Sun microsystems

Crypto Key Management Station

Version 1.2

User’s Guide

Part Number: 96262
Revision B

Crypto Key Management Station

User's Guide

Version 1.2

Sun Microsystems, Inc.
www.sun.com

Part No. 96262
June 2007, Revision B

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

We welcome your feedback. Please contact the Global Learning Solutions Feedback System at:

SLSFS@Sun.com

or

Sun Learning Services
Sun Microsystems, Inc.
500 Eldorado Blvd, 06-307
Broomfield, CO 80021
USA

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

Adobe PostScript

Revision B • 96262

Summary of Changes

EC Number	Date	Revision	Description
	September 2006	Draft	Initial Draft
	October 2006	Preliminary	Updated to reflect product changes.
	November 2006	A	Added “KMS Command Line Interface Commands” chapter. Updated GUI screen descriptions to match screen changes.
	June 2007	B	Updated for new features in version 1.2: • Networked token operations—New configuration allowing you to write keys to any token residing on the network. • Air gap operations continue to be supported. • Token IP address—All tokens must have an IP address. • Media key export—Database backup encryption key is no longer included in the export file. Administrator can disable and re-enable this function. • Media key import—New function that allows the administrator to import media key data previously created by the media key export function. • Raw key import—New GUI screen to support this function. New chapters: • Chapter 1, “Crypto Key Management Station Overview.” • Appendix A, “CLI Command Quick Reference.” New GUI screens: • Keys > Media Key Import • Keys > Raw Key Load • Tokens > Token Selection Screen Updated GUI screens: • Drives > Modify • Drives > View • Keys > Media Key Export—Renamed from Keys > Export • Keys > Modify • Keys > View • Tokens > Create • Tokens > Modify • Tokens > View • Tokens > Write Device Keys • Tokens > Write Media Keys

EC Number	Date	Revision	Description
			New CLI commands: • export_media_key_disable • export_media_key_enable • import_media_key • search_tokens • send_permanent_ip • view_backup_key Updated CLI commands: • create_token • export_media_key—Renamed from export_key • import_raw_key—Renamed from import_kmedia • modify_token • reset_token • run_backup_db • view_drive • write_token

Contents

Preface

The *Crypto Key Management Station Key Management Station User's Guide* provides information about:

- Important Key Management Station (KMS) topics
- Procedures to configure and manage encryption at your site
- KMS GUI screens
- KMS CLI commands
- Crypto Key Management Station logging and error message facilities

This guide is intended for customers, service representatives, and anyone responsible for the configuration and management of the Crypto Key Management Station.

Organization

This guide is organized as follows:

Chapter	Use this chapter to:
Chapter 1, "Crypto Key Management Station Overview"	Understand the Crypto Key Management Station components and configurations.
Chapter 2, "KMS Software Overview"	Understand how the Crypto Key Management Station enables encryption at your site.
Chapter 3, "KMS Operator Roles and Login IDs"	Understand how to manage Key Management Station (KMS) login IDs.
Chapter 4, "KMS Management Tasks"	Understand the procedures to configure and manage encryption at your site.
Chapter 5, "KMS Graphical User Interface Screens"	Understand and use the KMS GUI screens.
Chapter 6, "KMS Command Line Interface Commands"	Understand and use the KMS CLI commands.

Chapter	Use this chapter to:
Chapter 7, "KMS Database"	Understand and manage the KMS database.
Chapter 8, "Crypto Key Management Station Support"	Understand and use the Crypto Key Management Station logging and error message facilities.
Chapter A, "CLI Quick Reference"	Quick reference of all CLI commands.

Related Information

These publications contain the additional information mentioned in this guide:

Publication Title	Part Number
Sun Ultra 20 Workstation Getting Started Guide This guide provides the information that you need to set up, power on, and configure the workstation hardware and software.	Sun: 819-2148-xx
These publications are for Sun StorageTek personnel or authorized third parties who install StorageTek tape and library products.	
Crypto Key Management Station Installation Manual	StorageTek: 96260
T10000 Tape Drive Installation Manual	StorageTek: 96173

These publications are related to the Crypto Key Management Station:

Publication Title	Part Number
Crypto Key Management Station Installation Manual	StorageTek: 96260
Crypto Key Management Station Configuration and Setup Guide	StorageTek: 96261
Crypto Key Management Station User's Guide	StorageTek: 96262
Crypto Key Management Station Systems Assurance Guide	StorageTek: TM0018

CHAPTER 1

Crypto Key Management Station Overview

The Sun Crypto Key Management Station is used to create, store, and manage encryption keys. It is an appliance dedicated to data-at-rest encryption.

Note – The Crypto Key Management Station must be kept in a secure location. Its database stores the encryption keys used by library drives to encrypt and decrypt data.

Sun Data-at-Rest Encryption Components

The following hardware and software components are required to implement and manage the Sun data-at-rest encryption solution.

- Crypto Key Management Station, a Sun Ultra 20 hardware platform pre-installed with the following:
  - Sun Crypto-Accelerator 6000 (SCA6000) card, to generate raw encryption keys
  - Secure version of the Solaris 10 operating system
  - Key Management Station (KMS) software application
  - External USB hard drive, for KMS database backups
  - Two Ethernet ports for encrypted communications to and from the Crypto Key Management Station
- Encryption-capable library tape drives, for storing encrypted data
- Physical tokens, for storing and transmitting encryption keys
- Token bay, to allow the physical tokens to communicate with the Crypto Key Management Station and the library drives
- Optional backup Crypto Key Management Station

Crypto Key Management Station Configurations

The Crypto Key Management Station solution can be implemented using either of the following configurations:

- Air gap—Provides the highest levels of security. The Crypto Key Management Station is not connected to any local area network (LAN) or wide-area network (WAN) and is not connected to the library drives. Transferring keys from the Crypto Key Management Station to the library drives requires direct user intervention. See "Air Gap Configuration" on page 2 for details.
- Networked token operations—Provides "hands-off" delivery of keys to the drives. The Crypto Key Management Station, encryption-capable library drives, and tokens are all connected to a LAN or WAN. See "Networked Token Configuration" on page 3 for an illustration.

Air Gap Configuration

With the air gap configuration, the Crypto Key Management Station is physically and logically isolated from the library drives. The hardware components are configured as follows:

- A token bay is attached directly to the Crypto Key Management Station through one Ethernet port on the Crypto Key Management Station.
- A second token bay is attached to the encryption-capable library drives through a local network.
- A backup Crypto Key Management Station can be attached through the second Ethernet port on the primary Crypto Key Management Station.

The Crypto Key Management Station and the library drives are separated by an "air gap." See FIGURE 1-1, "Air Gap Configuration" on page 3.

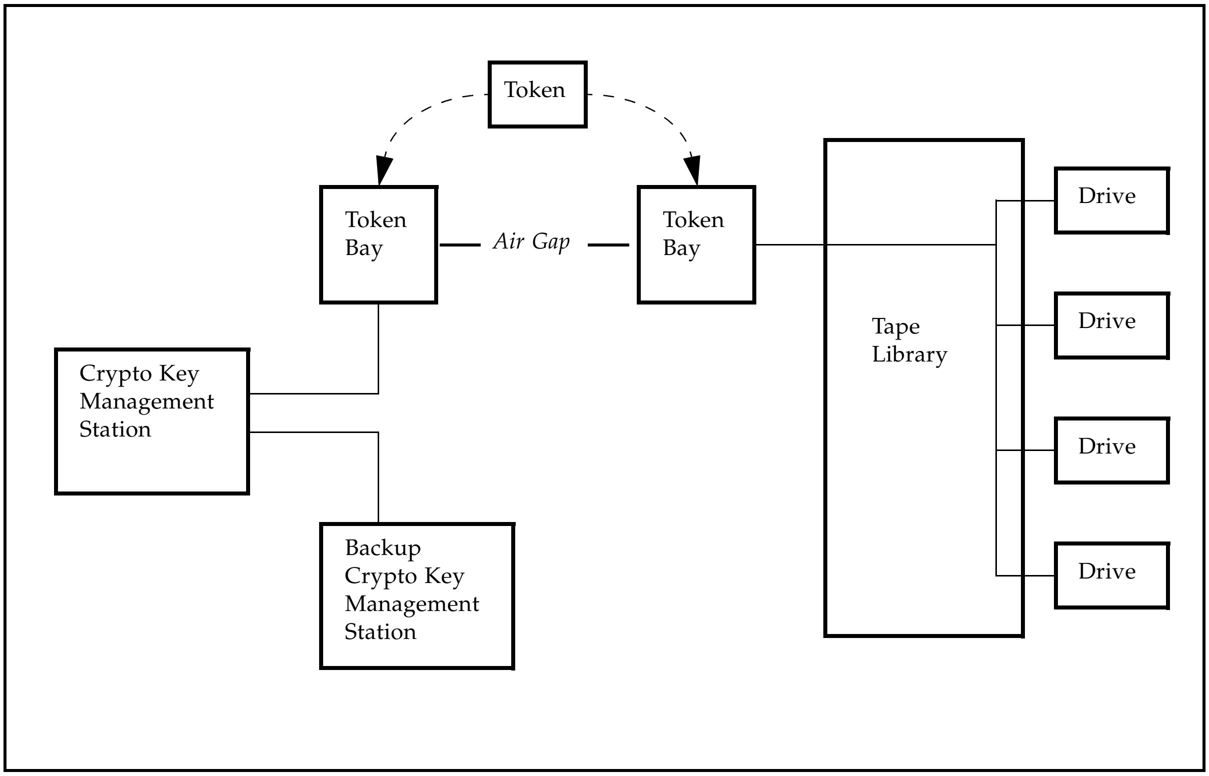

Token
Token Bay
Air Gap
Token Bay
Tape Library
Drive
Drive
Drive
Drive
Crypto Key Management Station
Backup Crypto Key Management Station

FIGURE 1-1 Air Gap Configuration

To write encryption keys to a token, you must insert the token in the Crypto Key Management Station token bay. Then to transmit the keys to the drives, you must physically carry the token and insert it in the library drive token bay. You can display the status of token only if it is inserted in the Crypto Key Management Station token bay.

Networked Token Configuration

With the networked token configuration, the Crypto Key Management Station, library drives, and token bays all reside on a corporate LAN or WAN. The hardware components are configured as follows:

- One Ethernet port on the Crypto Key Management Station is used to connect the Crypto Key Management Station to the network.
- Any number of token bays are attached to the library drive subnet.
- The encryption-capable library drives are also attached to the network.
- One token bay is attached to the Crypto Key Management Station subnet. This token bay is used only when you assign permanent IP settings to a new token.
- A backup Crypto Key Management Station can be attached through the second Ethernet port on the primary Crypto Key Management Station.

See FIGURE 1-2, "Networked Token Configuration" on page 4.

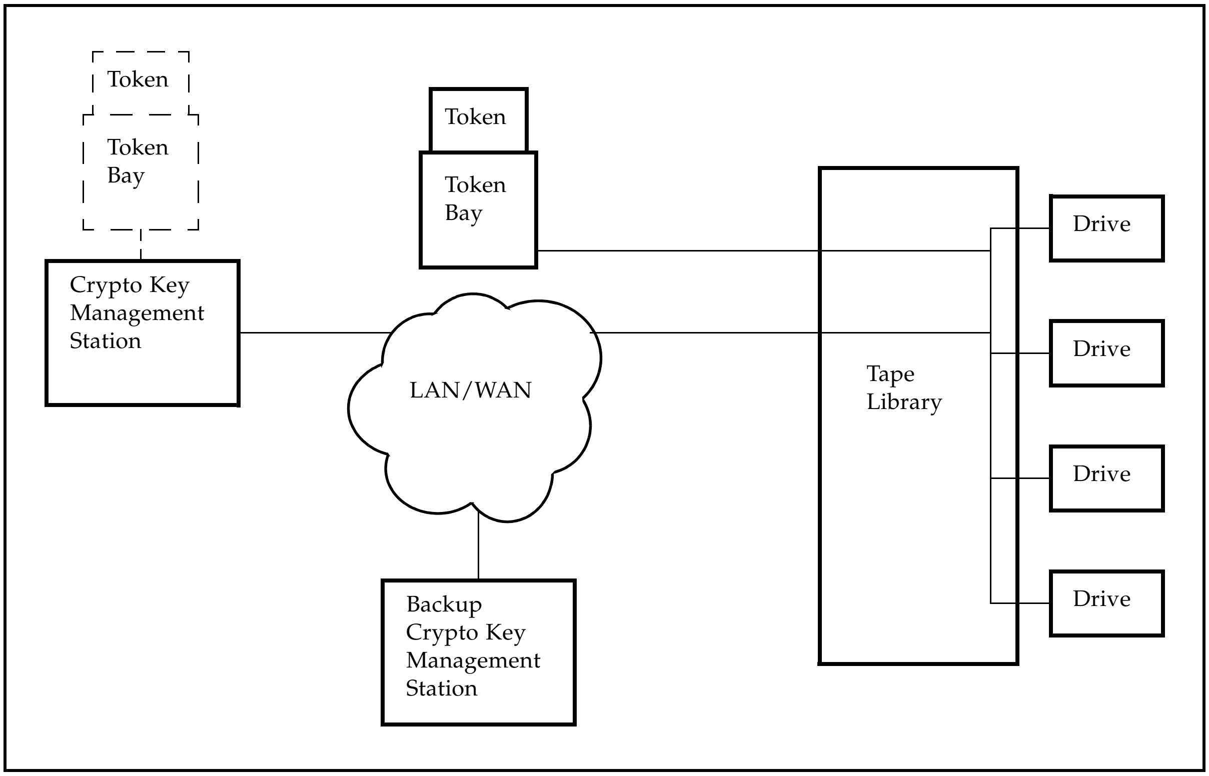


FIGURE 1-2 Networked Token Configuration

You can write encryption keys to any token inserted in a token bay on the network. Once it receives the keys, the token automatically transmits the keys to the library drives on the local subnet. You do not need to physically carry the tokens from one token bay to another.

Note – In FIGURE 1-2, the token bay and token outlined with dashed lines are used only when you initially configure a token for use. The token bay must be connected to the Crypto Key Management Station subnet so you can use the KMS software to assign permanent IP settings to the token. See "Token IP Settings" on page 11 and "Assign Permanent IP Settings to Tokens" on page 26 for details.

CHAPTER 2

KMS Software Overview

This chapter describes important elements of the Key Management Station (KMS) software. Understanding these elements will help you to implement and use the KMS software.

Encryption Drives

The Sun StorageTek T10000 tape drive supports data-at-rest encryption. The drive is shipped from the factory encryption-capable, but not encryption-enabled. You must explicitly enable the drive for encryption.

Note – For security reasons, once you enable a drive for encryption, you cannot reset it to non encryption mode in the field. The drive must be returned to the factory to disable encryption. All media keys are automatically erased from the drive's memory when it is powered down for shipment to the factory.

Characteristics of Encryption-Enabled Drives

An encryption-enabled drive has the following capabilities:

- Writes to tape in encrypted mode ONLY, using its assigned write key.
- Can read an encrypted tape, if it has the proper read key.
- Can read non encrypted tapes.
- Can overwrite a non encrypted tape from the beginning of tape (BOT).
- Cannot append to a non encrypted tape.
- Cannot mix encrypted and non encrypted data on the same tape.
- Cannot be re-set to non encryption mode.

A drive that has NOT been enabled for encryption cannot read or append to any encrypted tape. It can, however, overwrite an encrypted tape from the beginning of tape (BOT).

Identify Drives to the KMS Software

All drives to be enabled for encryption must be identified to the KMS software. To do this, you must provide the following information about each drive:

- Drive name—assigned by the user
- Crypto serial number—assigned by Sun Microsystems, Inc.
- Preset communication (PC) key—assigned by Sun Microsystems, Inc.

Drive Name

You must assign a unique name to each drive. The drive name is used to identify the drive to the KMS software. Optionally, you can assign a drive description.

Crypto Serial Number

The crypto serial number allows the enabling key token (EKT) to communicate with the correct tape drive. This number is unique for each drive. It is assigned at the factory and stored in the drive's nonvolatile memory.

Note – The crypto serial number does not need to be kept secure.

PC Key

The preset communication (PC) key is used to enable a tape drive for encryption. The device keys assigned to each drive by the KMS software are encrypted with the drive's PC key. (See "Device Keys" on page 8 for details.)

The PC key is unique for each drive. It is assigned at the factory and is stored in the drive's nonvolatile memory. It is provided to the customer from Sun Microsystems, Inc. from a secure central database, via one of the following methods of secure communication:

- Secure e-mail
- CD delivered with the Crypto Key Management Station

Note – The PC key must be kept secure.

Enable Encryption in a Drive

A drive is enabled for encryption through the following process. For details, see the following topics:

- "Identify Drives for Encryption" on page 25
- "Create Device Keys and Transmit them to the Drives—Networked Token Operations" on page 29
- "Create Device Keys and Transmit them to the Drives—Air Gap Operations" on page 31

1. You identify the drive to the KMS software. To do this, you must assign a drive name and provide the drive's crypto serial number and PC key. This information is stored in the KMS database.
2. You select the drive for encryption.
3. The KMS software creates a unique set of device keys for the drive. Three raw keys are randomly selected to become the device key. The device key package is encrypted with the drive's unique PC key.
4. The KMS software writes the encrypted device keys and the drive's crypto serial number to the enabling key token (EKT).
5. The EKT sends a broadcast message containing the drives' crypto serial numbers and a time stamp. To do this, the token must be on the same IP subnet as the drives.
6. The drives use the PC key stored in nonvolatile memory to decrypt the device keys.
7. The drive is now set to encryption-enabled mode, and the device keys are stored in nonvolatile memory in the drive. The device keys are deleted from the EKT.

Note – To read and write encrypted data on a tape, the drive must have the correct media keys. See "Media Keys" on page 8.

Drive Pools

A drive pool is a logical collection of tape drives. Drive pools allow you to manage a group of drives all at once.

You must assign a unique name to each drive pool. Optionally, you can assign a description. After creating a drive pool, you can assign any number of drives to it. Each drive can be assigned to only one drive pool.

Through drive pool/key set mappings, all drives in a drive pool share the same read and write keys. See "Drive Pool/Key Set Mappings" on page 11.

Keys

The KMS software uses the following types of keys:

- Raw keys
- Device keys
- Media keys

Raw Keys

A raw key is a string of 32 bytes (256 bits), in a random bit pattern. Raws keys are the source of device and media keys; they have not yet been assigned to drives or key sets.

Raw keys are typically generated by the Sun Crypto Accelerator 6000 (SCA6000) MARS card included in the Crypto Key Management Station. You can also import them from CD-ROM provided by an external source of your choice.

Once raw keys are generated, you must import them to the KMS database to make them available for use. When a device or media key is needed, a raw key is selected from the KMS database.

Device Keys

Device keys are used to enable drives for encryption. They also protect media keys while they reside on the operating key token (OKT). They are stored in the drive's nonvolatile memory.

Device keys are created automatically by the KMS software when an enabling key token (EKT) is written. See "Enable Encryption in a Drive" on page 6 for details on how device keys are created and transmitted.

Note – To ensure that device keys are kept secure, their values are never displayed.

Media Keys

Media keys are used by encryption-enabled drives to encrypt (write) and decrypt (read) data on tape. The Crypto Key Management Station supports a symmetric key scheme, in which the same key is used for both encryption and decryption.

A drive can read encrypted data from a tape only if the key that was used to write the data is resident in the drive's memory. When encrypted data is written to tape, the key ID for the write key is written to tape in plain text so the tape drive knows which key value to use to decrypt the data.

Note – To ensure that media key values are kept secure, only the key ID of the media key, not the key value, is written to tape.

Manage Media Keys

Each drive can store up to 32 media keys—1 read/write key and 31 read keys. The drive uses the write key to encrypt all data the drive writes to tape. It also uses the write key value to decrypt data previously encrypted with the same key. Likewise, the drive uses each read key to decrypt data previously encrypted with the corresponding key.

When you implement encryption at your site, you may want to implement a process that updates write keys regularly. For example, you may want to create new write keys each month; when you create a new write key for a drive pool, the old write key is assigned as a read key.

Note – For initial configurations, it is recommended that all tape drives in a library use the same write key and share the same set of read keys.

Drive Request for Media Keys

If a drive cannot decrypt data on a tape because it does not possess the correct read key, it sends a message, via the token, to the KMS software indicating the key ID it needs. To display these messages, see the Drives > Modify GUI screen or the modify_drive CLI command. You can then transmit that key to the drive.

Transmit Media Keys to the Drives

Drives are provided with media keys through the following process. For details, see the following topics:

- "Create Key Sets" on page 33
- "Create and Assign Media Keys to Key Sets" on page 34
- "Map Key Sets to Drive Pools" on page 36
- "Transmit Media Keys to the Drives—Networked Token Operations" on page 37
- "Transmit Media Keys to the Drives—Air Gap Operations" on page 38

1. You direct the KMS software to create media keys from raw keys. The KMS software selects one raw key for each media key created. Each media key is assigned a unique key ID.
2. You assign the media keys to key sets.
3. You assign key sets to drive pools.

Note – At this time, you identify the write key for the drive pool. All drives in the drive pool share the same read and write keys.

---

4. You identify the drive pools to which you want to transfer media keys.
5. You direct the KMS software to write the media keys assigned to these drive pools to the operating key token (OKT).

   When written to the OKT, the media keys are encrypted with the device keys of the drives in the drive pool. They are encrypted in separate messages for each drive in the drive pool.
6. The OKT sends a broadcast message containing the drives' crypto serial numbers and a time stamp. To do this, the token must be on the same IP subnet as the drives.
7. Affected drives request the new keys if the time stamp indicates newer keys than those stored in the drives.

8. The drives use the device keys stored in nonvolatile memory to decrypt the media keys.
9. The media keys are stored in volatile memory in the drive.

Note – The media keys are lost from the drive's memory in the event of a power loss or re-initialization. When the drive re-initializes, it looks for the OKT, to retrieve the media keys. Therefore, it is important that the OKT be kept resident on same IP subnet as the library drives.

Media Key Security

Note – Media keys must be kept secure.

Media keys reside in any of the following locations:

- KMS database – To ensure the security of media keys, the KMS database is encrypted, and the Crypto Key Management Station should be kept in a secure location.
- OKT – To ensure their security, media keys are encrypted on the OKT.
- Drive – To ensure their security, media keys on a drive are stored in volatile memory and are not accessible by any external commands.

Note – The media keys are erased from the drive's memory whenever the drive is powered down or removed from the library. When the drive re-initializes, it must recover the media keys to be able to read and write to tape. For this reason, it is recommended that the OKT be kept in the token bay connected to the encryption drives.

Key Sets

A key set is a logical collection of media keys. Key sets allow you to organize write and read keys together for encryption and decryption.

You must assign a unique name to each key set. Optionally, you can assign a description.

After creating a key set, you can create media keys and assign them to the set. A key can be assigned to any number of key sets. Each key set can have a maximum of 32 media keys.

Media keys are assigned to individual drives through drive pool/key set mappings. All drives in a drive pool share the same media keys. See "Drive Pool/Key Set Mappings" on page 11.

Drive Pool/Key Set Mappings

Drive pool/key set mappings are used to assign groups of media keys (key sets) to groups of drives (drive pools). Through these mappings, all drives in a drive pool share the same read and write keys. A drive pool can be mapped to any number of key sets, as long as the total number of keys in all key sets mapped to the pool does not exceed 32.

When mapping a key set to a drive pool, you must designate which key is to be the write key for the pool. A drive pool can have only one write key at a time. The write key can be any key from any of the key sets mapped to the pool. All drives in the drive pool use that key for encryption when writing data to tape.

All other keys in the key set are read-only keys. Any of the 32 keys in the key set can be used to read data from the tape.

Once mapping is complete, you can transfer media keys to the drives in the drive pool. See "Enabling Key Token (EKT)" on page 14.

Tokens

Tokens are used to perform the following functions:

- Transferring device and media keys from the Crypto Key Management Station to the encryption drives
- Transferring error and status messages from the drives to the KMS software

Physical Tokens

The Crypto Key Management Station comes with two physical tokens, which are handheld, microprocessor-based devices. You use the tokens to transfer encryption information between the Crypto Key Management Station and the library drives. For details, see the following topics.

- For networked token operations:
  - "Create Device Keys and Transmit them to the Drives—Networked Token Operations" on page 29
  - "Transmit Media Keys to the Drives—Networked Token Operations" on page 37
- For air gap operations:
  - "Create Device Keys and Transmit them to the Drives—Air Gap Operations" on page 31
  - "Transmit Media Keys to the Drives—Air Gap Operations" on page 38

Token IP Settings

All tokens are delivered from the factory with the following default IP settings:

- IP address = 10.0.0.2
- Netmask = 255.0.0.0
- Gateway IP = 10.0.0.254

Before a token can be used on your network, the Crypto Key Management Station administrator must use the send_permanent_ip CLI command to assign to the token permanent IP settings compatible with your network. These settings are stored in the token's nonvolatile memory and are therefore retained when the token is removed from a token bay.

The KMS software does not require each token IP address to be unique. However, the following considerations apply:

- In order to ensure that keys are transmitted to and from the correct token, each token IP address must be unique within a subnet supporting a given group of tape drives.
- For networked token operations, it is recommended that each token IP address be unique across the network.

For networked token operations, each token needs only a permanent IP address. For air gap operations, each token needs both a permanent IP address and a temporary IP address.

Permanent IP Address

A token's permanent IP address must be on the same subnet as the encryption-capable library drives. The permanent IP address is used to communicate with the token, as follows:

- For networked token operations, both the library drives and the KMS software use the permanent IP address to communicate with the token.
- For air gap operations, only the library drives use the permanent IP address to communicate with the token. The KMS software uses a temporary IP address.

See "Assign Permanent IP Settings to Tokens" on page 26 for additional details.

Temporary IP Address

Note – Temporary IP addresses are used with air gap operations only.

A token's temporary IP address must be on the same subnet as the Crypto Key Management Station. The KMS software uses the temporary IP address to communicate with the token when writing keys.

When you use either the Tokens > Write Device Keys or Tokens > Write Media Keys GUI screens or the write_token CLI command to write keys to a token, the KMS software assigns a temporary IP address to the token. The value assigned is the IP address specified in the Tokens > Create GUI screen or the create_token CLI command.

The temporary IP address is stored in the token's volatile memory and is therefore erased when the token is removed from a token bay.

Token Identification

Before a physical token can be used to transmit keys, it must be identified to the KMS software. To do this, you use the Tokens > Create GUI screen or the create_token CLI command. See "Identify Tokens to the KMS Software" on page 28 for details.

When identifying a token to the KMS software, you must provide the following information about each token:

- Token ID
- MAC address
- IP address

Token ID

You must assign a unique ID to each physical token. Optionally, you can assign a description.

MAC Address

The media access control (MAC) address allows the Crypto Key Management Station to communicate with the token. The MAC address, which is unique for each token, is assigned at the factory and is stored in the token's nonvolatile memory. It is also printed on the token cartridge label.

The MAC address is a 48-bit hexadecimal number, consisting of 12 hexadecimal digits, separated into six groups of two digits each. Each pair is separated by a colon. For example, 00:90:C2:73:EF:6A. The first 24 bits identify the manufacturer, and the next 24 bits identify the type of device and provide a unique serial number for the token.

IP Address

Whenever the KMS software needs to write keys to a token, it locates the correct token using the IP address you have specified in the KMS database.

- For networked token operations, this is the permanent IP address, which was previously assigned with the send_permanent_ip CLI command.
- For air gap operations, this is a temporary IP address that must be on the same subnet as the Crypto Key Management Station.

You can use any of the following GUI screens and or CLI commands to display the IP address specified in the KMS database.

- Tokens > Create or create_token
- Tokens > Modifyor modify_token
- Tokens > Token Selection Screen
- Tokens > View or view_token

Logical Token Types

There is only one type of physical token, but each physical token can perform either of two logical functions:

- Enabling key token (EKT)
- Operating key token (OKT)

Note – There is also a token type called "new key token (NKT)," which indicates either the token is new or it has been reset and therefore has not had keys of any type written to it.

You can use the Tokens > View GUI screen or the view_token CLI command to display the token type.

Enabling Key Token (EKT)

EKTs are used to transfer encrypted device keys to the tape drives. Device keys, which are created by the KMS software, enable drives for encryption.

Once the device keys have been successfully transmitted to a drive, they are maintained in the drive's nonvolatile memory and are deleted from the EKT memory. The EKT is no longer necessary, unless you need it to add more drives or replace an existing drive.

See "Enable Encryption in a Drive" on page 6 for details on how the EKT is used to transfer device keys to the drives.

Operating Key Token (OKT)

OKTs are used to transfer encrypted media keys, created by the KMS software, to the tape drives. A tape drive must have the proper media keys to read and write encrypted data on a tape. Each OKT can hold media keys for up to 1850 tape drives.

All of the following conditions must be met in order for you to write an OKT:

- You must select one or more drive pools for writing to the token.
- Each selected drive pool must have drives assigned to it.
- Each selected drive pool must have one or more key sets assigned to it.
- Each selected drive pool must have a designated write key.
- The total number of keys in all key sets assigned to each selected drive pool cannot exceed 32.

Attach a Token to the Crypto Key Management Station

The following process occurs whenever a token is inserted in a token bay that is either on the Crypto Key Management Station LAN/WAN or attached directly to the Crypto Key Management Station:

1. The KMS software and the token authenticate one another by exchanging an encrypted password. If authentication fails, the connection between the two is dropped.

2. If authentication is successful, the KMS software uses the token's MAC address to access the token's information from the KMS database.

3. The token sends any error and status messages it has received from the drives to the KMS software. The messages may indicate that the drives need or have received device or media keys. To display these messages, see the Tokens > Modify GUI screen or the modify_token CLI command.

4. You can now write device or media keys to the token for transfer to the drives. See "Enable Encryption in a Drive" on page 6 and "Transmit Media Keys to the Drives" on page 9 for details.

CHAPTER 3

KMS Operator Roles and Login IDs

Security features built into the Crypto Key Management Station control both user authentication and user authorization. The security features include:

- Login IDs – Login IDs control user authentication. Each user must have a valid, active login ID and password to log in to the Crypto Key Management Station.
- Operator roles – Operator roles control user authorization. Each login ID is assigned an operator role, which determines the types of requests the user can submit through the Key Management Station (KMS) GUI or command line interface (CLI).

Login IDs

To log in to the Crypto Key Management Station workstation, a user must have a valid login ID. Only one login ID can be logged in to the workstation at a time.

Your installation can have any number of login IDs, depending on your needs. Each login ID must be unique within the system. Login IDs cannot be deleted, but they can be made inactive. Users with inactive login IDs are not allowed to log in to the workstation.

Passwords

Each login ID must be assigned a password. KMS passwords follow Sun's strong password rules: they consist of 8–20 printable characters, and the first 8 characters must include a lowercase letter, an uppercase letter, a number, and a special character.

A login ID's password expires every 90 days. When assigning a new password, you cannot reuse the previous three passwords assigned to the login ID.

For security purposes, passwords are stored in the KMS database as hashed strings, not clear text.

Operator Roles

The KMS software supports three operator roles that conform to the Federal Information Processing Standard (FIPS) Level 2 security requirements. Each operator role has specific actions that it is authorized to perform. The operator roles are:

- Administrator
- Security Officer
- User

Each login ID must be assigned one and only one operator role. The operator role determines which KMS GUI screens the user can access, and therefore which actions the user can perform.

Multiple login IDs can have the same operator role. The same user can assume more than one role by using multiple login IDs.

Login IDs can be created by users who are assigned either the Administrator or Security Officer operator roles.

Operator Role Functions

Following are descriptions of the functions each KMS operator role is authorized to perform.

Administrator

The Administrator manages keys and login IDs. This includes the following functions:

- Importing raw keys into the KMS database
- Creating and maintaining key sets
- Creating and maintaining media keys
- Assigning media keys to key sets
- Exporting media keys to a file
- Creating and maintaining Administrator and Security Officer login IDs

Security Officer

The Security Officer manages device keys and login IDs. This includes the following functions:

- Identifying physical tokens
- Transmitting device keys to drives via the enabling key token (EKT)
- Creating and maintaining Security Officer and User login IDs

User

The User manages drives and media keys. This includes the following functions:

- Identifying drives to be enabled for encryption
- Creating and maintaining drive pools
- Assigning drives to drive pools
- Mapping key sets to drive pools
- Assigning the write key for a drive pool
- Identifying physical tokens
- Transmitting media (read and write) keys to drives through the operating key token (OKT)

Table 3-1 lists the KMS GUI screens that each operator role is authorized to access.

TABLE 3-1 KMS GUI Screens by Operator Role

Operator Role	KMS Screens
User	Drives > Create Drives > Modify Drives > View Drive Pools > Create Drive Pools > Modify Drive Pools > View Login Mapping > Modify Mapping > View Tokens > Create Tokens > Modify Tokens > Token Selection Screen Tokens > View Tokens > Write Media Keys
Security Officer	Drives > View Login Operators > Create Operators > Modify Operators > View Tokens > Create Tokens > Modify Tokens > Token Selection Screen Tokens > View Tokens > Token Selection Screen
Administrator	Key Sets > Create Key Sets > Modify Key Sets > View Keys > Create Keys > Media Key Export Keys > Media Key Import Keys > Modify Keys > Raw Key Load Keys > View Login Operators > Create Operators > Modify Operators > View

CHAPTER 4

KMS Management Tasks

This chapter describes procedures used to manage the Crypto Key Management Station and the encryption drives. Most of these tasks are performed using Key Management Station (KMS) GUI screens.

Note – See "Log in to the KMS GUI on the Crypto Key Management Station" on page 41 for detailed instructions on accessing the KMS screens.

Note – Each task in this chapter identifies the KMS login ID required to perform it.

Overview of Management Tasks

In order for drives to read and write encrypted data on tapes, the following conditions must exist:

- The drives must be enabled for encryption.
- The drives must have the proper media (read and write) keys.

A series of tasks must be performed in the proper order, to establish these conditions. Table 4-1, "Encryption Processes and Detailed Tasks" on page 22, identifies the tasks, grouping them by high-level process. The table also identifies the operator role required to perform each task. For detailed instructions, see the identified task and page.

TABLE 4-1 Encryption Processes and Detailed Tasks

Process	Operator Role	Task	Page
Create login IDs	Administrator	Create Security Officer Login IDs	23
	Security Officer	Create User Login IDs	24
Identify drives for encryption	User	Identify Drives for Encryption	25
Prepare tokens for use	kmsadmin login ID	Assign Permanent IP Settings to Tokens	26
	Security Officer or User	Identify Tokens to the KMS Software	28
Enable drives for encryption	Security Officer	Create Device Keys and Transmit them to the Drives—Networked Token Operations or Create Device Keys and Transmit them to the Drives—Air Gap Operations	29 31
Create media keys	Administrator	Create Key Sets	33
		Create and Assign Media Keys to Key Sets	34
Define drive pool/key set mappings	User	Create Drive Pools and Assign Drives to Them	35
		Map Key Sets to Drive Pools	36
Transfer media keys to the drives	User	Transmit Media Keys to the Drives—Networked Token Operations or Transmit Media Keys to the Drives—Air Gap Operations	37 38

Management Task Instructions

This section provides detailed instructions for enabling and managing drive encryption capabilities.

▼ Create Security Officer Login IDs

Operator Role: Administrator

Screen Navigation: **Operators > Create**

You can create multiple login IDs with the Security Officer role.

Note – You must create at least one Security Officer login ID. Security Officer is the only operator role that can write to the enabling key token (EKT), which enables the tape drives for encryption.

---

1. **Log in as Administrator.**
2. **Select Operators > Create.**
3. **Enter the Login ID, Description (optional), Password, and Confirm Password.**
4. **In the Role field, click Security Officer.**
5. **In the Status field, click Active.**
6. **Click Apply.**

▼ Create User Login IDs

Operator Role: Security Officer

Screen Navigation: **Operators > Create**

You can create multiple login IDs with the User operator role.

Note – You must create at least one User login ID. User is the only operator role that can create the operating key token (OKT), which transfers media keys to the drives so they can read and write encrypted data.

---

1. **Log in as Security Officer.**
2. **Select Operators > Create.**
3. **Enter the Login ID, Description (optional), Password, and Confirm Password.**
4. **In the Role field, click User.**
5. **In the Status field, click Active.**
6. **Click Apply.**

▼ Identify Drives for Encryption

Operator Role: User

Screen Navigation: **Drives > Create**

Use this procedure to designate the tape drives that you want to enable for encryption. You can perform this procedure in either of the following ways:

- Import Drive Data from CD
- Enter Drive Data Manually

▼ Import Drive Data from CD

Note – Before you begin this task, you must obtain the drive data CD for the tape drive, which is provided by Sun Microsystems, Inc.

1. **Log in as User.**
2. **Select Drives > Create.**
3. **Enter Drive Name, Description (optional), and CD Path.**
4. **Insert the drive data CD into the Crypto Key Management Station CD/DVD drive.**
5. **Click Import Now.**

   The **PC Key**, **Confirm PC Key**, and **Crypto Serial Number** fields are filled in automatically with data from the CD.
6. **Click Apply.**

▼ Enter Drive Data Manually

Note – Before you begin this task, verify that you have the PC key and crypto serial number (CSN) for the tape drive. These are unique numbers for each tape drive.

1. **Log in as User.**
2. **Select Drives > Create.**
3. **Enter Drive Name, Description (optional), PC Key, Confirm PC Key, and Crypto Serial Number.**
4. **Click Apply.**

▼ Assign Permanent IP Settings to Tokens

Operator Role:	You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.
CLI Command:	`send_permanent_ip`

Physical tokens are used to transfer encryption information from the Crypto Key Management Station to the drives. Before a token can be used on your network, you must assign permanent IP network settings to it.

Note – In order to perform this activity, you must have a token bay attached directly to Crypto Key Management Station.

Note – Before you perform this activity, you must obtain the following information for the token: 1) the unique MAC address, which is printed on the token label; 2) the permanent IP settings to be used by the encryption-capable library drives to communicate with the token.

---

1. **Power on the Crypto Key Management Station workstation.**
2. **Log in to the workstation using the `kmsadmin` login ID.**

```
Login: kmsadmin
Password: password
```

where *password* is the password assigned to the `kmsadmin` login ID. See your Crypto Key Management Station administrator for assistance.

3. **Select Launch > Applications > Utilities to open a Terminal window.**
4. **Insert a physical token into the token bay attached directly to the Crypto Key Management Station.**
5. **Issue the command to assign the permanent IP settings.**

```
# /opt/SUNWkms/app/tools/send_permanent_ip -i token_IP_address
-m netmask -g gateway_IP_address token_MAC_address
```

where:

- *token_ip_address* is the permanent IP address you want to assign to the token. This IP address must be on the same subnet as the library drives.
- *netmask* is the netmask for the network on which the token resides.
- *gateway_IP_address* is the IP address of the gateway node on which the token resides.
- *token_MAC_address* is the MAC address assigned to the token.

6. **Verify that the token has successfully received the settings.**

```
# /opt/SUNWkms/app/tools/search_tokens
```

In the display, use the MAC address to locate the token you have just updated and verify that the IP settings are correct.

7. **For future reference, you may want to write the IP address on the token's label.**

8. **Log out of the workstation.**

▼ Identify Tokens to the KMS Software

Operator Role:	Security Officer or User
Screen Navigation:	**Tokens > Create**

Physical tokens are used to transfer encryption information from the Crypto Key Management Station to the drives. Each physical token can perform two logical functions.

- As an enabling key token (EKT), the token is used to transfer device keys to the drives.
- As an operating key token (OKT), the token is used to transfer media keys to the drives.

Each physical token must be identified to the KMS software before it can be used to transfer device or media keys.

Note – Before you perform this activity, the Crypto Key Management Station administrator must use the `send_permanent_ip` CLI command to assign permanent IP settings to the token. You must obtain from the administrator the following information for the token: 1) the unique MAC address, which is printed on the token label; 2) the IP address to be used by the KMS software to communicate with the token.

---

1. **Log in as Security Officer or User.**
2. **Select Tokens > Create.**
3. **Enter Token ID, Description (optional), Token Version, MAC Address, and IP address.**

Note – The IP address is assigned as follows:

- For networked token operations, this is an IP address on the same subnet as the library drives.
- For air gap operations, this is an IP address on the same subnet as the Crypto Key Management Station.

---

4. **Click Apply.**

You can now use the token to transfer keys to the library drives.

▼ Create Device Keys and Transmit them to the Drives—Networked Token Operations

Operator Role: Security Officer

Screen Navigation: **Tokens > Write Device Keys**

Note – This task applies to networked token operations only. If you are using air gap operations see "Create Device Keys and Transmit them to the Drives—Air Gap Operations" on page 31.

Use this procedure to create encrypted device keys, write them to an enabling key token (EKT), and then automatically transmit them to the drives.

Note – To perform this task, the token to which you write keys must be on the same subnet as the drives you want to receive the keys.

---

1. **Log in as Security Officer.**
2. **Select Tokens > View.**

   To verify that the KMS software is successfully communicating with the token, check the **Last Contact** field. This field is automatically updated by the KMS software at frequent intervals, so if communications are successful, the field displays a current date and time.
3. **Select Tokens > Write Device Keys.**

   The **Tokens > Token Selection Screen** appears.
4. **Select the token to which you want to write the device keys.**

   The **Tokens > Write Device Keys** screen appears.
5. **Click the check boxes next to the drives you want to enable.**
6. **If you are enabling a drive for the first time or the drive has been reset, click the Use PCKeys check box for that drive.**
7. **To indicate that you are using networked token operations, leave the Locally-attached Token check box blank.**
8. **Click Apply.**

   The keys are written to the token, and a message appears indicating that the EKT has been written.
9. **The token automatically begins transmitting the keys to the drives.**

   A message appears indicating that the keys have been transmitted. You can also select **Drives > View** and verify that the **Status** field displays "Yellow." This indicates that the drive has successfully received device keys.

   To read and write data, the drive needs media keys from an operating key token (OKT).

Note – The token can be used to transmit other keys, as the device keys are stored on the drives and in the KMS database.

▼ Create Device Keys and Transmit them to the Drives—Air Gap Operations

Operator Role: Security Officer

Screen Navigation: **Tokens > Write Device Keys**

Note – This task applies to air gap operations only. If you are using networked token operations see "Create Device Keys and Transmit them to the Drives—Networked Token Operations" on page 29.

This procedure is done in two parts:

- Create and Write Device Keys to the EKT
- Transmit Device Keys From the EKT to the Drives

▼ Create and Write Device Keys to the EKT

1. **Log in as Security Officer.**
2. **Verify that the token bay is properly powered on and connected to the Crypto Key Management Station.**
3. **Insert the token in the appropriate slot of the token bay.**
4. **Verify that the second LED from the left on the token bay is solid green. This indicates the token bay is communicating with the Crypto Key Management Station.**
5. **Select Tokens > Write Device Keys.**

   The **Tokens > Token Selection Screen** appears.
6. **Select the token to which you want to write the device keys.**

   The **Tokens > Write Device Keys** screen appears.
7. **Click the check boxes next to the drives you want to enable.**
8. **If you are enabling a drive for the first time or the drive has been reset, click the Use PCKeys check box for that drive.**
9. **To indicate that you are using air gap operations, click the Locally-attached Token check box.**
10. **Click Apply.**

    In order to communicate with the token, the KMS software assigns to the token the IP address displayed on the **Tokens > Token Selection Screen**, as a temporary IP address. This IP address is stored in the token's volatile memory.

    The keys are written to the token, and a message appears indicating that the EKT has been written.

Note – The token does NOT automatically transmit the keys to the drives.

▼ Transmit Device Keys From the EKT to the Drives

1. **Verify that the library drive token bay is properly powered on and connected to the tape drives.**
2. **Insert the enabling key token in the appropriate slot of the drive token bay.**
3. **Observe the encryption LED on the rear of the tape drives. After about ten seconds, the token delivers the enabling keys to each drive that you have previously designated for encryption.**
4. **Wait for the third LED from the left on the rear of each tape drive to turn from red to solid amber. You can also select Drives > View and verify that the Status field displays "Yellow." This indicates that the drive has successfully received device keys.**

   To read and write data, the drive need media keys from an operating key token (OKT).
5. **When all drive LEDs have turned to solid amber, remove the token from the token bay.**

Note – The token can be used to transmit other keys, as the device keys are now stored on the drives and in the KMS database.

▼ Create Key Sets

Operator Role: Administrator

Screen Navigation: **Key Sets > Create**

1. **Log in as Administrator.**
2. **Select Key Sets > Create.**
3. **Enter Key Set Name and Description (optional).**
4. **Click Apply.**

▼ Create and Assign Media Keys to Key Sets

Operator Role: Administrator

Screen Navigation: **Keys > Create**

Note – Keys must be assigned to key sets when they are created, therefore, you must perform the "Create Key Sets" on page 33 procedure before you can perform this one.

---

1. **Log in as Administrator.**
2. **Select Keys > Create.**

Note – If there are no raw keys available to create keys, you must import raw keys into the KMS database. See "Import Raw Keys to the KMS Database" on page 202.

---

3. **Click New Key in the upper right corner of the window.**

   The Key ID, **Crypto Key**, **Confirm Key**, and **Key Set** fields are populated with data from the raw keys in the KMS database.

4. **Enter Description (optional).**
5. **Click the appropriate Key Set name for the key.**
6. **Click Apply.**

▼ Create Drive Pools and Assign Drives to Them

Operator Role:	User
Screen Navigation:	**Drive Pools > Create**

1. **Log in as User.**
2. **Select Drive Pools > Create.**
3. **Enter Drive Pool Name and Description (optional).**
4. **In the Available Enabled Drives column, click one or more drives that you want to add to the drive pool.**

Note – The Available Enabled Drives list contains drives you created in "Identify Drives for Encryption" on page 25 that have not already been assigned to a drive pool.

5. **Click Add Drive.**
6. **Click Apply.**

▼ Map Key Sets to Drive Pools

Operator Role:	User
Screen Navigation:	**Mapping > View/Modify**

1. **Log in as User.**
2. **Select Mapping > View**
3. **In the Drive Pool Name list, click a pool to which you want to assign key sets. The Mapping > Modify screen appears.**
4. **In the Available Keysets box, click a key set you want to assign to the drive pool.**

Note – The Available Keysets list contains key sets you created in "Create Key Sets" on page 33 that have not already been assigned to a drive pool.

---

5. **Click Add Keysets.**
6. **Repeat Step 4 and Step 5 until you have specified all the key sets you want to assign to the pool.**
7. **In the Write Key ID pull-down menu, click the key you want to assign as the write key for this drive pool. All drives in the drive pool share the same write key.**

Note – The Write Key pull-down menu contains a list of all keys assigned to the key sets you have selected for this drive pool.

---

8. **Click Apply.**
9. **A message appears indicating that the pool has been modified.**

▼ Transmit Media Keys to the Drives—Networked Token Operations

Operator Role:	User
Screen Navigation:	**Tokens > Write Media Keys**

Note – This task applies to networked token operations only. If you are using air gap operations, see "Transmit Media Keys to the Drives—Air Gap Operations" on page 38.

Use this procedure to write media keys from the KMS database to an operating key token (OKT), and then automatically transmit them to the drives.

Note – To perform this task, the token to which you write keys must be on the same subnet as the drives you want to receive the keys.

---

1. **Log in as User.**
2. **Select Tokens > View.**

   To verify that the KMS software is successfully communicating with the token, check the **Last Contact** field. This field is automatically updated by the KMS software at frequent intervals, so if communications are successful, the field displays a current date and time
3. **Select Tokens > Write Media Keys.**

   The **Tokens > Token Selection Screen** appears.
4. **Select the token to which you want to write the media keys.**

   The **Tokens > Write Media Keys** screen appears.
5. **Click the check box next to the drive pools whose keys you want to write to the token.**
6. **To indicate that you are using networked token operations, leave the Locally-attached Token check box blank.**
7. **Click Apply.**

   A message appears indicating that the OKT has been written.
8. **The token automatically begins transmitting the keys to the drives.**

   A message appears indicating that the keys have been transmitted. You can also select **Drives > View** and verify that the **Status** field displays "Green." This indicates that the drive has successfully received media keys.

Note – The operating key token (OKT) must remain on the network, accessible to the drives. The media keys are not stored in drive memory; therefore, whenever an encryption-enabled tape drive is power-cycled or rebooted, it queries the OKT for the media keys.

▼ Transmit Media Keys to the Drives—Air Gap Operations

Operator Role:	User
Screen Navigation:	**Tokens > Write Media Keys**

Note – This task applies to air gap operations only. If you are using networked token operations, see "Transmit Media Keys to the Drives—Networked Token Operations" on page 37.

This procedure is done in two parts:

- Write Media Keys to the OKT
- Transmit Media Keys from the OKT to the Drives

▼ Write Media Keys to the OKT

1. **Log in as User.**
2. **Verify that the token bay is properly powered on and connected to the Crypto Key Management Station.**
3. **Insert the token in the appropriate slot of the token bay.**
4. **Verify that the second LED from the left on the token bay is solid green. This indicates the token bay is communicating with the Crypto Key Management Station.**
5. **Select Tokens > Write Media Keys.**

   The **Tokens > Token Selection Screen** appears.
6. **Select the token to which you want to write the media keys.**

   The **Tokens > Write Media Keys** screen appears.
7. **Click the check box next to the drive pools whose keys you want to write to the token.**
8. **To indicate that you are using air gap operations, click the Locally-attached Token check box.**
9. **Click Apply.**

   In order to communicate with the token, the KMS software assigns a temporary IP address to the token. The value is the IP address displayed on the **Tokens > Token Selection Screen**. This IP address is stored in the token's volatile memory.

   The keys are written to the token, and a message appears indicating that the OKT has been written.

Note – The token does NOT automatically transmit the keys to the drives.

▼ Transmit Media Keys from the OKT to the Drives

1. **Verify that the library drive token bay is properly powered on and connected to the tape drives.**

2. **Insert the operating key token (OKT) in the appropriate slot of the drive token bay.**
3. **Observe the encryption LEDs on the rear of the tape drives. After about ten seconds, the token delivers the read and write keys to each drive included in the drive pool/key set mappings defined in** "Map Key Sets to Drive Pools" on page 36**.**
4. **Wait for the third LED from the left on the rear of each tape drive to turn from amber to solid green. You can also select Drives > View and verify that the Status field displays "Green." This indicates that the drive has successfully received media keys.**

Note – The operating key token (OKT) must remain in the library drive token bay slot. The media keys are not stored in drive memory; therefore, whenever an encryption-enabled tape drive is power-cycled or rebooted, it queries the OKT for the media keys.

5. **Log out of the Crypto Key Management Station.**

CHAPTER 5

KMS Graphical User Interface Screens

The Key Management Station (KMS) graphical user interface (GUI) allows you to manage the Crypto Key Management Station from a Web browser.

Using the KMS GUI

To run the KMS GUI, you must be using Mozilla 1.7.xx. This version of Mozilla is shipped with Solaris 10, which is installed on the KMS server. If you are logging into the KMS GUI remotely, you need to verify that you are running the correct version of the browser.

You can use either of the following methods to log in to the KMS GUI:

- Log in to the KMS GUI on the Crypto Key Management Station
- Log in to the KMS GUI from a Remote Host

Note – Only one user at a time can be logged in to the KMS software.

▼ Log in to the KMS GUI on the Crypto Key Management Station

Use this procedure to log in to the Crypto Key Management Station workstation and start the KMS GUI.

1. **Power on the Crypto Key Management Station workstation.**
2. **Log in to the workstation.**

   ```
   Login: kmsuser
   Password: password
   ```

   where *password* is the password assigned to the `kmsuser` login ID. See your Crypto Key Management Station administrator for assistance.
3. **Start a Web browser by doing either of the following:**
   - Double-click the **Web Browser** icon on the desktop.

- Select **Launch** > **Web Browser**.

The KMS GUI starts automatically and the Login screen appears.

4. **Log in to the KMS GUI.**

```
Login: KMS_login
Password: password
```

where:

- *KMS_login* is the KMS login ID you have been assigned.
- *password* is the password assigned to this login ID.

Note – The login ID you use determines the screens you can access. See "Operator Roles" on page 18.

▼ Log in to the KMS GUI from a Remote Host

Use this procedure to log in to the KMS GUI from a remote host.

Note – Before you perform this activity, you must obtain the host name or IP address of the Crypto Key Management Station and the port number of the KMS GUI. See your Crypto Key Management Station administrator for assistance.

---

1. **Start a supported Web browser on your host.**
2. **In the Location Bar, enter the host name/IP address and port of the KMS GUI.**

`https://`*nnn*`.`*nnn*`.`*nnn*`.`*nnn*`:`*port* or
`https://`*hostname:port*

where:

- *nnn*.*nnn*.*nnn*.*nnn* is the IP address of the Crypto Key Management Station.
- *hostname* is the host name of the Crypto Key Management Station.
- *port* is the port number of the KMS GUI.

The Login screen of the KMS GUI appears.

3. **Log in to the KMS GUI.**

```
Login: KMS_login
Password: password
```

where:

- *KMS_login* is the KMS login ID you have been assigned.
- *password* is the password assigned to this login ID.

Note – The login ID you use determines the screens you can access. See "Operator Roles" on page 18.

Connection Time-out Period

The default KMS connection time-out period is set to 10 minutes. The login session times out automatically if a user does not perform any activity for 10 minutes, and the user will need to log in again to resume using the KMS software.

CLI Functionality Not in the GUI

The following KMS CLI commands have no comparable KMS GUI screens. These functions can be carried out through the CLI only.

- backup_db
- export_media_key_disable
- export_media_key_enable
- history_token
- mkkeys
- reset_token
- restore_db
- run_backup_db
- run_restore_db
- search_tokens
- send_permanent_ip
- view_backup_key

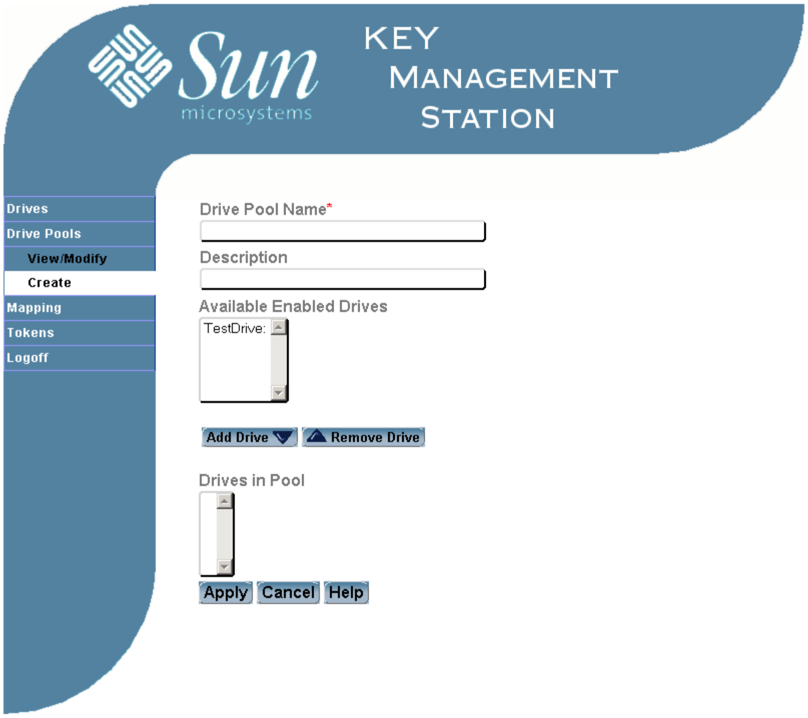
KMS GUI Screens

This section includes detailed descriptions of all KMS GUI screens, arranged in alphabetical order by screen navigation path. For example, **Drives > Create** indicates the GUI screen accessed by clicking **Drives** and then **Create** from the left navigation menu.

Once you have started the KMS GUI, you can use any screen for which you have sufficient authorization. See Table 3-1 “KMS GUI Screens by Operator Role” on page 20 for details.

Drive Pools > Create

Sample Screen



Description

Allows you to create a drive pool. Optionally, you can assign encryption-enabled drives to it.

Note – If you choose not to assign drives to the drive pool at this time, you can do so later using the **Drive Pools > Modify** screen or the `modify_drivepool` CLI command.

Operator Role

User

Screen Fields

Drive Pool Name

Required.

Name of the drive pool you want to create. Unique for each pool.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Description

Optional.

Description of the drive pool. Can be anything that describes the drive pool, such as the function or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

Available Enabled Drives

Optional.

The list displays the names and descriptions of all drives that have been enabled for encryption but have not been assigned to a drive pool. The name and description of each are separated by a colon (:).

To add a drive to the drive pool, click the drive name in the Available Enabled Drives column, and then click **Add Drive**. The drive name is moved to the Drives in Pool column.

Drives in Pool

Optional.

The list displays the names and descriptions of all drives that have been assigned to the drive pool. The name and description of each are separated by a colon (:).

To remove a drive from the drive pool, click the drive name in the Drives in Pool column, and then click **Remove Drive**. The drive name is moved to the Available Enabled Drives column.

Buttons

Add Drive

Click to add the selected drive to the drive pool.

Remove Drive

Click to remove the selected drive from the drive pool.

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

Click to display online help for the screen.

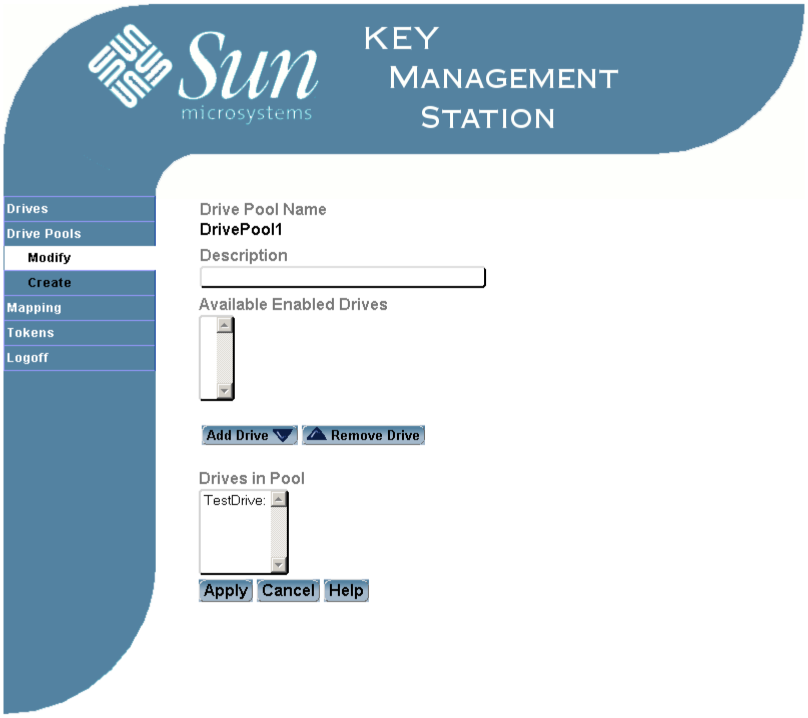
See Also

- Drives > Create
- Drive Pools > Modify
- Drive Pools > View

- Mapping > Modify
- Mapping > View

Drive Pools > Modify

Sample Screen



Drive Pool Name
DrivePool1

Description

Available Enabled Drives

Drives in Pool
TestDrive:

Description

Allows you to modify the description of a drive pool and to add or remove drives from the pool.

Operator Role

User

Screen Fields

Drive Pool Name

Display only.

Name of the drive pool. Unique for each pool.

Description

Description of the drive pool. Can be anything that describes the drive pool, such as the function or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

The screen displays the value assigned previously. You can leave it as is or make changes.

Available Enabled Drives

The list displays the names and descriptions of all drives that have been enabled for encryption but have not been assigned to a drive pool. The name and description of each are separated by a colon (:).

To add a drive to the drive pool, click the drive name in the Available Enabled Drives column, and then click **Add Drive**. The drive name is moved to the Drives in Pool column.

Drives in Pool

The list displays the names and descriptions of all drives that have been assigned to the drive pool. The name and description of each are separated by a colon (:).

To remove a drive from the drive pool, click the drive name in the Drives in Pool column, and then click **Remove Drive**. The drive name is moved to the Available Enabled Drives column.

Buttons

Add Drive

Click to add the selected drive to the drive pool.

Remove Drive

Click to remove the selected drive from the drive pool.

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

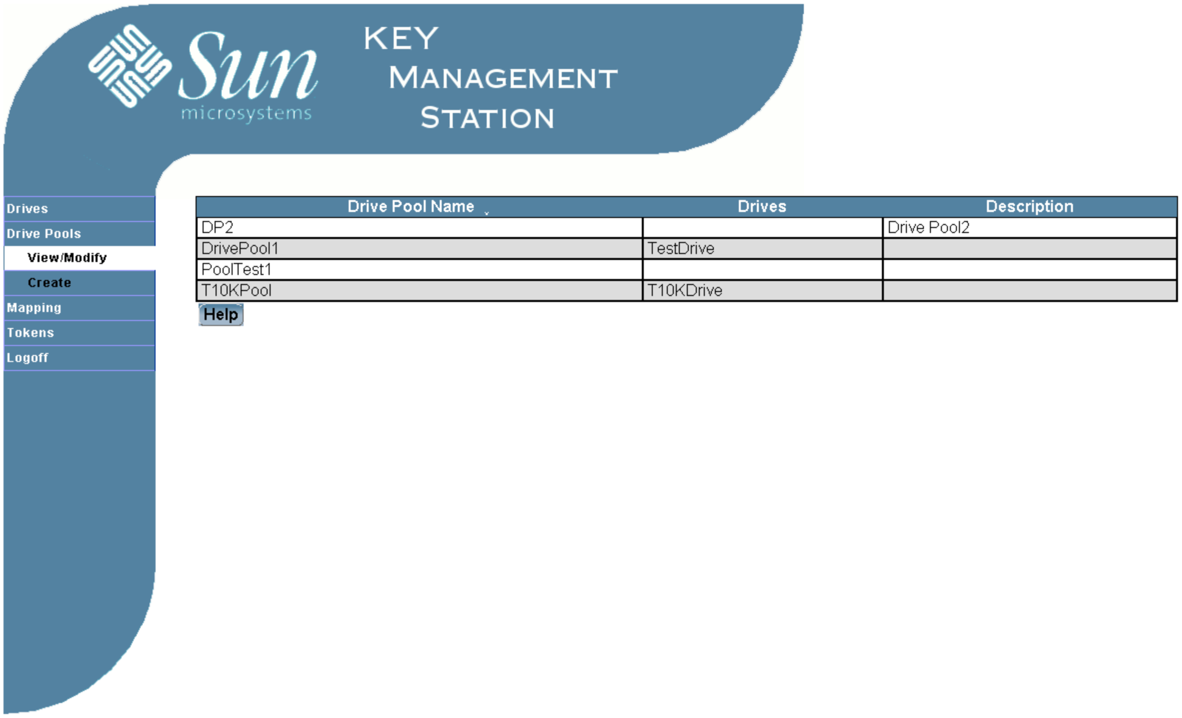
Click to display online help for the screen.

See Also

- Drives > Create
- Drive Pools > Create
- Drive Pools > View
- Mapping > Modify
- Mapping > View

Drive Pools > View

Sample Screen



Drive Pool Name	Drives	Description
DP2		Drive Pool2
DrivePool1	TestDrive	
PoolTest1		
T10KPool	T10KDrive	

Description

Allows you to display information about drive pools.

Operator Role

User

Screen Fields

Note – Click any screen field to modify the drive pool information. The Drive Pools > Modify screen appears.

Drive Pool Name

Display only.

Name of the drive pool. Unique for each pool.

Drives

Display only.

Names of the drives that have been assigned to the drive pool. Individual names are separated by a semicolon (`;`).

Description

Display only.

Description of the drive pool. Can be anything that describes the drive pool, such as the function or department.

Buttons

Help

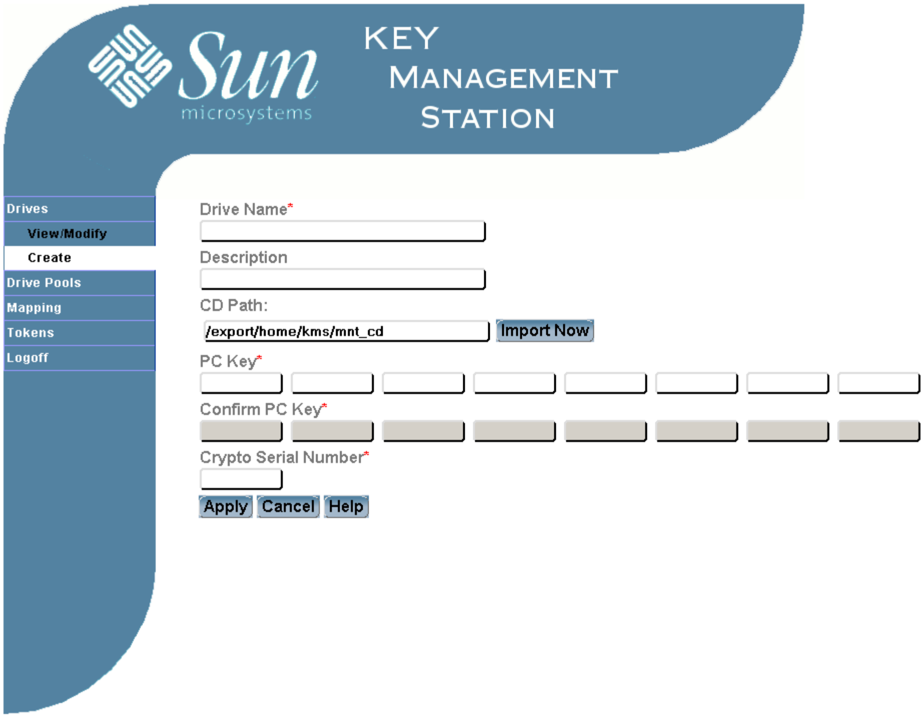
Click to display online help for the screen.

See Also

- Drives > Create
- Drive Pools > Create
- Drive Pools > Modify
- Mapping > Modify
- Mapping > View

Drives > Create

Sample Screen



Drive Name*

Description

CD Path: /export/home/kms/mnt_cd

PC Key*

Confirm PC Key*

Crypto Serial Number*

Description

Allows you to identify a drive you want to enable for encryption. You can use either of the following methods:

- Import the drive data from a CD provided by Sun Microsystems, Inc. Each drive has its own CD. The drive's unique preset communication (PC) key and crypto serial number are provided on the CD.
- Enter the drive data manually. You need to obtain the drive's unique preset communication (PC) key and crypto serial number before performing this activity.

Operator Role

User

Screen Fields

Drive Name

Required.

Name of the drive you want to enable for encryption. Unique for each drive.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Description

Optional.

Description of the drive. Can be anything that describes the drive, such as the physical location within the library.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), _ (underscore), and spaces.

CD Path

Required if you select **Import Now**. Ignored if you do not select **Import Now**.

Imports the PC key and crypto serial number for the drive from the CD located at `/export/home/kms/mnt_cd`. You can obtain this CD from Sun Microsystems, Inc.

Note – Because this CD contains sensitive information, such as the PC key for the drive, it must be kept secure.

You can modify the location of the CD by entering the full path of the CD mount point.

PC Key

Required.

Preset communication (PC) key assigned to this drive by Sun Microsystems, Inc. Unique for each drive. This number is provided to your Sun support representative using one of the following methods:

- From a secure central database
- By secure e-mail
- By CD delivered with the Crypto Key Management Station

Note – This number must be kept secure.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

Confirm PC Key

Required.

For security purposes, re-enter the PC Key entered in the previous field. The two entries must match exactly.

Crypto Serial Number

Required.

Crypto serial number assigned to this drive by Sun Microsystems, Inc. and stored in the drive’s nonvolatile memory. Unique for each drive.

Note – This number does not need to be kept secure.

1–6 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

Buttons

Import Now

Click to import the drive data from the designated CD.

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

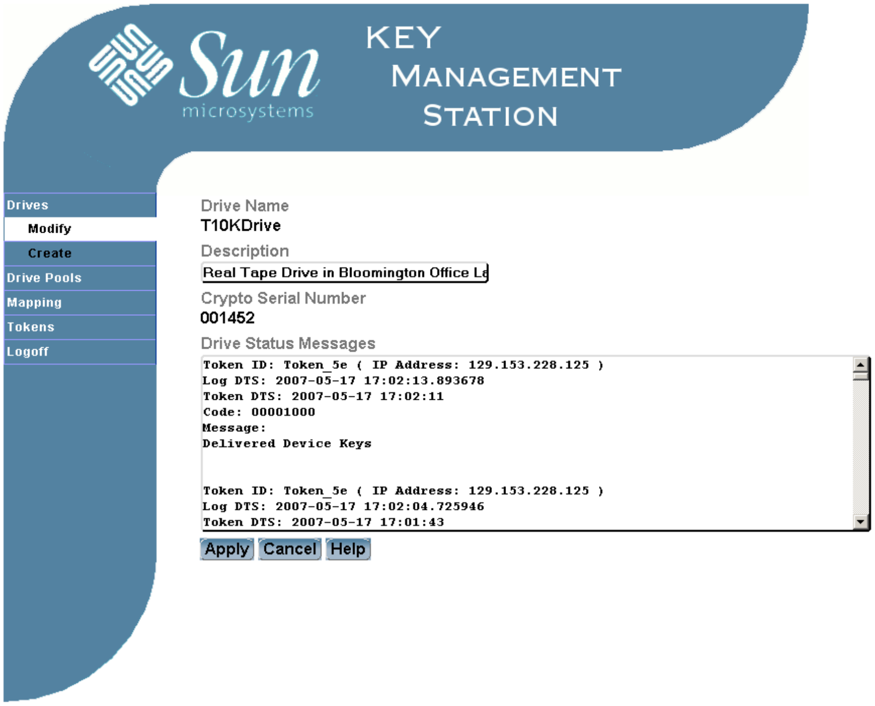
Click to display online help for the screen.

See Also

- Drives > Modify
- Drives > View
- Tokens > Write Device Keys

Drives > Modify

Sample Screen



Drive Name
T10KDrive

Description
Real Tape Drive in Bloomington Office Lo

Crypto Serial Number
001452

Drive Status Messages

```
Token ID: Token_5e ( IP Address: 129.153.228.125 )
Log DTS: 2007-05-17 17:02:13.893678
Token DTS: 2007-05-17 17:02:11
Code: 00001000
Message:
Delivered Device Keys


Token ID: Token_5e ( IP Address: 129.153.228.125 )
Log DTS: 2007-05-17 17:02:04.725946
Token DTS: 2007-05-17 17:01:43
```

Description

Allows you to modify the description of a drive.

Also displays detailed messages about interactions between the drive and the Key Management Station software.

Operator Role

User

Screen Fields

Drive Name

Display only.

Drive that has been designated for encryption capability.

Description

Description of the drive. Can be anything that describes the drive, such as the physical location within the library.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

The screen displays the value assigned previously. You can leave it as is or make changes.

Crypto Serial Number

Display only.

Crypto serial number assigned to this drive by Sun Microsystems, Inc. and stored in the drive's nonvolatile memory. Unique for each drive.

Note – This number does not need to be kept secure.

Drive Status Messages

Display only.

Detailed status and error messages for the drive. These are updated whenever information such as media or device keys or new drive pool mappings are transmitted to the drive. The messages are displayed in reverse chronological order (that is, most recent messages at the top).

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

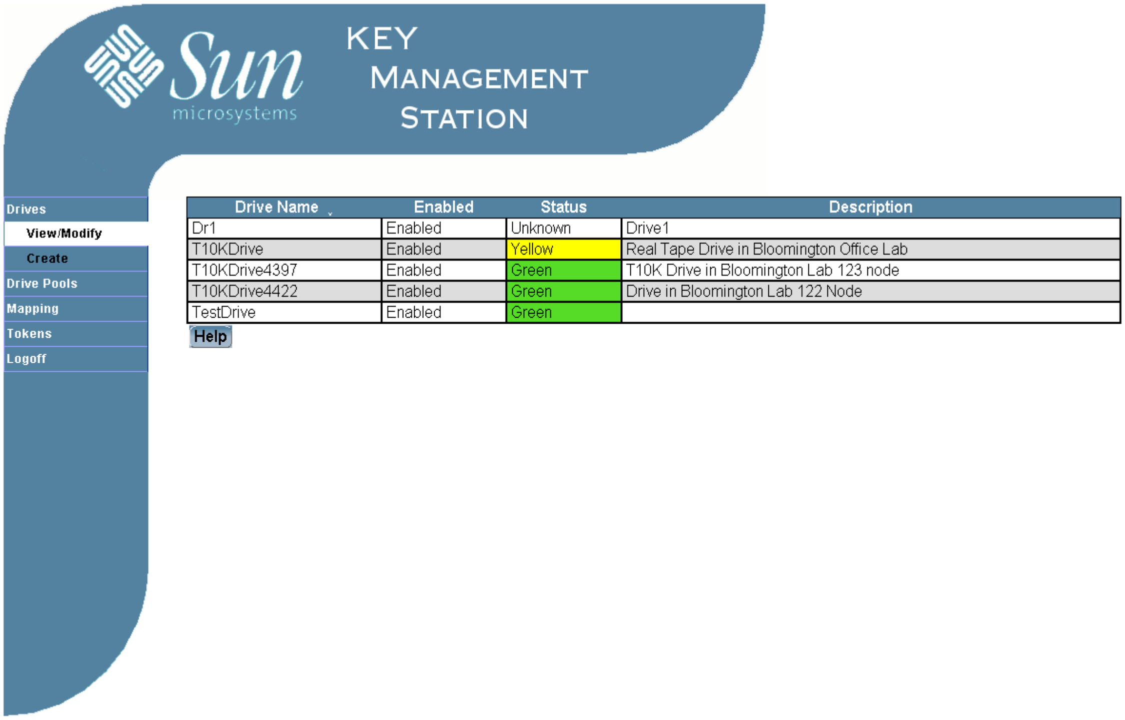
Click to display online help for the screen.

See Also

- Drives > Create
- Drives > View
- Tokens > Write Device Keys

Drives > View

Sample Screen



Drive Name	Enabled	Status	Description
Dr1	Enabled	Unknown	Drive1
T10KDrive	Enabled	Yellow	Real Tape Drive in Bloomington Office Lab
T10KDrive4397	Enabled	Green	T10K Drive in Bloomington Lab 123 node
T10KDrive4422	Enabled	Green	Drive in Bloomington Lab 122 Node
TestDrive	Enabled	Green	

Description

Display information about drives identified for encryption capability.

Operator Role

Security Officer or User

Screen Fields

Note – Click any screen field to modify the drive information. The Drives > Modify screen appears.

Drive Name

Display only.

Drive that has been designated for encryption capability.

Enabled

Display only.

Indicates whether device keys have been transmitted to the drive, enabling it for encryption.

Status

Display only.

Current status of the drive, for networked token operations. Last reported status, for air gap operations. Options are:

- Red—Drive is either not enabled for encryption or is in a reset state.
- Yellow - Pending—Device keys for the drive have been written to a token but have not yet been transmitted to the drive.
- Yellow—Device keys have been transmitted successfully to the drive.
- Green - Pending—Media keys for the drive have been written to a token but have not yet been transmitted to the drive.
- Green—Media keys have been transmitted successfully to the drive.

Description

Display only.

Description of the drive. Can be anything that describes the drive, such as the physical location within the library.

Buttons

Help

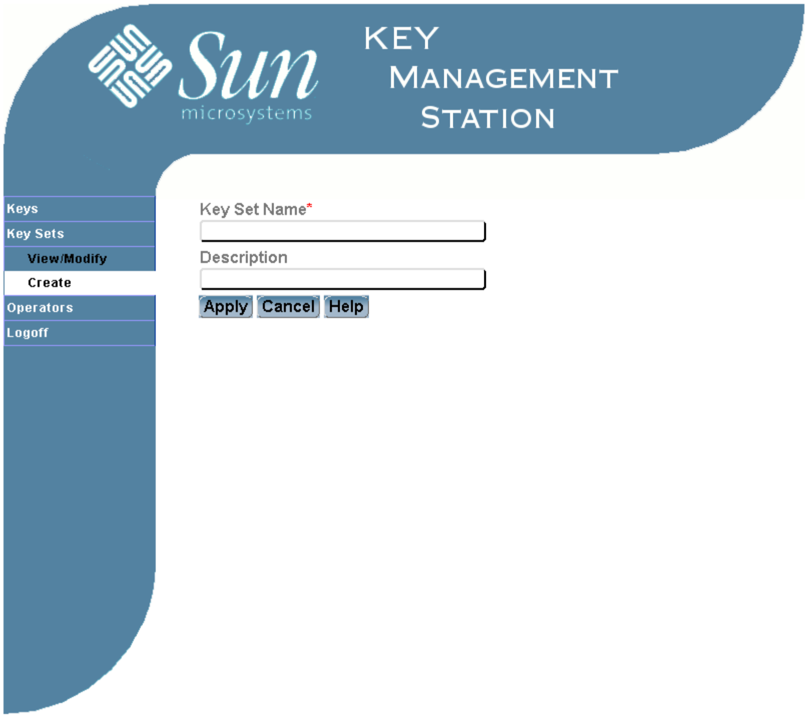
Click to display online help for the screen.

See Also

- Drives > Create
- Drives > Modify
- Tokens > Write Device Keys

Key Sets > Create

Sample Screen



Description

Allows you to create key sets.

Operator Role

Administrator

Screen Fields

Key Set Name

Required.

Name of the key set you want to create.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Description

Optional.

Description of the key set. Can be anything that describes the key set, such as the function, date, or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

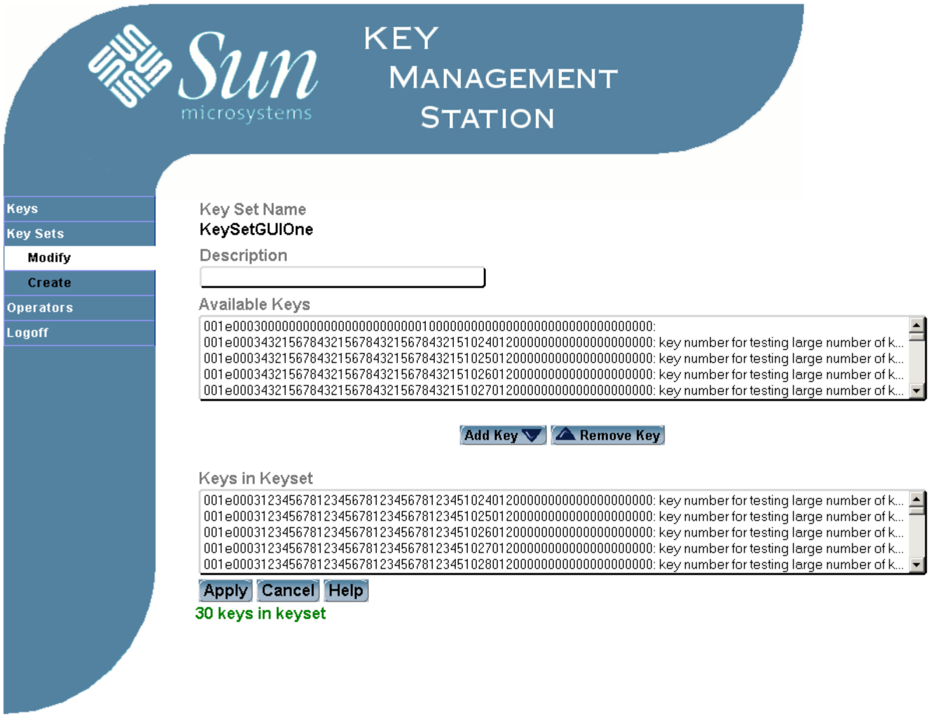
Click to display online help for the screen.

See Also

- Key Sets > Modify
- Key Sets > View
- Keys > Create
- Mapping > Modify
- Mapping > View

Key Sets > Modify

Sample Screen



Key Set Name
KeySetGUIOne

Description

Available Keys

```
001e000300000000000000000000000100000000000000000000000000000000:
001e0003432156784321567843215678432151024012000000000000000000000: key number for testing large number of k...
001e0003432156784321567843215678432151025012000000000000000000000: key number for testing large number of k...
001e0003432156784321567843215678432151026012000000000000000000000: key number for testing large number of k...
001e0003432156784321567843215678432151027012000000000000000000000: key number for testing large number of k...
```

Keys in Keyset

```
001e0003123456781234567812345678123451024012000000000000000000000: key number for testing large number of k...
001e0003123456781234567812345678123451025012000000000000000000000: key number for testing large number of k...
001e0003123456781234567812345678123451026012000000000000000000000: key number for testing large number of k...
001e0003123456781234567812345678123451027012000000000000000000000: key number for testing large number of k...
001e0003123456781234567812345678123451028012000000000000000000000: key number for testing large number of k...
```

30 keys in keyset

Description

Allows you to modify the description of a key set and to designate the media keys that are assigned to it.

Note – You CANNOT modify a key set that has been mapped to a drive pool.

Operator Role

Administrator

Screen Fields

Key Set Name

  Display only.

  Name of the key set.

Description

Description of the key set. Can be anything that describes the key set, such as the function, date, or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

The screen displays the value assigned previously. You can leave it as is or make changes.

Available Keys

The list displays the names and descriptions of all active media keys.

Note – Inactive keys are not displayed in this list, as they cannot be assigned to a key set.

To add a key to the key set, click the key name in the Available Keys box, and then click **Add Key**. The key name is moved to the Keys in Keyset box.

Keys in Keyset

The list displays the names and descriptions of all media keys that have been assigned to the key set. The name and description of each are separated by a colon (:).

To remove a media key from the key set, click the key name in the Keys in Keyset column, and then click **Remove Key**. The key name is moved to the Available Keys column.

Buttons

Add Key

Click to add the selected keys to the key set.

Remove Key

Click to remove the selected keys from the key set.

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

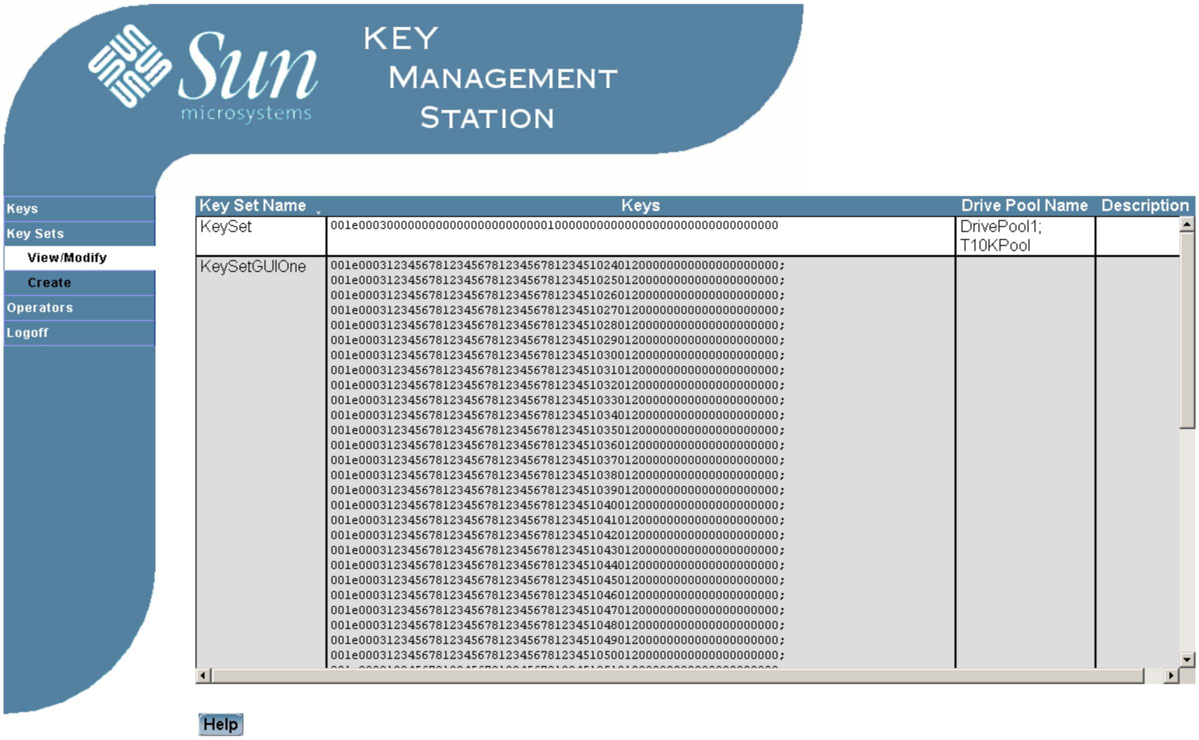
Click to display online help for the screen.

See Also

- Key Sets > Create
- Key Sets > View
- Keys > Create
- Mapping > Modify
- Mapping > View

Key Sets > View

Sample Screen



Key Set Name	Keys	Drive Pool Name	Description
KeySet	001e000300000000000000000000000010000000000000000000000000000000	DrivePool1; T10KPool	

KeySetGUIOne	001e00031234567812345678123456781234510240120000000000000000000000;
	001e00031234567812345678123456781234510250120000000000000000000000;
	001e00031234567812345678123456781234510260120000000000000000000000;
	001e00031234567812345678123456781234510270120000000000000000000000;
	001e00031234567812345678123456781234510280120000000000000000000000;
	001e00031234567812345678123456781234510290120000000000000000000000;
	001e00031234567812345678123456781234510300120000000000000000000000;
	001e00031234567812345678123456781234510310120000000000000000000000;
	001e00031234567812345678123456781234510320120000000000000000000000;
	001e00031234567812345678123456781234510330120000000000000000000000;
	001e00031234567812345678123456781234510340120000000000000000000000;
	001e00031234567812345678123456781234510350120000000000000000000000;
	001e00031234567812345678123456781234510360120000000000000000000000;
	001e00031234567812345678123456781234510370120000000000000000000000;
	001e00031234567812345678123456781234510380120000000000000000000000;
	001e00031234567812345678123456781234510390120000000000000000000000;
	001e00031234567812345678123456781234510400120000000000000000000000;
	001e00031234567812345678123456781234510410120000000000000000000000;
	001e00031234567812345678123456781234510420120000000000000000000000;
	001e00031234567812345678123456781234510430120000000000000000000000;
	001e00031234567812345678123456781234510440120000000000000000000000;
	001e00031234567812345678123456781234510450120000000000000000000000;
	001e00031234567812345678123456781234510460120000000000000000000000;
	001e00031234567812345678123456781234510470120000000000000000000000;
	001e00031234567812345678123456781234510480120000000000000000000000;
	001e00031234567812345678123456781234510490120000000000000000000000;
	001e00031234567812345678123456781234510500120000000000000000000000;		

Description

Allows you to display information about key sets.

Operator Role

Administrator

Screen Fields

Note – Click any screen field to modify the key set information. The Key Sets > Modify screen appears.

Key Set Name

Display only.

Name of the key set.

Keys

Display only.

Key IDs of the media keys that have been assigned to the key set. Individual IDs are separated by a semicolon (;).

Drive Pool Name

Display only.

Name of the drive pool to which the key set has been assigned.

Description

Display only.

Description of the key set. Can be anything that describes the key set, such as the function, date, or department.

Buttons

Help

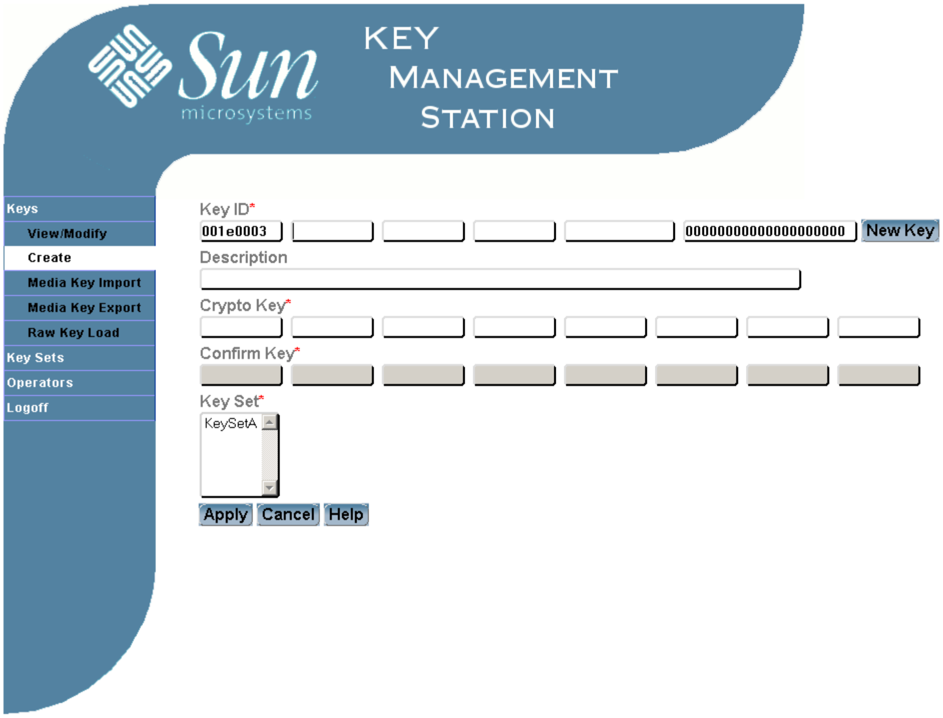
Click to display online help for the screen.

See Also

- Key Sets > Create
- Key Sets > Modify
- Keys > Create
- Mapping > Modify
- Mapping > View

Keys > Create

Sample Screen



Key ID*
001e0003 00000000000000000000
Description
Crypto Key*
Confirm Key*
Key Set*
KeySetA

Description

Allows you to add a media key to the KMS database. You can use either of the following methods:

- Create the key automatically from the raw keys in the KMS database. The key value is randomly selected from the raw keys, and the key ID is assigned automatically. Raw keys must be available in the KMS database.
- Add the key manually from an external source. You must obtain the key value and key ID and then enter them manually.

You must also assign the new media key to a key set. By default, media keys are created with an "active" status.

Operator Role

Administrator

Screen Fields

Key ID

Display only, if you are creating keys automatically. Required, if you are creating keys manually.

Visible ID for the media key.

Note – The first four and the last ten bytes of the key ID are assigned by the KMS software and cannot be modified.

---

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

This value can be entered either of two ways:

- Supplied from the KMS database when you click **New Key**.
- Entered manually from another source.

Note – If this field is not filled in when you click **New Key**, it means there are no raw keys available to create media keys. See your Crypto Key Management Station administrator for assistance.

Description

Optional.

Description of the media key. Can be anything that describes the key, such as the function, date, or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), _ (underscore), and spaces.

Crypto Key

Display only, if creating keys automatically. Required, if creating keys manually.

Cryptographic media key value.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

Confirm Key

Display only, if creating keys automatically. Required, if creating keys manually.

For security purposes, the Crypto Key is either re-displayed on the screen when you click **New Key,** or it must be re-entered manually. If re-entered manually, the two entries must match exactly.

Key Set

Required.

The list displays the names of all key sets that have not been assigned to a drive pool.

Click the key set to which you want to assign this media key.

Note – Using this screen, you must assign the key to only one key set. To assign the key to additional key sets or to remove the key from all key sets, you can use the **Key Sets > Modify** screen or the `modify_keyset` CLI command.

Buttons

New Key

Click to create a new key from the raw keys in the KMS database. Raw keys must be available.

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

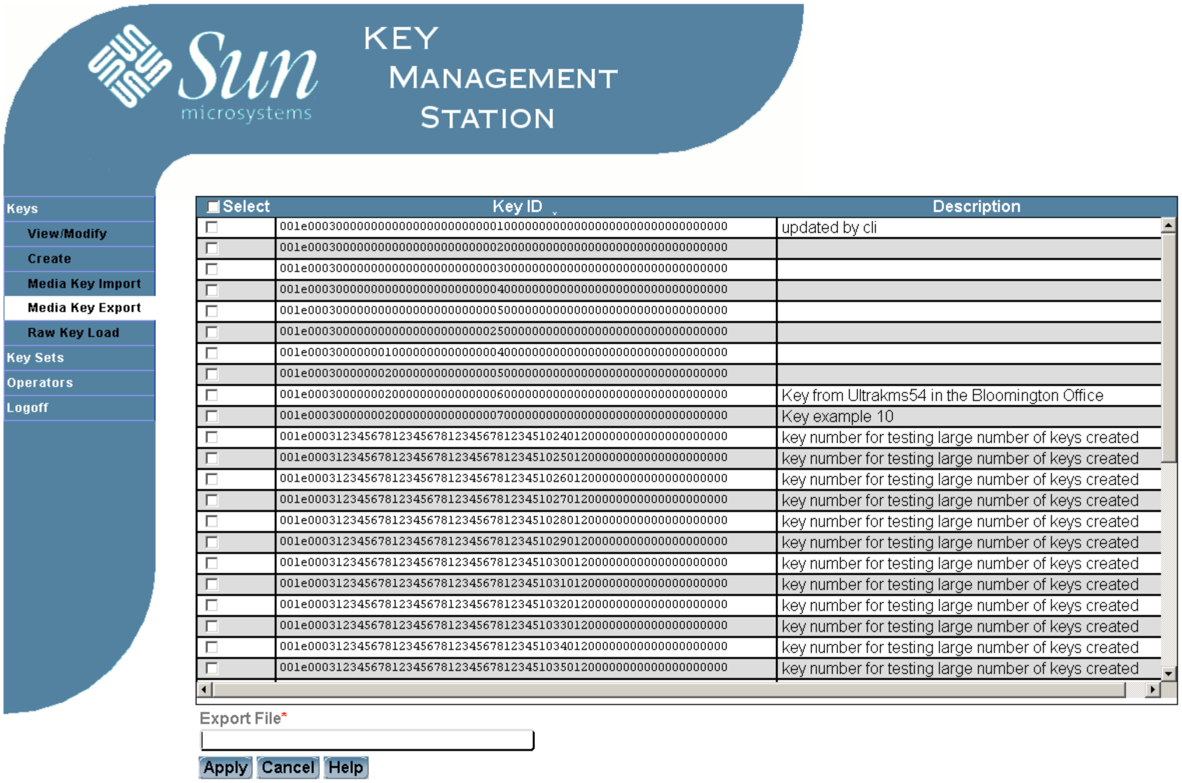
Click to display online help for the screen.

See Also

- Key Sets > Create
- Key Sets > Modify
- Key Sets > View
- Keys > Media Key Export
- Keys > Media Key Import
- Keys > Modify
- Keys > Raw Key Load
- Keys > View

Keys > Media Key Export

Sample Screen



☐ Select	Key ID	Description
☐	001e000300000000000000000000000100000000000000000000000000000000	updated by cli
☐	001e000300000000000000000000000200000000000000000000000000000000	
☐	001e000300000000000000000000000300000000000000000000000000000000	
☐	001e000300000000000000000000000400000000000000000000000000000000	
☐	001e000300000000000000000000000500000000000000000000000000000000	
☐	001e000300000000000000000000000250000000000000000000000000000000	
☐	001e000300000001000000000000000400000000000000000000000000000000	
☐	001e000300000002000000000000000500000000000000000000000000000000	
☐	001e000300000002000000000000000600000000000000000000000000000000	Key from Ultrakms54 in the Bloomington Office
☐	001e000300000002000000000000000700000000000000000000000000000000	Key example 10
☐	001e000312345678123456781234567812345102401200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345102501200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345102601200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345102701200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345102801200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345102901200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345103001200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345103101200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345103201200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345103301200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345103401200000000000000000000	key number for testing large number of keys created
☐	001e000312345678123456781234567812345103501200000000000000000000	key number for testing large number of keys created

Export File*

Description

Note – This activity is not available if the Crypto Key Management Station administrator has disabled it with the `export_media_key_disable` CLI command. To re-enable this activity, the administrator must use the `export_media_key_enable` command.

Allows you to export selected media keys to a designated file. The data is written in ASCII text format and includes the file checksum value, media key IDs, key values, and key descriptions.

You might use this activity to transfer media keys from one Crypto Key Management Station to another, or to safely offload keys from the KMS database before performing a software upgrade.

This activity does not export the database backup encryption key. To view this key, the Crypto Key Management Station administrator can use the `view_backup_key` CLI command.

Note – The export file is a useful record of the encryption key data used at your site. Because this data is very sensitive, you should ensure that the file and any hardcopy printouts of it are kept in a secure location. For added security, you can encrypt the file using standard Solaris tools. See the `encrypt` man page for details.

Note – An export file created using KMS version 1.2 or later is not compatible with prior releases of the KMS software.

Operator Role

Administrator

Screen Fields

Select

Optional.

Click to indicate that this key is to be exported. You must select at least one key to perform the export operation.

Click the check box by the column heading to select all items in the list; click again to de-select all items.

Key ID

Display only.

Visible ID for the media key.

Only keys that have been assigned to a key set are displayed.

Description

Display only.

Description of the media key. Can be anything that describes the key, such as the function, date, or department.

Export File

Required.

Name of the file to which you want to export the data. The file is created in the `/export/home/kms/mnt_keys` directory. You must specify a new file name; if the file already exists, it will NOT be overwritten.

Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), and _ (underscore). Spaces are NOT allowed.

The data is written in ASCII text format. Following is a sample export file.

```
# media key file d3787356ad2b80d3f3bae76026d404e0f2ee6d94
001e000300000000000000000000000100000000000000000000000000000000
00,5944aea0d90d53d1a69b934d0a9d7d37354bc6d8e8fa3d354877e6a9cca
fa8c9,updated by cli
001e000300000002000000000000000600000000000000000000000000000000
00,2459dde57b1a3f0439bad8acabc62fa127ea3ee29e26bac780f341e8bc6
81db0,Key from Ultrakms54 in the Bloomington Office
001e000300000002000000000000000700000000000000000000000000000000
00,aad5b62e6672723c8d2107a1a1bf846faa9b742499051fb8a22dc3f310f
46b92,Key example 10
```

Buttons

Apply

Click to export the keys to the specified file.

Cancel

Click to cancel the changes.

Help

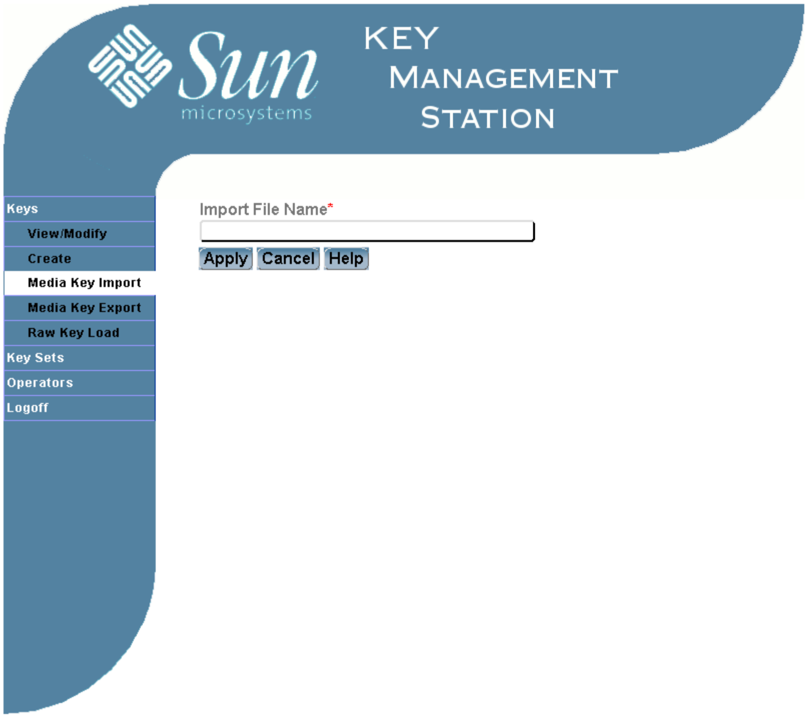
Click to display online help for the screen.

See Also

- Keys > Create
- Keys > Media Key Import
- Keys > Raw Key Load
- Keys > View

Keys > Media Key Import

Sample Screen



Import File Name*

Description

Allows you to import media keys to the Key Management Station database. The keys must have been previously written to an ASCII text export file using the **Keys > Media Key Export** GUI screen or the `export_media_key` CLI command. The export file must have been created using KMS version 1.2 or later.

You might use this activity to transfer media keys from one Crypto Key Management Station to another, or to restore keys to the KMS database after a software upgrade.

Note – Before performing this activity, you must obtain the name of the export file containing the media keys. The file must be located in the `/export/home/kms/mnt_keys` directory. If the export file has been modified in any way, the keys cannot be imported into the KMS database.

Note – Only new media keys are imported. If you have already imported media keys, any duplicates are rejected.

Operator Role

Administrator

Screen Fields

Import File Name

Required.

Name of the file containing the media keys you want to import. The file must be located in the `/export/home/kms/mnt_keys` directory.

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

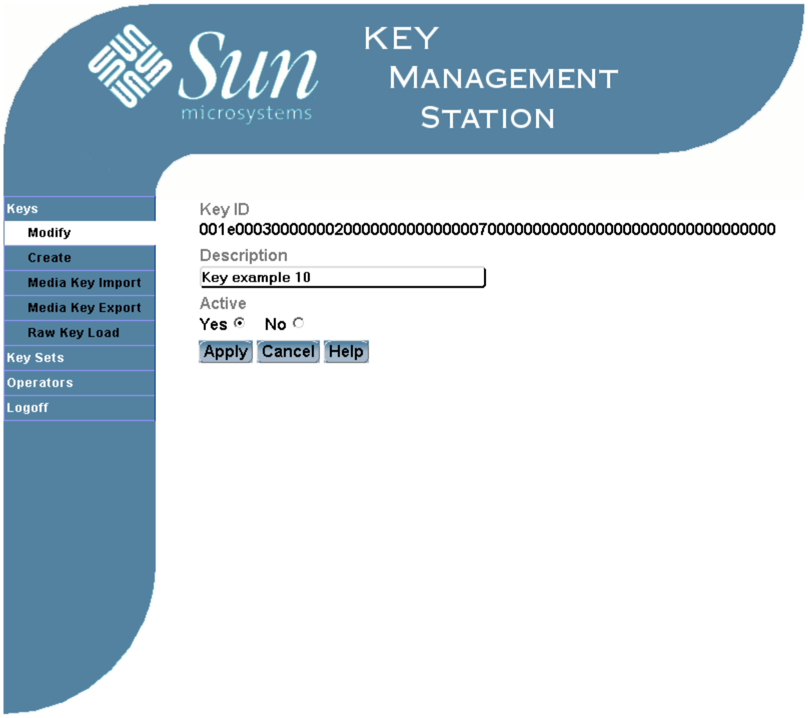
Click to display online help for the screen.

See Also

- Keys > Create
- Keys > Media Key Export
- Keys > Modify
- Keys > Raw Key Load
- Keys > View

Keys > Modify

Sample Screen



Key ID
001e000300000002000000000000000700000000000000000000000000000000

Description
Key example 10

Active
Yes ● No ○

Description

Allows you to modify the description and status of a media key.

Note – You cannot modify a key if it has been assigned to a key set.

Operator Role

Administrator

Screen Fields

Key ID

Display only.

Visible ID for the media key.

Description

Description of the media key. Can be anything that describes the key, such as the function, date, or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

The screen displays the value assigned previously. You can leave it as is or make changes.

Active

Indicates whether the key is active. Only one value can be assigned at a time.

- Yes – Key is active.
- No – Key is inactive; cannot be assigned to a key set.

The screen displays the value assigned previously. You can leave it as is or make changes.

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

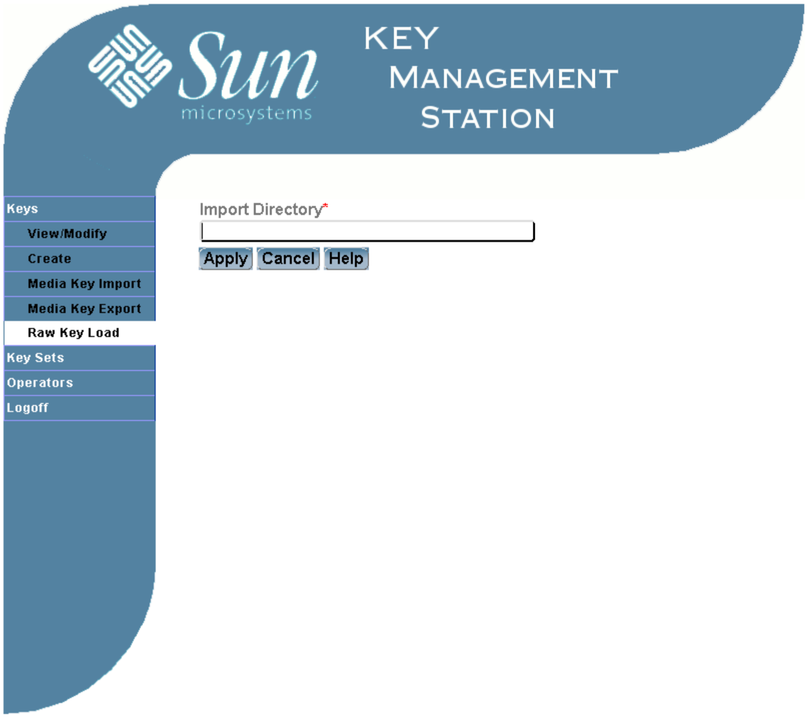
Click to display online help for the screen.

See Also

- Key Sets > Create
- Key Sets > View
- Keys > Create
- Keys > Media Key Export
- Keys > Media Key Import
- Keys > Raw Key Load
- Keys > View

Keys > Raw Key Load

Sample Screen



Description

Allows you to import raw keys to the KMS database. The raw keys are usually generated, using the `mkkeys` script, from the Sun Crypto Accelerator 6000 (SCA6000) card included in the Crypto Key Management Station. They can also be imported from an outside source.

After the raw keys have been successfully imported, the files created by the `mkkey` script (`rawdata.dat`, `checksums.txt`, `ident.txt`, `info.txt`, and `length.txt`) are automatically deleted.

Note – Before performing this activity, you must obtain the full path of the directory containing the raw keys.

Note – Only new raw keys are imported. If you have already imported raw keys, any duplicates are rejected.

Note – Prior to KMS v1.2, this activity was performed with the **Keys > Import** GUI screen or the `import_kmedia` CLI command.

Operator Role

Administrator

Screen Fields

Import Directory

Required.

Full path of the directory containing the raw keys you want to import. If you are importing from the Sun Crypto Accelerator 6000 (SCA6000) card included in the Crypto Key Management Station, this directory is typically named `/export/home/kms/mnt_cd`.

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

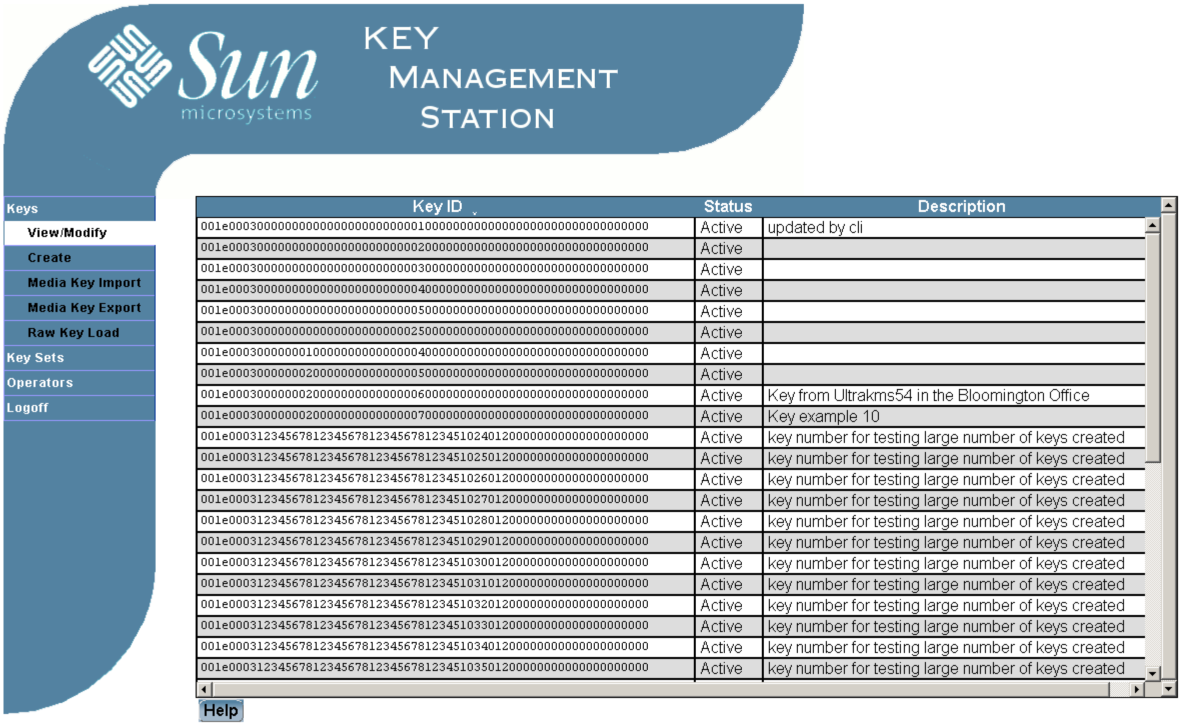
Click to display online help for the screen.

See Also

- Key Sets > Create
- Key Sets > View
- Keys > Create
- Keys > Media Key Export
- Keys > Media Key Import
- Keys > View

Keys > View

Sample Screen



Key ID	Status	Description
001e000300000000000000000000000100000000000000000000000000000000	Active	updated by cli
001e000300000000000000000000000200000000000000000000000000000000	Active	
001e000300000000000000000000000300000000000000000000000000000000	Active	
001e000300000000000000000000000400000000000000000000000000000000	Active	
001e000300000000000000000000000500000000000000000000000000000000	Active	
001e000300000000000000000000000250000000000000000000000000000000	Active	
001e000300000001000000000000000400000000000000000000000000000000	Active	
001e000300000002000000000000000500000000000000000000000000000000	Active	
001e000300000002000000000000000600000000000000000000000000000000	Active	Key from Ultrakms54 in the Bloomington Office
001e000300000002000000000000000700000000000000000000000000000000	Active	Key example 10
001e000312345678123456781234567812345102401200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345102501200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345102601200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345102701200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345102801200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345102901200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345103001200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345103101200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345103201200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345103301200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345103401200000000000000000000	Active	key number for testing large number of keys created
001e000312345678123456781234567812345103501200000000000000000000	Active	key number for testing large number of keys created

Description

Allows you to display information about media keys.

Operator Role

Administrator

Screen Fields

Note – Click any screen field to modify the key information; the Keys > Modify screen appears. You can modify a key only if it has not been assigned to a key set.

Key ID

Display only.

Visible ID for the media key.

Status

Display only.

Current status of the media key.

- Active – Key is active
- Inactive – Key has been revoked; it cannot be assigned to a key set.

Description

Display only.

Description of the media key. Can be anything that describes the key, such as the function, date, or department.

Buttons

Help

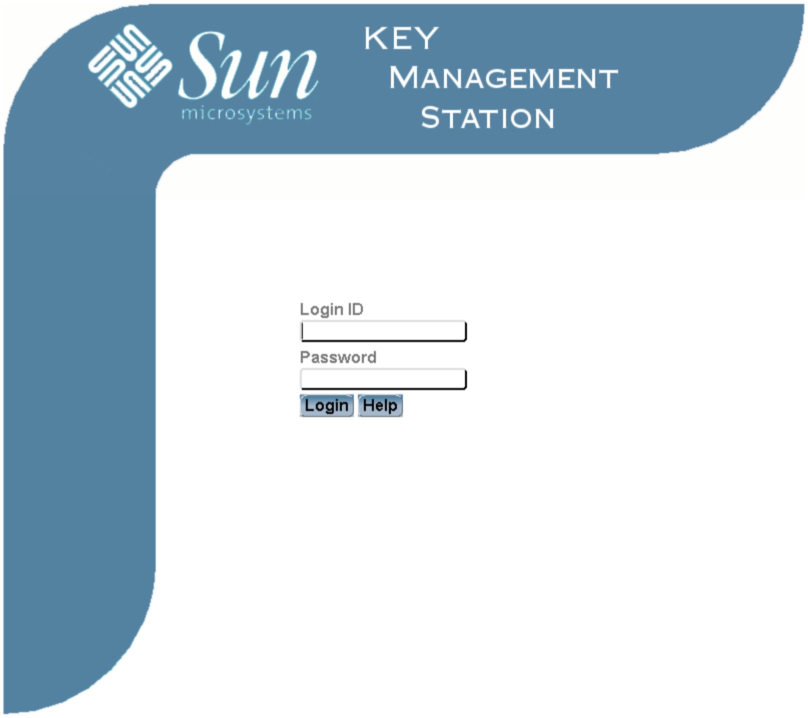
Click to display online help for the screen.

See Also

- Key Sets > View
- Keys > Create
- Keys > Media Key Export
- Keys > Media Key Import
- Keys > Modify
- Keys > Raw Key Load

Login

Sample Screen



Description

Allows you to log in to the KMS GUI.

Note – You must have a valid login ID and password to use this screen. See your system administrator for details.

Operator Role

Any

Screen Fields

Login ID

Required.

Login ID you want to use for this session.

Password

Required.

Password assigned to the login ID.

Buttons

Login

Click to log in to the KMS application.

Help

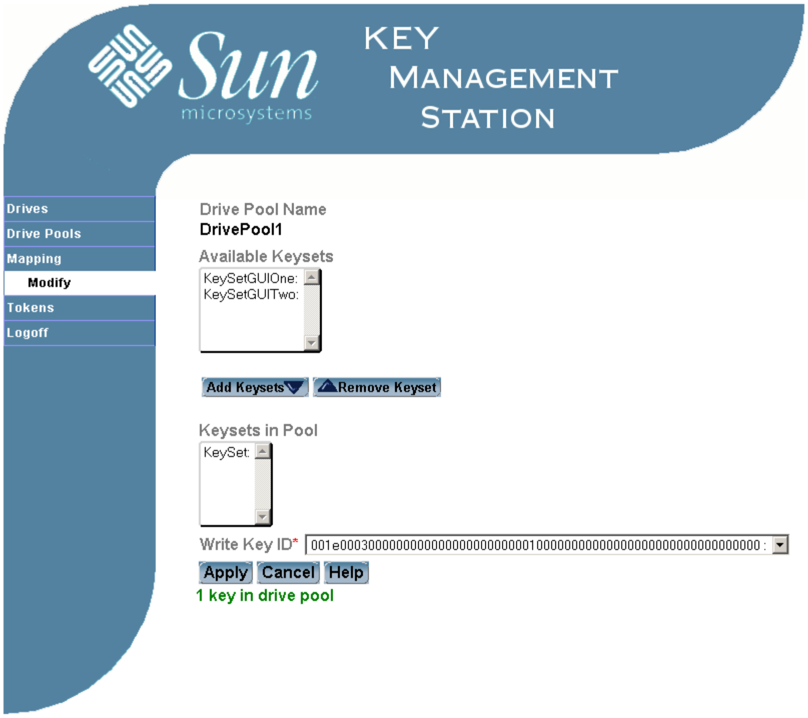
Click to display online help for the screen.

See Also

- Operators > Create
- Operators > View

Mapping > Modify

Sample Screen



Drive Pool Name
DrivePool1

Available Keysets
KeySetGUIOne:
KeySetGUITwo:

Keysets in Pool
KeySet:

Write Key ID* 001e0003000000000000000000000001000000000000000000000000000000000 :

1 key in drive pool

Description

Allows you to assign key sets to a selected drive pool. A drive pool can have any number of key sets.

Also allows you to designate the write key for the drive pool. A drive pool can have only one write key at a time. The write key must be assigned if key sets are assigned to the drive pool.

Note – Empty key sets (those with no assigned keys) cannot be mapped to a drive pool.

Note – The total number of keys in all key sets mapped to a single drive pool cannot exceed 32.

Operator Role

User

Screen Fields

Drive Pool Name

Display only.

Name of the drive pool. Unique for each pool.

Available Keysets

The list displays the names and descriptions of all non empty key sets that have not already been assigned to this drive pool. The name and description of each are separated by a colon (:).

To add a key set to the drive pool, click the key set name in the Available Keysets column, and then click **Add Key Set**. The key set name is moved to the Keysets in Pool column.

Note – The total number of keys in all key sets mapped to the drive pool cannot exceed 32.

Keysets in Pool

The list displays the names and descriptions of all key sets that have been assigned to the drive pool. The name and description of each are separated by a colon (:).

To remove a key set from the drive pool, click the key set name in the Keysets in Pool column, and then click **Remove Key Set**. The key set name is moved to the Available Keysets column.

Write Key

Write key for the drive pool. You can specify any key from all the key sets assigned to the drive pool.

You must designate a write key if at least one key set is assigned to the drive pool. You do not need to designate a write key if no key sets are assigned to the drive pool.

The screen displays the value assigned previously. You can leave it as is or make changes.

Buttons

Add Keyset

Click to add the selected key sets to the drive pool.

Remove Keyset

Click to remove the selected key sets from the drive pool.

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

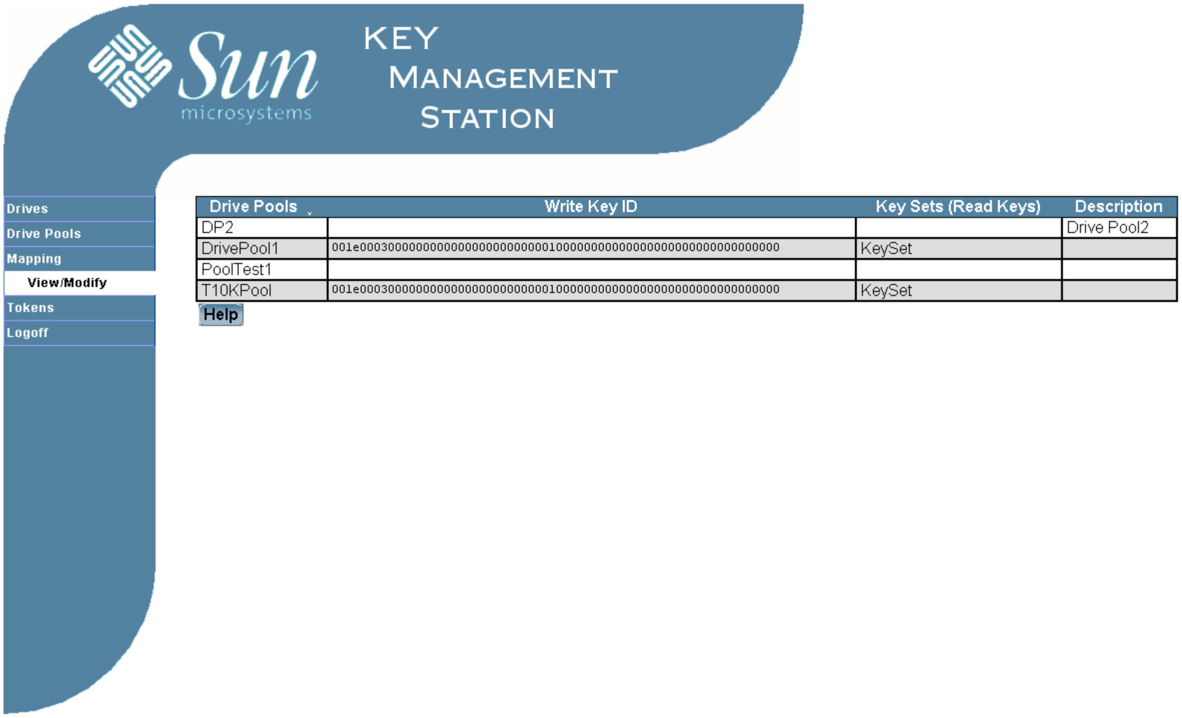
Click to display online help for the screen.

See Also

- Drive Pools > Create
- Drive Pools > View
- Key Sets > Create
- Key Sets > View
- Mapping > View

Mapping > View

Sample Screen



Drive Pools	Write Key ID	Key Sets (Read Keys)	Description
DP2			Drive Pool2
DrivePool1	001e0003000000000000000000000001000000000000000000000000000000000	KeySet	
PoolTest1			
T10KPool	001e0003000000000000000000000001000000000000000000000000000000000	KeySet	

Description

Allows you to display drive pool/key set mapping information. This includes the key sets and the write key assigned to each drive pool.

Operator Role

User

Screen Fields

Note – Click any screen field to modify the drive pool/key set mapping information. The Mapping > Modify screen appears.

Drive Pools

Display only.

Name of the drive pool. Unique for each pool.

Write Key

Display only.

Current write key for the drive pool. A value appears if there is at least one key set assigned to the drive pool. No value appears if no key sets are assigned to the drive pool.

Key Sets (Read Keys)

Display only.

Names of the key sets that have been assigned to the drive pool. Individual names are separated by a semicolon (;).

Description

Display only.

Description of the drive pool. Can be anything that describes the drive pool, such as the function or department.

Buttons

Help

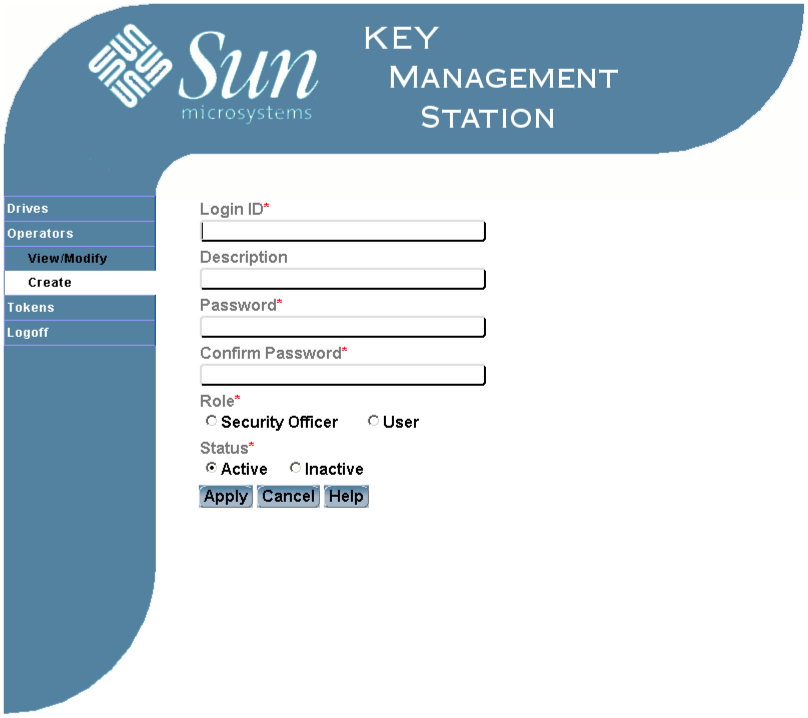
Click to display online help for the screen.

See Also

- Drive Pools > Create
- Drive Pools > View
- Key Sets > Create
- Key Sets > View
- Mapping > View
- Mapping > Modify

Operators > Create

Sample Screen



Login ID*

Description

Password*

Confirm Password*

Role*
○ Security Officer ○ User

Status*
● Active ○ Inactive

Description

Allows you to create a new KMS login ID. You must assign a password, operator role, and status (active or inactive) to each login ID.

Operator Role

Administrator, to create login IDs with the Administrator operator role

Administrator or Security Officer, to create login IDs with the Security Officer operator role

Security Officer, to create login IDs with the User operator role

Screen Fields

Login ID

Required.

Login ID you want to create. Unique for each user.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Description

Optional.

Description of the login ID. Can be anything that describes the user, such as the name, department, or operator role.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

Password

Required.

Password you want to assign to the login ID.

Note – You cannot reuse the previous three passwords that have been assigned to the login ID.

8–20 printable characters. The first eight characters must include at least ONE EACH of the following:

- Lowercase letter (a–z)
- Uppercase letter (A–Z)
- Number (0–9)
- Special character (~!@#$%^&*()_+`-={}|[]\:";’<>?,./)

Confirm Password

Required.

For security purposes, re-enter the password you entered in the previous field. The two entries must match exactly.

Role

Required.

Operator role you want to assign to the login ID. This determines the KMS GUI screens and CLI commands the login ID is authorized to access. Only one value can be assigned at a time. There is no default. Options are:

- Administrator
- Security Officer
- User

Note – You can assign only the operator roles for which you have sufficient authorization. If you are using the Administrator role, you can assign only the Administrator and Security Officer roles. If you are using the Security Officer role, you can assign only the Security Officer and User roles.

Status

Required.

Status you want to assign to the login ID. This determines whether the login ID is valid for logging in to the Key Management Station. Only one value can be assigned at a time.

- Active – Login ID is valid for use; this is the default.
- Inactive – Login ID is not valid for use.

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

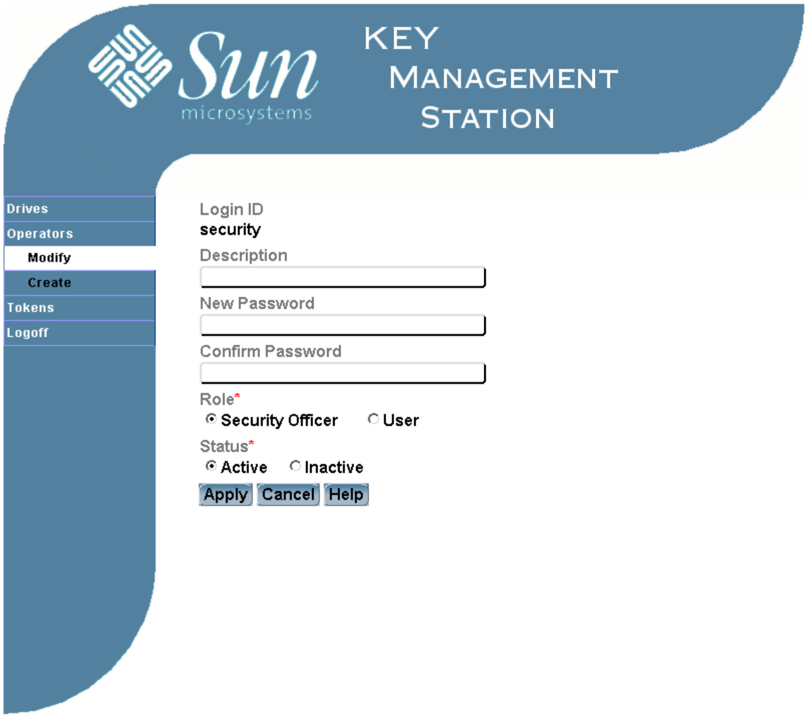
Click to display online help for the screen.

See Also

- Login
- Operators > Modify
- Operators > View

Operators > Modify

Sample Screen



Login ID
security

Description

New Password

Confirm Password

Role*
● Security Officer ○ User

Status*
● Active ○ Inactive

Description

Allows you to modify the description, password, operator role, or status of an existing login ID.

Note – You cannot change the operator role or status of the `KmsAdm` login ID, which is the default Crypto Key Management Station administrator supplied with the product.

Operator Role

Administrator, to modify login IDs with the Administrator operator role

Administrator or Security Officer, to modify login IDs with the Security Officer operator role

Security Officer, to modify login IDs with the User operator role

Screen Fields

Login ID

Display only.

Login ID assigned to the user. Unique for each user.

Description

Description of the login ID. Can be anything that describes the user, such as the name, department, or operator role.

The screen displays the value assigned previously. You can leave it as is or make changes.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

New Password

Password you want to assign to the login ID.

Note – You cannot reuse the previous three passwords that have been assigned to the login ID.

8–20 printable characters. The first eight characters must include at least ONE EACH of the following:

- Lowercase letter (a–z)
- Uppercase letter (A–Z)
- Number (0–9)
- Special character (~!@#$%^&*()_+`-={}|[]\:";’<>?,./)

Confirm Password

For security purposes, re-enter the password you entered in the previous field. The two entries must match exactly.

The screen displays the value assigned previously. You can leave it as is or make changes.

Role

Operator role you want to assign to the login ID. This determines the KMS GUI screens and CLI commands the login ID is authorized to access. Only one value can be assigned at a time. There is no default. Options are:

- Administrator
- Security Officer
- User

Note – You can assign only the operator roles for which you have sufficient authorization. If you are using the Administrator role, you can assign only the Administrator and Security Officer roles. If you are using the Security Officer role, you can assign only the Security Officer and User roles.

The screen displays the value assigned previously. You can leave it as is or make changes.

Status

Status you want to assign to the login ID. This determines whether the login ID is valid for logging in to the Key Management Station. Only one value can be assigned at a time.

- Active – Login ID is valid for use; this is the default.
- Inactive – Login ID is not valid for use.

The screen displays the value assigned previously. You can leave it as is or make changes.

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

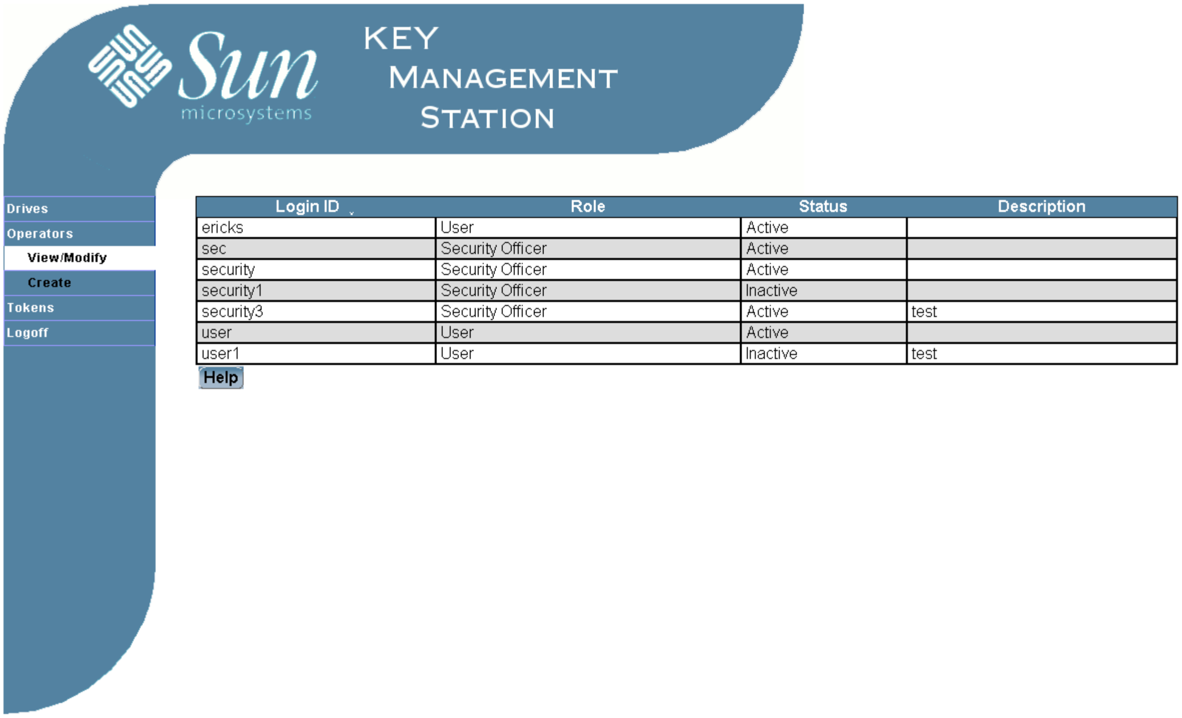
Click to display online help for the screen.

See Also

- Login
- Operators > Create
- Operators > View

Operators > View

Sample Screen



Login ID	Role	Status	Description
ericks	User	Active	
sec	Security Officer	Active	
security	Security Officer	Active	
security1	Security Officer	Inactive	
security3	Security Officer	Active	test
user	User	Active	
user1	User	Inactive	test

Description

Allows you to display information about login IDs.

Note – You can display only the operator roles for which you have sufficient authority. If you are using the Administrator role, you can display only the Administrator and Security Officer roles. If you are using the Security Officer role, you can display only the Security Officer and User roles.

Operator Role

Administrator, to display login IDs with the Administrator operator role

Administrator or Security Officer, to display login IDs with the Security Officer operator role

Security Officer, to display login IDs with the User operator role

Screen Fields

Note – Click any screen field to modify the login ID information. The Operators > Modify screen appears.

Login ID

Display only.

Login ID assigned to the user. Unique for each user.

Role

Display only.

Operator role assigned to the login ID. Determines which KMS GUI screens the login ID is authorized to access. Options are:

- Administrator
- Security Officer
- User

Note – You can display only the operator roles for which you have sufficient authorization. If you are using the Administrator role, you can display only the Administrator and Security Officer roles. If you are using the Security Officer role, you can display only the Security Officer and User roles.

Status

Display only.

Current status of the login ID. Determines whether the login ID is valid for logging in to the Key Management Station.

- Active – Login ID is valid for use.
- Inactive – Login ID is not valid for use.

Description

Display only.

Description of the login ID. Can be anything that describes the user, such as the name, department, or operator role.

Buttons

Help

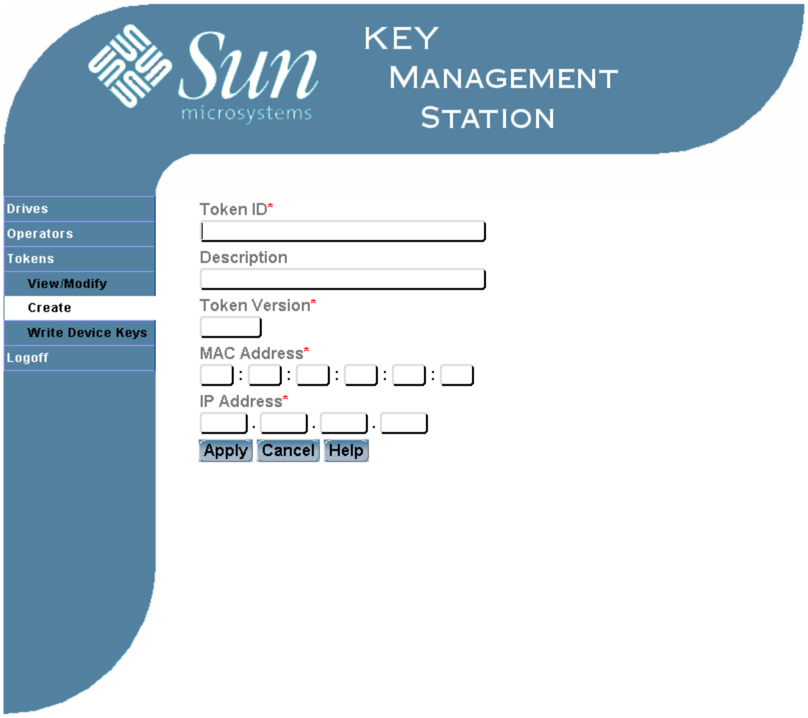
Click to display online help for the screen.

See Also

- Login
- Operators > Create
- Operators > Modify

Tokens > Create

Sample Screen



Description

Allows you to identify a physical token that you want to use for transmitting media or device keys.

Note – Before you perform this activity, the Crypto Key Management Station administrator must use the `send_permanent_ip` CLI command to assign permanent IP settings to the token. You must obtain from the administrator the following information for the token: 1) the unique MAC address, which is printed on the token label; 2) the IP address to be used by the KMS software to communicate with the token.

Operator Role

Security Officer or User

Screen Fields

Token ID

Required.

ID of the physical token you want to use for transmitting media or device keys. Must be unique for each token.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Description

Optional.

Description of the token. Can be anything that describes the token, such as the type of token or date created.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), _ (underscore), and spaces.

Token Version

Required.

Current version of the token firmware.

Four digits, in the format *nn*.*nn*. For example, 01.20.

MAC Address

Required.

MAC address of the physical token. Unique for each token. Printed on the token label.

Twelve hexadecimal digits, separated into six groups of two digits each. For example, `00.90.C2.67.89.ab`. Each group must have two printable hex digits, with leading zeroes as needed. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

IP Address

Required.

Static IP address the KMS software uses to communicate with the token.

- For networked token operations, this is an IP address on the same subnet as the library drives.
- For air gap operations, this is an IP address on the same subnet as the Crypto Key Management Station.

The default IP address for a new token is 10.0.0.2.

32-bit numeric address, in dotted decimal notation, *nnn*.*nnn*.*nnn*.*nnn*. Valid values for *nnn* are 0 to 255. For example, `123.119.01.73`.

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

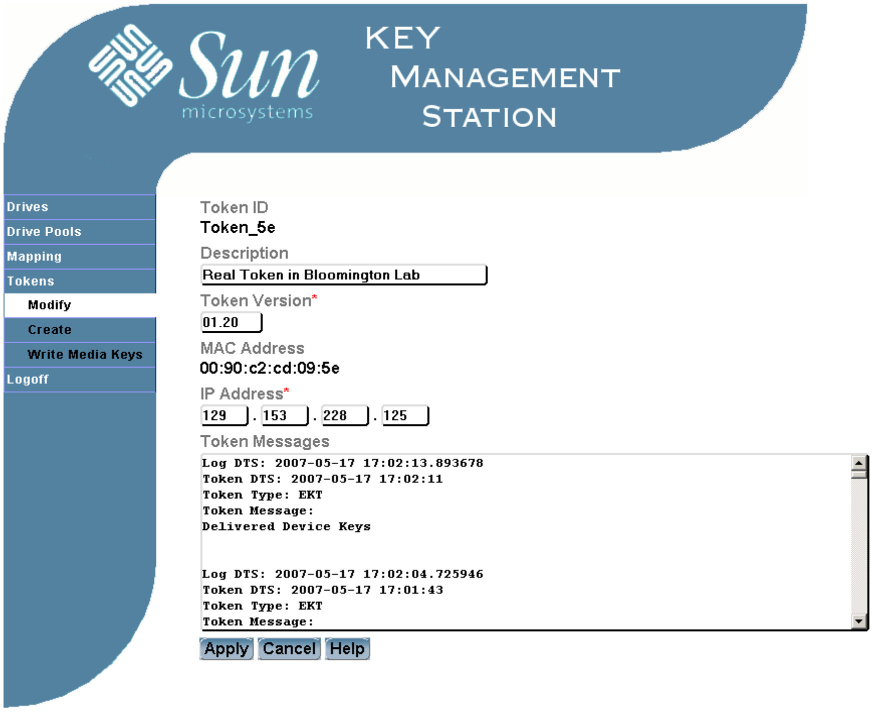
Click to display online help for the screen.

See Also

- Tokens > Modify
- Tokens > Token Selection Screen
- Tokens > View
- Tokens > Write Device Keys
- Tokens > Write Media Keys

Tokens > Modify

Sample Screen



Token ID
Token_5e

Description
Real Token in Bloomington Lab

Token Version*
01.20

MAC Address
00:90:c2:cd:09:5e

IP Address*
129 . 153 . 228 . 125

Token Messages

```
Log DTS: 2007-05-17 17:02:13.893678
Token DTS: 2007-05-17 17:02:11
Token Type: EKT
Token Message:
Delivered Device Keys


Log DTS: 2007-05-17 17:02:04.725946
Token DTS: 2007-05-17 17:01:43
Token Type: EKT
Token Message:
```

Description

Allows you to modify information for a physical token.

Also displays detailed messages about how the token has been used to transmit device or media keys to the drives.

Operator Role

Security Officer or User

Screen Fields

Token ID

Display only.

ID of the token. Unique for each token.

Description

Description of the token. Can be anything that describes the token, such as the type of token or date created.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

The screen displays the value assigned previously. You can leave it as is or make changes.

Token Version

Current version of the token firmware.

Four digits, in the format *nn*.*nn*. For example, 01.20.

The screen displays the value assigned previously. You can leave it as is or make changes.

MAC Address

Display only.

MAC address of the physical token. Unique for each token. Printed on the token label.

IP Address

Static IP address the KMS software uses to communicate with the token.

- For networked token operations, this is an IP address on the same subnet as the library drives.
- For air gap operations, this is an IP address on the same subnet as the Crypto Key Management Station.

32-bit numeric address, in dotted decimal notation, *nnn*.*nnn*.*nnn*.*nnn*. Valid values for *nnn* are 0 to 255. For example, `123.119.01.73`.

The screen displays the value assigned previously. You can leave it as is or make changes.

Token Messages

Display only.

Detailed status messages for the token. These are updated whenever the token is used to transmit media or device keys to a drive. The messages are displayed in reverse chronological order (that is, most recent messages at the top).

Buttons

Apply

Click to apply the changes.

Cancel

Click to cancel the changes.

Help

Click to display online help for the screen.

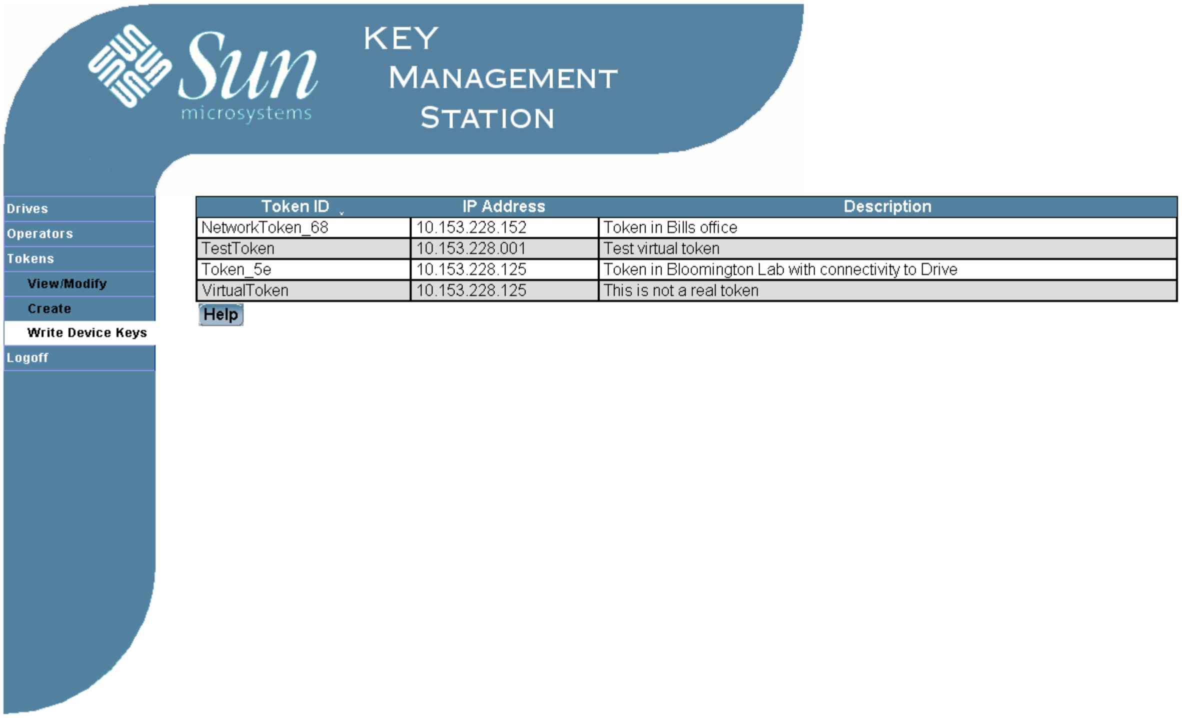
See Also

- Tokens > Create
- Tokens > Token Selection Screen
- Tokens > View

- Tokens > Write Device Keys
- Tokens > Write Media Keys

Tokens > Token Selection Screen

Sample Screen



Token ID	IP Address	Description
NetworkToken_68	10.153.228.152	Token in Bills office
TestToken	10.153.228.001	Test virtual token
Token_5e	10.153.228.125	Token in Bloomington Lab with connectivity to Drive
VirtualToken	10.153.228.125	This is not a real token

Description

Allows you to select the token to which you want to write device or media keys.

Note – This is an intermediate screen that appears when you select either Tokens > Write Device Keys or Tokens > Write Media Keys.

Click any screen field to select the token. The Tokens > Write Device Keys or Tokens > Write Media Keys screen appears.

The token you select must be on same IP subnet as the drives to which you want to transmit the device or media keys.

Operator Role

Security Officer or User

Screen Fields

Token ID

Display only.

ID of the token. Unique for each token.

IP Address

Display only.

Static IP address the KMS software uses to communicate with the token.

- For networked token operations, this is an IP address on the same subnet as the library drives.
- For air gap operations, this is an IP address on the same subnet as the Crypto Key Management Station.

Description

Display only.

Description of the token. Can be anything that describes the token, such as the type of token or date created.

Buttons

Help

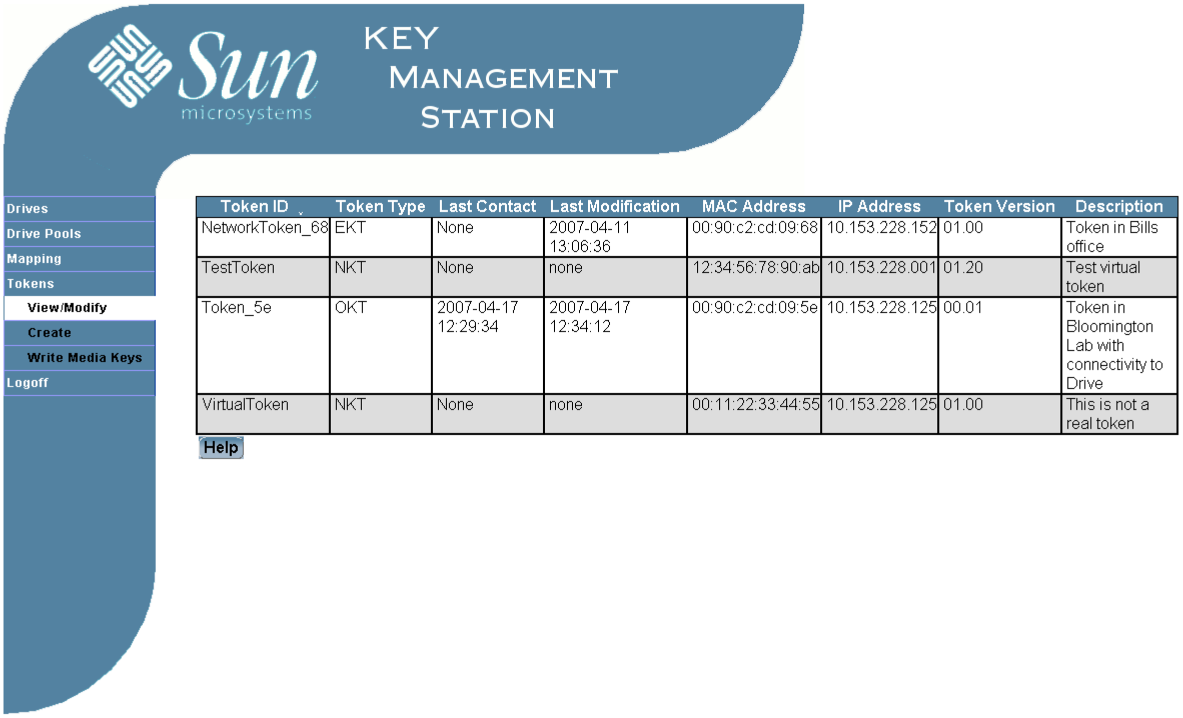
Click to display online help for the screen.

See Also

- Tokens > Create
- Tokens > View
- Tokens > Write Device Keys
- Tokens > Write Media Keys

Tokens > View

Sample Screen



Token ID	Token Type	Last Contact	Last Modification	MAC Address	IP Address	Token Version	Description
NetworkToken_68	EKT	None	2007-04-11 13:06:36	00:90:c2:cd:09:68	10.153.228.152	01.00	Token in Bills office
TestToken	NKT	None	none	12:34:56:78:90:ab	10.153.228.001	01.20	Test virtual token
Token_5e	OKT	2007-04-17 12:29:34	2007-04-17 12:34:12	00:90:c2:cd:09:5e	10.153.228.125	00.01	Token in Bloomington Lab with connectivity to Drive
VirtualToken	NKT	None	none	00:11:22:33:44:55	10.153.228.125	01.00	This is not a real token

Description

Allows you to display information for physical tokens.

Operator Role

Security Officer or User

Screen Fields

Note – Click any screen field to modify the token information. The Tokens > Modify screen appears.

Token ID

Display only.

ID of the token. Unique for each token.

Token Type

Display only.

Indicates the most recent function of the token. Options are:

- EKT—Enabling key token. Token was last used to transmit device keys to the tape drives.
- NKT—New key token. Token has been identified to the KMS software but has not yet been used to transmit keys, or has been reset and cleared of all keys.
- OKT—Operating key token. Token was last used to transmit media keys to the tape drives.

Last Contact

Display only.

Most recent date and time when the token was successfully contacted by the Key Management Station software. Shows that the token is on the network and accessible to the KMS software. Automatically updated by the KMS software every polling interval (default is every 15 seconds), if communications are successful.

Last Modification

Display only.

Date and time when the token was last modified. Automatically updated by the Key Management Station software whenever media or device keys are written to the token.

MAC Address

Display only.

MAC address of the physical token. Unique for each token. Printed on the token label.

IP Address

Display only.

Static IP address the KMS software uses to communicate with the token.

- For networked token operations, this is an IP address on the same subnet as the library drives.
- For air gap operations, this is an IP address on the same subnet as the Crypto Key Management Station.

Token Version

Display only.

Current version of the token firmware.

Description

Display only.

Description of the token. Can be anything that describes the token, such as the type of token or date created.

Buttons

Help

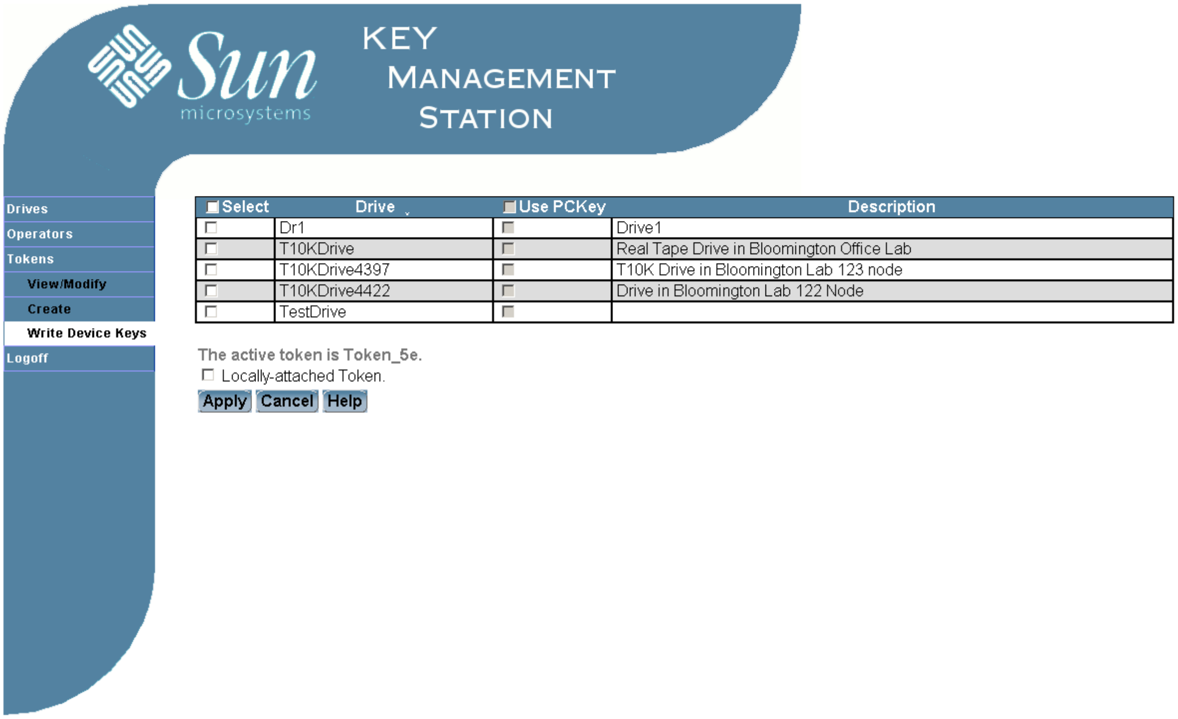
Click to display online help for the screen.

See Also

- Tokens > Create
- Tokens > Modify
- Tokens > Token Selection Screen
- Tokens > Write Device Keys
- Tokens > Write Media Keys

Tokens > Write Device Keys

Sample Screen



☐ Select	Drive	☐ Use PCKey	Description
☐	Dr1	☐	Drive1
☐	T10KDrive	☐	Real Tape Drive in Bloomington Office Lab
☐	T10KDrive4397	☐	T10K Drive in Bloomington Lab 123 node
☐	T10KDrive4422	☐	Drive in Bloomington Lab 122 Node
☐	TestDrive	☐	

The active token is Token_5e.

☐ Locally-attached Token.

Description

Note – This screen is accessed from the Tokens > Token Selection Screen.

Allows you to write device keys to an enabling key token (EKT).

You must specify the drives to which you want to transmit device keys. Additionally, you must indicate drives that have been reset or have not previously received device keys.

Note – Raw keys must be available in the KMS database. For each drive you specify, three raw keys are used to create a set of encrypted device keys on the physical token.

Before you perform this activity, you must verify the following:

- The KMS software is successfully communicating with the token. Use the **Tokens > View** GUI screen or the `view_token` CLI command and note the Last Contact field.
- The drives to which you want to transmit keys are on the same subnet as the token you have selected.

Networked Token Operations

You must NOT indicate that this is a locally attached token.

Once the keys have been written successfully to the token, the token automatically transmits the keys to the drives.

Air Gap Operations

You must indicate that this is a locally attached token. This notifies the KMS software that prior to sending the keys to the token, it must assign a temporary IP address to the token. It uses the IP address value assigned previously with the **Tokens > Create** GUI screen or `create_token` CLI command.

Once the keys have been written successfully to the token, the token does NOT automatically transmit the keys to the drives. In order for the drives to receive the keys, you must remove the token from the Crypto Key Management Station token bay and insert it in the drive token bay.

Operator Role

Security Officer

Screen Fields

Select

Optional.

Click to indicate that you want to write device keys for this drive to the token. You must select at least one drive to perform the write operation.

Click the check box by the column heading to select all items in the list; click again to de-select all items.

Drive

Display only.

Drive that has been designated for encryption capability.

Use PCKey

Indicates the drive is currently in a reset state (that is, the drive does not have device keys). This causes the device key package to be encrypted using the drive's PC key.

Note – Specify this option only if the drive has NOT been enabled for encryption previously, or if the drive is currently in a reset state.

Note – This selection is ignored if you have not selected the drive in the Select column.

Click the check box by the column heading to select all items in the list; click again to de-select all items.

Description

Display only.

Description of the drive. Can be anything that describes the drive, such as the physical location within the library.

Locally-attached Token

Optional.

Indicates that the token is inserted in a token bay that is connected directly to the Crypto Key Management Station.

Buttons

Apply

Click to begin writing the specified data to the token.

Cancel

Click to cancel the changes.

Help

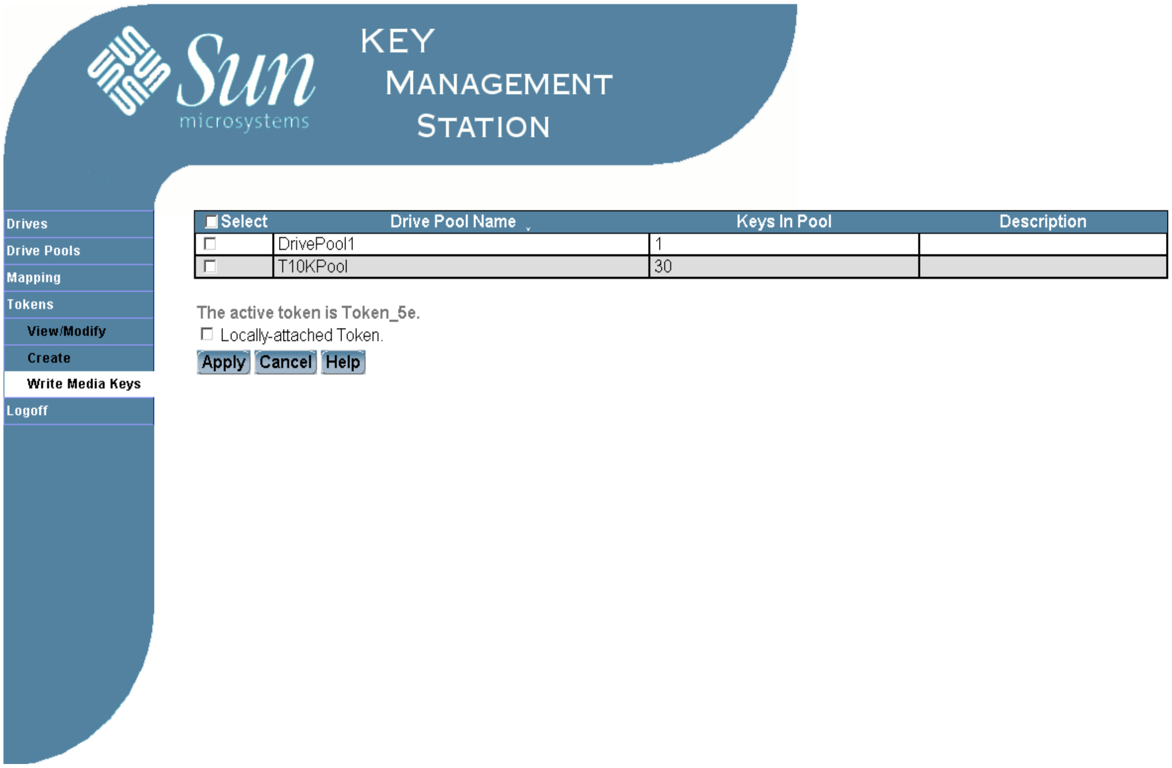
Click to display online help for the screen.

See Also

- Drives > Create
- Drives > View
- Tokens > Create
- Tokens > Token Selection Screen
- Tokens > View
- Tokens > Write Media Keys

Tokens > Write Media Keys

Sample Screen



□ Select	Drive Pool Name	Keys In Pool	Description
□	DrivePool1	1	
□	T10KPool	30	

The active token is Token_5e.

□ Locally-attached Token.

Description

Note – This screen is accessed from the Tokens > Token Selection Screen.

Allows you to write media keys to an operating key token (OKT).

You must specify the drive pools to which you want to transmit media keys.

Note – To be eligible for media keys, a drive pool must be assigned both a write key and at least one drive.

Before you perform this activity, you must verify the following:

- The KMS software is successfully communicating with the token. Use the **Tokens > View** GUI screen or the `view_token` CLI command and note the Last Contact field.
- The drives to which you want to transmit keys are on the same subnet as the token you have selected.

Networked Token Operations

You must NOT indicate that this is a locally attached token.

Once the keys have been written successfully to the token, the token automatically transmits the keys to the drives.

Air Gap Operations

You must indicate that this is a locally attached token. This notifies the KMS software that prior to sending the keys to the token, it must assign a temporary IP address to the token. It uses the IP address value assigned previously with the **Tokens > Create** GUI screen or `create_token` CLI command.

Once the keys have been written successfully to the token, the token does NOT automatically transmit the keys to the drives. In order for the drives to receive the keys, you must remove the token from the Crypto Key Management Station token bay and insert it in the drive token bay.

Operator Role

User

Screen Fields

Select

Optional.

Click to indicate that this drive pool is to have media keys written to the token. You must select at least one drive pool to perform the write operation.

Click the check box by the column heading to select all items in the list; click again to de-select all items.

Drive Pool Name

Display only.

Name of the drive pool. Unique for each pool.

Keys in Pool

Display only.

Total number of media keys assigned to the drive pool.

Description

Display only.

Description of the drive pool. Can be anything that describes the drive pool, such as the function or department.

Locally-attached Token

Optional.

Indicates that the token is inserted in a token bay that is connected directly to the Crypto Key Management Station.

Fill in the check box as follows:

- Select the check box if you are using air gap operations.
- Leave the check box blank if you are using networked token operations.

Buttons

Apply

Click to begin writing the specified data to the token.

Cancel

Click to cancel the changes.

Help

Click to display online help for the screen.

See Also

- Mapping > Modify
- Mapping > View
- Tokens > Create
- Tokens > Token Selection Screen
- Tokens > View

CHAPTER 6

KMS Command Line Interface Commands

Overview

The Key Management Station (KMS) command line interface (CLI) allows you to manage the Crypto Key Management Station from a terminal window.

Syntax Conventions

The following typographic conventions are used in describing CLI command syntax and examples.

TABLE 6-1 Typographic conventions for commands and examples

Typeface or Symbol	Meaning	Example
`AaBb123`	Name of command or option; on-screen user input or computer output; names of files and directories.	`create_keyset`
AaBb123	Italics indicate a variable placeholder, to be replaced with a real name or value.	`create_keyset` *key_set_name*
`[ ]`	Square brackets contain options that are not required.	`create_keyset [-d` *description*`]`
|	The pipe separates options, only one of which may be used at a time.	`view_key -a |` *key_ID1*
`...`	The ellipsis indicates that an option supports a list of values.	`view_key` *key_ID1*`[` *key_ID2* `...]`

Issuing Commands

Only one user at a time can use either the GUI or the CLI. If a user is already logged in to the GUI, you cannot issue commands through the CLI (including view commands).

CLI Functionality Not in the GUI

The following KMS CLI commands have no comparable KMS GUI screens. These functions can be carried out through the CLI only.

- backup_db
- export_media_key_disable
- export_media_key_enable
- history_token
- mkkeys
- reset_token
- restore_db
- run_backup_db
- run_restore_db
- search_tokens
- send_permanent_ip
- view_backup_key

CLI Commands

This section includes detailed descriptions of all KMS CLI commands, arranged in alphabetical order by command name. You can use any command for which you have sufficient authorization.

backup_db

Name

backup_db – Back up the KMS database.

Synopsis

`backup_db` *path_name*

Description

Allows you to perform a full backup of the KMS database. Two sets of backup files are written:

- Backup and digest files for KMS login ID data:

  `ultrakms-opr.`*host_name–time_stamp*`.dump`
  `ultrakms-opr.`*host_name–time_stamp*`.digest`

- Backup and digest files for KMS encryption key data:

  `ultrakms-keys.`*host_name–time_stamp*`.dump`
  `ultrakms-keys.`*host_name–time_stamp*`.digest`

where:

- *host_name* is the ID assigned to the Crypto Key Management Station workstation.
- *time_stamp* is the date and time when the backup is created.

Note – The digest files contain the key value used to encrypt the corresponding dump files. You need to provide this value when you restore the database.

You can specify the directory where you want the backup files to be written. The default is `/export/home/kms/mnt_backups`.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.

Options

path_name

Required.

Full path of the directory where you want the backups to be written. Typically, this is `/export/home/kms`.

Examples

Example 1:

```
kmsadmin@kms$ backup_db /export/home/kms
Performing full backup

#*********************************************************************
******
#* RECORD THIS DIGEST VALUE! IT IS REQUIRED TO RESTORE THE BACKUP.
*
#*                                                                    *
#* DUMP FILE: ultrakms-opr.kms-00000000-20061030162100341802.dump
*
#* DIGEST:   59886ed47b4cb5fd7a1f0baaa5f92128f30ca81a                 *
#*********************************************************************
******


#*********************************************************************
******
#* RECORD THIS DIGEST VALUE! IT IS REQUIRED TO RESTORE THE BACKUP.
*
#*                                                                    *
#* DUMP FILE: ultrakms-keys.kms-00000000-20061030162100341802.dump
*
#* DIGEST:   5f5e0d61bd6705455d692eee6d8601ff26f0b3af                 *
#*********************************************************************
******

kmsadmin@kms$
```

See Also

- restore_db
- run_restore_db

create_drive

Name

`create_drive` — Identify a drive you want to enable for encryption.

Synopsis

Import drive data from CD:

```
create_drive [-o operator] [-p password] -i [-d description] drive_name
```

Enter drive data manually:

```
create_drive [-o operator] [-p password] -s serial_number -k PC_key
[-d description] drive_name
```

Description

Allows you to identify a drive you want to enable for encryption. You can use either of the following methods:

- Import the drive data from a CD provided by Sun Microsystems, Inc. Each drive has its own CD. The drive's unique preset communication (PC) key and crypto serial number are provided on the CD.
- Enter the drive data manually. You need to obtain the drive's unique preset communication (PC) key and crypto serial number before performing this activity.

Operator Role

User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You must use either the `-s` and `-k` options together, or the `-i` option. All three options cannot be used together.

`-s` *serial_number*

Required, unless you use the `-i` option.

Crypto serial number assigned to this drive by Sun Microsystems, Inc. and stored in the drive's nonvolatile memory. Unique for each drive.

Note – This number does not need to be kept secure.

`-k` *PC_key*

Required, unless you use the `-i` option.

Preset communication (PC) key assigned to this drive by Sun Microsystems, Inc. Unique for each drive. This number is provided to your Sun support representative using one of the following methods:

- From a secure central database
- By secure e-mail
- By CD delivered with the Crypto Key Management Station

Note – This number must be kept secure.

---

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

`-i`

Required, unless you use the `-s` and `-k` options.

Imports the PC key and crypto serial number for the drive from the CD located at `/export/home/kms/mnt_cd`. You can obtain this CD from Sun Microsystems, Inc.

Note – Because this CD contains sensitive information, such as the PC key for the drive, it must be kept secure.

`[-d` *description*`]`

Optional.

Description of the drive. Can be anything that describes the drive, such as the physical location within the library.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), - (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes (`"`). For example, `" Detailed description of item "`.

---

drive_name

Required.

Name of the drive you want to enable for encryption. Unique for each drive.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1 (enter drive data manually):

```
kmsuser@kms$ create_drive -o Kmsuser -p !Password1! Drive10
-k 23ed68f253c1f9a1a6da657a7253cc82fcabb44efe59a234bc06230807b8d183
-s 00008a -d “Test Drive 10”
kmsuser@kms$
```

Example 2 (import drive data from CD):

```
kmsuser@kms$ create_drive -o Kmsuser -p !Password1! -i Drive12 -d “Test
Drive 12”
kmsuser@kms$
```

See Also

- modify_drive
- view_drive

create_drivepool

Name

`create_drivepool` — Create a drive pool and optionally assign drives to it.

Synopsis

```
create_drivepool [-o login_ID] [-p password]
[-a drive_name1[,drive_name2,...]] [-d description] drive_pool_name
```

Description

Allows you to create a drive pool. Optionally, you can assign encryption-enabled drives to it.

Note – If you choose not to assign drives to the drive pool at this time, you can do so later using the **Drive Pools > Modify** screen or the `modify_drivepool` CLI command.

Operator Role

User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`[-a` *drive_name1*`[,`*drive_name2*`,...]]`

Optional.

Name of a drive you want to add to the drive pool.

Note – Only drives that have been enabled for encryption can be added to a drive pool.

You can specify a list of items by separating them with commas. For example, `Item1,Item2,Item3`.

[-d *description*]

Optional.

Description of the drive pool. Can be anything that describes the drive pool, such as the function or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, . (period), - (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes ("). For example, `" Detailed description of item "`.

---

drive_pool_name

Required.

Name of the drive pool you want to create. Unique for each pool.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1 (create drive pool with no drives):

```
kmsuser@kms$  create_drivepool  -o Kmsuser -p !Password1! -d "Test Drive
Pool" DrivePool10
kmsuser@kms$
```

Example 2 (create drive pool with drives):

```
kmsuser@kms$  create_drivepool  -o Kmsuser -p !Password1! -d "Test Pool"
-a Drive0 DrivePool11
kmsuser@kms$
```

See Also

- modify_drivepool
- view_drivepool

create_key

Name

`create_key` — Create a media key and assign it to a key set.

Synopsis

Create from raw keys:

```
create_key [-o login_ID] [-p password] -s key_set_name -r
[-d description]
```

Create manually:

```
create_key [-o login_ID] [-p password] -s key_set_name -c crypto_key
[-d description] key_ID
```

Description

Allows you to add a media key to the KMS database. You can use either of the following methods:

- Create the key automatically from the raw keys in the KMS database. The key value is randomly selected from the raw keys, and the key ID is assigned automatically. Raw keys must be available in the KMS database.
- Add the key manually from an external source. You must obtain the key value and key ID and then enter them manually.

You must also assign the new media key to a key set. By default, media keys are created with an “active” status.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`-s` *key_set_name*

Required.

Name of the key set to which you want to assign the media key.

Note – Using this command, you must assign the key to only one key set. To assign the key to additional key sets or to remove the key from all key sets, you can use the **Key Sets** > **Modify** screen or the `modify_keyset` CLI command.

`[-d` *description*`]`

Optional.

Description of the media key. Can be anything that describes the key, such as the function, date, or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), `_` (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes (`"`). For example, `" Detailed description of item "`.

Note – You must use either the `-c` and *key_ID* options together, or the `-r` option alone. All three options cannot be used together.

`-r`

Required, if creating media keys automatically.

Click to create a new key from the raw keys in the KMS database. Raw keys must be available.

`-c` *crypto_key*

Required, if creating media keys manually.

Cryptographic media key value.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

key_ID

Required, if creating keys manually. Display only, if creating keys automatically.

Visible ID for the media key.

Note – The first four and the last ten bytes of the key ID are assigned by the KMS software and cannot be modified.

---

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

This value can be entered either of two ways:

- Supplied from the KMS database when you click **New Key**.
- Entered manually from another source.

If you are creating media keys automatically and there are no raw keys available, see your Crypto Key Management Station administrator for assistance.

Examples

Example 1 (create key automatically):

```
kmsuser@kms$ create_key -o KmsAdm -p !Password1! -d "New Key" -r
-s KeySet10

ID                            :
001e00030000000000000000000000070000000000000000000000000000000000
Value                         :
243473244b215fa03089d70fe4b1707193535ae91129a1f6778d60f688ad3a8b
Source                       : Generated by mkkeys Tue Oct 17 20:14:49
2006 GMT.

Description                   : New Key
kmsuser@kms$
```

Example 2 (create key manually):

```
kmsuser@kms$  create_key -o KmsAdm -p !Password1! -d "Example Key 1"
-s KeySet10 -c
243473244b215fa03089d70fe4b1707193535ae91129a1f6778d60f688ad3b2b
001e00030000000000000000000000090000000000000000000000000000000000

ID                            :
001e00030000000000000000000000090000000000000000000000000000000000
Value                         :
243473244b215fa03089d70fe4b1707193535ae91129a1f6778d60f688ad3b2b
Source                        : CLI
Description                   : Example Key 1

kmsuser@kms$
```

See Also

- modify_key
- view_key

create_keyset

Name

`create_keyset` — Create a key set.

Synopsis

`create_keyset [-o` *login_ID*`] [-p` *password*`] [-d` *description*`]` *key_set_name*

Description

Allows you to create key sets.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`[-d` *description*`]`

Optional.

Description of the key set. Can be anything that describes the key set, such as the function, date, or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), `_` (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes ("). For example, `" Detailed description of item "`.

key_set_name

Required.

Name of the key set you want to create.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1:

```
kmsuser@kms$ create_keyset  -o KmsAdm -p !Password1! -d "Example keyset"
KeySet10
kmsuser@kms$
```

See Also

- modify_keyset
- view_keyset

create_operator

Name

`create_operator` — Create a KMS login ID.

Synopsis

`create_operator [-o` *login_ID*`] [-p` *password*`] -c` *password* `-r` *role*
`[-d` *description*`]` *login_ID*

Description

Allows you to create a new KMS login ID. You must assign a password, operator role, and status (active or inactive) to each login ID.

Operator Role

Administrator, to create login IDs with the Administrator operator role

Administrator or Security Officer, to create login IDs with the Security Officer operator role

Security Officer, to create login IDs with the User operator role

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`-c` *password*

Required.

Password you want to assign to the login ID.

Note – You cannot reuse the previous three passwords that have been assigned to the login ID.

8–20 printable characters. The first eight characters must include at least ONE EACH of the following:

- Lowercase letter (a–z)
- Uppercase letter (A–Z)
- Number (0–9)
- Special character (`` ~!@#$%^&*()_+`-={}|[]\:";’<>?,./ ``)

`-r` *role*

Required.

Operator role you want to assign to the login ID. This determines the KMS GUI screens and CLI commands the login ID is authorized to access. Only one value can be assigned at a time. There is no default. Options are:

- `administrator`
- `security_officer`
- `user`

Note – You can assign only the operator roles for which you have sufficient authorization. If you are using the Administrator role, you can assign only the Administrator and Security Officer roles. If you are using the Security Officer role, you can assign only the Security Officer and User roles.

`[-d` *description*`]`

Optional.

Description of the login ID. Can be anything that describes the user, such as the name, department, or operator role.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), - (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes ("). For example, `" Detailed description of item "`.

---

login_ID

Required.

Login ID you want to create. Unique for each user.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1 (create Administrator login ID):

```
kmsuser@kms$ create_operator -o KmsAdm -p !Password1! -c !Password1!
-r administrator -d "Example Login ID" NewAdmin
kmsuser@kms$
```

Example 2 (create User login ID):

```
kmsuser@kms$  create_operator -o Kmssec -p !Password1!  -c !Password1!
-r user NewUser
kmsuser@kms$
```

See Also

- create_operator
- view_operator

create_token

Name

`create_token` — Identify a physical token to be used in transmitting keys.

Synopsis

```
create_token [-o login_ID] [-p password] -m MAC_address -v version
[-d description] -i IP_address token_ID
```

Description

Allows you to identify a physical token that you want to use for transmitting media or device keys.

Note – Before you perform this activity, the Crypto Key Management Station administrator must use the `send_permanent_ip` CLI command to assign permanent IP settings to the token. You must obtain from the administrator the following information for the token: 1) the unique MAC address, which is printed on the token label; 2) the IP address to be used by the KMS software to communicate with the token.

Operator Role

Security Officer or User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`-m` *MAC_address*

Required.

MAC address of the physical token. Unique for each token. Printed on the token label.

Twelve hexadecimal digits, separated into six groups of two digits each. For example, `00.90.C2.67.89.ab`. Each group must have two printable hex digits, with leading zeroes as needed. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

`-v` *version*

Required.

Current version of the token firmware.

Four digits, in the format *nn.nn*. For example, 01.20.

`[-d` *description*`]`

Optional.

Description of the token. Can be anything that describes the token, such as the type of token or date created.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), - (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes ("). For example, `" Detailed description of item "`.

`-i` *IP_address*

Required.

Static IP address the KMS software uses to communicate with the token.

- For networked token operations, this is an IP address on the same subnet as the library drives.
- For air gap operations, this is an IP address on the same subnet as the Crypto Key Management Station.

The default IP address for a new token is 10.0.0.2.

32-bit numeric address, in dotted decimal notation, *nnn.nnn.nnn.nnn*. Valid values for *nnn* are 0 to 255. For example, `123.119.01.73`.

token_ID

Required.

ID of the physical token you want to use for transmitting media or device keys. Must be unique for each token.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1:

```
kmsuser@kms$ create_token  -o Kmssec -p !Password1! -m 00:90:c2:11:18:23
-v 01.20 -i 10.0.0.99 -d "Example token" Token10
kmsuser@kms$
```

See Also

- modify_token
- send_permanent_ip
- view_token

export_media_key

Name

`export_media_key` — Export specified media keys to an ASCII text file.

Synopsis

```
export_media_key [-o login_ID] [-p password] -f file_name
[key_ID1[ key_ID2 ...]]
```

Description

Note – With KMS 1.2, this command replaces the `export_key` command.

Note – This activity is not available if the Crypto Key Management Station administrator has disabled it with the `export_media_key_disable` CLI command. To re-enable this activity, the administrator must use the `export_media_key_enable` command.

Allows you to export selected media keys to a designated file. The data is written in ASCII text format and includes the file checksum value, media key IDs, key values, and key descriptions.

You might use this activity to transfer media keys from one Crypto Key Management Station to another, or to safely offload keys from the KMS database before performing a software upgrade.

This activity does not export the database backup encryption key. To view this key, the Crypto Key Management Station administrator can use the `view_backup_key` CLI command.

Note – The export file is a useful record of the encryption key data used at your site. Because this data is very sensitive, you should ensure that the file and any hardcopy printouts of it are kept in a secure location. For added security, you can encrypt the file using standard Solaris tools. See the `encrypt` man page for details.

Note – An export file created using KMS version 1.2 or later is not compatible with prior releases of the KMS software.

Operator Role

Administrator

Options

[-o *login_ID*]

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

[-p *password*]

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

-f *file_name*

Required.

Name of the file to which you want to export the data. The file is created in the `/export/home/kms/mnt_keys` directory. You must specify a new file name; if the file already exists, it will NOT be overwritten.

[*key_ID1* [*key_ID2* ...]]

Optional.

Key IDs of the media keys you want to export. You can specify only media keys that have been assigned to a key set.

Note – If you do not specify this option, all media keys are exported.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

Examples

Example 1 (export all media keys):

```
kmsuser@kms$  export_media_key -o KmsAdm -p !Password1! -f AllKeyExample
kmsuser@kms$
```

Example of file:

```
# media key file a9d937abf8aae0ca306f3c69a986b5d48bad96af
001e000300000000000000000000000100000000000000000000000000000000,8f6bb
05ab9d7ed754c444c1298a9b298182f96d63af7fa89a4e477b15497d8ed,
001e000312345678123456781234567812345102401200000000000000000000,12345
67812345678123456781234567812345678123456781234567812341024,key number
for testing large number of keys created
001e000312345678123456781234567812345102501200000000000000000000,12345
67812345678123456781234567812345678123456781234567812341025,key number
for testing large number of keys created
```

Example 2 (export specified media keys):

```
kmsuser@kms$ export_key -o KmsAdm -p !Password1! -f SelectKeyExample
001e000343215678432156784321567843215105201200000000000000000000
001e000343215678432156784321567843215105301200000000000000000000
kmsuser@kms$
```

Example of file:

```
# media key file 148713cc655bf653d0f6801f6bb125f94077b55e
001e000343215678432156784321567843215105201200000000000000000000,43215
67843215678432156784321567843215678432156784321567843211081,key number
for testing large number of keys created
001e000343215678432156784321567843215105301200000000000000000000,43215
67843215678432156784321567843215678432156784321567843211082,key number
for testing large number of keys created
```

See Also

- export_media_key_disable
- export_media_key_enable
- import_media_key
- view_key

export_media_key_disable

Name

`export_media_key_disable` — Disable the media key export activity in both the GUI and the CLI.

Synopsis

`export_media_key_disaable [-o` *login_ID*`] [-p` *password*`]`

Description

Allows you to disable the media key export activity. The **Keys > Media Key Export** GUI screen and the `export_media_key` CLI command are both disabled.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Examples

Example 1:

```
kmsuser@kms$ export_media_key_disable -o KmsAdm -p !Password1!
kmsuser@kms$
kmsuser@kms$ export_media_key -o KmsAdm -p !Password1! -f ExportFile
export_media_key failed - key export disabled
kmsuser@kms$
```

See Also

- export_media_key_enable
- import_media_key

export_media_key_enable

Name

`export_media_key_enable` — Enable the media key export activity in both the GUI and the CLI.

Synopsis

`export_media_key_enable [-o` *login_ID*`] [-p` *password*`]`

Description

Allows you to enable the media key export activity. The **Keys > Media Key Export** GUI screen and the `export_media_key` CLI command are both enabled.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Examples

Example 1:

```
kmsuser@kms$ export_media_key_enable -o KmsAdm -p !Password1!
kmsuser@kms$
```

See Also

- import_media_key

- export_media_key_disable

history_token

Name

`history_token` — Display history for a physical token.

Synopsis

`history_token [-o` *login_ID*`] [-p` *password*`]` *token_ID*

Description

Allows you to display the history of when data was written to a physical token.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

Security Officer or User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

token_ID

Required.

ID of the token. Unique for each token.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1:

```
kmsuser@kms$ history_token -o Kmsuser -p !Password1! Token_2
2006-10-17 15:08:44.083348 Drive_Pool_1                   O
2006-10-18 15:28:18.847799 Drive_Pool_1                   O
2006-10-18 15:59:10.038955 Drive_Pool_1                   O
2006-10-18 16:14:00.478769 Drive_Pool_1                   O
kmsuser@kms$
```

See Also

- create_token
- view_token
- modify_token
- reset_token
- write_token

import_media_key

Name

`import_media_key` — Allows you to import media keys from a previously created export file.

Synopsis

`import_media_key [-o` *login_ID*`] [-p` *password*`]` *file_name*

Description

Allows you to import media keys to the Key Management Station database. The keys must have been previously written to an ASCII text export file using the **Keys > Media Key Export** GUI screen or the `export_media_key` CLI command. The export file must have been created using KMS version 1.2 or later.

You might use this activity to transfer media keys from one Crypto Key Management Station to another, or to restore keys to the KMS database after a software upgrade.

Note – Before performing this activity, you must obtain the name of the export file containing the media keys. The file must be located in the `/export/home/kms/mnt_keys` directory. If the export file has been modified in any way, the keys cannot be imported into the KMS database.

Note – Only new media keys are imported. If you have already imported media keys, any duplicates are rejected.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

file_name

Required.

Name of the file containing the media keys you want to import. The file must be located in the /export/home/kms/mnt_keys directory.

Examples

Example 1 (successful import of all keys):

```
kmsuser@kms$ import_media_key -o KmsAdm -p !Password1! SelectKeyFile
PF9 keys imported.
kmsuser@kms$
```

Example 2 (duplicate keys rejected):

```
kmsuser@kms$ import_media_key -o KmsAdm -p !Password1! AllKeyFile
42 keys imported, 2 keys rejected as duplicates.
kmsuser@kms$
```

See Also

- export_media_key
- import_raw_key

import_raw_key

Name

import_raw_key—Import raw keys to the KMS database.

Synopsis

`import_raw_key [-o` *login_ID*`] [-p` *password*`]` *path_name*

Description

Allows you to import raw keys to the KMS database. The raw keys are usually generated, using the `mkkeys` script, from the Sun Crypto Accelerator 6000 (SCA6000) card included in the Crypto Key Management Station. They can also be imported from an outside source.

After the raw keys have been successfully imported, the files created by the `mkkey` script (`rawdata.dat`, `checksums.txt`, `ident.txt`, `info.txt`, and `length.txt`) are automatically deleted.

Note – Before performing this activity, you must obtain the full path of the directory containing the raw keys.

Note – Only new raw keys are imported. If you have already imported raw keys, any duplicates are rejected.

Note – Prior to KMS v1.2, this activity was performed with the **Keys > Import** GUI screen or the `import_kmedia` CLI command.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the KMS_PASSWORD environment variable is used, if it has been defined.

path_name

Required.

Full path of the directory containing the raw keys you want to import. If you are importing from the Sun Crypto Accelerator 6000 (SCA6000) card included in the Crypto Key Management Station, this directory is typically named /export/home/kms/mnt_cd.

Examples

Example 1 (successful key import):

```
kmsuser@kms$ import_raw_key -o KmsAdm -p !Password1!
/export/home/kms/mnt_cd
Raw keys import complete - 1024 keys imported.
kmsuser@kms$
```

Example 2 (unsuccessful key import—raw keys not found):

```
kmsuser@kms$ import_raw_key -o KmsAdm -p !Password1!
/export/home/kms/mnt_cd
import_raw_key - [Errno 2] No such file or directory:
'/export/home/kms/mnt_cd/checksums.txt'
kmsuser@kms$
```

See Also

- create_key
- mkkeys

mkkeys

Name

`mkkeys` — Generate raw keys.

Synopsis

`mkkeys -k` *count* `[-i` *text*`]`

Description

Allows you to generate raw keys to be imported later into the KMS database. The raw keys are usually generated from the Sun Crypto Accelerator 6000 (SCA6000) card included in the Crypto Key Management Station. They can also be imported from an outside source.

This script creates the following files in the `/export/home/kms/mnt_cd` directory:

- rawdata.dat—Contains the raw key values.
- checksums.txt—Contains checksums for the remaining files.
- ident.txt—Contains either user-entered comments or a system-generated timestamp, depending on whether the `-i` option was used at the time the mkkeys script was run.
- info.txt—Optional file. Can be edited by the user to contain any textual information.
- length.txt—Specifies the length of the rawdata.dat file, in bytes.

Note – This script fails if raw keys already exist. You must import the raw keys into the KMS database before proceeding.

Note – This script fails if a CD is mounted on `/export/home/kms/mnt_cd`. You must unmount the CD before proceeding.

After using this script, you can use the `import_raw_key` CLI command to import the raw keys into the KMS database.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.

Options

-k *key_count*

Required.

Specifies the number of keys to create, in 1024-key increments. Valid entries are `1-8`, where `1` = 1024, `2` = 2048, etc.

`[-i` *text*`]`

Optional.

Specifies a text string to be written to the `ident.txt` file in the `/export/home/kms/mnt_cd` directory.

If you do not specify this option, the `ident.txt` file contains a message indicating the date and time when the raw keys are generated and the process used to create them (in this case, the `mkkeys` script).

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes ("). For example, `" Detailed description of item "`.

Examples

Example 1 (successful key generation):

```
kmsadmin@kms$ mkkeys -k 1
kmsadmin@kms$
```

Example 2 (unsuccessful—existing raw keys have not yet been imported into the KMS database):

```
kmsadmin@kms$ mkkeys -k 1
mkkeys: File 'rawdata.dat' exists; remove files from directory
/export/home/kms/mnt_cd before generating new keys.
kmsadmin@kms$
```

See Also

- import_raw_key

modify_drive

Name

`modify_drive` — Modify the description of a drive.

Synopsis

`modify_drive [-o` *login_ID*`] [-p` *password*`] [-d` *new_description*`]` *drive_name*

Description

Allows you to modify the description of a drive.

Operator Role

User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`[-d` *new_description*`]`

Optional.

Description of the drive. Can be anything that describes the drive, such as the physical location within the library.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes ("). For example, `" Detailed description of item "`.

drive_name

Required.

Drive that has been designated for encryption capability.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1:

```
kmsuser@kms$ modify_drive -o Kmsuser -p !Password1! Drive0
-d NewDescription
kmsuser@kms$
```

See Also

- create_drive
- view_drive

modify_drivepool

Name

`modify_drivepool` — Modify drive pool description and add or remove drives from the pool.

Synopsis

```
modify_drivepool [-o login_ID] [-p password]
[-a drive_name1[,drive_name2,...]] [-r drive_name1[,drive_name2,...]]
[-d new_description] drive_pool_name
```

Description

Allows you to modify the description of a drive pool and to add or remove drives from the pool.

Operator Role

User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`[-a` *drive_name1*`[,`*drive_name2*`,...]]`

Optional.

Name of a drive you want to add to the drive pool.

Note – Only drives that have been enabled for encryption can be added to a drive pool.

You can specify a list of items by separating them with commas. For example, `Item1,Item2,Item3`.

`[-r` *drive_name1*`[,`*drive_name2*`,...]`

Optional.

Name of a drive you want to remove from the drive pool.

You can specify a list of items by separating them with commas. For example, `Item1,Item2,Item3`.

`[-d` *new_description*`]`

Optional.

Description of the drive pool. Can be anything that describes the drive pool, such as the function or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes ("). For example, `" Detailed description of item "`.

drive_pool_name

Required.

Name of the drive pool. Unique for each pool.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1 (remove drives from pool and change its description):

```
kmsuser@kms$ modify_drivepool -o Kmsuser -p !Password1!
-d "Test Pool 11" -r Drive0 DrivePool11
Removing Drive0
kmsuser@kms$
```

Example 2 (add drives to pool):

```
kmsuser@kms$ modify_drivepool -o Kmsuser -p !Password1! DrivePool11
-a Drive0
Adding Drive0
kmsuser@kms$
```

See Also

- create_drivepool
- view_drivepool

modify_key

Name

`modify_key` — Modify the description and status of a media key.

Synopsis

`modify_key [-o` *login_ID*`] [-p` *password*`] [-A | -I] [-d` *new_description*`]` *key_ID*

Description

Allows you to modify the description and status of a media key.

Note – You cannot modify a key if it has been assigned to a key set.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You can can specify either `-A` or `-I`, but not both.

`[-A]`

Optional.

Indicates that you want to activate the key.

`[-I]`

Optional.

Indicates that you want to de-activate the key.

`[-d` *new_description*`]`

Optional.

Description of the media key. Can be anything that describes the key, such as the function, date, or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes (`"`). For example, `" Detailed description of item "`.

---

key_ID

Required.

Visible ID for the media key.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

Examples

Example 1 (activate a media key):

```
kmsuser@kms$ modify_key -o KmsAdm -p !Password1! -A
001e000300000000000000000000000900000000000000000000000000000000
kmsuser@kms$
```

Example 2 (de-activate a media key):

```
kmsuser@kms$  modify_key -o KmsAdm -p !Password1! -d "Key Example 9" -I
001e000300000000000000000000000900000000000000000000000000000000
kmsuser@kms$
```

See Also

- create_key
- view_key

modify_keyset

Name

`modify_keyset` — Modify a key set description and add or remove media keys from the key set.

Synopsis

`modify_keyset [-o` *login_ID*`] [-p` *password*`] [-a` *key_ID1*`[,`*key_ID2*`,...]] [-r` *key_ID1*`[,`*key_ID2*`,...]] [-d` *new_description*`]` *key_set_name*

Description

Allows you to modify the description of a key set and to designate the media keys that are assigned to it.

Note – You CANNOT modify a key set that has been mapped to a drive pool.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`-a` *key_ID1*`[,`*key_ID2*`,...]`

Optional.

Key ID of a media key you want to add to the key set.

Note – Only active media keys can be added to a key set.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

You can specify a list of items by separating them with commas. For example, `Item1,Item2,Item3`.

`-r` *key_ID1*`[,`*key_ID2*`,...]`

Optional.

Key ID of a media key you want to remove from the key set.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

You can specify a list of items by separating them with commas. For example, `Item1,Item2,Item3`.

`[-d` *new_description*`]`

Optional.

Description of the key set. Can be anything that describes the key set, such as the function, date, or department.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), - (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes ("). For example, `" Detailed description of item "`.

---

key_set_name

Required.

Name of the key set.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1 (modify key set description and remove a key):

```
kmsuser@kms$ modify_keyset  -o KmsAdm -p !Password1! -d "Example Keyset
10" -r
001e000300000000000000000000000900000000000000000000000000000000
KeySet10
Removing
001e000300000000000000000000000900000000000000000000000000000000
kmsuser@kms$
```

Example 2 (add keys to a key set):

```
kmsuser@kms$  modify_keyset  -o KmsAdm -p !Password1! KeySet10 -a
001e000300000000000000000000000900000000000000000000000000000000,001e0
00300000000000000000000000700000000000000000000000000000000
Adding
001e000300000000000000000000000900000000000000000000000000000000
Adding
001e000300000000000000000000000700000000000000000000000000000000
kmsuser@kms$
```

See Also

- create_keyset
- view_keyset

modify_mapping

Name

`modify_mapping` — Modify the key set mappings for a drive pool.

Synopsis

```
modify_mapping [-o login_ID] [-p password] [-a key_set1[,key_set2,...]]
[-r key_set1[,key_set2,...]] [-w key_ID] drive_pool_name
```

Description

Allows you to assign key sets to a selected drive pool. A drive pool can have any number of key sets.

Also allows you to designate the write key for the drive pool. A drive pool can have only one write key at a time. The write key must be assigned if key sets are assigned to the drive pool.

Note – Empty key sets (those with no assigned keys) cannot be mapped to a drive pool.

Note – The total number of keys in all key sets mapped to a single drive pool cannot exceed 32.

Operator Role

User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`[-a` *key_set1*`[,`*key_set2*`,...]]`

Name of a key set you want to assign to the drive pool.

Note – Only key sets with media keys can be assigned to a drive pool.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with commas. For example, `Item1,Item2,Item3`.

`[-r` *key_set1*`[,`*key_set2*`,...]]`

Name of a key set you want to remove from the drive pool.

You can specify a list of items by separating them with commas. For example, `Item1,Item2,Item3`.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

`[-w` *key_ID*`]`

Write key for the drive pool. You can specify any key from all the key sets assigned to the drive pool.

You must designate a write key if at least one key set is assigned to the drive pool. You do not need to designate a write key if no key sets are assigned to the drive pool.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

Examples

Example 1 (add key sets to a drive pool):

```
kmsuser@kms$ modify_mapping -o Kmsuser -p !Password1! DrivePool10 -a
KeySet10,KeySet20 -w
001e0003000000000000000000000000900000000000000000000000000000000
kmsuser@kms$
```

Example 2 (remove a key set from a drive pool):

```
kmsuser@kms$  modify_mapping -o Kmsuser -p !Password1! DrivePool10 -r
KeySet20
kmsuser@kms$
```

See Also

- view_mapping

modify_operator

Name

`modify_operator` — Modify a login ID.

Synopsis

```
modify_operator [-o login_ID] [-p password] [-c change_password]
[-a | -i] [-r role] [-d new_description] login_ID
```

Description

Allows you to modify the description, password, operator role, or status of an existing login ID.

Note – You cannot change the operator role or status of the `KmsAdm` login ID, which is the default Crypto Key Management Station administrator supplied with the product.

Operator Role

Administrator, to modify login IDs with the Administrator operator role

Administrator or Security Officer, to modify login IDs with the Security Officer operator role

Security Officer, to modify login IDs with the User operator role

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`[-c` *new_password*`]`

Optional.

Password you want to assign to the login ID.

Note – You cannot reuse the previous three passwords that have been assigned to the login ID.

8–20 printable characters. The first eight characters must include at least ONE EACH of the following:

- Lowercase letter (a–z)
- Uppercase letter (A–Z)
- Number (0–9)
- Special character (`~!@#$%^&*()_+‘-={}|[]\:";’<>?,./`)

Note – You can specify either `-a` or `-i`, but not both.

`[-a | -i]`

Optional.

Status you want to assign to the login ID. This determines whether the login ID is valid for logging in to the Key Management Station. Only one value can be assigned at a time.

- -a – Login ID is valid for use; this is the default.
- -i – Login ID is not valid for use.

`-r` *role*

Optional.

Operator role you want to assign to the login ID. This determines the KMS GUI screens and CLI commands the login ID is authorized to access. Only one value can be assigned at a time. There is no default. Options are:

- `administrator`
- `security_officer`
- `user`

Note – You can assign only the operator roles for which you have sufficient authorization. If you are using the Administrator role, you can assign only the Administrator and Security Officer roles. If you are using the Security Officer role, you can assign only the Security Officer and User roles.

`[-d` *new_description*`]`

Optional.

Description of the login ID. Can be anything that describes the user, such as the name, department, or operator role.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), - (dash), _ (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes (`"`). For example, `" Detailed description of item "`.

login_ID

Required.

Login ID assigned to the user. Unique for each user.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1 (change a login ID’s role and description):

```
kmsuser@kms$ modify_operator -o KmsAdm -p !Password1! NewAdmin -r
security_officer -d “New Security Officer ID”
kmsuser@kms$
```

Example 2 (change a login ID’s password):

```
kmsuser@kms$  modify_operator -o KmsAdm -p !Password1! NewAdmin -c
{Access2}
kmsuser@kms$
```

Example 3 (make a login ID inactive):

```
kmsuser@kms$ modify_operator -o KmsAdm -p !Password1! NewAdmin -i
kmsuser@kms$
```

Example 4 (make a login ID active):

```
kmsuser@kms$ modify_operator -o KmsAdm -p !Password1! NewAdmin -a
kmsuser@kms$
```

See Also

- create_operator
- view_operator

modify_token

Name

`modify_token` — Modify information for a physical token.

Synopsis

modify_token [-o *login_ID*] [-p *password*] [-m *MAC_address*] [-v *version*] [-d *new_description*] [-i *IP_address*] *token_name*

Description

Allows you to modify information for a physical token.

Operator Role

Security Officer or User

Options

[-o *login_ID*]

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

[-p *password*]

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

[-m *MAC_address*]

Optional.

MAC address of the physical token. Unique for each token. Printed on the token label.

Twelve hexadecimal digits, separated into six groups of two digits each. For example, `00.90.C2.67.89.ab`. Each group must have two printable hex digits, with leading zeroes as needed. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

[-v *version*]

Optional.

Current version of the token firmware.

Four digits, in the format *nn*.*nn*. For example, 01.20.

`[-d` *description*`]`

Optional.

Description of the token. Can be anything that describes the token, such as the type of token or date created.

0–256 characters. Valid characters are a to z, A to Z, 0 to 9, `.` (period), `-` (dash), `_` (underscore), and spaces.

Note – Entries with spaces must be enclosed in double-quotes (`"`). For example, `" Detailed description of item "`.

`[-i` *IP_address*`]`

Optional.

Static IP address the KMS software uses to communicate with the token.

- For networked token operations, this is an IP address on the same subnet as the library drives.
- For air gap operations, this is an IP address on the same subnet as the Crypto Key Management Station.

32-bit numeric address, in dotted decimal notation, *nnn*`.`*nnn*`.`*nnn*`.`*nnn*. Valid values for *nnn* are 0 to 255. For example, `123.119.01.73`.

token_ID

Required.

ID of the token. Unique for each token.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1 (change a token's version and description):

```
kmsuser@kms$ modify_token  -o Kmsuser -p !Password1! Token10 -d "Token
example 10" -v 01.20
kmsuser@kms$
```

Example 2 (change a token's MAC address):

```
kmsuser@kms$ modify_token  -o Kmsuser -p !Password1! Token10
-m 00:90:c2:11:18:23
kmsuser@kms$
```

Example 3 (change a token's IP address):

```
kmsuser@kms$ modify_token  -o Kmsuser -p !Password1! Token10
-i 10.0.0.98
kmsuser@kms$
```

See Also

- create_token

- view_token

reset_token

Name

`reset_token` — Reset a physical token.

Synopsis

`reset_token [-o` *login_ID*`] [-p` *password*`]` *token_id*

Description

Allows you to reset a physical token, causing it to re-initialize.

Note – This command performs the same function as pushing the Reset button on the physical token.

Note – Before you perform this activity, you must verify that The KMS software is successfully communicating with the token. Use the **Tokens > View** GUI screen or the `view_token` CLI command and check the Last Contact field.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

User or Security Officer

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

token_id

Required.

ID of the token. Unique for each token.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

Examples

Example 1:

```
kmsuser@kms$ reset_token -o Kmssec -p !Password1! Token_5e
Token 'Token_5e' reset complete - status OK
kmsuser@kms$
```

See Also

- write_token

restore_db

Name

`restore_db` — Restore the KMS database from backup.

Synopsis

`restore_db -k` *backup_encryption_key* `-c` *checksum* *dump_file*

Description

Allows you to restore the KMS database from KMS backup files and their associated digest files.

Encrypted backup files are created automatically during normal KMS operations or by the KMS `backup_db` script. There are two sets of backup files:

- Backup and digest files for KMS login ID data:

  `ultrakms-opr.`*host_name–time_stamp*`.dump`
  `ultrakms-opr.`*host_name–time_stamp*`.digest`

- Backup and digest files for KMS encryption key data:

  `ultrakms-keys.`*host_name–time_stamp*`.dump`
  `ultrakms-keys.`*host_name–time_stamp*`.digest`

where:

- *host_name* is the ID assigned to the Crypto Key Management Station workstation.
- *time_stamp* is the date and time when the backup is created.

Note – To perform a complete restoration of the KMS database, you must restore both the `ultrakms-opr` and the `ultrakms-keys` backup files.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.

Options

`-k` *backup_encryption_key*

Required.

Encryption key value used to encrypt the database backup files. This entry must match the key value for the encrypted backup files specified in the *dump_file* option. To display the current backup encryption key, use the `view_backup_key` CLI command.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

`-c` *checksum*

Required.

File checksum provided by the `backup_db` script. *checksum* is a 40-character hexadecimal string representing the SHA1 digest value for the dump file. The digest is generated and displayed when the dump is performed. Its value was also stored in the `.digest` file associated with the dump.

dump_file

Required.

Full path of the dump file from which you want to perform the restore. Options are:

- `ultrakms-opr.`*host_name–time_stamp*`.dump` – Dump file for the operator database
- `ultrakms-keys.`*host_name–time_stamp*`.dump` – Dump file for the encryption keys database

where:

- *host_name* is the ID assigned to the Crypto Key Management Station workstation.
- *time_stamp* is the date and time when the backup is created.

Examples

Example 1:

```
kmsadmin@kms$ restore_db -k
0000000000000000000000000000000000000000000000000000000000000000 -c
622e2f2c303d37ba85db9045d0b93943f2782265 ultrakms-keys.KmsHost-
00000000-2007_05_03,17_58_11_56,UTC.dump
done!

kmsadmin@kms$
```

See Also

- backup_db

run_backup_db

Name

`run_backup_db` — Create a full backup of the KMS database.

Synopsis

`run_backup_db [-d` *data_directory*`]`

Description

Allows you to perform a full backup of the KMS database. Two sets of backup files are written:

- Backup and digest files for KMS login ID data:

  `ultrakms-opr.`*host_name–time_stamp*`.dump`
  `ultrakms-opr.`*host_name–time_stamp*`.digest`

- Backup and digest files for KMS encryption key data:

  `ultrakms-keys.`*host_name–time_stamp*`.dump`
  `ultrakms-keys.`*host_name–time_stamp*`.digest`

where:

- *host_name* is the ID assigned to the Crypto Key Management Station workstation.
- *time_stamp* is the date and time when the backup is created.

Note – The digest files contain the key value used to encrypt the corresponding dump files. You need to provide this value when you restore the database.

You can specify the directory where you want the backup files to be written. The default is `/export/home/kms/mnt_backups`.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.

Options

`[-d` *data_directory*`]`

Optional.

Full path of the directory where you want the backup files written.

If you do no specify this option, the default path is used:
`/export/home/kms/mnt_backups`

Examples

Example 1:

```
kmsadmin@kms$ run_backup_db
Backing up databases to /export/home/kms/mnt_backups
Performing full backup

#************************************************************************
******
#* RECORD THIS DIGEST VALUE! IT IS REQUIRED TO RESTORE THE BACKUP.
*
#*                                                                      *
#* DUMP FILE: ultrakms-opr.kms-00000000-20061030180745714128.dump
*
#* DIGEST:    afb246d7cc1f5e09e362e54d05b672f906af591d                 *
#************************************************************************
******


#************************************************************************
******
#* RECORD THIS DIGEST VALUE! IT IS REQUIRED TO RESTORE THE BACKUP.
*
#*                                                                      *
#* DUMP FILE: ultrakms-keys.kms-00000000-20061030180745714128.dump
*
#* DIGEST:    f607225a13fd5dd529df5c2e04f4954f71deec33                 *
#************************************************************************
******

kmsadmin@kms$
```

See Also

- run_restore_db
- backup_db
- restore_db

run_restore_db

Name

`run_restore_db` — Restore the KMS database.

Synopsis

```
run_restore_db [-f] [-d data_directory] [-k backup_encryption_key]
dump_ID | latest | list
```

Description

Allows you to restore the KMS database from KMS backup files and their associated digest files.

Encrypted backup files are created automatically during normal KMS operations or by the KMS `backup_db` script. There are two sets of backup files:

- Backup and digest files for KMS login ID data:

  `ultrakms-opr.`*host_name–time_stamp*`.dump`
  `ultrakms-opr.`*host_name–time_stamp*`.digest`

- Backup and digest files for KMS encryption key data:

  `ultrakms-keys.`*host_name–time_stamp*`.dump`
  `ultrakms-keys.`*host_name–time_stamp*`.digest`

where:

- *host_name* is the ID assigned to the Crypto Key Management Station workstation.
- *time_stamp* is the date and time when the backup is created.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.

Options

`[-d` *data_directory*`]`

Optional.

Full path of the directory where the backup files are located.

If you do not specify this option, the default is used:
`/export/home/kms/mnt_backups`

`[-f]`

Optional.

Suppresses the confirmation prompt.

`[-k` *backup_encryption_key*`]`

Optional.

Key value used to encrypt the database backup files. This entry must match the key value for the encrypted backup files specified by the `-d` option. To display the current backup encryption key, use the `view_backup_key` CLI command.

If you do not specify this option, the value defined for the `KMS_BACKUPKEY` environment variable is used.

dump_ID `| latest | list`

Required.

Backup file set to use. Options are:

- *dump_ID* – The set to be used. It is part of the backup and digest file names and has the form *host_name–KMS_ID–date_time*.
- `latest` – Uses the most recent set found in the data directory.
- `list` – Displays the dump IDs for backup files found in the data directory. The dump IDs are listed in oldest to most-recent order.

Examples

Example 1 (display all backup dump IDs in a specified directory):

```
kmsadmin@kms$ run_restore_db -k
0000000000000000000000000000000000000000000000000000000000000000 -d
/tmp list
KmsHost-00000000-2007_05_03,17_58_11_56,UTC: 936 blocks
KmstHost-00000000-2007_05_04,13_48_58_38,UTC: 936 blocks
kmsadmin@kms$
```

Example 2 (restore from the most recent backup set in a specified directory):

```
kmsadmin@kms$ run_restore_db -k
0000000000000000000000000000000000000000000000000000000000000000 -d
/tmp latest
KMS database backup files with dumpid KmsHost-00000001-
2007_05_02,17_40_24_05,UTC found in /tmp.
Press 'Return' to proceed with restore, 'Control-C' to cancel.

Restoring 'keys' database from /tmp/ultrakms-keys.KmsHost-00000001-
2007_05_02,17_40_24_05,UTC.dump
done!
Restoring 'opr' database from /tmp/ultrakms-opr.KmsHost-00000001-
2007_05_02,17_40_24_05,UTC.dump
done!
kmsadmin@kms$
```

Example 3 (restore from a specified backup set in the default directory):

```
kmsadmin@kms$ run_restore_db -k
0000000000000000000000000000000000000000000000000000000000000000
KmsHost-00000001-2007_05_02,17_40_24_05,UTC
KMS database backup files with dumpid KmsHost-00000001-
2007_05_02,17_40_24_05,UTC found in /export/home/kms/mnt_backups.
```

```
Press 'Return' to proceed with restore, 'Control-C' to cancel.

Restoring 'keys' database from /export/home/kms/mnt_backups/ultrakms-
keys.KmsHost-00000001-2007_05_02,17_40_24_05,UTC.dump
done!
Restoring 'opr' database from /export/home/kms/mnt_backups/ultrakms-
opr.KmsHost-00000001-2007_05_02,17_40_24_05,UTC.dump
done!
kmsadmin@kms$
```

Example 4 (restore from a specified backup set, suppressing the confirmation prompt):

```
kmsadmin@kms$ run_restore_db -k
0000000000000000000000000000000000000000000000000000000000000000 -f
KmsHost-00000001-2007_05_02,17_40_24_05,UTC
Restoring 'keys' database from /export/home/kms/mnt_backups/ultrakms-
keys.KmsHost-00000001-2007_05_02,17_40_24_05,UTC.dump
done!
Restoring 'opr' database from /export/home/kms/mnt_backups/ultrakms-
opr.KmsHost-00000001-2007_05_02,17_40_24_05,UTC.dump
done!
kmsadmin@kms$
```

See Also

- run_backup_db
- restore_db
- backup_db

search_tokens

Name

`search_tokens` — Display current token IP settings.

Synopsis

```
search_tokens
```

Description

Display current IP network settings for all tokens in communication with the Crypto Key Management Station. The KMS software polls continuously for available tokens and displays the current settings from each. You can use this command to verify that tokens are active and have the correct IP settings.

Note – This command finds tokens on the same IP subnet as the Crypto Key Management Station only. It does not find remote tokens.

Note – This command runs continuously until you press `Ctl-c`.

Operator Role

You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.

Options

None.

Examples

Example 1:

```
kmsadmin@kms$ search_tokens
Press 'Control-C' to stop the search
Found 'Token Info: FW V1.2n 00:90:c2:cd:09:ab NMask=255.0.0.0  GWayIP=
118.0.0.254' at 118.157.228.001
Found 'Token Info: FW V1.2n 00:90:c2:cd:09:43 NMask=255.255.255.0
GWayIP=118.153.228.1' at 118.153.228.126
Found 'Token Info: FW V1.2n 00:90:c2:cd:09:43 NMask=255.255.255.0
GWayIP=118.153.228.1' at 118.153.228.126
Found 'Token Info: FW V1.2n 00:90:c2:cd:09:ab NMask=255.0.0.0  GWayIP=
118.0.0.254' at 118.157.228.001
```

```
Found 'Token Info: FW V1.2n 00:90:c2:cd:09:ab NMask=255.0.0.0  GWayIP=
118.0.0.254' at 118.157.228.001
^CCancelled
kmsadmin@kms$
```

See Also

- create_token
- send_permanent_ip

send_permanent_ip

Name

`send_permanent_ip` — Assign permanent IP settings to a specified physical token.

Synopsis

`send_permanent_ip -i` *token_IP_address* `-m` *netmask* `-g` *gateway_IP_address* *token_MAC_address*

Description

Note – Before you perform this activity, you must insert the token into a token bay attached directly to the Crypto Key Management Station.

Allows you to assign permanent IP network settings to a specified physical token. These settings are stored in the token's nonvolatile memory and are therefore retained when the token is removed from the token bay.

All tokens are delivered from the factory with the following default IP settings:

- IP address = 10.0.0.2
- Netmask = 255.0.0.0
- Gateway IP = 10.0.0.254

Before you can use the token on your network, you must use this command to assign IP settings compatible with your network.

The IP address you assign must be on the same subnet as the encryption-capable library drives. The IP address is used to communicate with the token, as follows:

- For networked token operations, both the library drives and the KMS software use this IP address to communicate with the token.
- For air gap operations, only the library drives use this IP address to communicate with the token. The KMS software uses a temporary IP address assigned by the **Tokens > Write Device Keys** or **Tokens > Write Media Keys** GUI screens or the `write_token` CLI command.

Note – After using this command, you can use the **Tokens > Create** GUI screen or the `create_token` CLI command to identify the token to the KMS software.

Operator Role

You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.

Options

-i *IP_address*

Required.

Permanent IP address you want to assign to the token. For both air gap and networked token operations, the IP address must be on the same subnet as the library drives.

32-bit numeric address, in dotted decimal notation, *nnn*.*nnn*.*nnn*.*nnn*. Valid values for *nnn* are 0 to 255. For example, `123.119.01.73`.

-m *netmask*

Required.

Netmask for the network on which the token resides.

32-bit numeric address, in dotted decimal notation, *nnn*.*nnn*.*nnn*.*nnn*. Valid values for *nnn* are 0 to 255. For example, `123.119.01.73`.

-g *gateway*

Required.

IP address of the gateway node for the network on which the token resides.

32-bit numeric address, in dotted decimal notation, *nnn*.*nnn*.*nnn*.*nnn*. Valid values for *nnn* are 0 to 255. For example, `123.119.01.73`.

token_MAC_address

Required.

MAC address of the physical token. Unique for each token. Printed on the token label.

Note – In order for the command to be successful, the MAC address you specify must match the MAC address assigned to the token inserted in the Crypto Key Management Station token bay.

Twelve hexadecimal digits, separated into six groups of two digits each. For example, `00.90.C2.67.89.ab`. Each group must have two printable hex digits, with leading zeroes as needed. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

Examples

Example 1 (successful operation):

```
kmsadmin@kms$ send_permanent_ip -i 118.157.228.126 -m 255.0.0.0 -g
118.0.0.254 00:90:c2:cd:09:ab
About to send IP information
Press 'Return' to proceed, 'Control-C' to cancel

Sending IP information for token with MAC address 00:90:c2:cd:09:ab
Finished
kmsadmin@kms$
```

Example 2 (cancelled operation):

```
kmsadmin@kms$ send_permanent_ip -i 118.157.228.001 -m 255.0.0.0 -g
118.0.0.254 00:90:c2:cd:09:ab
About to send IP information
Press 'Return' to proceed, 'Control-C' to cancel
^CCancelled

kmsadmin@kms$
```

See Also

- create_token
- send_permanent_ip

show_status

Name

`show_status` — Display KMS software configuration information.

Synopsis

```
show_status
```

Description

Display information about the configuration of the KMS software.

Operator Role

You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.

Options

None

Examples

Example 1:

```
kmsadmin@kms$ show_status
Version: 1.2.0
Operating mode: STANDARD
Peer: NONE
Database backup storage device: mounted
GUI service: online
GUI server: running
GUI default locale setting: en_US.UTF-8
Communication service: online
Communication server: running
PostgreSQL server: running
Power-up self-test status: passed
nge0: not present or unconfigured
e1000g0: address 129.153.228.118 mask ffffff80
e1000g1: address 10.0.0.1 mask ff000000
kmsadmin@kms$
```

See Also

None

view_backup_key

Name

`view_backup_key` — Display the current database backup encryption key.

Synopsis

`view_backup_key [-o` *login_ID*`] [-p` *password*`]`

Description

Display the current database backup encryption key.

Note – This activity cannot be performed from the KMS GUI.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Examples

Example 1:

```
kmsuser@kms$ view_backup_key -o Kmsadmin -p !Password1!
0000000000000000000000000000000000000000000000000000000000000000

kmsuser@kms$
```

See Also

- export_media_key

- view_key

view_drive

Name

`view_drive` — Display encryption drive information.

Synopsis

```
view_drive [-o login_ID] [-p password] -a | -u | -d drive_name
| drive_name1[ drive_name2 ...]
```

Description

Display information about drives identified for encryption capability.

Options allow you to display the following:

- Summary list of all drives in the KMS database
- Summary list of all drives not assigned to a drive pool.
- Summary list of all drive pools to which a specified drive is assigned.
- Detailed information about a specified drive. This includes the description, PC key, crypto serial number, and detailed messages about interactions between the drive and the KMS software.

Operator Role

Security Officer or User for -a option

User only for all other options

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You must specify only one of the following options: `-a`, `-u`, `-d`, or *drive_name*. If you are logged in using the Security Officer role, you can use the `-a` option only.

`-a`

Lists all drives in KMS database.

`-u`

Lists all drives not assigned to any drive pool.

`-d` *drive_name*

Lists all drive pools associated with the specified drive.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

drive_name1 `[` *drive_name2* `...]`

Displays detail for the specified drive, including the following:

Description, PC key, and crypto serial number.

Detailed status and error messages for the drive. These are updated whenever information such as media or device keys or new drive pool mappings are transmitted to the drive. The messages are displayed in reverse chronological order (that is, most recent messages at the top).

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

Examples

Example 1 (list all drives):

```
kmsuser@kms$ view_drive -o Kmssecurity -p !Password1! -a
Drive0
Drive2
Drive3
kmsuser@kms$
```

Example 2 (list all drives not assigned to a drive pool):

```
kmsuser@kms$ view_drive -o Kmsuser -p !Password1! -u
Drive2
Drive3
kmsuser@kms$
```

Example 3 (list all drive pools to which a specified drive is assigned):

```
kmsuser@kms$ view_drive -o Kmsuser -p !Password1! -d Drive0
TestDrivePool
kmsuser@kms$
```

Example 4 (display detailed drive information):

```
kmsuser@kms$ view_drive -o Kmsuser -p !Password1! T10KDrive
Name                          : T10KDrive
Serial #                      : 001452
PCKey                         : 42d77cf1d06b17c2629e42ec34f
```

```
b9d277017d9b93fce6205e8b16a7a0d309ea5
Description                   : Real Tape Drive in Blooming
ton Office Lab
Messages                      :

Token ID: Token_5e ( IP Address: 129.153.228.125 )
Token DTS: 2007-05-03 10:45:10
Code: 000061fd
Message:
EKT built assuming drive in reset state -- drive is not reset


Token ID: Token_5e ( IP Address: 129.153.228.125 )
Token DTS: 2007-05-03 10:02:44
Code: 000061fd
Message:
EKT built assuming drive in reset state -- drive is not reset

kmsuser@kms$
```

See Also

- create_drive
- modify_drive

view_drivepool

Name

`view_drivepool` — Display drive pool information.

Synopsis

`view_drivepool [-o` *login_ID*`] [-p` *password*`] -a | -k` *drive_pool1*`[` *drive_pool2* `...] | -d` *drive_pool1*`[` *drive_pool2* `...] |` *drive_pool1*`[` *drive_pool2* `...]`

Description

Allows you to display information about drive pools.

Options allow you to display the following:

- Summary list of all drive pools in the KMS database
- All key sets assigned to a specified drive pool
- All drives assigned to a specified drive pool
- Detailed information about a specified drive pool. This includes the description, total number of keys assigned, and the key ID of the write key.

Operator Role

User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You must specify only one of the following options: `-a`, `-k`, `-d`, or *drive_pool*.

`-a`

Lists all drive pools in the KMS database.

`-k` *drive_pool1*`[` *drive_pool2* `...]`

Lists all key sets assigned to a specified drive pool.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

`-d` *drive_pool1* `[` *drive_pool2* `...]`

Lists all drives assigned to the specified drive pool.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

drive_pool1 `[` *drive_pool2* `...]`

Displays detailed information about the specified drive pool, including the key sets and the write key assigned to it.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

Examples

Example 1(list all drive pools):

```
kmsuser@kms$ view_drivepool -o Kmsuser -p !Password1! -a
Drive_Pool_1
DrivePool5
TestDrivePool
kmsuser@kms$
```

Example 2 (list all key sets assigned to a drive pool):

```
kmsuser@kms$ view_drivepool -o Kmsuser -p !Password1! -k Drive_Pool_1
KeySet2
kmsuser@kms$
```

Example 3 (list all drives assigned to a drive pool):

```
kmsuser@kms$ view_drivepool -o Kmsuser -p !Password1! -d TestDrivePool
Drive0
kmsuser@kms$
```

Example 4 (display detail about a drive pool):

```
kmsuser@kms$ view_drivepool -o Kmsuser -p !Password1! DrivePool10

Name                          : DrivePool10
Write key                     :
001e00030000000000000000000000090000000000000000000000000000000000
Drives                        : None
Key Sets                      : KeySet10, KeySet20
```

```
Keys                              : 2
Description                       : Test Drive Pool

kmsuser@kms$
```

See Also

- create_drivepool
- view_drivepool

view_key

Name

`view_key` — Display media key information.

Synopsis

`view_key [-o` *login_ID*`] [-p` *password*`] -a |` *key_ID1*`[` *key_ID2* `...]`

Description

Allows you to display information about media keys.

Options allow you to display the following:

- Summary list of key IDs for all media keys in the KMS database
- Detailed information about a specified media key. This includes the key's status and description, and how it was created.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You must specify either `-a` or *key_ID*, but not both.

`-a`

Lists the key IDs of all media keys in the KMS database.

key_ID1`[` *key_ID2* `...]`

Displays detailed information about the specified media key. You must specify the key ID.

64 hexadecimal digits. You can enter upper- or lower-case hex digits, but the display is shown in all upper-case.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

Examples

Example 1 (list key IDs of all media keys):

```
kmsuser@kms$ view_key -o KmsAdm -p !Password1! -a
001e000300000000000000000000000100000000000000000000000000000000
001e000300000000000000000000000200000000000000000000000000000000
001e000300000000000000000000000300000000000000000000000000000000
001e000300000000000000000000000400000000000000000000000000000000
001e000300000000000000000000000500000000000000000000000000000000
001e000300000000000000000000000600000000000000000000000000000000
kmsuser@kms$
```

Example 2 (display detail for specified media keys):

```
kmsuser@kms$ view_key -o KmsAdm -p !Password1!
001e000300000000000000000000000100000000000000000000000000000000
001e000300000000000000000000000200000000000000000000000000000000

Name                          :
001e000300000000000000000000000100000000000000000000000000000000
Source                        : Kms
Status                        : Active
Description                   : media key 1


Name                          :
001e000300000000000000000000000200000000000000000000000000000000
Source                       : Generated by mkkeys Tue Oct 17 20:14:49
2006 GMT.
Status                        : Active
Description                   : media key 2

kmsuser@kms$
```

See Also

- create_key
- modify_key

view_keyset

Name

`view_keyset` — Display key set information.

Synopsis

`view_keyset [-o` *login_ID*`] [-p` *password*`] -a |` *key_set_name1*`[` *key_set_name2* `...]`

Description

Allows you to display information about key sets.

Options allow you to display the following:

- Summary list of all key sets in the KMS database
- Detailed information about a specified key set. This includes the description, total number and key IDs of all keys assigned.

Operator Role

Administrator

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You must specify either `-a` or *key_set_name*, but not both.

`-a`

Lists all key sets in the KMS database.

key_set_name1`[` *key_set_name2* `...]`

Displays detailed information about the specified key set.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

Examples

Example 1 (list all key sets):

```
kmsuser@kms$ view_keyset -o KmsAdm -p !Password1! -a
Keyset1
KeySet2
KeySet3
kmsuser@kms$
```

Example 2 (display detail about specified key sets):

```
kmsuser@kms$  view_keyset -o KmsAdm -p !Password1! KeySet1 KeySet3

Name                           : KeySet1
Key count                      : 2
Keys                           :

001e000300000000000000000000000100000000000000000000000000000000

001e000300000000000000000000000600000000000000000000000000000000
Description                    : Test keyset


Name                           : KeySet3
Key count                      : 2
Keys                           :

001e000300000000000000000000000100000000000000000000000000000000

001e000300000000000000000000000200000000000000000000000000000000
Description                    : Description

kmsuser@kms$
```

See Also

- create_keyset
- modify_keyset

view_mapping

Name

`view_mapping` — Display drive pool/key set mapping information.

Synopsis

```
view_mapping [-o login_ID] [-p password]
-a | drive_pool_name1[ drive_pool_name2 ...]
```

Description

Allows you to display drive pool/key set mapping information. This includes the key sets and the write key assigned to each drive pool.

Operator Role

User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You must specify either `-a` or *drive_pool_name*, but not both.

`-a`

Displays key set mappings for all drive pools in the KMS database.

drive_pool_name1`[` *drive_pool_name2* `...]`

Displays key set mappings for the specified drive pool only.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

Examples

Example 1 (display mapping information for all drive pools):

```
kmsuser@kms$ view_mapping -o Kmsuser -p !Password1! -a
Drive Pool: Drive_Pool_1
    Write Key:
001e0003000000000000000000000006000000000000000000000000000000000
    Key sets: KeySet2
    Total keys: 2
Drive Pool: DrivePool5
    No assigned key sets.
Drive Pool: TestDrivePool
    Write Key:
001e0003000000000000000000000004000000000000000000000000000000000
    Key sets: KeySet3
    Total keys: 2
kmsuser@kms$
```

Example 2 (display mapping information for specified drive pools):

```
kmsuser@kms$ view_mapping -o Kmsuser -p !Password1! TestDrivePool
Drive_Pool_1
Drive Pool: TestDrivePool
    Write Key:
001e0003000000000000000000000004000000000000000000000000000000000
    Key sets: KeySet3
    Total keys: 2
Drive Pool: Drive_Pool_1
    Write Key:
001e0003000000000000000000000006000000000000000000000000000000000
    Key sets: KeySet3
    Total keys: 2
kmsuser@kms$
```

See Also

- modify_mapping

view_operator

Name

`view_operator` — Display login ID information.

Synopsis

```
[view_operator [-o login_ID] [-p password] -a | login_ID1[ login_ID2 ...]
```

Description

Allows you to display information about login IDs.

Note – You can display only the operator roles for which you have sufficient authority. If you are using the Administrator role, you can display only the Administrator and Security Officer roles. If you are using the Security Officer role, you can display only the Security Officer and User roles.

Options allow you to display the following:

- Summary list of all login IDs you are authorized to display
- Detailed information about a specified login ID. This includes the assigned role and status.

Operator Role

Administrator, to display login IDs with the Administrator operator role

Administrator or Security Officer, to display login IDs with the Security Officer operator role

Security Officer, to display login IDs with the User operator role

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You must specify either `-a` or *login_ID*, but not both.

`-a`

Lists all login IDs you are authorized to display.

login_ID1 `[` *login_ID2* `...]`

Displays detailed information for the specified login ID.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

Examples

Example 1 (list all login IDs, using Security Officer role):

```
kmsuser@kms$ view_operator -o Kmssec -p !Password1! -a
Kmssec
Kmsuser
kmsuser@kms$
```

Example 2 (list all login IDs, using Administrator role):

```
kmsuser@kms$ view_operator -o KmsAdm -p !Password1! -a
KmsAdm
Kmssec
kmsuser@kms$
```

Example 3 (display detail for specified login IDs):

```
kmsuser@kms$ view_operator -o KmsAdm -p !Password1! KmsAdm Kmssec

Name                          : KmsAdm
Role                          : administrator
Description                   : Default Administrator


Name                          : Kmssec
Role                          : security_officer
Description                   : Security Officer

kmsuser@kms$
```

See Also

- create_operator
- modify_operator

view_token

Name

`view_token` — Display physical token information.

Synopsis

`view_token [-o` *login_ID*`] [-p` *password*`] -a |` *token_ID1*`[` *token_ID2* `...]`

Description

Allows you to display information for physical tokens.

Options allow you to display the following:

- Summary list of all physical tokens in the KMS database.
- Detailed information for a specified token. This includes the current firmware version, MAC address, last modification date, and description.

Operator Role

Security Officer or User

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

Note – You must specify either `-a` or *token_ID*, but not both.

`[-a]`

Lists all physical tokens in the KMS database.

token_ID1`[` *token_ID2* `...]`

Displays detailed information for the specified physical token.

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

Examples

Example 1 (list all physical tokens):

```
kmsuser@kms$ view_token -o Kmsuser -p !Password1! -a
Token_2
tokenid
kmsuser@kms$
```

Example 2 (display detailed information for specified tokens):

```
kmsuser@kms$ view_token -o Kmsuser -p !Password1! Token10 Token_5e

Name                           : Token10
Type                           : NKT
Version                        : 01.20
MAC Address                    : 00:90:c2:11:18:23
IP Address                     : 10.0.0.99
Last Modified                  : none
Last Contact                   : None
Description                    : Example token
Messages                       :
no messages

Name                           : Token_5e
Type                           : OKT
Version                        : 01.20
MAC Address                    : 00:90:c2:cd:09:5e
IP Address                     : 129.153.228.125
Last Modified                  : 2007-04-27 11:09:59
Last Contact                   : Thu May  3 12:55:38 2007
Description                    : Real Token in Bloomington Lab
Messages                       :
Token DTS: 2007-05-03 10:45:10
Token Type: EKT
Token Message:
EKT built assuming drive in reset state -- drive is not reset


Token DTS: 2007-05-03 10:02:44
Token Type: EKT
Token Message:
EKT built assuming drive in reset state -- drive is not reset


kmsuser@kms$
```

See Also

- create_token
- modify_token

write_token

Name

`write_token`— Write an enabling key token (EKT) or an operating key token (OKT).

Synopsis

Write device keys to an EKT:

```
write_token [-o login_ID] [-p password] [-t token_type] [-r] [-l]
token_ID drive_name1 [drive_name2 ...]
```

Write media keys to an OKT:

```
write_token [-o login_ID] [-p password] [-t token_type] [-l] token_ID
drive_pool_name1 [drive_pool_name2 ...]
```

Note – The *token_ID* must come before the *drive_name* or *drive_pool_name*.

Description

Allows you to write either an enabling key token (EKT) or an operating key token (OKT).

Before you perform this activity, you must verify the following:

- The KMS software is successfully communicating with the token. Use the **Tokens > View** GUI screen or the `view_token` CLI command and note the Last Contact field.
- The drives to which you want to transmit keys are on the same subnet as the token you have selected.

Networked Token Operations

You must NOT indicate that this is a locally attached token.

Once the keys have been written successfully to the token, the token automatically transmits the keys to the drives.

Air Gap Operations

You must indicate that this is a locally attached token. This notifies the KMS software that prior to sending the keys to the token, it must assign a temporary IP address to the token. It uses the IP address value assigned previously with the **Tokens > Create** GUI screen or `create_token` CLI command.

Once the keys have been written successfully to the token, the token does NOT automatically transmit the keys to the drives. In order for the drives to receive the keys, you must remove the token from the Crypto Key Management Station token bay and insert it in the drive token bay.

Write Device Keys to an EKT

You must specify the drives to which you want to transmit device keys. Additionally, you must indicate drives that have been reset or have not previously received device keys.

Note – Raw keys must be available in the KMS database. For each drive you specify, three raw keys are used to create a set of encrypted device keys on the physical token.

Write Media Keys to an OKT

You must specify the drive pools to which you want to transmit media keys.

Note – To be eligible for media keys, a drive pool must be assigned both a write key and at least one drive.

Operator Role

Security Officer to write an EKT

User to write an OKT

Options

`[-o` *login_ID*`]`

Login ID you want to use to perform this command. Used to verify that you have sufficient authority to execute the command.

If you do not specify a login ID, the value assigned to the `KMS_OPERATOR` environment variable is used, if it has been defined.

`[-p` *password*`]`

Password assigned to your login ID.

If you do not specify a password, the value assigned to the `KMS_PASSWORD` environment variable is used, if it has been defined.

`-t` *token_type*

Required.

Type of token you want to write. Options are:

- `e` – Enabling key token (EKT); used to transfer device keys to the encryption drives.
- `o` – Operating key token (OKT); used to transfer media keys to the encryption drives.

Note – The `-r` option is valid only if the *token_type* is “`e`” (that is, you are writing an EKT).

`[-r]`

Note – With KMS 1.2, this option replaces the `-z` option.

Optional.

Indicates the drive is currently in a reset state (that is, the drive does not have device keys). This causes the device key package to be encrypted using the drive's PC key.

Note – Specify this option only if the drive has NOT been enabled for encryption previously, or if the drive is currently in a reset state.

`[-l]`

Optional.

Indicates that the token is inserted in a token bay that is connected directly to the Crypto Key Management Station.

Note – Specify this option only if you are using air gap operations.

---

drive_name1 `[` *drive_name2* `...]`

Drive to which you want to transmit device keys. Valid only if the *token_type* is "`e`" (that is, you are writing an EKT).

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

drive_pool1 `[` *drive_pool2* `...]`

Drive pool to which you want to transmit media keys. Valid only if the *token_type* is "`o`" (that is, you are writing an OKT).

1–20 alphanumeric characters. Valid characters are a to z, A to Z, 0 to 9, and _ (underscore). Embedded spaces are NOT allowed; leading and trailing spaces are ignored.

You can specify a list of items by separating them with spaces. For example, `Item1 Item2 Item3`.

token_ID

Required.

ID of the token to which you want to write device or media keys. The token must be on same IP subnet as the drives to which you want to transmit the keys.

Examples

Example 1 (write an EKT and reset the drives):

```
kmsuser@kms$ write_token -o Kmssec -p !Password1! -t e -r Token_5e
DriveCLI
Prepping zeroized drive
Token 'Token_5e' key write complete
kmsuser@kms$
```

Example 2 (write an EKT without resetting the drives):

```
kmsuser@kms$ write_token -o Kmssec -p !Password1! -t enabling Token_5e
DriveCLI

Token 'Token_5e' key write complete
kmsuser@kms$
```

Example 3 (write an OKT—networked token operations):

```
kmsuser@kms$ write_token -o Kmsuser -p !Password1! -t o Token_5e
T10KDrivePool

Token 'Token_5e' key write complete
kmsuser@kms$
```

Example 4 (write an OKT—air gap operations):

```
kmsuser@kms$ write_token -o Kmsuser -p !Password1! -t o -l Token_5e
T10KDrivePool

Token 'Token_5e' key write complete
kmsuser@kms$
```

See Also

- reset_token

CHAPTER 7

KMS Database

This chapter describes the Key Management Station (KMS) database and the tasks required to manage it.

Database Contents

The KMS database contains information used when creating and transmitting encryption keys between the Crypto Key Management Station, the tokens, and the tape drive. It includes all information entered through the KMS GUI screens and CLI commands, such as:

- Token IP addresses
- Drive preset communication (PC) keys
- Drive crypto serial numbers
- Raw keys
- Media keys
- Device keys
- Drive pool/key set mappings

The database also contains the Crypto Key Management Station ID, the database encryption key, and the USB database backup encryption key.

Note – For security purposes, data cannot be deleted from the KMS database.

PC Keys and Crypto Serial Numbers

Each drive has a unique PC key and crypto serial number, which are assigned at the factory. These numbers must be entered in to the KMS database to enable a tape drive for encryption.

When you identify a drive to be enabled for encryption, you can use either of the following methods to supply these numbers:

- Enter the drive data manually. You need to obtain the drive's unique preset communication (PC) key and crypto serial number before performing this activity.
- Import the drive data from a CD provided by Sun Microsystems, Inc. Each drive has its own CD. The drive's unique preset communication (PC) key and crypto serial number are provided on the CD. See "Import PC Keys and Crypto Serial Numbers From an External Source", below, for details.

▼ Import PC Keys and Crypto Serial Numbers From an External Source

Operator Role: User

Screen Navigation: **Drives > Create**

1. **Log in to the workstation using the** `kmsuser` **login ID.**
2. **Start a Browser Window by doing either of the following:**
   - Double-click the **Browser Window** icon on the desktop.
   - Select **Start > Browser Window**.

   The KMS GUI starts automatically.
3. **Log in to the KMS GUI using a login ID with the User operator role.**

   `Login:` *User_login*
   `Password:` *password*

   where:
   - *User_login* is the KMS login ID.
   - *password* is the password assigned to the login ID.

   See your Crypto Key Management Station administrator for assistance.
4. **Select Launch > Applications > Utilities to open a Terminal window.**
5. **In the Terminal window, switch to the** `root` **user.**

   ```
   # su root
   ```
6. **Load the drive CD in the DVD drive (each drive has its own CD).**
7. **Mount the CD.**

   ```
   # /opt/SUNWkms/app/sbin/mount_cd
   ```
8. **In the KMS GUI, select Drives > Create.**
9. **In the CD Path field, enter the full path name of the CD mount point.**
10. **Click Import Now.**
11. **Click Apply.**
12. **In the Terminal window, unmount the CD.**

    ```
    # /opt/SUNWkms/app/sbin/umount_cd
    ```
13. **Remove the CD from the DVD drive.**

14. **Repeat Step 6 through Step 13 for each drive you want to identify.**

15. **In the Terminal window, log out as `root`.**

```
# exit
```

Raw Keys

Raw keys are used to create device keys and media keys. Raw keys must be loaded in to the KMS database to be used.

▼ Generate Raw Keys

Typically, raw keys are generated by the Sun Crypto Accelerator 6000 (SCA6000) card that is shipped with the Crypto Key Management Station.

Operator Role:	None
Screen Navigation:	None; this procedure does not involve the KMS GUI.

1. **Power on the Crypto Key Management Station workstation.**

2. **Log in to the workstation using the `kmsadmin` login ID.**

```
Login: kmsadmin
Password: password
```

where *password* is the password assigned to the `kmsadmin` login ID. See your Crypto Key Management Station administrator for assistance.

3. **Select Launch > Applications > Utilities to open a Terminal window.**

4. **Issue the command to create the raw keys from the SCA6000 card.**

```
# /opt/SUNWkms/app/mars/mkkeys -k n
```

where *n* indicates the number of raw keys to be created. Valid entries are 1–8, to be multiplied by 1024 to determine the number of raw keys. For example, an entry of 1 indicates 1024 raw keys, 2 indicates 2048, and so on.

Note – The more raw keys there are in the KMS database, the longer it takes to perform a database backup. Therefore it is recommended that you create only 1024 raw keys at a time.

---

5. **Verify that the keys have been created.**

```
# cd /export/home/kms/mnt_cd
# ls -l rawdata.dat
```

`rawdata.dat` is the file that contains the raw keys. Verify that the time stamp for this file matches the time when you ran the `mkkeys` command.

6. **Log out of the workstation.**

Import Raw Keys to the KMS Database

You can use either of the following methods to import raw keys in to the KMS database.

- Import raw keys generated by the Sun Crypto Accelerator 6000 (SCA6000) card. See "Import Raw Keys From the SCA6000 Card".
- Import keys from an external source. See "Import Raw Keys From an External Source".

▼ Import Raw Keys From the SCA6000 Card

Operator Role:	Administrator
Screen Navigation:	**Keys > Raw Key Load**

1. **Log in to the KMS GUI as Administrator. (See** "Log in to the KMS GUI on the Crypto Key Management Station" on page 41 **for detailed instructions.)**
2. **Select Keys > Raw Key Load.**
3. **In the Import Directory field, enter the full path name of the directory where the** `rawdata.dat` **file resides (this is the file containing the raw keys).**

```
/export/home/kms/mnt_cd
```

4. **Click Apply.**

▼ Import Raw Keys From an External Source

Operator Role:	Administrator
Screen Navigation:	**Keys > Raw Key Load**

1. **Log in to the workstation using the** `kmsuser` **login ID.**
2. **Start a Browser Window by doing either of the following:**
   - Double-click the **Browser Window** icon on the desktop.
   - Select **Launch > Browser Window**.

   The KMS GUI starts automatically.
3. **Log in to the KMS GUI using a login ID with the Administrator operator role.**

   `Login:` *Administrator_login*
   `Password:` *password*

   where:
   - *Administrator_login* is the KMS login ID.
   - *password* is the password assigned to the login ID.

   See your Crypto Key Management Station administrator for assistance.
4. **Select Launch > Applications > Utilities to open a Terminal window.**
5. **In the Terminal window, switch to the** `root` **user.**

```
# su root
```

6. **Load the CD into the DVD drive.**
7. **Mount the CD.**

```
# /opt/SUNWkms/app/sbin/mount_cd
```

8. **In the KMS GUI, select Keys > Raw Key Load.**
9. **In the Import Directory field, enter the full path name of the CD mount point.**
10. **Click Apply.**
11. **In the Terminal window, unmount the CD.**

```
# /opt/SUNWkms/app/sbin/umount_cd
```

12. **Remove the CD from the DVD drive.**
13. **In the Terminal window, log out as** `root`**.**

```
# exit
```

Database Backup

KMS database backups are written to the external USB hard drive.

The backups are encrypted by the Sun Crypto Accelerator 6000 (SCA6000) card. When the Crypto Key Management Station is installed, you specify the 256-bit key used to encrypt the backups. When you export media keys to an ASCII file, the database backup encryption key is NOT included. (See "Keys > Media Key Export" on page 67 for details.) The Crypto Key Management Station administrator can display the backup key with the view_backup_key CLI command.

Note – Backups are always of the entire database; incremental backups are not supported.

Database backups are performed in either of the following ways:

- Automatically, by the KMS software
- Manually, by an authorized administrator

Automatic Backups

The KMS software automatically backs up the database whenever either of the following events occurs:

- A user logs out of the KMS GUI.
- An enabling key token (EKT) or operating key token (OKT) is written.

Manual Backups

An authorized Crypto Key Management Station administrator can perform database backups at any time using either the backup_db or run_backup_db CLI commands. You cannot use the GUI to back up the database.

Both CLI commands allow you to specify the directory where you want the backup files to be written. The default is `/export/home/kms/mnt_backups`.

See the backup_db and run_backup_db CLI commands for details.

Remote Backups

The Crypto Key Management Station is shipped with a template `cron` script to perform periodic remote backups. An authorized Crypto Key Management Station administrator can modify this script to meet the requirements at your site.

Database Restoration

The database can be restored from the encrypted backup saved on the external hard drive. An authorized Crypto Key Management Station administrator can perform restorations using the (CLI). You cannot use the GUI to restore the database.

See the restore_db and run_restore_db CLI commands for details.

CHAPTER 8

Crypto Key Management Station Support

This chapter describes the Crypto Key Management Station logging facility.

Logs

The Crypto Key Management Station logging features complies with FIPS 140-2 certification requirements. Events are logged using the native Solaris logging mechanism.

The following events are logged:

- Users logging in to and out of the Crypto Key Management Station
- Any action resulting in a change to the KMS database
- Any communication with tokens

New entries are added to the end of the log file, so that existing entries are not overwritten. When the log file reaches a predefined size, the existing data is compressed and written to a versioned copy. New entries continue to be written to the active log file.

Log files are written in ASCII text. Each entry includes the following fields separated by tabs:

- Date and time of the event
- Login ID of the user who initiated the event. A dash (–) indicates no associated login ID.
- Description of the event
- Process that caused the event (such as GUI, CLI, script)
- Outcome of the event (success or failure)

Log entries do not contain sensitive data, such as cryptographic keys. For example, a log entry may indicate the date and time when a particular user wrote to a token, but the contents of the token are not logged.

An authorized Crypto Key Management Station administrator can view logs from the command line interface (CLI). You cannot view logs from the GUI.

CLI Quick Reference

Command	Synopsis
backup_db – Back up the KMS database. **Operator Role:** You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.	`backup_db` *path_name*
`create_drive` — Identify a drive you want to enable for encryption. **Operator Role:** User	Import drive data from CD: `create_drive [-o` *operator*`] [-p` *password*`] -i [-d` *description*`]` *drive_name* Enter drive data manually: `create_drive [-o` *operator*`] [-p` *password*`] -s` *serial_number* `-k` *PC_key* `[-d` *description*`]` *drive_name*
`create_drivepool` — Create a drive pool and optionally assign drives to it. **Operator Role:** User	`create_drivepool [-o` *login_ID*`] [-p` *password*`] [-a` *drive_name1*`[,`*drive_name2*`,...]] [-d` *description*`]` *drive_pool_name*
`create_key` — Create a media key and assign it to a key set. **Operator Role:** Administrator	Create from raw keys: `create_key [-o` *login_ID*`] [-p` *password*`] -s` *key_set_name* `-r [-d` *description*`]` Create manually: `create_key [-o` *login_ID*`] [-p` *password*`] -s` *key_set_name* `-c` *crypto_key* `[-d` *description*`]` *key_ID*
`create_keyset` — Create a key set. **Operator Role:** Administrator	`create_keyset [-o` *login_ID*`] [-p` *password*`] [-d` *description*`]` *key_set_name*

Command	Synopsis
create_operator — Create a KMS login ID. **Operator Role:** Administrator, to create login IDs with the Administrator operator role Administrator or Security Officer, to create login IDs with the Security Officer operator role Security Officer, to create login IDs with the User operator role	create_operator [-o *login_ID*] [-p *password*] -c *password* -r *role* [-d *description*] *login_ID*
create_token — Identify a physical token to be used in transmitting keys. **Operator Role:** Security Officer or User	create_token [-o *login_ID*] [-p *password*] -m *MAC_address* -v *version* [-d *description*] -i *IP_address* *token_ID*
export_media_key — Export specified media keys to an ASCII text file. **Operator Role:** Administrator	export_media_key [-o *login_ID*] [-p *password*] -f *file_name* [*key_ID1*[*key_ID2* ...]]
export_media_key_disable — Disable the media key export activity in both the GUI and the CLI. **Operator Role:** Administrator	export_media_key_disaable [-o *login_ID*] [-p *password*]
export_media_key_enable — Enable the media key export activity in both the GUI and the CLI. **Operator Role:** Administrator	export_media_key_enable [-o *login_ID*] [-p *password*]
history_token — Display history for a physical token. **Operator Role:** Security Officer or User	history_token [-o *login_ID*] [-p *password*] *token_ID*
import_media_key — Allows you to import media keys from a previously created export file. **Operator Role:** Administrator	import_media_key [-o *login_ID*] [-p *password*] *file_name*
import_raw_key—Import raw keys to the KMS database. **Operator Role:** Administrator	import_raw_key [-o *login_ID*] [-p *password*] *path_name*

Command	Synopsis
`mkkeys` — Generate raw keys. **Operator Role:** You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.	`mkkeys -k` *count* `[-i` *text*`]`
`modify_drive` — Modify the description of a drive. **Operator Role:** User	`modify_drive [-o` *login_ID*`] [-p` *password*`] [-d` *new_description*`]` *drive_name*
`modify_drivepool` — Modify drive pool description and add or remove drives from the pool. **Operator Role:** User	`modify_drivepool [-o` *login_ID*`] [-p` *password*`] [-a` *drive_name1*`[,`*drive_name2*`,...]] [-r` *drive_name1*`[,`*drive_name2*`,...]] [-d` *new_description*`]` *drive_pool_name*
`modify_key` — Modify the description and status of a media key. **Operator Role:** Administrator	`modify_key [-o` *login_ID*`] [-p` *password*`] [-A | -I] [-d` *new_description*`]` *key_ID*
`modify_keyset` — Modify a key set description and add or remove media keys from the key set. **Operator Role:** Administrator	`modify_keyset [-o` *login_ID*`] [-p` *password*`] [-a` *key_ID1*`[,`*key_ID2*`,...]] [-r` *key_ID1*`[,`*key_ID2*`,...]] [-d` *new_description*`]` *key_set_name*
`modify_mapping` — Modify the key set mappings for a drive pool. **Operator Role:** User	`modify_mapping [-o` *login_ID*`] [-p` *password*`] [-a` *key_set1*`[,`*key_set2*`,...]] [-r` *key_set1*`[,`*key_set2*`,...]] [-w` *key_ID*`]` *drive_pool_name*
`modify_operator` — Modify a login ID. **Operator Role:** Administrator, to modify login IDs with the Administrator operator role Administrator or Security Officer, to modify login IDs with the Security Officer operator role Security Officer, to modify login IDs with the User operator role	`modify_operator [-o` *login_ID*`] [-p` *password*`] [-c` *change_password*`] [-a | -i] [-r` *role*`] [-d` *new_description*`]` *login_ID*
`modify_token` — Modify information for a physical token. **Operator Role:** Security Officer or User	`modify_token [-o` *login_ID*`] [-p` *password*`] [-m` *MAC_address*`] [-v` *version*`] [-d` *new_description*`] [-i` *IP_address*`]` *token_name*
`reset_token` — Reset a physical token. **Operator Role:** User or Security Officer	`reset_token [-o` *login_ID*`] [-p` *password*`]` *token_id*

Command	Synopsis
`restore_db` — Restore the KMS database from backup. **Operator Role:** You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.	`restore_db -k` *backup_encryption_key* `-c` *checksum* *dump_file*
`run_backup_db` — Create a full backup of the KMS database. **Operator Role:** You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.	`run_backup_db [-d` *data_directory*`]`

`run_restore_db` — Restore the KMS database.
Operator Role: You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.
	`run_restore_db [-f] [-d` *data_directory*`]`
	`[-k` *backup_encryption_key*`]` *dump_ID* `| latest | list`

`search_tokens` — Display current token IP settings. **Operator Role:** You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.	`search_tokens`
`send_permanent_ip` — Assign permanent IP settings to a specified physical token. **Operator Role:** You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.	`send_permanent_ip -i` *token_IP_address* `-m` *netmask* `-g` *gateway_IP_address* *token_MAC_address*
`show_status` — Display KMS software configuration information. **Operator Role:** You must be logged in to the Crypto Key Management Station workstation using the `kmsadmin` login ID. No operator role is involved.	`show_status`
`view_backup_key` — Display the current database backup encryption key. **Operator Role:** Administrator	`view_backup_key [-o` *login_ID*`] [-p` *password*`]`

Command	Synopsis
`view_drive` — Display encryption drive information. **Operator Role:** Security Officer or User for -a option User only for all other options	`view_drive [-o` *login_ID*`] [-p` *password*`] -a | -u | -d` *drive_name* | *drive_name1*`[` *drive_name2* `...]`
`view_drivepool` — Display drive pool information. **Operator Role:** User	`view_drivepool [-o` *login_ID*`] [-p` *password*`] -a | -k` *drive_pool1*`[` *drive_pool2* `...] | -d` *drive_pool1*`[` *drive_pool2* `...] |` *drive_poo1l*`[` *drive_pool2* `...]`
`view_key` — Display media key information. **Operator Role:** Administrator	`view_key [-o` *login_ID*`] [-p` *password*`] -a |` *key_ID1*`[` *key_ID2* `...]`
`view_keyset` — Display key set information. **Operator Role:** Administrator	`view_keyset [-o` *login_ID*`] [-p` *password*`] -a |` *key_set_name1*`[` *key_set_name2* `...]`
`view_mapping` — Display drive pool/key set mapping information. **Operator Role:** User	`view_mapping [-o` *login_ID*`] [-p` *password*`] -a |` *drive_pool_name1*`[` *drive_pool_name2* `...]`
`view_operator` — Display login ID information. **Operator Role:** Administrator, to display login IDs with the Administrator operator role Administrator or Security Officer, to display login IDs with the Security Officer operator role Security Officer, to display login IDs with the User operator role	`[view_operator [-o` *login_ID*`] [-p` *password*`] -a |` *login_ID1*`[` *login_ID2* `...]`
`view_token` — Display physical token information. **Operator Role:** Security Officer or User	`view_token [-o` *login_ID*`] [-p` *password*`] -a |` *token_ID1*`[` *token_ID2* `...]`

`write_token`— Write an enabling key token (EKT) or an operating key token (OKT).
Operator Role: Security Officer to write an EKT
User to write an OKT
	Write device keys to an EKT:
	`write_token [-o` *login_ID*`] [-p` *password*`] [-t` *token_type*`] [-r] [-l]` *token_ID drive_name1* `[`*drive_name2* `...]`
	Write media keys to an OKT:
	`write_token [-o` *login_ID*`] [-p` *password*`] [-t` *token_type*`] [-l]` *token_ID drive_pool_name1* `[`*drive_pool_name2* `...]`
	The *token_ID* must come before the *drive_name* or *drive_pool_name.*

Index

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** 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 33009311 • **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