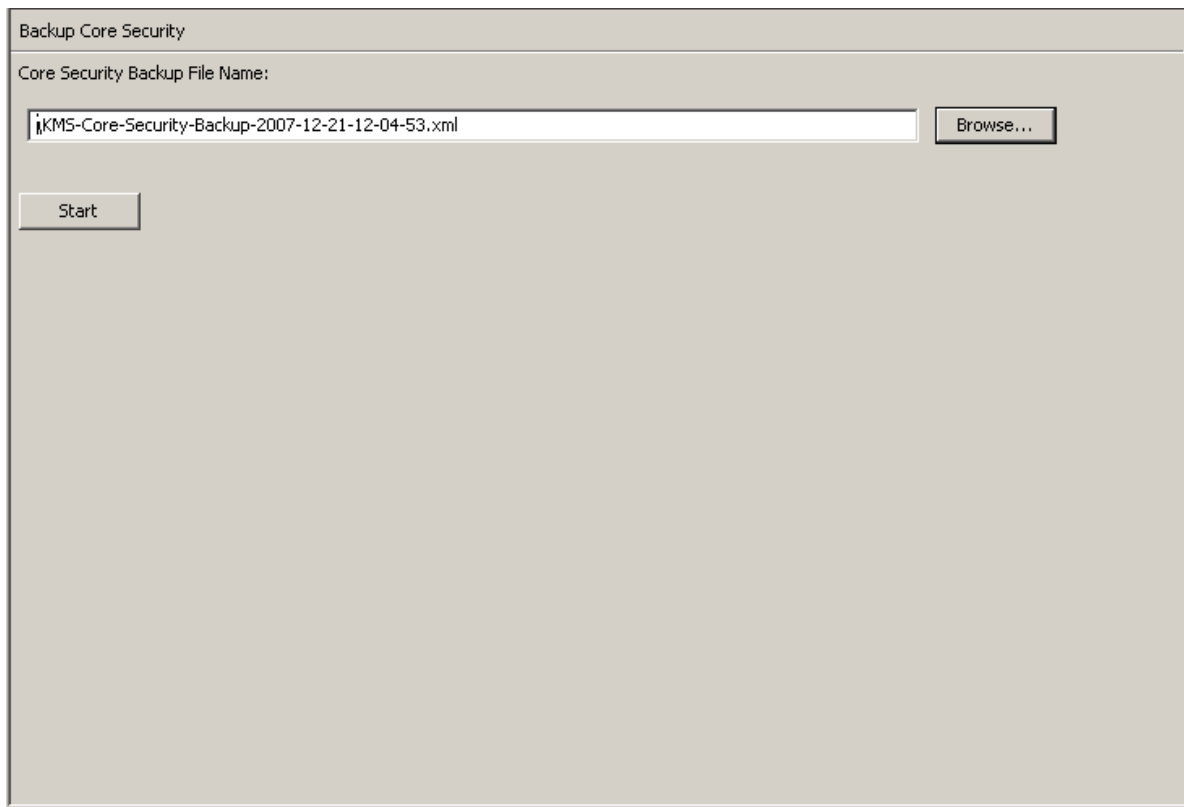
---

1. From the Core Security menu, select Backup Core Security. The Backup Core Security dialog box is displayed.

---

**Note** – The Core Security Backup File names are automatically generated. However, you can edit the names, and you can also click the Browse button to select a destination path.

---



Backup Core Security

Core Security Backup File Name:

KMS-Core-Security-Backup-2007-12-21-12-04-53.xml

Browse...

Start

2. Select the Start button to create the Core Security Backup file and download it to the user-specified destination.
3. When the backup is completed, a message is displayed. Click the Close button to close this dialog box
4. You are returned to the Backup Core Security screen.

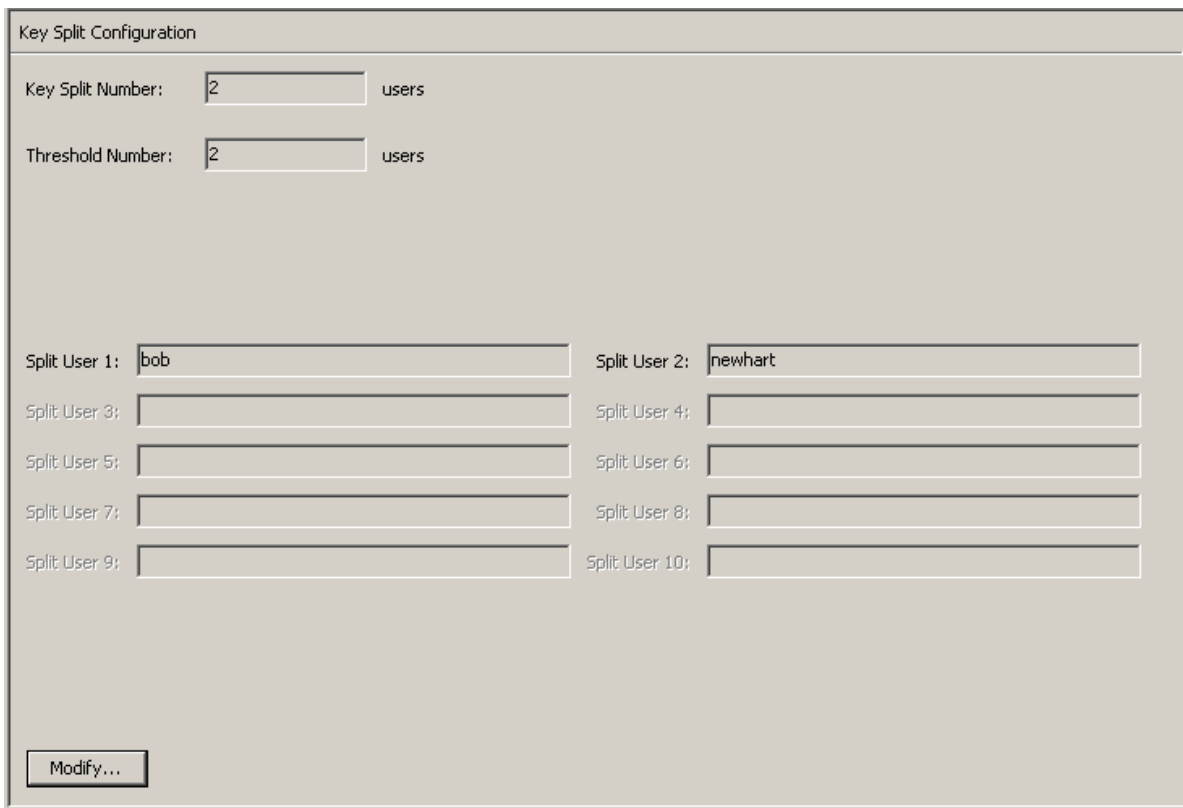
## Key Split Configuration

The Key Split Configuration menu option gives the Security Officer the ability to view and modify the key split credentials for the KMA.

### Viewing the Key Split Configuration

To view the Key Split Configuration:

1. From the Core Security menu, select Key Split Configuration. The Key Split Configuration dialog box is displayed.



The image shows a 'Key Split Configuration' dialog box. It has a title bar with the text 'Key Split Configuration'. Inside the dialog, there are two input fields at the top: 'Key Split Number:' with a value of '2' and 'users' to its right, and 'Threshold Number:' with a value of '2' and 'users' to its right. Below these are ten input fields for 'Split User' names, arranged in two columns. The first column contains 'Split User 1:' with 'bob', 'Split User 3:', 'Split User 5:', 'Split User 7:', and 'Split User 9:'. The second column contains 'Split User 2:' with 'newhart', 'Split User 4:', 'Split User 6:', 'Split User 8:', and 'Split User 10:'. At the bottom left of the dialog is a button labeled 'Modify...'.

The fields and their descriptions are given below:

#### Key Split Number

Displays the number of key splits. The maximum is 10.

#### Threshold Number

Displays the number of users that are necessary to authenticate a quorum.

#### Split User (1-10)

Displays the user names of the existing split.

If you want to modify the Key Split user names, passphrases, and threshold number, click the Modify button. For more information, refer to [“Modifying the Key Split Configuration” on page 178](#).

## Modifying the Key Split Configuration

To modify the Key Split configuration:

1. From the Key Split Configuration screen, click the Modify button. The Modify Key Split Configuration dialog box is displayed.

Modify Key Split Configuration

Key Split Number:  users

Threshold Number:  users

Please enter your username and passphrase:

|                |                                      |             |                      |                     |                      |
|----------------|--------------------------------------|-------------|----------------------|---------------------|----------------------|
| Split User 1:  | <input type="text" value="bob"/>     | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 2:  | <input type="text" value="newhart"/> | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 3:  | <input type="text"/>                 | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 4:  | <input type="text"/>                 | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 5:  | <input type="text"/>                 | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 6:  | <input type="text"/>                 | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 7:  | <input type="text"/>                 | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 8:  | <input type="text"/>                 | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 9:  | <input type="text"/>                 | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |
| Split User 10: | <input type="text"/>                 | Passphrase: | <input type="text"/> | Confirm Passphrase: | <input type="text"/> |

2. Complete the following parameters and click the OK button:

### Key Split Number

Type a new value for the number of key splits. The maximum number is 10.

### Threshold Number

Type a new value for the number of users that will be required to form a quorum.

### Split User $x$

Type the new user name. For each Split User, complete its associated Passphrase and Confirm Passphrase fields.

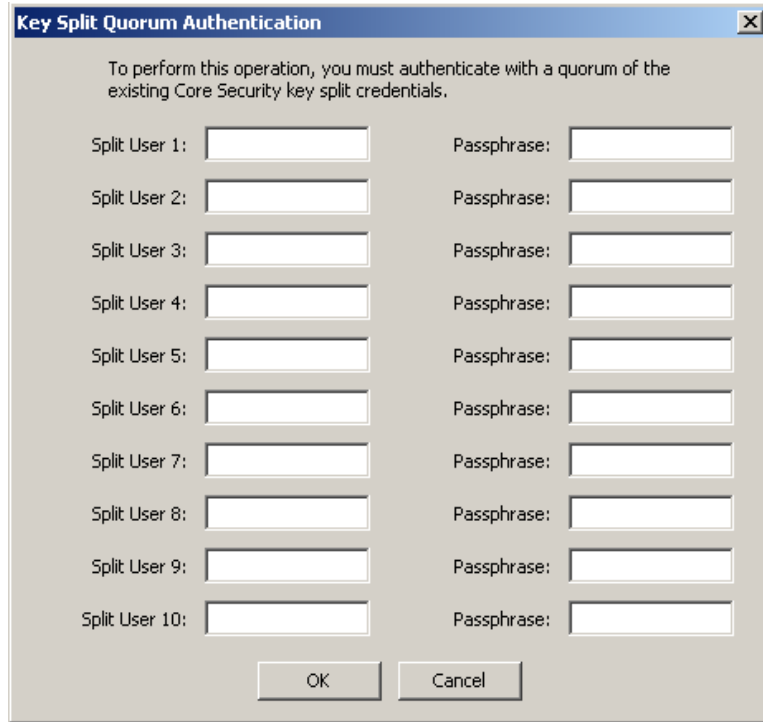
---

**Note** – The number of Split User fields that are enabled is dependent on the value that you entered in the Key Split Number field.

---

3. Click the Save button after the last user name and passphrase is entered.

- The Key Split Quorum Authentication dialog box is displayed after the new Key Split credentials are entered. Type the user name and passphrase for the existing quorum credentials and click the OK button. This is required to set “new” credentials set in [Step 2](#) and [Step 3](#).



The dialog box is titled "Key Split Quorum Authentication" and contains the following text: "To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials." Below this text are ten rows of input fields, each labeled "Split User 1:" through "Split User 10:" on the left and "Passphrase:" on the right. At the bottom of the dialog are two buttons: "OK" and "Cancel".

- The system updates the old configuration information with the new configuration in the database. The new configuration is displayed in the Key Split Credentials screen.

---

**Note** – The Core Security Key material is re-wrapped using the updated Key Split credentials.

---

- Create a new Core Security backup (see [“Creating a Core Security Backup” on page 175](#)).

---

**Note** – Destroy all old Core Security backup files to ensure that the previous Key Split Credentials cannot be used to destroy a backup.

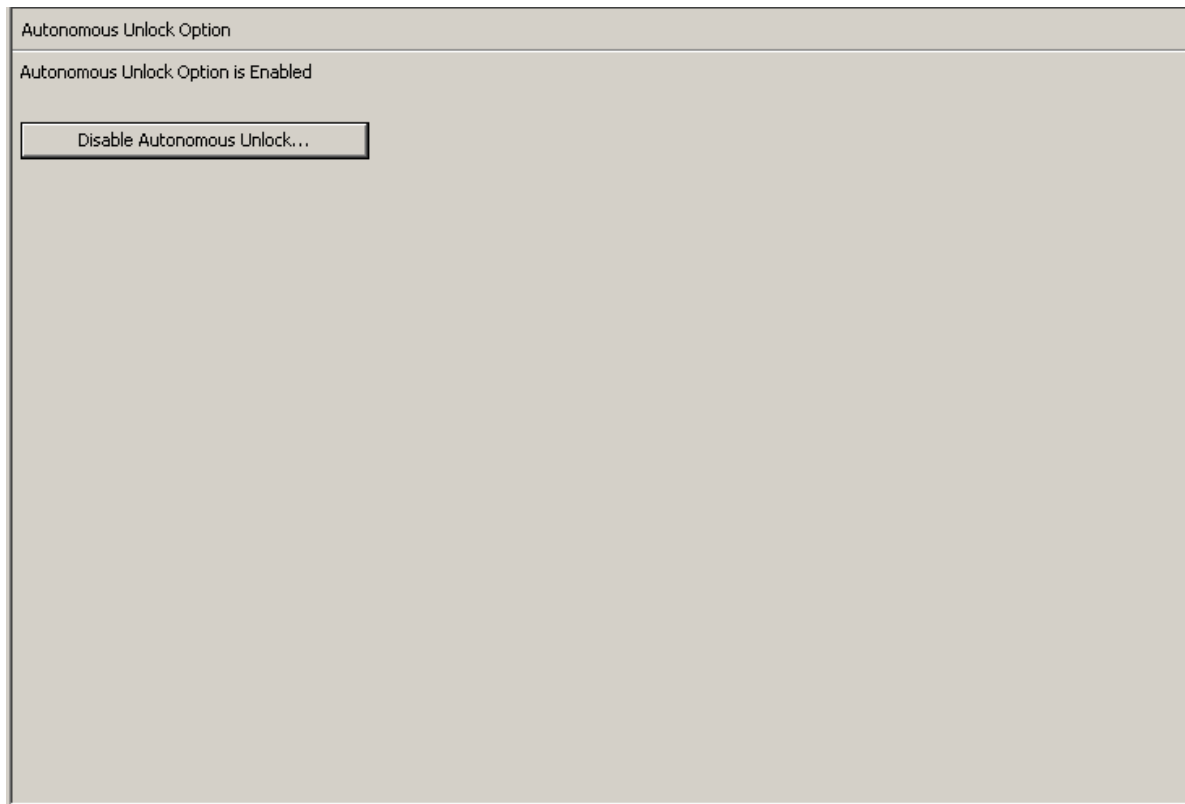
---

## Autonomous Unlock Option

The Autonomous Unlock Option menu option gives the Security Officer the ability to enable or disable the autonomous option for the KMA.

To enable or disable the Autonomous Unlock option:

1. From the Core Security menu, select Autonomous Unlock Option. The Autonomous Unlock Option screen is displayed, indicating the current autonomous status.



2. Depending on the current autonomous boot status, click the Enable Autonomous Unlock to enable this option or click the Disable Autonomous Unlock to disable the option.

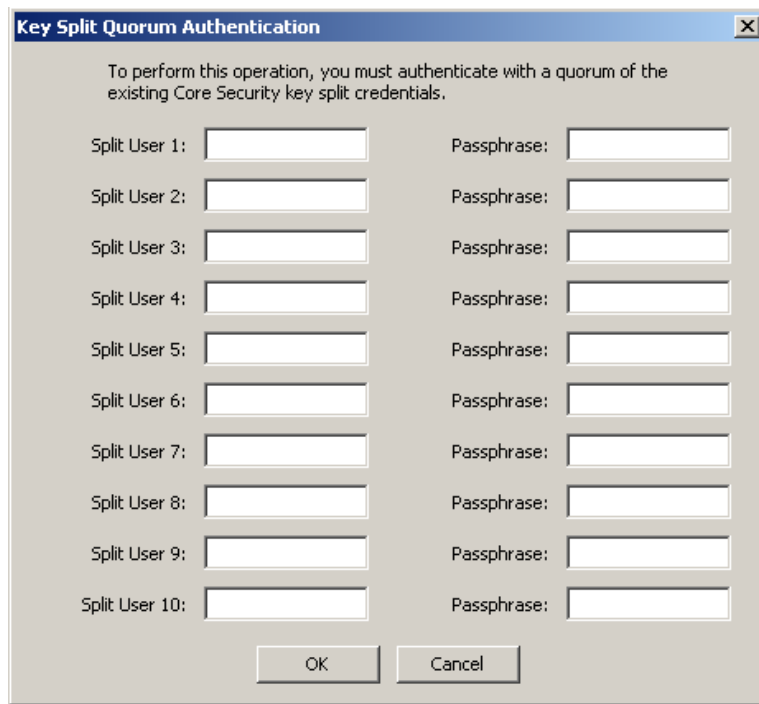
---

### Notes –

- The Lock/Unlock button toggles between states and sets the KMA locked state opposite to the current state.
  - You must provide a quorum to enable or disable the Autonomous Unlock Option.
-



3. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



The dialog box is titled "Key Split Quorum Authentication" and contains the following text: "To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials." Below this text are ten rows of input fields. Each row consists of a label (e.g., "Split User 1:", "Split User 2:", ..., "Split User 10:") followed by a text box, and then the label "Passphrase:" followed by another text box. At the bottom of the dialog box are two buttons: "OK" and "Cancel".

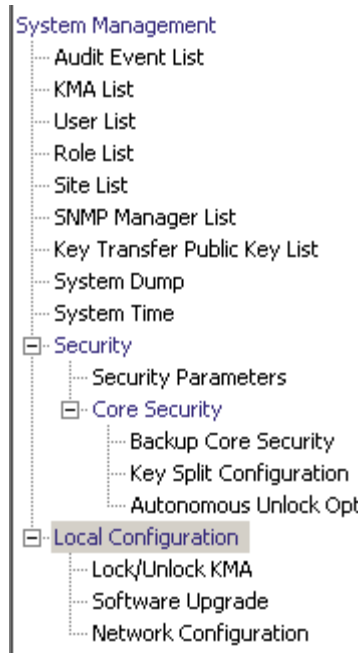
4. Choosing the OK button after the last user name and passphrase is entered, sends the user names and passphrases to the KMA for authentication.
5. If the authentication is successful, the Key Split Quorum Authentication dialog box closes and the new autonomous boot option is set for the KMA.

---

# Local Configuration Menu

The Local Configuration menu includes the following options:

- Lock/Unlock the KMA
- Upgrade the software (see [“Software Upgrade Menu” on page 269](#))
- Network configuration information.



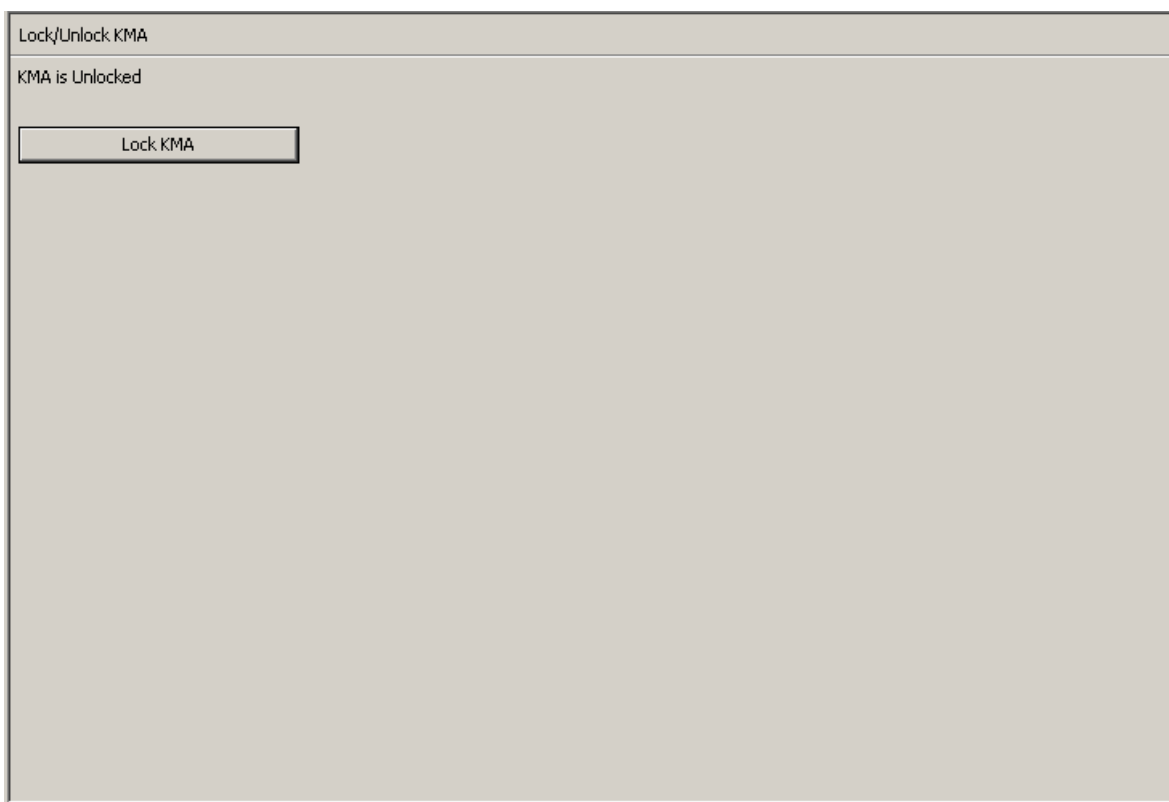
## Lock/Unlock KMA

The Lock/Unlock KMA menu option gives the Security Officer the ability to lock and unlock the KMA's Core Security. Please see [“Core Security” on page 173](#) for details on Core Security and the behavior of the KMA when Core Security is locked and unlocked.

### Locking the KMA

To lock the KMA:

1. From the Local Configuration menu, select **Lock/Unlock KMA**. The Lock/Unlock KMA screen is displayed, indicating the state of the KMA. In this example, it is “Unlocked.”



2. Click the Lock KMA button to lock the KMA. Once the button is pressed, it changes to Unlock KMA, indicating the new lock state and the allowed operation. The KMA is now locked.

---

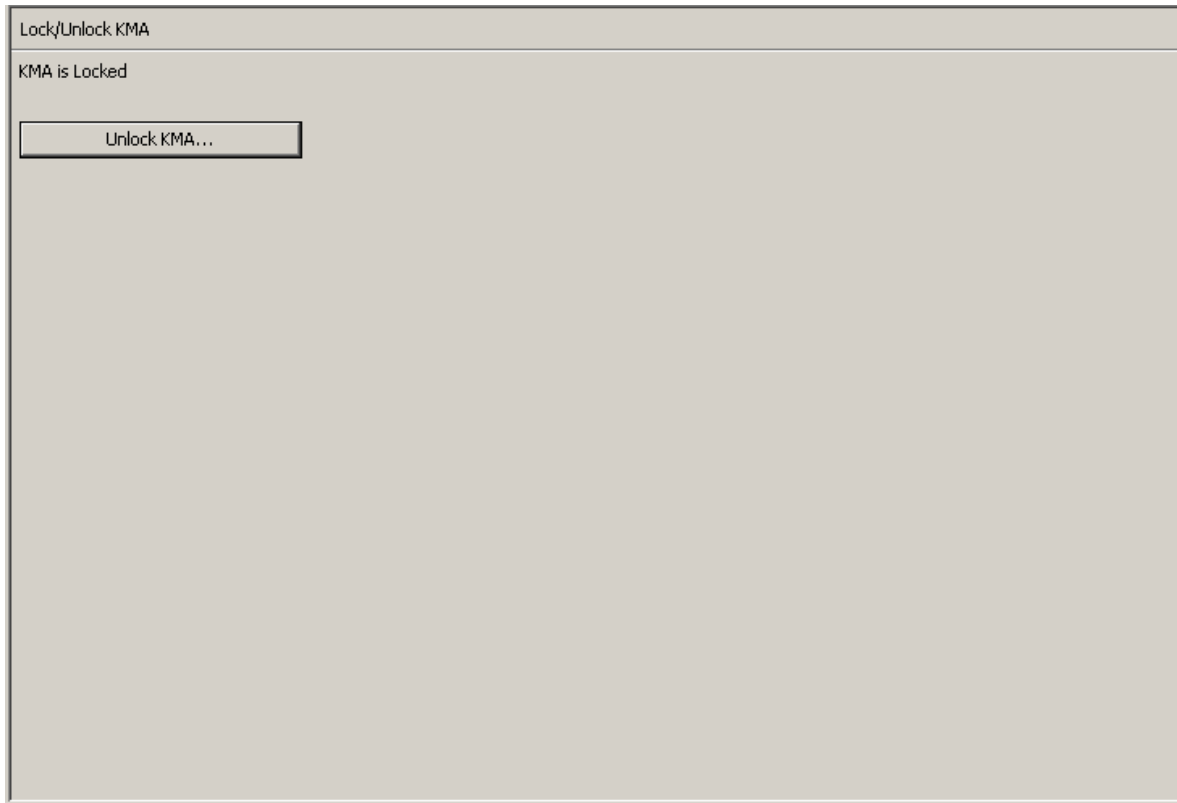
**Note** – The Lock KMA/Unlock KMA button toggles between states and sets the KMA locked state opposite to the current state. Once a button is pressed, the text label and button label change to indicate the new lock state and the allowed operation.

---

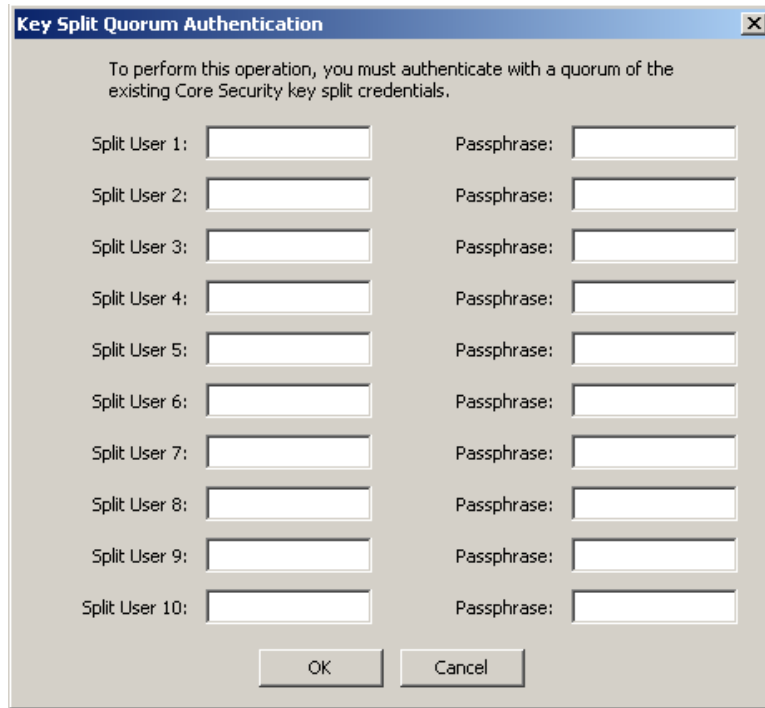
## Unlocking the KMA

To unlock the KMA:

1. From the Lock/Unlock KMA screen click the **Unlock KMA** button.



2. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.

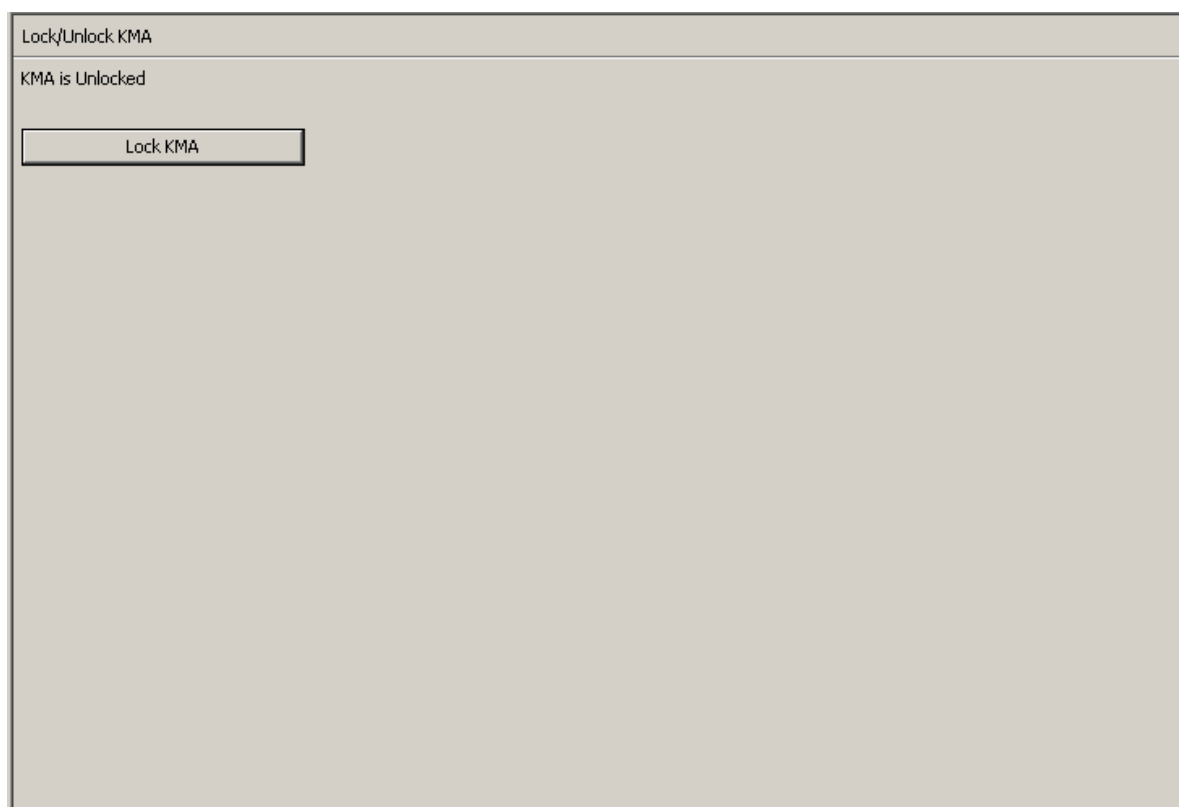


The dialog box is titled "Key Split Quorum Authentication" and contains a close button (X) in the top right corner. Below the title bar, there is a message: "To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials." The main area of the dialog contains ten rows of input fields. Each row has a label "Split User 1:" through "Split User 10:" followed by a text input field, and a label "Passphrase:" followed by a password input field. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

| Split User 1:        | Passphrase:              |
|----------------------|--------------------------|
| <input type="text"/> | <input type="password"/> |
| Split User 2:        | Passphrase:              |
| <input type="text"/> | <input type="password"/> |
| Split User 3:        | Passphrase:              |
| <input type="text"/> | <input type="password"/> |
| Split User 4:        | Passphrase:              |
| <input type="text"/> | <input type="password"/> |
| Split User 5:        | Passphrase:              |
| <input type="text"/> | <input type="password"/> |
| Split User 6:        | Passphrase:              |
| <input type="text"/> | <input type="password"/> |
| Split User 7:        | Passphrase:              |
| <input type="text"/> | <input type="password"/> |
| Split User 8:        | Passphrase:              |
| <input type="text"/> | <input type="password"/> |
| Split User 9:        | Passphrase:              |
| <input type="text"/> | <input type="password"/> |
| Split User 10:       | Passphrase:              |
| <input type="text"/> | <input type="password"/> |

OK Cancel

3. Click the OK button after the last user name and passphrase is entered. The user names and passphrases are sent to the KMA for authentication.
4. If the authentication is successful, the Key Split Quorum Authentication dialog box closes and the KMA is unlocked.

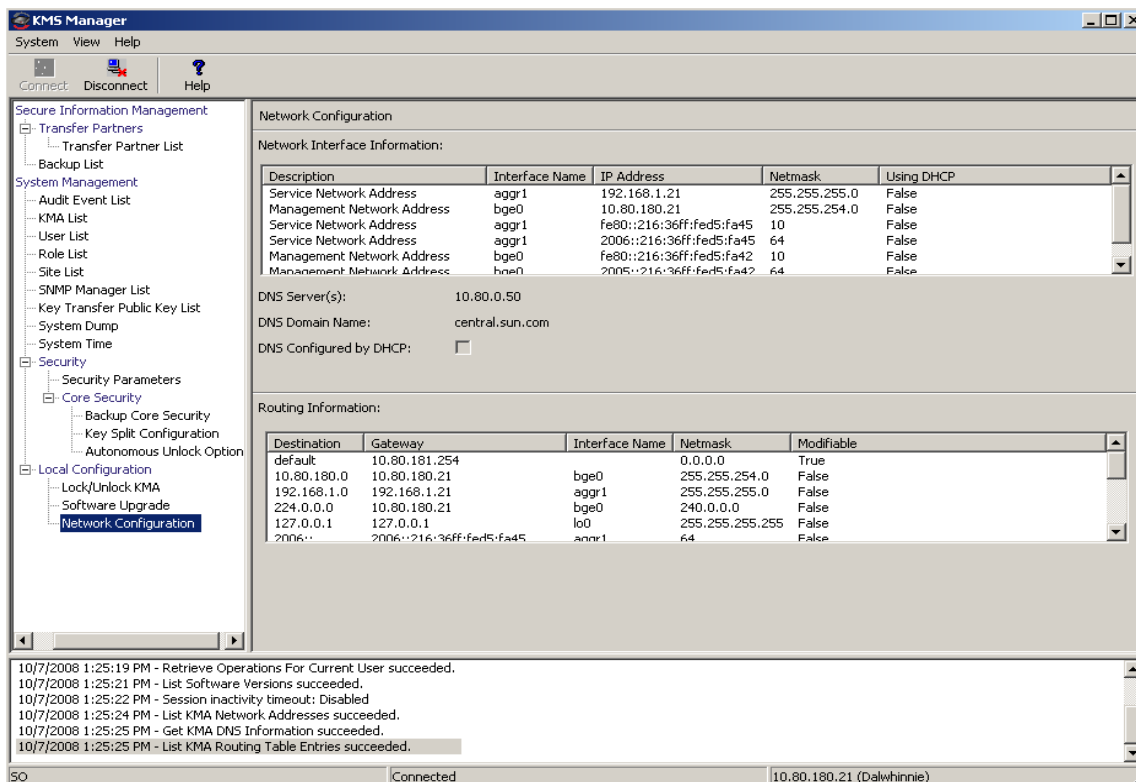


## Network Configuration Information

The Network Configuration menu option shows network configuration settings for the KMA to which you are currently connected. These settings are established in the configuration screens described in [“Using the KMS Console” on page 287](#).

### Displaying the Network Configuration

To display the network configuration, from the Local Configuration menu, select **Network Configuration**. The Network Configuration screen is displayed.



The fields are described below:

#### Description

Displays whether the related information applies to the Management or Service Network Address.

#### Interface Name

The Management or Service Network Hostname established in the QuickStart program.

#### IP Address

The IP address of the Management or Service Network.

#### Netmask

The Subnet Mask address for the Management or Service Network.

**DNS Server(s)**

One or more DNS name servers (if any) used by this KMA.

**DNS Domain Name**

The DNS domain (if any) used by this KMA.

**DNS Configured by DHCP**

An indication whether these DNS settings were configured implicitly by DHCP.

**Using DHCP**

Indicates whether or not the Management or Service Network uses DHCP.

**Destination**

The subnet that network traffic goes to from this KMA.

**Gateway**

The Gateway IP address that network traffic is routed to for the Management or Service Network.

**Modifiable**

Indicates whether or not the Gateway configuration is modifiable. Gateways that are configured automatically are not modifiable.



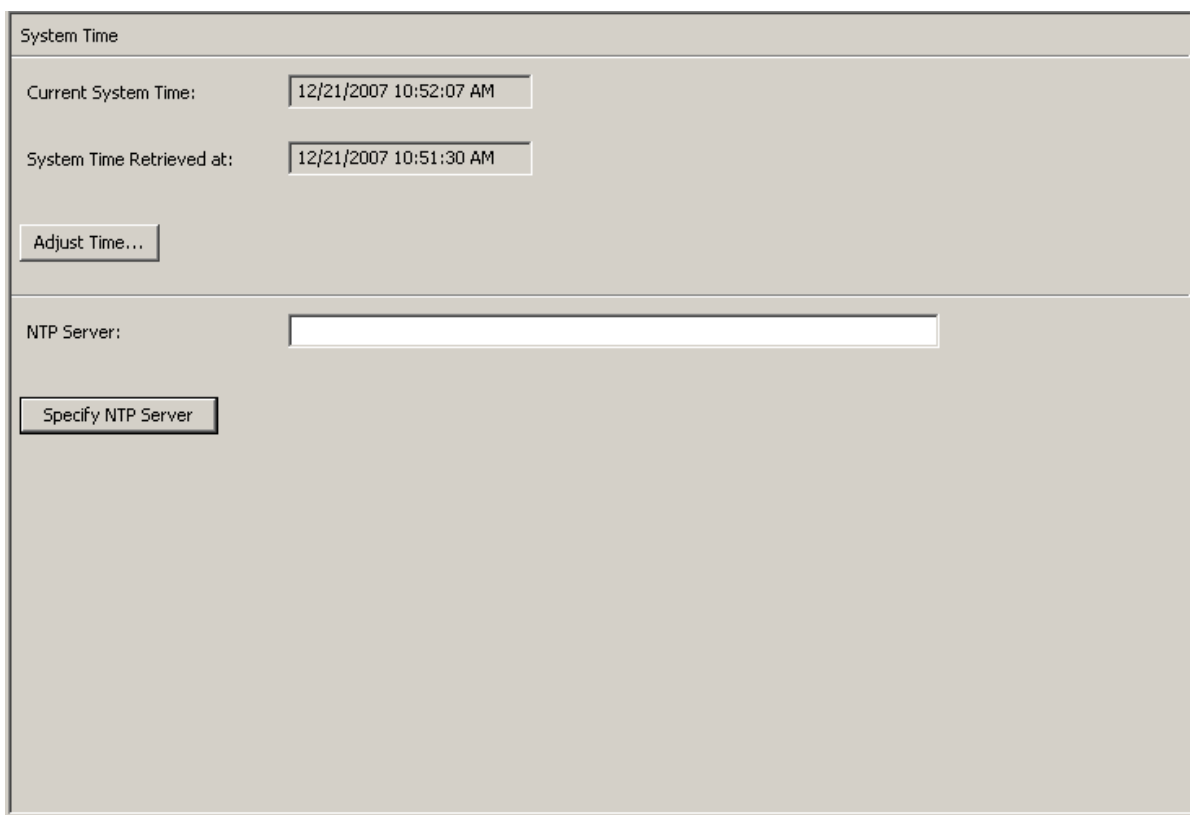
## System Time Menu

The System Time menu option gives the user the ability to set the system clock to which the user is connected. To ensure the correct operation of the KMS solution, it is very important to maintain the times reported by each KMA in a Cluster within five minutes of each other.

### Retrieving the Local Clock Information

To retrieve the local clock information:

From the System Management menu, select **System Time**. The System Time screen is displayed.



The screenshot shows a window titled "System Time". It contains two text fields: "Current System Time:" with the value "12/21/2007 10:52:07 AM" and "System Time Retrieved at:" with the value "12/21/2007 10:51:30 AM". Below these fields is a button labeled "Adjust Time...". Further down, there is a label "NTP Server:" followed by an empty text input field. At the bottom left of the window is a button labeled "Specify NTP Server".

The fields and their descriptions are given below:

**Current System Time**

Displays the current system time.

**System Time Retrieved At**

Displays the local Client time when the KMA's system time was retrieved.

**Adjust Time**

Click this button to modify the system time.

If you want to modify the KMA's clock, click the Adjust Time button. For more information, refer to ["Adjusting the KMA's Local Clock"](#) below.

**NTP Server**

Displays the NTP server that this KMA uses (if any).

**Specify NTP Server**

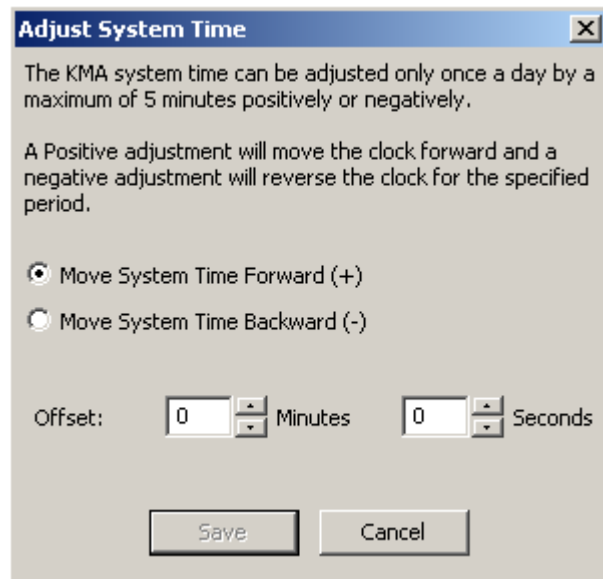
Click this button to specify the NTP server to be used by this KMA.

## Adjusting the KMA's Local Clock

**You can only adjust a KMA's clock once a day by a maximum of plus or minus 5 minutes.** A positive (+) adjustment slowly moves the clock forward, whereas a negative (-) slowly moves the clock backward.

To adjust the KMA's local time:

1. From the System Time menu, click the Adjust Time button. The Adjust System Time dialog box is displayed.



2. Select the "Move System Time Forward (+)" radio button if you want to apply a positive adjustment to the clock. Otherwise, select the "Move System Time Backward (-)" radio button if you want to apply a negative adjustment to the clock.
3. In the Offset Minutes text box, select a numeric value.
4. In the Offset Seconds text box, select a numeric value.

---

**Note** – If the specified offset is too large, an Error message is displayed, prompting you to type a smaller value. Click the OK button to close this dialog box and type a new value.

---

5. Click the Save button to accept the changes. The System clock is adjusted.

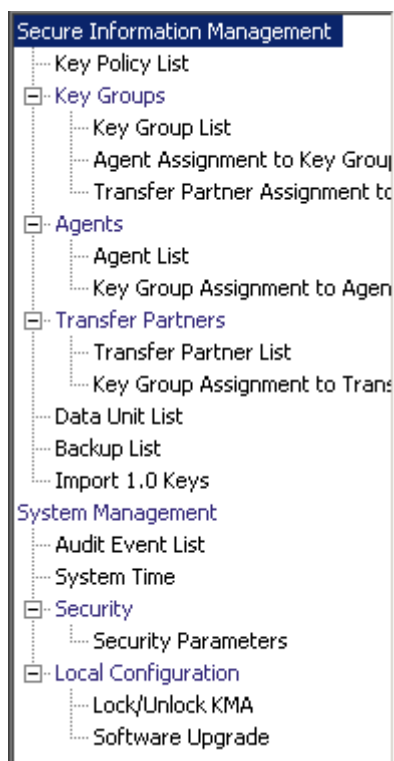


## Compliance Officer Operations

This chapter describes the operations that a user who has been given a Compliance Officer role can perform. If you have been assigned multiple roles, refer to the appropriate chapter for instructions on performing the specific role.

### Compliance Officer Role

The Compliance Officer manages the flow of data through your organization and has the ability to define and deploy data contexts (Key Groups) and rules that determine how data is protected and ultimately destroyed (Key Policies). The menus that provide these functions are shown below.



## Key Policies

Key Policies provide guidance for managing data. The KMS Manager uses Key Policies to determine how data is protected and destroyed. Key Policies must be created before keys can be created and delivered to agents.

Only a Compliance Officer can create and modify Key Policies. This ensures that the data complies with a policy throughout the data's lifetime.

## Key Policy List Menu

The Key Policies List menu allows you to manage the Key Policies in your organizations.

The Key Policy List menu option gives you the ability to:

- View Key Policies
- View/Modify a Key Policy's Details
- Create a Key Policy
- Delete existing Key Policies.

## Viewing Key Policies

To view Key Policies:


1. From the Secure Information Management menu, select **Key Policy List**. The Key Policy List screen is displayed.

Key Policy List

Filter: Key Policy ID =  +

Use Refresh Reset | < << >> >

Results in page: 1 (last page)

| Key Policy ID  | Description | Key Type | Encryption Period | Cryptoperiod | Allow Export From | Allow Import To |
|---|-------------|----------|-------------------|--------------|-------------------|-----------------|
| MyKeyPolicy   | The desc    | AES-256  | 1 Year            | 2 Years      | True              | True            |

Details... Create... Delete

You can also scroll through the database and filter the Key Policy list by any of the following keys:

- Key Policy ID
- Description
- Key Type
- Encryption Period
- Cryptoperiod
- Allow Export From
- Allow Import To.

The **Use** button applies the filter to the displayed list for the Key Policy.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA.  
Possible values are:

- Key Policy ID
- Description
- Key Type
- Encryption Period
- Cryptoperiod
- Allow Export From
- Allow Import To

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

**Filter Value text box:**

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

**Filter Value combo box:**

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.



Click this button to add additional filters.



Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

**Use:**

Click this button to apply the selected filters to the displayed list and go to the first page.

**Refresh:**

Click this button to refresh the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.





Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

**Key Policy ID**

Displays the unique identifier that distinguishes each Key Policy. This value can be between 1 and 64 (inclusive) characters. Key Policy IDs cannot be changed once they are created.

**Description**

Describes the Key Policy. This value can be between 1 and 64 (inclusive) characters.

**Key Type**

Indicates the type of encryption algorithm that Keys associated with this Key Policy use. Possible values are: AES-256 .

---

**Note** – Encryption Period and Cryptoperiod begin when the key is first given to an Agent. Encryption period and Cryptoperiod cannot be changed for a policy. This is to avoid a change in the Key Policy from affecting large numbers of keys.

---

**Encryption Period**

Displays how long keys associated with this Key Policy can be used to encrypt or decrypt data. The time interval units are: minutes, hours, days, week, months, or years.

**Cryptoperiod**

Displays how long keys associated with this Key Policy can be used to decrypt (but not encrypt) data. The time interval units are: minutes, hours, days, week, months, or years.

**Allow Export From**

Indicates whether Data Units associated with this Key Policy can be exported. Possible values are True or False.

**Allow Import To**

Indicates whether Data Units associated with this Key Policy can be imported. Possible values are True or False.

If you want to create a Key Policy, click the Create button. For more information, refer to [“Creating a Key Policy” on page 198](#).

If you want to view / modify a Key Policy, highlight the Key Policy and click the Details button. For more information, refer to [“Viewing/Modifying a Key Policy” on page 200](#).

If you want to delete a Key Policy, click the Delete button. For more information, refer to [“Deleting a Key Policy” on page 201](#).

## Creating a Key Policy

To create a Key Policy:

1. From the Key Policy List screen, click the Create button. The Create Key Policy dialog box is displayed.

A screenshot of the 'Create Key Policy' dialog box. The dialog has a title bar with the text 'Create Key Policy \*' and a close button. It contains several input fields: 'Key Policy ID' with the value 'AnotherPolicy', 'Description' with the value 'Just a test', 'Encryption Period' with a value of '1' and a dropdown menu set to 'Year(s)', and 'Cryptoperiod' with a value of '1' and a dropdown menu set to 'Year(s)'. There are two checkboxes under the 'Flags' section, both of which are checked: 'Allow Export From' and 'Allow Import To'. The 'Key Type' field is set to 'AES-256'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Key Policy ID: AnotherPolicy

Description: Just a test

Encryption Period: 1 Year(s)

Cryptoperiod: 1 Year(s)

Flags: ☒ Allow Export From  
☒ Allow Import To

Key Type: AES-256

Save Cancel

2. Complete the following parameters:

### Key Policy ID

Type a value that identifies the policy. This value can be between 1 and 64 (inclusive) characters.

### Description

Type a value that describes the policy. This value can be between 1 and 64 (inclusive) characters. This field can be blank.

### Encryption Period

Displays how long keys associated with this Key Policy can be used to encrypt or decrypt data. The time interval units are: minutes, hours, days, week, months, or years.

### Cryptoperiod

Displays how long keys associated with this Key Policy can be used to decrypt (but not encrypt) data. The time interval units are: minutes, hours, days, week, months, or years.

**Flags****Allow Export From**

Indicates whether Data Units associated with this Key Policy can be exported.  
Possible values are True or False.

**Allow Import To**

Indicates whether Data Units associated with this Key Policy can be exported.  
Possible values are True or False.


- Click the Save button to save the Key Policy. The new Key Policy is displayed in the Key Policy List screen. It can now be used by Key Groups.

Key Policy List

Filter: Key Policy ID =  +

Use Refresh Reset | < << >> >

Results in page: 2 (last page)

| Key Policy ID  | Description | Key Type | Encryption Period | Cryptoperiod | Allow Export From | Allow Import To |
|---|-------------|----------|-------------------|--------------|-------------------|-----------------|
| AnotherPolicy   | Just a test | AES-256  | 1 Year            | 1 Year       | True              | True            |
| MyKeyPolicy   | The desc    | AES-256  | 1 Year            | 2 Years      | True              | True            |

Details... Create... Delete

## Viewing/Modifying a Key Policy

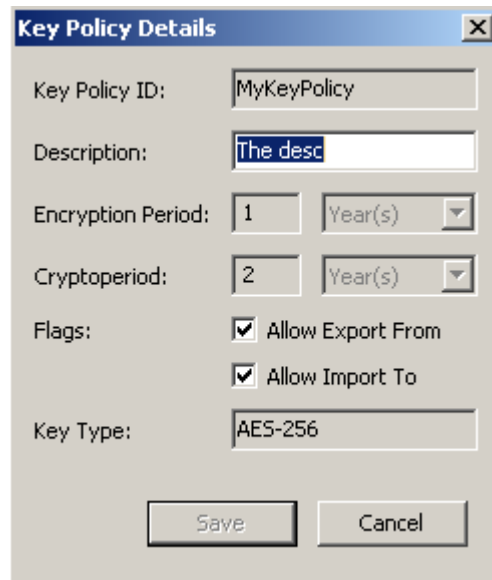
---

**Note** – Only a Compliance Officer can view a Key Policy’s detailed information.

---

To modify a Key Policy’s details:

1. From the Key Policy List screen, double-click a Key Policy for which you want more information or highlight a Key Policy and click the Details button. The Key Policy Details dialog box is displayed.



The image shows a 'Key Policy Details' dialog box with the following fields and controls:

- Key Policy ID:** A text box containing 'MyKeyPolicy'.
- Description:** A text box containing 'The desc'.
- Encryption Period:** A numeric input box with '1' and a dropdown menu set to 'Year(s)'.
- Cryptoperiod:** A numeric input box with '2' and a dropdown menu set to 'Year(s)'.
- Flags:** Two checked checkboxes labeled 'Allow Export From' and 'Allow Import To'.
- Key Type:** A text box containing 'AES-256'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

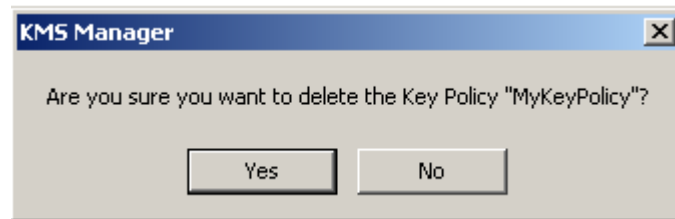
2. You can change the Description, Allow Export From, and Allow Import To fields, as required. When you are finished, click the Save button to save the changes. After the system verifies and validates the new Key Policy, the Key Group is associated with the new Key Policy.
3. If you click the Cancel button, your changes will not be saved and the dialog box will close.

## Deleting a Key Policy

A key policy can only be deleted if it is not used by any Key Group or key.

To delete a Key Policy:

1. From the Key Policy List screen, highlight the Key Policy you want to delete and click the Delete button. The following dialog box is displayed, prompting you to confirm that you want to delete the specific Key Policy.



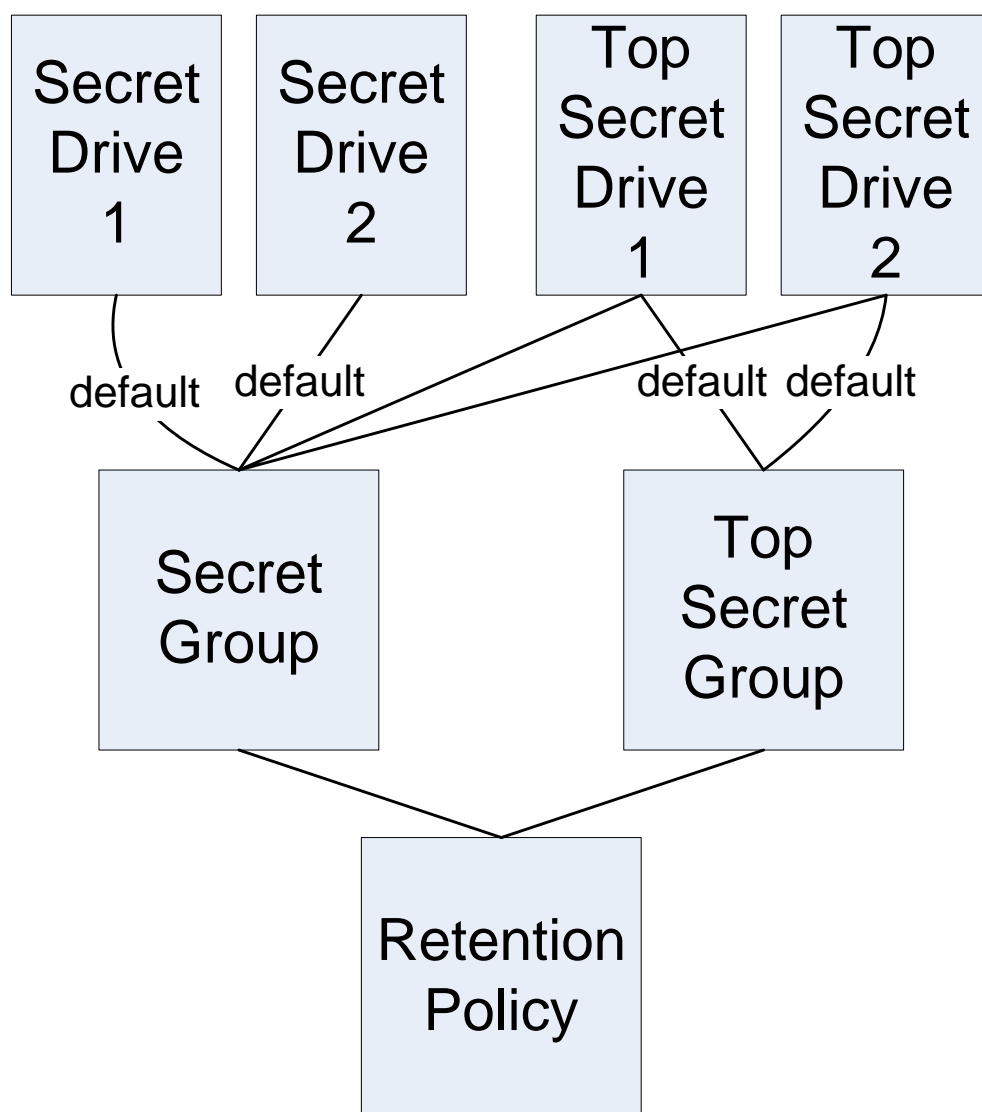
2. Click the Yes button to delete the Key Policy. The Key Policy is removed from the database. You are returned to the Key Policy List screen, where the Key Policy is removed from the list.

## Key Groups

A Key Group represents a data context that determines the Key Policy to which it applies and the Agents that can access it. When a Key is assigned to an agent and is first used for a Data Unit, it is associated with a Key Group. When you create a Key Group, you must select a Key Policy. The selected Key Policy is applied to Keys in that Key Group.

Agents are associated with Key Groups. An Agent has one or more keys groups that it is allowed to access. An Agent can only retrieve keys belonging to Key Groups it is allowed to access. An Agent may also have a default key group. When an agent allocates a new key, the key is placed in the agents default key group. An agent can only allocate new keys if it has a default key group.

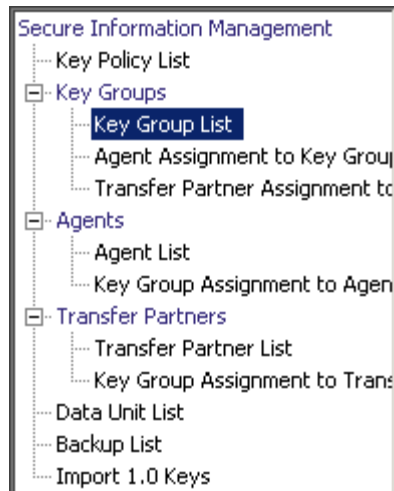
[FIGURE 6-1 on page 203](#) shows the relationship between Key Groups, Key Policies, Agents, and Data Units.



**FIGURE 6-1** Key Group Relationship with Key Policies, Agents, Data Units

## Key Groups Menu

The Key Groups menu includes the Key Group List menu option, which allows the Compliance Officer to manage Key Groups.



## Key Group List Menu

The Key Group List menu option gives the user the ability to:

- View Key Groups
- Create a Key Group
- Modify existing Key Groups
- Delete existing Key Groups



## Viewing Key Groups

To view all Key Groups:

1. From the Key Groups menu, select **Key Group List**. The Key Group List screen is displayed.

Key Group List

Filter: Key Group ID ▾ = ▾  +

Use Refresh Reset | < << >> >

Results in page: 2 (last page)

| Key Group ID ▲ | Description                 | Key Policy ID |
|----------------|-----------------------------|---------------|
| Key Group 1    | This is the first Key Group | MyKeyPolicy   |
| MyKeyGroup     | This is a key group         | MyKeyPolicy   |

Details... Create... Delete

You can scroll through the database and filter through the Key Group list by any of the following keys:

- Key Group ID
- Description
- Key Policy ID.

The Use button applies the filter to the displayed list for the Key Group.

The fields and their descriptions are given below:

### Filter:

Select filter options to filter the displayed list of Key Groups. Only Key Groups that satisfy all filters will be displayed.

### Filter Attribute combo box:

Click the down-arrow and select an attribute to filter by. Possible values are:

- Key Group ID
- Description
- Key Policy ID.

**Filter Operator box:**

Click the down-arrow and select the filter operation to apply to the selected attribute. Possible values are:

- Equals =
- Not equal <>;
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty.

**Filter Value text box:**

Type a value to filter the selected attribute by.

**Filter Value combo box:**

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.



Click this button to add additional filters.



Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

**Use:**

Click this button to apply the selected filters to the displayed list and go to the first page.

**Refresh:**

Click this button to refresh the displayed list. This does not apply filters selected since the last Use or Reset, and does not change the page of the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of items that can be displayed on the current page. Appends “(last page)” to the number of items if you are at the end of the list. The maximum number of items displayed on a page is defined by the Query Page Size value on the Options dialog.

**Key Group ID**

Displays the unique identifier that distinguishes each Key Group. This value can be between 1 and 64 (inclusive) characters. The Key Group ID cannot be changed once it is defined.

**Description**

Describes the Key Group. This value can be between 1 and 64 (inclusive) characters.

**Key Policy ID**

Displays a unique identifier for an existing Key Policy that applies for every Data Unit in the Key Group.

The Key Policy ID for an existing Key Group cannot be changed. This is to avoid a change affecting a large number of keys.

If you want to create a Key Group, click the Create button. For more information, refer to [“Creating a Key Group” on page 208](#).

If you want to view/modify a Key Group, highlight the Key Group and click the Details button. For more information, refer to [“Viewing/Modifying a Key Group’s Details” on page 210](#).

If you want to delete a Key Group, click the Delete button. For more information, refer to [“Deleting a Key Group” on page 211](#).

## Creating a Key Group

To create a new Key Group:

1. From the Key Group List screen, click the Create button. The Create Key Group dialog box is displayed.

A screenshot of the 'Create Key Group' dialog box. It has a title bar with the text 'Create Key Group' and a close button (X). The dialog contains three input fields: 'Key Group ID:' with a text box, 'Description:' with a text box, and 'Key Policy ID:' with a dropdown menu showing 'Please Select a Key Policy'. At the bottom are two buttons: 'Save' and 'Cancel'.

2. Complete the following parameters:

### Key Group ID

Type a value that identifies the Key Group. This value can be between 1 and 64 (inclusive) characters.

### Description

Type a value that describes the Key Group. This value can be between 1 and 64 (inclusive) characters.

### Key Policy ID

Click the down-arrow and select the Key Policy with which you want to associate this Key Group. When creating a new Key Group, existing Key Policies are displayed.

3. Click the Save button. The new Key Group is created and saved in the database and is displayed in the Key Group List screen. It can now be used by Data Units, Agents, etc.

Key Group List

Filter: Key Group ID ▾ = ▾  +

Use Refresh Reset | < << >>

Results in page: 3 (last page)

| Key Group ID ▴  | Description                 | Key Policy ID |
|-----------------|-----------------------------|---------------|
| Customer Rec... | Evaluation Lists            | MyKeyPolicy   |
| Key Group 1     | This is the first Key Group | MyKeyPolicy   |
| MyKeyGroup      | This is a key group         | MyKeyPolicy   |

Details... Create... Delete

## Viewing/Modifying a Key Group's Details

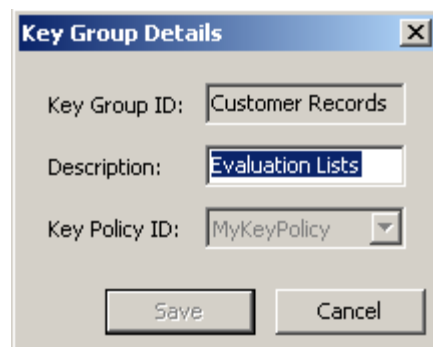
---

**Note** – If you are not a Compliance Officer, when you view a Key Group's detailed information, all fields, including the Save button are disabled.

---

To modify a Key Group:

1. From the Key Group List screen, double-click a Key Group entry for which you want more information or highlight a Key Group entry and click the Details button. The Key Group Details dialog box is displayed.

A screenshot of the 'Key Group Details' dialog box. It has a title bar with the text 'Key Group Details' and a close button (X). Inside the dialog, there are three fields: 'Key Group ID:' with the value 'Customer Records', 'Description:' with the value 'Evaluation Lists', and 'Key Policy ID:' with a dropdown menu showing 'MyKeyPolicy'. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

The following parameters are displayed:

**Key Group ID:**

Uniquely identifies the Key Group. This field is read-only.

**Description:**

Type a value that describes the Key Group. This value can be between 1 and 64 (inclusive) characters. This field can be blank.

**Key Policy ID:**

Displays a unique identifier for an existing Key Policy that is associated with the Key Group and all the Keys in the Key Group. This field is read-only.

2. The Description field is the only field that can be modified. When you are finished, click the Save button to save the changes. You are returned to the Key Group List screen.

## Deleting a Key Group

---

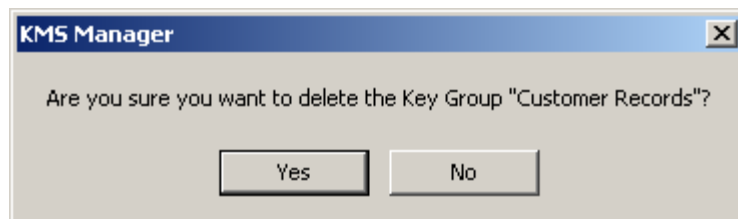
**Note** – You cannot delete a Key Group if it is active, that is, to which Agents or Data Units are assigned.

---

To delete a Key Group:

1. From the Key Groups List screen, highlight the Key Group you want to delete and click the Delete button. The following Confirmation dialog box is displayed, prompting you to confirm that you want to delete the selected Key Group.

A Key Group can only be deleted if it is not used by any key and is not associated with any Agent.



2. Click the Yes button to delete the Key Group. The Key Group and its associated entries are deleted from the database. You are returned to the Key Groups List screen, where the Key Group is no longer listed.

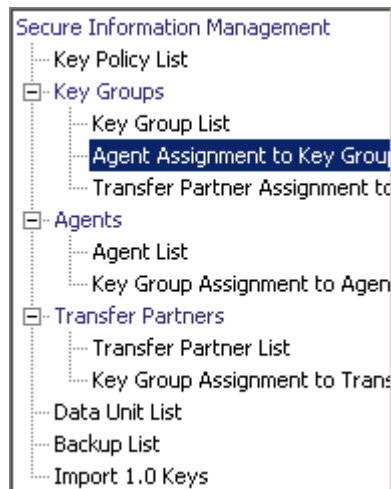
## Agent Assignment to Key Groups Menu

The Agent Assignment to Key Groups menu option gives the user the ability to assign Agents to Key Groups. When you assign Agents to Key Groups, it determines the storage devices that the Agent can access. It is the converse of the Key Group Assignment menu option under the Agents menu, both accomplishing the same result.

---

**Important** – You must set a default Key Group for an Agent before that Agent can allocate keys.

---



To view Agents assignments, from the Key Groups menu, select Agent Assignment to Key Groups. The Agent Assignment to Key Groups screen is displayed.



Agent Assignment to Key Groups

| Key Groups   | Agents Allowed Access | Agents Not Allowed Access  |
|--|-----------------------|--|
| <div>Customer Records</div> <div>Key Group 1</div> <div>MyKeyGroup</div> |                       | <div>MyAgent</div> <div>MyAgent1</div> <div>SO-owned Agent</div> |

<


>

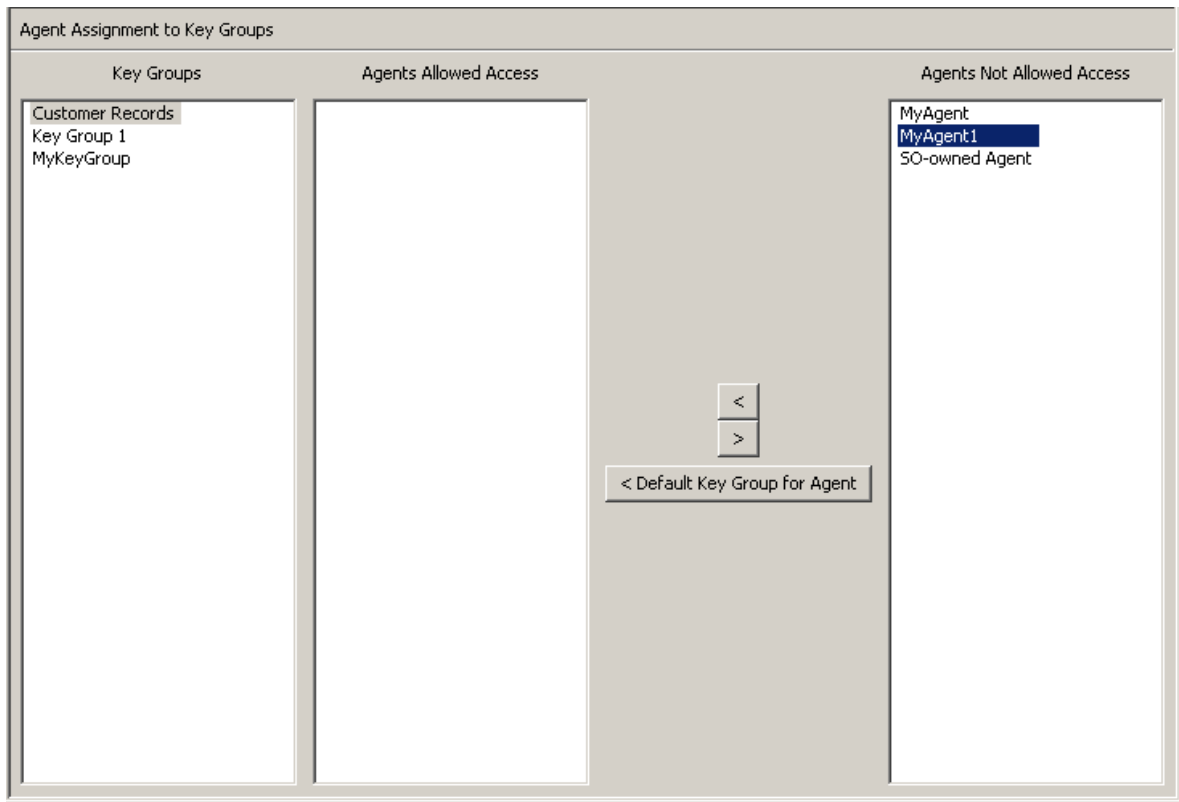
< Default Key Group for Agent

The Key Groups column lists the Key Groups. The Agents Allowed Access column lists the Agents that are assigned to the selected Key Group(s). The Agents Not Allowed Access column lists the Agents that are not assigned to the selected Key Group(s).

## Assigning an Agent to a Key Group

To assign an Agent to a Key Group:

1. In the Key Groups column, highlight the Key Group you want. In the Agents Not Allowed Access column, highlight the Agent you want to add and click the Move to  button.



2. The selected Agent is moved to the Agents Allowed Access column, indicating that the Agent is successfully added to the selected Key Group's Agent list.

Agent Assignment to Key Groups

| Key Groups                                    | Agents Allowed Access | Agents Not Allowed Access |
|---|-----------------------|---------------------------|
| Customer Records<br>Key Group 1<br>MyKeyGroup | MyAgent1              | MyAgent<br>SO-owned Agent |

To assign Agents to a Key Group and set the Default Key Group:


1. From the Agent Assignment to Key Groups screen, select the Key Group you want in the Key Groups list.
2. In the Agents Not Allowed Access list, select one or more Agents you want to add and set the Default Key Group for.
3. Click the Default Key Group for Agent button. The selected Agents are moved to the Agents Allowed Access list and their Default Key Group is set to the Key Group. The Agents are now allowed access to the Key Group.

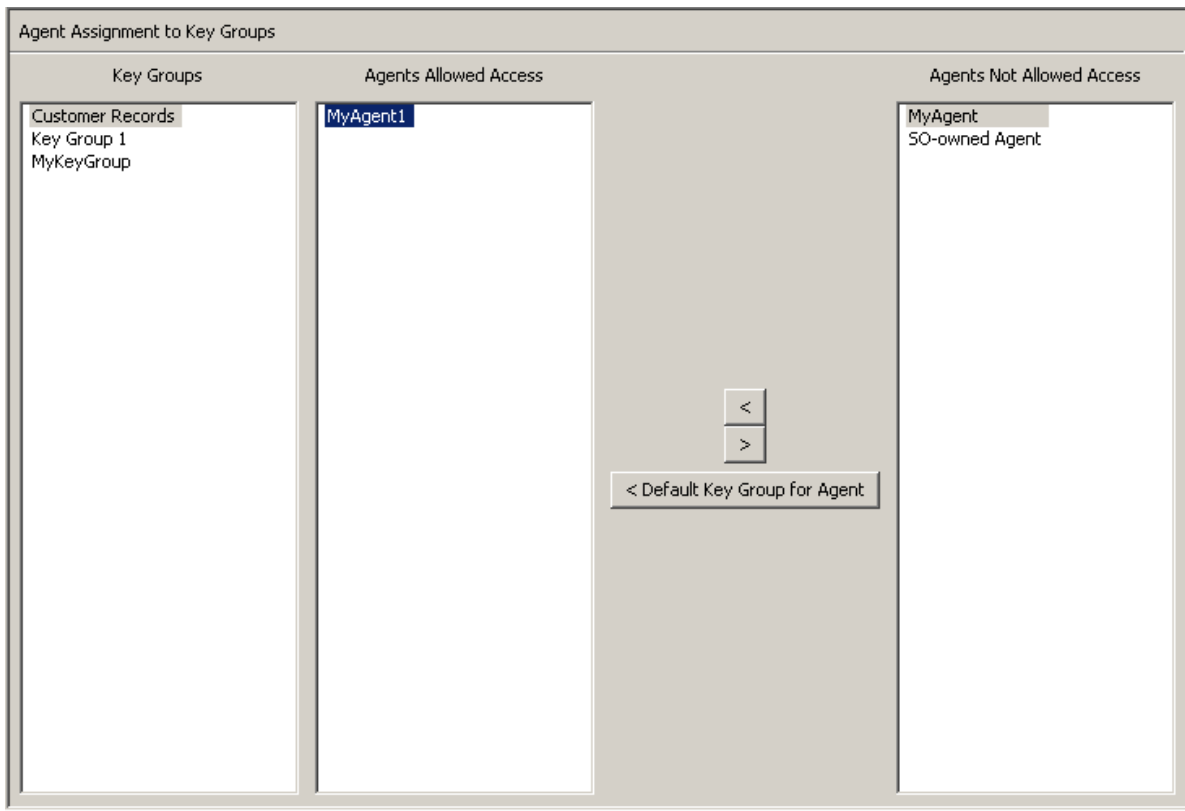
To set the Default Key Group for already assigned Agents:

1. From the Agent Assignment to Key Groups screen, select the Key Group you want in the Key Groups list.
2. In the Agents Allowed Access list, select one or more Agents that do not have the selected Key Group as their Default Key Group.
3. Click the Default Key Group for Agent button. The selected Agents' Default Key Group is set to the Key Group.

## Removing an Agent from a Key Group

To remove an Agent from a Key Group's Agent list:

1. In the Key Groups column, highlight the Key Group you want. In the Agents Allowed Access column, highlight the Agent you want to remove, and click the Move from  button.



2. The selected entry is removed from the Agents Allowed Access column and is listed in the Agents Not Allowed Access column. It is no longer assigned to the selected Key Group.

Agent Assignment to Key Groups

| Key Groups  | Agents Allowed Access | Agents Not Allowed Access  |
|---|-----------------------|--|
| <div>Customer Records</div> <div>Key Group 1</div> <div>MyKeyGroup</div>    |                       | <div>MyAgent</div> <div>MyAgent1</div> <div>SO-owned Agent</div> |
| <div>&lt;</div> <div>&gt;</div> <div>&lt; Default Key Group for Agent</div> |                       |  |

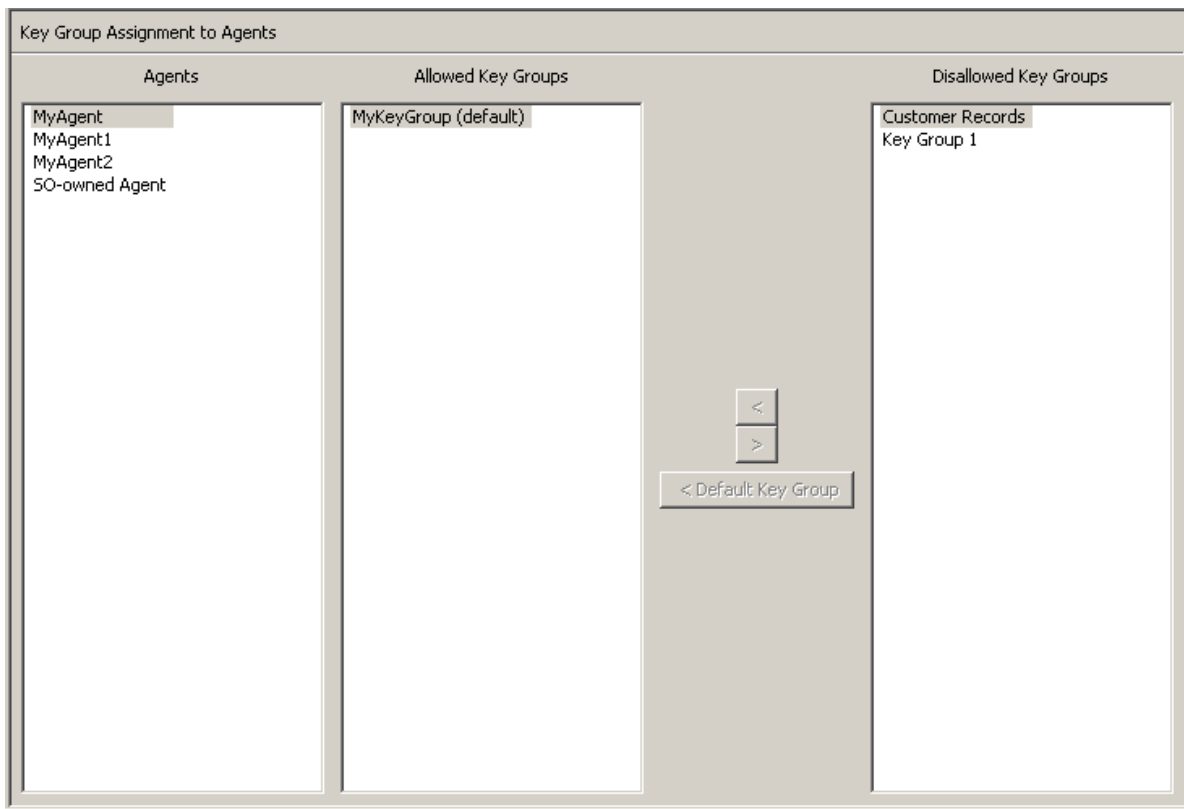
## Key Group Assignment to Agents Menu

The Key Group Assignment to Agents menu option allows you to assign Key Groups to Agents. It is the converse of the Agent Assignment to Key Groups menu option, both accomplishing the same result.



To view the Key Groups:

1. From the Agents menu, select Key Group Assignment. The Key Group Assignment to Agents screen is displayed.



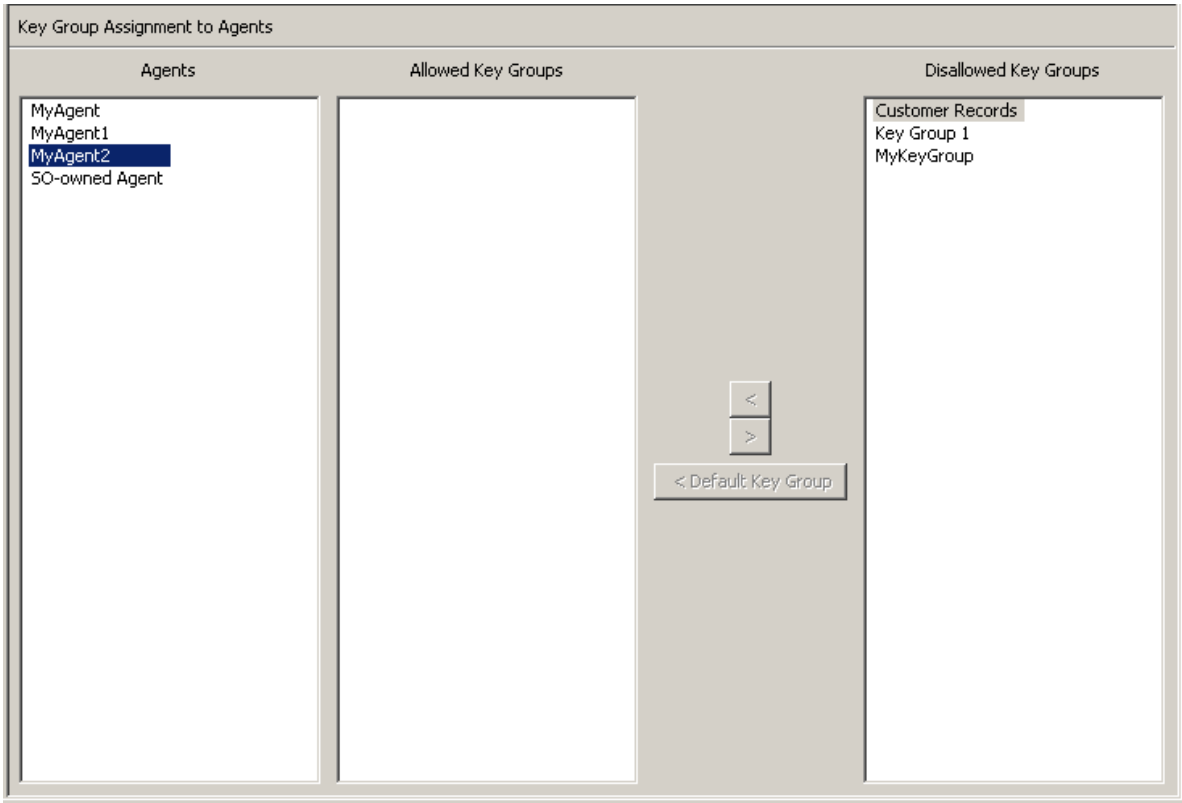
The image shows a software window titled "Key Group Assignment to Agents". It is divided into three main columns: "Agents", "Allowed Key Groups", and "Disallowed Key Groups".

- Agents column:** Contains a list of agents: "MyAgent", "MyAgent1", "MyAgent2", and "SO-owned Agent". "MyAgent" is currently selected and highlighted.
- Allowed Key Groups column:** Contains a list of key groups: "MyKeyGroup (default)".
- Disallowed Key Groups column:** Contains a list of key groups: "Customer Records" and "Key Group 1". "Customer Records" is currently selected and highlighted.

In the center, between the "Allowed" and "Disallowed" columns, there are two small buttons: "<" (left arrow) and ">" (right arrow). Below these buttons is a button labeled "< Default Key Group".

The Agents column lists the Agents in the database. The Allowed Key Groups column lists the Key Groups which the Agent can access. The Disallowed Key Groups column lists the Key Groups which the Agent cannot access.


2. Clicking an Agent entry displays the Key Group that are members or non-members of the selected Agent.

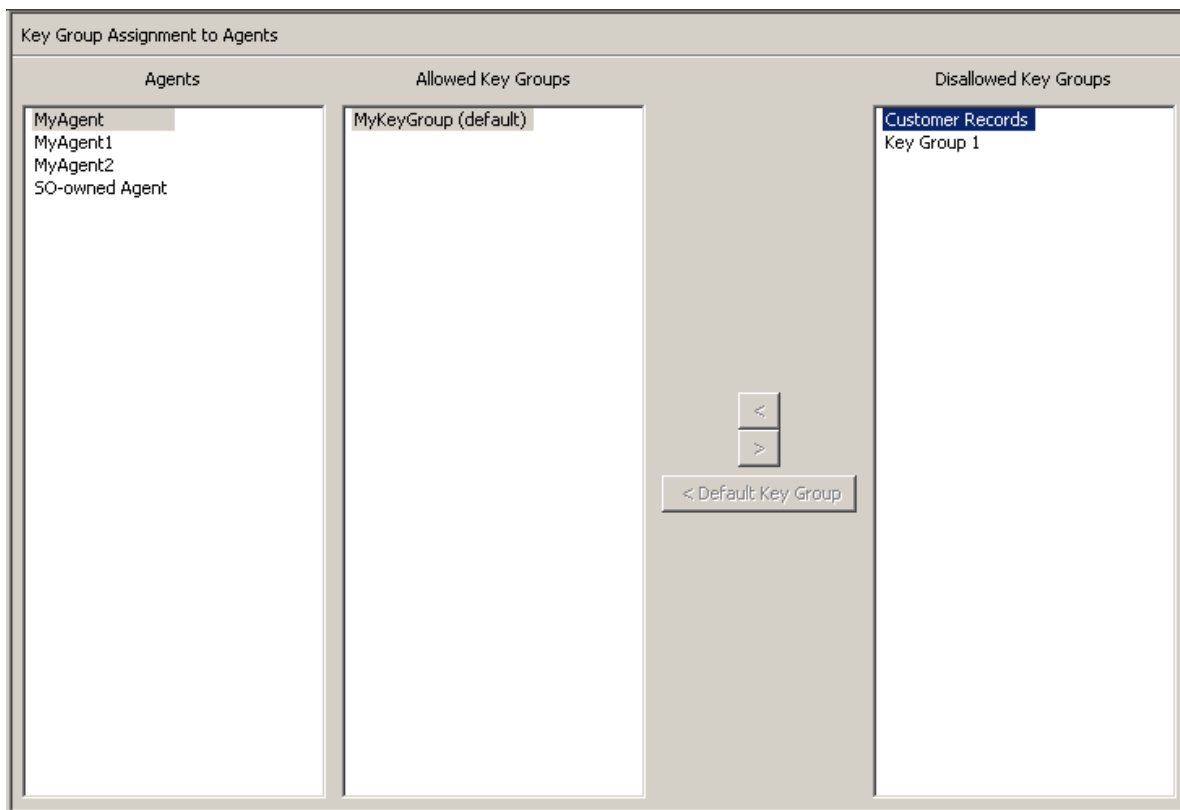




## Assigning a Key Group to an Agent

To assign a Key Group to an Agent:

1. From the Key Group Assignment to Agents screen, in the Agents column, highlight the Agent you want. In the Disallowed Key Groups column, highlight the Key Group you want to add and click the Move to  button.



The screenshot shows the 'Key Group Assignment to Agents' interface. It consists of three main columns: 'Agents', 'Allowed Key Groups', and 'Disallowed Key Groups'. In the 'Agents' column, 'MyAgent' is selected. In the 'Disallowed Key Groups' column, 'Customer Records' is selected. In the center, there are two buttons: a left arrow and a right arrow. Below these is a button labeled '< Default Key Group'.

| Agents  | Allowed Key Groups   | Disallowed Key Groups           |
|---|----------------------|---------------------------------|
| MyAgent<br>MyAgent1<br>MyAgent2<br>SO-owned Agent | MyKeyGroup (default) | Customer Records<br>Key Group 1 |

2. The selected entry is moved to the Allowed Key Groups column and the Key Group is successfully added to the selected Agent.

Key Group Assignment to Agents

| Agents         | Allowed Key Groups   | Disallowed Key Groups |
|----------------|----------------------|-----------------------|
| MyAgent        | Customer Records     | Key Group 1           |
| MyAgent1       | MyKeyGroup (default) |                       |
| MyAgent2       |                      |                       |
| SO-owned Agent |                      |                       |

< >

< Default Key Group

To assign a Key Group to an Agent as the Default Key Group:

1. From the Key Group Assignment to Agents screen, select the Agent you want in the Agents list.
2. In the Disallowed Key Groups list, select one Key Group you want to add and set the Default Key Group for.
3. Click the Default Key Group button. The selected Key Group is moved to the Allowed Key Groups list and is set as the Default Key Group for the Agent. The Agent is now allowed access to the Key Group.


To set an already assigned Key Group to the Default Key Group:

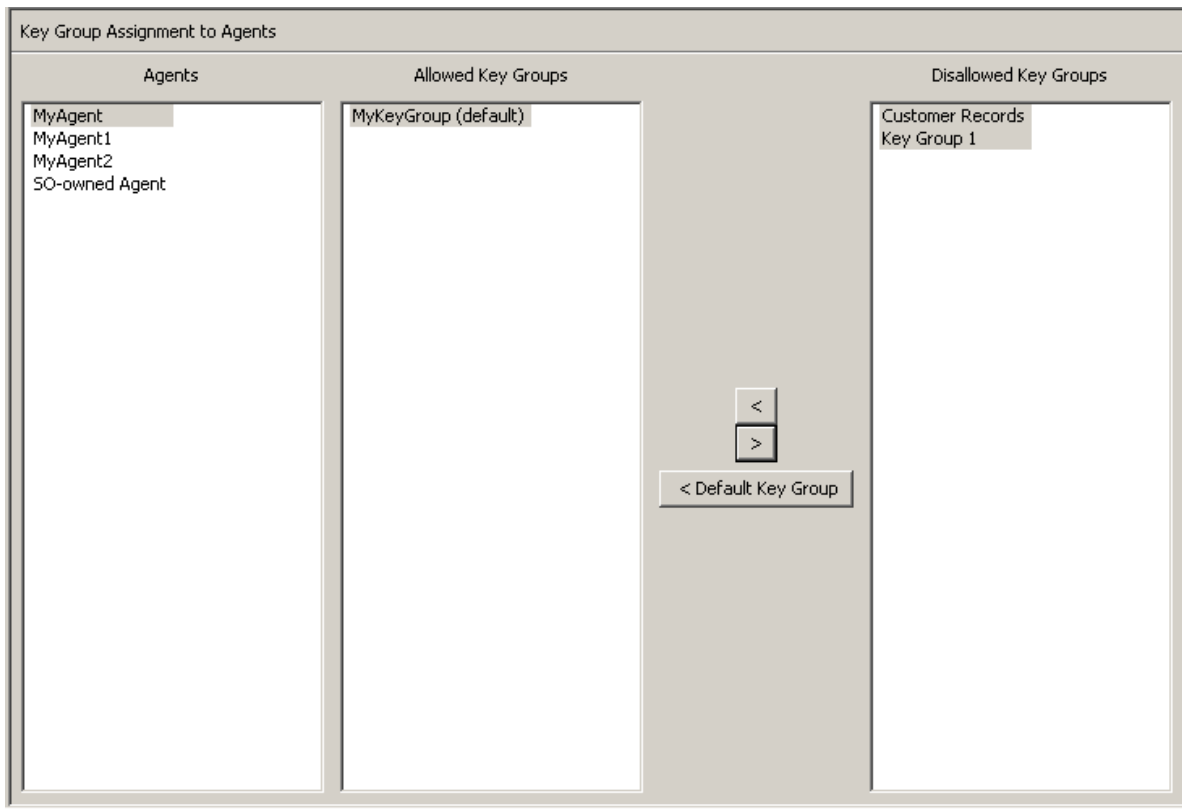
1. From the Key Group Assignment to Agents screen, select the Agent you want in the Agents list.
2. In the Allowed Key Groups list, select one Key Group that is not the Default Key Group for the Agent.

Click the Default Key Group button. The Agent's Default Key Group is set to the selected Key Group.

## Removing a Key Group from an Agent

To remove a Key Group to an Agent:

1. From the Key Group Assignment to Agents screen, in the Agents column, highlight the Agent you want. In the Allowed Key Groups column, highlight the Key Group you want to remove and click the Move from  button.



The screenshot shows the 'Key Group Assignment to Agents' interface. It consists of three main columns: 'Agents', 'Allowed Key Groups', and 'Disallowed Key Groups'. In the 'Agents' column, 'MyAgent' is highlighted. In the 'Allowed Key Groups' column, 'MyKeyGroup (default)' is highlighted. In the 'Disallowed Key Groups' column, 'Customer Records' and 'Key Group 1' are listed. Between the columns are two buttons: '<' and '>'. Below these buttons is a button labeled '< Default Key Group'.

| Agents         | Allowed Key Groups   | Disallowed Key Groups |
|----------------|----------------------|-----------------------|
| MyAgent        | MyKeyGroup (default) | Customer Records      |
| MyAgent1       |                      | Key Group 1           |
| MyAgent2       |                      |                       |
| SO-owned Agent |                      |                       |

2. The selected entry is removed from the Allowed Key Groups column to the Non-member of Info. Groups column and is no longer assigned to the Agent.

Key Group Assignment to Agents

Agents

MyAgent  
MyAgent1  
MyAgent2  
SO-owned Agent

Allowed Key Groups

Disallowed Key Groups

Customer Records  
Key Group 1  
MyKeyGroup

<

>

< Default Key Group

## Key Group Assignment to Transfer Partners Menu

The Key Group Assignment to Transfer Partners menu option allows you to assign Key Groups to Transfer Partners.



## Viewing Key Group Assignments


To view Key Group assignments, from the Transfer Partners menu, select Key Group Assignment to Transfer Partners. The following screen is displayed.

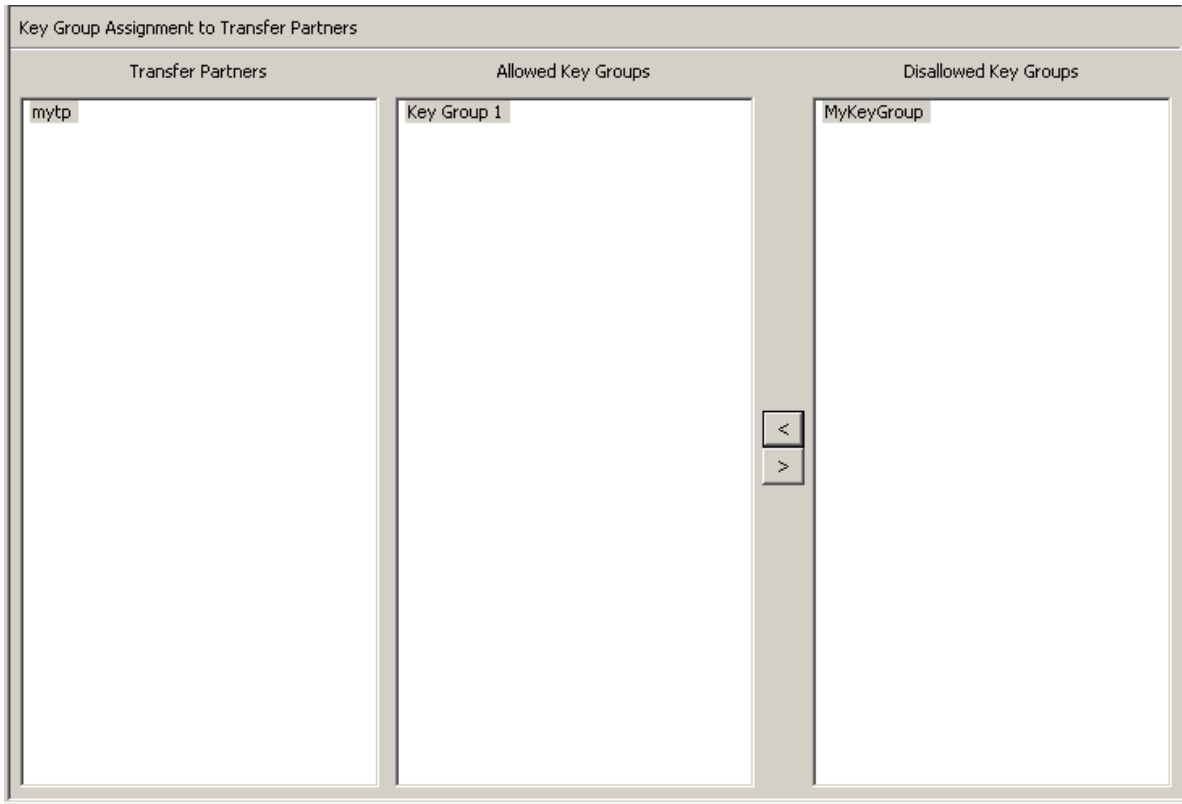
| Transfer Partners | Allowed Key Groups | Disallowed Key Groups     |
|-------------------|--------------------|---------------------------|
| mytp              |                    | Key Group 1<br>MyKeyGroup |

The screen shows the Key Groups that can access a Transfer Partner. The Allowed Key Groups column lists the Key Groups assigned to the selected Transfer Partner. The Disallowed Key Groups column displays the Key Groups not assigned to the Transfer Partner.

## Adding a Key Group to a Transfer Partner

To add a Key Group to a Transfer Partner list:

1. In the Transfer Partners column, highlight the Transfer Partner you want to affect. In the Disallowed Key Groups column, highlight the Key Group you want to add and click the Move to  button.



The dialog box titled "Key Group Assignment to Transfer Partners" contains three columns: "Transfer Partners", "Allowed Key Groups", and "Disallowed Key Groups".


- The "Transfer Partners" column contains the text "mytp".
- The "Allowed Key Groups" column contains the text "Key Group 1".
- The "Disallowed Key Groups" column contains the text "MyKeyGroup".

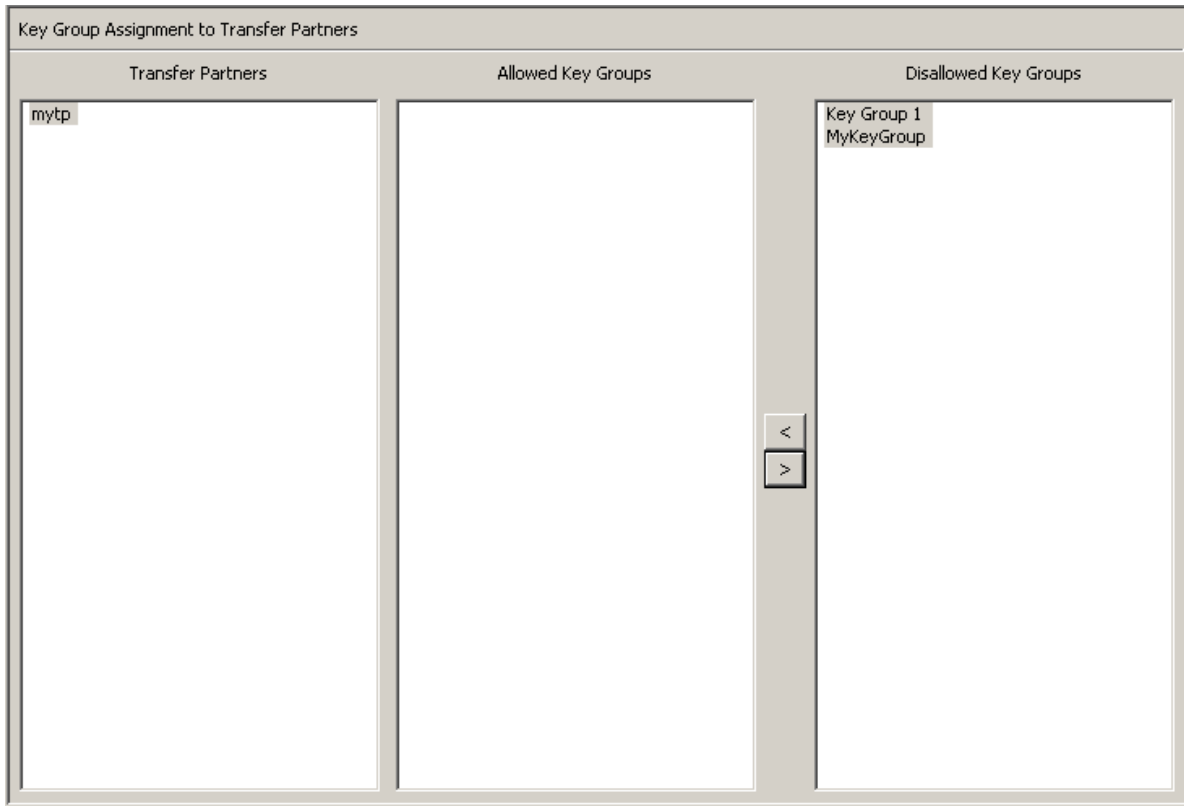
Between the "Allowed Key Groups" and "Disallowed Key Groups" columns, there are two buttons: a left-pointing arrow (<) and a right-pointing arrow (>).

2. The selected Key Group is moved to the Allowed Key Groups column, indicating that the Transfer Partner can now access that Key Group.

## Removing a Key Group from a Transfer Partner

To remove a Key Group list from a Transfer Partner:

1. In the Transfer Partners column, highlight the Transfer Partner you want to affect. In the Allowed Key Groups column, highlight the Key Group you want to remove and click the Move from  button.

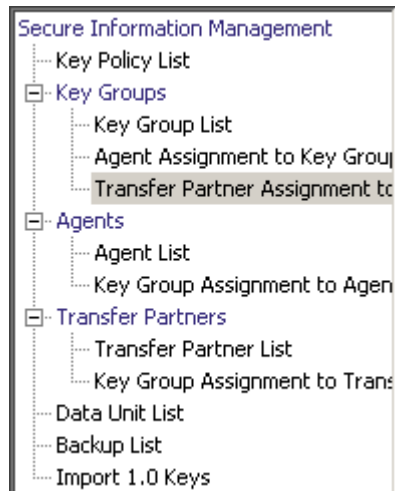


2. The selected Key Group is moved to the Disallowed Key Groups column, indicating that the Transfer Partner cannot access that Key Group.



## Transfer Partner Assignment to Key Groups Menu

The Transfer Partner Assignment to Key Groups menu allows you to add a key transfer partner to the set of key transfer partners that are permitted access to a specific key group.



## Viewing Transfer Group Assignments

To view Transfer Group assignments, from the Key Groups menu, select Transfer Partner Assignment to Key Groups. The following screen is displayed.


Transfer Partner Assignment to Key Groups

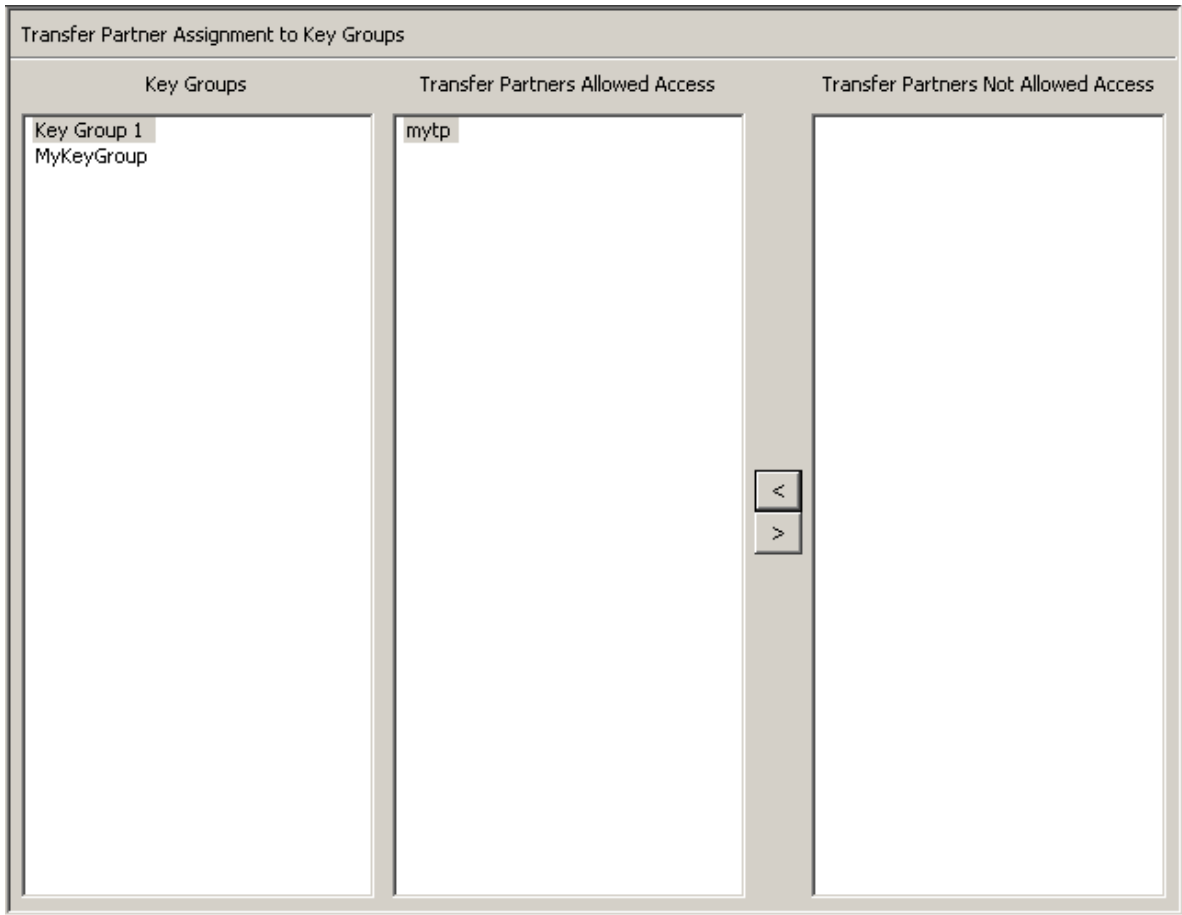
| Key Groups                | Transfer Partners Allowed Access | Transfer Partners Not Allowed Access |
|---------------------------|----------------------------------|--------------------------------------|
| Key Group 1<br>MyKeyGroup |                                  | mytp                                 |

The screen shows the Transfer Partners that can access a Key Group. The Transfer Partners Allowed Access column lists the Transfer Partners assigned to the Key Group. The Transfer Partners Not Allowed Access column displays the Transfer Partners not assigned to the Key Group.

## Adding a Transfer Partner to a Key Group

To add a Transfer Partner to a Key Group:

1. In the Key Groups column, highlight the Key Group you want to affect. In the Transfer Partners Allowed Access column, highlight the Key Group you want to add and click the Move to  button.



The dialog box titled "Transfer Partner Assignment to Key Groups" contains three columns: "Key Groups", "Transfer Partners Allowed Access", and "Transfer Partners Not Allowed Access".


| Key Groups                | Transfer Partners Allowed Access | Transfer Partners Not Allowed Access |
|---------------------------|----------------------------------|--------------------------------------|
| Key Group 1<br>MyKeyGroup | mytp                             |                                      |

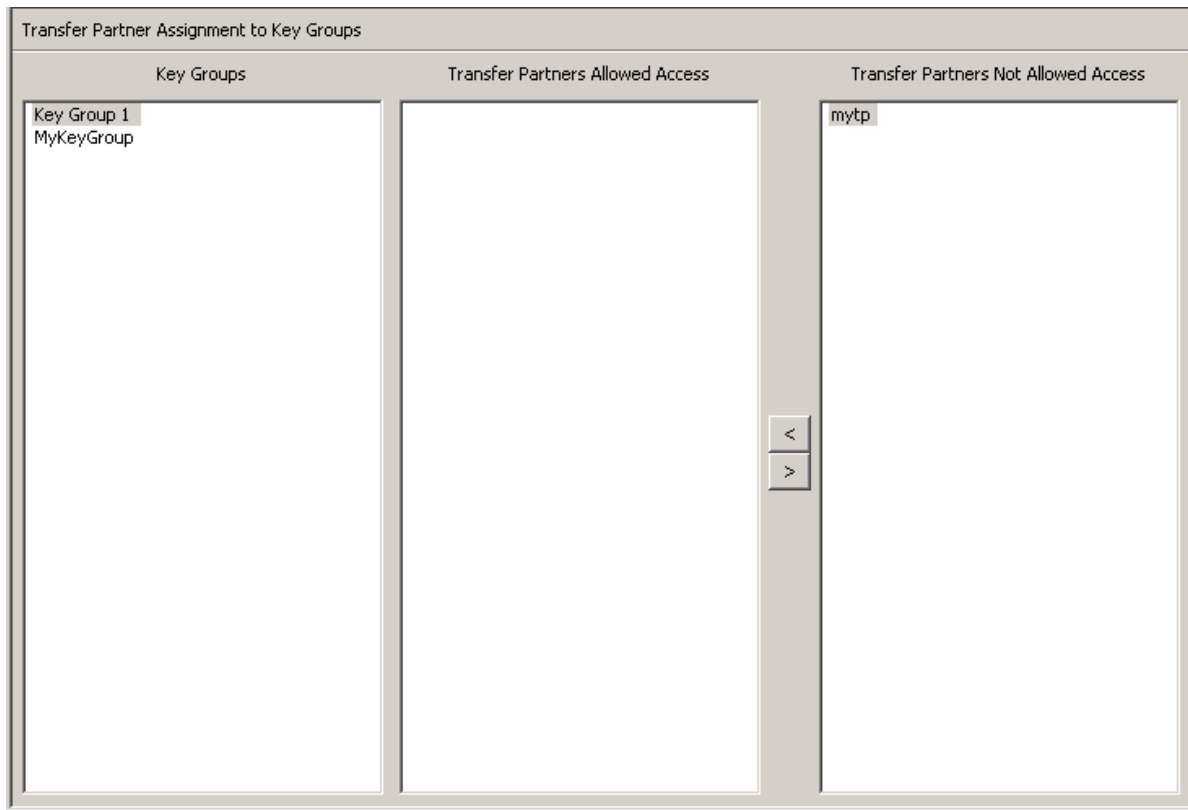
Below the columns are two buttons: "<" and ">".

2. The selected Transfer Partner is moved to the Transfer Partners Allowed Access column, indicating that the Key Group can now access that Transfer Partner.

## Removing a Transfer Partner from a Key Group

To remove a Transfer Partner from a Key Group:

1. In the Key Groups column, highlight the Key Group you want to affect. In the Transfer Partners Allowed Access column, highlight the Transfer Partner you want to remove and click the Move from  button.

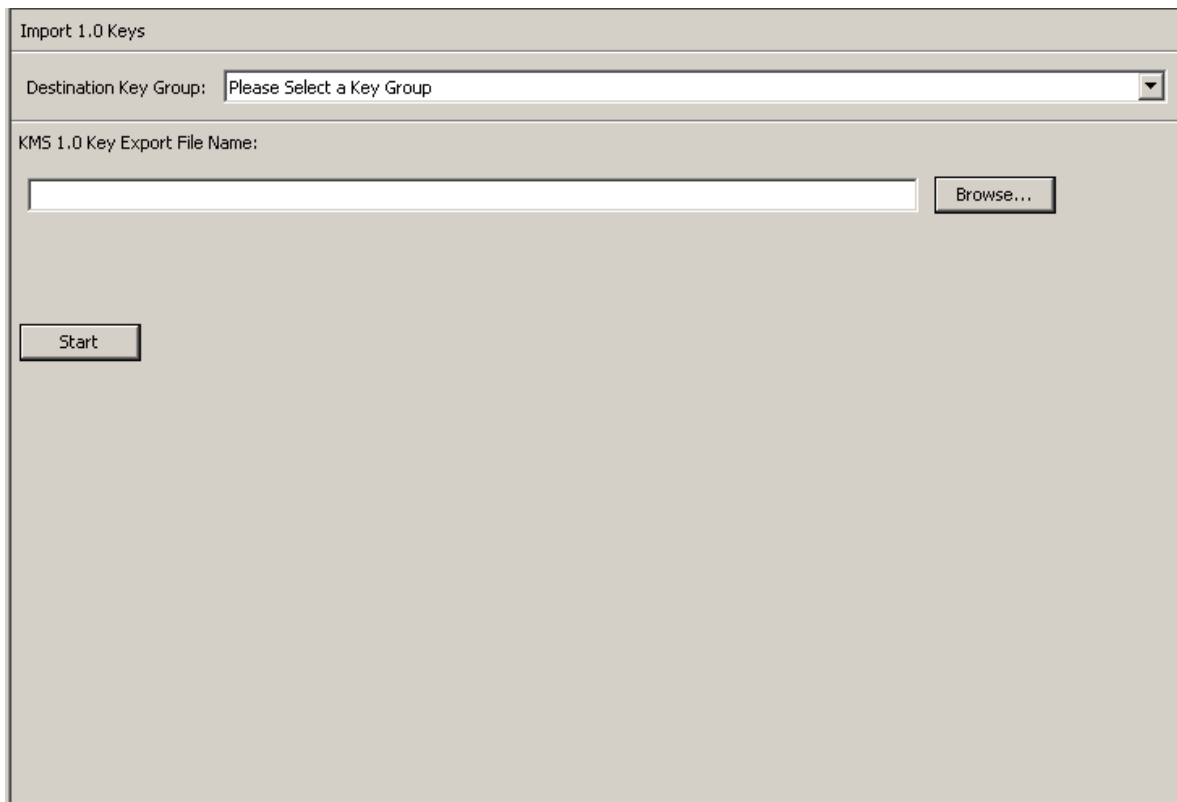


2. The selected Transfer Partner is moved to the Transfer Partners Not Allowed Access column, indicating that the Key Group cannot access that Transfer Partner.

## Importing a KMS 1.0 Key Export File

To import a KMS 1.0 Key Export file to the KMA and to create a new Key for each Key in this file:

1. Go to the KMS 1.2 system and export the keys into a file. Only keys exported from KMS 1.2 systems can be imported. KMS 1.0 and 1.1 systems must be upgraded to 1.2 before exporting keys.
2. From the Secure Information Management menu, select **Import 1.0 Keys**.



Import 1.0 Keys

Destination Key Group: Please Select a Key Group

KMS 1.0 Key Export File Name:

Browse...

Start

3. Complete the following parameters:

**Destination Key Group**

Select the Destination Key Group into which these keys will be imported.

**KMS 1.0 Key Export File Name**

Type the name of the KMS 1.0 Key Export file.

**Browse**

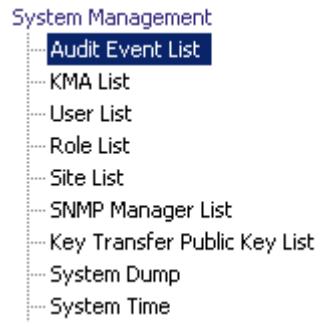
Click this button to locate the file.

**Start**

Click this button to begin to upload the KMS 1.0 keys file to the KMA, and a new Key is created for each Key it contains. Each new Key is associated with the Key Group you selected. Messages are displayed indicating when the file is uploaded and applied.

# Audit Event List Menu

The Audit Event List menu gives you the ability to view the Audit Log events.



## Viewing Audit Logs

To view the Audit Log events:

From the System Management menu, select Audit Event List. The Audit Event List screen is displayed.

Audit Event List

Filter: 

Created Date

 Set Date to  Set Date +

Don't Show Short Term  Use Refresh Reset | < << >> >

Results in page: 20

| Created Date ▾      | Operation                     | Severity | Condition                    | Message Values   |
|---------------------|-------------------------------|----------|------------------------------|--|
| 1/5/2008 1:38:29 PM | Retrieve Entity Certificate   | Success  | Success                      | Certificate Serial Number = 151C5F81291373F000000000...    |
| 1/5/2008 1:38:23 PM | Retrieve Root CA Certificate  | Success  | Success                      |  |
| 1/5/2008 1:38:15 PM | Retrieve Entity Certificate   | Error    | Invalid Challenge response   |  |
| 1/5/2008 1:38:09 PM | Retrieve Root CA Certificate  | Success  | Success                      |  |
| 1/4/2008 4:44:25 PM | Retrieve Entity Certificate   | Success  | Success                      | Certificate Serial Number = 151C5F81291373F000000000...    |
| 1/4/2008 4:44:25 PM | Retrieve Root CA Certificate  | Success  | Success                      |  |
| 1/4/2008 2:48:39 PM | List Key Transfer Public Keys | Success  | Success                      |  |
| 1/4/2008 2:48:28 PM | Create Key Transfer Key Pair  | Success  | Success                      |  |
| 1/4/2008 2:43:29 PM | List Key Transfer Public Keys | Success  | Success                      |  |
| 1/4/2008 2:42:56 PM | Create Key Transfer Key Pair  | Success  | Success                      |  |
| 1/4/2008 2:42:29 PM | List Key Transfer Public Keys | Success  | Success                      |  |
| 1/4/2008 2:41:35 PM | List Key Transfer Public Keys | Success  | Success                      |  |
| 1/4/2008 2:41:18 PM | Create Key Transfer Key Pair  | Success  | Success                      |  |
| 1/4/2008 2:40:12 PM | List Key Transfer Public Keys | Success  | Success                      |  |
| 1/4/2008 2:38:52 PM | Retrieve Entity Certificate   | Success  | Success                      | Certificate Serial Number = 151C5F81291373F000000000...    |
| 1/4/2008 2:38:52 PM | Retrieve Root CA Certificate  | Success  | Success                      |  |
| 1/4/2008 2:28:03 PM | List Key Transfer Public Keys | Success  | Success                      |  |
| 1/4/2008 2:27:59 PM | Create Transfer Partner       | Success  | Success                      | Transfer Partner ID = mytp, Description = a descr, Cont... |
| 1/4/2008 2:27:38 PM | Create Transfer Partner       | Error    | Public Key ID already exists | Transfer Partner ID = mytp, Description = a descr, Cont... |
| 1/4/2008 2:26:22 PM | Retrieve Entity Certificate   | Success  | Success                      | Certificate Serial Number = 151C5F81291373F000000000...    |

Details...

You can also scroll through the database and filter the Audit Event list by any of the following keys:

- Created Date
- Operation
- Severity
- Condition
- Entity ID
- Entity Network Address
- KMA ID
- KMA Name
- Class
- Retention Term
- Audit Log ID.

The **Use** button applies the filter to the displayed list for the Audit Log.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- Created Date
- Operation
- Severity
- Condition
- Entity ID
- Entity Network Address
- KMA Name
- Class
- Retention Term
- Audit Log ID

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Empty
- Not empty

**Filter Value 1 box:**

If you selected the Date filter, click Set Date to specify start date and time. The value appears as a starting value of the filter key range. If you selected any other filter, type a value in this field.

**Filter Value 2 box:**

If you selected the Date filter, click Set Date to select an end date and time. The value appears as a ending value of the filter key range.

**Filter Value 3 box:**

Click the down-arrow and select one of the following filters:

- Don't Show Short Term
- Show All Retentions



**Created Date**

Displays the date and time that the Audit Event was created.

**Operation**

Displays the operation that resulted in the creation of the Audit Event record.

**Severity**

Indicates the severity of the condition if the operation was not successful. Possible values are Success (no error), Warning, or Error.

**Condition**

Indicates whether the operation was successful or not.

---

**Note** – Errors are highlighted in red; Warnings are highlighted in yellow. If you hover the cursor over an error message, a more detailed description of the error is displayed.

---

**Event Message**

Displays detailed information of the Audit Event entry.

**Entity ID**

Displays the user who performed the operation.

**Entity Network Address**

Displays the network address of the entity that generated the Audit Event.

**KMA ID**

Displays the Appliance that originally created the Audit Event entry.

**KMA Name**

Displays the user-supplied identifier that distinguishes each Appliance in a Cluster.

**Class**

Identifies the class of operations to which the Audit Event entry belongs. Possible values are:

- Agent Access Control Management Operations
- Agent Client Generated Audits
- Agent Management Operations
- Appliance Management Operations
- Audit Log Agent Operations
- Audit Log Management Operations
- Audit Log Operations
- Backup Management Operations
- CA Operations
- Cluster Client Communication
- Cluster Operations
- Communication and Authentication
- Console Security Management Operations
- Data Unit Agent Operations
- Data Unit Management Operations

- Discovery Operations
- Key Group Agent Operations
- Key Group Management Operations
- Key Policy Management Operations
- License Key Management Operations
- Local Management Operations
- Management Client Generated Audits
- Passphrase Agent Operations
- Replication Operations
- Retrieve Certificate Operations
- Role Management operations
- SNMP Management Operations
- Security Management Operations
- Security Parameter Management Operations
- Security Violation
- Site Management Operations
- System Messages
- User Management Operations.

#### **Retention Term**

Displays the defined length of time that the Audit Event record is retained. Possible values are and their descriptions are:

##### **Long Term**

Event records that must be stored for a lengthy period of time.

##### **Medium Term**

Event records that must be stored for a medium length period of time.

##### **Short Term**

Event records that must be stored for a short period of time.

#### **Audit Log Entry ID**

Displays a system-generated unique identifier that distinguishes each type of Audit Event entry.

#### **Audit Log ID**

Displays a system-generated unique identifier that distinguishes each Audit Event entry.

If you want more detailed information on an Audit Log, highlight the Audit Log and click the Details button. For more information, refer to [“Viewing Audit Log Details”](#) below.

Click the Export button to export the Audit Log. For more information, refer to [“Exporting an Audit Log”](#) on page 240.

## Viewing Audit Log Details

To view Audit Log details:

1. From the Audit Event List screen, select the Audit Log entry on which you want more information and click the Details button or double-click the entry. The Audit Event Details dialog box is displayed, where all fields are disabled, except for the Previous, Close, and Next buttons.

|                         |                                  |
|-------------------------|----------------------------------|
| Audit Log ID:           | A97AE3858F84A6B10000000000000474 |
| KMA ID:                 | A97AE3858F84A6B1                 |
| KMA Name:               | Drumguish                        |
| Audit Log Entry ID:     | 000001000000                     |
| Class:                  | System Messages                  |
| Retention Term:         | Medium Term                      |
| Operation:              | Start Database                   |
| Severity:               | Success                          |
| Condition:              | Success                          |
| Created Date:           | 10/7/2008 2:21:21 PM             |
| Entity ID:              |                                  |
| Entity Network Address: |                                  |
| Message Values:         |                                  |
| Solution:               | No recommended action            |

Previous Close Next

2. Click the Previous or Next buttons to access the previous or next Audit Event, or the Close button to return to the Audit Event List screen.

## Exporting an Audit Log

The Export function allows the user to export all or specific Audit Log entries to a text file on the user's workstation. The user can then bring up the file in a spreadsheet application.

To export an Audit Log:

1. From the Audit Event List screen, either select `Save Report...` from the View menu or press Ctrl-S.
2. When you are finished, click the Start button to initiate the export process. If you have filtered the entries in the Audit Event List screen, only those entries are exported. Otherwise, all audit events are exported.
3. When the export process is completed, the number of Audit Logs that have been exported is shown at the bottom of the dialog box.
4. Click the Close button to close this dialog box and return to the Audit Event List screen.

---

## Data Units Menu

For procedures on using the Data Units menu, refer to [“Data Unit List Menu” on page 258](#).

## Other Functions

A Compliance Officer can also:

- View the Audit Event List
- View the System Time
- Lock/Unlock KMA status.

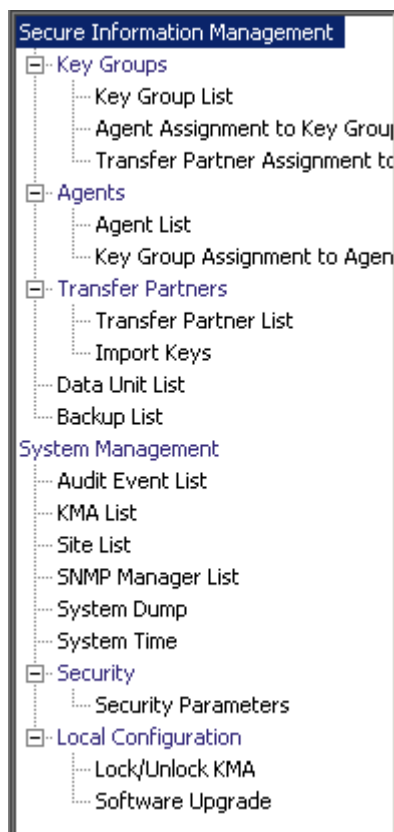
For procedures on viewing the these functions, refer to [Chapter 5, “Security Officer Operations”](#).

## Operator Operations

This chapter describes the operations that a user who has been given an Operator role can perform. If you have been assigned multiple roles, refer to the appropriate chapter for instructions on performing the specific role.

### Operator Role

As the Operator, you are responsible for managing the day-to-day operations of the system.



## Key Groups Menu

The Key Groups menu contains the following menu options.



It allows you to:

- View a list of Key Groups
- View Agent to Key Group Assignments
- View Transfer Partner to Key Group Assignments.

### Key Group List

The Key Group List menu option gives the user the ability to manage your Key Group. For procedures, refer to [“Key Group List Menu” on page 204](#).

### Agent Assignment to Key Groups

The Agent Assignment to Key Groups menu option gives the user the ability to view Agents to Key Groups. For procedures, refer to [“Agent Assignment to Key Groups Menu” on page 212](#).

### Transfer Partner Assignment to Key Groups

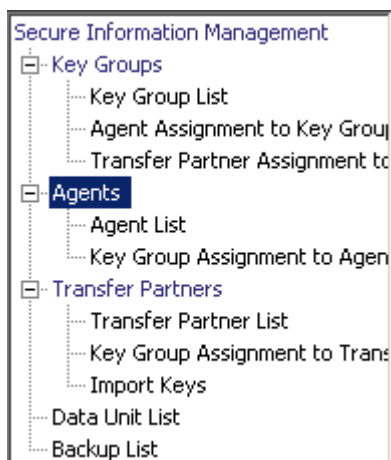
The Transfer Partner Assignment to Key Groups option allows the user to view a key transfer partner to the set of key transfer partners that are allowed access to a specific key group. For procedures, refer to [“Transfer Partner Assignment to Key Groups Menu” on page 229](#).



## Agent List Menu

The Agent List menu option allows you to:

- View Agents
- Create Agents
- View/Modify an Agent
- Delete existing Agents.



## Viewing the Agent List

The Agent List menu option allows the user to view all Agents associated with a specific Key Group.

To view this screen:

1. From the Agents menu, select **Agent List**. The Agent List screen is displayed.
2. Click the down-arrow beside the Key Group field and select a Key Group. The Agents that are associated with the Key Group are displayed.

Agent List

Filter: Agent ID =  +

Key Group 1 Use Refresh Reset | < << >>

Results in page: 3 (last page)

| Agent ID       | Description           | Site    | Default Key Group | Enabled | Failed Login Attempts | Enrolled |
|----------------|-----------------------|---------|-------------------|---------|-----------------------|----------|
| MyAgent        | agentdesc for MyAgent |         | MyKeyGroup        | True    | 0                     | True     |
| MyAgent1       | agentdesc for MyAgent |         | MyKeyGroup        | True    | 0                     | False    |
| SO-owned Agent | agent for testing.    | Toronto |                   | True    | 0                     | False    |

Details... Create... Delete Activity History...

You can also scroll through the lists and filter the Agents lists by any of the following keys:

- Agent ID
- Description
- Site
- Default Key Group
- Enabled
- Failed Login Attempts
- Enrolled.

The **Use** button applies the filter to the displayed list for the Agent.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA.  
Possible values are:

- Agent ID
- Description
- Site
- Default Key Group
- Enabled
- Failed Login Attempts
- Enrolled

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

**Filter Value text box:**

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

**Filter Value combo box:**

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.



Click this button to add additional filters.



Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

**Show Agents in any Key Group:**

A canned filter to filter the Agents by their Key Group association, only Agents that are associated with the selected Key Group will be shown. Click the down-arrow and select a Key Group to filter by.

**Use:**

Click this button to apply the selected filters to the displayed list and go to the first page.

**Refresh:**

Click this button to refresh the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

**Agent ID**

Displays the user-specified unique identifier that distinguishes each Agent.

**Description**

Describes the Agent.

**Site**

Displays a unique identifier that indicates the Site to which the Agent belongs.

**Default Key Group**

The key group associated with all keys created by this agent if the agent does not explicitly specify a different key group.

**Enabled**

Indicates the status of the Agent. Possible values are: True or False. If this field is False, the Agent cannot establish a session with the KMA.

**Failed Login Attempts**

Displays the number of times that an attempted logon has failed

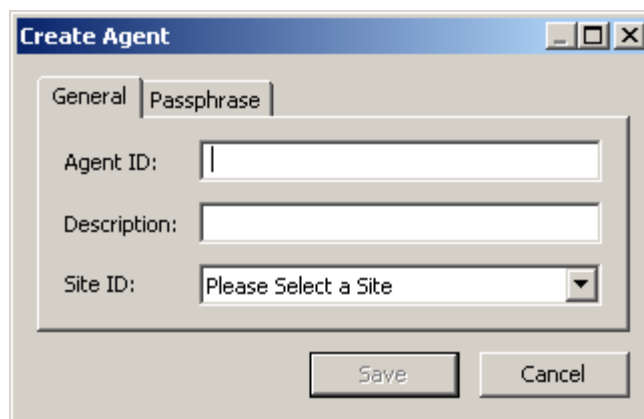
**Enrolled**

Indicates whether the Agent has enrolled successfully with the KMS Cluster. Possible values are True or False. This field is False if the Agent is the first created or if the Agent's passphrase is changed.

## Creating an Agent

To create an Agent:

1. From the Agents List screen, click the Create button. The Create Agent dialog box is displayed with the General tab open.



The image shows the 'Create Agent' dialog box with the 'General' tab selected. It contains three input fields: 'Agent ID' (a text box), 'Description' (a text box), and 'Site ID' (a dropdown menu with the text 'Please Select a Site'). At the bottom right are 'Save' and 'Cancel' buttons.

2. Complete the following parameters:

### Agent ID

Type a value that uniquely identifies the Agent. This value can be between 1 and 64 (inclusive) characters.

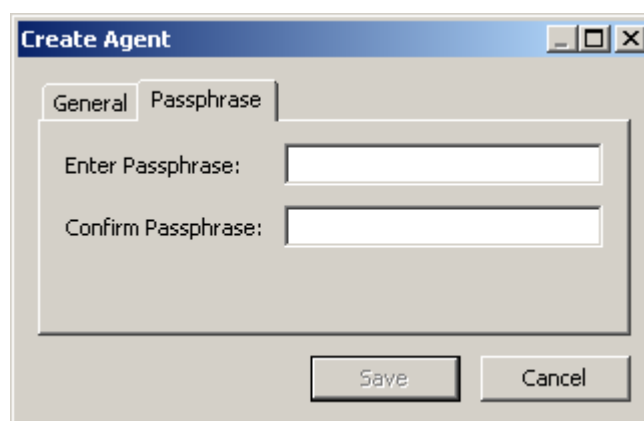
### Description

Type a value that describes the Agent. This value can be between 1 and 64 (inclusive) characters.

### Site ID

Click the down-arrow and highlight the Site to which the Agent belongs. This field is optional.

3. Open the Passphrase tab.



The image shows the 'Create Agent' dialog box with the 'Passphrase' tab selected. It contains two input fields: 'Enter Passphrase:' (a text box) and 'Confirm Passphrase:' (a text box). At the bottom right are 'Save' and 'Cancel' buttons.

4. Complete the following parameters:

#### Passphrase

Type the passphrase for this user. The minimum value is 8 characters; the maximum value is 64 characters. The default value is 8.

Passphrase requirements:

- A passphrase must not contain the user's Agent ID.
- A passphrase must contain three of the four character classes: uppercase, lowercase, numeric, or special characters.

The following special characters are allowed:

' ~ ! @ # \$ % ^ & \* ( ) - \_ = + [ ] { } \ | ; : ' " < > , . / ?

- Control characters, including tabs and linefeeds, are not allowed.

---

**Note** – To modify the minimum length requirement for passphrases, see [“Modifying the Security Parameters” on page 172](#).

---

#### Confirm Passphrase

Type the same value that you entered in the Enter Passphrase field.

An example of a completed Create Agent dialog box is shown below.

The screenshot shows a Windows-style dialog box titled "Create Agent \*". It has two tabs: "General" and "Passphrase". The "Passphrase" tab is selected. Inside the dialog, there are three input fields: "Agent ID" containing "MyAgent2", "Description" containing "agentdesc for MyAgent", and "Site ID" which is a dropdown menu currently showing "Louisville". At the bottom right of the dialog are two buttons: "Save" and "Cancel".

5. Click the Save button. The Agent record is added to the database and is displayed in the Agent List screen.
6. Complete the agent-specific enrollment procedure using the agent-specific interface. For example, for Sun drives, the VOP (Virtual Operator Panel) must be used to complete the enrollment procedure.

Agent List

Filter: Agent ID =  +

Key Group 1 Use Refresh Reset | < << >>

Results in page: 4 (last page)

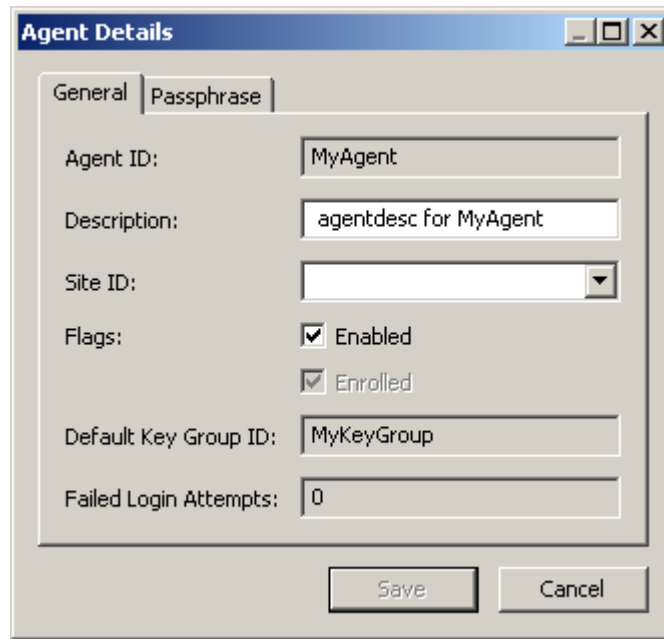
| Agent ID       | Description           | Site     | Default Key Group | Enabled | Failed Login Attempts | Enrolled |
|----------------|-----------------------|----------|-------------------|---------|-----------------------|----------|
| MyAgent        | agentdesc for MyAgent |          | MyKeyGroup        | True    | 0                     | True     |
| MyAgent1       | agentdesc for MyAgent |          | MyKeyGroup        | True    | 0                     | False    |
| MyAgent2       | agentdesc for MyAgent | Louis... |                   | True    | 0                     | False    |
| SO-owned Agent | agent for testing.    | Toronto  |                   | True    | 0                     | False    |

Details... Create... Delete Activity History...

## Viewing/Modifying an Agent

To modify an Agent's details:

1. From the Agents List screen, double-click an Agent entry for which you want more information or highlight an Agent entry and click the Details button. The Agents Details dialog box is displayed.

The image shows a Windows-style dialog box titled "Agent Details". It has two tabs: "General" (selected) and "Passphrase". The "General" tab contains several fields: "Agent ID:" with the value "MyAgent", "Description:" with the value "agentdesc for MyAgent", "Site ID:" with a dropdown arrow, "Flags:" with two checked checkboxes labeled "Enabled" and "Enrolled", "Default Key Group ID:" with the value "MyKeyGroup", and "Failed Login Attempts:" with the value "0". At the bottom right are "Save" and "Cancel" buttons.

2. Open the General tab and modify the following fields, as required:

- Description
- Site ID
- Flags - Enabled

---

**Note** – You should only change the Agent's passphrase if you believe that the passphrase has been compromised. For procedures, refer to [“Setting an Agent's Passphrase” on page 253](#).

---

3. When you are finished, click the Save button. The changes are made to the KMS Manager database and you are returned to the Agents List screen.

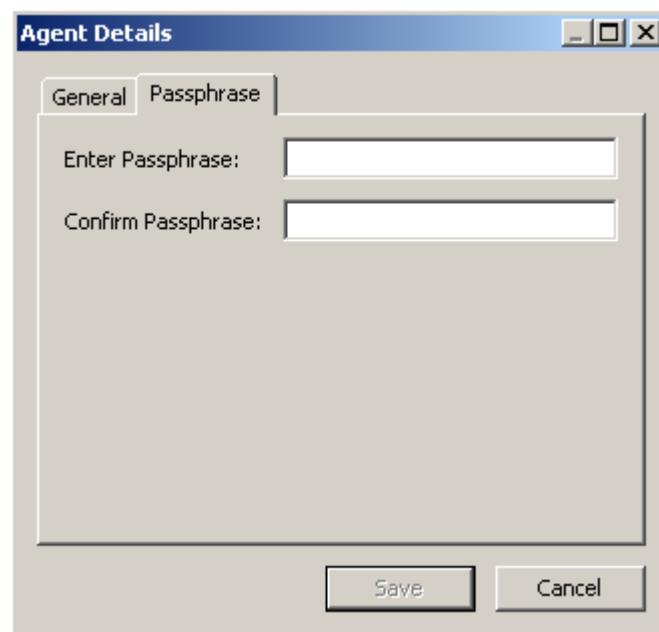


## Setting an Agent's Passphrase

When you set an Agent's passphrase, you are effectively revoking the Agent certificate that enables the Agent to authenticate itself with the KMA. As the Operator, you may want to set an Agent's passphrase certificate if you believe that the Agent certificate and/or passphrase has been compromised.

To set an Agent's passphrase:

1. From the Agents List screen, double-click the Agent entry whose passphrase you want to set or highlight the Agent entry and click the Details button. The Agent Details dialog box is displayed. Open the Passphrase tab.

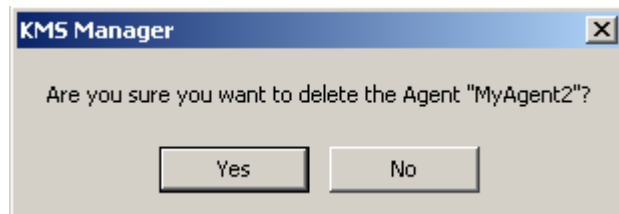
The image shows a Windows-style dialog box titled "Agent Details". It has two tabs: "General" and "Passphrase". The "Passphrase" tab is currently selected. Inside the dialog, there are two text input fields. The first is labeled "Enter Passphrase:" and the second is labeled "Confirm Passphrase:". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

2. Modify the following fields and click the Save button:
  - Enter Passphrase
  - Confirm Passphrase.
3. The changes are made to the database and you are returned to the Agents List screen.
4. Re-enroll the Agent using the agent-specific procedure. For example, for Sun tape drives, the VOP (Virtual Operator Panel) must be used to re-enroll the Agent with the KMS Cluster. After changing an Agent's passphrase, the Agent will not be able to make requests to the KMS Cluster until it is re-enrolled.

## Deleting Agents

To delete an Agent:

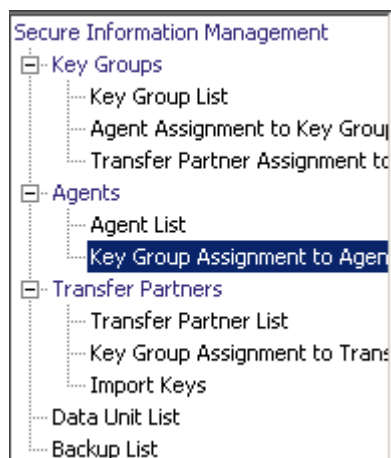
1. From the Agents List screen, highlight the Agent you want to delete. The following dialog box is displayed, prompting you to confirm that you want to delete the selected Agent.



2. Click the Yes button to delete the Agent. The Agent is removed from the database and you are returned to the Agents List screen, where the deleted Agent is no longer listed.

## Key Group Assignment to Agents Menu

The Key Group Assignment to Agents menu option allows you to view Key Groups assigned to Agents. For procedures, refer to [“Key Group Assignment to Agents Menu” on page 218](#).



## Import Keys Menu

This menu option imports keys and data units into a KMS Cluster. The keys and data unit information are contained in a key transfer file received from a key transfer partner.

---

**Note** – Use this screen to upload and import keys to the KMS Cluster. These keys are exported from another KMS Cluster.

---

To import keys:

1. From the Transfer Partners menu, select Import Keys. The Import Keys screen is displayed.

Import Keys

Destination Key Group:

Sending Transfer Partner:

Key Transfer File Name:

2. Complete the following parameters:

**Destination Key Group:**

Select the Destination Key Group into which these keys will be imported.

The “Allow Imports” flag for this Key Group's key policy must be checked. This Key Group must be an allowed Key Group for the selected sending Transfer Partner.

**Sending Transfer Partner:**

Select the Sending Transfer Partner which exported these keys.

**Key Transfer File:**

Type the name of the Key Transfer file. You can also click Browse to select a destination path.

3. Click the Start button to begin the upload and key import process. Messages are displayed, indicating when the file is uploaded and applied.

---

## Data Units

Data Units are logical storage devices, such as disks, tapes, objects. Data Units are secured by valid Key Policies that are associated with their Key Groups. Agent must have access to the selected Data Unit.

---

**Note** – An Operator can perform all functions, except modify a Data Unit's Key Group. Only a Compliance Officer can modify a Data Unit's Key Group.

---

## Data Unit List Menu

The Data Unit List menu contains the following menu options:



It allows you to:

- View Data Units
- View/Modify Data Unit details
- View the activity history for a Data Unit
- Destroy post-operational keys for a Data Unit.

## Viewing Data Units

To view Data Units, from the Data Units menu, select Data Unit List. The Data Unit List screen is displayed.

Data Unit List

Filter:  =

Results in page: 15 (last page)

| Data Unit ID ▲                   | External Unique ID                               | Description                  |
|----------------------------------|--|------------------------------|
| D75BB76E261B05F64AA938305DEDD3B9 |  |                              |
| FDAC7620B1491D5014B42E4F7C533F8E |  |                              |
| FDAC7620B1491D5041A98D806AEC18B5 | 745F33ACECA3E509297643D214B29E1CB9BD4CDF9456...  |                              |
| FDAC7620B1491D5065906BDAC533C0DB | B49548C84E2B68B90B8100830730F1910956497C5CB4C... |                              |
| FDAC7620B1491D5065B3DB5B991A4F18 | 91BB80FFB62BC006C4BD61E45E6D1C8ABFD29FDDA7A5...  |                              |
| FDAC7620B1491D506CB5E9AB176DB3B0 | 563513FE2096254BAF1D069518FE950D79734341E7C7B... |                              |
| FDAC7620B1491D506DC3C3B2E286AD0F | FD8F94E8CC77FA07E30CDA204C2E2C6EE3835179E4A5...  | Description for Data Unit te |
| FDAC7620B1491D5077E2EAE578D79F2D | D89550D598A811C2F140BF5D880BE842DCDDA9CD826F...  |                              |
| FDAC7620B1491D507D0919C428CF50E0 | F1DA375B1243A8F557ECFFF9010D663B5E01FBDA0924...  |                              |
| FDAC7620B1491D5090E82378AEEAD80D | 9D697FCCA082AF775C0244500444EF0DF155D96FF9C3...  |                              |
| FDAC7620B1491D509DA29E93ACD06FD2 | 9A20955340BFAD0EA7B498B31A2D2499726A88B006C1...  |                              |
| FDAC7620B1491D50B543A1A1312417E1 | 3E5BAFE1923CE8C49F913B62989228DC92EA5E72A711...  |                              |
| FDAC7620B1491D50F37D23722C616818 | 45B1180CB4AD661D41EADBC783B9745BE42D2B075EBB...  |                              |
| FDAC7620B1491D50FAB86E1F886F559B |  |                              |
| FDAC7620B1491D50FFF4DB6487307C4A | 37FA9EBBA83122591DFB921156003A4C1DDF3AFAEB73...  |                              |

Details... Activity History... Destroy Keys... Modify Key Group... Export Keys...

You can also scroll through the database and filter the Data Unit list by any of the following keys:

- Data Unit ID
- External Unique ID
- Description
- External Tag
- Created Date
- Imported
- Exported
- State.

The **Use** button applies the filter to the displayed list for the Data Unit.

The fields and their descriptions are given below:

**Filter:**

Displays the fields that you can use to filter the results of queries made to the KMA.

Possible values are:

- Data Unit ID
- External Unique ID
- Description
- External Tag
- Created Date
- Imported
- Exported
- State

**Filter Operator box:**

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

**Show Data Units in Any Key Group. Use:**

Click this button to apply the filter to the displayed list.

**Refresh:**

Click this button to refresh the list.

**Reset:**

Click this button to remove all filters and reset the displayed list to the first page.



Click this button to go to the first page of the list.



Click this button to go to the previous page.



Click this button to go to the next page.

**Results in Page:**

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.



**Data Unit ID**

Displays a system-generated unique identifier that distinguishes each Data Unit.

**External Unique ID**

Displays a unique external identifier for the Data Unit.

This value is sent to the KMS by the Agent and may not be externally visible to an end user. For LTO Gen 4 tapes, this is the cartridge serial number burned into the cartridge when it is manufactured. Do not confuse this value with a volser on an optical barcode or in an ANSI tape label. This value is not used for Sun tape drives.

**Description**

Describes the Data Unit.

**External Tag**

Describes a unique external tag for the Data Unit.

For tapes that are in a Sun tape library, or tapes that have ANSI standard labels, this field will be the volser. If the tape is in a library and has an ANSI label, the library volser (i.e., optical bar code) will be used if it differs from the volser contained in the ANSI label. For tapes written in stand-alone drives without ANSI labels, this field will be blank.

**Created Date**

Indicates the date and time when the Data Unit was created/registered.

**Imported**

Indicates whether the Data Unit has been imported.

**Exported**

Indicates whether the Data Unit has been exported.

**State**

Indicates the state of the Data Unit. Possible values are:

- No Key: Set when the Data Unit has been created, but has not yet had any keys created.
- Readable: Set when the Data Unit has keys that allow at least some parts of the Data Unit to be decrypted (read).
- Normal: Set when the Data Unit has keys that allow at least some parts of the Data Unit to be decrypted (read). In addition, the Data Unit has at least one protect-and-process state key that can be used to encrypt data. The Data Unit is therefore writable.
- Needs ReKey: Set when the Data Unit has keys that allow at least some parts of the Data Unit to be decrypted (read). However, the Data Unit does not have at least one protect-and-process state key.

If data is written to this tape, it will automatically be given a new protect and process key.

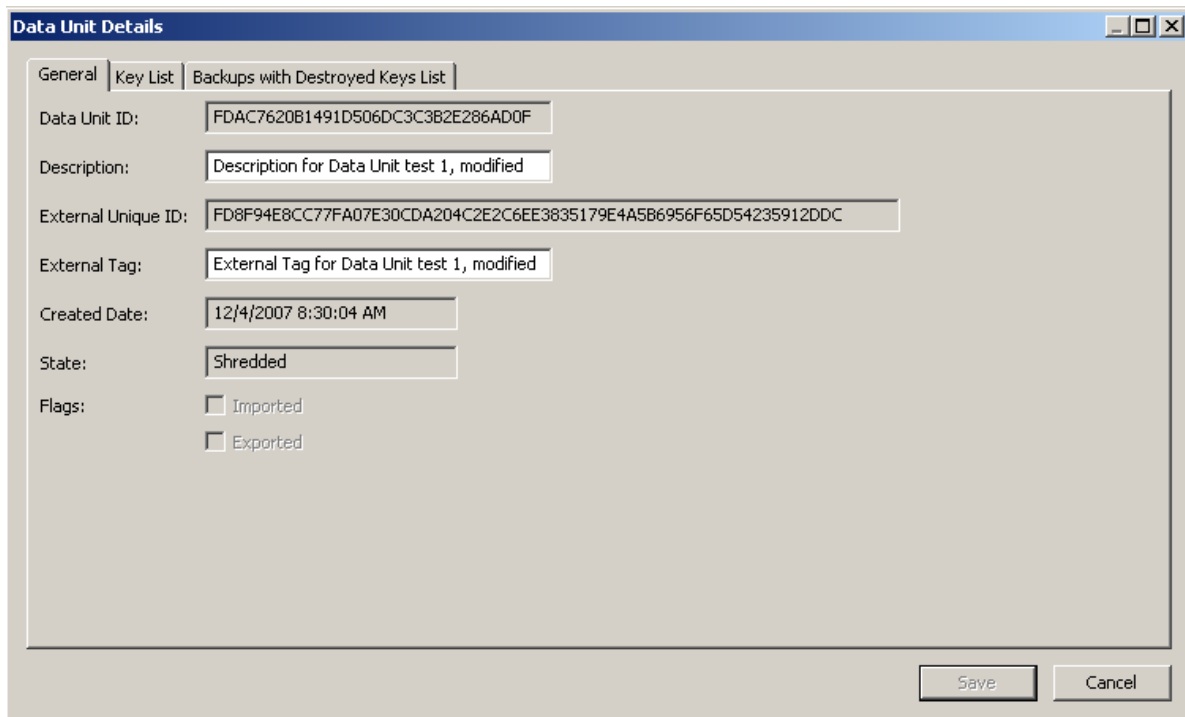
- Shredded: Set when all of the keys for this Data Unit are destroyed. The Data Unit cannot be read or written. However, a new key can be created for this Data Unit, moving its state back to Normal.

## Viewing/Modifying Data Unit Details

**Note** – If you are not an Operator, when you view a Data Unit’s detailed information, all fields, including the Save button are disabled. If you are a Compliance Officer, the Key Group field is enabled.

To modify a Data Unit’s information:

1. From the Data Unit List screen, select the Data Unit you want to modify and click the Details button. The Data Unit Details dialog box is displayed.

The image shows a 'Data Unit Details' dialog box with a title bar and standard window controls. It has three tabs: 'General' (selected), 'Key List', and 'Backups with Destroyed Keys List'. The 'General' tab contains several fields: 'Data Unit ID' with a hexadecimal value, 'Description' with a text value, 'External Unique ID' with a long hexadecimal value, 'External Tag' with a text value, 'Created Date' with a date and time, 'State' with a dropdown menu set to 'Shredded', and 'Flags' with two unchecked checkboxes labeled 'Imported' and 'Exported'. At the bottom right are 'Save' and 'Cancel' buttons.

**Data Unit Details**

General | Key List | Backups with Destroyed Keys List

Data Unit ID: FDAC7620B1491D506DC3C3B2E286AD0F

Description: Description for Data Unit test 1, modified

External Unique ID: FD8F94E8CC77FA07E30CDA204C2E2C6EE3835179E4A5B6956F65D54235912DDC

External Tag: External Tag for Data Unit test 1, modified

Created Date: 12/4/2007 8:30:04 AM

State: Shredded

Flags: ☐ Imported ☐ Exported

Save Cancel

2. You can modify the following parameters:

### Description

Type a new value. The original information is provided by the Software Encryption Driver during registration. This value can be between 1 and 64 (inclusive) characters or blank.

### External Tag

Type a unique external identifier for the Data Unit. This value can be between 1 and 64 (inclusive) characters or blank. This field typically contains the label or barcode of the tape cartridge.

3. Click the Save button to save your changes.

The following are non-editable fields:

### *General Tab*

- Data Unit ID
- External Unique ID
- Created Date
- State
- Flags Imported/Exported

### *Key List Tab*

**Data Unit Details**

General | **Key List** | Backups with Destroyed Keys List

Data Unit ID: FDAC7620B1491D506DC3C3B2E286AD0F

Data Unit Description: Description for Data Unit test 1, modified

Key List

Filter: **Key ID** =  +

Use Refresh Reset | < << >> >

Results in page: 1 (last page)

| Key ID  | Key Type | Created Date         | Activation Date ▾    | Destroyed Date       |
|---|----------|----------------------|----------------------|----------------------|
| FDAC7620B1491D503AC99FEDBCC45D40CBC536982E... | AES-256  | 12/4/2007 8:20:53 AM | 12/4/2007 8:30:04 AM | 12/4/2007 8:30:04 AM |

Details... Compromise... Activity History... Save Report...

Save Cancel

#### **Data Unit ID**

Uniquely identifies the Data Unit.

#### **Data Unit Description**

Describes the Data Unit.

#### **Key ID**

Displays the key information for the Data Unit.

#### **Key Type**

Indicates the type of encryption algorithm that this key uses. Possible values are:  
AES-256.

**Created Date**

Displays the date and time when the key was created.

**Activation Date**

Displays the date and time when the key was activated. This is the date and time when the key was first given to an Agent. It is the starting date and time for the key's encryption period and cryptoperiod.

**Destroyed Date**

Displays the date when the key was destroyed. If the field is blank, then the key is not destroyed.

**Destruction Comment**

Displays any user-supplied information about the destruction of the key. If the field is blank, then the key is not destroyed.

**Imported**

Indicates whether the Data Unit has been imported.

**Exported**

Indicates whether the Data Unit has been exported.

**Key Group**

Displays the Key Group associated with the Data Unit.

**Encryption End Date**

Displays the date and time when the key will no longer be used or was stopped from being used for encrypting data.

**Deactivation Date**

Displays the date and time when the key will be or was deactivated.

**Compromised Date**

Displays the date when the key was compromised. If the field is blank, then the key is not compromised.

**Compromised Comment**

Displays any user-supplied information about compromising the key. If the field is blank, then the key is not compromised.

**Key State**

Indicates the Data Unit's key state. Possible values are:

**Generated**

Set when the Key has been created on one KMA in a KMS Cluster. It remains generated until it has been replicated to at least one other KMA in a multi-KMS Cluster. In a Cluster with only a single KMA, the Key remains generated until it has been recorded in at least one backup.

**Ready**

Set when the Key has been protected against loss by replication or a backup. A ready Key is available for assignment.

**Protect and Process**

Set when the Key has been assigned when an encryption agent requests a new key be created. A Key in this state can be used for both encryption and decryption.

**Process Only**

Set when the Key has been assigned but its encryption period has expired. A Key in this state can be used for decryption but not for encryption.

**Deactivated**

Set when the Key has passed its cryptoperiod but may still be needed to process (decrypt) information.

**Compromised**

Set when the Key has been released to or discovered by an unauthorized entity. A Key in this state can be used for decryption but not for encryption.

**Incompletely Destroyed**

Set when the Key has been destroyed but it still appears in at least one backup.

**Completely Destroyed**

Set when all of the backups in which the destroyed Key appears have been destroyed.

**Compromised and Incompletely Destroyed**

Set when the compromised Key still appears in at least one backup.

**Compromised and Completely Destroyed**

Set when all of the backups in which the compromised Key appears have been destroyed.

**Recovery Activated**

Indicates whether the Key has been linked to the data unit by a recovery action. This condition occurs when a Key is used for a Data Unit by one KMA in a KMS Cluster and then, due to a failure, the Key is later requested for the Data Unit from a different KMA. If the failure (such as a network outage) has prevented the allocation of the Key to the data from being propagated to the second KMA, the second KMA will create the linkage to the data unit. Such a Key is "recovery activated," and an administrator may want to evaluate the system for KMA or network outages. Possible values are: True and False.

## Backups with Destroyed Keys List Tab

**Data Unit Details**

General | Key List | **Backups with Destroyed Keys List**

Data Unit ID: FDAC7620B1491D506DC3C3B2E286AD0F

Data Unit Description: Description for Data Unit test 1, modified

Backup List

Filter: Backup ID = [ ] +

Use Refresh Reset | < << >> >

Results in page: 2 (last page)

| Backup ID                          | Created Date ▾       | Destroyed Date | Pending | Completed Date       | Download  |
|------------------------------------|----------------------|----------------|---------|----------------------|-----------|
| FDAC7620B1491D50000000000000000002 | 12/4/2007 8:30:18 AM |                | True    | 12/4/2007 8:30:22 AM | 12/4/2007 |
| FDAC7620B1491D50000000000000000001 | 12/4/2007 8:26:49 AM |                | True    | 12/4/2007 8:26:52 AM | 12/4/2007 |

Details... Save Report...

Save Cancel

A Data Unit cannot be considered “completely destroyed” until all Backups containing the Data Unit Key(s) have been destroyed.

The Backups with Destroyed Keys List tab of the Data Unit Details dialog helps you identify those Backups that contain Data Unit Key(s) for the selected Data Unit and the destruction status of those Backups.

The logic for determining if a Backup does contain a particular Data Unit Key is as follows:

A Backup contains a Data Unit Key, if the Backup was created after the Data Unit Key was created **and** the Data Unit Key has not been destroyed, or if it has been destroyed **and** its destruction took place after the Backup was created.

However, the date-time comparison needs to take into consideration that the clocks of the various KMAs in a Cluster might not be synchronized automatically (if an NTP server is not specified) and hence may be reporting different times. To account for the possibility of time discrepancies among KMAs, a Backup Time Window is used in the comparison. The Backup Time Window is fixed at five minutes. Using the Backup Time Window, the comparison check behaves as follows:

A Backup contains a Data Unit Key if the Backup was created within five minutes of the backup creation or later **and** the Data Unit Key was destroyed within five minutes of the Backup creation or later.

The Backup Time Window is used to minimize the likelihood of falsely reporting that a Data Unit does not exist in a particular backup when in fact it does. Such a case is known as a “false negative” and seriously undermines compliance requirements for data destruction. Utilization of the Backup Time Window does, however, increase the

likelihood of falsely reporting that a Data Unit Key does belong in a Backup when in fact it does not. Unlike “false negatives,” “false positives” do not undermine compliance requirements for data destruction.

**Data Unit ID**

Uniquely identifies the Data Unit.

**Data Unit Description**

Describes the Data Unit.

**Data Unit Destruction Status**

Indicates the Destruction status of the Data Unit.

**Backup ID**

Identifies the backup.

**Created Date**

Displays when the date and time when the backup file was created (that is, when the backup started).

**Destroyed Date**

Displays the date and time when the backup file was destroyed.

**Pending:**

Indicates whether the backup is still pending. Possible values are True or False.

**Completed Date:**

Displays the date and time when the backup file was completed.

**Downloaded Date:**

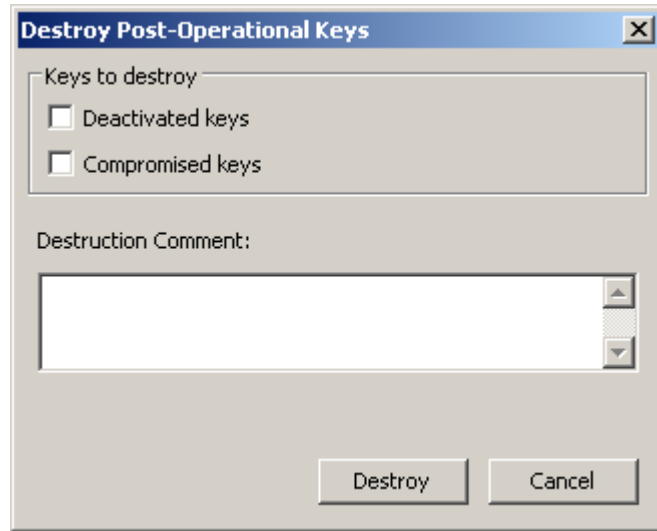
Displays the date and time when the backup file was downloaded.

4. Click the Save button to save your changes.

## Destroying Post-operational Keys

To destroy post-operational keys associated with a data unit:

1. From the Data Unit List screen, highlight the Data Unit you want to destroy and click the Destroy Keys button.
2. The following dialog box is displayed, prompting you to specify the keys to destroy.



### Deactivated keys

Select this checkbox if you want to destroy the keys that have passed their cryptoperiod but still may be needed to process (decrypt) data information.

### Compromised keys

Select this checkbox if you want to destroy the keys that have been released to or discovered by an unauthorized entity.

### Destruction Comment

Type a comment about the destruction of these keys.

3. If you click the Destroy button, another dialog box is displayed confirming the destruction of these keys.
4. Click the Yes button. Another dialog box is displayed showing the number of Keys that have been destroyed.



## Software Upgrade Menu

The Software Upgrade menu option allows the Operator to upload a software upgrade file to the KMA and immediately apply the upgrade. The software updates are signed by Sun and verified by the KMA before they are applied.

### Guidelines for Performing Software Upgrades

- Before you execute this function, back up your system. For procedures, refer to [“Creating a Backup” on page 277](#).
- Use a KMS Manager GUI release that matches the upgrade version you want to load on the KMA(s).
- The upload and apply process can be lengthy if the KMS Manager is remotely connected to the KMA or if the connection between the KMS Manager and KMA is slow. To mitigate this, the software upgrade file can be downloaded to a laptop or workstation that has the KMS Manager installed and the laptop or workstation connected to the same subnet as the KMA. The presence of a router between the KMS Manager and the KMA may slow down the upgrade process.
- The upload and apply processes, with a good connection between the KMS Manager and the KMA, optimally take about 30 minutes. The activate process optimally takes about 5 to 15 minutes. If the uploading process is very slow, try connecting to the same subnet as the KMA.
- If any of the upgrade processes fail (upload, verify, apply, activate, switch replication version), the KMS Manager will generate audit messages describing the reason for the failure and a suggested solution.
- Technical Support accounts will be disabled on the upgraded KMAs and the accounts and will need to be re-enabled if needed.

## Uploading and Applying Software Upgrades

To upgrade the KMA:

1. Download the software upgrade file to your PC or workstation from the delivery location. The version is visible in the file name.

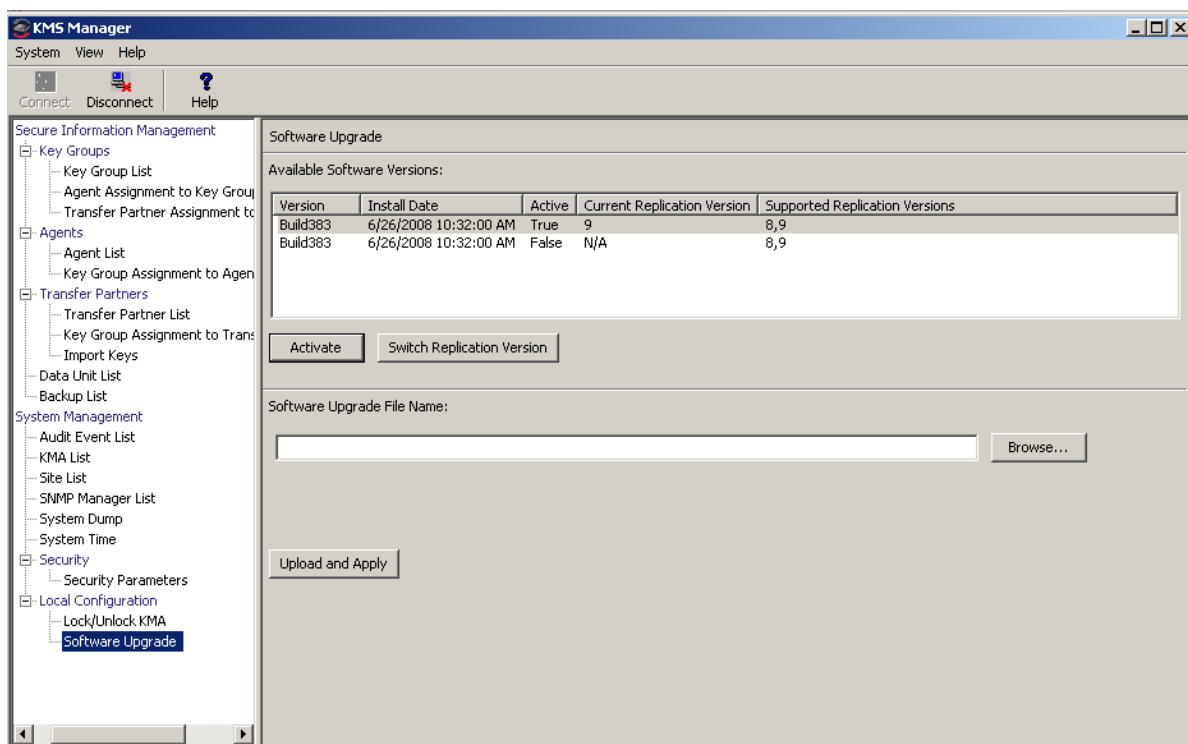
---

**Note** – Save the file to a location where you can navigate from the KMS Manager GUI.

---

2. From the Local Configuration menu, select **Software Upgrade**. The Software Upgrade screen is displayed.

The active version of the software is highlighted, the **Active** column is set to **True**, and an inactive version is shown.



The buttons appearing on this screen include:

### Activate

Select an inactive software version and then click this button to activate the selected software version. Messages are displayed, indicating when this software version is activated and the KMA reboots.

**Switch Replication Version**

Select the active software version and then click this button to switch the current replication version.

**Software Upgrade File Name**

Type the name of the software upgrade file.

**Browse**

Click this button to locate the software upgrade file on your local system.

**Upload and Apply**

Click this button to begin the upload and apply process. Messages are displayed, indicating when the software upgrade file is uploaded and applied.

3. In the Software Upgrade File Name field, type the name of the software upgrade file. You can also select the Browse button to locate the file. Click the Upload and Apply button.

The KMS starts the upload, verify, and apply process and displays a progress indicator showing which step the process is at.

4. Make sure there is a current backup of the KMS Cluster.

To activate the upgrade file, select the new version from the list of available versions at the top of the screen and click the **Activate** button. Until activated, the new version will remain inactive on the system.

---

**Note** – Activate the upgrade file on each KMA in a KMS Cluster. Since the upload process adds some traffic to the network, you may not want to upload KMAs simultaneously in a busy Cluster.

---

5. Reboot each KMA in the KMS Cluster. Users remain connected until the reboot is complete. When you access the Software Upgrade screen again, the new uploaded software version is shown as the active version.

The new software version may include new features available only when the KMS Cluster replication version is changed to a higher value. The KMS Cluster must be switched to the new replication version to enable all new features in the new software version.

6. Log in to a KMA that has been activated and navigate to the Software Upgrade screen. If the **Supported Replication Versions** column includes a higher version than the **Current Replication Version** column, click the **Switch Replication Version** button.

The **Current Replication Version** will now display the higher version, and the successful replication switch is sent to all other KMAs in the KMS Cluster.

## Backup List Menu

For procedures on viewing a Backup file's detailed information, refer to ["Backup List Menu" on page 273](#).

## Audit Event List Menu

For procedures to view an audit event list, refer to ["Audit Event List Menu" on page 235](#).

## KMA List Menu

For procedures to view the list of KMAs, refer to ["KMA List Menu" on page 97](#).

## Site List Menu

For procedures to view a list of sites, refer to ["Site List Menu" on page 123](#).

## SNMP Manager List Menu

For procedures to view the list of SNMP managers, refer to ["SNMP Manager List Menu" on page 131](#).

## System Time Menu

For procedures on viewing the KMA's time, refer to ["System Time Menu" on page 189](#).

## Lock/Unlock KMA Menu

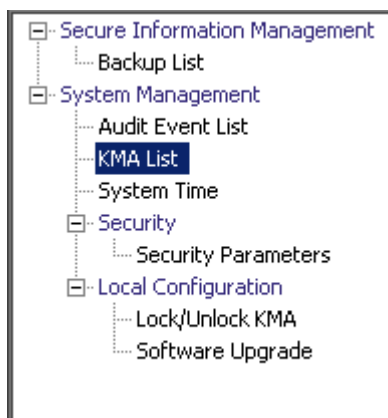
For procedures on viewing the KMA locking status, refer to ["Lock/Unlock KMA" on page 183](#).

## Backup Operator Operations

This chapter describes the operations that a user who has been given a Backup Operator role can perform. If you have been assigned other roles, refer to the appropriate chapter for instructions on performing the specific role.

### Backup Operator Role

As the Backup Operator, you are responsible for securing and storing data and their keys.



### Backup List Menu

The Backups List menu option allows the Backup Operator to:

- View the history of the Backups and confirm their destruction status
- Create Backups.

## Viewing Backup Files History

To view Backup files history:

From the Backups menu, select **Backup List**. The Backup List screen is displayed.

The screenshot shows the 'Backup List' window. At the top, there is a filter section with a dropdown menu set to 'Backup ID', an equals sign, another dropdown menu, and a text input field. To the right of the filter are buttons for 'Use', 'Refresh', 'Reset', and navigation arrows. Below the filter, it says 'Results in page: 2 (last page)'. The main area contains a table with the following data:

| Backup ID                         | KMA ID           | Created Date         | Destroyed Date | Destruction Status | Destr |
|-----------------------------------|------------------|----------------------|----------------|--------------------|-------|
| 9CE46A4BB276A9FB00000000000000001 | 9CE46A4BB276A9FB | 1/7/2008 10:33:15 AM |                | PENDING            |       |
| 9CE46A4BB276A9FB00000000000000002 | 9CE46A4BB276A9FB | 1/7/2008 10:39:37 AM |                | PENDING            |       |

At the bottom of the window, there are buttons for 'Details...', 'Create Backup...', 'Restore...', and 'Confirm Destruction...'.

If you want more detailed information on a Backup, highlight the Backup and click the Details button. For more information, refer to [“Viewing Backup Details”](#).

Click the Create Backup button to create a Backup. For more information, refer to [“Creating a Backup” on page 277](#).

Click the Confirm Destruction button to confirm the destruction of a Backup. For more information, refer to [“Confirming a Backup’s Destruction” on page 278](#).

## Viewing Backup Details

The Backup Details dialog box is used to view the details of a Backup file.

---

**Note** – Backup files are downloaded to the machine where the KMS Manager is running when the backup is created.

---

To view the details of a Backup file:

1. From the Backups List screen, double-click the Backup entry for which you want more information or highlight the Backup entry and click the Details button. The Backup Details dialog box is displayed, with all fields disabled.

|                      |                                  |
|----------------------|----------------------------------|
| Backup ID:           | FDAC7620B1491D500000000000000001 |
| KMA ID:              | FDAC7620B1491D50                 |
| Created Date:        | 12/4/2007 8:26:49 AM             |
| Completed Date:      | 12/4/2007 8:26:52 AM             |
| Downloaded Date:     | 12/4/2007 8:28:13 AM             |
| Destroyed Date:      |                                  |
| Destruction Status:  | PENDING                          |
| Destruction Comment: |                                  |

Close

2. The fields and their descriptions are given below:

### Backup ID

Displays a system-generated unique identifier that distinguishes each Backup file.

### KMA ID

Displays the KMA on which this Backup file is generated.

### Created Date

Displays the date and time when the Backup file was created.

### Completed Date

Displays the date and time when the Backup file was completed.

### Downloaded Date

Displays the date and time the Backup file was downloaded.

**Destroyed Date**

Displays the date when the Backup file was destroyed.

**Destruction Status**

Indicates the status of the backup with respect to its destruction.

**Destruction Comment**

Displays user-supplied information on the Backup file's destruction.

3. Click the Close button to close this dialog box.



## Creating a Backup

---

**Important** – The Security Officer must back up Core Security Key material before the Backup Officer can create a backup. See [“Creating a Core Security Backup” on page 175](#).

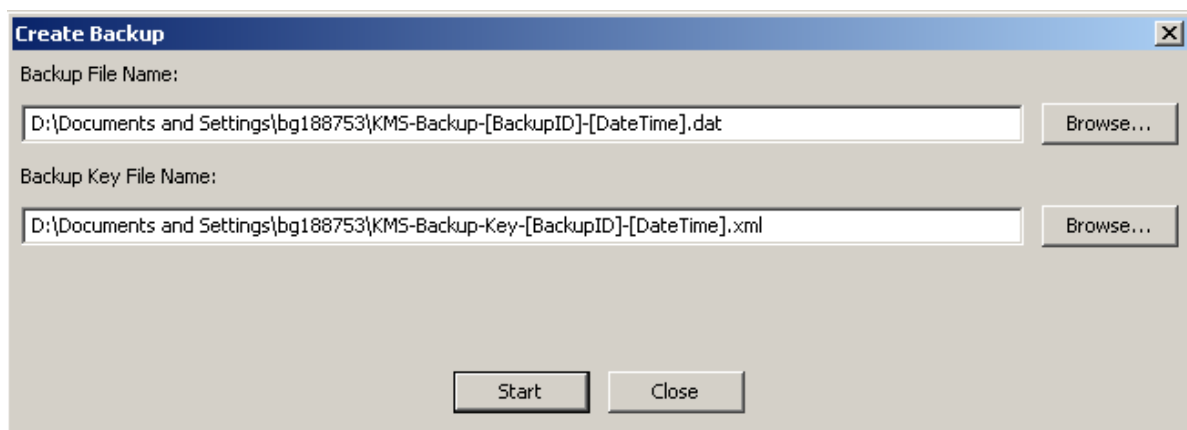
---

At any given time, there is only one Backup file and one Restore file on a KMA.

This option gives the user the ability to create a Backup that consists of two files: a Backup file and a Backup key file.

To create a Backup:

1. From the Backup List screen, click the Create Backup button. The Create Backup dialog box is displayed.



---

**Note** – Backup File and Backup Key File names are automatically generated. You can, however, edit the names. You can also click the Browse button to select a destination path.

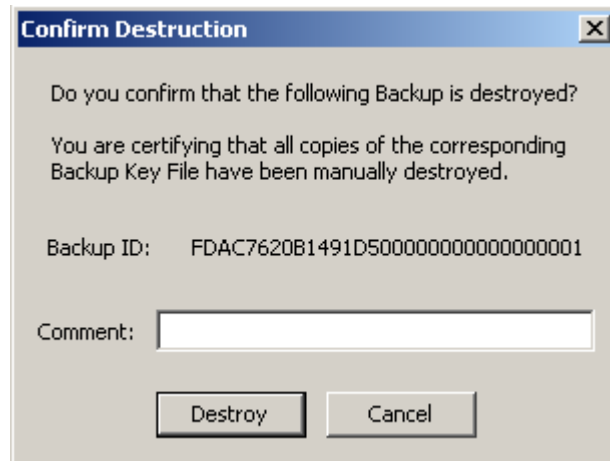
---

2. Click the Start button to create the Backup file and download the Backup key file to the user-specified destination.
3. When the Backup is completed, a message indicating this is displayed. Click the Close button to close this dialog box.
4. You are returned to the Backup List screen, where the new created Backup File is displayed.

## Confirming a Backup's Destruction

To confirm a backup's destruction:

1. From the Backup List screen, highlight the Backup you want to destroy and click the Confirm Destruction button. The following dialog box is displayed, confirming that you want to update the destruction status for the selected Backup. Before proceeding, ensure that all copies of the corresponding Backup Key file have been manually destroyed.



2. If you are certain that all copies of the corresponding backup key file have been manually destroyed, click the Yes button. Otherwise, click the No button to stop the process.
3. If you chose the Yes button, the backup and the Data Units that were associated with it are 'completely destroyed'.

## Backup Command Line Utility

The Backup Command Line utility allows you to launch a backup from the command line instead of from the Backup List menu. You can also schedule automated backups.

This utility is installed with the KMS Manager GUI using the same installer.

### Solaris Syntax

```
KMS_Backup [-UserID userid] [-Passphrase passphrase]  
           -KMAIPAddress IPaddress -BackupFilePath pathname  
           [-Retries retries] [-Timeout timeout]
```

### Windows Syntax

```
KMSBackupUtility [-UserID userid] [-Passphrase passphrase]  
                -KMAIPAddress IPaddress -BackupFilePath pathname  
                [-Retries retries] [-Timeout timeout]
```

### Parameter Descriptions

#### *userid*

The Backup Operator user ID. This **must** be a Backup Operator.

#### *passphrase*

The passphrase for the user ID.

---

**Note** – If the *userid* or *passphrase* value is not specified, the utility prompts for these values.

---

#### *IPaddress*

The KMA Management Network Address on which to launch the backup.

#### *pathname*

The location where the Backup File and Backup Key File should be downloaded on your system.

**retries**

The number of times that this utility tries to connect to the KMA, if the KMA is busy. The default is **60**.

**timeout**

The timeout value in seconds between these entries. The default is **60**.

## Example

The following example creates a Backup File (format: KMS-Backup-*backupid-timestamp.dat*) and a Backup Key File (format: KMS-BackupKey-*backupid-timestamp.xml*).

```
KMS_Backup -UserID MyBackupOperator -Passphrase secret2Me
           -KMAIPAddress 129.80.60.172
           -BackupFilePath /tmp/MyKMSDownloads
```

## IPv6 Addresses with Zone IDs

For Windows system users, the Backup Command Line utility allows you to enter link-local IPv6 addresses, however, you must perform some initial setup first.

---

**Note** – You must enter a Zone ID whenever you specify a link-local address (that is, an IPv6 address that begins with “fe80”). You can specify a Zone ID by appending it to the end of an IPv6 address, following a percent sign (%).

---

1. Display a command prompt window and determine which Zone IDs are available on your Windows system.

```
netsh interface ipv6 show interface
```

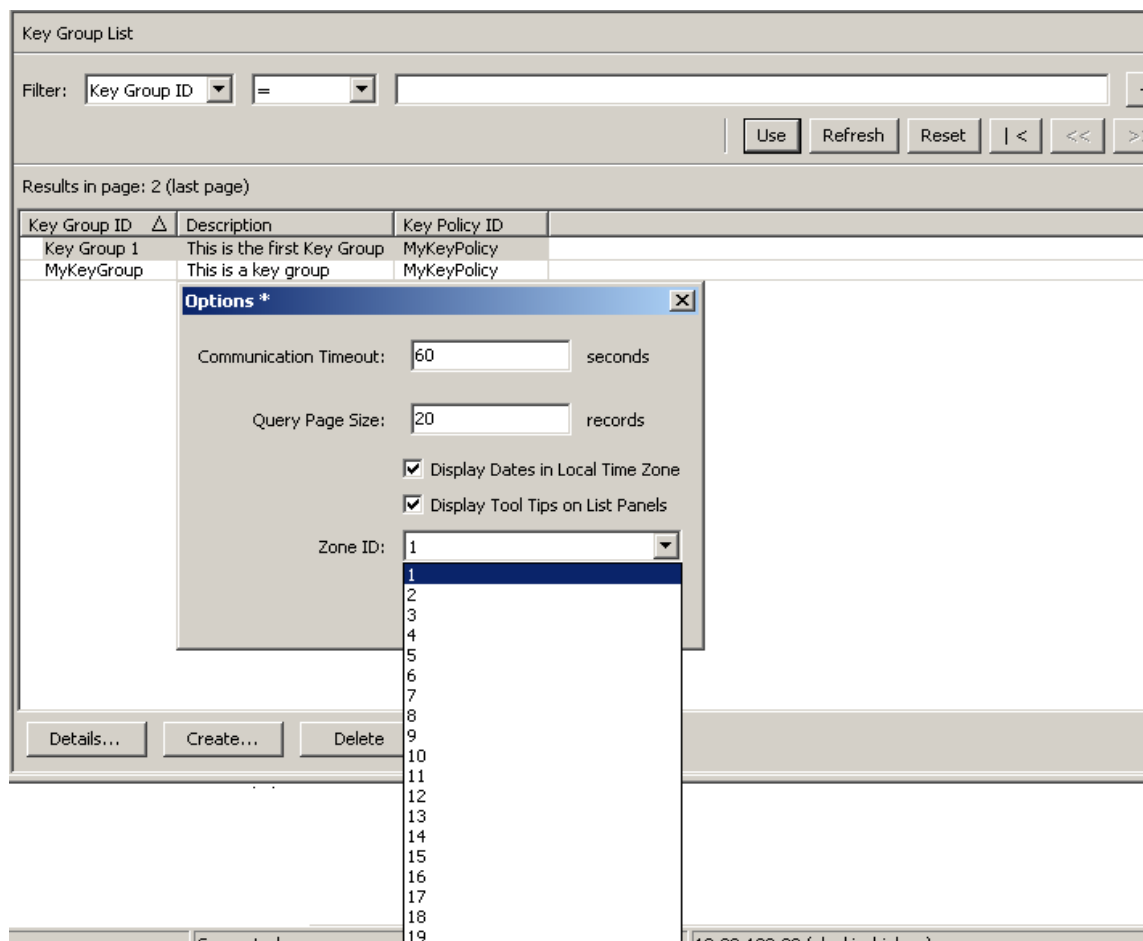
The Zone IDs appear in the **Idx** column in the output of this command. Look for entries that show a **State** of “Connected.”

2. Use the **ping** command to confirm network connectivity using one of these Zone IDs. For example:

```
ping fe80::216:36ff:fed5:fba2%4
```

3. Invoke the Backup Utility and specify a link-local IPv6 address. Include the Zone ID (for example, “%4”) at the end of the address.

- Before you bring up the Connect dialog in the KMS Manager GUI, display the Options dialog and select the appropriate Zone ID.



- Click the Save button.

## KMA List Menu

The KMA List menu option allows you to:

- View KMAs (refer to [“Viewing KMAs” on page 98](#))
- Create a KMA (refer to [“Creating a KMA” on page 102](#))
- Modify a KMA’s information (refer to [“Viewing/Modifying a KMA’s Details” on page 105](#))
- Delete a KMA (refer to [“Deleting a KMA” on page 108](#))
- Modify a Key Pool size

---

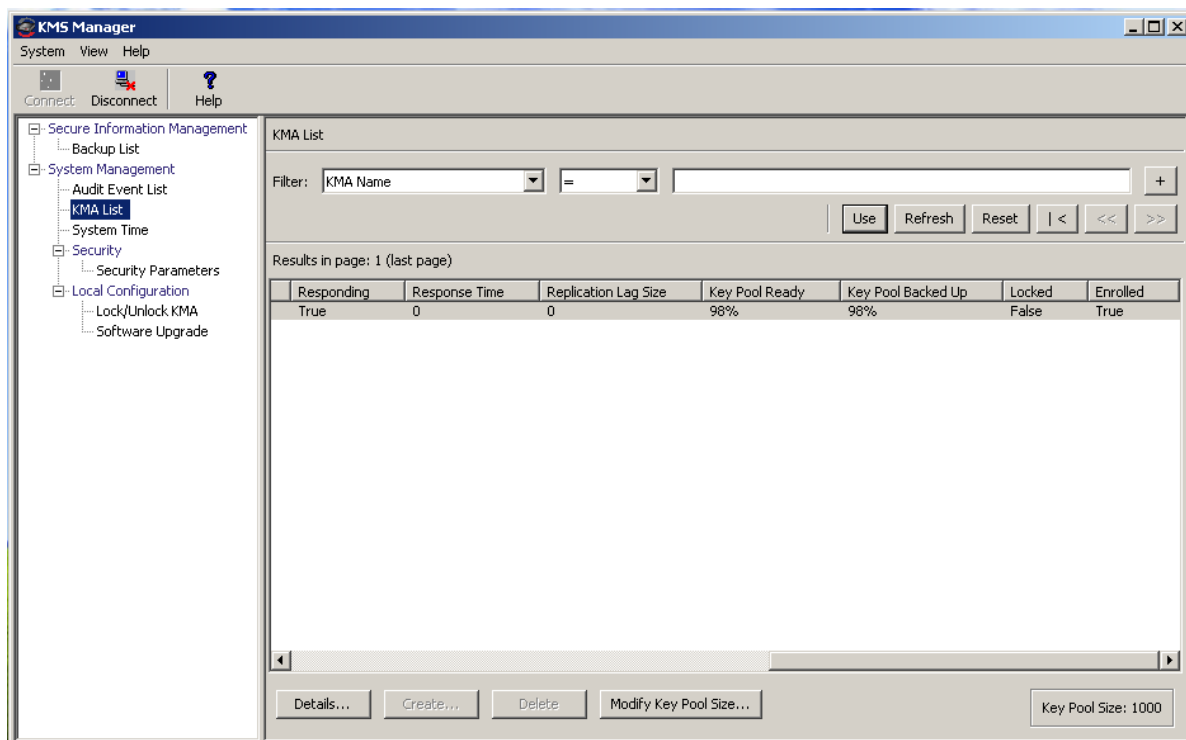
**Note** – Backup Operators can view KMA details and modify Key Pool sizes.

---

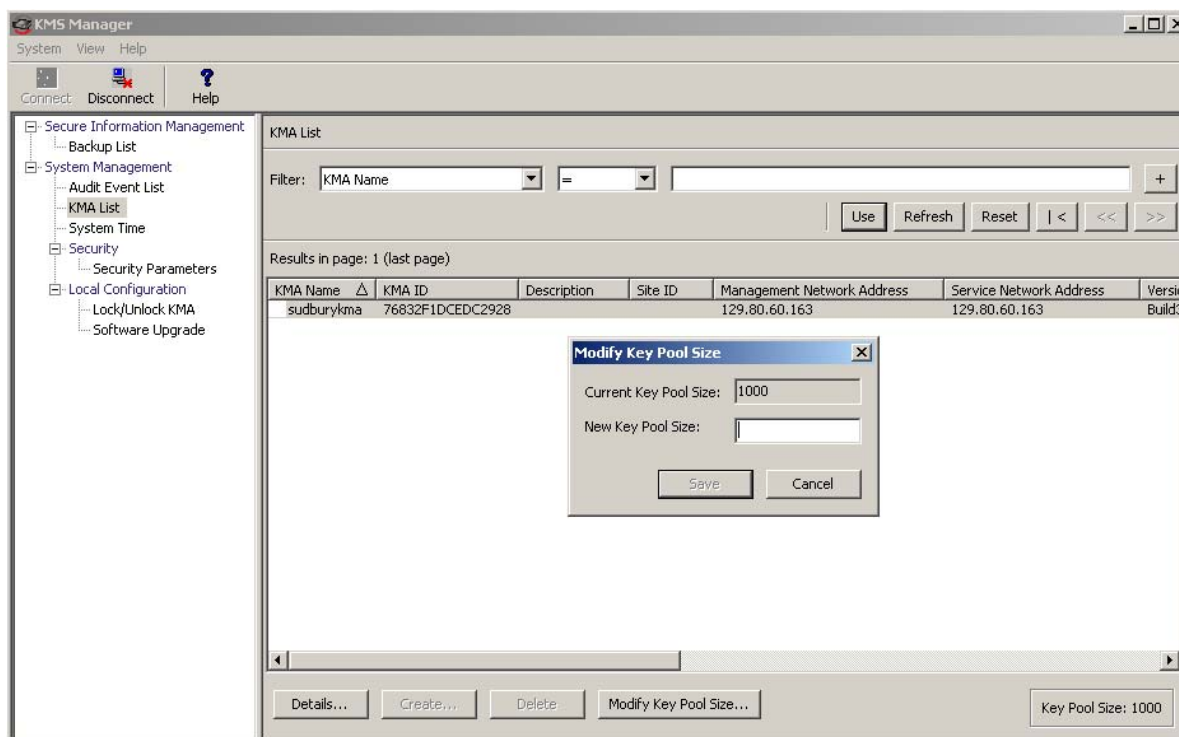
## Modifying a Key Pool Size

To modify a Key Pool size:

1. From the System Management menu, select KMA List. The right side of the KMA List screen is displayed below.



2. Click **Modify Key Pool Size**. The following screen is displayed.



3. Supply the new Key Pool size.

## Other Functions

A Backup Operator can also:

- View Audit Event List
- View the System time
- View the KMA locking status.

For procedures on viewing the Audit Log, refer to [“Audit Event List Menu” on page 235](#).

For procedures on viewing the KMA’s time, refer to [“System Time Menu” on page 189](#).

For procedures on viewing the KMA locking status, refer to [“Lock/Unlock KMA” on page 183](#).



## Auditor Operations

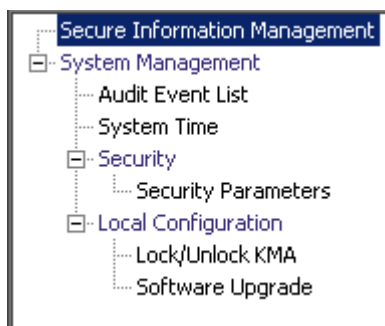
---

This chapter describes the operations that a user who has been given an Auditor role can perform. If you have been assigned other roles, refer to the appropriate chapter for instructions on performing the specific role.

---

### Auditor Role

As the Auditor, you can view the Audit List events and the KMA.



### Audit List Menu

For procedures on using the Audit List menu, refer to [“Audit Event List Menu” on page 235](#).

### Security Parameters Menu

The Security Parameters List menu gives the Auditor the ability to view the KMA’s security parameters. For procedures on using the Security Parameters menu, refer to [“Security Parameters Menu” on page 170](#).

## Other Functions

An Auditor can also:

- View the Lock/Unlock the KMA status.
- View the system time

For procedures on viewing the lock/unlock KMA status, refer to [“Lock/Unlock KMA” on page 183](#).

For procedures on adjusting the KMA’s time, refer to [“System Time Menu” on page 189](#).

For procedures on viewing the installed software versions, refer to [“Software Upgrade Menu” on page 269](#).

## Using the KMS Console

---

This chapter describes the options in the KMS Console.

---

### What is the KMS Console?

The KMS Console is a terminal text-based interface that allows a user to configure basic function of the KMA. It is accessed by physically connecting a video monitor and keyboard to the KMA or by the “remote console” function in the ELOM web browser interface (see [“Starting the Embedded Light Out Manager” on page 20](#)).

The KMS Console automatically launched by the operating system when the KMA boots up and cannot be terminated by a user. Depending on the roles that a user is assigned, the options in the KMS Console differ.

Before a user can login to the KMS Console, the user accounts must be created in the KMS Manager. The user must use the same username/passphrase that was used for authentication in the KMS to login to the KMS Console.

---

**Note** – Only the first Security Officer account is created when the QuickStart program is launched.

---

---

## Logging into the KMA

After the KMA boots up, the following information is displayed.

```
Sun Microsystems, Inc.  
Key Management System Version xxx (Buildxxx) -- <KMAname>  
-----  
Please enter your User ID:
```

1. At the prompt, type your username and press **<Enter>**.
2. At the Please enter your Passphrase: prompt, type your passphrase and press **<Enter>**. Depending on the role(s) the user is assigned, the options on the KMS Console differ. The menu shows the version of the KMA and the logged on user.

User role operations are discussed on the following pages. They include:

- Operator (see [“Operator Role Functions” on page 292](#))
- Security Officer (see [“Security Officer Role Functions” on page 299](#))
- Other Roles (see [“Other Role Functions” on page 319](#))

## Operator

The following menu illustrates the options for an Operator role.

```
Key Management System Version xxx (KMA1)
-----
Please enter your User ID: OP

Please enter your Passphrase:

Key Management System Version xxx (OP on KMA1)
-----

(1)  Reboot KMA
(2)  Shutdown KMA
(3)  Technical Support
(4)  Primary Administrator
(5)  Set Keyboard Layout
(0)  Logout
-----

Please enter your choice:
```

## Security Officer

The following menu illustrates the options for an Security Officer role.

```
Key Management System Version xxx (KMA1)
-----
Please enter your User ID: SO

Please enter your Passphrase:

Key Management System Version xxx (SO on KMA1)
-----

(1)      Log KMA Back into Cluster
(2)      Set User's Passphrase
(3)      Set KMA Management IP Addresses
(4)      Set KMA Service IP Addresses
(5)      Modify Gateway Settings
(6)      Set DNS Settings
(7)      Reset to Factory Default State
(8)      Technical Support
(9)      Primary Administrator
(10)     Set Keyboard Layout
(0)      Logout
-----
Please enter your choice:
```

---

**Note** – If the user has been assigned both Operator and Security roles, then the menu options are combined as follows:

```

Key Management System Version xxx (KMA1)
-----
Please enter your User ID:

Please enter your Passphrase:

Key Management System Version xxx (xx on KMA1)
-----

(1)      Log KMA Back into Cluster
(2)      Set User's Passphrase
(3)      Set KMA Management IP Addresses
(4)      Set KMA Service IP Addresses
(5)      Modify Gateway Settings
(6)      Set DNS Settings
(7)      Reset to Factory Default State
(8)      Technical Support
(9)      Primary Administrator
(10)     Set Keyboard Layout
(0)      Logout
-----
Please enter your choice:

```

---

## Other Roles

For all other roles, that is, Backup Operator, Compliance Officer, and Auditor, a menu that is similar to the following is displayed. The only options available are to logout from the KMA and to set the keyboard layout.

```

Key Management System Version xxx (col)
-----

(1)  Set Keyboard Layout
(0)  Logout
-----
Please enter your choice:

```

## Operator Role Functions

This section describes the functions that an Operator can perform. They are:

- Rebooting the KMA
- Shutting down the KMA
- Enabling/disabling Technical Support
- Disabling the Primary Administrator
- Setting the keyboard layout
- Logging out of the KMA.

The Operator's menu is shown below.

```
Key Management System Version xxx (KMA1)
-----
Please enter your User ID: OP

Please enter your Passphrase:

Key Management System Version xxx (OP on KMA1)
-----

(1)  Reboot KMA
(2)  Shutdown KMA
(3)  Technical Support
(4)  Primary Administrator
(5)  Set Keyboard Layout
(0)  Logout
-----
Please enter your choice:
```

---

**Note** – The Technical Support and Primary Administrator menu items appear only when their settings are currently enabled.

---



## Rebooting the KMA

The Reboot KMA menu option allows an operator to stop and restart the KMA and reboot the operating system. This function is for troubleshooting purposes only.

To reboot the KMA:

1. At the `Please enter your choice:` prompt on the main menu, type **1** and press `<Enter>`. The following information is displayed, indicating that the support account is enabled.

```
Reboot KMA
-----
Press Ctrl-c to abort.
Are you sure that you want to reboot the KMA? [y/n]:
```

2. At the prompt, type **y** and press `<Enter>`. The current KMS Console session terminates as the KMA starts to reboot. After the KMA reboots, the KMS Console login prompt is displayed.

## Shutting Down the KMA

This option allows you to terminate (shut down) all services on the KMA and to physically shut down the KMA itself.

To shut down the KMA:

1. At the `Please enter your choice:` prompt on the main menu, type **2** and press `<Enter>`. The following information is displayed, indicating that the support account is enabled.

```
Shutdown KMA
-----
Press Ctrl-c to abort
Are you sure that you want to shut down the KMA? [y/n]:
```

2. At the prompt, type **y** and press `<Enter>`. The following information is displayed, indicating that the system is shutting down.

Shutting down...

3. The shutdown sequence is displayed. When it is finished, the following information is displayed.

Power down.

4. The KMA is now powered off. The KMA can be powered on using either the power button or the ELOM remote power control function.

## Enabling the Technical Support Account

The Technical Support menu option allows an operator to enable/disable the Operating System's support account and SSH access for that account. By default, both the Technical Support account and SSH access are disabled. Since the passphrase for the support account is only known by Sun Support, enabling of this account does not grant the Console user any further access to the KMA.

1. To enable the Technical Support account:

At the `Please enter your choice:` prompt on the main menu, type **3** and press `<Enter>`. The following information is displayed, indicating that the support account is disabled.

```
Technical Support
-----
Press Ctrl-c to abort.
Please refer to accompanying user documentation for Technical
Support contact information.
The support account is currently DISABLED.
***** IMPORTANT *****
Enabling the support account and SSH access is a security
risk. These should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
*****
Would you like to ENABLE this account? [y/n]:
```

2. At the prompt, type **y** and press `<Enter>`. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to commit these changes? [y/n]:
```

3. At the prompt, type **y** and press `<Enter>`. The following information is displayed, indicating that the account is enabled. Press `<Enter>` to return to the main menu.

```
Press Enter to continue:
```

## Disabling the Technical Support Account

To disable the Technical Support account:

1. At the Please enter your choice: prompt on the main menu, type **3** and press <Enter>. The following information is displayed, indicating that the support account is enabled.

```
Technical Support
-----
Press Ctrl-c to abort.
Please refer to accompanying user documentation for Technical
Support contact information.
The support account is currently ENABLED.
***** IMPORTANT *****
Enabling the support account and SSH access is a security
risk. These should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
*****
Would you like to DISABLE this account? [y/n]:
```

2. At the prompt, type **y** to disable the account and press <Enter>.
3. The following information is displayed, prompting you to confirm the change.  
Are you sure that you want to commit these changes? [y/n]:
4. At the prompt, type **y** and press <Enter>. The SSH service automatically stops.

## Disabling the Primary Administrator

The Primary Administrator menu option allows you to enable/disable Primary Administrator access on the KMA.

---

**Note** – This task can be *enabled* only by the Security Officer; it can be *disabled* by either an Operator or a Security Officer.

---

Disabling Primary Administrator access takes place immediately. If someone is connected as a Primary Administrator, and then this access is disabled, the next command they attempt will fail.

1. To disable Primary Administrator access:

At the Please enter your choice: prompt on the main menu, type 4 and press <Enter>. The following information is displayed, indicating that the access is enabled.

```
Primary Administrator
-----

Press Ctrl-c to abort.

The Primary Administrator role is currently ENABLED.

Would you like to DISABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to DISABLE these privileges for the
support account? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. At the prompt, type y to disable the account and press <Enter>.

3. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. At the prompt, type y and press <Enter>. The Primary Administrator access has been disabled.

## Setting the Keyboard Layout

This option allows you to change the keyboard layout from English to a variety of languages.

---

**Note** – The keyboard layout should be set to match the layout of the keyboard attached to the KMA in order for the KMA to correctly interpret key presses.

---

To set the keyboard layout:

1. At the Please enter your choice: prompt on the main menu, type **5** and press <Enter>. The following keyboard layouts are displayed.

```

Set Keyboard Layout
-----

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian      ( 2) Belarusian   ( 3) Belgian
( 4) Bulgarian    ( 5) Croatian     ( 6) Danish
( 7) Dutch         ( 8) Finnish      ( 9) French
(10) German        (11) Icelandic    (12) Italian
(13) Japanese-type6 (14) Japanese     (15) Korean
(16) Malta_UK      (17) Malta_US     (18) Norwegian
(19) Portuguese    (20) Russian       (21) Serbia-And-Montenegro
(22) Slovenian     (23) Slovakian    (24) Spanish
(25) Swedish       (26) Swiss-French (27) Swiss-German
(28) Taiwanese     (29) TurkishQ     (30) TurkishF
(31) UK-English    (32) US-English

The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:

```

2. At the Please enter the number for the keyboard layout: prompt, enter the number you want to change the keyboard layout to. The new keyboard layout is applied.
3. The following information is displayed. Press <Enter> to continue.

## Logging Out

To log out of the current KMS Console session:

1. At the `Please enter your choice:` prompt on the main menu, type **0** and press `<Enter>`.
2. The current session terminates and the login prompt is displayed allowing the user to re-enter the KMS Console.

## Security Officer Role Functions

This section describes the functions that a Security Officer can perform. They are:

- Logging the KMA into the Cluster
- Setting a User's Passphrase
- Setting the KMA Management IP addresses
- Setting the KMA Service IP addresses
- Modifying the Gateway settings
- Specifying the DNS settings
- Resetting the KMA to the Factory Default State
- Enabling/Disabling Technical Support
- Enabling/Disabling the Primary Administrator
- Setting the keyboard layout
- Logging out of the KMA.

The Security Officer's menu is shown below.

```

Key Management System Version xxx (KMA1)
-----
Please enter your User ID: SO

Please enter your Passphrase:

Key Management System Version xxx (SO on KMA1)
-----

(1)      Log KMA Back into Cluster
(2)      Set User's Passphrase
(3)      Set KMA Management IP Addresses
(4)      Set KMA Service IP Addresses
(5)      Modify Gateway Settings
(6)      Set DNS Settings
(7)      Reset to Factory Default State
(8)      Technical Support
(9)      Primary Administrator
(10)     Set Keyboard Layout
(0)      Logout
-----
Please enter your choice:

```

## Logging the KMA Back into the Cluster

This menu option allows a Security Officer to log the KMA back into the Cluster after its passphrase has been changed. Before you can perform this task:

1. Bring up the KMS Manager.
2. Log in to an existing KMA as a Security Officer.
3. Navigate to the KMA List panel.
4. Create a KMA entry.

To log the KMA into the Cluster:

1. At the `Please enter your choice:` prompt on the main menu, type **1** and press `<Enter>`. The following information is displayed.

```
Log KMA Back into Cluster
-----
Press Ctrl-c to abort.
Please enter the Management Network IP Address of an existing
KMA in the cluster:

The KMA Passphrase is a Passphrase that you have
previously configured for this KMA to join a Cluster.

Please enter this KMA's Passphrase:
```

2. Log in to an existing KMA (for example, 129.80.60.172) as a Security Officer.
3. At the prompt, type the passphrase that was originally configured for the KMA, to join the Cluster and press `<Enter>`.

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #1:

Please enter Key Split Passphrase #1:

Press Enter to continue:
```

4. Enter the first Key Split user name established during QuickStart for the first KMA in the KMS Manager Modify Key Split Credentials function (refer to [“Modifying the Key Split Configuration”](#) on page 178).

---

**Note** – The Security Officer needs to know how many Key Split users to enter, that is, what the Key Split Threshold is. In this example, the Key Split Threshold is 2.

---



5. Type the passphrase for the Key Split user, and press <Enter>.

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #2:

Please enter Key Split Passphrase #2:

Press Enter to continue:
```

6. Enter the second Key Split user name.
7. Type the passphrase for the Key Split user, and press <Enter>

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #3:

Are you sure that you want to log the KMA back into the Cluster?
[y/n]: n

Press Enter to continue:
```

8. Press <enter> next to Key Split User Name #3 to end Key Split user authorization.
9. Type **n**, and press <Enter>.

## Setting a User's Passphrase

This menu option allows a Security Officer to set the passphrase for any user, including the Security Officer.

To set a user's passphrase:

1. At the Please enter your choice: prompt on the main menu, type **2** and press <Enter>. The following information is displayed.

```
Set User's Passphrase
-----
Press Ctrl-c to abort.
Please enter the User Name:
```

2. At the prompt, type the name of the user and press <Enter>. The following information is displayed.

```
Passphrases must be at least 8 characters and at most 64
characters in length.
Passphrases must not contain the User's User Name.
Passphrases must contain characters from 3 of 4 character
classes (uppercase, lowercase, numeric, other).

Please enter the desired Passphrase:

Please re-enter the desired Passphrase:

Press Enter to continue:
```

3. At the prompt, type the passphrase and press <Enter>.
4. At the Please re-enter the desired Passphrase: prompt, type the same passphrase and press <Enter>. The following information is displayed, indicating that the passphrase is set. Press <Enter> to return to the main menu.

Press Enter to continue:

## Setting the KMA Management IP Address

This option modifies the Management address settings for the KMA. Initially, this information is set in the QuickStart program (see [“Specifying the Network Configuration” on page 27](#)), and can be changed here.

Note that in a large, multi-site Cluster, drives may only have connections to a subset of all the KMAs in the Cluster. This caution applies to the set of KMAs the drive can connect to.

---

**Caution –** This function should be used carefully. If you change the information for one KMA, all the other KMAs receive the updates immediately, assuming they are connected. If the KMA is disconnected, it updates the other KMAs when it is able to reconnect.

However, if for example you have two KMAs that are not connected to each other (network outage), and you change both IP addresses, they will not be able to reconnect when the network is repaired.

In this case, you must use the procedure for [“Logging the KMA Back into the Cluster” on page 300](#) on one KMA to reconnect it with the other, and the Passphrase must be updated first. For example, if KMAs A and B are disconnected, and you change both IP addresses, then you must log into A and change B's passphrase. Then log into B's console and use the procedure for [“Logging the KMA Back into the Cluster” on page 300](#) to re-attach it to A.

Care must also be taken with tape drives. Tape drives do not automatically receive the updated IP information; they only get updated IP information when a tape is mounted. Thus, if you are in a typical environment where tape jobs only run at night, and you change all the KMA's IP addresses during the day, the drives will not be able to communicate with any KMA. If this happens, the drives must be re-enrolled with the KMS Cluster. To avoid this, change KMA IP addresses one at a time, wait for all drives to receive the change, then change the next.

---

To set the KMA Management IP addresses:

1. At the Please enter your choice: prompt on the main menu, type **3** and press <Enter>.

The current KMA Management IP address settings are displayed. The IPv6 address fields are blank when the KMA is not configured to use IPv6 addresses.

```

Set KMA Management IP Addresses
-----

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other KMAs or Users in your system.

Current settings:
  Management Configuration : Static
  Management IP Address    : 10.80.180.39
  Management Subnet Mask   : 255.255.254.0
  Management IPv6 Addresses: fe80::216:36ff:feca:15b6/10
                           2005::216:36ff:feca:15b6/64

Do you want to configure the Management Network interface to have
an IPv6 address? [y/n]:

Do you want to use DHCP to configure the Management Network
interface? [y/n]:

Please enter the Management Network IP Address [10.80.180.39]:

Please enter the Management Network Subnet Mask [255.255.254.0]:

Are you sure that you want to commit these changes? [y/n]: y
  
```

2. Type either **n** or **y** at the Do you want to configure the Management Network interface to have an IPv6 address prompt.
3. Type either **n** or **y** at the Do you want to use DHCP to configure the Management Network interface prompt. If you type **n**, go to [Step 4](#). If you type **y**, go to [Step 6](#).
4. At the prompt, type the Management Network IP address and press <Enter>.
5. At the Please enter the Management Network Subnet Mask: prompt, type the subnet mask address, (for example **255.255.254.0**) and press <Enter>.
6. Type **y** at the Are you sure that you want to commit these changes? [y/n]: prompt.

## Setting the KMA Service IP Addresses

This option modifies the Service address settings for the KMA. Initially, this information is set in the QuickStart program (see [“Specifying the Network Configuration” on page 27](#)), and can be changed here.

Note that in a large, multi-site Cluster, drives may only have connections to a subset of all the KMAs in the Cluster. This caution applies to the set of KMAs the drive can connect to.

---

**Caution –** This function should be used carefully. If you change the information for one KMA, all the other KMAs receive the updates immediately, assuming they are connected. If the KMA is disconnected, it updates the other KMAs when it is able to reconnect.

However, if for example you have two KMAs that are not connected to each other (network outage), and you change both IP addresses, they will not be able to reconnect when the network is repaired.

In this case, you must use the procedure for [“Logging the KMA Back into the Cluster” on page 300](#) on one KMA to reconnect it with the other, and the Passphrase must be updated first. For example, if KMAs A and B are disconnected, and you change both IP addresses, then you must log into A and change B's passphrase. Then log into B's console and use the procedure for [“Logging the KMA Back into the Cluster” on page 300](#) to re-attach it to A.

Care must also be taken with tape drives. Tape drives do not automatically receive the updated IP information; they only get updated IP information when a tape is mounted. Thus, if you are in a typical environment where tape jobs only run at night, and you change all the KMA's IP addresses during the day, the drives will not be able to communicate with any KMA. If this happens, the drives must be re-enrolled with the KMS Cluster. To avoid this, change KMA IP addresses one at a time, wait for all drives to receive the change, then change the next.

---

The current KMA Service IP address settings are displayed. The IPv6 address fields are blank when the KMA is not configured to use IPv6 addresses.

```

Set KMA Service IP Addresses
-----

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other Agents in your system.

Current settings:
  Service Configuration : Static
  Service IP Address    : 192.168.1.39
  Service Subnet Mask   : 255.255.255.0
  Service IPv6 Addresses: fe80::216:36ff:feca:15b9/10
                        2005::216:36ff:feca:15b9/64

Do you want to configure the Service Network interface to have an
IPv6 address?
[y/n]: y

Do you want to use DHCP to configure the Service Network interface?
[y/n]: n

Please enter the Service Network IP Address [192.168.1.39]:

Please enter the Service Network Subnet Mask [255.255.255.0]:

Are you sure that you want to commit these changes? [y/n]: y

```

1. At the Please enter your choice: prompt on the main menu, type **4** and press <Enter>.
2. Type either **n** or **y** at the Do you want to configure the Service Network interface to have an IPv6 address prompt.
3. Type either **n** or **y** at the Do you want to use DHCP to configure the Service Network interface prompt. If you type **n**, go to [Step 4](#). If you type **y**, go to [Step 6](#).
4. At the prompt, type the Service Network IP address and press <Enter>.
5. At the Please enter the Service Network Subnet Mask: prompt, type the subnet mask address, (for example **255.255.255.0**) and press <Enter>.
6. Type **y** at the Are you sure that you want to commit these changes? [y/n]: prompt.

## Viewing/Adding/Deleting Gateways

This menu option shows the current gateway settings (five gateways to a page) on the Management (M) and Service (S) network interfaces and asks the user to add a gateway, remove a gateway, or accept the current gateway configuration.

```

Modify Gateway Settings
-----

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

  # Destination                Gateway                Netmask                IF
  -----
  1 default                    10.80.181.254         0.0.0.0                M
  2 default                    10.80.181.21          0.0.0.0                M
  3 default                    192.168.1.119         0.0.0.0                S
  4 10.0.0.0                   10.80.180.25          255.255.254.0         M
*  5 10.80.180.0               10.80.180.39          255.255.254.0         M

Press Enter to continue:

Modify Gateway Settings
-----

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

  # Destination                Gateway                Netmask                IF
  -----
*  6 192.168.1.0               192.168.1.39          255.255.255.0         S
  7 192.168.25.0               10.80.180.25          255.255.255.0         M
  8 192.168.26.0               10.80.180.25          255.255.255.0         M
*  9 127.0.0.1                 127.0.0.1             255.255.255.255
* 10 fe80::                     fe80::216:36ff:feca:15b6 10                    M

(1) Continue
(2) Back
1

```

# Modify Gateway Settings

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are indicated with an asterisk (\*). Management routes are indicated with an 'M', and service routes with an 'S'.

| #    | Destination | Gateway                  | Netmask | IF |
|------|-------------|--------------------------|---------|----|
| * 11 | fe80::      | fe80::216:36ff:feca:15b9 | 10      | S  |

You can add a route, delete a route, or exit the gateway configuration. Please choose one of the following:

- (1) Add a gateway
  - (2) Remove a configured gateway (only if modifiable)
  - (3) Exit gateway configuration
  - (4) Display again
- 3

1. At the Please enter your choice: prompt on the main menu, type **5** and press <Enter>.
2. At the (1)Continue (2)Back prompt, type **1** to display the next few gateways or **2** to display the previous few gateways.
3. When the last gateways are displayed, at the Please choose one of the following: prompt, type **1, 2, 3, or 4** and press <Enter>.

---

**Note** – If at any time the user presses Ctrl+c, no changes are saved and the user is returned to the main menu.

---



## Specifying the DNS Settings

This menu option shows the DNS settings, and prompts the user for a new DNS domain (if you want to configure one) and the DNS server IP addresses.

```

Set DNS Configuration
-----

Press Ctrl-c to abort.

DNS configuration is optional, but necessary if this KMA
will be configured using hostnames instead of IP addresses.

Current DNS configuration:

Domain: central.sun.com
Nameservers: 10.80.0.5

Please enter the DNS Domain (blank to unconfigure DNS):
central.sun.com

Up to 3 DNS Name Servers can be entered. Enter each name
server separately, and enter a blank name to finish.

Please enter DNS Server IP Address #1: 10.80.0.5

Please enter DNS Server IP Address #2:

```

1. At the Please enter your choice: prompt on the main menu, type **6** and press <Enter>.
2. Enter the DNS domain name at the Please enter the DNS Domain (blank to unconfigure DNS): prompt.
3. Enter the DNS server IP address at the Please enter DNS Server IP address prompt. You can enter up to three IP addresses.
4. Press <Enter>, without specifying an IP address, to finish.

## Resetting the KMA to the Factory Default

This menu option allows a Security Officer to reset the KMA to its factory default state.

---

**Warning** – The reset is not recoverable; the information on the KMA is gone.

---

This is a destructive process that results in the loss of all data that is stored on the hard disk. The system is forced to reboot and the file systems are reformatted and prepared to use the new encryption keys.

To reset the KMA to the factory default:

1. At the `Please enter your choice:` prompt on the main menu, type **4** and press `<Enter>`. The following information is displayed.

```
Reset to Factory Default State
-----

Press Ctrl-c to abort.

WARNING:
All information stored on this KMA will be destroyed!
Access to all protected data will be lost unless a backup
of the KMA data has been created or Cluster Peer
KMAs are present.
Please consult the Administrative Guide before proceeding
with this operation.

The system will be rebooted after performing the reset.

Zeroize KMA before resetting (this process will take approximately
4 hours) [y/n]:

Are you sure that you want to reset the KMA to the
Factory Default State?

Type RESET to confirm: no

Press Enter to continue:
```

---

**Warning** – All information on this KMA will be destroyed. Access to all protected data will be lost unless a backup of the KMA's data has been created or Cluster Peer KMAs are present.

---

2. At the `Zeroize KMA before resetting` prompt, enter either **n** or **y**. If you enter **y**, this will securely wipe all information off the hard drive.

---

**Note** – This operation takes approximately four hours.

---

3. At the `Type RESET to confirm` prompt, type `RESET` and press `<Enter>`. The following information is displayed, indicating that the KMA is resetting.

Resetting...

4. Once the authentication is completed, you are returned to QuickStart. See [“Running the QuickStart Program” on page 25](#).

## Enabling the Technical Support Account

The Technical Support menu option allows an operator to enable/disable the Operating System's support account and SSH access for that account. By default, both the Technical Support account and SSH access are disabled. Since the passphrase for the support account is only known by Sun Support, enabling of this account does not grant the Console user any further access to the KMA.

1. To enable the Technical Support account:

At the `Please enter your choice:` prompt on the main menu, type **5** and press `<Enter>`. The following information is displayed, indicating that the support account is disabled.

```
Technical Support
-----
Press Ctrl-c to abort.
Please refer to accompanying user documentation for Technical
Support contact information.
The support account is currently DISABLED.
***** IMPORTANT *****
Enabling the support account and SSH access is a security
risk. These should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
*****
Would you like to ENABLE this account? [y/n]:
```

2. At the prompt, type **y** to enable the account and press `<Enter>`. The following information is displayed, indicating that the SSH access is disabled. Enabling SSH access allows Technical Support to diagnose a problem remotely.

```
SSH access for the support account is currently DISABLED.
Enabling SSH access for the support account allows a
Technical Support representative to connect to the KMA
from a remote location in order to diagnose a potential
problem.
Would you like to ENABLE SSH access for the support account? [y/n]:
```

3. At the prompt, type **y** and press `<Enter>`. The following information is displayed, indicating the purpose of SSH Host keys.

When a Technical Support representative connects to the KMA using SSH, SSH host keys must be verified via an alternative secure communication channel in order to detect a potential "man-in-the-middle" attack. Please record and store these SSH host keys securely.

SSH host keys are generated when SSH is enabled for the first time. They may be subsequently regenerated to invalidate the existing SSH host keys.

Would you like to regenerate the SSH host keys? [y/n]:

4. At the prompt, type **y** and press <Enter>. The following information is displayed, prompting you to confirm the change.

Are you sure that you want to commit these changes? [y/n]:

5. At the prompt, type **y** and press <Enter>. The following information is displayed, indicating that the account is enabled. Press <Enter> to return to the main menu.

Press Enter to continue:

## Disabling the Technical Support Account

To disable the Technical Support account:

1. At the Please enter your choice: prompt on the main menu, type **5** and press <Enter>. The following information is displayed, indicating that the support account is enabled.

```
Technical Support
-----
Press Ctrl-c to abort.
Please refer to accompanying user documentation for Technical
Support contact information.
The support account is currently ENABLED.
***** IMPORTANT *****
Enabling the support account and SSH access is a security
risk. These should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
*****
Would you like to DISABLE this account? [y/n]:
```

2. At the prompt, type **y** to disable the account and press <Enter>.
3. The following information is displayed, prompting you to confirm the change.  
Are you sure that you want to commit these changes? [y/n]:
4. At the prompt, type **y** and press <Enter>. The SSH service automatically stops.

## Enabling the Primary Administrator

The Primary Administrator menu option allows you to enable/disable Primary Administrator access on the KMA.

- To enable Primary Administrator access, you must first enable Technical Support (option 5).
- This task can be *enabled* only by the Security Officer; it can be *disabled* by either an Operator or a Security Officer.

---

**Caution** – The Primary Administrator function allows someone logged in as Technical Support to gain Primary Administrator access, equivalent to root access. While dangerous, this may be necessary in some situations to recover the system from a problem, however, you may need direct guidance from back line support or engineering.

---

1. To enable Primary Administrator access:

At the Please enter your choice: prompt on the main menu, type **6** and press <Enter>. The following information is displayed, indicating that the access is disabled.

```
Primary Administrator
-----

Press Ctrl-c to abort.

The Primary Administrator role is currently DISABLED.

***** WARNING *****
Providing the support account with Primary Administrator
privileges
is a security risk. This setting should not be left enabled unless
required for troubleshooting purposes.

Ensure that these privileges are disabled when not required.
*****

Would you like to ENABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to ENABLE these privileges for the
support account, assuming this security risk? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. At the prompt, type **y** to enable the account and press <Enter>.
3. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to ENABLE these privileges for the
support account, assuming this security risk? [y/n]:
```

4. At the prompt, type **y** and press <Enter>. The Primary Administrator access has been enabled.

## Disabling the Primary Administrator

The Primary Administrator menu option allows you to enable/disable Primary Administrator access on the KMA.

---

**Note** – This task can be *enabled* only by the Security Officer; it can be *disabled* by either an Operator or a Security Officer.

---

Disabling Primary Administrator access takes place immediately. If someone is connected as a Primary Administrator, and then this access is disabled, the next command they attempt will fail.

1. To disable Primary Administrator access:

At the Please enter your choice: prompt on the main menu, type **6** and press <Enter>. The following information is displayed, indicating that the access is enabled.

```
Primary Administrator
-----

Press Ctrl-c to abort.

The Primary Administrator role is currently ENABLED.

Would you like to DISABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to DISABLE these privileges for the
support account? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. At the prompt, type **y** to disable the account and press <Enter>.

3. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. At the prompt, type **y** and press <Enter>. The Primary Administrator access has been disabled.



## Setting the Keyboard Layout

This option allows you to change the keyboard layout from English to a variety of languages.

---

**Note** – The keyboard layout should be set to match the layout of the keyboard attached to the KMA in order for the KMA to correctly interpret key presses.

---

To set the keyboard layout:

1. At the `Please enter your choice:` prompt on the main menu, type `7` and press `<Enter>`. The following keyboard layouts are displayed.

```
Set Keyboard Layout
-----

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian      ( 2) Belarusian   ( 3) Belgian
( 4) Bulgarian     ( 5) Croatian     ( 6) Danish
( 7) Dutch         ( 8) Finnish      ( 9) French
(10) German        (11) Icelandic    (12) Italian
(13) Japanese-type6 (14) Japanese     (15) Korean
(16) Malta_UK      (17) Malta_US     (18) Norwegian
(19) Portuguese    (20) Russian      (21) Serbia-And-Montenegro
(22) Slovenian     (23) Slovakian    (24) Spanish
(25) Swedish       (26) Swiss-French (27) Swiss-German
(28) Taiwanese     (29) TurkishQ     (30) TurkishF
(31) UK-English    (32) US-English

The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:
```

2. At the `Please enter the keyboard layout [ US-English ] :` prompt, enter the language to want to change the keyboard layout to.
3. At the prompt, type `y` and press `<Enter>`. The following information is displayed, indicating that the change has been made. Press `<Enter>` to return to the main menu.

The keyboard layout has been applied successfully.

Press Enter to continue:

## Logging Out

To log out of the current KMS Console session:

1. At the `Please enter your choice:` prompt on the main menu, type **0** and press `<Enter>`.
2. The current session terminates and the login prompt is displayed allowing the user to re-enter the KMS Console.

## Other Role Functions

This section describes the functions the other roles (Compliance Officer, Backup Operator, Auditor) can perform. They are:

- Setting the keyboard layout
- Logging out of the KMA

```
Key Management System Version xxx (col)
```

```
-----
```

```
(1) Set Keyboard Layout
```

```
(0) Logout
```

```
-----
```

```
Please enter your choice:
```

## Setting the Keyboard Layout

This option allows you to change the keyboard layout from English to a variety of languages.

---

**Note** – The keyboard layout should be set to match the layout of the keyboard attached to the KMA in order for the KMA to correctly interpret key presses.

---

To set the keyboard layout:

1. At the Please enter your choice: prompt on the main menu, type **1** and press <Enter>. The following keyboard layouts are displayed.

```

Set Keyboard Layout
-----

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian      ( 2) Belarusian   ( 3) Belgian
( 4) Bulgarian    ( 5) Croatian     ( 6) Danish
( 7) Dutch         ( 8) Finnish      ( 9) French
(10) German        (11) Icelandic    (12) Italian
(13) Japanese-type6 (14) Japanese     (15) Korean
(16) Malta_UK      (17) Malta_US     (18) Norwegian
(19) Portuguese    (20) Russian       (21) Serbia-And-Montenegro
(22) Slovenian     (23) Slovakian    (24) Spanish
(25) Swedish       (26) Swiss-French (27) Swiss-German
(28) Taiwanese     (29) TurkishQ     (30) TurkishF
(31) UK-English    (32) US-English

The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:

```

2. At the Please enter the keyboard layout [ US-English ] : prompt, enter the language to want to change the keyboard layout to.
3. At the prompt, type **y** and press <Enter>. The following information is displayed, indicating that the change has been made. Press <Enter> to return to the main menu.

The keyboard layout has been applied successfully.

Press Enter to continue:

## Logging Out

To log out of the current KMS Console session:

1. At the `Please enter your choice:` prompt on the main menu, type **0** and press `<Enter>`.
2. The current session terminates and the login prompt is displayed allowing the user to re-enter the KMS Console.



## SNMP Management Information Base (MIB) Data

This appendix describes SNMP information for users who have configured an SNMP Agent in their network and have defined SNMP Managers in the KMS Manager GUI. When at least one SNMP Manager is defined in the KMS Manager GUI, the KMAs will send SNMP Informs to the IP address of that SNMP Manager(s).

The KMAs use Object Identifiers (OIDs) to send the following information:

**TABLE P-1** KMA Object Identifiers

| OID Value          | Type   | Description           |
|--------------------|--------|-----------------------|
| 1.3.6.1.4.1.42.2   | ---    | Generic trap          |
| 1.3.6.1.4.1.42.2.1 | string | Date/time             |
| 1.3.6.1.4.1.42.2.2 | string | Audit event class     |
| 1.3.6.1.4.1.42.2.3 | string | Audit event operation |
| 1.3.6.1.4.1.42.2.4 | string | Audit event condition |
| 1.3.6.1.4.1.42.2.5 | string | Entity ID             |
| 1.3.6.1.4.1.42.2.6 | string | Network address       |
| 1.3.6.1.4.1.42.2.7 | string | Message               |

Refer to [“SNMP Manager List Menu” on page 131](#) for details on viewing, creating, and modifying SNMP managers.





---

# Glossary

---

---

## A

**Abnormal end of task**

(**abend**) A software or hardware problem that terminates a computer processing task.

**Advanced Encryption**

**Standard (AES)** A FIPS-approved NIST cryptographic standard used to protect electronic data.

**AES** See Advanced Encryption Standard.

**Agent** Various types of encryption agents can be created to interact with the KMS for creating and obtaining keying material. The Sun StorageTek T10000 models A and B, T9840D, and the HP LTO4 tape drives are types of encryption agents when enabled for encrypting.

**Agent API** See Agent Library API.

**Agent Library** The Agent Library is used by an Agent to retrieve key material from a KMS.

**Agent Library API** The API provided by the Agent Library. Agents call this API.

**Audit** See Audit Log.

**Audit Log** The KMS Cluster maintains a log of all auditable event occurring throughout the system. Agents may contribute entries to this log for auditable events.

**Auditor** A user role that can view system audit trails (Audit List events and KMA security parameters).

**Autonomous Lock** When autonomous unlock is enabled a quorum of Security Officers is required to unlock a locked KMA. When disabled, the KMA can be unlocked by any Security Officer.

---

## B

**Backup File**The file created during the backup process that contains all the information needed to restore a KMA. Encrypted with a key generated specifically for the backup. The key is contained in the corresponding backup key file.

**Backup Key File**A file generated during the backup process containing the key used to encrypt the backup file. This file is encrypted using the system master key. The master key is extracted from the core security backup file using a quorum of the key split credentials.

**Backup Operator**A user role that is responsible for securing and storing data and keys.

**BOT**Beginning of Tape.

---

## C

**CA**See Certificate Authority (CA).

**Certificate**A Certificate is a digitally-signed document that serves to validate the holder's authorization and name. The document consists of a specially formatted block of data that contains the name of the certificate holder (Subject DN), a serial number, validity dates, holder's public key, Issuer's DN, and the digital signature of the Issuer for authentication. The Issuer attests that the holder's name is the one associated with the public key in the document.

**Certificate Authority**

**(CA)**A Certificate Authority registers end-users, issues their certificates, and can also create CAs below them. The KMAs themselves act as the certificate authority to issue certificates to users, agents, and other KMAs.

**Cluster**A Cluster is a set of Key Management Appliances that are grouped together into a single system to enhance fault tolerance, availability, and scalability.

**Communications key**Adds another layer of encryption and authentication during transmission over a LAN from the token to the drive.

**Compliance Officer**A user role that manages the flow of data through your organization and can define and deploy data contexts (Key Groups) and rules that determine how data is protected and ultimately destroyed (Key Policies).

**Critical Security**

**Parameter**Security-related information (for example, secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.

**Crypto-Accelerator**A Crypto-Accelerator is a hardware device (a card) that can be used to increase the rate of data encryption/decryption, thereby improving system performance in high demand conditions.

**Crypto-active**And encryption-capable tape drive that has had the encryption feature turned on in the drive.

**Crypto-ready**A tape drive that has the ability to turn on device encryption and become encryption-capable.

**Cryptography**The art of protecting information by transforming it (encrypting) into an unreadable format, called cipher text. Only those who possess a special *key* can decipher (decrypt) the message into its original form.

**Cryptoperiods**The length of time in which a key can be used for encryption. It starts when the key is first assigned to the drive. This value corresponds to the “Originator Usage Period” in NIST 800-57.

---

## D

**Data Unit**Data units are abstract entities within the KMS that represent storage objects associated with KMS policies and encryption keys. The concrete definition of a data unit is defined by the Encryption Agent that creates it. For tape drives, a data unit is a tape cartridge.

**Device key**Enables the tape drive for encryption. KMS Version 1.x term.

---

## E

**EKT**Enabling key token (device keys). KMS Version 1.x term.

**Enable key**Unique 64 character key used to enable the tape drive. See also PC Key.

**Encryption**The translation of data into a secret code. Encryption is one of the most effective ways to achieve data security. To read an encrypted file, you must have access to a special key or password that enables you to decipher it.

---

## F

**FIPS**Federal Information Processions Standards. The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration and Laboratories, which develops and promotes standards and technology, including:

- Computer Security Division and Resource Center (CSRC)
- Federal Information Processing Standards (FIPS)

For more information visit:  
<http://www.nist.gov/>

---

## G

**GUI**Graphical User Interface.

---

## H

### Hash Message Authentication Code

**(HMAC)**In cryptography, a keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key.

---

## I

**Internet Protocol (IP)**A protocol used to route data from its source to its destination in an Internet environment.

### Internet Protocol (IP)

**address**A four-byte value that identifies a device and makes it accessible through a network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0 to 255. For example, 129.80.145.23 could be an IP address.  
Also known as TCP/IP address.

---

## K

**Key**A key in this context is a symmetric data encryption key. Agents can request new key material for encrypting data corresponding to one or more Data Units. A key belongs to a single Key Group so that only Agents associated with the Key Group can access the key. Keys have encryption and decryption cryptoperiods that are dictated by the Key Policy associated with the Key Group of the particular key. The type of key (that is, its length and algorithm) is specified by the Encryption Agent.

**Keys**A random string of bits generated by the key management system, entered from the keyboard or purchased. Types of keys include:

- Device keys enable the tape drive encryption feature.
- Media keys encrypt and decrypt customer data on a tape cartridge.
- PC Keys enable the tape drive for encryption.
- Communication key adds another layer of encryption (authentication) to the media key during transmission over the LAN from the token to the drive.
- Split keys are unique to each drive and work with the wrap key for protection.
- Wrap keys encrypt the media key on the LAN and the token.

**Key Group** Key Groups are used for organizing keys and associating them with a Key Policy. Key Groups are also used to enforce access to the key material by the Encryption Agents.

#### **Key Management**

**Appliance (KMA)** A SunFire X2100-M2 server preloaded with the KMS software. The appliance is a proven, dual-core processor with a Solaris 10 operating system that delivers policy-based key management and key provisioning services.

#### **Key Management System**

**(KMS)** A system providing key management. The Sun StorageTek system has a KMS component providing key management on behalf of encryption agents.

**Key Policy** A Key Policy provides settings for the cryptoperiods to be applied to keys. Each Key Group has a Key Policy, and a Key Policy may apply to zero or more Key Groups. The encryption and decryption cryptoperiods specified on the policy limit the usage of keys and trigger key life cycle events, such as the deactivation or destructions of keys.

Key Policies also control where keys governed by the Key Policy can be exported to other Key Transfer Partners or imported from other Key Transfer Partners.

**Key Transfer File** A file containing keys and associated data units (if defined) used to move key material from one KMS Cluster to another. Both parties to the transfer must configure a key transfer partner of the other party to the exchange. The key transfer file is signed and encrypted to ensure both privacy of the transferred information as well its integrity.

**Key Transfer Partner** The Key Transfer Partner is the recipient of keys being exported from one KMS to another.

**KMA** See Key Management Appliance.

**KMS** See Key Management System.

**KMS Cluster** A set of one or more interconnected KMAs. All the KMAs in a KMS Cluster should have identical information. This will not be the case only when a KMS is down, or when a newly created piece of information has not yet propagated through all KMAs in the KMS Cluster. An action taken on any KMA in the KMS Cluster will eventually propagate to all KMAs in the KMS Cluster.

---

## M

**Media key** Encrypts and decrypts customer data on a tape cartridge.

---

## N

**network** An arrangement of nodes and branches that connects data processing devices to one another through software and hardware links to facilitate information interchange.

**NIST** National Institute of Standards and Technology.

---

## O

**OKT**Operational key token (media keys). KMS Version 1.x term.

**Operator**A user role responsible for managing the day-to-day operations of the system.

---

## P

**PC Key**Enables the tape drive to read and write in encrypted mode.

---

## R

**Read key**This is a media key that is used when reading data from a tape.

**Rijndael algorithm**An algorithm selected by the U.S. National Institute of Standards and Technology (NIST) for the Advanced Encryption Standard (AES). Pronounced “rain-dahl,” the algorithm was designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, whose surnames are reflected in the cipher's name.

**RSA**In cryptography, **RSA** is an algorithm for public-key cryptography created by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. The letters **RSA** are the initials of their surnames.

---

## S

### Secure Hash Algorithms

**(SHA)**Secure Hash Algorithms are cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.

**Security Officer**A user role that manages security settings, users, sites, and Transfer Partners.

**Security Policy**A rigorous statement of the sensitivity of organizational data, various subjects that can potentially access that data, and the rules under which that access is managed and controlled.

**Shamir's Secret Sharing**An algorithm in cryptography where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore a quorum or threshold scheme is used.

**Site**A site is an attribute of each KMS and Encryption Agent that indicates network proximity, or locality. Encryption Agents should try first to contact a KMA at the same site, then try to contact a KMA at a different site if no KMA at the local site responds.

**System Dump**A user-invoked operation that results in all the relevant data being collected into a single file and then that file being downloaded to the machine from which the user invoked this operation. Once the download is complete, this file is deleted from the KMA.

---

## T

**T10000 tape drive**The T10000 tape drive is a small, modular, high-performance tape drive designed for high-capacity storage of data—up to 500 gigabytes (GB) of uncompressed data.

**Token**KMS Version 1.x term.

Tokens are handheld, intelligent devices that connect to a token bay with an Ethernet connection. The two roles of the tokens are:

- Enabling key token
- Operational key token

**Token bay**KMS Version 1.x term.

A chassis that houses the physical tokens and provides power and connectivity for one or two tokens through the rear blind-mating connector. The token bay is compatible with a standard 19-inch rack—a 1U form factor. The token bay comes in two styles: desktop and rack-mount.

**Transport Layer Security**

(TLS)A cryptographic protocol that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.

---

## U

**UID**A string that serves as a unique identifier for a KMS entity, e.g. an encryption agent or user.

**Ultra Tape Drive**

**Encryption Agent**Ultra-compliant encrypting tape drives utilize Ultra Tape Drive Encryption Agent software for key management. These drives acquire key material from the KMS to be used with tape volumes. Each write from BOT results in the use of fresh key material being used for encryption of data on the volume. Consequently, the definition of a data unit maps to a tape volume where the external ID of the data unit is the volume serial number.

**UTC**Coordinated Universal Time.

---

## V

**Volume Serial Number**A six-character alphanumeric label used to identify a tape volume.

## W

**Wrap key**Encrypts the media keys on the LAN and on the token.

**Write key**This is a media key that is used when writing data to a tape.

---

## Z

**Zeroize**To erase electronically stored data, cryptographic keys, and Critical Security Parameters by altering or deleting the contents of the data storage to prevent recovery of the data.



# Index

---

## A

- abnormal end of task (abend), defined 325
- adding agents to a KMA, QuickStart Program 50
- adding gateways, KMS Console 307
- adding gateways, QuickStart Program 29
- adding gateways, QuickStart program 29
- Adjust System Time menu 191
- Advanced Encryption Standard (AES), defined 325
- AES, defined 325
- Agent Assignment to Key Groups menu 212
- Agent library API, defined 325
- Agent library, defined 325
- Agent List menu 245
- Agent, defined 325
- Agent, definition 1
- Agents
  - assigning a Key Group to 221
  - assigning to a Key Group 214
  - creating 249
  - deleting 254
  - removing a Key Group from 223
  - removing an Agent from a Key Group 216
  - setting passphrases 253
  - viewing an Agent list 246
  - viewing or modifying agent details 252
- applying software upgrades 270
- assigning a Key Group to a Transfer Partner 227
- assigning a Key Group to an Agent 221
- assigning a Transfer Partner to a Key Group 231
- assigning an Agent to a Key Group 214
- audience, intended xxi
- Audit Event List menu 235
- Audit Logs
  - defined 325

- exporting 240
  - viewing 235
  - viewing details 239

## Auditor

- defined 325
- description 13
- operations 285
- role 285

autonomous lock, defined 325

Autonomous Unlock Option menu 180

Autonomous Unlock option, caution 37

## B

Backup command line utility

- description 279

- IPv6 addresses with Zone IDs 280

backup Core Security 175

backup file, defined 326

backup files

- confirming destruction of 278

- creating 277

- restoring 165

- viewing details 163, 275

- viewing history 160, 274

backup key file, defined 326

Backup List menu 159, 273

Backup Operator

- defined 326

- description 13

- operations 273

- role 273

## C

Certificate Authority, defined 326

certificate, defined 326

changing the passphrase 90

clock, adjusting the local clock 191

Cluster

- connecting to 85

- defined 326

- definition 1

- joining an existing, QuickStart program 40

- logging the KMA back into 300

Cluster profile

- creating 85

- deleting 89

command line utility, Backup

- description 279

- IPv6 addresses with Zone IDs 280

- communications key, defined 326
- Compliance Officer
  - defined 326
  - description 13
  - operations 193
  - role 193
- configuration settings, specifying 91
- configuration, network information 187
- configuring Key Transfer Partners 139
- configuring the Cluster, QuickStart program 33
- confirming destruction of backup files 278
- connecting to the KMS 85
- console, remote connection to (ELOM) 20
- contacting Sun Microsystems StorageTek Support xxiv
- conventions, typographic xxvi
- Core Security
  - creating a backup 175
  - description 173
- Core Security Management menu 174
- creating a Cluster profile 85
- creating a Core Security backup 175
- creating a Key Transfer Public Key 158
- creating a KMA 102
- creating a site 127
- creating a system dump 168
- creating a Transfer Partner 147
- creating a user 113
- creating an Agent 249
- creating an SNMP Manager 134
- creating backup files 277
- creating Key Groups 208
- creating Key Policies 198
- critical security parameter, defined 326
- Crypto-Accelerator, defined 326
- crypto-active, defined 326
- cryptography, defined 327
- cryptoperiods 327
- crypto-ready, defined 326
- customer support xxiii
- customer-accessible documents, website xxii
- customer-initiated maintenance (CIM) xxiv

## D

- Data Unit List menu 258
- data unit, defined 327
- Data Units
  - description 258

- destroying post-operational keys 268
  - modifying details 262
  - viewing 259
  - viewing details 262
- deleting a Cluster profile 89
- deleting a KMA 108
- deleting a site 130
- deleting Agents 254
- deleting an SNMP Manager 137
- deleting gateways, KMS Console 307
- deleting gateways, QuickStart Program 29
- deleting gateways, QuickStart program 29
- deleting Key Groups 211
- deleting Key Policies 201
- deleting users 119
- destroying post-operational keys 268
- device key, defined 327
- dimensions, T10000 tape drive 331
- disabling the Primary Administrator, KMS
  - Console 296, 316
- disabling the technical support account, KMS
  - Console 295, 314
- disconnecting from the KMA 89
- docs.sun xxii

## E

- EKT (enabling key token), defined 327
- ELOM *See* Embedded Lights Out Manager
- Embedded Lights Out Manager (ELOM)
  - connecting through ELOM 20
  - using a network connection 21
- enable key, defined 327
- enabling the Primary Administrator, KMS
  - Console 315
- enabling the technical support account, KMS
  - Console 294, 312
- encryption, defined 327
- enrolling tape drives, QuickStart Program 50
- entering initial Security Officer user credentials, QuickStart program 36
- entering Key Split Credentials, QuickStart program 34
- exiting from the KMS Manager 93
- exporting Audit Logs 240
- exporting keys 141

## F

FIPS (Federal Information Processions Standards), defined 327

## G

Glossary 325

GUI (graphical user interface), defined 327

## H

Hash Message Authentication Code (HMAC), defined 328

help, technical support xxiii

## I

Import Keys menu 256

importing a KMS 1.0 Key Export file 233

importing keys 141

initializing the KMA, QuickStart program 32

Internet Protocol (IP) address, defined 328

Internet Protocol (IP), defined 328

invoking the KMS Manager 68

## J

joining an existing Cluster, QuickStart program 40

## K

Key Export file, importing a KMS 1.0 file 233

Key Group Assignment to Agents menu 218

Key Group Assignment to Transfer Partners menu 225

Key Group List menu 204

Key Group, defined 329

Key Groups

- assigning a Transfer Partner to 231

- assigning an Agent to 214

- assigning to an Agent 221

- assigning to Transfer Partners 227

- assigning Transfer Partners to 229

- creating 208

- definition 202

- deleting 211

- removing an Agent from 216

- removing from a Transfer Partner 228

- removing from an Agent 223

- removing Transfer Partners from 232

- viewing 205

- viewing Key Group assignments to Transfer Partners 226

- viewing or modifying details 210

- viewing Transfer Partners assigned to 230

Key Groups menu 204, 244

Key Management Appliance (KMA)

- adding gateways 29, 307

- adjusting the local clock 191

- connecting to 20

- creating 102

- defined 329

- definition 1

- deleting 108

- deleting gateways 29, 307

- disconnecting from 89

- locking KMA core security 183

- locking or unlocking core security 183

- logging back into the Cluster 300

- logging into 288

- modifying a Key Pool size 282

- rebooting 293

- resetting to the factory default 310

- setting a passphrase 107

- setting the Management IP addresses 303

- setting the Service IP addresses 305

- setting up and managing 18

- shutting down 293

- specifying the DNS settings 31, 309

- TCP/IP connections to 11

- unlocking core security 184

- viewing 98

- viewing gateways 29, 307

- viewing or modifying details 105

- viewing SNMP Managers 131

Key Management Appliance (KMA), network configuration information for 187

Key Management System (KMS)

- Cluster, definition 1

- concepts

  - Agents 2

  - data units, key, key groups, and key policies 10

  - initial setup, direct connect or remote console 3

  - initial setup, QuickStart program 4

  - key lifecycle 4

  - KMS Clusters 2

  - KMS states and transitions 6

  - network connections 2

  - state transition 5

  - users and role-based access control 9

- defined 329

- description 51

- installing 52
- introduction 1
- invoking the KMS Manager
  - Solaris startup 68
  - Windows startup 68
- states
  - active 6
  - compromised 7
  - deactivated 7
  - destroyed 7
  - destroyed compromised 7
  - pre-activation 6
- typical network deployment 12
- user roles 13
- Key Policies
  - creating 198
  - deleting 201
  - description 194
  - modifying 200
  - viewing 194, 200
- Key Policy List menu 194
- Key Policy, defined 329
- Key Sharing, overview 138
- Key Split Configuration menu 177
- Key Split Credentials
  - entering 34
  - modifying 178
  - viewing 177
- Key Transfer File, defined 329
- Key Transfer Partner, defined 329
- Key Transfer Partners
  - configuring 139
  - feature description 138
- Key Transfer process 139
- Key Transfer Public Key
  - creating 158
  - viewing details 157
  - viewing the list of 154
- Key Transfer Public Key List menu 154
- Key Transfer, overview 138
- key, defined 328
- keyboard layout, setting 297
- keys
  - defined 328
  - destroying post-operational keys 268
  - exporting and importing 141
  - importing from a Key Transfer file 256
- KMA List Menu 97, 282
- KMA *See* Key Management Appliance
- KMS Cluster, defined 329
- KMS Console

- Auditor options 291
- Backup Operator options 291
- Compliance Officer options 291
- description 287
- Operator functions
  - disabling the Primary Administrator 296
  - disabling the technical support account 295
  - enabling the technical support account 294
  - logging out 298
  - rebooting the KMA 293
  - setting the keyboard layout 297
  - shutting down the KMA 293
- Operator options 289
- other role functions
  - logging out 321
  - setting the keyboard layout 320
- Security Officer functions
  - adding gateways 307
  - deleting gateways 307
  - disabling the Primary Administrator 316
  - disabling the technical support account 314
  - enabling the Primary Administrator 315
  - enabling the technical support account 312
  - logging out 318
  - logging the KMA back into the Cluster 300
  - resetting the KMA to the factory default 310
  - setting a user's passphrase 302
  - setting the keyboard layout 317
  - setting the KMA Management IP addresses 303
  - setting the KMA Service IP addresses 305
  - specifying the DNS settings 309
  - viewing gateways 307
- Security Officer options 290
- using 287
- KMS Manager
  - changing the passphrase 90
  - connecting to the KMS Cluster 85
  - creating a Cluster profile 85
  - deleting a Cluster profile 89
  - exiting from 93
- GUI
  - definition 1
  - Help menu 72
  - Menu accelerator keys 74
  - overview 69
  - Shortcut keys 74
  - System Menu 70
  - Toolbar buttons 74
  - View menu 71
- GUI panes 76
- operation details pane 77
- operations tree pane 76
- session audit log pane 78
- software requirements 13
- specifying configuration settings 91

- status bar 79
- using online help 75
- using the System menu 85

KMS *See* Key Management System

## L

- local clock, adjusting 191
- Local Configuration menu 182
- Lock/Unlock KMA menu 183
- locking KMA core security 183
- locking the KMA 183
- logging into the Key Management Appliance 288
- logging out of the KMS Console session 298, 318, 321
- logging the KMA back into the Cluster, KMS Console 300

## M

- Management Information Base (MIB), SNMP information 323
- media key, defined 329
- menu
  - Adjust System Time 191
  - Agent Assignment to Key Groups 212
  - Agent List 245
  - Audit Event List 235
  - Autonomous Unlock 180
  - Backup List 159, 273
  - Core Security Management 174
  - Data Unit List 258
  - Help 72
  - Import Keys 256
  - Key Group Assignment to Agents 218
  - Key Group Assignment to Transfer Partners 225
  - Key Group List 204
  - Key Groups 204, 244
  - Key Policy List 194
  - Key Split Configuration 177
  - Key Transfer Public Key List 154
  - KMA List 97, 282
  - Local Configuration 182
  - Lock/Unlock KMA 183
  - Role List 120
  - Security Parameters 170
  - Site List 123
  - SNMP Manager List 131
  - Software Upgrade 269
  - System 70, 85
  - System Dump 168

- System Time 189
- Transfer Partner Assignment to Key Groups 229
- Transfer Partners 142
- Transfer Partners List 143
- User List 109
- View 71
- menu accelerator keys 74
- modifying a Data Unit's details 262
- modifying a Key Pool size 282
- modifying agent details 252
- modifying Key Group details 210
- modifying Key Policies 200
- modifying Key Split Credentials 178
- modifying KMA details 105
- modifying security parameters 172
- modifying site details 129
- modifying SNMP Manager details 136
- modifying user details 115

## N

- network configuration information 187
- network configuration, specifying 27
- network, defined 329
- NIST, defined 329

## O

- OKT, defined 330
- online help, using 13, 75
- operations, role-based 14
- Operator
  - defined 330
  - description 13
  - operations 243
  - role 243
- Operator functions
  - disabling the Primary Administrator 296
  - disabling the technical support account 295
  - enabling the technical support account 294
  - logging out of the KMS Console session 298
  - rebooting the KMA, KMS Console 293
  - setting the keyboard layout 297
  - shutting down the KMA 293
- other role functions
  - logging out 321
  - setting the keyboard layout 320

## P

- partners web site, SUN xxii
- passphrase
  - changing 90
  - setting 117
  - setting for a KMA 107
  - setting for a user 302
- PC Key, defined 330
- Post-operational Keys, destroying 268
- Preface xxi
- Primary Administrator, disabling 296, 316

## Q

- QuickStart program
  - adding agents to a KMA 50
  - adding gateways 29
  - configuring the Cluster 33
  - deleting gateways 29
  - enrolling tape drives 50
  - entering initial Security Officer user credentials 36
  - entering Key Split Credentials 34
  - initializing the KMA 32
  - joining an existing Cluster 40
  - restoring a Cluster from a backup 43
  - running 25
  - setting the Key Pool size 38
  - setting the KMA Management IP address 27
  - setting the KMA Service IP address 28
  - specifying the Autonomous Unlock preference 37
  - specifying the DNS settings 31
  - specifying the network configuration 27
  - starting 26
  - synchronizing KMA time 39
  - viewing gateways 29

## R

- read key, defined 330
- rebooting the KMA, KMS Console 293
- remote connection to the console, ELOM 20
- removing a Key Group from a Transfer Partner 228
- removing a Key Group from an Agent 223
- removing a Transfer Partner from a Key Group 232
- removing an Agent from a Key Group 216
- resetting the KMA to the factory default 310

- resetting the KMA to the factory default, KMS Console 310
- restoring a backup 165
- restoring a Cluster from a backup, QuickStart Program 43
- retrieving security parameters 170
- retrieving the system time 189
- Rijndael algorithm, defined 330
- Role List menu 120
- role, viewing operations for 122
- role-based operations 14
- roles, Key Management System 13
- roles, viewing 120
- RSA, defined 330

## S

- Secure Hash Algorithms (SHA), defined 330
- Security Officer
  - defined 330
  - description 13
  - operations 95
  - role 96
- Security Officer functions
  - adding gateways 307
  - deleting gateways 307
  - disabling the Primary Administrator 316
  - disabling the technical support account 314
  - enabling the Primary Administrator 315
  - enabling the technical support account 312
  - logging the KMA back into the Cluster 300
  - resetting the KMA to the factory default 310
  - setting a user's passphrase 302
  - setting the keyboard layout 317
  - setting the KMA Management IP addresses 303
  - setting the KMA Service IP addresses 305
  - specifying the DNS settings 309
  - viewing gateways 307
- security parameters
  - modifying 172
  - retrieving 170
- Security Parameters menu 170
- security policy, defined 330
- setting a KMA passphrase 107
- setting a user passphrase 117
- setting a user's passphrase, KMS Console 302
- setting an Agent's passphrase 253
- setting the Key Pool size, QuickStart program 38
- setting the keyboard layout 297

- setting the keyboard layout, KMS Console 297, 317, 320
- setting the KMA Management IP address, KMS Console 303
- setting the KMA Management IP address, QuickStart program 27
- setting the KMA Service IP address, KMS Console 305
- setting the KMA Service IP address, QuickStart program 28
- Shamir's Secret Sharing, defined 330
- shortcut keys 74
- shutting down the KMA 293
- site details, viewing or modifying 129
- Site List menu 123
- site, defined 330
- sites
  - creating 127
  - deleting 130
  - viewing 124
- size of tape drive 331
- SNMP
  - Management Information Base information 323
- SNMP Manager
  - creating 134
  - deleting 137
  - viewing for a KMA 131
  - viewing or modifying details 136
- SNMP Manager List menu 131
- software downloads, website xxii
- software requirements, KMS 13
- Software Upgrade menu 269
- software upgrades, uploading and applying 270
- specifying configuration settings 91
- specifying the Autonomous Unlock preference, QuickStart program 37
- specifying the DNS settings
  - QuickStart program 31
- specifying the DNS settings, KMS Console 309
- specifying the network configuration, QuickStart program 27
- starting the KMA, QuickStart program 32
- starting the KMS Manager 68
- starting the QuickStart program 26
- states and transitions, KMS 6
- support, technical xxiii
- synchronizing KMA time, QuickStart program 39
- system dump

- creating 168
- defined 331
- System Dump menu 168
- system menu, using 85
- System Time menu 189
- system time, retrieving 189

## T

- T10000 tape drive
  - defined 331
  - description of 331
  - size 331
- technical support xxiii
- technical support account
  - disabling 295
  - enabling 294
- token bay, defined 331
- token, defined 331
- toolbar buttons 74
- Transfer Partner Assignment to Key Groups menu 229
- Transfer Partners
  - assigning a Key Group to 227
  - assigning to a Key Group 231
  - assigning to Key Groups 229
  - creating 147
  - deleting 153
  - importing Keys and Data Units from a key transfer file 256
  - Key Group Assignment to 225
  - List 143
  - removing from a Key Group 232
  - removing Key Groups from 228
  - viewing and modifying details 150
  - viewing assignments to Key Groups 230
  - viewing Key Group assignments to 226
- Transfer Partners menu 142
- Transport Layer Security (TLS), defined 331
- troubleshooting xxiii

## U

- UID, defined 331
- Ultra Tape Drive Encryption Agent, defined 331
- unlocking KMA core security 184
- unlocking the KMA 183
- uploading software upgrades 270
- user details, viewing or modifying 115
- User List menu 109

- user passphrase, setting 117
- user roles, Key Management System 13
- users
  - creating 113
  - deleting 119
  - viewing 110
- using online help 75
- using the KMS Console 287
- using the System menu 85
- UTC, defined 331
- utility, Backup command line
  - description 279
  - IPv6 addresses with Zone IDs 280

## V

- viewing a Data Unit's details 262
- viewing agent details 252
- viewing Audit Log details 239
- viewing Audit Logs 235
- viewing backup files details 163, 275
- viewing Backup Files history 160
- viewing backup files history 274
- viewing Data Units 259
- viewing gateways, KMS Console 307
- viewing gateways, QuickStart Program 29
- viewing gateways, QuickStart program 29
- viewing Key Group assignments to Transfer Partners 226
- viewing Key Group details 210
- viewing Key Groups 205
- viewing Key Policies 200
- viewing key policies 194
- viewing Key Transfer Public Key details 157
- viewing KMA details 105
- viewing KMA SNMP Managers 131
- viewing KMAs 98
- viewing operations for 122
- viewing roles 120
- viewing site details 129
- viewing sites 124
- viewing SNMP Manager details 136
- viewing the Agent List 246
- viewing the Key Split credentials 177
- viewing the Key Transfer Public Key list 154
- viewing Transfer Partner assignments to Key Groups 230
- viewing user details 115
- viewing users 110

- volume serial number, defined 331

## W

- web site, SUN xxii
- worldwide offices, SUN xxiv
- wrap key, defined 332
- write key, defined 332

## Z

- zeroize
  - defined 332
  - resetting the KMA to the factory default 310





Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web [sun.com](http://sun.com)



ARGENTINA: 5411-4317-5636 • AUSTRALIA: 1-800-550-786 • AUSTRIA: 43-1-601-26-0 • BALKANS: 301-6188-111 • BELGIUM: 32-2-704 89 83 • BRAZIL: 55-11-51872100 • BRUNEI: 65-216-8333 • CANADA: 1-800-422-8020 (GENERAL); 416-964-2001 (LEARNING MANAGEMENT SYSTEM SALES, TORONTO) • CHILE: 562-372-4500 • COLOMBIA: 571-629-2323  
CZECH REPUBLIC: 420-2-330093111 • DENMARK: 45 4556 5040 • EGYPT: 00 202 570 9442 • FINLAND: 358-9-525-561 • FRANCE: 33-1-41-33-17-17 • GERMANY: 49-89-460-08-2788 • GREECE: 30-01-6188101 • HONG KONG: 852-2877-7077 • HUNGARY: 361-202-4415 • INDIA: 91-80-229-8989 • INDONESIA: 65-216-8333 • IRELAND: 353-1-668-4377  
ISRAEL: 972-9-9710500 • ITALY: 39-02-9259511 • JAPAN: 81-3-5779-1820 • KOREA: 82-2-3453-6602 • MALAYSIA: 603-2116-1887 • MIDDLE EAST: 00 9714 3366333 • MEXICO: 525-261-0344 • NETHERLANDS: 31-33-4515200 • NEW ZEALAND: 0800-786-338 • NORTH WEST AFRICA: 00 9714 3366333 • NORWAY: FROM NORWAY: 47-22023950, To NORWAY: 47-23369650 • PAKISTAN: 00-9714-3366333 • PEOPLE'S REPUBLIC OF CHINA: 8610-6803-5588 • PHILIPPINES: 632-885-7867 • POLAND: 48-22-8747848 • PORTUGAL: 351-21-413-4000 • RUSSIA: 7-095-935-8411 • SAUDI ARABIA: 00 9714 3366333 • SINGAPORE: 65-216-8300 • SOUTH AFRICA: 27-11-256-6300 • SPAIN: 34-902-210-412 • SRI LANKA: 65-2168333 • SWEDEN: 46-8-631 22 00 • SWITZERLAND: 41-1-908-90-50 (GERMAN) 41-22-999-0444 (FRENCH) • TAIWAN: 886-2-25185735 • THAILAND: 662-344-6855 • TURKEY: 90 212 335 22 00 • UNITED KINGDOM: 44-1276-416-520 • UNITED STATES: 1-800-422-8020 • VENEZUELA: 582-905-3800 • VIETNAM: 65-216-8333 • WORLDWIDE  
HEADQUARTERS: 1-650-960-1300

**SUN™** THE NETWORK IS THE COMPUTER ©2006 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.