Oracle® Key Manager 3

Installation and Administration Guide

E41579-11
April 2020

Oracle Key Manager 3 Installation and Administration Guide,

E41579-11

Contents

2 Install the KMA

3 Configure a KMA with QuickStart

12 Sites, KMAs, Agents, and Data Units

B Configure the Network for the SL4000

C OKM-ICSF Integration

D Switch Configurations

E Advanced Security Transparent Data Encryption (TDE)

F Solaris ZFS Encryption

G Upgrade and Configure Integrated Lights Out Manager (ILOM)

Index

List of Figures

List of Tables

Preface

This guide provides planning, overview, configuration, and administration information for the Oracle Key Manager (OKM) software. This guide is intended for storage administrators, system programmers, and operators responsible for configuring and maintaining the OKM software at their site.

What's New

This section summarizes new and enhanced features for Oracle Key Manager 3.

May 2017 - Release 3.3

- A Thales nShield Solo module, a hardware security module, can be installed in an Oracle SPARC key management appliance (KMA).

December 2018 - Release 3.3.2

- New replication version 16
- Support for IBM LTO 8
- Option to set accepted TLS versions
- Support for X.509v3 certificates signed using the SHA-256 hashing algorithm
- Oracle Key Manager GUI and CLIs can be installed on Microsoft Windows Server 2012, Microsoft Windows 10, and Microsoft Windows 8 systems
- Changed password policy for Technical Support account
- New System Dump subcommand on the OKM CLI

April 2020

- Introduction of the T8-1 hardware platform.

Related Documentation

For additional OKM documentation, see: http://docs.oracle.com/en/storage/storage-software/oracle-key-manager/index.html.

Refer to the white paper *Oracle Key Management Overview*, available at: https://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

About Oracle Key Manager

Oracle Key Manager (OKM) provides data security by creating, storing, and managing the encryption keys to encrypt stored data (device-based encryption). OKM supports both open systems and enterprise platforms.

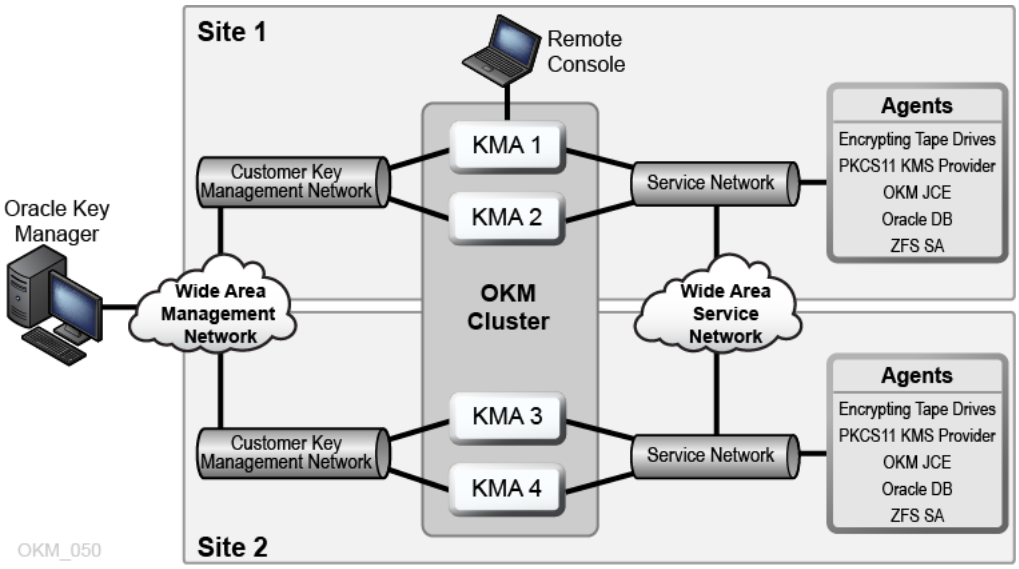
OKM Clusters

A cluster is a group of Key Management Appliances (KMAs) that are aware of each other and fully replicate information to each other. The cluster provides encryption endpoints (agents) a high availability service from which they can retrieve keys.

- Clusters must contain a minimum of two KMAs and maximum of 20 KMAs.
- New keys generated at any site replicate to all other KMAs in the cluster.
- You can define sites to provide a logical grouping of KMAs within the cluster, for example a site representing the KMAs in a particular data center. You can associate encryption agents with a specific site to preference KMAs within that site.
- All administrative changes propagate to all other KMAs in the cluster.
- You can cluster multiple KMAs con a dedicated private, local, or wide area network.
- Any KMA in a cluster can service any agent on the network.
- You can use any KMA in the cluster for administration functions.

> **Note:**
>
> KMAs in one cluster will be unaware of those in other clusters.

Figure 1-1 OKM Cluster Overview



Monitoring OKM

OKM supports monitoring using Oracle Enterprise Manager with the OKM plug-in, remote syslog, SNMP, or Oracle Hardware Management Pack. The Oracle Service Delivery Platform (SDP2) may be deployed for monitoring tape libraries and their encrypting tape drives on the service network.

Mixed Clusters and Upgrading Older KMAs

A mixed cluster contains KMAs running different OKM version. There are compatibility considerations when using a mixed cluster.

- Sun Fire KMAs cannot be directly upgraded to OKM 3.x, but can communicate with OKM 3.x KMAs in the same cluster.
- Sun Fire KMAs can be migrated to OKM 3.0.2 by submitting a request to have an Oracle customer service representative perform the migration. The process is described in the Oracle Support Document 1670455.1 published on the My Oracle Support site.
- Sun Fire X4170 M2 KMAs that have been migrated to OKM 3.0.2 should be upgraded to OKM 3.3 or higher, following a manual procedure. This manual procedure is described in the Oracle Support Document 229422.1 published on the My Oracle Support site.
- KMAs running an OKM release earlier than OKM 3.1 should not be added to an OKM cluster where there are KMAs are running newer OKM releases. Instead, they should be initialized into their own temporary cluster, upgraded to OKM 3.3 or later, and then reset to factory default settings. They can then be added to the existing OKM cluster.
- OKM 3.1 and later releases are not supported on Sun Fire X2100/X2200 M2 KMAs. These KMAs should be replaced with SPARC KMAs.
- OKM 3.x KMAs can join an existing OKM 2.x cluster using a KMA running KMS 2.2 or later.

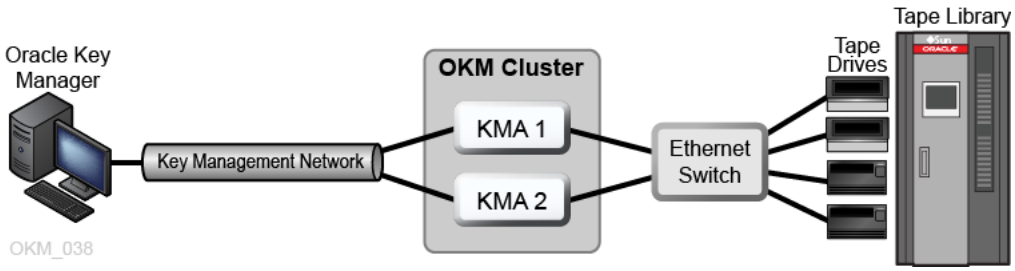
Sample OKM Cluster Configurations

Single Site OKM Configuration

A single site configuration contains the OKM cluster and agents at a single site.

The figure below shows a single site with two KMAs in a cluster. The service network includes multiple tape drives (agents).

Figure 1-2 Single Site Configuration

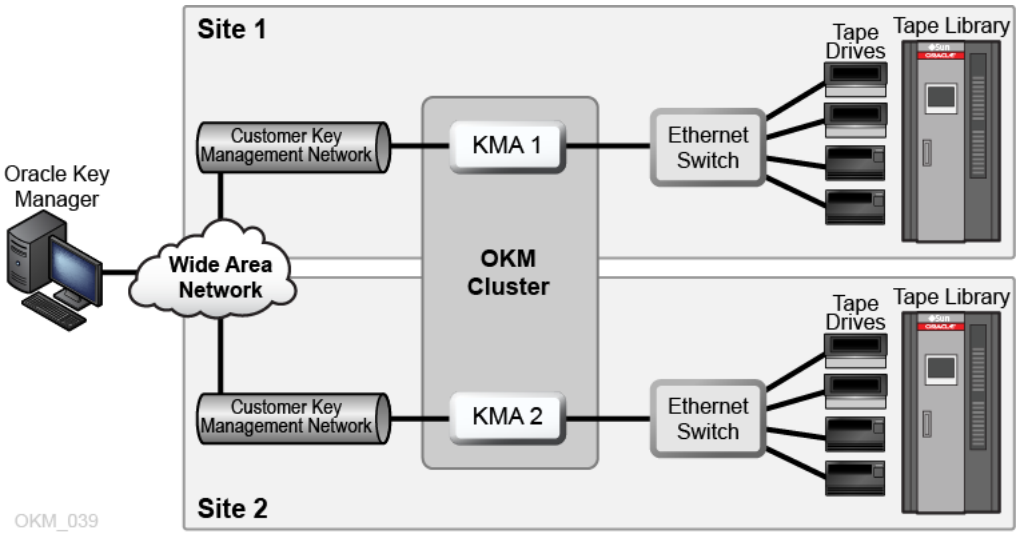


Dual Sites OKM Configuration

A dual site configuration has the OKM cluster split between multiple physical locations.

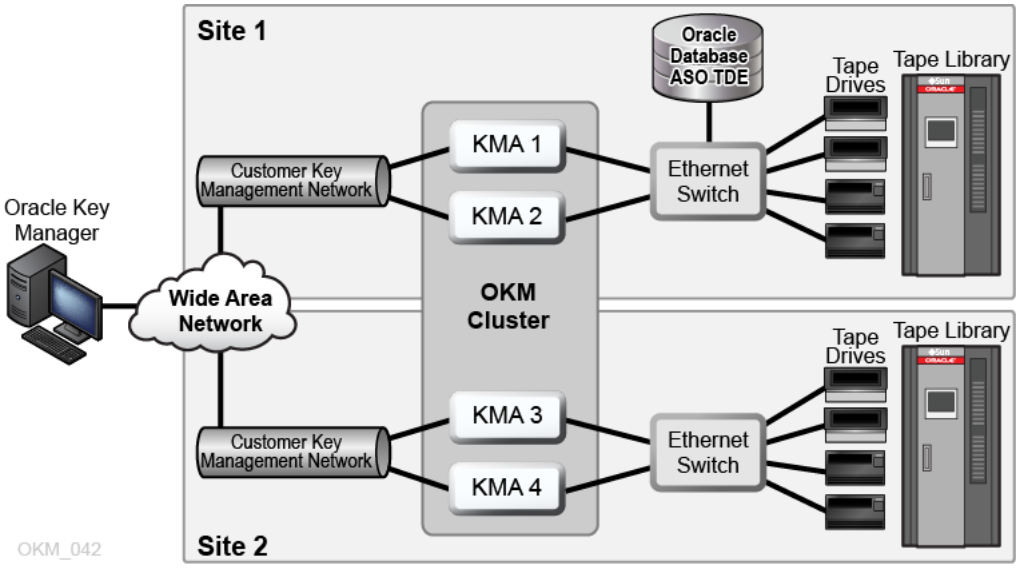
In the figure below, each site contains a KMA. The KMAs are managed over a wide area network, and both KMAs belong to the same OKM cluster. In this configuration, Oracle recommends geographically-dispersed sites.

Figure 1-3 Dual Site Configuration



In the figure below, four KMAs in a cluster are supporting two automated tape libraries and an Oracle database with Advanced Security Transparent Data Encryption (TDE) solution. For more information, refer to Advanced Security Transparent Data Encryption (TDE).

Figure 1-4 Database Example

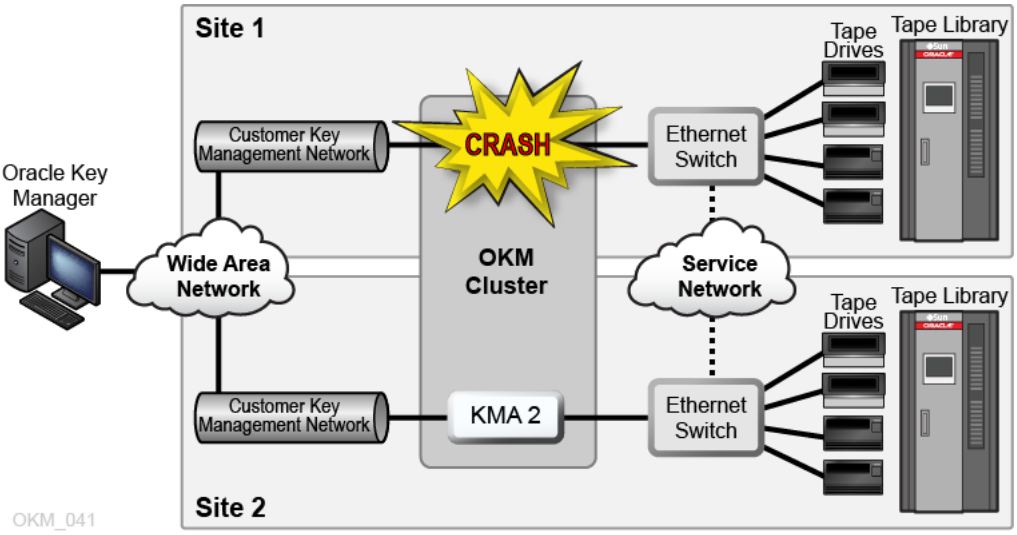


Dual Sites OKM Configuration with Disaster Recovery

Having multiple geographically disperse sites form the cluster reduces the risk of a disaster destroying the entire cluster.

In the figure below, there are two wide area networks — one for key management and one for service. The OKM GUI communicates with both KMAs in the cluster, and the service wide area network allows either KMA to communicate with the agents.

Figure 1-5 Disaster Recovery Configuration



Multiple Sites OKM Configuration with Partitioned Library

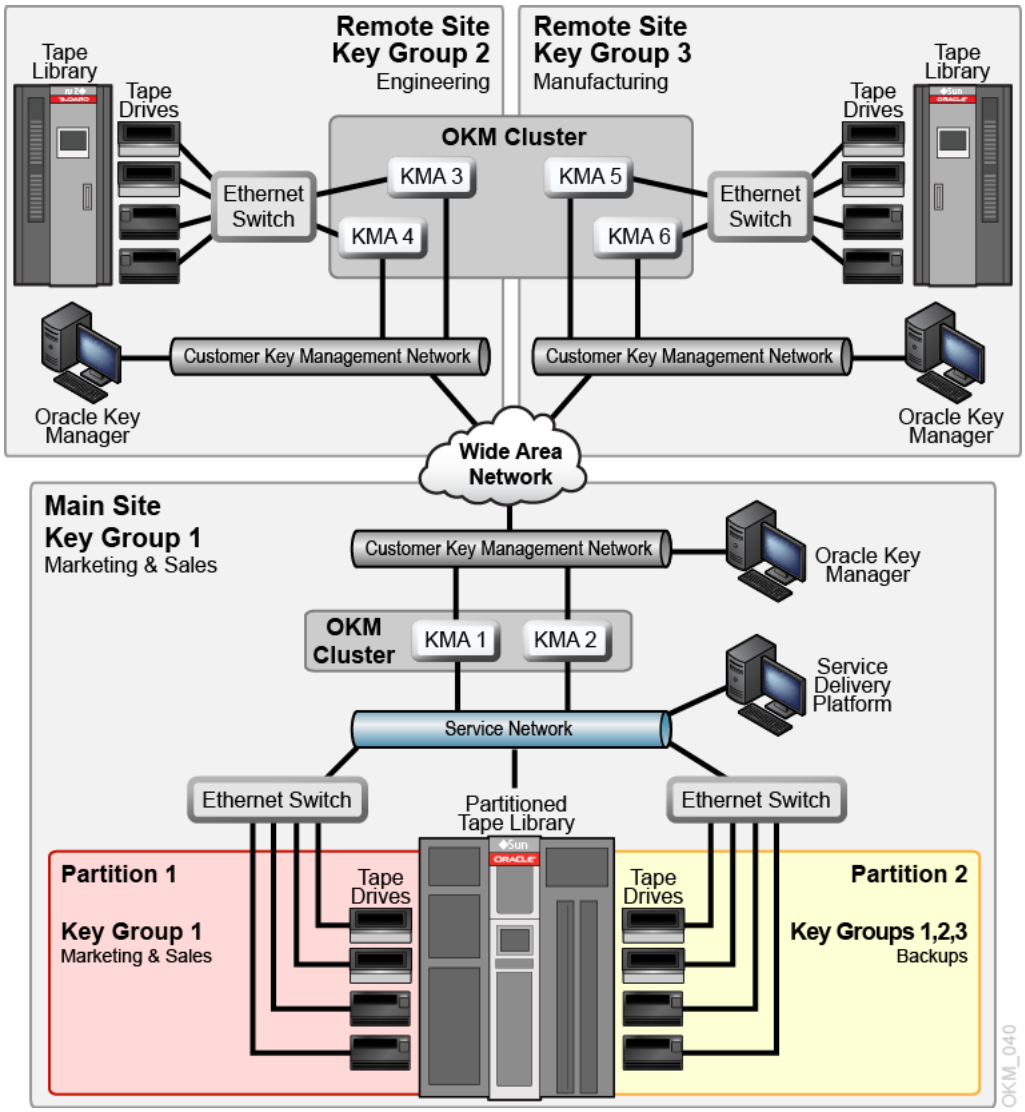
When using encryption-capable tape drives, partitions can add a layer of data security. Partitions can:

- Limit access to tape drives and data cartridges.
- Separate different encryption key groups.
- Isolate clients as service centers.
- Be dedicated for specific tasks.
- Give multiple departments, organizations, and companies access to appropriate sized library resources.

The figure below shows two remote sites and a local (main) site, all within one OKM cluster. The main site contains a partitioned library with specific key groups that provide backup facilities for all the KMAs (1–6) and media within the cluster.

For more information about partitioning, see the tape library's documentation.

Figure 1-6 Multiple Site Configuration



Agents (Encryption Endpoints)

Agents are devices or applications that use cryptographic keys to encrypt and decrypt data.

Agents obtain encryption key material from OKM over a secure (TLS) session and communicate with KMAs through the agent API (a set of software interfaces incorporated into the agent hardware or software). See How Agents Retrieve Keys from a KMA.

Agents must remain connected to the OKM network in the event an encryption key is needed. KMAs and agents can be logically grouped to create a site, where agents reference KMAs within the site to which they are assigned. Always install and test encryption end points before adding the encryption capability to them.

Types of endpoints include:

- Oracle Database with Transparent Data Encryption (TDE)
- Oracle Solaris 11 ZFS Encryption
- ZFS Storage Appliance
- Java Applications using Java Cryptographic Extension Provider
- Encryption Capable Tape Drives

See also: Enroll Agents.

How Agents Retrieve Keys from a KMA

Agents retrieve keys from the KMA cluster through discovery, load balancing, and failover.

Discovery

Agents (encryption endpoints) send a discover cluster request to a KMA. The KMA that receives the discover cluster request provides the following information for each KMA: IP addresses (IPv4 and IPv6), Site Name, KMA ID, KMA Name, KMA Version, KMA Status. The status can be either responding (indicates if the KMA is responding on the network) or locked (indicates if the KMA is currently locked).

Agents periodically retrieve this information as part of a key request operation (not when the endpoint is idle) and always request it as part of enrollment and whenever the agent is IPLed. Whenever an agent discovers a new response state for a KMA, it updates the cluster information with the new status.

Load Balancing

During normal operations, agents use their local table of cluster information to select a KMA for key retrieval. The agents use an algorithm to select a KMA from the same site as the agent. If all KMAs within a site are either locked or not responding, then the agents attempts to access a KMA from another site. If KMAs from other sites cannot be reached, the attempt to retrieve keys will time out and force a failover.

Failover

The ability for agents to failover to remote sites can improve agent reliability and availability when local KMAs are down or slow to respond (such as timeout situations because of heavy workloads).

Whenever an agent cannot communicate with any of the KMAs in a cluster, the agent then uses an algorithm to select a KMA for a failover attempt. When selecting, the agent's information about the cluster state is used again. agents attempt a failover up to three times before giving up and returning an error to the host application.

An agent may occasionally choose a non-responding KMA during a failover attempt if all other KMAs are not responding. However, because information about the cluster may be stale, the KMA may actually be online and responding

Oracle Database with Transparent Data Encryption (TDE)

Use OKM with Transparent Data Encryption (TDE) to manage encryption or decryption of sensitive database information.

Transparent Data Encryption, a feature of Oracle Database 11gR2 and higher, provides database encryption and decryption services for:

- Oracle Database products
- Oracle Real Application Clusters (Oracle RAC)
- Oracle Data Guard
- Oracle Extended Database Machine
- Oracle Recovery Manager (RMAN)
- Oracle Data Pump

Refer to Advanced Security Transparent Data Encryption (TDE). For more information, see the white paper *Oracle Advanced Security Transparent Data Encryption Best Practices* (http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf).

Oracle Solaris 11 ZFS Encryption

Use OKM with Oracle Solaris 11 ZFS to manage encryption and decryption of files in ZFS storage pools.

You can configure ZFS to use OKM's PKCS#11 provider, pkcs11_kms, to retrieve encryption keys from an OKM cluster. This requires a configured OKM cluster and a Solaris 11 system with established connectivity to KMAs in this OKM cluster. Once a Solaris 11 administrator installs and configures pkcs11_kms, the administrator can request that pkcs11_kms create a key, and then direct ZFS to use it.

ZFS Storage Appliance

The Oracle ZFS Storage Appliance supports encrypted storage using OKM for protection of its encryption keys. It supports KMAs running OKM 2.5.2 and later.

See the ZFSSA product documentation for more details.

http://docs.oracle.com/en/storage/#nas

Java Applications using Java Cryptographic Extension Provider

The Java Cryptographic Extension Provider for Oracle Key Manager (OKM JCE Provider) implements the KeyGenerator, KeyStore, and Cipher services. It enables Java applications (running Oracle's HotSpot JRE version 7 and version 8) written to the Java Cryptography Architecture (JCA) interface to create, retrieve, utilize, and destroy symmetric encryption keys through an OKM cluster. This Provider implements the subset of JCE's capabilities germaine to OKM.

The OKM JCE Provider version 1.3 is compatible with Oracle Java Runtime Environment version 7 and version 8. It supports only KMAs that are running OKM 3.0.2 and later.

You can download the OKM JCE Provider from the My Oracle Support site where it is published as Patch ID 26915167.

Encryption Capable Tape Drives

Only specific tape drive models and types support encryption with OKM.

- StorageTek T10000A
- StorageTek T10000B
- StorageTek T10000C
- StorageTek T10000D
- StorageTek T9840D
- HP LTO-4 (requires HP Dione card)
- HP LTO-5 and 6
- IBM LTO-4, 5, 6, 7 and 8 (all require an encryption card)

See also: Enroll Tape Drives .

Table 1-1 FIPS 140-2 Compliant Tape Drives

Tape Drive	FIPS 140-2 Level
T10000A	1
T10000B	2
T10000C	1
T10000D	1
T9840D	1
LTO4 (HP and IBM)	No plans for FIPS
LTO5 (HP and IBM)	No plans for FIPS
LTO6 (HP and IBM)	No plans for FIPS
LTO7 (IBM)	No plans for FIPS
LTO8 (IBM)	No plans for FIPS

Note:

LTO drives alone may be FIPS-validated, but not necessarily in specific encryption applications.

FIPS 140-2 levels of security for the above tape drives include:

- Level 1 – The basic level with production-grade requirements.
- Level 2 – Adds requirements for physical tamper evidence and role-based authentication. Built on a validated operating platform. This selection provides a higher level of security for the KMAs and tape drives.

T-series Tape Drive Encryption Behavior

T10000C and T10000D drives running firmware versions 1.57.30x (T10000C) or 4.06.106 (T10000D) and later do not require encryption enablement keys. For earlier drives and firmware versions, the Oracle support representative must request an encryption license key for each drive.

Table 1-2 T-Series Tape Drive Encryption Behavior

Tape Drive Type	Non-encrypted Tapes	Encrypted Tapes
Not enrolled for encryption	• Fully compatible • Read, write, and append	• Not capable of reading, writing, or appending • Can re-write from the beginning of tape (BOT)
Enrolled for encryption	• Read capability only • Not capable of appending • Can re-write from the beginning-of-tape (BOT)	• Fully compatible • Read with correct keys • Write with current write key

LTO Tape Drive Encryption Behavior

There are no enablement or drive data requirements for LTO tape drives. The only preparation is to ensure you have the information to assign the IP addresses and agent names for the tape drives in OKM manager.

LTO-8 drives can read and write one generation back. LTO-5, 6, and 7 drives can read two generations back and write one generation back. For best capacity and performance, always use cartridges of the same generation as your drives.

Table 1-3 LTO 5,6,7 and 8 Encryption Behavior

Drive Behavior	Functionality for Drive Not Enrolled for Encryption	Functionality for Drive Enrolled for Encryption
Read same generation non-encryption data	OK non-encrypted	OK non-encryption
Read same generation *encrypted* data	Error	OK encrypted if correct key available.
Write same generation from BOT	OK non-encrypted	OK encrypted.
Append write same generation *encrypted* data	N/A	OK encrypted if correct key available
Read one generation backwards non-encrypted data	OK non-encrypted	OK non-encrypted
Read one generation backwards *encrypted* data	Error	OK encrypted if correct key available
Write one generation backwards from BOT	OK non-encrypted	OK encrypted.
Append write one generation backwards *encrypted* data	N/A	OK encrypted if correct key available

Table 1-3 (Cont.) LTO 5,6,7 and 8 Encryption Behavior

Drive Behavior	Functionality for Drive Not Enrolled for Encryption	Functionality for Drive Enrolled for Encryption
Read two generations backwards non-encrypted data (does not apply to LTO-8 drives)	OK non-encrypted	OK non-encrypted
Read two generations backwards *encrypted* data (does not apply to LTO-8 drives)	Error	OK encrypted if correct key available
Append write same generation to non-encrypted data (Space EOD, Read to EOD, and write)	OK non-encrypted	IBM: Mixing of encrypted and non-encrypted data on a single tape not allowed. HP: OK encrypted if correct key available
Append write same generation to *encrypted* data (Space EOD, Read to EOD, and write)	Space EOD = OK non-encrypted Read to EOD = Error	IBM: OK encrypted if the correct key is available, but with the proper read key. HP: OK encrypted if correct key available
Append write one generation back to non-encrypted Data (Space EOD, Read to EOD, and write)	OK non-encrypted	IBM: Mixing of encrypted and non-encrypted data on a single tape not allowed. HP: OK encrypted if correct key available
Append write one generation back to *encrypted* data (Space EOD, Read to EOD, and write)	Space EOD = OK non-encrypted Read to EOD = Error	IBM: OK encrypted if the correct key is available, but with the proper read key. HP: OK encrypted if correct key available

Updating Tape Drive Firmware

Keep all drive firmware up-to-date to access to the latest features and fixes.

1. Go to My Oracle Support at: `http://support.oracle.com` and sign in.
2. Click the **Patches & Updates** tab.
3. Click **Product or Family (Advanced).**
4. In the **Start Typing...** field, type in the product information (for example, "Oracle Key Manager"), and click **Search** to see the latest firmware for each release.

The firmware levels listed are subject to change. Visit Oracle Support to access the latest firmware.

Table 1-4 Firmware Compatibilities

Drive	SL8500	SL4000	SL3000	SL500	SL150
T10000D	L–FRS_8.0.5 (no 3590 drive support) D (FC) – 4.06.107 D (FICON) – 4.07.xxx	L -1.0.0.65.27025 D – 4.15.102	L–FRS_3.62 (no 3590 drive support) D (FC) – 4.06.107 D (FICON) – 4.07.xxx	NA	NA
T10000C	L–FRS_7.0.0 D–1.53.316	L -1.0.0.65.27025 D – 3.66.101	L–FRS_3.0.0 D–1.53.316	NA	NA
T10000B	L–3.98b D–1.38.x09	NA	L–FRS_2.00 D (FC) – 1.38.x07 D (FICON) – 1.38.x09	NA	NA
T10000A	L–3.11c D (FC) – 1.37.113 D (FICON) – 1.37.114	NA	L–FRS_2.00 D (FC) – 1.37.113 D (FICON) – 1.37.114	NA	NA
T9840D	L–3.98 D–1.42.x07	NA	L–FRS_2.00 D–1.42.x07	NA	NA
LTO-8	L–8.60 D (IBM) - HB82	L–1.0.0.65.27025 D (IBM) - HB82	L–4.50 D (IBM) - HB82	NA	L–3.50 (LME) D (IBM) - HB83
LTO-7	L-8.60 D (IBM) - HB82	L-1.0.0.68.29240 D (IBM) - HB82	L-4.50 D (IBM) - HB82	NA	L-3.50 (LME) D (IBM) - HB83
LTO-6	L–8.01 D (IBM) - CT94 D (HP) - J2AS	L–1.0.0.65.27025 D (IBM) - G9P2 D (HP) - J5MS	L–4.0 D (IBM) - CT94 D (HP) - J2AS	L–1483 D (IBM) - BBNH D (HP) - J2AS NA for SAS	L -2.50 D (HP) –33ES SAS D (HP) –23DS FC D (IBM) -E6RF FC and SAS without OKM compatibility
LTO-5	D(IBM) - BBNH D (HP) - I5BS	L–1.0.0.65.27025 D (IBM) - G350 D (HP) - I6PS	D (IBM) - BBNH D (HP) - I5BS	L–1373 D (IBM) - BBNH D (HP) - I5BS	IBM - NA L (HP) – 1.80 D (HP) –Z68S SAS D (HP) –Y68S FC

Table 1-4 (Cont.) Firmware Compatibilities

Drive	SL8500	SL4000	SL3000	SL500	SL150
LTO-4	L–FRS_4.70 D (IBM) - BBH4 D (HP) - H64S	NA	L–FRS_2.30 D (IBM) - BBH4 D (HP) - H64S	L–1373 D (IBM) - BBH4 D (HP) - H64S	NA

Legend:

L – library firmware level
D – drive firmware level
FC– Fibre Channel
NA – Not Applicable. Not supported.

Note:

If you use Multi-Drive Virtual Operator Panel (MD-VOP), version 1.1 (minimum) is required. It is recommended that you use the most current version of MD-VOP.

Table 1-5 Minimum Virtual Op Panel (VOP) Version

Tape Drive	Minimum VOP Version
T10000A, B, C, D	1.0.18
T9840D	1.0.12
HP LTO-4	1.0.12
HP LTO-5	1.0.16
HP LTO-6	1.0.18
IBM LTO-4	1.0.14
IBM LTO-5	1.0.16
IBM LTO-6	1.0.18
IBM LTO-7	MD-VOP 2.4.1
IBM LTO-8	MD-VOP 2.4.1

Key Management Appliance

A Key Management Appliance (KMA) is a server node within an OKM cluster. OKM has been released on numerous hardware platforms. Only specific versions of OKM are supported on certain hardware platforms.

The KMA delivers policy-based lifecycle key management, authentication, access control, and key provisioning services. The KMA ensures that all storage devices are registered and authenticated, and that all encryption key creation, provisioning, and deletion is in accordance with prescribed policies.

Table 1-6 OKM Support for Each Server Platform

Hardware Platform	Supported OKM Version
SPARC T8-1	OKM 3.3.2
SPARC T7-1	OKM 3.1 - 3.3.2
Netra SPARC T4-1	OKM 3.0 - 3.3.2
Sun Fire X4170 M2	OKM 2.3 - 2.5.3, OKM 3.0.2 - 3.3.2
Sun Fire X2200 M2	OKM 2.1 - 2.5.3, OKM 3.0.2
Sun Fire X2100 M2	OKM 2.1 - 2.5.3, OKM 3.0.2

For installation and configuration of the Sun Fire KMAs, refer to the OKM 2.5 documentation.

SPARC T8-1 Server

OKM 3.3.2 introduced the SPARC T8-1 server as the OKM hardware platform.

The OKM hardware configuration of this server includes:

- 4.13 GHz 32-core SPARC M7 Processor
- 128 GB of DRAM
- 1.2 TB disk drive with Solaris and OKM pre-installed
- Four 10 Gigabit Ethernet ports
- Redundant power supplies
- Six PCIe Gen 3 adapter slots (8 lanes each)

For other server specifications, including environment and power requirements, see: https://docs.oracle.com/cd/E79179_01/

SPARC T7-1 Server

OKM 3.1 introduced the SPARC T7-1 server as the OKM hardware platform.

The OKM hardware configuration of this server includes:

- 4.13 GHz 32-core SPARC M7 Processor
- 128 GB of DRAM
- 600 GB disk drive (if manufactured before October 2018) or 1.2 TB disk drive (if manufactured after October 2018) with Solaris and OKM pre-installed.
- Four 10 Gigabit Ethernet ports
- Redundant power supplies
- Six PCIe Gen 3 adapter slots (8 lanes each)

For other server specifications, including environment and power requirements, see: http://docs.oracle.com/cd/E54976_01/index.html

Netra SPARC T4-1

OKM 3.0 introduced the Netra SPARC T4-1 server as the OKM hardware platform.

The OKM hardware configuration of this server includes:

- 2.85 GHz four-core SPARC T4 Processor
- 32 GB of DRAM (four 8 GB DIMMs)
- 600 GB SAS 10K RPM 2.5-inch disk drive with Solaris and OKM pre-installed
- Four Gigabit Ethernet ports
- Redundant power supplies
- Five PCIe Gen 2 adapter slots (8 lanes each)
- DVD drive (disabled — not used with OKM)

For other server specifications, including environment and power requirements, see: http://docs.oracle.com/cd/E23203_01/index.html

Cryptographic Card for KMA

Pre-install or add a cryptographic card to the KMA to provide a FIPS 140-2 Level 3 certified cryptographic device.

The cryptographic card may sometimes be referred to as the Hardware Security Module (HSM). See the *Oracle Key Manager Security Guide* for more information.

SPARC KMAs running OKM 3.3 or later use the Thales nShield Solo PCIe card.

Sun Fire KMAs and SPARC KMAs running a release before OKM 3.3 use the Sun Cryptographic Accelerator (SCA) 6000 card . The firmware on the SCA 6000 card had previously undergone FIPS 140-2 Level 3 certification. However, this certification has been revoked as of December 31, 2015, and is no longer certified.

Thales Smart Card and Smart Card Reader

A smart card reader and smart card come with the Thales nSheild Solo+ installation kit. Retain the smart card and reader for installing and servicing the Thales card.

The customer should retain the smart card reader device and associated smart cards in the event the Thales card requires service. The Thales card operates securely without the smart cards once OKM has been configured to use the cryptographic card. Therefore, there is no security risk is an unauthorized individual acquires access to the smart cards.

Networking

OKM uses TCP/IP networking (dual stack IPv4 and IPv6) for the connections between KMAs, agents, and workstations.

Tape drive agents should not be on public networks. Connect tape drive agents to KMAs in a private service network.

- Network Connections on the KMA

- Managed Switches
- Network Routing Configuration

Network Connections on the KMA

Each KMA has connections for the management network, service network, and ILOM.

The figure below shows the KMA network connections for the SPARC T7-1. The KMA network connections on a SPARC T8-1 are similar.

> **Note:**
>
> Each Ethernet connection requires an IP address. Addresses not assigned using DHCP must be static.

Figure 1-7 KMA Network Connections Example — SPARC T7-1

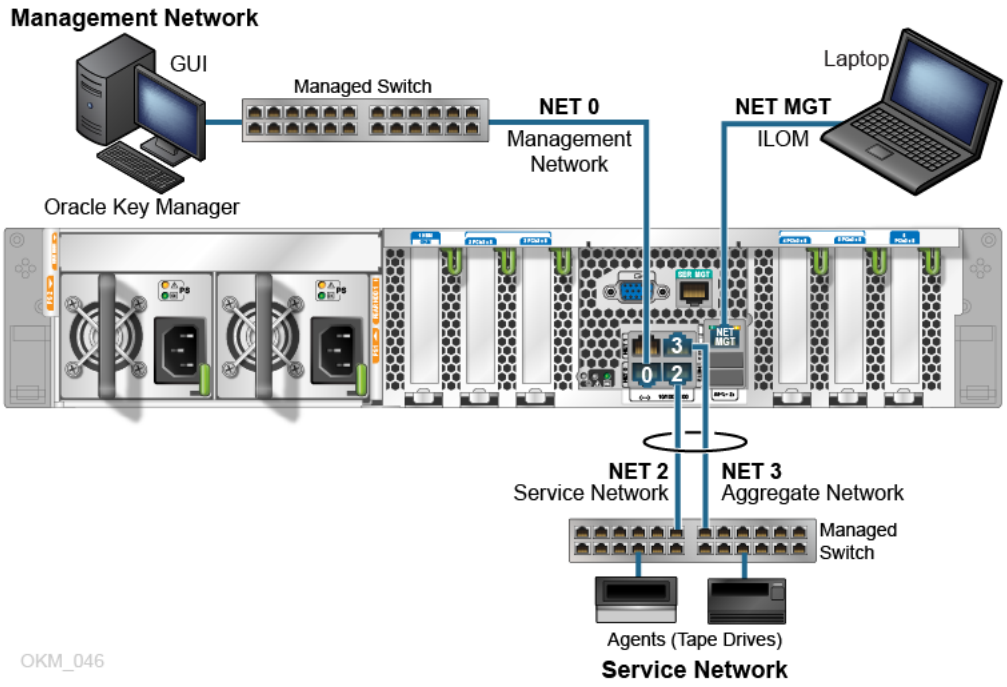


Table 1-7 KMA Network Connections - T8-1, T7-1, T4-1, and X4170 M2

Port	Connects To	Description
SER MGT	Service Rep Laptop	Serial connection to the ILOM. The ILOM IP address is most easily configured using this connection.
NET MGT	Service Rep Laptop	Optional Ethernet connection to the ILOM. This port is not available until you configure the ILOM IP address.

Table 1-7 (Cont.) KMA Network Connections - T8-1, T7-1, T4-1, and X4170 M2

Port	Connects To	Description
NET 0	OKM GUI	Required connection to the Management Network. This network connects the server to the OKM GUI as well as to other KMAs in the cluster. The Management Network can be local, remote, or a combination of both. Customers are expected to provide the management network.
NET 2	Service Network	Required connection to the Service Network. This network connects the server to the tape drives, either directly or through Ethernet switches.
NET 3	Aggregate Network	Optional connection to the Aggregated Network and provides aggregation with NET 2.

Management Network

The management network connects the KMA to other KMAs in the cluster for peer-to-peer replication.

The OKM Manager GUI, CLI, and other admin tools (such as Remote Console, Oracle Enterprise Manager, and SNMP) use the management network. Customers are expected to provide the management network. Use a gigabit Ethernet, or faster, connection for optimal replication and performance.

Agents may also connect to the management network if the service network is inappropriate due to its isolation properties. For additional security and to isolate LAN traffic, you may want to use Virtual Local Area Networks (VLANs) to connect to the management network.

Service Network and Port Aggregation

The service network connects the OKM cluster to the agents and isolates key retrievals from other network traffic. The physical ports of the KMA can optionally be aggregated into a single virtual port.

Agents may connect to the OKM cluster by the management network, if desired.

You can optionally aggregate the physical Ethernet interfaces of the service network (NET 2/LAN 2 and NET3/LAN 3) into a single virtual interface. Aggregating these ports provides additional availability — if a failure occurs with either port, the other port maintains connectivity. Make sure the Ethernet switch ports have the correct configuration:

- Set to auto negotiate settings for duplex (should be full duplex).
- Set to auto negotiate speed settings, the KMA ports are capable of gigabit speeds.
- Using identical speeds, such as: both set to 100 Mbps (auto speed negotiating may work fine).

> **Note:**
>
> - There may be an order or connection dependency. Create the aggregation group on the switch *before* connecting the KMAs service port.
> - If the aggregated IP address (IPv4 or IPv6) is not responding, reboot the KMA.

A System Dump using the Management GUI will contain aggregated port information. The information is gathered using `dladm` commands.

Managed Switches

Oracle recommends a managed switch for connecting KMAs to encryption agents on private service networks. A managed switch supplies connectivity to unmanaged switches and to routers for the wide area service network.

Managed switches:

- Improve serviceability through better switch diagnostics and service network troubleshooting.
- Can minimize single points of failure on the service network through use of redundant connections and spanning tree protocol.
- Provide support for aggregation of the KMA service network interfaces to minimize single point of failure on the KMA's service interface.

Supported Managed Switch Models:

- Brocade ICX 6430 Switch (included in the Switch Accessory Kit)
- 3COM Switch 4500G 24-Port (3CR17761-91)
- Extreme Networks Summit X150-24t Switch Other managed switches can be used but engineering only provides configuration guidance on the switches above.

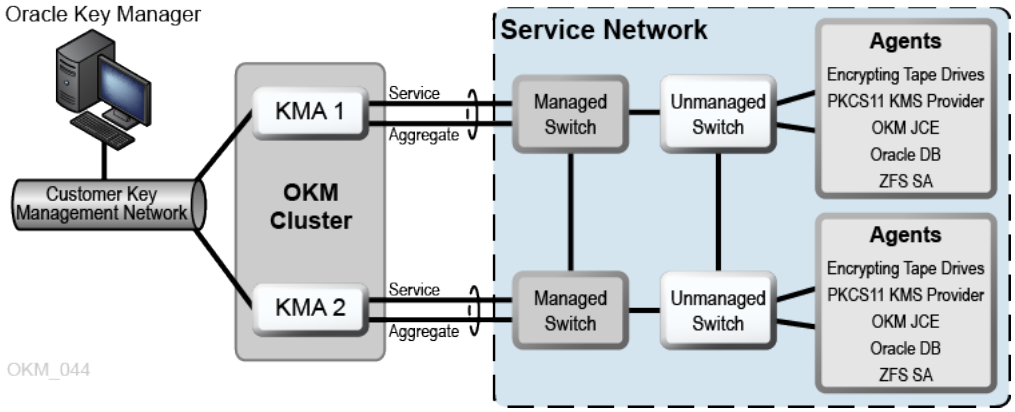
Port Mirroring

You can mirror ports to use a network analyzer in the service network. Ports can be mirrored on Brocade ICX 6430 switches. For configuration instructions, consult Brocade ICX 6430 Switch Configuration.

Managed Switch Configuration Example

In a managed switch configuration, if either a KMA or managed switch should fail, the agents still have a communication path to the other KMA. The managed switches are connected to unmanaged switches containing redundant paths requiring a spanning tree configuration. (Managed switches must be enabled for spanning tree whenever the cabling includes redundancy.) The service network interfaces are aggregated into a single virtual interface (see Service Network and Port Aggregation).

Figure 1-8 Managed Switch Configuration



Network Routing Configuration

Properly configure the network routing to prevent errors.

The routing configuration of a KMA affects responses to agent discovery requests. Mistakes in the routing configuration can lead to erroneous cluster information being provided to agents. This could cause agents to attempt communication with KMAs that they cannot reach over the network.

When planning the OKM network, observe the following:

- Use the KMA console network menu option to configure a route between sites. Do not configure a default route.

> **Note:**
>
> Oracle does not recommend starting with a multi-site service network topology.

- When planning for a multi-site service network, determine a subnet addressing scheme for the KMA service ports and drives. You must avoid duplicate network addresses and use of 172.18.18.x networks (a common convention).
- Use of default gateway settings can affect failover performance. Consult a network engineer to plan for failover capability.

Part Numbers for OKM Components

Table 1-8 KMA Server Order Numbers

Order Number	Description
7115065	Oracle Key Manager 3
7114954	Hardware Security Module - 140-2 PCIe Card (SCA 6000) with FIPS support and level 3 security (for factory installation).

Table 1-8 (Cont.) KMA Server Order Numbers

Order Number	Description
7115395	Hardware Security Module - 140-2 PCIe Card (Thales) with FIPS support and level 3 security. This hardware security module is compatible with SPARC KMAs only.

Table 1-9 Switch Accessory Kit Order Numbers

Order Number	Description
7104584	Switch Accessory Kit (SAK). Includes 24-port managed switch and a rack power cord, two Ethernet cables, and switch mounting hardware.

The switch can support a maximum of 22 tape drive agents. Additional switch accessory kits might be needed depending on the number of encrypting tape drives supported by the library.

Order Ethernet cables to connect the switch to encrypting tape drives.

Table 1-10 Ethernet Cable Order Numbers

Order Number	Description
CABLE10187033-Z-A	8 feet CAT5e Ethernet cable (for factory installation)
CABLE10187033-Z-N	8 feet CAT5e Ethernet cable
CABLE10187034-Z-A	35 feet CAT5e Ethernet cable (for factory installation)
CABLE10187034-Z-N	35 feet CAT5e Ethernet cable
CABLE10187037-Z-A	55 feet CAT5e Ethernet cable (for factory installation)
CABLE10187037-Z-N	55 feet CAT5e Ethernet cable

Table 1-11 Power Cable Part Numbers

ATO Power Cord	PTO Equivalent	Description	Amps	Voltage	Cable
333A-25-10-AR	X312F-N	Pwrcord, Argentina, 2.5m, IRAM2073, 10A,C13	10	250	180-1999-02
333A-25-10-AU	X386L-N	Pwrcord, Australian, 2.5m, SA3112, 10A,C13	10	250	180-1998-02
333A-25-10-BR	X333A-25-10-BR-N	Pwrcord, Brazil,2.5m,NBR14136, 10A, C13	10	250	180-2296-01
333A-25-10-CH	X314L-N	Pwrcord, Swiss,2.5m,SEV1011, 10A, C13	10	250	180-1994-02
333A-25-10-CN	X328L	Pwrcord, China,2.5m,GB2099, 10A, C13	10	250	180-1982-02
333A-25-10-DK	X383L-N	Pwrcord, Denmark,2.5m, DEMKO107, 10A,C13	10	250	180-1995-02
333A-25-10-EURO	X312L-N	Pwrcord, Euro,2.5m,CEE7/VII,10A, C13	10	250	180-1993-02

Table 1-11 (Cont.) Power Cable Part Numbers

ATO Power Cord	PTO Equivalent	Description	Amps	Voltage	Cable
333A-25-10-IL	X333A-25-10-IL-N	Pwrcord, Israel,2.5m,SI-32, 10A,C13	10	250	180-2130-02
333A-25-10-IN	X333A-25-10-IN-N	Pwrcord, India,2.5m,IS1293,10A,C13	10	250	180-2449-01
333A-25-10-IT	X384L-N	Pwrcord, Italian,2.5m,CEI23, 10A,C13	10	250	180-1996-02
333A-25-10-KR	X312G-N	Pwrcord, Korea,2.5m,KSC8305,10A, C13	10	250	180-1662-03
333A-25-10-TW	X332A-N	Pwrcord, Taiwan,2.5m, CNS10917, 10A, C13	10	125	180-2121-02
333A-25-10-UK	X317L-N	Pwrcord, UK,2.5m,BS1363A, 10A,C13	10	250	180-1997-02
333A-25-10-ZA	X333A-25-10-ZA-N	Pwrcord, South Africa,2.5m,SANS164, 10A,C13	10	250	180-2298-01
333A-25-15-JP	X333A-25-15-JP-N	Pwrcord, Japan,2.5m,PSE5-15, 15A, C13	15	125	180-2243-01
333A-25-15-NEMA	X311L	Pwrcord, N.A./Asia,2.5m, 5-15P,15A, C13	15	125	180-1097-02
333A-25-15-TW	X333A-25-15-TW-N	Pwrcord, Taiwan,2.5M, CNS10917, 15A,C13	15	125	180-2333-01
333F-20-10-NEMA	X320A-N	Pwrcord, N.A./Asia,2.0m, 6-15P,10A, C13	10	250	180-2164-01
333F-25-15-JP	X333F-25-15-JP-N	Pwrcord, Japan,2.5m,PSE6-15, 15A, C13	15	250	180-2244-01
333J-40-15-NEMA	X336L	Pwrcord, N.A./Asia,4.0m, L6-20P,15A, C13	15	250	180-2070-01
333R-40-10-309	X332T	Pwrcord, INTL,4.0m, IEC309-IP44, 10A,C13	10	250	180-2071-01

Table 1-12 Oracle Rack II (Redwood) Power Cord Part Numbers

ATO Power Cord	PTO Equivalent	Description	Amps	Voltage	Cable
SR-JUMP-1MC13	XSR-JUMP-1MC13-N	Pwrcord, Jmpr,SR2,1.0m,C14RA, 13A, C13	13	250	180-2379-01
SR-JUMP-2MC13	XSR-JUMP-2MC13-N	Pwrcord, Jmpr,SR2,2.0m,C14RA, 13A, C13	13	250	180-2380-01

Table 1-13 Oracle Rack (NGR) Power Cord Part Numbers

ATO Power Cord	PTO Equivalent	Description	Amps	Voltage	Cable
333W-10-13-C14RA	X9237-1-A-N	Pwrcord, Jmpr,1.0m,C14RA,13A,C13	13	250	180-2082-01

Table 1-13 (Cont.) Oracle Rack (NGR) Power Cord Part Numbers

ATO Power Cord	PTO Equivalent	Description	Amps	Voltage	Cable
333W-25-13-C14RA	X9238-1-A-N	Pwrcord, Jmpr,2.5m,C14RA,13A,C13	13	250	180-2085-01

Table 1-14 Non-Oracle Rack Power Cord Part Numbers

ATO Power Cord	PTO Equivalent	Description	Amps	Voltage	Cable
333V-20-15-C14	X333V-20-15-C14-N	Pwrcord, Jmpr,Straight,2.0m,C14,15A, C13	15	250	180-2442-01
333V-30-15-C14	X333V-30-15-C14-N	Pwrcord, Jmpr,Straight,3.0m,C14,15A, C13	15	250	180-2443-01

2
Install the KMA

Use these procedures to install SPARC KMAs and initially configure the ILOM. For Sun Fire KMA installation, refer to the OKM 2.5 documentation.

> **Caution:**
>
> Installation is a two person task due to the weight of the server. Attempting installation alone could result in injury or equipment damage.

Prepare for the Installation

Make sure the installation site is ready, the hardware is acclimated, and the installation tools are available before installing the KMA.

Installation Planning Checklist

Use this checklist to make sure you have properly planned for the installation.

Review OKM Configurations:

- See Sample OKM Cluster Configurations

Review Server Requirements:

- Review the KMA server specifications (Key Management Appliance).
- Review KMA rack specifications (Verify the Rack Meets the Specifications for Installing a KMA).

- Ensure the site meets temperature, humidity, cooling, and power requirements for the server.
  - For the SPARC T8-1 server specifications, see: https://docs.oracle.com/cd/E79179_01/
  - For the SPARC T7-1 server specifications, see: http://docs.oracle.com/cd/E54976_01/
  - Verify the circuit breaker locations and ratings.
  - For the redundant power option, ensure there is an additional APC power switch.
- Have the customer consider applying tamper evident security labels to each KMA. Customers are responsible for acquiring these labels.

Review Network Requirements:

- See Networking

Review Agent Requirements:

- See Agents (Encryption Endpoints)

Plan User Roles:

- See Available Roles
- See Valid Operations for Each Role

Prepare for Delivery:

- Ensure authorized personnel are available to handle and accept delivery. The OKM Key Management Appliance (KMA) is considered a secure item.
- Ensure there is a plan to dispose of or recycle packing material.

Order Components:

- Select Part Numbers for OKM Components

Verify or Obtain a Cryptographic Card

The optional cryptographic card provides a FIPS 140-2 Level 3 certified cryptographic device.

If you wish to use a cryptographic card with the KMA, check to see if one is already installed. If not, obtain the card (SCA 6000 or Thales nShield Solo+).

See also: Cryptographic Card for KMA.

Verify the Site is Ready for Installation

Survey the installation site and make sure it meets all requirements.

Ensure that the installation site has the following:

- Sufficient space to install and maintain the servers.
- Trained representatives to install the equipment. More than one person might be required to install equipment in the rack or to remove equipment from the rack.

- Correct configuration and versions of firmware available for tape drive encryption end points (see Table 1-4).
- Rack suitable for KMA installation.

Verify the Rack Meets the Specifications for Installing a KMA

Verify the rack is compatible before installing the KMA. The rack should be a standard, RETMA 19-inch, four post rack or cabinet.

> **Note:**
>
> Two-post racks are not supported by the T7-1 or T8-1 servers. The T4-1 server can be installed in a four post or two post rack or cabinet.

Only 9.5 mm square hole and M6 round mounting holes are supported.

The sliding rails are compatible with racks which meet the following standards:

- Horizontal opening and unit vertical pitch conforming to ANSI/EIA 310-D-1992 or IEC 60927 standards.
- Distance between front and rear mounting planes between 610 mm and 915 mm (24 in. to 36 in.).
- Clearance depth to a front cabinet door must be at least 27 mm (1.06 in.).
- Clearance depth to a rear cabinet door at least 900 mm (35.5 in.) to incorporate cable management or 700 mm (27.5 in.) without cable management.
- Clearance width between structural supports and cable troughs and between front and rear mounting planes is at least 456 mm (18 in.).

Provide adequate service clearance for rack components:

- Front service clearance 48.5 in. (1.23 m) minimum
- Rear service clearance 36 in. (914.4 mm) minimum

Consider the total weight when you place equipment into the rack. To prevent an unbalanced situation:

- Load equipment in a rack from the bottom to the top.
- Install the heaviest equipment on the bottom and the lightest on the top.
- Install an anti-tilt bar (if necessary) to provide additional stability.

Verify there is adequate cooling for the servers.

- Ensure that the temperature in the rack does not exceed the maximum ambient rated temperatures for all of the equipment installed in the rack.
- Ensure that there is adequate cooling to support *all* of the equipment in the rack.

Verify the rack has the proper power connections and ground.

- When removing power from any equipment, make sure it does not effect other equipment in the rack.

Acclimate the Equipment to the Environment

Allow the equipment to acclimate to the humidity and temperature of the installation environment to prevent equipment damage.

1. Acclimate the server to the installation environment. It is recommended that the server remain in the shipping crate for 24 hours.
2. To ensure no one tampers with the equipment while it sits, you can apply tamper evident security labels to the KMA top cover and to the hard disk drive so that tampering requires breaking the label.

Obtain Required Installation Tools

Obtain all necessary tools to facilitate a smooth installation.

- Standard field service tools including standard and Phillips screwdrivers, Torx driver and bits, and side cutters; tools necessary to mount the servers in a rack.
- Serial or null modem cable (PN: 24100134) with DB-9 connector.
- Adapter (PN: 10402019).
- Straight Ethernet cable (PN: 24100216) 10-ft.
- Cross-over Ethernet cable (PN: 24100163) 10-ft.
- Virtual Operator Panel — if encrypting tape drives you will need to enroll them with OKM. Minimum versions supporting tape drive models are listed in Table 1-5. Oracle recommends using the most current version of MD-VOP.
- Service laptop with support software.

Obtain Necessary Documentation

Make sure the installation team has a copy of all required documentation.

- *EIS Installation Checklist for Oracle Key Manager (OKM) 3.0 Tape Encryption Product* or a more current version.
- *EIS Installation Checklist for the Oracle Key Manager Switch Accessory Kit (Brocade ICX 6430)*

SPARC T8-1

SPARC T8 Series Servers Product Notes

SPARC T8 Series Servers Security Guide

SPARC T8-1 Installation Guide

SPARC T8 Series Servers Administration Guide

SPARC T8-1 Server Service Manual

`https://docs.oracle.com/cd/E79179_01/`

SPARC T7-1

SPARC T7 Series Servers Product Notes

SPARC T7 Series Security Guide

SPARC T7-1 Installation Guide

SPARC T7 Series Servers Administration Guide

SPARC T7-1 Server Service Manual

http://docs.oracle.com/cd/E54976_01/

Netra SPARC T4-1

Oracle ILOM Feature Updates and Release Notes Firmware Release 3.2

Oracle Netra SPARC T4-1 Server Product Notes

Oracle Netra SPARC T4-1 Server Installation Guide

Oracle Netra SPARC T4-1 Server Service Manual

http://docs.oracle.com/cd/E23203_01/index.html

Unpack and Inventory Contents

Unpack and verify the contents of any shipping containers. Make sure there is no physical damage or loose parts.

Verify that you have the following components:

- Key Management Appliance (server)
- If the KMA arrived with an *installed* cryptographic card, there should be a package labeled Additional Parts which contains the smart card and smart card reader. These parts cannot be ordered separately and need to be available to the service engineer if service is required post installation.
- Rack mount kit
- Power cables
- Switch accessory kit
  - Brocade ICX6430-24 switch
  - Rack mounting hardware
  - Rack power cord
  - Ethernet cables (2) CAT5E eight feet long

SPARC T7-1 or T8-1 Server Installation

This list is an overview of installing the SPARC T7-1 or T8-1 KMA. For complete installation instructions, use the server's *Installation Guide*.

Refer to the T8-1 Installation Guide at https://docs.oracle.com/cd/E79179_01/html/E80507/index.html.

Refer to the T7-1 Installation Guide at: https://docs.oracle.com/cd/E54976_01/html/E54979/index.html.

1. Acclimate the server to the installation environment. The server should remain in the shipping crate for at least 24 hours.
2. Prepare the KMA and rack for installation. Tasks include:
   - Stabilize a rack
   - Unpack the contents of the shipping crate.
   - Install the rackmount hardware
   - Attach slide rail assemblies to the rack
3. Install the server in the rack using the supplied hardware. Tasks include:
   - Install the server into the slide rail assemblies
   - (Optional) Prepare the cable management assembly (CMA) for installation
   - Attach the CMA to the server, if applicable
   - Verify operation of the slide rails and CMA
4. Connect cables to the KMA:
   - Serial cable to SER MGT port
   - Ethernet cable to the NET MGT post

     Caution:

     Do not apply power until instructed to do so.

     This appliance includes a service processor (SP) that is used to configure and boot the host server. To properly configure the host server and view SP messages, *do not apply power* to the server until you make the SP and host networking connections.

   - Power cord to the power supplies and to separate power sources

     Do not power on the KMA at this time.

     When you connect the power cords, the SP initializes and the power supply LEDs light. After a few minutes, the SP login prompt displays on the terminal device. At this time, the KMA is not initialized or powered on.
5. Install another KMA, if applicable.

Install the Cryptographic Card in a SPARC T7-1 or T8-1 Server

Install the optional Thales nShield Solo+ card into slot 5 of the KMA.

1. To access the slot to install the cryptographic card, follow the procedures in the server's service manual regarding Servicing PCIe Cards. This includes using an antistatic wrist strap, powering off the server, removing of power supply cords, extending the server to the maintenance position, and removing the top cover.
2. For the Thales nShield Solo+ card:
   - Attach the low profile bracket to the card. Refer to Chapter 4 of the *Thales e-Security nShield Solo Installation Guide* and the section titled "Fitting a module bracket."

- Verify the Mode switch has remained in the O position.

3. Install the cryptographic card in to slot 5 of the KMA.

Netra SPARC T4-1 Server Installation

For most installations, follow the *Netra SPARC T4-1 Server Installation Guide*. For a 19-in rack with 4-post sliding rails, you must modify the standard installation.

Find the *Netra SPARC T4-1 Server Installation Guide* in the server accessory kit or at: https://docs.oracle.com/cd/E23203_01/index.html.

For a 4-post sliding rail, the *Netra Installation Guide* has you secure the slide onto the short and long brackets at the front and rear of the rack. Instead, *use a medium bracket* rather than the short bracket. Use one of the following methods:

- Use M6 screws (452721200037) and M6 threaded strips (in the unlabeled bag) to securely attach the medium and large brackets to the rack. The M6 screws already have washers with them. With this approach, you can use the flat washers (452721200051) to attach the large bracket to the slide.
- Use 10-32 screws (452721200039), flat washers (452721200051), and 10-32 threaded strips in order to securely attach the medium and large brackets to the rack.

Install the T4-1 Server in a 19-Inch, 4-Post Sliding Rail Rack

Use these modified procedures when installing a 4-post sliding rail rack.

Follow the instructions in "Install the Server (19-inch, 4-Post Sliding Rail Rackmount Kit)" procedure in the *Netra SPARC T4-1 Server Installation Guide* until you come to the step to attach the short brackets. Use the steps below to install the medium bracket instead.

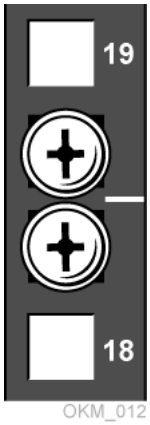
> **Note:**
>
> This process is much easier to perform if you have someone to assist you. Aligning the brackets in the rack may require one person in front of the rack and another in back.

1. Align the two screws and threaded strips so that they appear above and below a white line that separates unit markers (other racks might use a different indicator for the unit marker). This helps to line up the screw holes in the threaded strips with the square holes in the rack.

> **Note:**
>
> - If you used M6 screws and M6 threaded strips to attach the medium and large brackets to the rack, then you do not need to use extra 5 mm x 15 mm flat washers.
> - Alternatively, you may use extra 5 mm x 15 mm flat washers (similar to 452721200051 but not 5mm x 13mm) to attach the brackets to the slides. The 5mm x 15mm flat washers are too wide to fit side by side when you attach the brackets to the rack.

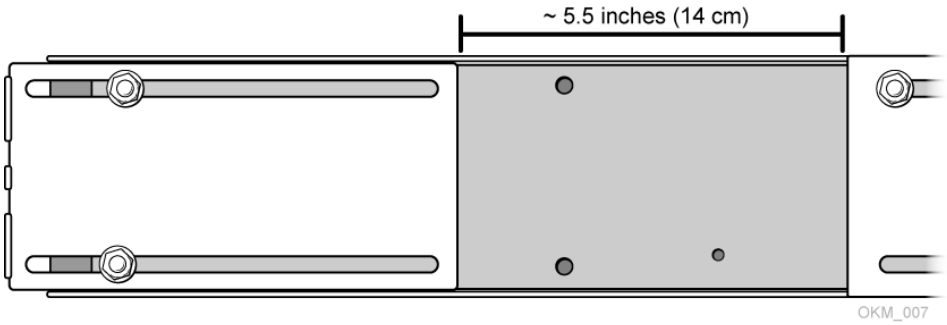
Refer to Figure 2-1 for an example of this alignment.

Figure 2-1 Example of Screw Alignment in Rack



2. Attach the medium and long brackets to the slide, spacing the two brackets approximately 140 mm (5.5 in.) apart. Attach the slide as far forward on the brackets as possible to be able to slide the server far enough out of the rack for servicing. Refer to Figure 2-2.

Figure 2-2 Medium/Long Bracket Attachment



3. Position the brackets and slide so that the long bracket is toward the rear of the rack and the brackets are inside the facings. Then fit the brackets between the facings and the threaded strips. They should fit fairly snugly between the facings of the rack; there should not be much horizontal *play*. Adjust them as needed.

The flat side of the brackets should line up with the edge on the rack. Tighten the rack screws moderately securely. See Figure 2-3 and Figure 2-4 for views of the rack.

Figure 2-3 View of Brackets at Front of Rack

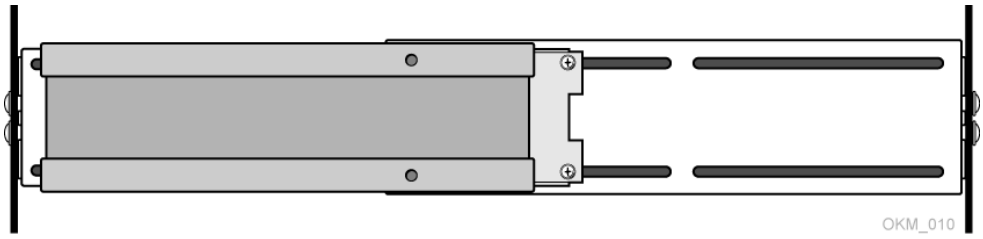
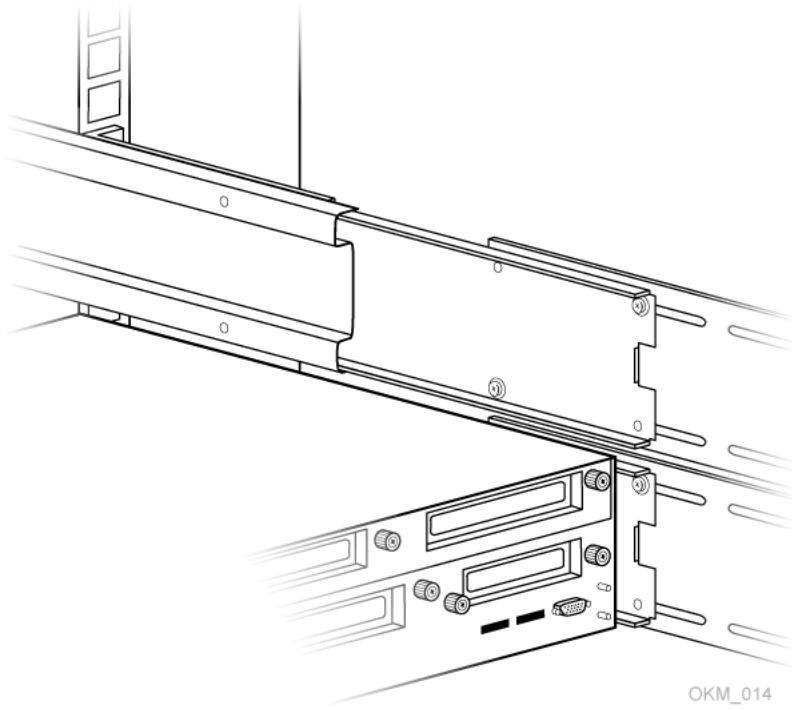


Figure 2-4 View of Brackets at Rear of Rack



4. Install the server onto the slide, and adjust the fit as needed.
5. Remove the server, tighten the rack and bracket screws, and then re-install the server onto the slide.

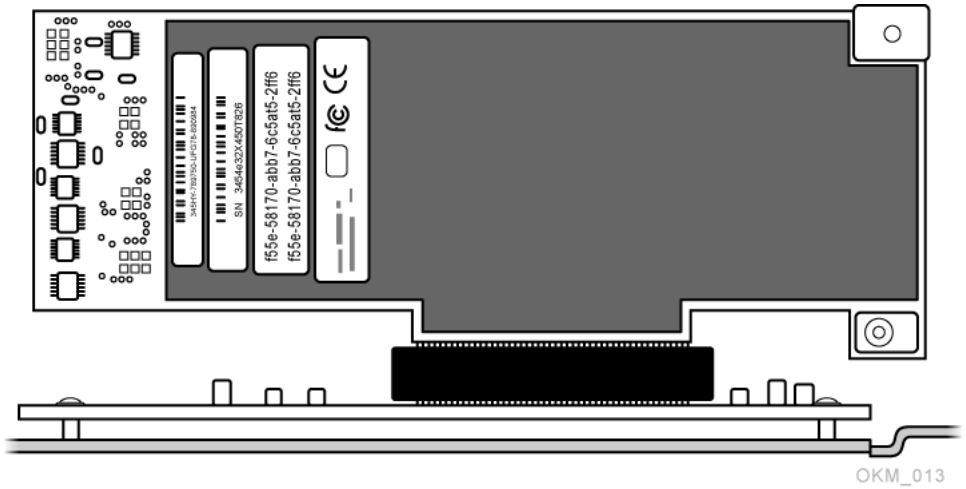
> **Caution:**
>
> Do not leave the server pulled out for long periods of time; rack mount kits may not be sturdy. It is safer to pull the server all the way out of the rack and place it on a bench. Also, it's a two-person job to put the server back onto its sliding rackmount.

Install the Cryptographic Card into a Netra SPARC T4-1

Install the optional cryptographic card into slot 2 of the KMA.

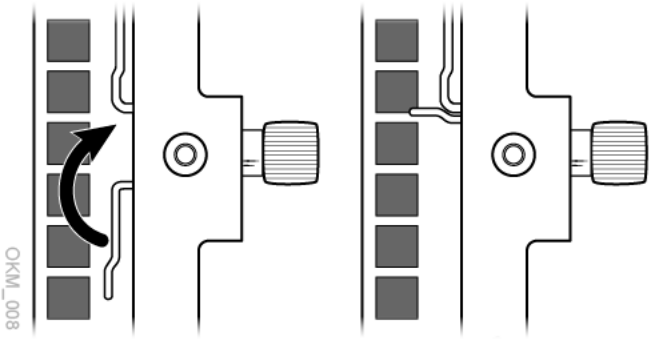
1. Obtain the cryptographic card. Either SCA 6000 or Thales nShield Solo+.
2. Install the card in the PCIe2 slot 2 (below the mezzanine board) using a PCIe riser.

Figure 2-5 SCA 6000 Card Installed with Riser



3. After you seat the card into place, secure it tightly by placing your thumbs on the left and right sides of the back edge of the card and gently but firmly rocking your thumbs back and forth.
4. Locate the clasp that is near the green captive screw but on the inside of the box.
5. Rotate this clasp clockwise back into place so that the green captive screw can screw into it.

Figure 2-6 Clasp Position



> **Caution:**
>
> Be careful when you rotate the clasp back against the side of the box. Do not force it. The clasp warps if you try to use two thumbs or a screwdriver. Observe the filler in the other slot to see how the clasp fits into place. Then go back and do the thumb rocking described above until you can gently rotate the clasp into place.

Initial ILOM Configuration

Use the ILOM to initially setup the T8-1, T7-1, T4-1, or X4170 M2 KMAs.

As soon as you apply power to the KMA—by plugging the server in to the power source—and after a one or two minute boot period, the ILOM provides a remote connection to the console.

> **Note:**
>
> This section has some basic ILOM commands to configure the server. Refer to the *Integrated Lights Out Manager Administration Guide* for more information.

1. Configure your laptop before accessing ILOM.
2. **IMPORTANT**: Do not connect the power cord to the server. Wait until instructed below. The ILOM starts as soon as you connect power, even if the server is powered-off. This is why you prepare and connect the laptop before connecting the power cord.
3. Obtain the IP address for the ILOM.
4. Using the table below as a reference, connect all cables as required.

Table 2-1 KMA Network Connections - T8-1, T7-1, and T4-1

Port	Connects To	Description
SER MGT	Service Rep Laptop	Serial connection to the ILOM. The ILOM IP address is most easily configured using this connection.
NET MGT	ILOM	Optional Ethernet connection to the ILOM. This port is not available until you configure the ILOM IP address.
NET 0	Management Network	Required connection to the Management Network (a switch) and to other KMAs in the cluster. The Management Network can be local, remote, or a combination of both. Customers are expected to provide the management network.
NET 2	Service Network	Required connection to the Service Network. This network connects the server to encryption agents, such as tape drives, either directly, or through Ethernet switches.
NET 3	Aggregate Network	Optional connection to the Aggregated Network and provides aggregation with NET 2.

5. Connect a null modem serial cable to the SER MGT port. Connect the other end to a laptop PC serial port.
6. Start a HyperTerminal session on the laptop. This allows you to watch the boot process.
7. Verify the default settings are:
   - 8-bits
   - No Parity
   - 1 stop-bit
   - 9600 baud rate
   - Disable both hardware (CTS/RTS) and software (XON/XOFF) flow control
8. Connect the server power cord to the power source. Do not power-on the server. The ILOM starts as soon as you connect power.
9. Once the boot completes, press [Enter] a few times to get to the ILOM login prompt. Log in as the system root user. See ILOM Security Hardening for details about this user.
10. Configure the ILOM IP address.
11. Enter the following commands. These commands are case sensitive.

    ```
    show /SP/networkset /SP/network/ pendingipdiscovery=staticset /SP/
    network/ pendingipaddress=ipaddressset /SP/network/
    pendingipnetmask=netmaskset /SP/network/
    pendingipgateway=gatewayset /SP/network/ commitpending=true
    ```

12. On a SPARC T8-1, SPARC T7-1 or Netra SPARC T4-1 server, enter the following commands to set the auto-boot property. There is a space after the question mark but not before it. These commands are case sensitive.

    ```
    show /HOST/bootmodeset /HOST/bootmode script="setenv auto-boot? true"show /HOST/
    bootmode
    ```

13. Log off of the ILOM and exit.
14. Go to Launch the QuickStart from the ILOM Web Interface to continue the installation.

3
Configure a KMA with QuickStart

Use the QuickStart program to configure a newly-installed, factory-default KMA.

About the QuickStart Wizard

The KMA QuickStart is a wizard that guides you through configuring a factory-default KMA.

Since the QuickStart program establishes critical security parameters, Oracle recommends that customers run it themselves. The Oracle service rep can use the QuickStart Configuration Checklist to help the customer step through the wizard. After you have configured a KMA, you cannot run the QuickStart program again unless you reset the KMA to its factory-default state (see Reset the KMA to the Factory Default).

Important: The initial configuration is a multi-step process that requires collaboration between the installers and the customer to complete.

Before running the QuickStart program, verify you have:

- Installed the components of the Oracle Key Manager, including the KMA, network cables, and switches.
- Configured the Integrated Lights Out Manager (ILOM).
- Configured the BIOS on a Sun Fire X4170M2 KMA

> **Caution:**
>
> Do not perform a "Core Security Backup" when using "simple settings" or settings that will change before going to a production environment. Wait until all user's have entered their appropriate credentials, passphrases, and quorum details before creating a Core Security Backup for the first time.

Best Practices When Running the QuickStart Wizard after KMA Installation

During the initial configuration when all the required users may not be available, use simple entries when entering information such as the key split size, split threshold, and quorum. For example, use an initial value such as `1 of 1`.

Once the structure of the KMAs and the OKM Cluster are complete, you can change this information to the production values at a later time using the OKM Manager. This can help speed up the installation and configuration.

During the QuickStart Wizard, customers will want to keep the following information confidential: User IDs, Passphrases, and Key Split Credentials.

QuickStart Configuration Checklist

This list provides a summary of the steps to configure a KMA with the QuickStart program.

- **Enable the Technical Support Account**.

  To assist in troubleshooting network configurations, you might want to enable the technical support account for the network configuration steps.

- **Specify the network configurations** (Management and Service).

  Supporting IPv4 and IPv6?

  Hostname, IP address, and netmask for the:

  - Management network - LAN 0
  - *Integrated* lights out manager - LAN 1 (previously configured)
  - Service network - LAN 2
  - Additional aggregate service network - LAN 3 (Net2 and Net3 on a Sun Fire X4170 M2)
  - DHCP

- **View, add, or delete** (modify) **gateways**.

  The gateway should be accessible through the management network connection. Gateways required if there is a router between the KMA and the OKM Manager.

- **Set the DNS configurations.**

  DNS configuration is optional; however, necessary if the KMA is using hostnames instead of IP addresses.

  > **Note:**
  >
  > DNS requires an IPv4 address/protocol, IPv6 is not used.

- **Initialize the KMA**.

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

> **Note:**
>
> A KMA Name cannot be altered once set using the QuickStart program. It can only be changed by resetting the KMA to the factory defaults and running QuickStart again.

- **Configure the cluster**.

  You can now use this KMA to create a new Cluster, or join an existing Cluster.

  (1) Create New Cluster

  (2) Join Existing Cluster

  (3) Restore Cluster from Backup

- **Enter Key Split credentials**.

  When creating a new cluster the key split credentials (M of N) must be specified. The Key Split credentials are used to wrap splits of the Core Security Key Material which protects Data Unit Keys. A Key Split credential, consisting of a unique User Name and Passphrase, is required for each Key Split.

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

  – Initial recommendations are to *keep this simple*.

  – This information cannot be recovered from the system if it is lost.

  – Backups cannot be restored without this information.

  – Loss of this information will result in unrecoverable data.

- **Enter Security Officer credentials**.

  You will be creating a Security Officer role, which is required to do this installation. *Make sure* you have the person performing that role available to do this QuickStart.

- **Specify the Autonomous Unlocking preference.**

  Autonomous Unlocking allows the KMA to enter a fully operational state after a hard or soft reset without requiring the entry of a quorum of passphrases using the OKM Manager. This information should not be written down and should be entered by the person to which they belong.

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

  > **Note:**
  >
  > The recommendation for maximum security is to use the default and have Autonomous Unlocking off. Autonomous unlocking selection:

  – If yes, the KMA will automatically unlock after a reboot.

  – If no, the KMA will remain locked until manually unlocked.

> **Note:**
>
> Unlocking requires a quorum.

- **Set the Key Pool size**.

  Each KMA pre-generates and maintains a pool of keys. These pre-operational keys must be backed up or replicated before a KMA passes them to an Agent.

  A smaller key pool size prevents unnecessary initial database and backup size; however, might require frequent backups. Key pool size is 1,000 - 200,000 keys.

- **Synchronize the time**.

  KMAs in a Cluster *must* keep their clocks synchronized. Internally, all KMAs use UTC time (coordinated universal time). Use of an external Network Time Protocol (NTP) server is recommended.

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

> **Note:**
>
> Do not make a mistake setting the system time manually. Adjustments through the OKM Manager GUI are restricted to plus, or minus, 5 minutes per day.

- **Start or join a cluster.**

  After customers have completed going through the QuickStart Wizard, they must install the OKM Manager and finish setting up the OKM Cluster.

Launch the KMA QuickStart Program

There are two ways to launch the QuickStart from the ILOM: the web interface or the CLI.

- Launch the QuickStart from the ILOM Web Interface
- Launch the QuickStart from the ILOM CLI

Accessing the ILOM Interfaces

Connect to the ILOM IP address on the KMA Management Network (NET MGT). The ILOM can also be accessed by physically connecting a terminal to the SER MGT port on the KMA, but this is typically only done by an Oracle Service Representative during KMA installation or service.

The table below provides details about the Lights Out Manager interfaces available for each KMA server model.

Table 3-1 Lights Out Manager Interface for Each KMA Server Model

KMA Server Model	Lights Out Manager Interface
SPARC T7-1 or T8-1 Netra SPARC T4-1	ILOM, Web or CLI
Sun Fire X4170 M2	ILOM, Web only
Sun Fire X2100 M2 Sun Fire X2200 M2	ELOM, Web only Refer to the OKM 2.5 documentation for more information.

See Upgrade and Configure Integrated Lights Out Manager (ILOM) for additional procedures.

See the following documents for details about the ILOM for your KMA.

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance*
- *Oracle ILOM 3.1 Configuration and Maintenance Guide*

What happens once the KMA startup completes?

The KMA behaves differently after startup depending on if it is in the factory-default state or was already configured.

- If the KMA is in the factory-default state, the KMA QuickStart program automatically launches and guides you through the initial KMA configuration. See Review QuickStart Information and Set Keyboard Layout.
- If the KMA has already been configured for your site, the OKM Console appears and you can display or make changes to the KMA configuration. See OKM Console .

Launch the QuickStart from the ILOM Web Interface

Launch QuickStart from a web browser using a workstation connected to the KMA management network.

1. Using a workstation on the KMA Management Network, launch a web browser.
2. Connect to the KMA ILOM using the IP address of the KMA Service Processor. This IP address was assigned at installation.

   Because the certificate in the ILOM does not match the Service Processor IP address, the web browser displays one or more certificate warnings.
3. Click **OK** or **Yes** to bypass the certificate warnings.
4. Log in as the system root user.
5. In the Navigation Bar, select **Host Management**, then select **Power Control**.
6. If the KMA host is powered off, power it on (from the **Settings** drop-down, select **Power On**, and then click **Save**).
7. In the Navigation Bar, select **Remote Control**, then select **Redirection**.
8. Select **Use serial redirection**, then click **Launch Remote Console**.

9. In the dialog box, select **Open with Java(TM) Web Start Launcher** and click **OK** to open the Remote Host Console Java applet. Accept any warnings that may be displayed.
10. In the dialog box, click **Run** to start the Remote Host Console. Accept any warnings that may be displayed.
11. Monitor the startup messages that appear in the Remote Host Console, including the status of the hardware security module.

    ```
    Console unavailable while KMA Maintenance is in progress...
    ```

12. Once the KMA startup completes, the KMA QuickStart program automatically launches and guides you through the initial KMA configuration. See Review QuickStart Information and Set Keyboard Layout.

Launch the QuickStart from the ILOM CLI

Use the ILOM CLI to launch the QuickStart on the SPARC servers.

1. Using a workstation on the KMA Management Network (NET MGT), establish a Secure Shell (SSH) connection to the KMA Service Processor.

   ```
   $ ssh SP_ipaddress
   ```

   where *SP_address* is the IP address of the KMA Service Processor. This was assigned by your Oracle Service Representative at installation.
2. Log in using the system root account and password.
3. Display the power status of the KMA.

   ```
   -> show /System power_state
   ```

4. If the KMA host is powered off, power it on.

   ```
   -> start /System
   ```

5. Start the Remote Host Console.

   ```
   -> start /Host/console
   ```

6. Monitor the startup messages that appear in the Remote Host Console, including the status of the hardware security module.

   ```
   Console unavailable while KMA Maintenance is in progress...
   ```

7. Once the KMA startup completes, the KMA QuickStart program automatically launches and guides you through the initial KMA configuration. See Review QuickStart Information and Set Keyboard Layout.

Record the Configuration Information

Collect the configuration information for the KMA and cluster so that you have a record for the future. Do not record passphrases.

KMA Configuration Information

Server Processor

Network address:
User name and passphrase:

Keyboard Type (if KMA is x86):

Management network interface

Using IPv6 address (yes/no):
Using DHCP (yes/no):
If not using DHCP, IP address and netmask:

Management Network Gateway

Type (default, host or network):
IP address:

Service Network Gateway (if needed)

Type (default, host or network):
IP address:
DNS Server IP addresses (if any), up to 3:
Acceptable TLS versions (TLS v1.0+, v1.1+, v1.2 only):
KMA name:

Cluster Configuration Information

Key split credentials

Threshold:
Number defined:
Key split user names and passphrases

Initial Security Officer

User name:
Passphrase:

Key Pool Size (typically 1000):

Certificate Signature Algorithm (SHA 256 /SHA-1):

Autonomous Unlock (yes/no):

External NTP server (if any):

Review QuickStart Information and Set Keyboard Layout

The first step of the QuickStart has you review information and set the keyboard layout (if using a SunFire KMA).

> **Note:**
>
> If you press `Ctrl`-c anytime during the QuickStart program, no changes are saved and you return to the Welcome screen.

1. This procedure assumes you have launched the QuickStart. If not, see Launch the KMA QuickStart Program.
2. Review the instructions on the QuickStart Welcome screen and press **Enter**.

3. On SunFire-based KMAs, specify the keyboard layout.
4. Proceed to Configure the Network in QuickStart.

Configure the Network in QuickStart

Use the QuickStart to provide the KMA with network configuration information. Configuring the network is a multi-step process within the wizard.

Perform the following tasks in the order listed:

- Set KMA Management IP Addresses (using QuickStart)
- Enable Technical Support Account (using QuickStart)
- Set the KMA Service IP Addresses (using QuickStart)
- Modify Gateway Settings (using QuickStart)
- Set DNS Configuration (using QuickStart)
- Set Acceptable TLS Versions (using QuickStart)

Set KMA Management IP Addresses (using QuickStart)

Set the KMA management IP address after reviewing the instructions on the QuickStart Welcome screen.

1. To access the following prompts of the QuickStart, make sure you have completed Review QuickStart Information and Set Keyboard Layout.
2. Type either **n** or **y** to configure IPv6.
3. Type either **n** or **y** to use DHCP for the IPv4 interface.

> **Note:**
>
> If you elect to use DHCP, any host name information provided by the DHCP server is ignored. Any DNS information provided by the DHCP server is presented in Set DNS Configuration (using QuickStart).

4. Type the Management Network IP address and press **Enter**.
5. Type the Subnet Mask address (for example 255.255.254.0) and press **Enter**.
6. Proceed to Enable Technical Support Account (using QuickStart).

Enable Technical Support Account (using QuickStart)

Optionally, enable the technical support account after setting the KMA management IP addresses within the QuickStart wizard. The Technical Support account can assist in troubleshooting network configurations.

1. Type **y** or **n** when prompted to configure the support account.

> **Note:**
>
> QuickStart will disable the support account after you complete Set DNS Configuration (using QuickStart). After completing the QuickStart, you can enable or disable the support account at anytime using the OKM console (see Enable the Technical Support Account (using OKM Console)).

2. Proceed to Set the KMA Service IP Addresses (using QuickStart).

Set the KMA Service IP Addresses (using QuickStart)

Set the KMA service IP addresses after setting the technical support account within the QuickStart wizard.

1. Type either **n** or **y** when prompted to configure IPv6.
2. Type either **n** or **y** when prompted to use DHCP for the IPv4 interface.
3. Type the Service Network IP address and press **Enter**.
4. Type the Subnet Mask address (for example 255.255.254.0) and press **Enter**.
5. Proceed to Modify Gateway Settings (using QuickStart).

Modify Gateway Settings (using QuickStart)

Modify the gateway settings after setting the KMA service IP addresses within the QuickStart wizard.

1. Enter **1** to display the next gateway setting or **2** to return to the previous gateway setting. For example:

```
   # Destination       Gateway          Netmask            IF
---- ----------------- ---------------- ------------------- --
   1 default           10.172.181.254   0.0.0.0             M
   2 default           10.172.181.21    0.0.0.0             M
   3 default           192.168.1.119    0.0.0.0             S
   4 10.0.0.0          10.172.180.25    255.255.254.0       M
*  5 10.172.180.0      10.172.180.39    255.255.254.0       M
...
```

2. At the `Please choose one of the following:` prompt, type **1**, **2**, **3**, or **4** and press **Enter**.

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

3. Proceed to Set DNS Configuration (using QuickStart).

Set DNS Configuration (using QuickStart)

Set the DNS configuration after modifying the gateway settings within the QuickStart wizard. Entering DNS information is optional.

> **Note:**
>
> If you elected to use DHCP on the management network in Set KMA Management IP Addresses (using QuickStart), the KMA displays any DNS settings from a DHCP server on the management network. You can enter information to override these DNS settings.

1. When prompted, enter the DNS domain name.
2. When prompted, enter the DNS server IP address. You can enter up to three addresses.
3. Press **Enter**, without specifying an IP address, to finish.
4. Proceed to Set Acceptable TLS Versions (using QuickStart).

Set Acceptable TLS Versions (using QuickStart)

Set the TLS versions after setting the DNS configuration within the QuickStart Wizard.

1. When prompted, select the TLS versions to enable:

```
(1) TLSv1.0 and higher
(2) TLSv1.1 and higher
(3) TLSv1.2 and higher
```

2. Proceed to Name the KMA.

By default, a KMA will accept connections using TLSv1.0, TLSv1.1 or TLSv1.2 While TLSv1.0 is no longer considered secure, if you have KMAs in the cluster running OKM versions prior to OKM 3.1.0, or you have Agents (such as tape drives) that cannot connect using later versions of TLS, you may need to leave all versions of TLS enabled.

OpenSSL 0.9.x and 1.0.0 do not support TLS v1.2. If you configure a KMA to accept only connections that use TLS v1.2, the KMA will not accept connections from an OKM GUI or CLI that uses OpenSSL 0.9.x or 1.0.0. You should plan on installing the latest OKM GUI and CLIs if migrating to OKM 3.3.2.

Table 3-2 Tape Drive TLS Compatibility

Tape Drive Type	Supported Version of TLS
StorageTek T10000 and 9840	v1.0
IBM LTO with Belisarius 4.x	v1.0
IBM LTO with Belisarius 5.x or LKM	v1.2

Name the KMA

Name the KMA after completing the network configuration within the QuickStart wizard. Each KMA must have a unique name within the cluster.

This procedure assumes you have completed the prior steps in the QuickStart. If not, see Launch the KMA QuickStart Program.

1. To access the following prompts of the QuickStart, make sure you have completed Configure the Network in QuickStart.
2. **IMPORTANT**: You cannot alter the KMA Name after you set it using the QuickStart. The only way to change the name is by resetting the KMA to factory default and running QuickStart again.
3. At the prompt, type a unique identifier for the KMA. This name will also be used for the host name for the KMA. Press **Enter**.
4. Select what to do with the KMA:
   - Enter 1 and then see Create a New Cluster with QuickStart.
   - Enter 2 and then see Add a KMA to an Existing Cluster.
   - Enter 3 and then see Restore a Cluster from a Backup.

Create a New Cluster with QuickStart

Create a new cluster after naming the KMA within the QuickStart wizard and selecting option 1.

These procedures assume you have completed the prior steps in the QuickStart. If not, see Launch the KMA QuickStart Program.

- Enter Key Split Credentials (using QuickStart)
- Enter Initial Security Officer Credentials (using QuickStart)
- Specify Autonomous Unlocking Preference
- Set the Key Pool Size (using QuickStart)
- Select Certificate Signature Algorithm (using QuickStart)
- Synchronize the KMA Time (using QuickStart)

Enter Key Split Credentials (using QuickStart)

Enter Key Split Credentials after naming the KMA and selecting option 1 to create a new cluster within the QuickStart wizard.

Key Split Credentials user IDs and passphrases should be entered by the individual who owns that user ID and passphrase. Using one person to collect and enter this information defeats the purpose of having the Key Split Credentials. If it is impractical for all members of the Key Split Credentials to enter this information at this time, enter a simple set of credentials now, and then enter the full credentials later in the OKM Manager. However, doing this creates a security risk. If a Core Security backup is created with simple Key Split Credentials, it can then be used to restore a backup.

1. To access the following prompts of the QuickStart, make sure you have entered 1 in the last step of Name the KMA.
2. Type the key splits to generate (1 to 10) and press **Enter**.
3. Type the number of required keys splits to obtain a quorum and press **Enter**.
4. Type the user name for the first Key Split user and press **Enter**.
5. Type the passphrase and press **Enter**. Re-enter the passphrase and press **Enter**.
6. Repeat until all user names and passphrases have been entered for the selected Key Split size.

> **Note:**
>
> The Key Split user names and passphrases are independent of other user accounts that are established for KMA administration. Oracle recommends that key split user names be different from KMA user names.

7. Proceed to Enter Initial Security Officer Credentials (using QuickStart).

Enter Initial Security Officer Credentials (using QuickStart)

Enter initial security officer credentials after entering the key split credentials within the QuickStart wizard.

1. When prompted, create the initial Security Officer user (used to logon to the KMA using the OKM Manager). Enter the Security Officer's username and passphrase.

> **Note:**
>
> All KMAs have their own passphrases that are independent of passphrases assigned to users and agents. The first KMA in a cluster is assigned a random passphrase. If this KMA's certificate expires, and you want to retrieve its entity certificate from another KMA in the cluster, you would have to use the OKM Manager to set the passphrase to a known value. For procedures, refer to Change a KMA Passphrase (Log the KMA Out of the Cluster).

2. Proceed to Specify Autonomous Unlocking Preference.

Specify Autonomous Unlocking Preference

Specify the automnomous unlocking preference after entering the initial security officer credentials within the QuickStart wizard.

Autonomous unlocking allows the KMA to become fully operational after a reset without requiring the entry of a quorum of passphrases. You can change this option from the OKM Manager at a later time.

> **Caution:**
>
> While enabling autonomous unlocking is more convenient and increases the availability of the OKM cluster, it creates security risks.
>
> When autonomous unlocking is enabled, a powered-off KMA must retain sufficient information to start up fully and begin decrypting stored keys. This means a stolen KMA can be powered up, and an attacker can begin extracting keys for the KMA. While it is not easy to extract keys, a knowledgeable attacker will be able to dump all keys off the KMA. No cryptographic attacks are needed.
>
> If autonomous unlocking is disabled, cryptographic attacks are required to extract keys from a stolen KMA.

1. When prompted, type **y** (to enable) or **n** (to disable). Press **Enter**.
2. Proceed to Set the Key Pool Size (using QuickStart).

Set the Key Pool Size (using QuickStart)

Set the key pool size after specifying the autonomous unlocking preference within the QuickStart wizard.

Each KMA generates and maintains a pool of preoperational keys, which must be backed up or replicated before the KMA passes them to an agent.

1. At the prompt, enter the key pool size. The value entered determines the initial size that the new KMA generates and maintains.
2. Proceed to Select Certificate Signature Algorithm (using QuickStart).

Select Certificate Signature Algorithm (using QuickStart)

Select the certificate signature algorithm after setting the key pool size within the QuickStart wizard.

A Root CA certificate is generated when the cluster is first initialized. This Root CA certificate is used to generate certificates for KMA, user, and agent entities. The Root CA certificate and the entity certificates can be X.509v3 certificates signed using the SHA-256 hashing algorithm, or they can be X.509v1 certificates signed using the SHA-1 hashing algorithm.

1. When prompted, enter **1** for SHA256 (default) or **2** for SHA1.

   Always select SHA256, unless you are deploying encryption endpoints that do not support SHA2.
2. Proceed to Synchronize the KMA Time (using QuickStart).

Synchronize the KMA Time (using QuickStart)

Synchronize the KMA time after selecting the certificate algorithm within the QuickStart wizard.

KMAs in a cluster must keep their clocks synchronized. Internally, all KMAs use UTC time (Coordinated Universal Time). You can also use the OKM Manager to adjust date and time settings to local time.

1. When prompt, optionally enter the NTP server host name or IP address.

> **Note:**
>
> You can provide an IPv6 address for this NTP server. This IPv6 address must not include square brackets or a prefix length.

2. If an NTP server is not available, press **Enter**. Then, enter the date and time in one of the specified formats, or press **Enter** to use the displayed date and time.
3. At the prompt, press **Enter**. KMA initialization is complete.
4. Press **Enter** to exit. The QuickStart program terminates and a login prompt is displayed (refer to Log into the KMA). The KMA now has the minimum system configuration that is required to communicate with the OKM Manager.
5. Your next step is to use OKM Manager to connect to and configure the cluster. For procedures, refer to Configure the Cluster .

Add a KMA to an Existing Cluster

Create the KMA in the OKM GUI and then use the QuickStart to add the KMA to an existing cluster. Add a new KMA to the cluster only during times of light loads.

Prerequisites:

1. See Restrictions on Adding a New KMA to a Cluster. Verify the new KMA is compatible with existing KMAs in the cluster.
2. Set the replication version to the highest value supported by all KMAs in the cluster. Refer to Switch the Replication Version.
3. The Security Officer must use the OKM GUI to create the KMA entry in the database (see Create a KMA). The KMA Name specified during the KMA QuickStart process must match the KMA name used in the database.

Add the KMA using QuickStart:

1. Verify all prerequisites are complete.
2. To access the following prompts of the QuickStart, make sure you have entered 2 in the last step of Name the KMA.
3. At the QuickStart prompt, type the network address of one KMA in the existing cluster, and then press **Enter**.
4. At the prompt, type the passphrase for the KMA and press **Enter**.
5. Enter the required number of Key Split user names and passwords.

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

6. Once you have entered a sufficient number of Key Split user names and passphrases to form a quorum. Enter a blank name to finish.
7. The KMA being added checks the firmware version against the existing versions in the cluster. If it is not compatible, the new KMA displays an error and presents the option to upgrade or downgrade the firmware. If you select "Yes", then the KMA being added will:
   - Grab the code from the existing KMA in the cluster
   - Download the code for its own
   - Install the code

   This process takes about 25 to 30 minutes to complete. Once this process completes, reboot the KMA. After the KMA comes back online from the reboot, continue with the QuickStart program.
8. Consider accelerating initial updates to the new KMA. Review Accelerate Updates to the New KMA in a Cluster before typing **y** at the prompt.
9. You will see `This KMA has joined the Cluster`. Press **Enter** to exit. The QuickStart program terminates and a login prompt is displayed (refer to Log into the KMA). The KMA now has the minimum system configuration that is required to communicate with the OKM Manager.
10. Use the OKM Manager to connect to and configure the cluster. For procedures, refer to Configure the Cluster .
11. The OKM cluster begins to propagate information to the newly added KMA. This causes the new KMA to be very busy until it has caught up with the existing KMAs in the cluster. The other KMAs are also busy. You can observe this activity from the OKM Manager by viewing the KMAs as described by View and Modify KMA Settings.
12. Observe the Replication Lag Size value of the new KMA. Initially, this value is high. Periodically refresh the information displayed in this panel by pulling down the View menu and selecting Refresh or by pressing the **F5** key. Once the Replication Lag Size value of this KMA drops to a similar value of other KMAs in the cluster, then you can unlock the KMA as described by Lock/Unlock the KMA.
13. The KMA remains locked after it has been added to the cluster. Wait until the KMA has been synchronized (that is, until it has "caught up" with other KMAs in the cluster) before you unlock it. Do not add another KMA to the cluster until you unlock the just-added KMA.

Restrictions on Adding a New KMA to a Cluster

OKM 3.3.2 introduces more restrictions when joining a new KMA into an existing cluster. Verify your KMAs are compatible before adding one to a cluster.

An OKM 3.3.2 KMA cannot be added to an existing OKM cluster with KMAs running a version below OKM 3.1. Assess the types of KMAs in your OKM cluster and the OKM releases they run:

- Netra SPARC T4 KMAs running OKM 3.0.x must be upgraded to OKM 3.1 or later.
- Sun Fire X4170 M2 KMAs running OKM 3.0.2 must be upgraded to OKM 3.1 or later.
- Sun Fire X2100/X2200 M2 KMAs do not support OKM 3.1 and later releases. These KMAs should be replaced with SPARC KMAs.

Accelerate Updates to the New KMA in a Cluster

If the cluster's replication version is at least 12, consider accelerating initial updates to the new KMA to speed up the time it takes to incorporate the KMA into the cluster.

If you choose to accelerate updates, perform an OKM backup on a peer KMA (preferably one in the same site as the new KMA) before adding the new KMA to the cluster. Also, ensure that the peer KMA on which you created a backup is currently responding on the network. These steps help the new KMA find a cached backup to download and apply.

The KMA you specified identifies another KMA that has the largest cached backup in this cluster, downloads that backup, and then applies it to its local database. This process is equivalent to replicating the data but at a much faster rate. Informational messages appear during this process.

For example:

```
Waiting 10 seconds for the join to propagate to Peer KMAs...
Querying Peer KMAs to find the active ones...
Querying active Peer KMAs to find cached backup sizes...
Peer KMA at IP Address 10.172.180.39 has a cached backup size of 729136 bytes.
Downloading the cached backup from this Peer KMA...
Downloaded the cached backup from this Peer KMA.
Initialized the Key Store.
Performed maintenance on the Key Store.
Applying the cached backup to the local database...
..................................................
Applied the cached backup to the local database.
Successfully accelerated initial updates on this KMA.
```

Later, the newly joined KMA automatically replicates any data that is not in the backup.

If an error occurs during this process, QuickStart displays the above prompt again (in case the error is due to a temporary condition). QuickStart also displays the above prompt again if the KMA cannot find a peer KMA that has a cached backup.

However, if more than 5 minutes has elapsed since the first time the above prompt was displayed, then QuickStart displays the following message and no longer displays the above prompt:

```
Failed to accelerate initial updates on this KMA after 300 seconds.
This KMA will gradually be updated with information from other KMAs.
```

Restore a Cluster from a Backup

Use the QuickStart to restore a KMA from a backup in the event that all KMAs in a cluster have failed.

After selecting the Restore a Cluster option in the QuickStart, proceed to the following sections.

- Create Security Officer and Provide Quorum Login
- Set Time Information
- Restore a Backup (completed using OKM Manager)

Create Security Officer and Provide Quorum Login

Create the security officer and quorum login that will be used to access the OKM GUI and restore the cluster.

1. To access the following prompts of the QuickStart, make sure you have entered 3 in the last step of Name the KMA.
2. At the prompt, enter the Security Officer's user name and password.

> **Note:**
>
> Oracle recommends you specify a new Security Officer name that did not exist in the OKM cluster when the last backup was performed. Enter a temporary restore Security Officer user ID (for example, RestoreSO) instead of the Security Officer user ID that existed before the restore.
>
> If you specify an existing Security Officer name and provide a different passphrase, the old passphrase is overwritten. If you specify an existing Security Officer name and other roles were added to that user before the last backup was performed, these other roles are no longer assigned to this User.

3. (Optional)— At the prompt, provide the quorum login user ID and password.

   If you choose to define initial quorum user credentials in QuickStart, you can enter a quorum login name and passphrase at this time so that the restore operation from the OKM Manager GUI is set to pending. Quorum members can then use this login and passphrase later to log in to the OKM Manager GUI and enter their credentials to approve the restore (see Restore a Backup).

   If you do not enter a quorum login user ID here, the only user that exists at the end of QuickStart is the Security Officer created above. In this case, all Key Split Credentials must be entered at once for the restore to occur.
4. Proceed to Set Time Information.

Set Time Information

Set the time information after providing the quorum login information within the QuickStart wizard.

1. If an NTP server is available in your network environment, at the prompt, enter the NTP server host name or IP address.
2. If an NTP server is not available, press **Enter**. Then, enter the date and time in one of the specified formats, or press **Enter** to use the displayed date and time.

   Ensure the date and time are accurate. Key lifecycles are based on time intervals, and the original creation times for the keys are contained in the backup. An accurate time setting on the replacement KMA is essential to preserve the expected key lifecycles.
3. Once you see `KMA initialization complete!`, press **Enter** to exit. The QuickStart program terminates and a login prompt is displayed.
4. Proceed to Restore a Backup to use OKM Manager to finish the restoration.

4

Install OKM Manager

OKM Manager is a client application installed on your workstation used to configure, control, and monitor KMAs. To install OKM manager, first uninstall all previous versions, then download and launch the installation wizard.

Supported Platforms for OKM Manager

OKM Manager is supported only on certain platforms.

You do not need administrator (Windows) or root (Solaris) privileges to install and run OKM Manager.

- Solaris 10 — 10/09 (update 8) x86, 9/10 (update 9) SPARC, 9/10 (update 9) x86
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7 Business and Enterprise
- Microsoft Windows Server 2016, 2012, 2008 version 6.0

Uninstall Previous Versions of OKM Manager

Uninstall any previous OKM Manager versions before installing the new OKM Manager.

There are two methods for uninstalling OKM Manager:

Uninstall OKM Manager by Invoking the Executable File

Invoke the executable file to uninstall the OKM Manager. This method works for both Windows and Solaris.

1. Navigate to the directory listed below, which resides under the directory where the OKM Manager was installed.
   - `_Oracle Key Manager_installation` (for OKM 3.3.2 and above)

- `Uninstall_Oracle_Key_Manager` (for OKM 3.3 and below)

2. To launch the uninstall process, invoke:

   For Windows:

   - `Change Oracle Key Manager Installation.exe` (for OKM 3.3.2 and above)
   - `Uninstall_Oracle_Key_Manager.exe` (for OKM 3.3 and below)

   For Solaris:

   - `Change Oracle Key Manager Installation` (for OKM 3.3.2 and above)
   - `Uninstall_Oracle_Key_Manager` (for OKM 3.3 and below)

3. The Preparing Setup window displays while the install/uninstall program prepares for the uninstall process.
4. After launching the uninstaller, click **Next**.

> **Note:**
>
> Uninstallation will not remove your connection profiles.

5. When the uninstall process completes, click **Finish**.

Uninstall OKM Manager with Add/Remove Programs (Windows Only)

As an alternative to invoking the executable, you can use the add/remove programs option on Windows.

1. Click **Start**, select **Settings**, **Control Panel**, double-click **Add or Remove Programs**. Select OKM Manager, then click **Change/Remove**.
2. The Preparing Setup window displays while the install/uninstall program prepares for the uninstall process.
3. After launching the uninstaller, click **Next**.

> **Note:**
>
> Uninstallation will not remove your connection profiles.

4. When the uninstall process completes, click **Finish**.

Download the OKM Installer

Download the OKM installer from My Oracle Support.

1. Log in to the My Oracle Support (MOS): `https://support.oracle.com/`
2. Open the **Patches & Updates** tab (near the top of the window).
3. In the **Patch Search** pane, with the Search tab open, click **Product or Family (Advanced)**.
4. Select the **Include all products in a family** check box.

5. In the Product field, type **OKM** and select Oracle Key Manager (OKM) from the menu.
6. In the Release field menu, select the appropriate OKM release (for example **Oracle Key Manager (OKM) 3.3.2)**.
7. Close the Release menu window and click the **Search** button.

Launch the OKM Installer

Windows and Solaris use different methods for launching the installer.

For Windows: Double-click the shortcut to start the installer program.

For Solaris:

1. Set your DISPLAY environment to identify the system to which this installer should be displayed.
   - If you start the installer program on the local Solaris system, set your DISPLAY environment variable to ":0.0."
   - Navigate to the directory where you downloaded the installer.
2. Invoke the installer.

   For example, if you downloaded the installer to the `/tmp` directory, and you plan to invoke it on your local Solaris system, you start the installer by entering the following commands at a shell prompt:

```
DISPLAY=:0.0
export DISPLAY
cd /tmp
ls OKMManager_solaris_3_3_2.bin
sh ./OKMManager_solaris_3_3_2.bin
```

> **Note:**
>
> If you invoke the installer on one Solaris system and want it to be displayed on another Solaris system, set your DISPLAY environment variable to identify the system on which it should be displayed.
>
> On the display system, first run the xhost(1) utility to allow access from the system from which you invoke the installer.
>
> For example, on the system (named "hosta") where you wish to display the installer, enter:

```
xhost +
```

On the system where you start the installer, enter:

```
ping hosta
DISPLAY=hosta:0.0
export DISPLAY
cd /tmp
ls OKMManager_solaris_3_3_2.bin
sh ./OKMManager_solaris_3_3_2.bin
```

Complete the OKM Installation Wizard

Follow the installation wizard prompts to install OKM.

1. Launch the installer (see Launch the OKM Installer).
2. Click **Next** on the Introduction screen of the installation wizard.
3. The Elevated Privileges window displays, telling you that you need elevated privileges to complete the installation (this screen does not appear on the Solaris installer). Click **Next**.
4. In the Choose Install Folder window, select the default folder, click **Next**, or supply your own installation folder, and click **Next**.
5. In the Choose Shortcut Folder window, select where to create the product icons and then click **Next**.
6. In Pre-Installation Summary window, review the settings and then click **Install**, or **Previous** to revise the setup.
7. Once the installation process completes, click **Done** to exit.

Launch OKM Manager

Windows and Solaris use different methods for launching OKM Manager.

For Windows: Double-click the startup icon to launch the OKM Manager application. Or, launch Windows Explorer, navigate to where you installed the OKM Manager, and launch OKM_Manager.exe.

For Solaris: Invoke the shortcut at a shell prompt by entering: `~/OKM_Manager` . Or, navigate to where you installed the OKM Manager and invoke it by entering: `./OKM_Manager`

5
Configure the Cluster

Use this list to configure the cluster. Follow the procedures referenced and then return to the list for the next step.

- Verify you have the correct version of OKM Manager installed.
  - Do not use older OKM GUIs (OKM 3.2 or earlier) to connect to KMAs running OKM 3.3 or later. You must use the OKM 3.3.2 GUI to upgrade a KMA to OKM 3.3.2. See Install OKM Manager .
- Connect to the cluster — see Connect to a KMA
- Review security parameters — see Review and Modify the Cluster Security Parameters
- Create a user — Create a User
- Login to the OKM manager with the new user
- Create key policies — see Create a Key Policy
- Create key groups — see Create a Key Group
- Create agents and define a default key group for each agent — see Create an Agent
- Backup core security — see Create a Core Security Backup
- Create a backup — see Create a Database Backup
- Create KMAs — Create a KMA and Configure a KMA with QuickStart
- Join the KMA to the cluster — Add a KMA to an Existing Cluster
- Enroll agents — Enroll Agents

Connect to a KMA

Connect to a KMA to use the OKM Manager to monitor or modify the KMA's configuration.

Available to: All roles

1. Before connecting to a KMA, verify at least one cluster profile exists and that a user has been created and enabled on the KMA. If you have not yet created a cluster profile, see Create a Cluster Profile.
2. From the **System** menu of OKM Manager, select **Connect** (or click **Connect** in the tool bar).
3. In the Connect to Cluster dialog, enter the following:
   - **User ID** — the name of the user who will connect to specified KMA. Or, if this is the first time that you are connecting to the KMA after the initial QuickStart process, enter the name of the Security Officer created during QuickStart.
   - **Passphrase** — the passphrase for the selected user.

- **Cluster Name** — the cluster to connect to.
- **Member KMAs** — the KMA to connect to within that cluster. If a KMA joined the cluster after you connected to that cluster, that KMA will not appear in the Member KMAs list. To update the list, enter the user name and passphrase, choose a cluster profile, and click **Refresh KMAs**.
- **IP Preference** — IPv4 only, IPv6 only, or IPv6 preferred.

4. Click **Connect**.

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

5. You can now use the OKM Manager to perform various operations.

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

Create a Cluster Profile

A single cluster profile covers the entire cluster and can be used by any user. Do not create a second cluster profile, unless you want to establish a second cluster or you have changed the IP addresses of all KMAs in the current cluster.

Available to: All roles

1. From the **System** menu of OKM Manager, select **Connect** (or click **Connect** in the tool bar).
2. In the Connect to Cluster dialog, click **New Cluster Profile**.
3. Enter the following in the Create Cluster Profile dialog:
   - **Cluster Name** — value that uniquely identifies the cluster profile name.
   - **Initial IP Address or Host Name** — the Service Network IP address or Host Name of the initial KMA in this cluster to connect to. Choosing which network to connect to depends on what network the computer system where the OKM Manager is running is connected to.
4. Click **OK**.

Delete a Cluster Profile

Delete a cluster profile that you no longer need.

Available to: All roles

1. From the **System** menu of OKM Manager, select **Connect** (or click **Connect** in the tool bar).
2. In the Connect to Cluster dialog, select the Cluster Name from the drop-down list. Click **Delete Cluster Profile**.
3. Confirm that you want to delete the cluster by clicking **Yes**.

Review and Modify the Cluster Security Parameters

Change security parameters, such as the FIPS Mode setting or the passphrase length, before configuring the cluster.

> **Note:**
>
> The **Master Key Provider** button is used only if you want the OKM cluster to obtain master keys from an IBM mainframe. The button is enabled only when the replication version of the OKM cluster is currently set to 11 or higher and the FIPS Mode Only value is "Off." See the OKM-ICSF Integration Guide for details.

Available to: All roles (can view parameters), Auditor (can view modify screen), Security Officer (can modify)

1. In the left navigation, expand **System Management**, then expand **Security**, and then select **Security Parameters**. Review the parameters.
2. To change a parameter, click **Modify...**
3. Modify the security parameters, as required. When finished, click **Save**.

Security Parameters

These parameters are selected when modifying security for the cluster.

Retention-related Fields
For the following six retention-related fields, there is a single audit log that resides in the largest file system in the KMA. The main reason for adjusting these parameters is to control how many audit log entries are returned in queries you issue from the Audit Event List menu (see View and Export Audit Logs). The KMA truncates (removes) old audit log entries based on the limit and lifetime of their retention term. For example, Short Term Audit Log entries are typically truncated more frequently than Medium Term Audit Log entries; Medium Term Audit Log entries are truncated more frequently than Long Term Audit Log entries.

- **Short Term Retention Audit Log Size Limit** — Displays the number of Short Term Audit Log entries that are retained before they are truncated. The default is 10,000. The minimum value is 1000; maximum value is 1,000,000.
- **Short Term Retention Audit Log Lifetime** — Displays the amount of time (in days) that Short Term Audit Log entries are retained before they are truncated. The default is 7 days. The minimum value is 7 days; maximum value is 25,185 days (approximately 69 years).
- **Medium Term Retention Audit Log Size Limit** — Displays the number of Medium Term Audit Log entries that are retained before they are truncated. The default is 100,000. The minimum value is 1000; maximum value is 1,000,000.
- **Medium Term Retention Audit Log Lifetime** — Displays the amount of time (in days) that Medium Term Audit Log entries are retained before they are truncated.

The default is 90 days. The minimum value is 7 days; maximum value is 25,185 days.

- **Long Term Retention Audit Log Size Limit** — Displays the number of Long Term Audit Log entries that are retained before they are truncated. The default is 1,000,000. The minimum value is 1000; maximum value is 1,000,000.
- **Long Term Retention Audit Log Lifetime** — Displays the amount of time (in days) that Long Term Audit Log entries are retained before they are truncated. The default is 730 days. The minimum value is 7 days; maximum value is 25,185 days.

Login Attempt Limit
Indicates the number of failed login attempts before an entity is disabled. The default is 5. The minimum value is 1; maximum value is 1000.

Passphrase Minimum Length
Displays the minimum length of the passphrase. The default is 8 characters. The minimum value is 8 characters; the maximum value is 64 characters.

Management Session Inactivity Timeout
Displays the maximum length of time (in minutes) an OKM Manager or Console login session can be left idle before being automatically logged out. Changing this value has no effect on sessions that are already in progress. The default is 15 minutes. The minimum value is 0, meaning no time is used; the maximum value is 60 minutes.

FIPS Mode Only
Displays the setting that determines whether KMAs in this OKM cluster allow communications involving keys with entities outside the cluster in either non-FIPS or FIPS compliant modes, or in FIPS compliant modes only. In a FIPS compliant mode, KMAs wrap keys with an Advanced Encryption Standard (AES) Wrapping Key before sending them to agents (such as tape drives).
Customers who have tape drives should be running tape drive firmware that supports AES Key Wrap with the OKM agent service. All PKCS#11 providers that support OKM, as well as the OKM JCE provider, include support for AES Key Wrap.
You can confirm whether your agents support AES Key Wrap by viewing the OKM audit log and noting that these agents are using the agent service operations listed below. Specify an audit filter for Operation and choose any of the following specific operations from the menu:

- Create Key v2
- Retrieve Key v2
- Retrieve Keys v2
- Retrieve Protect and Process Key v2

Any audit events in the resulting list confirm that the specified agent is using AES key wrap with the OKM cluster.
There are two possible values for this setting, "Off" and "On". If the current Replication Version is 8 or 9, this setting has a value of "Off" by default and cannot be modified. If the current Replication Version is 10 or higher, this value can be modified to either value.
If this value is set to "Off", the OKM cluster allows communications involving keys with entities outside the cluster in non-FIPS and FIPS compliant modes:

- The OKM cluster accepts key requests from agents using both the old KMS 2.0.x protocol (that does not wrap keys) and the FIPS 2.1 protocol (that does wrap keys).
- Keys from a KMS 1.x system may be imported into the OKM cluster.
- The OKM cluster allows the export and import of "v2.0" or "v2.1 (FIPS)" format key transfer files.

> **Note:**
>
> If the current Replication Version is 8 or 9, there may be KMS 2.0.x KMAs in the cluster that will not be capable of supporting the FIPS protocols for agent and transfer partner communication. KMAs running KMS 2.1 or higher support the FIPS protocols for agent and transfer partner communication even when the current Replication Version is 8 or 9. In this case, exports to transfer partner will be done only in the "v2.0" format because the export format of transfer partners will be set to "Default".

If this value is set to "On", then the OKM cluster allows communications involving keys with entities outside the cluster only in FIPS compliant modes:

- The OKM cluster accepts key requests from agents using only the FIPS 2.1 protocol.
- Keys from a KMS 1.x system cannot be imported into the OKM cluster because the KMS 1.x key export file is not FIPS compliant.
- The OKM cluster allows the export and import of "v2.1 (FIPS)" format key transfer files only.

> **Note:**
>
> For the keys in the OKM cluster to be FIPS compliant, all entities that receive keys from the cluster must handle the keys in a FIPS-compliant manner. Agents that receive keys must handle these keys in a FIPS-compliant manner when using them to process data. Key transfer partners that receive keys should also be operating with the FIPS Mode Only security parameter set to "On" in their cluster to ensure that exported keys maintain FIPS compliance. A key transfer partner can send and receive "v2.1 (FIPS)" format key transfer files with the FIPS Mode Only set to "Off".

See the Export Format parameter in View and Modify the Transfer Partner List for more information.

Pending Operation Credentials Lifetime
The amount of time (in days) that Key Split Credentials are retained as having approved a pending quorum operation. If an insufficient number of Key Split Credentials approve the pending quorum operation before this lifetime is reached, then these credentials expire. After they expire, Quorum Members must reapprove the pending quorum operation. The default is 2 days. This value is used only when the Replication Version is at least 11..

Enroll Agents

Enroll agents after you have configured the cluster.

When you enroll an agent, you provide its Agent ID, its passphrase, and an network address (IP address or host name) of one of the KMAs. The encryption endpoint associated with this agent can then use this OKM cluster.The procedure to enroll an agent is determined by the type of encryption endpoint associated with it:

- **Tape Drives** - Use the Virtual Operator Panel (VOP) to connect to a tape drive and then to enroll the agent associated with it (see the VOP documentation for instructions). With guidance from your Oracle service representative, enroll each tape drive agent. See Enroll Tape Drives .
- **Oracle Database Servers** - Agents associated with Oracle Database servers are enrolled when these Oracle Database servers are configured to use OKM (see Advanced Security Transparent Data Encryption (TDE)).
- **Oracle Solaris ZFS Filesystems** - Agents associated with Oracle Solaris ZFS filesystems are enrolled when these ZFS filesystems are configured to use OKM (see Solaris ZFS Encryption).
- **Oracle ZFS Storage Appliances** - Agents associated with Oracle ZFS Storage Appliances are enrolled when these ZFS Storage Appliances are configured to use OKM. This procedure is described in Oracle ZFS Storage Appliances documentation.
- **Java Applications that use the OKM JCE Provider** - Agents associated with Java applications that use the OKM JCE Provider are enrolled when the OKM JCE Provider is configured to use OKM. This procedure is described in the OKM JCE Provider documentation.

See also: Agents (Encryption Endpoints).

Record Agent Information

Collect agent information for your records.

Agent Type:

IP Address:

Agent ID:

Passphrase: (do not record here)

Default Key Group:

Roaming (true/false):

Can Revoke Keys (true/false):

Agent Type
The Agent Type can be a tape drive type (such as IBM LTO-7) or some other type of agent (such as ZFSSA, PKCS#11 application, Java application). The IP address is needed for tape drives when an Oracle service rep goes to configure them, and is useful when enrolling other types of agents.

Roaming
This attribute shows the opposite value of the Agent's One Time Passphrase attribute. For example, tape drive agents are not roaming agents, therefore the One Time Passphrase attribute should be set to True for these agents.

Can Revoke Keys?
This is an attribute of the Key Policy that is associated with the Default Key Group for that agent. For agents associated with a ZFS Storage Appliance, you must set this attribute to True on the associated Key Policy. You should set this attribute to True for Key Policies used by Java applications that use our OKM JCE Provider. You should set this attribute to False for Key Policies used by tape drive agents. Typically you should set this to False for Key Policies used by other types of agents.

6
Enroll Tape Drives

Enroll tape drives to allow them to retrieve keys used to read and write encrypted data.

Tape Drive Enrollment Process Overview

Enrolling tape drives requires certain steps to be completed by the installer, while other steps must be completed by the customer.

During installation when enrolling the tape drives, the customer can choose if they want to:

- Switch encryption on and off per tape drive.
- Use Tokens to transfer keys from the Token Bay (Version 1.x).
- Permanently encrypt or not.

Steps to enroll a tape drive:

1. Pre-requisite: Install and test tape drives within the tape library and create a private network to connect and configure the tape drives before adding the encryption capability.
2. Customer Task: Create agent IDs and passphrases in the KMAs.
3. Installer Task: Request the enablement keys from the website.
4. Installer Task: Download the enablement Keys to the tape drives (required for T-series tape drives only).
5. Installer Task: Activate the tape drives (agents).
6. Customer Task: Enroll the agents.
7. Customer Task: Assign the agents to a Key Group.

Required Tools for Tape Drive Enrollment

Tape drive enrollment requires specific tools. Verify you have these tools prior to enrolling the drives.

- Straight Ethernet cable, 10 ft (PN: 24100216) if connecting to an Ethernet switch.
- Cross-over Ethernet cable, 10 ft (PN: 24100163) if connecting directly to the drives.
- Service laptop (or personal computer)
- Oracle Virtual Operator Panel (VOP) -
  For VOP, if this is the initial configuration, use a secure point-to-point connection and the default IP address 10.0.0.1. Because all tape drives use the same default IP address, connecting them all to the same switch for the initial configuration will cause problems; unless you power the drives on and configure them one-by-one; including a new IP address.

Supported Tape Drives and Required Firmware Levels

OKM requires minimum drive firmware. Maintain the tape drive firmware at the most current firmware level.

Service Delivery Platform (SDP) does not support the LTO-4 drives. You may need to make adjustments to the network addresses if mixing tape drives on the same KMA and/or SDP network.

Table 6-1 Tape Drives Supported by OKM

Tape Drives	Interface Support	Minimum Firmware
IBM LTO-8	Fibre Channel	HB82 and LKM code 6.02.103 (ADI mode only)
IBM LTO-7	Fibre Channel	FA14
IBM LTO-6	Fibre Channel	CT94
HP LTO-6	Fibre Channel SCSI	J2AS 22CS (SL150) 329S (SL150)
IBM LTO-5	Fibre Channel	BBNH
HP LTO-5	Fibre Channel SCSI	I5BS Y5BS (SL150) X5AS (SL500) Z55S (SL150)
IBM LTO-4	Fibre Channel SCSI	BBH4 BBH4
HP LTO-4	Fibre Channel SCSI	H64S FC B63S (SL500)
T10000D	Fibre Channel/FCoE FICON	4.06.107 4.07.xxx

Table 6-1 (Cont.) Tape Drives Supported by OKM

Tape Drives	Interface Support	Minimum Firmware
T10000C	Fibre Channel FICON	1.53.316 1.53.316
T10000B	Fibre Channel FICON	1.38.x07 1.38.x09
T10000A	Fibre Channel FICON	1.37.113 1.37.114
T9840D	Fibre Channel FICON & ESCON	1.42.x07 1.42.x07

About the Ethernet Adapter Card for LTO Drives

Certain LTO tape drives require an adapter card to communicate with the OKM. These vendor-specific adapter cards are a translation device between the serial interface on the tape drive and the secure Ethernet port for use with OKM.

- HP Dione card — installed in encryption-capable HP LTO-4 drive trays
- IBM Belisarius card — installed in encryption-capable IBM LTO-4, 5, 6, an 7 drive trays.
- LKM card - installed in encryption capable IBM LTO-7 and 8 drive trays.

Re-enrollment does not require deleting the agent at the OKM, they can simply set a new passphrase for the agent and then re-enroll the drive using the VOP.

Each card includes a:

- Telnet server (for configuration and management)
- FTP server (for installing new firmware and retrieving firmware trace logs)
- Simple Object Access Protocol (SOAP) client (with TLS 1.0 support) for communication with the OKM

Compatibility with the OKM requires an appropriate level of drive firmware and adapter card firmware.

Use the instructions in the library service manuals for details about how to remove and replace the LTO tape drives and adapter cards in each type of library.

> **Caution:**
>
> The adapter cards contain ESD-sensitive components. Improper handling could result in damage to these components. Make sure to follow proper ESD precautions and procedures.

Gather Information about the Tape Drives

The installer should gather key information from the customer about their tape drives before enrollment.

- What is the drive number (serial or system) and IP address?
- Is this drive going to use tokens (KMS Version 1.x) to get media keys? Or use the appliance (KMA) to get the encryption keys?
- Does the customer want this drive to remain in encryption mode? Or do they want the ability to switch encryption on and off?

Obtain the T10000 Encryption Enablement Drive Data (Installer Task)

T10000 drives running firmware versions below 1.57.30x (T10000C) or 4.06.106 (T10000D) require Encryption Enablement Keys (E-keys). The installer must obtain the enablement data.

Drives with 1.57.30x or 4.06.106 and higher firmware levels display a *Licensed* status on VOP screens. Skip the following procedures and go to Enroll the Tape Drives (Customer Task) to complete an installation or replacement for these drives.

1. Using the VOP, connect to and power-on each tape drive.
2. Record the last eight digits of the tape drive serial number.
3. See "Retrieve Menu" in the "Using T10000 9840D VOP" chapter of the Oracle Virtual Operator Panel User's Guide to view drive data.
4. See "Configure Menu" in the "Using T10000 9840D VOP" chapter of the Oracle Virtual Operator Panel User's Guide to build information about the tape drives.
5. You will find this information helpful during the installation, activating, and enrollment process for the tape drives (called agents).
6. Request an Encryption Key File:
    a. Log in to the CRCApplications Web. **Access is Limited:** You must be an employee, have completed the training courses, and have your name included on the list to access this link.
    b. Select Request an Encryption key.
7. Complete the Encryption Request form.
    a. First name, last name, and e-mail address are automatically included.
    b. Provide a site ID and order number.
    c. Select the tape drive type.
    d. Complete the serial number for the selected tape drive.
    e. Add any optional remarks and click Request Key File.

    After submitting the Encryption File Request a prompt displays to download the file. This file contains the drive data you need to enable and enroll the drive. Family serial numbers start with:

- T10000A =5310 xxxxxxxx
- T10000B =5720 xxxxxxxx
- T10000C =5760 xxxxxxxx
- T10000D =5790 xxxxxxxx
- T9840D =5700 xxxxxxxx

When selecting the Driver Family type, the first four numbers are automatically filled in.

8. Continue with this process until you obtain all the drive data files for each tape drive you are going to enable.

   If you open the drive data file, using WordPad for example, you can see and verify the drive serial number, enablement key, and crypto serial number (CSN). For example:

   ```
   03B90866E66E1404C596FA0628B6335F435BB43302583AFDB4B121A6CB2C8E52
   000160
   02531002001232
   ```

9. Create a drive data file structure.

   When enabling multiple drives, it is best to create a file structure where each tape drive has its own folder. For example:

   ```
   crypto_drvs
       1234
           drive_data.txt
       1235
           drive_data.txt
       1236
       ...
   ```

   Under `crypto_drvs` are the folders for each tape drive using the serial numbers. In each serial number folder is the drive data file for that specific tape drive.

Activate the Tape Drives (Installer Task)

The installer must activate the tape drives before enrolling them in OKM. T10000 and LTO drives use different methods for activation.

Refer to the VOP documentation as necessary to complete the tasks below.

For T10000 Drives:

1. Configure and connect the laptop with the drive data file structure to the:
   - Tape drive—private network—using an Ethernet switch and standard cable (use the assigned IP addresses for the tape drives)
   - Tape drive—direct connect—using a cross-over Ethernet cable (use the default IP address 10.0.0.1)
2. Launch VOP and connect to a specific tape drive.
3. On the VOP main screen:
   - Take the drive offline.
   - Click Configure on the menu bar.

- Select the Drive Data command.

4. Build the tape drive information.

For LTO Drives:

1. Configure and connect a laptop to an LTO tape drive.
2. Start the executable ltoVOP file.
3. Enter the default IP address (10.0.0.1) and click Connect (A).

   When enrolling HP LTO-4 and IBM LTO tape drives into the OKM, you are enrolling the adapter card, not the actual tape drive. Therefore replacing the drive does not require re-enrollment, but replacing the adapter card or drive tray with a new adapter card does require re-enrollment.

> **Note:**
>
> For HP LTO-5 and LTO-6 tape drives, the ethernet port is integrated into the drive.

4. Set the drive Offline using VOP.
5. Select the Configure Drive tab.
   This tab allows you to configure the drive to use settings other than the default settings currently in the drive.
6. Enter the new IP address, netmask, and gateway information for the drive.
7. Click the Commit button.
8. Click the Service Drive tab to observe the commit process in the open display.
   - During the commit process, the tape drive goes offline, then IPLs to save the new settings to the adapter card.
   - When the drive comes back online, it is now using the new IP address entered in step 6.
   - Depending on the IP address of the tape drive, you may also need to change the IP address of the laptop to connect to the network.

Enroll the Tape Drives (Customer Task)

Drives must be enrolled to access keys from OKM. T10000 and LTO drives use different methods for enrollment.

For T10000 Drives:

1. After the drive reboots:
   - Take the drive offline.
   - Click Configure on the menu bar.
   - Select the Drive Data command.
2. See "Configure Menu" in the "Using T10000 9840D VOP" of the Oracle Virtual Operator Panel User's Guide to enroll the tape drives and commit the tape drive settings.

3. Click Retrieve on the menu bar and select the View Drive Data command.

For LTO Drives:

1. Click the Enroll Drive tab to start the tape drive enrollment process.
   - The tape drive and/or adapter card must be connected to the OKM network.
   - The OKM must be able to communicate with the adapter card and tape drive.

   > **Note:**
   >
   > The Agent must already be created with a passphrase assigned in the OKM before you can enroll the drive.

   See "Enroll Drive" in the "Using LTO VOP" chapter of the *Oracle Virtual Operator Panel User's Guide*.

   If you were to unenroll the Agent in situations—such as when turning encryption off—then you need to re-enroll the agent to turn encryption back on.

   The same passphrase must be re-entered or the agent must be recreated in the OKM before re-enrollment.
2. Enter the KMA Agent ID, KMA Service[1]IP Address, and Passphrase.
3. Click the Enroll button.
4. Click the Monitor Drive tab to observe the enroll process in the open display. See "Monitor Drive" in the "Using LTO VOP" chapter of the *Oracle Virtual Operator Panel User's Guide*.
5. Set the drive Online. Click the Online status indicator or click the Set Online button under either the Enroll Drive or Configure Drive tab.
6. Proceed to the next drive.

Assign Key Groups for Each Tape Drive (Customer Task)

Assign a key group to each tape drive you have enrolled. The tape drive will only retrieve keys from the key groups that you assign to it.

Use OKM manager to assign keys to the tape drives.

1. In the left navigation area, expand **Key Groups**, and then select **Agent Assignment to Key Groups**.
2. In the "Key Groups" column, highlight a key group.
3. Move agents between the "Agents Allowed Access" or the "Agents Not Allowed Access" column. To move, highlight the agent and then click **<** or **>** to add or remove agent access.

[1] The KMA has two network connections, Management and Service. Make sure you use the Service IP address and not the Management IP address.

> **Note:**
>
> You must set a default key group for an agent before that agent can allocate keys. When an agent creates a key (assigns it to a data unit), the key is placed into the agent's default key group.

4. To assign a default key group, select an agent and then click **< Default Key Group**.

Switch Encryption On and Off

Turn encryption on and off if the drive is in an environment that uses both encrypted and non-encrypted data.

To turn encryption off:

1. Use the Virtual Operator Panel and connect to the desired tape drive.
2. Select: Drive Operations > Reset Drive.
3. Reply "Yes" to the Are You Sure? dialog box.

   The drive must be in the RESET state to turn encryption off.
4. Click **Yes** to `Turn encryption off`.
5. Click **Commit**. The tape drive will reboot and be non-encrypting.

To turn encryption back on, use the Configuration menu.

Use Tokens to Transfer Encryption Keys

The tape drives can support Version 1.x and the use of Tokens to transfer encryption keys. However, Version 1.x is End-of-Life and is not recommended.

1. Using the Virtual Operator Panel, connect to the desired tape drive.
2. Select: Configure > Drive Data.
3. For the `Use tokens`: Parameter Value, click **Yes**.
4. Click **Commit**.

Rebuild the Media Information Region for T10000 Drives

Rebuild the MIR to recover from a bad RFID chip.

The T10000 tape drives use information recorded on each tape cartridge to reduce access times and manage the useful life of the cartridge. This information is recorded and stored in the cartridge's radio frequency identification (RFID) chip and at the beginning-of-tape (BOT) in an area known as the media information region (MIR).

Occasionally, the REBUILD MIR utility can try to recover from a bad RFID chip in the cartridge. If the utility fails, try the rebuild utility on more than one drive. If the utility still fails, create a dump file, and send it to technical support for analysis.

> **Note:**
>
> There is no special process to rebuild a MIR for the type of T10000 tape drive (A or B, and encryption-capable or unencrypted). The rebuild MIR process is an offline process that maps data and defects on the tape and does not care if the data is encrypted or not.

1. Make sure drive is unloaded before activating the Build MIR utility. `Rebuild MIR` flashes on the operator panel while the MIR is rebuilding.
2. Approximate time for a full tape Build MIR varies by the cartridge type:
   - Standard T1 Data cartridge is approximately 120 minutes.
   - Sport T1 Data cartridge is approximately 48 minutes.
3. If a `CHKxxxx` appears, see the FSC Dictionary for information.
4. Connect a tape drive to the VOP.
5. Use the Menu and Select buttons to navigate to the utility:
   - Press `Menu` to bypass
   - Press `Select` to activate.
6. When `Ld Cust Tp` appears, insert the write-enabled data cartridge with the invalid MIR.

   With encryption-capable tape drives, a series of messages may appear several times until the rebuild MIR operation continues. Examples of these messages include:

   ```
   KMS2.0: my_tcp_connect select returned 0 err=236(op now in progress)
   ```

   ```
   KMS2.0: AUDIT_CLIENT_GET_CLUSTER_Information_SOAP_ERROR
   ```

   ```
   KMS2.0: All drives keys turned off
   ```

   After these messages occur, the Rebuild MIR starts.
7. When the MIR is rebuilt, the cartridge unloads. Remove the cartridge.
8. Insert another write-enabled data cartridge requiring a MIR rebuild; or Press Menu to exit the build MIR submenu.

7

Basic OKM GUI Operations

Basic OKM GUI operations are tasks commonly completed by any user and apply to numerous GUI tasks.

- Disconnect from the KMA
- Access Online Help
- Filter Lists
- Export a List as a Text File (Save Report)
- Navigate OKM Manager with the Keyboard
- Specify OKM Manager Configuration Settings

Disconnect from the KMA

Disconnect from the KMA to terminate the OKM Manager connection with the KMA and cluster.

From the **System** menu of OKM Manager, select **Disconnect** (or click **Disconnect** in the tool bar).
The session Audit Log pane indicates the date and time you disconnected from the KMA.

Access Online Help

OKM Manger includes comprehensive online help. Access it from the OKM Manager interface.

From any OKM Manager screen, click the **Help** button that is located at the top of the panel for general help. Or navigate to a panel by either pressing the **Tab** key or by clicking somewhere within the panel. Then, press **F1** to view context-sensitive help.

Filter Lists

Apply filtering to lists to view a subset of the data.

1. From a list within OKM Manager (such as KMAs, Users, and so on), use the filter drop-down menus to select a criteria, and then entering a value into the field. Click **Use** to apply the filter.
2. Click a column name to sort by the attribute.
3. To clear the filter, click **Reset**.

Export a List as a Text File (Save Report)

Export list entries as a tab separated file that you can import into a spreadsheet application.

1. From any list screen within OKM manager, go to the **View** menu and then select **Save Report...** (or press Ctrl-S).
2. Click **Start** to initiate the export. If you have filtered the entries list, only those entries are exported.

Navigate OKM Manager with the Keyboard

Navigate through the OKM Manager using key strokes instead of the mouse.

Accelerator Keys: Accelerator keys provide keyboard shortcuts for menu items and dialog controls.

- **Alt+S:** Pulls down the System Menu.
- **Alt+V:** Pulls down the View Menu.
- **Alt+H:** Pulls down the Help Menu.
- **F1:**Display online help information about the current screen or dialog
- **F5:** Refreshes a List screen.

Navigational keys, such as up and down arrow keys, move the focus around various elements in the Oracle Key Manager GUI.

Navigating in Screens and Dialog Boxes:

- **Tab:** Navigates from one button, text field, check box, table, or combobox to the next one.
- **Shift+Tab:** Navigates from one button, text field, table, check box, or combobox to the previous one.
- **Up/down arrow key:** Displays the next/previous entry in a combobox or table.
- **Space:** Sets or clears the current check box.
- **Enter:** Invokes the operation of the current button, or brings up the details of the selected table entry.
- **Ctrl+Tab** (on Windows): Navigates across tabbed panes in a dialog box.
- **Left/right arrow keys:** Navigates across tabbed panes in a dialog box. First press Shift+Tab to navigate to the tab of the current tabbed pane.

Specify OKM Manager Configuration Settings

Set timeouts, page size, time zone, tool tips, and zone IDs.

Available to: All roles

1. From the **System** menu, select **Options....**

> **Note:**
>
> The options selected are stored in the Windows Registry or in "`~/.KMS Manager`" for other platforms (where ~ is the user's home directory). The Windows Registry key for these values is "`My Computer \HKEY_CURRENT_USER\Software\Sun Microsystems\KMS Manager`."

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

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

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

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

   Display Tool Tips on List Panels — Select this check box if you want to see a tool tip when you position the cursor over an item. This is the default.

   Zone ID — If your KMAs are configured to have IPv6 addresses and if you want to connect to one of them using an IPv6 link-local address (that is, one that begins with "fe80"), then select a Zone ID to use when connecting to that link-local address. See IPv6 Addresses with Zone IDs for more information.

IPv6 Addresses with Zone IDs

Windows users can enter link-local IPv6 addresses.

> **Note:**
>
> You must enter a Zone ID whenever you specify a link-local address (that is, an IPv6 address that begins with "fe80"). You can specify a Zone ID by appending it to the end of an IPv6 address, following a percent sign (%).

1. Display a command prompt window and determine which Zone IDs are available on your Windows system.

   ```
   netsh interface ipv6 show interface
   ```

   The Zone IDs appear in the Idx column in the output of this command. Look for entries that show a State of "Connected."

2. Use the ping command to confirm network connectivity using one of these Zone IDs. For example:

   ```
   ping fe80::216:36ff:fed5:fba2%4
   ```

3. Before you open the Connect dialog in the OKM Manager GUI, display the Options dialog and select the appropriate Zone ID.
4. Click **Save**.

8
Users and Roles

OKM manager limits access to certain functions based on the user and role. The security officer manages and creates users.

- Change Your Passphrase
- View a List of Users
- Create a User
- Modify a User's Details and Set the User's Passphrase
- Delete a User
- View Roles and Valid Operations

Change Your Passphrase

Users can change their own passphrase. Changing your passphrase does not invalidate your current user certificate.

1. From the **System** menu, select **Change Passphrase....**.

   This menu option is only enabled if you are connected to a KMA using your profile.

2. Update the passphrase. The phrase must meet the requirements listed in Passphrase Requirements.

Passphrase Requirements

Passphrases for Agents, KMAs, OKM users, and key split users must meet minimum requirements.

- Length between 8 and 64 characters (to modify the minimum length requirement for passphrases, see Review and Modify the Cluster Security Parameters)
- Must not contain the identifier or name of this agent, KMA, or user.
- Must contain three of the four character classes: uppercase, lowercase, numeric, or special characters.
- Can contain the following special characters:

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

- Cannot use control characters, including tabs and line feeds.

View a List of Users

View a list of all users configured to use OKM Manager.

Available to: Security Officer

From the **System Management** menu, select **User List**. See Filter Lists to filter the list.

Create a User

Create a user with a specific role to provide someone access to OKM Manager.

Available to: Security Officer (requires a quorum)

1. From the **System Management** menu, select **User List**. Click **Create...**
2. On the **General** tab, enter the following:
   - **User ID** — Uniquely identifies the user. Can be between 1 and 64 (inclusive) characters.
   - **Description** — Describes the user. This value can be between 1 and 64 (inclusive) characters.
   - **Roles** — The roles you want the user to perform.

   > **Note:**
   >
   > The Quorum Member check box is disabled (grayed out) if the KMA currently runs KMS 2.1 or earlier or if the replication version of the OKM cluster is currently set to 10 or lower.
3. Click the **Passphrase** tab and enter the passphrase. Confirm the passphrase (retype the same passphrase). The phrase must meet the requirements listed in Passphrase Requirements.
4. Creating a user requires a quorum. Within the Key Split Quorum Authentication dialog, the quorum must type their usernames and passphrases to authenticate the operation. See Quorum Authentication for more information.
5. Record User Information to keep track of OKM users.

Record User Information

Collect user information for future reference. Do not record passphrases for security reasons.

User ID:
Description:
Roles:

Modify a User's Details and Set the User's Passphrase

For security reasons, you may need to modify another user's details and passphrase.

Available to: Security Officer (requires a quorum for role or passphrase change)

> **Note:**
>
> The currently logged-in Security Officers cannot modify their own records.

1. From the **System Management** menu, select **User List**. Double-click a user (or highlight a user and click the **Details...**).
2. On the **General** tab, you can modify the Description, Roles, and Enabled Flag.
3. On the **Passphrase** tab. You can change the user's passphrase. The phrase must meet the requirements listed in Passphrase Requirements.
4. Click **Save**.
5. If you added user roles or changed the passphrase, within the Key Split Quorum Authentication dialog, the quorum must type their usernames and passphrases to authenticate the operation. See Quorum Authentication for more information.
6. Notify the user that their information has changed.

Delete a User

Delete a user to remove them from OKM Manager. Users cannot delete themselves.

Available to: Security Officer

1. From the **System Management** menu, select **User List**. Select the user you want to delete and click **Delete**.
2. Click **Yes** to confirm.

View Roles and Valid Operations

The security officer can view roles and a list of operations each role can perform.

Available to: Security Officer

1. To view the role list, expand **System Management**, select **Role List**. See Filter Lists to filter the list.
2. To view a list of operations for each role, highlight a role, and then click **Details...**

Available Roles

Each role determines which functions the user can perform. A user can have more than one role.

- **Security Officer** – manages security settings, users, sites, and transfer partners
- **Compliance Officer** – manages key policies and key groups and determines which agents and transfer partners can use key groups
- **Operator** – manages agents, data units, and keys
- **Backup Operator** – performs backups
- **Auditor** – views information about the OKM cluster
- **Quorum Member** – views and approves pending quorum operations.

Valid Operations for Each Role

The operations available to a user depend on their role. This table lists the actions each role can perform.

In the table, the entries mean the following:

- **Yes** – the role can perform the operation.
- **No** – the role cannot perform the operation.
- **Quorum** – the role can perform the operation but must also provide a quorum.

Table 8-1 System Operations/User Roles

Entity	Operation	Security Officer	Comp. Officer	Oper.	Backup Oper.	Auditor	Quorum Member
Console	Log In	Yes	Yes	Yes	Yes	Yes	Yes
Console	Set KMA Locale	Yes	No	No	No	No	No
Console	Set KMA IP Address	Yes	No	No	No	No	No
Console	Enable Tech Support	Yes	No	No	No	No	No
Console	Disable Tech Support	Yes	No	Yes	No	No	No
Console	Enable Primary Administrator	Yes	No	No	No	No	No
Console	Disable Primary Administrator	Yes	No	Yes	No	No	No
Console	Restart KMA	No	No	Yes	No	No	No
Console	Shutdown KMA	No	No	Yes	No	No	No
Console	Log OKM into Cluster	Quorum	No	No	No	No	No
Console	Set User's Passphrase	Yes	No	No	No	No	No
Console	Reset KMA	Yes	No	No	No	No	No
Console	Show Cluster Root CA Certificate Properties	Yes	Yes	Yes	Yes	Yes	Yes
Console	Re-key Root CA Certificate	Yes	No	No	No	No	No
Console	Logout	Yes	Yes	Yes	Yes	Yes	Yes
Connect	Log In	Yes	Yes	Yes	Yes	Yes	Yes
Connect	Create Profile	Yes	Yes	Yes	Yes	Yes	Yes
Connect	Delete Profile	Yes	Yes	Yes	Yes	Yes	Yes
Connect	Set Config Settings	Yes	Yes	Yes	Yes	Yes	Yes
Connect	Disconnect	Yes	Yes	Yes	Yes	Yes	Yes
Key Split Credentials	List	Yes	No	No	No	No	No
Key Split Credentials	Modify	Quorum	No	No	No	No	No
Autonomous Unlock	List	Yes	No	No	No	No	No

Table 8-1 (Cont.) System Operations/User Roles

Entity	Operation	Security Officer	Comp. Officer	Oper.	Backup Oper.	Auditor	Quorum Member
Autonomous Unlock	Modify	Quorum	No	No	No	No	No
Lock/Unlock KMA	List Status	Yes	Yes	Yes	Yes	Yes	No
Lock/Unlock KMA	Lock	Yes	No	No	No	No	No
Lock/Unlock KMA	Unlock	Quorum	No	No	No	No	No
Site	Create	Yes	No	No	No	No	No
Site	List	Yes	No	Yes	No	No	No
Site	Modify	Yes	No	No	No	No	No
Site	Delete	Yes	No	No	No	No	No
Security Parameters	List	Yes	Yes	Yes	Yes	Yes	No
Security Parameters	Modify	Yes	No	No	No	No	No
KMA	Create	Quorum	No	No	No	No	No
KMA	List	Yes	No	Yes	No	No	No
KMA	Modify	Quorum	No	No	No	No	No
KMA	Delete	Yes	No	No	No	No	No
User	Create	Quorum	No	No	No	No	No
User	List	Yes	No	No	No	No	No
User	Modify	Yes	No	No	No	No	No
User	Modify Passphrase	Quorum	No	No	No	No	No
User	Delete	Yes	No	No	No	No	No
Role	Add	Quorum	No	No	No	No	No
Role	List	Yes	No	No	No	No	No
Key Policy	Create	No	Yes	No	No	No	No
Key Policy	List	No	Yes	No	No	No	No
Key Policy	Modify	No	Yes	No	No	No	No
Key Policy	Delete	No	Yes	No	No	No	No
Key Group	Create	No	Yes	No	No	No	No
Key Group	List	No	Yes	Yes	No	No	No
Key Group	List Data Units	No	Yes	Yes	No	No	No
Key Group	List Agents	No	Yes	Yes	No	No	No
Key Group	Modify	No	Yes	No	No	No	No
Key Group	Delete	No	Yes	No	No	No	No
Agent	Create	No	No	Yes	No	No	No
Agent	List	No	Yes	Yes	No	No	No
Agent	Modify	No	No	Yes	No	No	No

Table 8-1 (Cont.) System Operations/User Roles

Entity	Operation	Security Officer	Comp. Officer	Oper.	Backup Oper.	Auditor	Quorum Member
Agent	Modify Passphrase	No	No	Yes	No	No	No
Agent	Delete	No	No	Yes	No	No	No
Agent/Key Group Assignment	List	No	Yes	Yes	No	No	No
Agent/Key Group Assignment	Modify	No	Yes	No	No	No	No
Data Unit	Create	No	No	No	No	No	No
Data Unit	List	No	Yes	Yes	No	No	No
Data Unit	Modify	No	No	Yes	No	No	No
Data Unit	Modify Key Group	No	Yes	No	No	No	No
Data Unit	Delete	No	No	No	No	No	No
Keys	List Data Unit Keys	No	Yes	Yes	No	No	No
Keys	Destroy	No	No	Yes	No	No	No
Keys	Compromise	No	Yes	No	No	No	No
Transfer Partners	Configure	Quorum	No	No	No	No	No
Transfer Partners	List	Yes	Yes	Yes	No	No	No
Transfer Partners	Modify	Quorum	No	No	No	No	No
Transfer Partners	Delete	Yes	No	No	No	No	No
Key Transfer Keys	List	Yes	No	No	No	No	No
Key Transfer Keys	Update	Yes	No	No	No	No	No
Transfer Partner Key Group Assignments	List	No	Yes	Yes	No	No	No
Transfer Partner Key Group Assignments	Modify	No	Yes	No	No	No	No
Backup	Create	No	No	No	Yes	No	No
Backup	List	Yes	Yes	Yes	Yes	No	No
Backup	List Backups with Destroyed Keys	No	Yes	Yes	No	No	No
Backup	Restore	Quorum	No	No	No	No	No
Backup	Confirm Destruction	No	No	No	Yes	No	No
Core Security Backup	Create	Yes	No	No	No	No	No
SNMP Manager	Create	Yes	No	No	No	No	No
SNMP Manager	List	Yes	No	Yes	No	Yes	No
SNMP Manager	Modify	Yes	No	No	No	No	No
SNMP Manager	Delete	Yes	No	No	No	No	No
Audit Event	View	Yes	Yes	Yes	Yes	Yes	No

Table 8-1 (Cont.) System Operations/User Roles

Entity	Operation	Security Officer	Comp. Officer	Oper.	Backup Oper.	Auditor	Quorum Member
Audit Event	View Agent History	No	Yes	Yes	No	No	No
Audit Event	View Data Unit History	No	Yes	Yes	No	No	No
Audit Event	View Data Unit Key History	No	Yes	Yes	No	No	No
System Dump	Create	Yes	No	Yes	No	No	No
System Time	List	Yes	Yes	Yes	Yes	Yes	No
System Time	Modify	Yes	No	No	No	No	No
NTP Server	List	Yes	Yes	Yes	Yes	Yes	No
NTP Server	Modify	Yes	No	No	No	No	No
Software Version	List	Yes	Yes	Yes	Yes	Yes	No
Software Version	Upgrade	No	No	Quorum	No	No	No
Software Version	Delete	No	No	Yes	No	No	No
Network Configuration	Display	Yes	Yes	Yes	Yes	Yes	No
Pending Quorum Operation	Approve	No	No	No	No	No	Quorum
Pending Quorum Operation	Delete	Yes	No	No	No	No	No
Key List	Query	No	Yes	Yes	No	No	No
Key List	List Activity History	No	Yes	Yes	No	No	No
Agent Performance List	Query	No	Yes	Yes	No	No	No
KMA Performance List	Query	Yes	Yes	Yes	Yes	Yes	Yes
Current Load	Query	Yes	Yes	Yes	Yes	Yes	Yes
Remote Syslog	List	Yes	No	No	No	Yes	No
Remote Syslog	Create	Yes	No	No	No	No	No
Remote Syslog	Modify	Yes	No	No	No	No	No
Remote Syslog	Delete	Yes	No	No	No	No	No
Remote Syslog	Test	Yes	No	No	No	No	No
Hardware Management Pack	Download MIB Bundle	Yes	No	No	No	No	No
Hardware Management Pack	Get Status	Yes	No	No	No	Yes	No
Hardware Management Pack	Enable	Yes	No	No	No	No	No
Hardware Management Pack	Disable	Yes	No	No	No	No	No
Hardware Management Pack	Test	Yes	No	No	No	No	No

9
Monitor KMAs

Use SNMP, HMP, and OKM Manager logs to monitor KMAs.

- Configure SNMP
- Configure the Hardware Management Pack (HMP)
- Display the Current Load
- View and Export Audit Logs
- Create a System Dump
- Send Messages to Remote Syslog Servers

Configure SNMP

Use SNMP to monitor KMAs in the cluster.

KMAs generate SNMP information for users who have configured an SNMP agent in the network and defined SNMP Managers in the OKM Manager GUI.

- SNMP Protocol Versions
- SNMP MIB Data
- View SNMP Managers for a KMA
- Create a New SNMP Manager
- Modify an SNMP Manager's Details
- Delete an SNMP Manager

SNMP Protocol Versions

An SNMP Manager can use either SNMPv3 or SNMPv2.

- v3 supports authentication, using user names and passphrases. Oracle recommends SNMPv3.
- v2 does not support authentication and does not use user names and passphrases.

  KMAs do not send SNMP informs to SNMP Managers configured to use SNMPv2 if the replication version of the OKM cluster is currently set to 10 or lower.

SNMP MIB Data

A table describing SNMP Management Information Base (MIB) information used by the KMA.

HMP uses additional MIBs. These may be downloaded from the KMA for installation in your SNMP Manager. See Configure the Hardware Management Pack (HMP) for more information and the list of MIBs.

Table 9-1 KMA Object Identifiers

OID Value	Type	Description
1.3.6.1.4.1.42.2.22.99.109.1	----	Generic trap
1.3.6.1.4.1.42.2.22.99.1	string	Date/time
1.3.6.1.4.1.42.2.22.99.2	string	Audit event class
1.3.6.1.4.1.42.2.22.99.3	string	Audit event operation
1.3.6.1.4.1.42.2.22.99.4	string	Audit event condition
1.3.6.1.4.1.42.2.22.99.5	string	Audit event severity
1.3.6.1.4.1.42.2.22.99.6	string	Entity ID
1.3.6.1.4.1.42.2.22.99.7	string	Network address
1.3.6.1.4.1.42.2.22.99.8	string	Message
1.3.6.1.4.1.42.2.22.99.9	string	Audit event solution

View SNMP Managers for a KMA

View a list of SNMP managers configured for the KMA.

Available to: Security Officer, Operator, Auditor

1. In the left navigation tree, expand **System Management**, and then select **SNMP Manager List**. See Filter Lists to filter the list.
2. For details, highlight an SNMP entry and click **Details...**.

Create a New SNMP Manager

Create an SNMP Manager to monitor KMAs within the cluster. KMAs will send SNMP Informs to the IP address of that SNMP Manager.

Available to: Security Officer

1. **If the SNMP agent is using v3**: Create an v3 user before creating an SNMP manager in your OKM cluster. The user should use SHA (not MD5) as the authentication protocol and DES as the privacy protocol. Refer to your SNMP agent documentation for more information.

   If the SNMP agent is using v2: For OKM versions prior to 3.3.2/replication versions prior to 16, you do not need to configure an authentication protocol or create an SNMP user. Only the "public" community for SNMPv2 is supported.
2. In the left navigation tree, expand System Management, and then select **SNMP Manager List**. Click the **Create...**

3. Complete the following:
   - **SNMP Manager ID** — Uniquely identifies the SNMP Manager. This value can be between 1 and 64 (inclusive) characters.
   - **Description** — Describes the SNMP Manager. This value can be between 1 and 64 (inclusive) characters. Optional.
   - **Network Address** — The SNMP Manager's network address.
   - **Enabled** — Select the Enabled check box to indicate SNMP is enabled.
   - **Protocol Version** — Select v3 or v2. For more information, see SNMP Protocol Versions.
   - **User Name** — The user name that is used to authenticate the SNMP Manager.
   - **Passphrase** — The passphrase that is used to authenticate the SNMP Manager.
   - **Community String** — The agent community string. Configuring `public` or `private` as valid community strings is a major security risk.
4. Click **Save**.

Modify an SNMP Manager's Details

Modify an SNMP Manager's details to update its information.

Available to: Security Officer

1. In the left navigation tree, expand **System Management**, and then select **SNMP Manager List**.
2. Double-click an SNMP Manager entry (or highlight an entry and click **Details...**).
3. Change the parameters, as required. Every time you modify a SNMP Manager's details, you must reenter the passphrase.
4. Click **Save**.

Delete an SNMP Manager

Delete an SNMP Manager when you no longer want it to receive SNMP information.

Available to: Security Officer

1. In the left navigation tree, expand **System Management**, and then select **SNMP Manager List**.
2. Highlight the SNMP Manager to delete, and then click **Delete...**
3. Confirm the deletion by clicking **Yes**.

Configure the Hardware Management Pack (HMP)

The hardware management pack installs components used to manage and configure the server. HMP can enhance ILOM's ability to report system details and assist with SNMP configuration.

The HMP is available only on Sun Fire X4170 M2, Netra SPARC T4-1, SPARC T7-1, and SPARC T8-1 servers. For more information about HMP, see https://docs.oracle.com/cd/E52095_01/.

Configuring HMP gives you access to the following:

- Event notification of hardware issues before they show up as OKM specific traps or as a KMA outage. These MIBs are configured to allow for enhanced monitoring of the KMA through SNMP `SUN-HW-MONITORING-MIB`, `SUN-HW-TRAP-MIB`, `SUN-STORAGE-MIB`. See Download the HMP MIBs from the OKM Manager GUI.
- Ability to use read-only `get` operations to the various MIBs provided.
- SNMP Receivelets — Oracle Enterprise Manager (OEM) Receivelets can be implemented that turn OKM SNMP `informs`/`traps` into OEM alerts.
- SNMP Fetchlets — This OEM facility can be used to leverage the MIBs installed with HMP for monitoring KMA host data.
- ILOM
  - O/S Information is displayed on the ILOM Summary Page when HMP is installed. When you are using the ILOM Command Line Interface (CLI), enter:`show /system primary_operating system`
  - Storage Monitoring is enabled when the HMP is installed. Enter the following ILOM CLI command:`show /system/storage`
  - View storage health information, enter: `show /system/storage health`

Download the HMP MIBs from the OKM Manager GUI

HMP uses specific MIBs. To view them, you can download them from OKM Manager or My Oracle Support.

Available to: Security Officer

Download from OKM Manager GUI

1. Select **Hardware Management Pack** on the **Local Configuration** menu.
2. Within the Hardware Management Pack panel, click **Download MIB Bundle**. Browse to a download location and then click **Start**.

Download from My Oracle Support

1. Click the **Patches & Updates** tab.
2. Click **Product or Family (Advanced)**.
3. In the Product field, enter **Oracle Hardware Management Pack**.
4. In the Release field, select the latest release from the menu.
5. In the Platform field, select the platform.

HMP Prerequisites

Before enabling HMP, verify all prerequisites are met.

- (Recommended) Configure the ILOM identification information using the ILOM BUI or CLI. The KMA SNMP daemon logs a warning when these fields are not

configured. The subsequent SNMP notifications will contain this information and aid with troubleshooting. The recommended fields to configure are:

  - SP Hostname
  - SP System Identifier
  - SP System Contact
  - SP System Location
  - Local Host Interconnect

- The Local Host Interconnect settings in Oracle ILOM must be in the Host Managed state (this is the default state). To verify using the ILOM user interface, navigate to ILOM Administration, and then select the Connectivity panel. On the Network tab's page, verify the Local Host Interconnect Status is "Host-Managed" and an IP address is shown, (typically)169.254.182.76.
- The ILOM Administration and Notifications must not have an alert rule configured for Alert ID 15, as this will be used when configuring HMP to have faults forwarded. From the ILOM BUI, navigate to ILOM Administration, then select the Notifications panel. On the Alerts tab, check Alert ID 15. From the ILOM CLI, "`show /SP/alertmgmt/rules/15`".
- IPMI must be enabled in the ILOM. For the ILOM BUI see ILOM Administration:ManagementAccess and the IPMI tab.

Enable/Disable HMP

Enable or disable HMP using OKM Manager.

Available to: Security Officer

1. Select **Hardware Management Pack** on the **Local Configuration** menu.
2. Within the Hardware Management Pack panel, click **Enable** to configure HMP or **Disable** to unconfigure it. Click **Test** to issue a test fault.

Display the Current Load

View current load information to see how busy the KMA is.

Available to: All roles

In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Current Load**. This menu allows you to query load information about the KMA the GUI is connected to.

View and Export Audit Logs

Audit logs provide information on KMA activity.

Available to: All roles, Auditor and Compliance Officer (can view Agent History, Data Unit History, Data Unit Key History)

1. From the **System Management** menu, select **Audit Event List**. See Filter Lists to filter the list.
2. To view detailed information, select an Audit Log entry in the list, and then click **Details...** (or double-click the entry).

3. To export a report, select **Save Report...** from the **View** menu (or press Ctrl-S).
4. Click **Start** to initiate the export. If you have filtered the entries in the Audit Event List screen, only those entries are exported. Otherwise, all audit events are exported.

Audit Log - Field Descriptions

The following are descriptions of the fields found within audit logs.

- **Created Date** - Date and time that the Audit Event was created.
- **Operation** - The operation that resulted in the creation of the Audit Event record.
- **Severity** - Indicates the severity of the condition if the operation was not successful. Possible values are Success (no error), Warning, or Error. If the Severity value is Error, the KMA that generated the event also issues an SNMP inform message with the event details.
- **Condition** - Indicates whether the operation was successful or not. Errors are highlighted in red. Warnings are highlighted in yellow. If you hover the cursor over an error message, a more detailed description of the error is displayed. If the Condition value is Server Busy, the KMA that generated the event also issues an SNMP inform message with the event details.
- **Event Message** - Detailed information of the Audit Event entry.
- **Entity ID** - If this Audit Event is generated in response to an operation requested by a user, agent, or peer KMA, then this field displays the user-specified identifier of that entity. Otherwise, this field is blank.
- **Entity Network Address** - If this Audit Event is generated in response to an operation requested by a user, agent, or peer KMA, then this field displays the network address of that entity. Otherwise, this field is blank.
- **KMA ID** - The name of the KMA that generated this audit event. This KMA name is the user-supplied identifier that distinguishes each KMA in a cluster.
- **KMA Name** - The user-supplied identifier that distinguishes each Appliance in a cluster.
- **Class** - Identifies the class of operations to which the Audit Event entry belongs. If the Class value is Security Violation, the KMA that generated the event also issues an SNMP inform message with the event details.
- **Retention Term** - The defined length of time that the Audit Event record is retained. Possible values are:
  - **Long Term** — Event records that must be stored for a lengthy time period.
  - **Medium Term** — Event records that must be stored for a medium length time period.
  - **Short Term** — Event records that must be stored for a short time period.
- **Audit Log Entry ID** - A system-generated unique identifier that distinguishes each type of Audit Event entry.
- **Audit Log ID** - A system-generated unique identifier that distinguishes each Audit Event entry.

Create a System Dump

Create a system dump to assist with troubleshooting an issue. The dump does not include any key information.

As a best practice, always create the system dump before you restart the KMA.

Available to: Security Officer, Operator

1. In the left navigation menu, expand **System Management**, and then select **System Dump**.
2. The dump file is an automatically-generated *.tar.Z file. If desired, click **Browse** to select a destination path.
3. Click **Start** button to begin the download.

Send Messages to Remote Syslog Servers

Configure each KMA in the cluster to send messages to one or more remote syslog servers.

- Configure TLS for Remote Syslog Communication
- Create a Remote Syslog Server
- View or Modify Remote Syslog Details
- Test Remote Syslog Support
- Delete a Remote Syslog Server

If an SNMP Manager is configured and enabled, KMAs will send SNMP informs for particular OKM audit events (such as Error, Server Busy, and Security Violation among others). If an entry for a remote syslog server has been defined for a KMA, then this KMA will also send to the remote syslog server messages for the same set of OKM audit events.

If the Hardware Management Pack feature has been enabled on a Sun Fire X4170 M2 KMA or a SPARC KMA, then hardware faults will also be forwarded.

KMAs running OKM 3.3.2 or later will send the following types of operating system messages:

- audit_warn(1M) messages from the Solaris audit service
- Operating system messages of the following RFC 5424 facility and severity levels:
  - Facility = audit, Severity = notice or lower
  - Facility = local0, Severity = alert or lower
  - Facility = local7, Severity = info or lower

If KMAs reside in different physical sites, then the Security Officer can choose, for example, to configure KMAs in one site to send messages to a remote syslog server at that site and to configure KMAs in another site to send messages to a remote syslog server in that other site. The Security Officer can configure a KMA to communicate with the remote syslog server(s) using either a TCP connection that is unencrypted or a TCP connection that is secured using Transport Layer Security (TLS). TLS uses certificates to authenticate and encrypt the communication between a KMA and the

remote syslog server. The KMA authenticates the remote syslog server by requesting its certificate and public key.

Optionally, you can configure the remote syslog server to use mutual authentication. Mutual authentication ensures that the remote syslog server accepts log messages only from authorized clients. When configured to use mutual authentication, the remote syslog server requests a certificate from the KMA to verify the identity of the KMA.

Configure TLS for Remote Syslog Communication

Configure TLS to secure the messages sent to the Remote Syslog server.

1. The administrator of the remote syslog server must install a certificate issued by a Certificate Authority (CA) on the syslog server.
2. The Security Officer must obtain the certificate of the Certificate Authority that issued this server certificate.
3. The Security Officer must then provide this CA certificate when enabling the remote syslog feature on the KMA.

> **Note:**
>
> This CA certificate is a root CA certificate.

4. The Security Officer must first acquire a certificate that was issued by a Certificate Authority (CA).
5. The Security Officer must then provide this client (KMA) certificate when enabling the remote syslog feature on that KMA.
6. The administrator of the remote syslog server must obtain the certificate of the Certificate Authority that issued this client (KMA) certificate and then install this CA certificate on the remote syslog server.

Create a Remote Syslog Server

A remote syslog server can communicate when KMAs that reside at a different physical site.

Available to: Security Officer

1. In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Remote Syslog**.
2. Click **Create...**
3. Enter the following information:
   - Destination ID of a remote syslog server. This value uniquely identifies the remote syslog server.
   - Network address (IP address, or if DNS is configured, host name) of the remote syslog server.
   - Select which network protocol (TCP Unencrypted or TLS) to use for communication with the remote syslog server. If you select TLS (either with server authentication or server and client authentication), do the following:

a. Enter the location of the Certificate Authority (CA) certificate file.

b. If you plan to use mutual authentication (using both server and client authentication) enter locations for the client (KMA) certificate file and client private key file. You can enter a password if the client private key is password protected.

> **Note:**
>
> Certificate and private key files must be in PEM format.

- Optionally, enter a port number on which the remote syslog service on the remote syslog server is listening. Port 514 is used by default for TCP Unencrypted, and port 6514 is used by default for TLS.
- Use the check box to select whether the remote syslog server is enabled.

4. Click **Save**.

View or Modify Remote Syslog Details

Modify the syslog details to update the syslog configuration.

Available to: Security Officer

1. In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Remote Syslog**.
2. Select a remote syslog server and click **Details...**
3. Update the settings as desired.
4. Click **Save**.

Test Remote Syslog Support

Send test messages to all defined remote syslog servers verify the configuration.

Available to: Security Officer

1. In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Remote Syslog**.
2. Select a remote syslog server and click **Test**.
3. Enter the text to be included in the test message and click the **Test** button. The KMA sends the test message to all defined remote syslog servers according to their respective defined settings.

Delete a Remote Syslog Server

Delete a syslog server to stop sending messages to it.

Available to: Security Officer

1. In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Remote Syslog**.
2. Select a remote syslog server and click **Delete**.

10
Backups

Create and use backups to restore the cluster following a disaster.

What is a Core Security Backup?

The Core Backup contains the Root Key Material which protects the Master Key, a symmetric key that protects the Data Unit Keys stored on the KMA.

The Root Key Material is key material that is generated when a cluster is initialized. The Core Security backup requires a quorum of users to unwrap the Root Key Material. This security mechanism enables two operational states for the KMA: *locked* and *unlocked*. For more information, see Lock/Unlock the KMA.

The Core Backup must precede the first Database Backup and then this core backup only needs to be repeated when members of the Key Split change (quorum). This is a security item handled and protected specially. This is required to restore any backup of the OKM. As a best practice, keep two copies of this backup in two secure locations on a portable media of the customers choice, such USB memory sticks or external hard drives. When a new Core Backup is created and secured, the old ones should be destroyed.

What is a Database Backup?

The database backup backs up the keys created by the KMAs within the cluster. Use a database backup in combination with a core security backup to recover from a disaster.

A Database Backup consists of two files: a Backup file and a Backup Key file. The filenames for the backup files are automatically generated, however, you can edit the names. Backup Operators are responsible for securing and storing data and their keys. Database Backups are encrypted with AES-256; and therefore, secure.

Things to consider:

- Old backups contain users, passwords, and other sensitive data you may not want to keep.
- Make and archive two current database backups in case of backup media failure.

- Never archive old copies of the database.
- If you routinely delete keys for policy or compliance reasons, the deleted keys can be recovered from prior backups.
- Make two identical copies to protect against backup media failure. This scheme also ensures another key was not issued during the backup, making the two copies different.
- Maintain offsite copies of the Core Security and Database backups.

Considerations When Performing Backups and Key Sharing

Backups and key sharing can be resource intensive. Take these considerations into account before backing up or sharing keys.

OKM backups and key sharing (import/export) are database intensive and reduce the response time on the KMA while it is performing the backup or key transfer operation. If possible, reduce tape drive workloads during the OKM backup and transfer window. If that is not possible, then consider the following options:

- Use the same KMA for backups and key sharing each time (most likely this is how cron jobs invoking the OKM backup utility will get set up).
- If the cluster is large enough, dedicate a KMA to be an administrative KMA.
  - This KMA should not have a service network connection so it would not be burdened with tape drive key requests at any time, especially during the backup or key transfer windows.
  - This KMA could also be used for OKM GUI sessions thus offloading the other KMAs from handling management related requests.
- Ensure fast management network connectivity of the backup and key transfer KMA. The faster the connection, the better it will be able to keep up with the additional load during backup and key transfer windows. This is true for all KMAs, but especially for the KMA performing backups as it will fall behind on servicing replication requests during the backup window. Having a fast network connection helps to minimize the replication backlog, such as lag.
- Put the backup and key transfer KMA in a site that is not used by tape drives. The tape drives then preference other KMAs within the site that they have been assigned and avoid using the backup and key transfer KMA.
- Add more KMAs to sites containing tape drives so that load balancing of key requests will occur across more KMAs. This reduces the number of key requests that the backup and key transfer KMA has to handle.

View Backup File Information

View information about backups, such as when it was created or destroyed.

Available to: All roles

1. In the left navigation tree, expand **Secure Information Management**, and then select **Backup List**. See Filter Lists to filter the list.
2. To view details for a specific backup, highlight the backup in the list, and then click **Details...**

Backup List - Field Descriptions

The following are descriptions of fields in the Backup List of OKM Manager.

- **Backup ID** — A system-generated unique identifier for each backup file.
- **KMA ID** — The KMA for which the backup file was generated.
- **Created Date** — Displays the date when the backup was created.
- **Destroyed Date** — Displays the date that the backup file was marked as being manually destroyed.
- **Destruction Status** — Indicates the whether the backup has been destroyed. Possible values are:
  - **NONE** — The backup file has not been destroyed and does not contain data unit keys that have been destroyed.
  - **PENDING** — The backup file has not yet been manually destroyed and contains copies of data unit keys that have been destroyed.
  - **DESTROYED** — The backup file has been manually destroyed.
- **Destruction Comment** — User-supplied comment on the backup's destruction.

Create a Core Security Backup

Create a core security backup to backs up root key material. Use a core security backup in combination with a database backup to restore a cluster after a disaster.

Always create a new core security backup after modifying the key split credentials. You must back up core security key material before creating a database backup.

> **Caution:**
>
> Carefully protect core security backup files. Any core security backup file can be used with any backup file/backup key file pair, therefore even old core security backup files remain useful.

Available to: Security Officer

1. In the left navigation menu, expand **Security**, then expand **Core Security**, and then select **Backup Core Security**.
2. OKM generates the backup file name automatically. Edit the name, if desired.
3. To change the destination path, click **Browse**.
4. Click **Start**.
5. When the backup completes, click **Close**.

Create a Database Backup

Create a backup file and backup key file to be used to restore the cluster following a disaster.

At any given time, there is only one backup file and one restore file on a KMA. You should store the backup files at a site geographically distant from the KMAs, such that disaster does not destroy all the data.

Available to: Backup Operator

1. The Security Officer must back up core security key material before the Backup Operator can create a backup.
2. From the **Backups** menu, select **Backup List**. Click **Create Backup**.
3. OKM automatically generates the file names. Modify the names, if desired.
4. Click **Browse** to select a destination path.
5. Click **Start**.
6. When the backup completes, click **Close**.

Restore a Backup

If all KMAs in a cluster have failed, upload and restore a backup file and backup key file to the KMA.

Available to: Security Officer (requires a quorum)

1. Before performing this procedures, ensure that you have completed the QuickStart and selected the Restore a Cluster from a Backup option.
2. **Best Practice:** Log in to OKM Manager as the temporary Security Officer established in Create Security Officer and Provide Quorum Login of the QuickStart.
3. In the left navigation tree, expand **Secure Information Management**, and then select **Backup List**. Click **Restore...**
4. Select a backup key file and backup file. These must match (meaning were created at the same time).
5. Select a core security backup. This can be older or newer than the backup key file and backup file. You can use any Core Security backup file with any backup key file and backup file.
6. Click **Start**.
7. Enter the Key Split Credentials. These must be Key Split Credential users that were in effect when the Core Security Backup was created.

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

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

8. When the restore completes, click **Close**.
9. Network settings are not restored. Update the IP address settings for the KMA. Refer to Set KMA Management IP Addresses and Set KMA Service IP Addresses.
10. **Best Practice:** Log in to the OKM Manager GUI using the original Security Officer user ID (the one that existed before the restore), and delete the temporary restore Security Officer user ID as a cleanup step. Refer to Delete a User.

Destroy a Backup

Destroy a backup to ensure that it cannot be used in the future.

Available to: Compliance Officer (view only), Backup Operator

1. Before proceeding, ensure that you have destroyed all copies of the corresponding backup key file.
2. From the **Backups** menu, select **Backup List**.
3. Select a backup, and then click **Confirm Destruction**.
4. If you are certain that all copies of the corresponding backup key file have been manually destroyed, click **Destroy**.

11

Keys, Key Policies, and Key Groups

Understand the difference between keys, key policies, and key groups to properly configure and manage OKM.

Keys are the actual key values (key material) and their associated metadata. Each KMA creates 1000 keys (default) when created. This may vary during installation. Each KMA controls and assigns its own keys. After issuing 10 keys the KMA creates 10 keys to replenish them. Keys are then replicated to all KMAs in the OKM.

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

Key groups associate keys and key policies. Each key group has a key policy and is assigned to agents. Agents are allowed to retrieve only the keys that are assigned to one of the agent's allowed key groups. Agents also have a default key group. When an agent creates a key (assigns it to a data unit), the key is placed into the agent's default key group.

> **Note:**
>
> For the system to function, you must define at least one key policy and one key group (assigned as the default key group) for all agents.

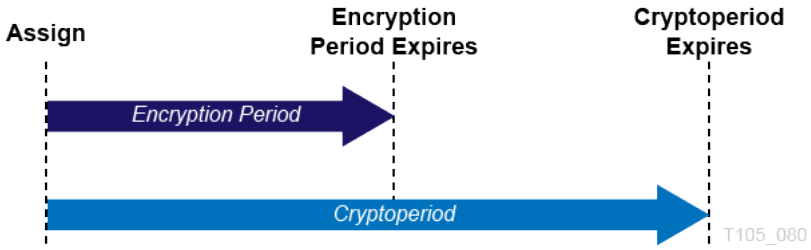
About Key Lifecycles

Keys undergo a lifecycle based on the key policy. A key will transition to multiple states throughout its lifecycle.

Encryption and Crypto Periods

The lifecycle imposed by the OKM is based on the NIST 800-57 guidelines. A few additional states are added to deal with nuances of the OKM. The encryption period is the period after a key is assigned that can be used to encrypt data. The cryptoperiod is the period that can be used for decryption. The two periods start at the same time when the key is assigned.

Figure 11-1 Key Lifecycle Periods



Key States and Transitions

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

- **Generated** — Indicates a key that has been created on one KMA in a OKM cluster. It remains generated until it has been replicated to at least one other KMA in a multi-OKM cluster. In a cluster with only a single KMA, a key must be recorded in at least one backup to transition out of the generated state.
- **Ready** — A ready state indicates that the key has been protected against loss by replication or a backup. A ready key is available for assignment. The "replicated" transition occurs when the key is replicated or (for a single OKM cluster) backed up.

Active
This state indicates that the key may be used to protect information (encrypt) or to process previously protected information (decrypt) NIST states that an active key may be designated to protect only, process only, or protect and process. Further, it specifically states that for symmetric data encryption keys, a key may be used for some time period to protect and process information and once this time period expires, the key may continue to be used for processing only.
Within the active state, the OKM adds two substates. These states are described in NIST, but are not specifically identified as states.

- **Protect-and-process** — A key in this state can be used for both encryption and decryption. A key is placed into this state when it is assigned. The assignment is done when an encryption agent requests a new key to be created.
- **Process only** — A key in this state can be used for decryption but not encryption. When an agent determines that none of the keys available to it for a specific data unit that is being read or written are in the protect-and-process state, it should create a new key.

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

Deactivated
This state indicates that the key has passed its cryptoperiod but may still be needed to process (decrypt) information. NIST specifically states that keys in this state may be used to process data.
The NIST guidelines state that if post-operational keys, including deactivated and compromised keys, need to remain accessible, they should be archived. This is a key

recovery process that allows keys to be recalled from an archive and made available for use.
The OKM provides archives in the form of KMA backups but cannot recall a single key from a backup. Therefore, the OKM retains post-operational phase keys in the OKM cluster and delivers them upon request from an agent.

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

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

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

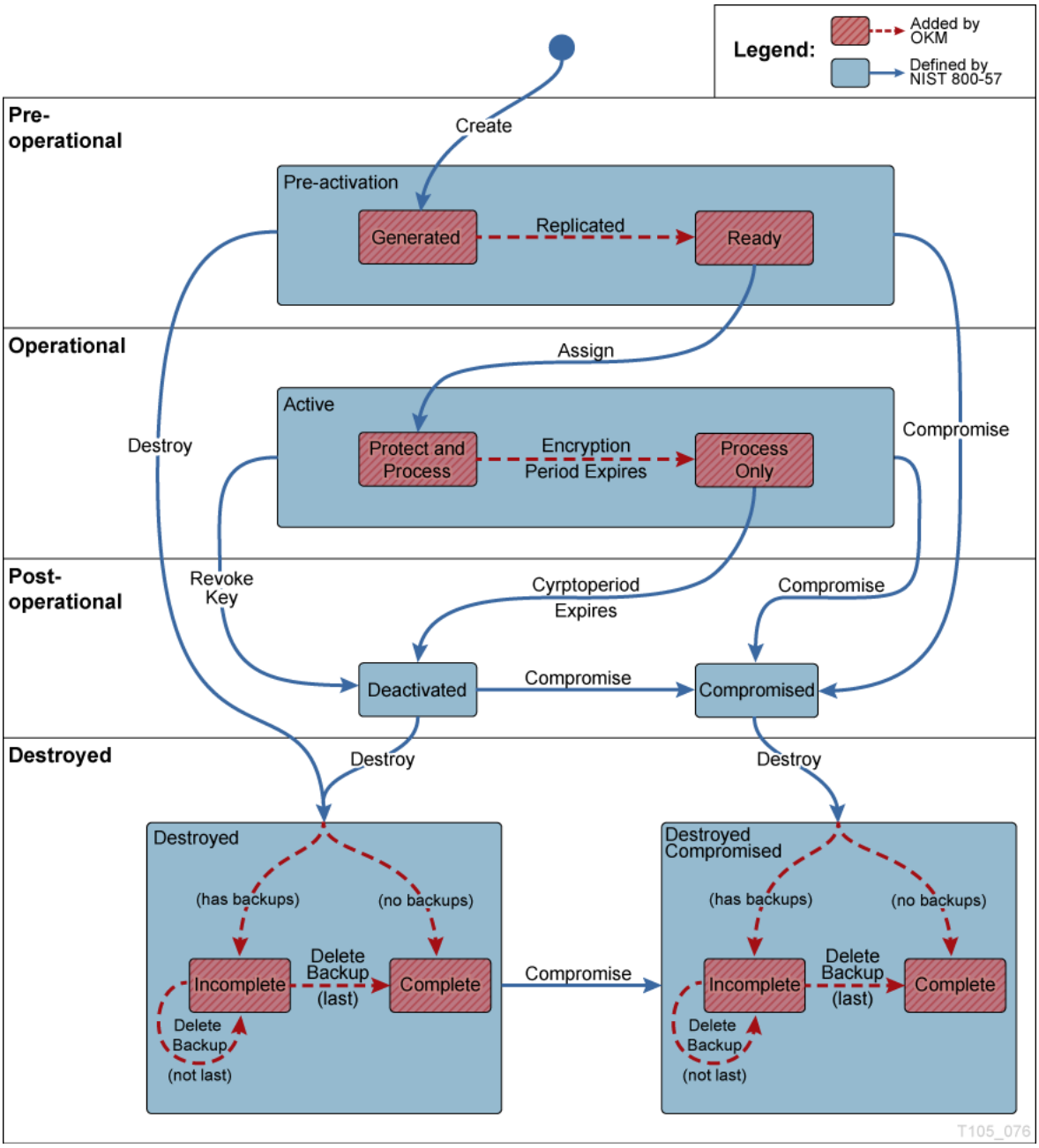
The NIST guidelines do not provide any basis for destroying keys based on time. Within the Destroyed and Destroyed Compromised states, the OKM defines two substates, incomplete and complete. These states are created because the OKM does not control the backups that it creates. A customer administrator must inform the OKM when a backup has been destroyed. Only after all backups have been destroyed can a key be considered truly destroyed.

- **Incomplete** — An Incomplete substate indicates that at least one backup still exists that contains the destroyed key. In this substate, the key does not exist in any KMA in the OKM cluster. Keys in this state cannot be delivered to agents.
- **Complete** — A Complete substate indicates that all backups containing the key have been destroyed. The key does not exist in any KMA, nor in any backup. Strictly speaking, backups that contain the key may well still exist. Although the OKM identifies the backups as destroyed, it is the responsibility of the user to ensure these backups have actually been destroyed.

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

In diagram below, states and transitions shown in red are added by the OKM. When examining keys in the OKM Manager, only the innermost state is listed.

Figure 11-2 State Transition Diagram



Manage Key Policies

Key policies determine the lifecycle of keys.

- Create a Key Policy
- View and Modify Key Policies
- Delete a Key Policy

Create a Key Policy

The key policy defines a key's lifecycle. Create key policies before creating and delivering keys to agents.

The encryption period and cryptoperiod begin when the key is first given to an agent. Once defined, the encryption period and cryptoperiod cannot be changed for a policy. This is to avoid a change in the key policy from affecting large numbers of keys.

Available to: Compliance Officer

1. In the left navigation menu, expand **Secure Information Management**, and then select **Key Policy List**. Click **Create...**
2. Complete the following:
   - **Key Policy ID** — Identifies the policy (can be between 1 and 64 characters).
   - **Description** — Describes the policy (can be between 1 and 64 characters, or leave this field blank).
   - **Encryption Period** — How long keys associated with this key policy can be used to encrypt or decrypt data. The time interval units are: minutes, hours, days, week, months, or years.
   - **Cryptoperiod** — How long keys associated with this key policy can be used to decrypt (but not encrypt) data. The time interval units are: minutes, hours, days, week, months, or years.
   - **Allow Export From** — When checked, data unit keys associated with this key policy can be exported.
   - **Allow Import To** — When checked, data unit keys associated with this key policy can be imported.
   - **Allow Agents To Revoke Keys** — When checked, allows agents using a key group that specifies this key policy can deactivate (revoke) the keys associated with them, even if the keys are in an operational state such as protect-and-process. The OKM cluster must use Replication Version 14 or later before this attribute can be set to **True**. Tape drive agents should use the default value (**False**). Applications using a pkcs11_kms provider (see OKM PKCS#11 Provider) should be configured to use an agent with a default key policy set to **True** if they want to call to revoke a key they will no longer use, such as in a re-key operation. ZFS encryption is an example of a pkcs11_kms application.
3. Click **Save**. Key groups can now use the new key policy.

View and Modify Key Policies

View a list of current key policies in use by the cluster. Modify a key policy to update how the policy handles keys.

Available to: Compliance Officer (can modify), All roles (can view)

1. In the left navigation menu, expand **Secure Information Management**, and then select **Key Policy List**. See Filter Lists to filter the list.
2. Double-click a key policy (or highlight a key policy and click **Details...**)
3. Change the information as required. Click **Save**.

Delete a Key Policy

Delete key policies that are not used by any key group or key.

Available to: Compliance Officer

1. In the left navigation menu, expand **Secure Information Management**, and then select **Key Policy List**.
2. Select the key policy, and then click **Delete**.
3. To confirm the deletion, click **Yes**.

Manage Key Groups

Key groups associate keys and key policies. Each key group can be assigned to agents. OKM applies the associated key policy to keys in that key group.

- Create a Key Group
- View and Modify Key Groups
- Delete a Key Group
- Assign Agents to Key Groups
- Assign a Transfer Partner to a Key Group
- Import a KMS 1.0 Key Export File

Create a Key Group

Associate a key group with an key policy. All keys generated within the group will follow the key policy.

Available to: Compliance Officer

1. In the left navigation area, expand **Key Groups**, and then select **Key Group List**.
2. Complete the following:
   - **Key Group ID** — Identifies the key group (can be between 1 and 64 characters).
   - **Description** — Describes the key group (can be between 1 and 64 characters)
   - **Key Policy ID** — The key policy to associate with this key group.
3. Click **Save**. Data units, agents, and so forth can now use the key group.

View and Modify Key Groups

View a list of key groups associated with the cluster. Modify the key group's settings.

Available to: Compliance Officer, All other roles can view-only

1. In the left navigation area, expand **Key Groups**, and then select **Key Group List**.
2. Double-click a key group (or highlight a key group, and click **Details...**).
3. Modify the fields as desired. Click **Save**.

Delete a Key Group

Delete inactive key groups that are not being used by any key and are not assigned to an agent.

Available to: Compliance Officer

1. In the left navigation area, expand **Key Groups**, and then select **Key Group List**.
2. Highlight the key group, and then click **Delete**.
3. To confirm the deletion, click **Yes**.

Assign Agents to Key Groups

Assign an agent to key groups to determine the storage devices the agent can access. Agents only retrieve keys from the key groups assigned to the agent.

This process accomplishes the same result as Assign Key Groups to an Agent.

Available to: Compliance Officer, Operator (can view-only)

1. In the left navigation area, expand **Key Groups**, and then select **Agent Assignment to Key Groups**.
2. In the "Key Groups" column, highlight a key group.
3. Move agents between the "Agents Allowed Access" or the "Agents Not Allowed Access" column. To move, highlight the agent and then click **<** or **>** to add or remove agent access.

> **Note:**
>
> You must set a default key group for an agent before that agent can allocate keys. When an agent creates a key (assigns it to a data unit), the key is placed into the agent's default key group.

4. To assign a default key group, select an agent and then click **< Default Key Group**.

Assign a Transfer Partner to a Key Group

Assigning a transfer partner to a key group is one step required when transferring keys to another cluster.

This process accomplishes the same result as Assign Key Groups to a Transfer Partner.

Available to: Compliance Officer, Operator (can view-only)

1. In the left navigation menu, expand **Key Groups**, and then select **Transfer Partner Assignment to Key Groups**.
2. Select a **Key Group** from the "Key Groups" column.
3. Move key groups between the "Transfer Partners Allowed Access" or the "Transfer Partners Not Allowed Access" column. To move, highlight the transfer partner, and then click **<** or **>** to allow or disallow access.

Import a KMS 1.0 Key Export File

Available to: Compliance Officer

Procedures:

1. Go to the KMS 1.2 system and export the keys into a file. Only keys exported from KMS 1.2 systems can be imported. KMS 1.0 and 1.1 systems must be upgraded to 1.2 before exporting keys.
2. From the **Secure Information Management** menu, select **Import 1.0 Keys**.
3. Select the **Destination Key Group** into which these keys will be imported.
4. Click **Browse**, and then locate the KMS 1.0 Key Export file.
5. Click **Start** to upload the KMS 1.0 keys file to the KMA. A new key is created for each key the file contains. Each new key is associated with the key group you selected.

Manage Keys

Keys are the actual key values (key material) and their associated metadata. The compliance officer can change the key group association and compromise keys.

- View and Modify Key Information
- Compromise Keys

View and Modify Key Information

Query keys to view information associated with a specific key. Update the key group or set the In Use By Data Unit flag.

Available to: Operator, Compliance Officer

1. From the **System Management** menu, select **Key List**. See Filter Lists to filter the list.
2. To view detailed information, select a key in the list, and then click **Details...** (or double-click a key).

   A Compliance Officer can change the key group this key is associated with. An Operator can change the In Use By Data Unit flag, which indicates whether this key is associated with a data unit.
3. Click the **Data Unit Info** tab to display information about the data unit that is associated with this key (if any).

Compromise Keys

Compromise a key when it is no longer secure and should not be used.

Available to: Compliance Officer

1. From the **Data Units** menu, select **Data Unit List**.
2. Select a data unit to modify, and then click **Details...**

3. Click the **Key List** tab.
4. Select the key(s) to compromise, and then click **Compromise**.
5. Click the **Yes** to confirm.
6. Type a comment about the compromise of the selected key(s). Click **Compromise**.
7. Click the **Yes** to confirm.

Transfer Keys Between Clusters

Key transfer allows keys and associated data units to be securely exchanged from one cluster to another.

Typically, you can use key transfer to exchange tapes between companies or within a company with multiple clusters. The key transfer process involves:

- Configure Key Transfer Partners — Each cluster configures the other cluster as a transfer partner. This requires each party to establish a public/private key pair and then provide the public key to the other party.
- Export a Transfer Partner Key/Import Transfer Partner Keys — The user exports keys from one cluster and imports them into the other. This step can be done many times. The transfer file is signed using the sending party's private key and encrypted using the receiving party's public key. This allows only the receiving party to decrypt the transfer file using their own private key. The receiving party can verify the file was in fact produced by the expected sender by using the sender's public key.

Configure Key Transfer Partners

Each cluster must configure the other cluster as a partner before transferring keys.

Both partners must complete the following steps to configure the other cluster as a partner:

- Create and Send a Key Transfer Public Key
- Create the Transfer Partner
- Assign Key Groups to a Transfer Partner

Create and Send a Key Transfer Public Key

OKM signs key transfer files with the key transfer public key. Provide partners with the key transfer public key, so they can import key transfer files.

Available to: Security Officer

1. In the left navigation tree, expand **System Management**, and then select **Key Transfer Public Key List**.
2. Click **Create...**
3. Provide the new key to all existing transfer partners:
   a. Select a Public Key in the list, and then click **Details...**
   b. Send this information to other cluster's administrator. Cut and paste the Public Key ID and Public Key into an e-mail or other agreed-upon form of

communication. The exact communication method should be sufficiently secure.

Create the Transfer Partner

The administrator of the receiving cluster must enter the public key information provided by the partner cluster.

These procedures use the key information sent in Create and Send a Key Transfer Public Key.

Available to: Security Officer (requires a quorum)

1. In the partner cluster, in the left navigation tree, expand **Secure Information Management**, an then select **Transfer Partner List**. Click **Create...**
2. Complete the following on the **General** tab:
   - **Transfer Partner ID** — Identifies the transfer partner (1 to 64 characters).
   - **Description** (optional) — Describes the transfer partner (1 to 64 characters).
   - **Contact Information** (optional) — Contact information about the transfer partner.
   - **Export Format** —The format you should select depends on the software version and FIPS Mode Only settings. To view the FIPS setting, see Review and Modify the Cluster Security Parameters).

     Table 11-1 Determining Export Format

Software Version — Importing KMA	FIPS Mode Only— Exporting Cluster	FIPS Mode Only— Importing Cluster	Export Format
2.0.2 or lower	Off	N/A	v2.0 or Default
2.0.2 or lower	On	N/A	v2.0
2.1 or higher	Off	Off	v2.1 (FIPS)
2.1 or higher	On	Off	v2.1 (FIPS)
2.1 or higher	Off	On	v2.1 (FIPS)
2.1 or higher	On	On	v2.1 (FIPS) or Default

     – **v2.0** —This transfer partner does not wrap keys when it exports them.
     – **v2.1 (FIPS)** —This transfer partner wraps keys when it exports them.
     – **Default** — Enables sharing keys between a cluster running KMS 2.1+ and another cluster in which all KMAs run KMS 2.0.x. This value effectively uses either "v2.0" or "v2.1 (FIPS)" behavior depending on the software version of the KMA importing the keys and the settings of the "FIPS Mode Only" security parameter on the exporting and importing OKM clusters.

       "Default" allows you to alter the format of the transfer partner's transfer files simply by changing the FIPS Mode Only security parameter instead of editing the transfer partner's Export Format setting directly, which requires a quorum.
   - **Flags - Enabled** — When selected, this transfer partner can share keys.

- **Flags - Allow Export To** — When selected, you can export keys to the transfer partner.
- **Flags - Allow Import From** — When selected, you can import keys from this transfer partner.

3. Complete the following on the Public Keys tab:
   - **New Public Key ID** — Enter the Public Key ID provided to you by the transfer partner.
   - **New Public Key** — Enter the Public Key provided to you by the transfer partner.
   - **New Public Key Fingerprint** — This read-only field shows the fingerprint, or hash value, of the new Public Key. Verify this fingerprint with the Partner to ensure the Public Key has not been tampered with, accidentally or deliberately, during transmission.
4. As you enter the Public Key, the system computes the fingerprint. Communicate with the partner cluster administrator using a different method than was used for the transfer of the key itself.

   Both administrators should look at their OKM and verify the fingerprint matches. A mismatch indicates the key has been damaged or modified during the transfer.
5. If the fingerprint is correct, click **Save**.
6. Enter the Key Split Quorum Authentication. See Quorum Authentication for more information.

Assign Key Groups to a Transfer Partner

The administrator must assign key groups for the transfer partner.

This process accomplishes the same result as Assign a Transfer Partner to a Key Group.

Available to: Compliance Officer, Operator (can view-only)

1. In the left navigation area, expand **Transfer Partners**, and then select **Key Group Assignment to Transfer Partners**.
2. Select a **Transfer Partner** in the "Transfer Partner" column.
3. Move key groups between the "Allowed Key Groups" or the "Disalowed Key Group" column. To move, highlight the key group, and then click **<** or **>** to allow or disallow access.

Export a Transfer Partner Key

Export keys to share them with a transfer partner.

Available to: Operator

1. Before exporting, verify the key meets the following requirements:

Table 11-2 Required Settings for Exporting a Key

Component	Values Required	How to Verify/Change
Key Policy	Allow Export From = True	View and Modify Key Policies

Table 11-2 (Cont.) Required Settings for Exporting a Key

Component	Values Required	How to Verify/Change
Key transfer partner	Enabled = True Allow Export To = True Export Format properly set for software version and FIPS settings (see Table 11-1)	View and Modify the Transfer Partner List
Key Group	Transfer partner is associated with the key's key group	Assign a Transfer Partner to a Key Group
Key State	Must not Protect and Process, Process Only, Deactivated, or Compromised Must be activated (Activation Date not empty) and not destroyed (Destroyed Date empty)	View and Modify Data Units

2. From the **Data Units** menu, select **Data Unit List**.
3. Select one or more data units (tapes) to be sent to the partner cluster. The External Tag is the barcode on the tapes.

   Keys associated with the selected data units must belong to key groups associated with key policies that have their `Allow Export From` flag set to "True." These keys must also be activated (their Activation Date is not empty) and not destroyed (their Destroyed Date is empty). See View and Modify Data Units.
4. Click **Export Keys**.
5. Select the destination transfer partner, select the Export Keys file name if necessary, and click **Start**.

   OKM only exports the Keys belonging to the key groups assigned to the partner cluster. See Assign a Transfer Partner to a Key Group.
6. Send the Transfer File to the partner cluster's administrator by e-mail or another agreed-upon form of communication or mechanism to move files.

Import Transfer Partner Keys

Import keys and data unit information contained in a key transfer file exported from another cluster.

Available to: Operator

1. From the **Transfer Partners** menu, select **Import Keys**.
2. Select the **Destination Key Group** into which these keys will be imported.

   The "Allow Imports" flag for this key group's key policy must be selected. This key group must be an allowed key group for the selected sending transfer partner.
3. Select the **Sending Transfer Partner** which exported these keys.

   The transfer partner must have Enabled = True, Allow Import From = True, proper Export Format (see Table 11-1), and proper key group assigned.
4. Click **Browse**, and locate the Key Transfer file.
5. Click **Start**.

View and Modify the Transfer Partner List

View a list of transfer partners. Modify the transfer partner settings.

Available to: Security Officer (requires a quorum to modify), Compliance Officer (can view), Operator (can view)

1. In the left navigation tree, expand **Secure Information Management**, select **Transfer Partner List**. See Filter Lists to filter the list.

   If the Export Format column shows N/A, the connected KMA runs KMS 2.0.x software and therefore does not allow the user to specify the Export Format setting.

2. Highlight a transfer partner ID, and then click **Details...**
3. Modify the information as required. Click **Save**.
4. Enter the Key Split Quorum Authentication. See Quorum Authentication for more information.

View the Key Transfer Public Key List

View a list of public keys used with transfer partners.

Available to: Security Officer

1. In the left navigation tree, expand **System Management**, and then select **Key Transfer Public Key List**. See Filter Lists to filter the list.
2. To view details, select a public key from the list, and then click the **Details...**

Delete a Transfer Partner

Delete a transfer partner that is no longer needed.

Available to: Security Officer

1. In the left navigation tree, expand **Secure Information Management**, select **Transfer Partner List**.
2. Highlight a transfer partner ID, and then click **Delete**.
3. Confirm the deletion by clicking **Yes**.

Sharing Keys with Older Clusters

Transfer keys differ in length depending on the OKM version used to create them. Some keys may not be compatible with certain versions of OKM.

Compatibility Restrictions for Transfer Partners

OKM_3.1+ KMAs generate key transfer keys that are a different length than those generated by KMAs running a previous OKM release. In addition, OKM 3.3 KMAs that have a Thales nShield Solo module generate key transfer keys that are longer than those that do not have a Thales nShield Solo module. Such changes introduce a compatibility concern with previous OKM releases.

The OKM 3.3 GUI supports key transfer keys of any of these lengths. Thus, it can be used to configure transfer partners while connected to KMAs running either the OKM 3.3 release or a previous OKM release. It cannot, however, configure a pre-OKM 3.1 KMA Transfer Partner using the longer key length.

- You must use the OKM 3.1 or later GUI to configure Transfer Partners on OKM clusters where OKM 3.1 or later KMAs reside.
- You cannot configure Transfer Partners for key sharing between an OKM cluster where OKM 3.1 or later KMAs reside and an OKM cluster where only OKM 2.5.3 (or lower) or OKM 3.0.2 (or lower) KMAs reside.

Transferring Keys in Mixed Clusters

If you add an OKM 3.1+ KMA to a cluster with OKM 2.x or 3.0.2 KMAs:

- Existing KMA transfer partner activities would remain unchanged and the transfer partners exchanges with older (earlier than OKM 3.1) clusters would not be affected.
- When sending a new transfer key, if the new key transfer key is generated on a KMA (earlier than OKM 3.1), then the new key would be accepted in pre-3.1 clusters. If the new transfer key is generated on the OKM 3.1 or later KMA, then it would be rejected by any pre-3.1 cluster.

Once a transfer partnership is established between two OKM clusters, customers can perform export key and import key operations on any KMA in the OKM cluster, even after a KMA in these OKM clusters is upgraded to the OKM 3.3 release. However, the compatibility issues described above are exposed when the customer attempts to create or modify a Transfer Partner. Also, customers must take these issues into consideration when a new key transfer key must be generated, and choose the correct KMA when generating this key.Key Transfer Keys can be used any KMA in an OKM cluster. Thus, when an OKM 3.1 or later KMA is added to a down-level OKM cluster, it uses any (smaller) Key Transfer Keys that have already been generated there. If the customer uses the OKM 3.1 or later KMA to create a new Key Transfer Key, then this KMA generates a Key Transfer Key with a longer length.

Mitigation when Transferring Keys in Mixed Clusters

If an OKM 3.1 or later cluster needs to exchange keys with a down-level OKM 3.x cluster:

- If possible, upgrade the other KMAs in this cluster to OKM 3.1 or later. (Upgrading all KMAs might not be possible if they are Sun Fire X86 KMAs).

If an OKM 3.1 or later cluster needs to exchange keys with an OKM 2.x cluster:

- If possible, add an OKM 3.1 or later KMA to the OKM 2.x cluster to create Transfer Partners using longer Key Transfer Keys.

12
Sites, KMAs, Agents, and Data Units

Use OKM Manager to configure and control sites, KMAs, agents, and data units.

- Manage KMAs
- Manage Sites
- Manage Agents
- Manage Data Units

Manage KMAs

Each KMA is a server node within the cluster. Create, delete, update, and view KMAs.

- Create a KMA
- View and Modify KMA Settings
- Change a KMA Passphrase (Log the KMA Out of the Cluster)
- Delete a KMA
- Query KMA Performance
- Modify Key Pool Size
- Lock/Unlock the KMA
- Upgrade Software on a KMA
- Check the Replication Version of the KMA
- Switch the Replication Version
- View KMA Network Configuration Information
- View and Adjust the KMA Clock
- Check the Cryptographic Card

See also: Key Management Appliance.

Create a KMA

Create a KMA definition within OKM Manger before adding it to the cluster using QuickStart.

Available to: Security Officer (requires a quorum)

1. From the **System Management** menu, select **KMA List**. Click **Create...**
2. Enter the following within the **General** tab:
   - **KMA Name** — Uniquely identifies the KMA in a cluster (can be between 1 and 64 characters).
   - **Description** — Describes the KMA (can be between 1 and 64 characters).

- **Site ID** (optional) — The site that the KMA belongs to,

3. Click the **Passphrase** tab, and then enter the passphrase for the user. See Passphrase Requirements.
4. Click **Save**.
5. Creating a KMA requires a Quorum. Within the Key Split Quorum Authentication dialog, the quorum must type their usernames and passphrases to authenticate the operation. See Quorum Authentication for more information.
6. Run the QuickStart program on the KMA(s) you created so that they can join the cluster. For procedures on joining a cluster, refer to Add a KMA to an Existing Cluster.

View and Modify KMA Settings

View a list of KMAs associated with the cluster. Modify KMA settings.

Available to: Security Officer (requires a quorum to modify), All other roles (can view)

1. From the **System Management** menu, select **KMA List**. See Filter Lists to narrow down the KMAs shown.
2. Double-click a KMA entry (or highlight a KMA entry and click **Details...**).
3. Modify the information as required. Click **Save**.
4. Modify KMA details requires a quorum. Within the Key Split Quorum Authentication dialog, the quorum must type their usernames and passphrases to authenticate the operation. See Quorum Authentication for more information.

KMA List - Field Descriptions

The following are descriptions of the fields in the KMA List of OKM Manager.

- **Version** - Version of the KMA software. For OKM 3.0 KMAs, the version string shows the following format: <OKM release>-5.11-<OKM build>. For example, 3.0.0-5.11-2012.
- **Responding** - Indicates whether the KMA is running. The values shown indicate whether each of the KMAs listed (that is, the remote KMAs) are responding to requests from the local KMA.
  - **True** — KMA is responding to requests from the local KMA.
  - **False** — Remote KMA is not responding to requests, perhaps because the remote KMA is down or the communications link to the remote KMA is down.
- **Responding on Service Network** - Indicates whether the KMA is responding on the service network. The values indicate whether each of the KMAs listed (that is, the remote KMAs) are responding to requests from the local KMA. Possible values are:
  - **Responding** — Remote KMA is responding to requests from the local KMA.
  - **Not Responding** — Remote KMA is not responding to requests, perhaps because the remote KMA is down or the communications link to the remote KMA is down. If the local KMA has configured a default route, then it is considered to have a route to remote KMAs. Other KMAs are shown as "Not Responding" if they do not respond on the service network.

  - **Not Accessible** — Remote KMA is not accessible to the local KMA, perhaps because the service network configuration does not provide a default or static route to that KMA. If a default or static route is not defined, then other KMAs may be shown as "Not Accessible." Older KMAs (OKM 2.3.x or earlier) are shown as "Responding."

- **Response Time** - Time (in milliseconds) the KMA takes to respond to a request on its management network. This is typically a few hundred milliseconds. It can be larger if a WAN connection exists between the local KMA and a remote KMA or if the communications link between KMAs is busy.
- **Replication Lag Size** - Number of updates before replication takes place. This number should be zero or a small value. Larger values indicate that replications are not completing in a timely manner, the communications link between KMAs is down or busy, or a remote KMA is down. This value will also be very large when a new KMA has just been added to the cluster.
- **Key Pool Ready** - Percentage of unallocated keys that are ready.
- **Key Pool Backed Up** - Percentage of the Key Pool that has been backed up. N/A indicates that the KMA cannot determine this value, because either the KMA runs down-level software or it is currently using a lower Replication Version.
- **Locked** - If true, the KMA is locked. N/A indicates that the KMA cannot determine this value, because either the KMA runs down-level software or it is currently using a lower Replication Version.
- **Enrolled** - If true, the KMA has successfully been added or logged into the cluster. This value is False when the KMA is first created and will change to True once the KMA has logged into the cluster. It can also be False when the KMA passphrase is changed. Once a KMA has logged in, the passphrase used to log in can no longer be used. The passphrase must be changed before the KMA can log in to the cluster again.
- **HSM Status** - Status of the hardware security module (cryptographic card). Possible values:
  - **Unknown** The KMA is running a software release older than KMS 2.2.
  - **Inactive** The KMA currently does not need to use the hardware security module, typically because the KMA is locked.
  - **Software** The hardware security module is not functional, and the KMA is using the software provider to generate keys.
  - **Hardware** The hardware security module is functional, and the KMA is using it to generate keys.
  - **SW Error/HW Error** The KMA encountered an error when it tried to query the status of the software provider (SW Error) or the hardware security module (HW Error).

> **Note:**
>
> Normally, the hardware security module is functional (Hardware). However, if the hardware security module becomes non-functional (Software) and the FIPS Mode Only security parameter is set to Off (see Review and Modify the Cluster Security Parameters), then the KMA switches to using the software provider to generate keys.

If the hardware security module becomes non-functional and the FIPS Mode Only security parameter is set to On, then the KMA cannot generate keys or return AES wrapped key material to agents.

If the value is Software, SW Error, or HW Error, check the hardware security module on this KMA (see Check the Cryptographic Card).

– **Not Present** The hardware security module is not present and the KMA is using the software provider to generate keys.

Change a KMA Passphrase (Log the KMA Out of the Cluster)

Changing the passphrase for a KMA effectively logs it out of the cluster. This means that it cannot propagate information to peer KMAs in the cluster.

Available to: Security Officer (requires a quorum)

1. Connect to another KMA in the cluster (not the KMA you want to change the passphrase on).
2. From the **System Management** menu, select **KMA List**. Double-click the KMA entry (or highlight a KMA entry and click **Details...**).
3. Click the Passphrase tab and modify the passphrase. Confirm the passphrase (retype the same passphrase). The phrase must meet the requirements listed in Passphrase Requirements.
4. Click **Save**.
5. Within the Key Split Quorum Authentication dialog, the quorum must type their usernames and passphrases to authenticate the operation (see Quorum Authentication).
6. The KMA is not able to communicate with the cluster until it is logged back in . If the KMA has been logged out of the cluster for at least a few hours, then lock the KMA before logging the KMA back into the cluster. After recent updates have been propagated to this KMA, as shown by the Replication Lag Size in the KMA List panel, unlock the KMA (see Lock/Unlock the KMA).
7. To log this KMA back into the cluster, see Log KMA Back into Cluster .

Delete a KMA

Delete a failed or decommissioned KMA to remove it from the cluster. The KMA must be offline before deleting it.

Available to: Security Officer

1. Before deleting a KMA, take it offline using the Console "Shutdown KMA" function. If you fail to do this, the KMA continues to function outside of the cluster and sends "stale information" to agents and users.
2. From the **System Management** menu, select **KMA List**. Highlight the KMA you want to delete, and then click **Delete**.
3. Confirm the deletion.

   The system removes any entries associated with the KMA and not used by any other entity. If you want a deleted KMA to rejoin a cluster, you must reset the KMA to the factory default and select option 2 from the QuickStart program.

Query KMA Performance

View rate values, processing times, and server busy notifications for the KMA.

Available to: All roles

1. From the **System Management** menu, select **KMA Performance**.
   - **Rate values** — The rate at which this KMA processed these requests within the selected time period. They are expressed as the average rate of these requests extrapolated over the selected rate display interval unit of time (for example, extrapolated average number of key requests per day). If you set the rate display interval to "entire time period," then the panel instead displays the count of requests this KMA processed within the selected time period.
   - **Processing times** — The average time in milliseconds this KMA has taken to process the requests issued within the selected time period. These processing times are from the perspective of the KMA and describe the amount of time required to process requests internally. They do not include transmission times over the network or the amount of time required to establish an SSL connection.

     The OKM cluster must use replication version 15 or later to report processing times.
   - **Server Busy** — information about Server Busy conditions that the local KMA encountered within the selected time period. This condition indicates that other OKM threads are currently accessing OKM information in a local database and can occur during long-running OKM operations (such as OKM backups).
2. Click **Details...** (or double-click a KMA) to display performance information about that KMA.

Modify Key Pool Size

The key pool size sets the maximum keys generated by the cluster. The default key pool size is 1000.

Available to: Backup Operator (can modify), All other roles (can view)

1. From the **System Management** menu, select **KMA List**.
2. Click **Modify Key Pool Size**.
3. Enter the new Key Pool size. Click **Save**.

Determine Key Pool Size

OKM administrators should know the worst case number of keys they expect to be created during of the OKM backup/key transfer window. The default key pool size of 1000 keys should be sufficient for most customers unless the estimated worst case key creation rate for the backup windows exceeds this.

> **Note:**
>
> KMAs pre-generate keys so a key creation request from an agent does not actually cause a key to be created on the KMA until the key pool maintainer runs within the server. When the server is busy the key pool maintainer can be delayed in its operations.

The total cluster key pool size must be large enough so that KMAs can hand out pre-generated keys from their key pool during the backup windows. When the key pool size is too small, KMAs can become drained of pre-generated keys and start returning "no ready key" errors. Tape drives failover to other KMAs when this happens, adding further disruption to the backup/key transfer window.

Administrators should observe the OKM backup window periodically as it will gradually grow as the database gets larger. Adjust the key pool size when the backup window exceeds a threshhold or if the key consumption rate grows due to changes in the overall tape workload.

Lock/Unlock the KMA

Lock a KMA to block it from accessing data unit keys and servicing agent requests.

Available to: Security Officer (unlocking requires a quorum)

1. In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Lock/Unlock KMA**.
2. Click **Lock KMA** or **Unlock KMA**.
3. Unlocking the KMA requires a quorum. Within the Key Split Quorum Authentication dialog, the existing quorum must type their usernames and passphrases to authenticate the operation. See Quorum Authentication for more information.

Enable or Disable Autonomous Unlock Option

Autonomous unlock allows the KMA to automatically unlock after a reset.

> **Note:**
>
> Oracle recommends disabling autonomous unlock for maximum security. When disabled, the KMA remains locked and unable to service agents until a quorum unlocks it.

Available to: Security Officer (requires a quorum)

1. In the left navigation menu, expand **System Management**, expand **Security**, expand **Core Security**, and then select **Autonomous Unlock Option**.
2. Click either **Enable Autonomous Unlock** or **Disable Autonomous Unlock**.
3. Within the Key Split Quorum Authentication dialog, the quorum must type their usernames and passphrases to authenticate the operation. See Quorum Authentication for more information.

Upgrade Software on a KMA

Upgrading software requires two separate steps: uploading and activating.

- The Operator uploads the software file to the KMA . See Upload the Software Upgrades.
- The Security Officer activates the software version that the Operator uploaded. See Activate a Software Version.

Version Requirements

Use a GUI release that matches the version you want to load on the KMA(s). 2.x GUIs cannot activate a software version on an 3.0.x KMA. Install and use an 3.0.x GUI before uploading or activating a software version on an 3.0.x KMA.

You cannot upgrade OKM 2.x KMAs to 3.0.x. You must upgrade KMAs running KMS 2.1 or earlier to 2.2 before upgrading to OKM 2.3 and later.

What to do if the upgrade process is really slow

The upload and apply process can be lengthy if the OKM Manager is remotely connected to the KMA or if the connection between the OKM Manager and KMA is slow. To mitigate this, the software upgrade file can be downloaded to a laptop or workstation that has the OKM Manager installed and the laptop or workstation connected to the same subnet as the KMA. The presence of a router between the OKM Manager and the KMA may slow down the upgrade process.

The upload and apply processes, with a good connection between the OKM Manager and the KMA, optimally take about 30 minutes. The activate process optimally takes about 5 to 15 minutes. If the uploading process is very slow, try connecting to the same subnet as the KMA.

Upload and apply the software upgrade file on each KMA one at a time (to help to spread out the network load), and then activate the software upgrade on each KMA one at a time (to minimize the number of KMAs that are offline concurrently).

If any of the upgrade processes fails (upload, verify, apply, activate, switch replication version), the OKM Manager generates audit messages describing the reason for the failure and a suggested solution.

Check the Software Version of a KMA

View the software version running on a specific KMA.

Available to: All roles

1. From the **System Management** menu, select **KMA List**.
2. Check the software level in the Version field.

   For OKM 3.0 KMAs, the version string shows the following format: <OKM release>-5.11-<OKM build>. For example, 3.0.0-5.11-2012.

Upload the Software Upgrades

Upload the software package to the KMA so that it can be activated.

Uploading software adds traffic to the network. Avoid uploading KMAs simultaneously in a busy cluster. Software updates are signed by Oracle and verified by the KMA before they are applied.

Available to: Operator

1. Before upgrading, create a backup (see to Create a Database Backup).
2. Download the software upgrade file, and save it to a location accessible to OKM Manager.
3. From the **Local Configuration** menu, select **Software Upgrade**.
4. Click **Browse**, and locate the upgrade file.
5. Click **Upload and Apply**.

Activate a Software Version

Activate a software version that has been already uploaded and applied.

Available to: Security Officer

1. Verify the Operator has uploaded the correct software version.

   For OKM 3.0.x KMAs, the version string has the following format: <OKM release>-5.11-<OKM build>. For example, 3.0.0-5.11-2027. For OKM 3.0.x KMAs, the Software Upgrade screen displays software versions in reverse chronological order. That is, the newest version appears at the top of the list. Check the Active column to see which version is active.
2. Before activating software, ensure there is a current backup of the OKM cluster.
3. In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Software Upgrade**.
4. Select the new software version, and then click **Activate**.

   > **Note:**
   >
   > The KMA restarts as part of the activate process. Since the KMA is offline while it restarts, you may not want to activate KMAs simultaneously in a cluster.

5. Software activation requires a quorum. Within the Key Split Quorum Authentication dialog, the quorum must type their usernames and passphrases to authenticate the operation. See Quorum Authentication for more information.
6. The Technical Support account is disabled on the upgraded KMAs, and the accounts must be reenabled if needed.

Check the Replication Version of the KMA

Some features require the replication version to be at a certain level. Verify the version using OKM Manager.

Available to: All Roles

1. In the left navigation menu, expand the **Local Configuration** menu, select **Software Upgrade**.
2. View the version in the **Current Replication Version** column.

See also: Switch the Replication Version.

Switch the Replication Version

Set the replication version to the highest value to support the most features.

The security officer must manually set the replication version. OKM never changes the version automatically. Switching the replication version on one KMA will set all KMAs in the cluster to that replication version (assuming the software version on the KMA supports that level).

Available to: Security Officer

1. Log in to a KMA that has been activated. In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Software Upgrade**.
2. If the Supported Replication Versions column includes a higher version than the Current Replication Version column, click **Switch Replication Version**.
3. Select a new replication version, and click **OK**. OKM will set all KMAs that can support the replication version.

Replication Version Features

The availability of certain features depends on the replication version of the KMA.

Table 12-1 Replication Version Features

Replication Version	KMS/OKM Version	Features Enabled
8	2.0	Everything related to initial release
9	2.0.2	Keys In Backup (ready keys appear in backups)
10	2.1	IPv6 addresses AES Key Wrap (FIPS Mode)
11	2.2	ICSF integration Distributed Quorum SNMP Protocol version 2c
12	2.3	Accelerate initial updates
13	2.4	Agent Roaming
14	2.5.2	Allow Agents to revoke keys

Table 12-1 (Cont.) Replication Version Features

Replication Version	KMS/OKM Version	Features Enabled
15	3.0	Processing times available in performance reports
16	3.3.2	Renew Root CA Certificate Acceptable TLS Versions SNMPv2 Community String

View KMA Network Configuration Information

View the network configuration of the KMA you are currently connected to.

Available to: All roles

1. In the left navigation menu, expand **System Management**, expand **Local Configuration**, and then select **Network Configuration**.
2. The page shows the network configuration for the KMA you are currently connected to.

View and Adjust the KMA Clock

Maintain the times reported by each KMA in a cluster within five minutes of each other to avoid operational issues.

You can provide an IPv6 address for an external NTP server. You can only adjust a KMA clock once a day by a maximum of plus or minus 5 minutes.

Available to: Security Officer, All other roles (can view)

1. In the left navigation menu, expand **System Management**, and then select **System Time**.
2. To change the time, click **Adjust Time**.
   a. Select the "Move System Time Forward (+)" or "Move System Time Backward(-)".
   b. In Offset Minutes and Offset Seconds, select a numeric value.

      If the specified offset greater than five minutes, you will receive an Error message. Click **OK** and enter a new value.
3. To sync to an NTP server, click **Specify NTP Server**. Enter the IPv6 address (must not include square brackets or a prefix length).

Check the Cryptographic Card

To identify a failed cryptographic card (also known as hardware security module), examine the rear of the KMA server and check the LEDs on the card.

Checking an SCA 6000 Card

A functional SCA 6000 card on a KMS 2.1, KMS 2.2, or OKM 2.3 and later KMA that has been initialized through the QuickStart program displays a flashing green Status LED (identified with an S) and solid green FIPS (F) and Initialized (I) LEDs. If the

Status LED is not flashing green and the FIPS and Initialized LEDs are not solid green, then the KMA has a faulty SCA 6000 card, which must be replaced if FIPS mode is required. See the *SCA 6000 User Guide* for a description of the LEDs on an SCA 6000 card.

Checking a Thales nShield Solo+

An existing SPARC KMA in a cluster may contain a failed Thales nShield Solo module. To identify a failed Thales module, examine the rear of the KMA server and check the Status LED on the Thales module. A functional Thales nShield Solo module on an OKM 3.3 or later KMA that has been initialized through the QuickStart program displays a solid-blue Status LED that blinks occasionally. If the Status LED displays a different pattern, contact Oracle Support.

Manage Sites

View, create, modify, and delete sites. A site is a physical location with at least one KMA. Sites help agents recover from a KMA failure and load balance.

- Create a Site
- View and Modify a Site
- Delete a Site

Create a Site

Create a site to identify KMAs that reside at the same physical location. Sites help agents to respond to KMA failures and load balance by connecting to local KMAs.

Available to: Security Officer

1. In the left navigation tree, expand **System Management**, and then select **Site List**. Click **Create...**
2. Enter the following:
   - **Site ID** — Uniquely identifies the site. This value can be between 1 and 64 characters.
   - **Description** — Uniquely describes the site. This value can be between 1 and 64 characters.
3. Click **Save**.
4. Assign KMAs and agents to the Site ID (see View and Modify KMA Settings and View and Modify Agents).

View and Modify a Site

View a list of sites configured for the cluster. Modify a site's description.

Available to: Security Officer, All other roles (can view)

1. In the left navigation tree, expand **System Management**, and then select **Site List**. See Filter Lists to filter the list.
2. To view or modify a specific site, click **Details...**
3. Change the Description field.

4. Click **Save**.

Delete a Site

Delete a site that is not assigned to any agents or KMAs.

Available to: Security Officer

1. If any agents or KMAs are specified to be at the site, you must assign them to a different site before deleting.
2. In the left navigation tree, expand **System Management**, and then select **Site List**.
3. Highlight the site to delete, and then click **Delete**.
4. Confirm the deletion by clicking **Yes**.

Manage Agents

View, create, modify, delete, and assign agents. Agents are devices or applications that use cryptographic keys from OKM to encrypt and decrypt data.

- Create an Agent
- View and Modify Agents
- Set an Agent's Passphrase
- Assign Key Groups to an Agent
- Delete Agents

Create an Agent

Create an agent to allow it to access the cluster.

Available to: Operator

1. From the **Agents** menu, select **Agent List**. Click **Create...**
2. On the **General** tab, complete the following:
   - **Agent ID** — Uniquely identifies the agent (between 1 and 64 characters).

     > **Note:**
     >
     > Agent IDs cannot be changed once created. If you replace the agent, you can reuse the name. However, passphrases can only be used once. You will need to give the agent a new passphrase.

   - **Description** — Describes the agent (can be between 1 and 64 characters).
   - **Site ID** (optiona) — Select a site from the drop-down list.
   - **One Time Passphrase** (checkbox) — If selected, the agent cannot retrieve its X.509 certificate without resetting its passphrase and re-enrolling with its agent ID and new passphrase. This is the default.

If unselected, then the agent can retrieve its X.509 certificate at any time, use CA and certificate services, and successfully authenticate through its agent ID and passphrase.

Tape drive agents should specify the default value. PKCS#11-type agents will find this setting to be more convenient, especially in cluster configurations where users may authenticate to the OKM from multiple nodes.

- **Default Key Group ID** — If you also have Compliance Officer privileges, click the down-arrow and highlight the default key group. You should define a default key group so that this agent can use keys in this key group to encrypt and decrypt data. See Assign Key Groups to an Agent for instructions on how to enable this agent to use keys in other key groups to decrypt data (read only).

3. On the **Passphrase** tab, enter a passphrase. For requirements, see Passphrase Requirements.
4. Click **Save**.
5. Complete the agent-specific enrollment procedure using the agent-specific interface. For example, for StorageTek drives, you must use the VOP (Virtual Operator Panel) to complete the enrollment procedure.

View and Modify Agents

View a list of agents. Modify an agent to update its information.

Available to: Operator, Compliance Officer (can view)

1. From the **Agents** menu, select **Agent List**. See Filter Lists to filter the list.
2. Select an agent from the list, and then click **Details...** (or double-click the agent).
3. Modify the fields, as required (see Create an Agent for field definitions).

> **Note:**
>
> Do not change the passphrase unless you believe it is compromised (see Set an Agent's Passphrase for more info).

4. When finished, click **Save**.

Agent List - Field Descriptions

The following are descriptions of fields in the Agent List of OKM Manager.

- **Agent ID** - The user-specified unique identifier that distinguishes each agent.
- **Description** - Describes the agent.
- **Site** - Unique identifier that indicates the Site to which the agent belongs.
- **Default Key Group** - The key group associated with all keys created by this agent if the agent does not explicitly specify a different key group.
- **Enabled** - Indicates the status of the agent. Possible values are True or False. If this field is False, the agent cannot establish a session with the KMA.
- **Failed Login Attempts** - The number of failed login attempts.

- **Enrolled** - Indicates whether the agent has enrolled successfully with the OKM cluster. Possible values are True or False. This field is False if the agent is the first created or if the agent's passphrase is changed.

Set an Agent's Passphrase

Set an agent's passphrase if you believe that the agent certificate or passphrase has been compromised.

When you set an agent's passphrase, you are effectively revoking the agent certificate that enables the agent to authenticate itself with the KMA.

Available to: Operator

1. From the **Agents** menu, select **Agent List**.
2. Select an agent from the list, and then click **Details...** (or double-click the agent).
3. On the **Passphrase** tab, modify the passphrase.
4. Click **Save**.
5. Re-enroll the agent using the agent-specific procedure. For example, for StorageTek tape drives, the VOP (Virtual Operator Panel) must be used to re-enroll the agent with the OKM cluster. After changing an agent's passphrase, the agent is not able to make requests to the OKM cluster until it is re-enrolled.

Assign Key Groups to an Agent

Assign a key group to an agent to determine the storage devices the agent can access.

This process accomplishes the same result as Assign Agents to Key Groups.

Available to: Compliance Officer, Operator (can view)

1. In the left navigation area, expand **Agents**, and then select **Key Group Assignment**.
2. Select an agent in the "Agents" list.
3. Move key groups between the "Allowed Key Groups" or the "Disalowed Key Group" column. To move, highlight the key group, and then click **<** or **>** to allow or disallow access.
4. You must set a default key group for an agent before that agent can allocate keys. To assign a default key group, select a key group and then click **< Default Key Group**.

Delete Agents

Delete an agent you no longer want to access OKM.

Available to: Operator

1. From the **Agents** menu, select **Agent List**.
2. Select the agent you want to delete, and then click **Delete**.
3. Click **Yes** to confirm.

Query Agent Performance

Display information about create key, retrieve key, and register key-wrapping requests issued by each agent.

Import key requests are not included in these values. HP and IBM LTO tape drives do not issue create key requests. They issue retrieve key requests instead.

Available to: Operator, Compliance Officer

1. From the **Agents** menu, select **Agent Performance List**. See Filter Lists to filter the list.
   - **Rate values** — the rate at which this agent issued these requests within the selected time period. They are expressed as the average rate of these requests extrapolated over the selected rate display interval unit of time (for example, extrapolated average number of Create Key requests per day). If you set the rate display interval to "entire time period," then this panel instead displays the count of requests this agent issued within the selected time period.
   - **Processing times** — the average time in milliseconds taken to process the requests that this agent has issued within the selected time period. These processing times are from the perspective of the KMA and describe the amount of time required to process requests internally. They do not include transmission times over the network or the amount of time required to establish an SSL connection. The OKM cluster must use replication version 15 or later before request processing times are available.
2. To display more information about an agent, select an agent and click **Details...** (or double-click an agent).

Manage Data Units

Data units represent data that is encrypted by agents (such as a tape cartridge for a tape drive agent).

- View and Modify Data Units
- View Data Unit Key Details
- View Backups with Destroyed Data Unit Keys
- View Key Counts for a Data Unit
- Destroy Keys for a Data Unit

View and Modify Data Units

View a list of data units associated with the cluster. Modify data unit details.

Available to: Operator (can modify), Compliance Officer (can modify Key Group and Compromise keys), All other roles (can view)

1. From the **Data Units** menu, select **Data Unit List**.
2. Select a data unit, and then click **Details...**
3. On the **General** tab, modify the information as required.

> **Note:**
>
> If the Description field contains the string "`PKCS#11v2.20`," this represents a special key used for Oracle Database Transparent Data Encryption (TDE). Do not change this field. Doing so can alter the way OKM interacts with TDE.

4. Click **Save**.

Data Unit List - Field Descriptions

The following are descriptions of the fields within the Data Unit List of OKM Manager.

- **Data Unit ID** - System-generated unique identifier that distinguishes each data unit.
- **External Unique ID** - Unique external identifier for the data unit.
  - This value is sent to the OKM by the agent and may not be externally visible to an end user. For LTO Gen 4 and Gen 5 tapes, this is the cartridge serial number burned into the cartridge when it is manufactured. Do not confuse this value with a volser on an optical barcode or in an ANSI tape label. This value is not used for StorageTek tape drives.
- **Description** - Describes the data unit.
- **External Tag** - Unique external tag for the data unit.
  - For tapes that are in a StorageTek tape library, or tapes that have ANSI standard labels, this field is the volser. If the tape is in a library and has an ANSI label, the library volser (that is, optical bar code) is used if it differs from the volser contained in the ANSI label. For tapes written in stand-alone drives without ANSI labels, this field is blank.
  - For data units written by LTO Gen 4 and Gen 5 tape drives, this field is padded on the right with blanks to fill in 32 characters. It may be more convenient for you to use the "Starts With ~" filter operator instead of the "Equals =" filter operator, so that you do not have to add the blanks to pad the External Tag. For example, if you use the "Starts With" filter, you could enter: "External Tag" ~ "ABCDEF". If you use the "Equals" filter for the same example, you would need to enter: "External Tag" = "ABCDEF " (padded to fill 32 characters).
- **Create Date** - Date and time when the data unit was created/registered.
- **Exported** - If true, the keys associated with this data unit have been exported.
- **Imported** - If true, the keys associated with this data unit have been imported.
- **State** - State of the data unit. Possible values are:
  - **No Key:** Set when the data unit has been created, but has not yet had any keys created.
  - **Readable:** Set when the data unit has keys that allow at least some parts of the data unit to be decrypted (read).
  - **Normal:** Set when the data unit has keys that allow at least some parts of the data unit to be decrypted (read). In addition, the data unit has at least one

protect-and-process state key that can be used to encrypt data. The data unit is therefore writable.

- **Needs Re-key**: Set when the data unit does not have at least one protect-and-process state key. Data should not be encrypted and written to this data unit until the data unit is rekeyed and a new, active key is assigned to it. It is the responsibility of the agent to avoid using a key that is not in protect-and-process state for encryption. The data unit may have keys that are in process only, deactivated, or compromised state. A key in any of these three states can be used for decryption.
- **Shredded:** Set when all of the keys for this data unit are destroyed. The data unit cannot be read or written. However, a new key can be created for this data unit, moving its state back to Normal.

View Data Unit Key Details

View a list of keys used by data units.

Available to: All roles, Operator (can change In Use By Data Unit checkbox)

1. From the **Data Units** menu, select **Data Unit List**.
2. Select a data unit, and then click **Details...**
3. Click the **Key List** tab (see below for a description of field).
4. Select a key, and then click **Details...**
5. If the Replication Version is at least 14, the Operator can change the **In Use By Data Unit** check box that indicates the relationship between this key and its associated data unit. Selecting this check box can help when a key policy that is used by tape drive agents is inadvertently updated to enable its **Allow Agents To Revoke Keys** attribute. See View and Modify Key Policies for a description of this attribute.

Key List - Field Descriptions

The following are descriptions of the fields within the Key List of OKM Manager.

- **Data Unit ID** - Uniquely identifies the data unit.
- **Data Unit Description** - Describes the data unit.
- **Key ID** - Key information for the data unit.
- **Key Type** - The type of encryption algorithm that this key uses. The only possible value is AES-256.
- **Created Date** - Date and time when the key was created.
- **Activation Date** - Date and time when the key was activated. This is the date and time when the key was first given to an agent. It is the starting date and time for the key's encryption period and cryptoperiod.
- **Destroyed Date** - Date when the key was destroyed. If the field is blank, then the key is not destroyed.
- **Destruction Comment** - User-supplied information about the destruction of the key. If the field is blank, then the key is not destroyed.
- **Exported** - If true, the key has been exported.

- **Imported** - If true, the key has been imported.
- **Derived** - If true, the Key has been derived from a Master Key generated by the Master Key Provider. Refer to OKM-ICSF Integration for detailed information.
- **Revoked** - If true, the key(s) associated with the data unit has been revoked by an agent. See View and Modify Key Policies. If the KMA to which the OKM GUI is connected runs OKM 2.5.2 or higher but the OKM cluster currently uses Replication Version 13 or earlier, then this attribute is shown as "(Unknown)."
- **Key Group** - Key group associated with the data unit.
- **Encryption End Date** - Date and time when the key will no longer be used or was stopped from being used for encrypting data.
- **Deactivation Date** - Date and time when the key will be or was deactivated.
- **Compromised Date** - Date when the key was compromised. If the field is blank, then the key is not compromised.
- **Compromised Comment** - User-supplied information about compromising the key. If the field is blank, then the key is not compromised.
- **Key State** - Data unit's key state. Possible values are:
  - **Generated** — Set when the key has been created on one KMA in a OKM cluster. It remains generated until it has been replicated to at least one other KMA in a multi-OKM cluster. In a cluster with only a single KMA, the key remains generated until it has been recorded in at least one backup.
  - **Ready** — Set when the key has been protected against loss by replication or a backup. A ready key is available for assignment.
  - **Protect and Process** — Set when the key has been assigned when an encryption agent requests a new key be created. A key in this state can be used for both encryption and decryption.
  - **Process Only** — Set when the key has been assigned but its encryption period has expired. A key in this state can be used for decryption but not for encryption.
  - **Deactivated** — Set when the key has passed its cryptoperiod but may still be needed to process (decrypt) information.
  - **Compromised** — Set when the key has been released to or discovered by an unauthorized entity. A key in this state can be used for decryption but not for encryption.
  - **Incompletely Destroyed** — Set when the key has been destroyed but it still appears in at least one backup.
  - **Completely Destroyed** — Set when all of the backups in which the destroyed key appears have been destroyed.
  - **Compromised and Incompletely Destroyed** — Set when the compromised key still appears in at least one backup.
  - **Compromised and Completely Destroyed** — Set when all of the backups in which the compromised key appears have been destroyed.
- **Recovery Activated** - Indicates whether the key has been linked to the data unit by a recovery action.
  - This condition occurs when a key is used for a data unit by one KMA in a OKM cluster and then, due to a failure, the key is later requested for the data unit

from a different KMA. If the failure (such as a network outage) has prevented the allocation of the key to the data from being propagated to the second KMA, the second KMA creates the linkage to the data unit. Such a key is "recovery activated," and an administrator may want to evaluate the system for KMA or network outages. Possible values are True and False.

View Backups with Destroyed Data Unit Keys

Verify that no current backups contain destroyed keys.

A data unit cannot be considered "completely destroyed" until you destroy all backups containing the data unit keys.

Available to: Operator, Compliance Officer

1. From the **Data Units** menu, select **Data Unit List**.
2. Select a data unit, and then click **Details...**
3. Click the **Backups with Destroyed Keys List** tab.

How OKM Determines if a Backup Contains a Data Unit Key

A backup contains a data unit key if the backup occurred after creating the data unit key but before destroying the data unit key.

To account for the possible time discrepancies between KMAs, OKM uses a fixed five minute backup time window when comparing date-times. The backup time window minimizes falsely reporting that a data unit does not exist in a particular backup when in fact it does. Such a case is known as a "false negative" and seriously undermines compliance requirements for data destruction. Unlike "false negatives," "false positives" do not undermine compliance requirements for data destruction, hence the five minute window.

View Key Counts for a Data Unit

View the number of keys associated with a data unit.

Available to: Operator, Compliance Officer

1. From the **Data Units** menu, select **Data Unit List**. Click **Key Counts**.
2. By default, the display shows all data units associated with more than one key. See Filter Lists to filter the list.

Destroy Keys for a Data Unit

Destroy keys associated with a data unit so that the key can no longer be used.

Available to: Operator

1. From the **Data Units** menu, select **Data Unit List**.
2. Select a data unit in the list, and then click **Destroy Keys**.
3. Specify the keys to destroy:

- **Deactivated keys** — Select this check box if you want to destroy the keys that have passed their cryptoperiod but still may be needed to process (decrypt) data information.
- **Compromised keys** — Select this check box if you want to destroy the keys that have been released to or discovered by an unauthorized entity.

4. Type a comment about the destruction of these keys.
5. Click **Destroy**. Click **Yes** to confirm.

13

Quorum Authentication

A quorum is a set number of authenticators. Some operations require a sufficient number of quorum users to enter their credentials. Requiring a quorum assures that no single person can make a critical change.

What Occurs If You Do Not Enter a Quorum

The results of not providing a quorum depends on the replication version.

- **10 or lower** — The operation fails and no information is updated in the OKM cluster.
- **11 or higher** — The operation is added to the list of pending quorum operations (see View Pending Operations). OKM does not make the update until a quorum approves the operation (see Approve Pending Quorum Operations). Pending quorum operations expire when not enough key split users approve an operation within the pending operation credentials lifetime.

Operations that Require a Quorum

Only some operations require a quorum.

- Create a KMA
- Change a KMA Passphrase (Log the KMA Out of the Cluster)
- Create a User
- Modify a User's Details and Set the User's Passphrase
- Configure Key Transfer Partners
- View and Modify the Transfer Partner List
- Restore a Backup
- Lock/Unlock the KMA
- Enable or Disable Autonomous Unlock Option
- Upload the Software Upgrades

View and Modify the Key Split Configuration

The key split configuration sets the number of users required to provide a quorum.

Available to: Security Officer (quorum required to modify)

1. In the left navigation menu, expand **Security**, then expand **Core Security**, and then select **Key Split Configuration**.
2. Click **Modify...** and complete the following:
   - **Key Split Number** — The number of key splits. The maximum is 10.
   - **Threshold Number** — The number of users that are necessary to authenticate a quorum.
   - **Split User (1-10)** — The user names of the existing split. For each Split User, complete its associated Passphrase and Confirm Passphrase fields.
3. Click **Save**.
4. To set "new" credentials requires the existing quorum. The existing quorum must type their usernames and passphrases to authenticate the operation.

   Once updated, OKM re-wraps the core security key using the updated key split credentials.
5. Create a new core security backup (see Create a Core Security Backup).
6. Destroy all old core security backup files to ensure that the previous key split credentials cannot be used to destroy a backup.

View Pending Operations

An operation will remain in the pending list until a quorum of users approves it or until it expires.

Available to: Quorum Member, Security Officer

1. From the **Secure Information Management** menu, select the **Pending Quorum Operation List**.
2. To view details, select an operation, and then click **Details**...
3. To get more information about this particular pending quorum operation, you can filter audit events displayed in the Audit Event List panel.
   a. From the **System Management** menu, select **Audit Event List**.
   b. Define a filter with the Operation filter set to Add Pending Quorum Operation. If you have several pending quorum operations, you may want to define another filter with Created Date specifying a time period around the Submitted Date of this particular pending quorum operation.
   c. Click the **Use** button to display those audit events that match this filter. The Message Values field of the filtered audit event should contain more information about the pending quorum operation.

Approve Pending Quorum Operations

A set number of quorum users must log in and approve pending operations.

Other users who have the Quorum Member role can also log in separately and approve a pending quorum operation. When a sufficient quorum users approves the pending quorum operation, OKM performs the operation.

Available to: Quorum Member

1. From the **Secure Information Management** menu, select the **Pending Quorum Operation List**.
2. Click **Approve Pending Operation**.
3. Enter the quorum user names and passphrases to authenticate the operation.

   If you do not provide a sufficient quorum of Key Split Credentials, the operation remains on the list of pending quorum operations.

Delete Pending Quorum Operations

Delete a pending operation to remove it from the pending operations list.

Available to: Security Officer

1. From the **Secure Information Management** menu, select the **Pending Quorum Operation List**.
2. Highlight a pending operation, and then click **Delete**.
3. Click **Yes** to confirm.

14
OKM Console

OKM Console is a terminal text-based interface used to configure basic functions of the KMA.

The operating system automatically launches OKM Console when the KMA starts up. The console cannot be terminated by a user. Depending on the roles that a user is assigned, the options in the console differ. Before you can login to the console, the security officer must create the user with OKM Manager. OKM Console uses the same user name and passphrase as for OKM Manager.

Log into the KMA

Log into the KMA to access the OKM Console. Use the same credentials as your OKM Manager user.

You can access OKM console from the ILOM or by physically connecting a terminal to the SER MGT port on the KMA. Physically connecting is typically only done by an Oracle service representative during KMA installation or service.

The operating system automatically launches the OKM Console when the KMA starts up. After the KMA starts up, it displays the following information:

```
Copyright (c) 2007, 2017, Oracle and/or its affiliates. All rights reserved.
Oracle Key Manager Version 3.3.2 (build2068) – examplekma
------------------------------------------------------------
Please enter your User ID:
```

1. Type your user name and press **Enter**.
2. Type your passphrase and press **Enter**.
3. The options on the OKM Console will differ depending on the role(s) assigned to the user (see User Role Menu Options). The menu shows the version of the KMA and the logged on user.

User Role Menu Options

Menu options vary depending on the role assigned to the user.

Operator Menu Options

These are the OKM console menu options available to an Operator user.

Menu Option	Procedures
Reboot KMA	Restart the KMA
Shutdown KMA	Shutdown the KMA
Technical Support	Disable the Technical Support Account
Primary Administrator	Disable the Primary Administrator
Set Keyboard Layout (appears only on SunFire KMAs)	Set the Keyboard Layout
Show cluster Root CA Certificate	Show Properties of the Root CA Certificate
Logout	Log Out of Current OKM Console Session

Security Officer Menu Options

These are the OKM console menu options available to a Security Officer user.

Menu Option	Procedures
Log KMA Back into Cluster	Log KMA Back into Cluster
Set User's Passphrase	Set a User's Passphrase
Set KMA Management IP Addresses	Set KMA Management IP Addresses
Set KMA Service IP Addresses	Set KMA Service IP Addresses
Modify Gateway Settings	View, Add, and Delete Gateways
Set Acceptable TLS Versions	Set Acceptable TLS Versions
Set DNS Settings	Specify the DNS Settings
Reset to factory Default State	Reset the KMA to the Factory Default
Technical Support	Disable the Technical Support Account Enable the Technical Support Account (using OKM Console)
Primary Administrator	Disable the Primary Administrator Enable the Primary Administrator
Set Keyboard Layout(appears only on SunFire KMAs)	Set the Keyboard Layout
Show cluster Root CA Certificate	Show Properties of the Root CA Certificate
Renew Root CA Certificate	Renew the Root CA Certificate
Logout	Log Out of Current OKM Console Session

Combined Operator and Security Officer Menu Options

These are the OKM console menu options for a user with both the Security Officer and Operator roles.

Menu Option	Procedures
Log KMA Back into Cluster	Log KMA Back into Cluster
Set User's Passphrase	Set a User's Passphrase
Set KMA Management IP Addresses	Set KMA Management IP Addresses
Set KMA Service IP Addresses	Set KMA Service IP Addresses
Modify Gateway Settings	View, Add, and Delete Gateways
Set Acceptable TLS Versions	Set Acceptable TLS Versions
Set DNS Settings	Specify the DNS Settings
Reset to factory Default State	Reset the KMA to the Factory Default
Reboot KMA	Restart the KMA
Shutdown KMA	Shutdown the KMA
Technical Support	Disable the Technical Support Account Enable the Technical Support Account (using OKM Console)
Primary Administrator	Disable the Primary Administrator Enable the Primary Administrator
Set Keyboard Layout (appears only on SunFire KMAs)	Set the Keyboard Layout
Show cluster Root CA Certificate	Show Properties of the Root CA Certificate
Renew Root CA Certificate	Renew the Root CA Certificate
Logout	Log Out of Current OKM Console Session

Menu Options for Other Roles

These are the OKM console menu options for users with the Backup Operator, Compliance Officer, Auditor, or Quorum Member role.

Menu Option	Procedures
Set Keyboard Layout (appears only on SunFire KMAs)	Set the Keyboard Layout
Show cluster Root CA Certificate	Show Properties of the Root CA Certificate
Logout	Log Out of Current OKM Console Session

OKM Console Functions

OKM Console functions allow a user to perform basic configuration and management functions on the KMA.

For a list of available functions for each user role, see User Role Menu Options.

- Log KMA Back into Cluster
- Set a User's Passphrase
- Set KMA Management IP Addresses

- Set KMA Service IP Addresses
- View, Add, and Delete Gateways
- Set Acceptable TLS Versions
- Specify the DNS Settings
- Reset the KMA to the Factory Default
- Restart the KMA
- Shutdown the KMA
- Enable the Technical Support Account (using OKM Console)
- Disable the Technical Support Account
- Disable the Primary Administrator
- Enable the Primary Administrator
- Set the Keyboard Layout
- Show Properties of the Root CA Certificate
- Renew the Root CA Certificate
- Log Out of Current OKM Console Session

Log KMA Back into Cluster

This OKM console function logs the KMA back into the cluster after its passphrase has been changed. The KMA must be known to the cluster. It cannot be a new KMA.

Available to: Security Officer (requires quorum)

1. If the KMA has been logged out of the cluster for at least a few hours, then lock the KMA before logging the KMA back into the cluster (see Lock/Unlock the KMA). After recent updates have been propagated to this KMA, as shown by the Replication Lag Size in the KMA List panel, unlock the KMA.
2. Choose a time of light operations to log the KMA back into the cluster. After logging the KMA in, it will take time for the existing cluster information to be replicated to the KMA, which can cause the cluster to become busy.
3. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Log KMA Back into Cluster` and press **Enter**.
4. At the prompt, type the IP address or host name of another KMA in the cluster and press **Enter**.
5. At the prompt for a passphrase, type the passphrase of the KMA and press **Enter**.
6. Enter the a quorum of key split user names and passphrases to complete the change.
7. To end the key split user authorization, leave the user name blank and press **Enter**.
8. When prompted, type **y** and press **Enter**.

Set a User's Passphrase

This OKM console function allows a Security Officer to set the passphrase for any user.

Available to: Security Officer (requires quorum)

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Set User's Passphrase` and press **Enter**.
2. At the prompt, type the name of the user and press **Enter**.
3. At the prompt, type the passphrase and press **Enter**.
4. Re-enter the same passphrase, and press **Enter**.
5. Enter the user names and passphrases for a quorum of split key users.
6. To end the key split user authorization, leave the user name blank and press **Enter**.
7. Press **Enter** to return to the main menu.

Set KMA Management IP Addresses

This OKM console function modifies the IP address settings for the management network interface of the KMA.

The KMA Management IP Addresses are initially defined in the QuickStart program (see Configure the Network in QuickStart). After you change these settings, this KMA propagates information about these changes to the other KMAs in the cluster.

> **Caution:**
>
> Use this function carefully. KMAs communicate with each other using their management network interface. Changing the IP address settings for the management network interface of a KMA can affect the network connectivity between the KMA and other KMAs.
>
> For example, you have two KMAs not currently communicating with each other (possibly due to a network outage or a change in the network environment). If you change the management IP addresses on both of them, they might not be able to communicate with each other after the network is repaired. In this case, try changing the passphrase of one of these KMAs and then use the procedure for Log KMA Back into Cluster .

Available to: Security Officer

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Set KMA Management IP Addresses` and press **Enter**.

   This displays the current KMA Management IP address settings. The IPv6 address fields are blank when the KMA is not configured to use IPv6 addresses.
2. Type either **n** or **y** at the `Do you want to configure the Management Network interface to have an IPv6 address` prompt.

3. Type either **n** or **y** at the `Do you want to use DHCP to configure the Management Network IPv4 interface` prompt. If you type **y**, skip to step 6.
4. At the prompt, type the Management Network IP address and press **Enter**.
5. At the `Please enter the Management Network Subnet Mask:` prompt, type the subnet mask address, (for example 255.255.254.0) and press **Enter**.
6. Type **y** at the `Are you sure that you want to commit these changes? [y/n]:` prompt.

Set KMA Service IP Addresses

This OKM console function modifies the IP address settings for the service network interface of the KMA.

The KMA service IP addresses are initially set in the QuickStart program (see Configure the Network in QuickStart). In a multi-site cluster where tape drives are deployed as OKM agents, the service network interfaces of KMAs in a particular site are typically configured to support network connectivity with tape drives at that site.

> **Caution:**
>
> This function should be used carefully. KMAs typically communicate with tape drives at the local site using their service network interface over a private service network. This means that changing the IP address settings for the service network interface of this KMA can affect the network connectivity between this KMA and the tape drives.
>
> Tape drives do not receive updated IP information immediately after you update the service IP addresses on a KMA; they typically get update IP information when a tape cartridge is mounted.
>
> Consider the example where tape jobs run only at night and you change the service IP addresses of all of the local KMAs during the day. In this case, the tape drives might not be able to communicate with the KMAs. If this happens, the drives must be re-enrolled with the OKM cluster. To avoid this, you should change service IP addresses on one KMA at a time and then wait for the tape drives to receive this change before proceeding to the next KMA.

Available to: Security Officer

1. Log in to OKM console. At the `Please enter your choice:` prompt on the main menu, select `Set KMA Service IP Addresses` and press **Enter**.

   This displays the current KMA Service IP address settings. The IPv6 address fields are blank when the KMA is not configured to use IPv6 addresses.
2. Type either **n** or **y** at the `Do you want to configure the Service Network interface to have an IPv6 address` prompt.
3. Type either **n** or **y** at the `Do you want to use DHCP to configure the Service Network IPv4 interface` prompt. If you type **y**, skip to step 6.
4. At the prompt, type the Service Network IP address and press **Enter**.

5. At the `Please enter the Service Network Subnet Mask:` prompt, type the subnet mask address, (for example 255.255.255.0) and press **Enter**.
6. Type **y** at the `Are you sure that you want to commit these changes? [y/n]:` prompt.

View, Add, and Delete Gateways

This OKM console function shows the current gateway settings (five gateways to a page) on the management and service network interfaces. Add a gateway, remove a gateway, or accept the current gateway configuration.

Available to: Security Officer

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Modify Gateway Settings` and press **Enter**.
2. At the `(1)Continue (2)Back` prompt, type **1** to display the next few gateways or **2** to display the previous few gateways.
3. When the last gateways are displayed, at the `Please choose one of the following:` prompt, select an option and then press **Enter**. Options are:
   - **1** (add gateway)
   - **2** (remove gateway)
   - **3** (exit)
   - **4** (display again)

Set Acceptable TLS Versions

This OKM console function sets the he minimum acceptable version of TLS. KMAs can accept connections using TLSv1.0, v1.1 or v1.2.

While v1.0 is no longer considered secure, if you have KMAs in the cluster running OKM versions prior to 3.1.0, or you have Agents (such as tape drives) that do not support later versions of TLS, you may need to leave all versions of TLS enabled. See for Table 3-2 tape drive TLS compatibility.

Available to: Security Officer

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Set Acceptable TLS Versions` and press **Enter**.
2. Select the TLS versions to enable, and then press **Enter**. Options include:
   - **1** (TLSv1.0 and higher)
   - **2** (TLSv1.1 and higher)
   - **3** (TLSv1.2 and higher)

Specify the DNS Settings

This OKM console function displays DNS settings and sets a new DNS domain and server IP address.

Available to: Security Officer

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Set DNS Settings` and press **Enter**.
2. Enter the DNS domain name at the `Please enter the DNS Domain (blank to unconfigure DNS):` prompt.
3. Enter the DNS server IP address at the `Please enter DNS Server IP address` prompt. You can enter up to three IP addresses.
4. Press **Enter**, without specifying an IP address, to finish.

Reset the KMA to the Factory Default

This OKM console function removes the KMA from the cluster and returns it to its factory default state.

> **Caution:**
>
> Use this function carefully. Removing a KMA from the cluster can affect the performance load on other KMAs.

Available to: Security Officer

1. If this KMA is the last one in the cluster, you should perform a backup before you reset this KMA to the factory default state.
2. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Reset to factory Default State` and press **Enter**.
3. At the `Type RESET to confirm` prompt, type **RESET** and press **Enter**.
4. Once the reset function completes, you are returned to QuickStart. See Configure a KMA with QuickStart .

Restart the KMA

This OKM console function stops and restarts the KMA and operating system. Use this function for troubleshooting purposes only.

Available to: Operator

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Reboot KMA`, and then press **Enter**.
2. At the prompt, type **y** and press **Enter**.

   The current OKM Console session terminates as the KMA begins to restart. After the KMA restarts, the OKM Console login prompt displays.

Shutdown the KMA

This OKM console function terminates (shuts down) all services on the KMA and physically shuts down the KMA.

Considerations When Shutting Down a KMA

- The KMA does not wait for replications to be completed. Any replications that did not complete before the shutdown will be completed after the KMA restarts.
- Any in-progress technical support sessions will be terminated.
- Any open KMA console sessions, including the one performing this procedure, will be terminated.
- Any open OKM Manager sessions to this KMA will return an error on any attempt to contact the KMA while it is shutdown.
- Long running actions, such as upgrades or backups will be terminated when the KMA is shutdown.
- Any in-process requests from Agents will fail while the KMA is shutdown. The Agent will then reconnect to a different KMA, if it can contact another KMA. If not, Agent requests (such as: retrieve a key during a tape mount) will fail.
- The KMA is not removed from the cluster while it is shut down. Other cluster members will attempt to contact the KMA while it is shut down (unless the KMA was logged out, see). One or more of the remaining KMAs will issue an SNMP INFORM when they are unable to contact the shut down KMA. If the KMA is not expected to be returned to service, the reset KMA procedure should be used instead of this one.

Available to: Operator

1. If the KMA has been shut down for at least a few hours and the Autonomous Unlock option is enabled, lock the KMA before restarting the KMA. After recent updates have been propagated to this KMA, as shown by the Replication Lag Size in the KMA List panel, unlock the KMA .
2. You should log the KMA out of the cluster before shutting it down to avoid other KMAs attempting to communicate with the shutdown KMA. See Change a KMA Passphrase (Log the KMA Out of the Cluster).
3. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Shutdown KMA`, and then press **Enter**.
4. When prompted, type **y** and press **Enter**. When finished with shutdown, it displays: `syncing files... done`
5. The KMA is now powered off. You can power on the KMA using either the power button or the remote power control function in the service processor.

Enable the Technical Support Account (using OKM Console)

This OKM console function enables the technical support account.

By default, both the Technical Support account and SSH access are disabled. Enabling the support account and SSH access is a security risk. Disable the support account unless it is required for troubleshooting purposes. If you enable the technical support account and then log into the KMA using this account, the KMA will automatically disconnect the SSH session after 10 minutes of inactivity.

Available to: Security Officer

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Technical Support`. Press **Enter**.
2. When prompted to enable the support account, type **y** and press **Enter**.
3. To confirm the change, type **y** and press **Enter**.

4. Carefully read the information about the SSH host keys. When prompted to regenerate the SSH host keys, type **y** and press **Enter**.
5. Record and store the SSH host keys somewhere secure.
6. Enter a passphrase. See Technical Support Account Password Requirements.
7. Enter the maximum number of days the passphrase is valid.

Technical Support Account Password Requirements

Beginning with OKM 3.3.2, password policies for the technical support account have changed for added security and compliance with the Solaris 11 Security Technical Implementation Guide (STIG), Release: 13.

- Minimum length of 15 characters
- Must include at least one special character
- Must include at least one numeric character
- Cannot contain dictionary words 3 characters or longer
- When changing the support account password after it has expired, the new password must differ from the previous password by at least 8 characters.

If you provide an invalid support account password, you have three more attempts to provide a valid password and each attempt has a 30-second timeout.

Disable the Technical Support Account

This OKM console function disables the technical support account.

Available to: Operator, Security Officer

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Technical Support`, and then press **Enter**.
2. When prompted to disable the support account, type **y** and press **Enter**.
3. When prompted to confirm the change, type **y** and press **Enter**. The SSH service automatically stops.

Enable the Primary Administrator

This OKM console function enables the primary administrator (equivalent to root access).

> **Caution:**
>
> Enabling this feature allows someone logged in as Technical Support to gain Primary Administrator access, equivalent to root access. Since the passphrase for the Primary Administrator is known only by Oracle Support, only someone from Oracle Support can gain Primary Administrator access. This may be necessary in some situations to recover the system from a problem, however, only do so with direct guidance from support.

Available to: Security Officer

1. You must first enable the Technical Support account (see Enable the Technical Support Account (using OKM Console)).
2. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Primary Administrator`. Press **Enter**.
3. When prompted to enable the privileges, type **y** and press **Enter**.
4. When prompted to confirm the change, type **y** and press **Enter**.

Disable the Primary Administrator

This OKM console function immediately disables the primary administrator and denies them access.

Available to: Operator, Security Officer

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Primary Administrator`. Press **Enter**.
2. When prompted to disable the account, type **y** and press **Enter**.
3. When prompted to confirm the change, type **y** and press **Enter**.

Set the Keyboard Layout

This OKM console function changes the keyboard layout from English to a variety of languages on SunFire KMAs.

Available to: All roles (but this option appears only on Sun Fire KMAs)

1. The keyboard layout should be set to match the layout of the keyboard attached to the KMA so that the KMA correctly interprets key presses.
2. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Set Keyboard Layout` and press **Enter**.
3. A list of keyboard layouts displays.
4. When prompted, enter the number corresponding to the keyboard layout you want to apply.

Show Properties of the Root CA Certificate

This OKM console function displays properties of the Root CA certificate in this cluster.

Available to: All roles

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Show cluster Root CA Certificate properties` and press **Enter**.
2. After viewing the Root CA certificate, press **Enter** to return to the main menu.

Renew the Root CA Certificate

This OKM console function renews the Root CA Certificate, signs it using the specified signature algorithm, and reissues certificates for itself and the other KMAs in the cluster.

Renewing updates credentials for all KMAs in the cluster, but does not automatically update or invalidate credentials for Agents and Users. This means that any already-enrolled Agents and Users can continue to communicate with this OKM cluster. If you changed the signature algorithm and X.509 certificate type during the renew, you may wish to re-enroll Agents and update User passwords so they begin using the new formats (see Task 4 and Task 5 of Generate and Sign Certificates Using SHA-256). If you change the signature algorithm to SHA-256, then the cluster will use an X.509v3 certificate for the Root CA certificate and all subsequently generated entity certificates. Otherwise, the certificate version will remain at X.509v1 for legacy compatibility purposes.

> **Note:**
>
> Renewing the Root CA certificate impacts activity in this cluster and makes the current backups obsolete. Always plan the renew in advance.

Available to: Security Officer

This menu option only appears with replication version 16 or later.

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, select `Renew Root CA Certificate` and press **Enter**.
2. Enter **1** for SHA256 (default) or **2** for SHA1 — If the encryption endpoints in this OKM environment will not support SHA2, enter **2**. Otherwise, enter **1**.

   See SHA Compatibility for information on agent compatibility.
3. When prompted to confirm the renew, type **y** and press **Enter**.
4. The following indicates the renew is complete and the OKM service has restarted:

   ```
   Root CA renew succeeded and OKM service has restarted. Please perform a backup
   as soon as possible.
   ```
5. Press **Enter** to return to the main menu.
6. You should create a new backup (see Create a Database Backup) and then destroy the older backups (see Destroy a Backup).
7. To display properties of the new Root CA Certificate, see Show Properties of the Root CA Certificate.

SHA Compatibility

Certain types of agents (encryption endpoints) are incompatibility with some versions of SHA.

Most types of OKM encryption endpoints support SHA-2 hashing algorithms and X.509v3 certificates. You can enroll agents associated with these encryption endpoints

in an OKM cluster where the Root CA certificate is an X.509v3 certificate that is signed using a SHA-2 hashing algorithm (such as SHA-256).

Some types of OKM encryption endpoints do not support SHA-2 hashing algorithms and X.509v3 certificates. You cannot enrolled agents associated with these encryption endpoints in an OKM Cluster where the Root CA certificate is an X.509v3 certificate that is signed using a SHA-2 hashing algorithm (such as SHA-256). Instead, you must enrolled the agents in an OKM Cluster where the Root CA certificate is a X.509v1 certificate that is signed using a SHA-1 hashing algorithm.

Encryption endpoints that have compatibility issues with SHA-2 certificates:

- HP LTO4 tape drives
- IBM LTO4/5/6/7 tape drives running Belisarius firmware version 4.x

All other encryption endpoints will work with SHA-2 certificates. Those specifically tested are:

- HP LTO5/6 tape drives
- IBM LTO4/5/6/7 tape drives running Belisarius firmware version 5.32.20
- PKCS#11 applications that use the KMS PKCS#11 Provider on Oracle Solaris and Oracle Linux, including ZFS file systems on Oracle Solaris 11 servers and ZFS Storage Appliance.
- Oracle Transparent Database Encryption (TDE) on Oracle Database servers
- Java applications that use the OKM JCE Provider

The Oracle Enterprise Manager plug-in for OKM also works with SHA-256 certificates.

Log Out of Current OKM Console Session

This OKM console function logs out the user from the OKM console session.

Available to: All roles

1. Log into OKM console. At the `Please enter your choice:` prompt on the main menu, type **0** and press **Enter**.
2. The current session terminates and the login prompt displays allowing the user to reenter the OKM Console.

15

Command Line Utilities

Use the command line utilities as an alternative to using OKM Manager to launch backups, export keys, import keys, and list data units.

> **Note:**
>
> The OKM Command Line utility supersedes the Backup Command Line utility. Oracle recommends you use the OKM Command Line utility whenever possible.

OKM Command Line Utility

Use the OKM command line utilitiy as an alternative to OKM Manager to create backups, export or import keys, list data units, and modify agents.

The OKM Command Line utility allows you to:

- Schedule automated backups
- Back up OKM core security
- Import and export keys
- Destroy keys
- List audit events
- List data units
- Create or modify multiple agents.

Unlike the Backup Command Line utility, this utility can use X.509 certificates to authenticate itself as a valid OKM user instead of a username and passphrase, so you are not required to enter a passphrase on the command line.

This utility is installed with the OKM Manager GUI using the same installer.

> **Note:**
>
> If you want to enter link-local IPv6 addresses, invoke the OKM Command Line Utility and specify the link-local IPv6 address. Include the Zone ID (for example, "%4") at the end of the address. Refer to IPv6 Addresses with Zone IDs to see what steps you must follow for the initial setup.
>
> If you are using Solaris, and wish to specify or display characters than cannot be represented in ASCII, then ensure that the appropriate Solaris locale has been installed on your Solaris system and then your environment has been configured to use this locale. Refer to the Solaris locale(1) and localeadm(1M) man pages for more information.

Supported Platforms

- Oracle Solaris 11
- Oracle Linux 6.x and 7
- Microsoft Windows Server 2016 and 2012
- Microsoft Windows 8 and 10

User Roles

The following table details the roles that can perform each function of the command line.

Table 15-1 OKM Command Line Utility - User Role Access

Action:	Role:
Backup	Backup Operator
Back up OKM Core Security	Security Officer
Import/Export Keys	Operator
Destroy Keys	Operator
List Audit Events	All Roles[1]
List Data Units	Operator/Compliance Officer
Create Agents	Operator
Set/Change Agent Default Key Group	Compliance Officer
Change Agent Properties	Operator
List Agents	Operator/Compliance Officer

1 If you specify agent IDs, data unit IDs, or key IDs, you must have the Operator or Compliance Officer role.

OKM Command Line Subcommand Descriptions

This section lists the subcommands of the OKM Command Line utility.

backup
Generates a backup of the OKM data and downloads this backup to a backup data file and a backup key file in the specified output directory.

```
okm backup [ [ [ --cacert=filename ]     [ --usercert=filename ] ]
               [ --directory=dirname ] ] | --oper=username
               [ --retries=retries ]     [ --timeout=timeout ]
               [ --verbose=boolean ]
                 --kma=networkaddress
                 --output=dirname
```

backupcs
Generates a backup of the OKM core security and stores this backup in an output file.

```
okm backupcs [ [ [ --cacert=filename ]   [ --usercert=filename ]]
                 [ --directory=dirname ] | --oper=username ]
                 [ --retries=retries ]   [ --timeout=timeout ]
                 [ --verbose=boolean ]
                   --kma=networkaddress
```

createagent
Creates a new agent.

```
okm createagent[ [ [ --cacert=filename ] [ --usercert=filename ] ]
                   [ --directory=dirname ] | --oper=username ]
                   [ --retries=retries ] [ --timeout=timeout ]
                   [ --verbose=boolean ]
                   [ --description=description ]
                   [ --site=siteid ]
                   [ --keygroup=defaultkeygroupid ]
                   [ --onetimepassphrase=boolean ]
                     --kma=networkaddress
                     --agent=agentid
                     --passphrase=agentpassphrase
```

currload
Displays load information about a KMA.

```
okm currload [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                 [ --directory=dirname ] ] | --oper=username
                 [ --retries=retries ] [ --timeout=timeout ]
               [ --verbose=boolean ]
                 --output=filename
                 --kma=networkaddress
```

destroykeys
Destroys deactivated or compromised keys.

```
okm destroykeys [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                    [ --directory=dirname ] | --oper=username ]
                    [ --retries=retries ] [ --timeout=timeout ]
                    [ --verbose=boolean ]
                      --kma=networkaddress
                      --duids=filename | --all=true
```

```
                    --keystate=keystate
                    --comment="text"
```

export
Creates a secure key file for a transfer partner that has been established with the OKM. All keys associated with a list of data units are exported using this key file and are protected using an AES-256-bit key that signs the key file. This list of data units is the result of the given filter string or file name. This key file can then be used to import the keys into the transfer partner's OKM using the `import` subcommand. Up to 1,000 data units can be exported on a single invocation of the `kms` command.

```
okm export [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] | --oper=username ]
               [ --retries=retries ] [ --timeout=timeout ]
               [ --listwait=waittime ] [ --verbose=boolean ]
                 --filter=filter | --duids=filename
                 --kma=networkaddress
                 --output=filename
                 --partner=transferpartnerid
```

import
Reads a secure key file for a transfer partner that has been established with the OKM. Keys and their associated data units are imported using this key file. The key transfer private key of the importing OKM is used to validate the key file. This file must be one that was previously exported from another OKM using the `export` subcommand.

```
okm import [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] ] | --oper=username
               [ --retries=retries ] [ --timeout=timeout ]
               [ --verbose=boolean ]
               [ --overrideeuiconflict=boolean ]
                 --kma=networkaddress
                 --input=filename
                 --partner=transferpartnerid
                 --keygroup=keygroupid
```

listagentperformance
Lists agents and performance information about them. This performance information includes rate or count values and average processing time for various create and retrieve key requests. You can filter the list to produce a specific report containing just a subset of the agents.

```
okm listagentperformance [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                           [ --directory=dirname ] | --oper=username ]
                           [ --filter=filter ]
                           [ --retries=retries ] [ --timeout=timeout ]
                           [ --listwait=waittime ] [ --verbose=boolean ]
                           [ --output=filename ]
                           [ --startdate=date ] [ --enddate=date ]
                           [ --localtimezone=boolean ]
                           [ --rateinterval=rateinterval ]
                             --kma=networkaddress
```

listagents
Lists agents and their properties. You can filter the list to produce a specific report containing just a subset of the agents.

```
okm listagents[ [ [ --cacert=filename ] [ --usercert=filename ] ]
                [ --directory=dirname ] | --oper=username ]
                [ --retries=retries ] [ --timeout=timeout ]
                [ --listwait=waittime ] [ --verbose=boolean ]
                [ --filter=filter ] [ --output=filename ]
                  --kma=networkaddress
```

listauditevents
Lists audit events.

```
okm listauditevents [ [ [ --cacert=filename ]
                        [ --usercert=filename ] ]
                        [ --directory=dirname ] |
                        [ --oper=username ]
                        [ --filter=filter ]
                        [ --localtimezone=boolean ]
                        [ --maxcount=count ]
                        [ --retries=retries ]
                        [ --timeout=timeout ]
                        [ --verbose=boolean ]
                        [ --output=filename ]
                        [ --agentids=agentids |
                          --dataunitids=dataunitds |
                          --keyids=keyids ]
                          --kma=networkaddress
```

listdu
Lists data units and their properties. This subcommand can be invoked before executing the `export` subcommand to determine the data units that are exported using the specified filter (if any).

```
okm listdu [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] ] | --oper=username
               [ --filter=filter ]
               [ --retries=retries ] [ --timeout=timeout ]
               [ --listwait=waittime ] [ --verbose=boolean ]
               [ --output=filename ]
                 --kma=networkaddress
```

listdukeycount
Lists data units that have associated keys and a count of these keys. You can filter the list to produce a specific report containing just a subset of the data units.

```
okm listdukeycount[ [ [ --cacert=filename ] [ --usercert=filename ] ]
                    [ --directory=dirname ] | --oper=username ]
                    [ --filter=filter ]
                    [ --retries=retries ] [ --timeout=timeout ]
                    [ --listwait=waittime ] [ --verbose=boolean ]
                    [ --output=filename ]
                      --kma=networkaddress
                      --duids=filename | --all=true
```

listkeys
Lists keys and their properties. You can filter the list to produce a specific report containing just a subset of the keys.

```
okm listkeys [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                 [ --directory=dirname ] | --oper=username ]
                 [ --filter=filter ]
```

```
                [ --retries=retries ] [ --timeout=timeout ]
                [ --listwait=waittime ] [ --verbose=boolean ]
                [ --output=filename ]
                  --kma=networkaddress
```

listkmaperformance
Lists KMAs and performance information about them. This performance information includes rate or count values and average processing time for key requests from agents, replication requests from peer KMAs, requests from users, and Server Busy conditions on the local KMA. You can filter the list to produce a specific report containing just a subset of the KMAs.

```
okm listkmaperformance [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                           [ --directory=dirname ] | --oper=username ]
                           [ --filter=filter ]
                           [ --retries=retries ] [ --timeout=timeout ]
                           [ --listwait=waittime ] [ --verbose=boolean ]
                           [ --output=filename ]
                           [ --startdate=date ] [ --enddate=date ]
                           [ --localtimezone=boolean ]
                           [ --rateinterval=rateinterval ]
                             --kma=networkaddress
```

modifyagent
Changes properties of an existing agent, including its default key group. You must also specify at least one of the following options: --enabled, --site, --description, --keygroup, --passphrase, --onetimepassphrase

```
okm modifyagent[ [ [ --cacert=filename ]   [ --usercert=filename ] ]
                   [ --directory=dirname ] | --oper=username ]
                   [ --retries=retries ]   [ --timeout=timeout ]
                   [ --verbose=boolean ]
                   [ --description=description ] |
                   [ --site=siteid ] |
                   [ --keygroup=defaultkeygroupid ] |
                   [ --passphrase=agentpassphrase ] |
                   [ --enabled=boolean ] |
                   [ --onetimepassphrase=boolean ]
                     --kma=networkaddress
                     --agent=agentid
```

systemdump
Generates and downloads a system dump file.

```
okm systemdump [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                   [ --directory=dirname ] | --oper=username ]
                   [ --retries=retries ] [ --timeout=timeout ]
                   [ --verbose=boolean ]
                   [ --contents=contents ]
                     --kma=networkaddress
                     --output=filename
```

OKM Command Line Options

These are the OKM Command Line commands options.

A long option name is separated from its value by an equals sign (=).

A short option name is separated from its value by a space.

> **Note:**
>
> Users must first export the Root CA and user X.509 certificates from the OKM Manager GUI before invoking this utility with the `--cacert`, `--directory`, and `--usercert` options.

Long Option Name	Short Name	Description
`--agent=`*agentid*	`-B`	Specifies an agent ID to be created or modified. This agent ID must be between 1 and 64 characters in length, inclusive.
`--agentids=`*agentids*	`-A`	Specifies a comma-separated list of agent IDs for associated audit events. Each agent ID must be between 1 and 64 characters in length. The OKM user must have the Operator or Compliance Officer role to be able to specify this option. This option is mutually exclusive with the `--dataunitids` and `--keyids` options.
`--all=`*true*	`-l`	Indicates that this utility destroys all deactivated or compromised keys, as indicated by the `--keystate` option, for all data units. This option is mutually exclusive with the `--duids` option.
`--cacert=`*filename*	`-a`	Specifies a OKM Root CA X.509 certificate PEM file for this utility to use to authenticate itself with the OKM. If not specified, then the utility looks for a ca.crt file in the directory specified by the `--directory` option. This option is mutually exclusive with the `--oper` option.
`--comment="`*text*`"`	`-C`	Specifies a comment describing the key destruction. This comment must be between 1 and 64 characters in length.
`--contents=`*contents*	`- c`	Specifies which types of information to include in the system dump file. "default" or not specifying this value results in the system dump containing the type of information included in OKM releases prior to 3.3.2. "stig" results in a report of Security Technical Implementation Guide analysis in a checklist file (in Extensible Configuration Checklist Description Format (XCCDF) .xml format) and an osss.txt file containing output (stdout and stderr) from running the Oracle Solaris 11 Security Scripts (OSSS) tool. "all" will include both the default and stig information.
`--dataunitids=`*datunitids*	`-D`	Specifies a comma-separated list of data unit IDs for associated audit events. Each data unit ID must be 32 hexadecimal characters. The OKM user must have the Operator or Compliance Officer role to be able to specify this option. This option is mutually exclusive with the `--agentids` and `--keyids` options.
`--description=`*description*	`-R`	Specifies a description of the agent being created or modified. The description must be between 1 and 64 characters in length, inclusive.
`--directory=`*dirname*	`-d`	Specifies a directory in which to search for a PEM file containing a OKM Root CA X.509 certificate and a PEM file containing a OKM user X.509 certificate. If not specified, then this utility looks for the certificate files in the current working directory. This option is mutually exclusive with the `--oper` option.
`--duids=`*filename*	`-i`	For key export or destruction, this option specifies a filename containing a set of data unit IDs, one per line, new line delimited. Each data unit ID must be 32 hexadecimal characters. On the `destroykeys` subcommand, if a particular data unit does not have any deactivated or compromised keys, then that data unit is ignored. If the specified file is empty, then the `destroykeys` subcommand destroys all deactivated or compromised keys for all data units (see the `--all` option). This option is mutually exclusive with the `--filter` and `--all` options.

Long Option Name	Short Name	Description
`--enddate`	`-e`	Specifies the end date and time of a performance query in the format: YYYY-MM-DD hh:mm:ss, representing a value in universal coordinated time (UTC) or local time if the localtimezone option is true. The default value is the present.
`--filter=`*filter*	`-f`	Specifies a filter string that is processed to generate either a list of data unit IDs to display or export or a list of audit events to display. The string must be enclosed in quotes (double quotes on Windows) if it contains white space (see "OKM Command Line Examples"). Exporting takes time proportional to the number of data units and keys, so typically you should specify a filter that reduces the set of data units. See "OKM Command Line Filter Parameters" for more information.
`--help`	`-h`	Displays help information.
`--input=`*filename*	`-i`	Specifies the file name from which data units and keys are to be imported. This file is also known as the key transfer file.
`--keygroup=`*keygroupid*	`-g`	Specifies the ID of a key group that is defined to the OKM.
`--keyids=`*keyids*	`-K`	Specifies a comma-separated list of key IDs for associated audit events. The OKM user must have the Operator or Compliance Officer role to be able to specify this option. This option is mutually exclusive with the `--agentids` and `--dataunitids` options.
`--keystate=`*keystate*	`-s`	Specifies the state of keys to be destroyed. The keystate value can be "`deact`" for deactivated keys, "`comp`" for compromised keys, or "`deact +comp`" for deactivated or compromised keys.
`--kma=`*networkaddress*	`-k`	Specifies the network address of the KMA to issue the request. The network address can be a host name, an IPv4 address, or an IPv6 address.
`--listwait=`*waittime*	`-w`	Specifies the number of seconds between List Data Units requests issued by the `export` and `listdu` subcommands. The default value is 2.
`--localtimezone=`*boolean*	`-L`	Displays timestamps of audit events in the local time zone instead of in universal coordinated time (UTC). Also, the StartDate and EndDate filters are interpreted to be in local time.
`--localtimezone`	`-L`	Specifies a boolean value to determine whether input and output times are in the local time zone instead of in Universal Coordinated Time (UTC). This affects the interpretation of input values such as start and end dates and the display of audit event timestamps. The boolean value can be "true" or "false."
`--maxcount=`*count*	`-c`	Specifies the maximum number of audit events to list. The default value is 20,000.
`--onetimepassphrase=`*boolean*	`-O`	Specifies a boolean value to determine whether the enrollment passphrase may be used only once for authentication. The boolean value can be "true" or "false".
`--oper=`*username*	`-b`	Specifies the OKM User ID for this utility to use to authenticate itself with the OKM. If specified, it prompts for the user's passphrase since certificates are not being used. This option is mutually exclusive with the `--cacert`, `--usercert`, and `--directory` options.

Long Option Name	Short Name	Description
`--output=`*filename* or *dirname*	`-o`	Specifies the file name where the results are stored. These results are the backup on `backup` and `backupcs` requests, the key transfer file on `export` requests, a listing of the data units and their properties on `listdu` requests, and a listing of audit events on `listauditevents` requests. On `listdu` and `listauditevents` requests, "-" may be specified for `stdout`, which is also the default. On `backup` requests, this option specifies the directory where the backup data file and backup key file are downloaded.
`--overrideeuiconflict=`*boolean*	`-O`	Specifies a boolean value to determine whether to override a conflict where an existing data unit has the same external unique ID as a data unit being imported. If this value is "true," then the existing data unit is updated to clear its external unique ID and the importing data unit retains its external unique ID. Otherwise, the import request fails. The boolean value can be "true" or "false."
`--partner=`*transferpartnerid*	`-p`	Specifies the ID of the transfer partner that is defined to the OKM and that is eligible to send or receive exported keys.
`--passphrase=`*passphrase*	`-P`	Specifies a passphrase for the agent being created or modified. Passphrases can be from 8 to 64 characters in length, inclusive. Passphrases must follow OKM passphrase rules.
`--rateinterval`	`-I`	Specifies the rate display interval. Request rates will be extrapolated over the selected rate display interval and displayed as the average number of requests per that selected interval (for example, extrapolated average number of Create Key requests per day). Possible values are "second", "minute", "hour", "day", "week", "month" "year" or "entire." Selecting "entire" causes the counts of each request type to be displayed instead of their rates. The default value is "entire".
`--rclientcert=`*filename*	`-C`	Specifies an X.509 certificate PEM file that has been issued by a Certificate Authority for this KMA.
`--rclientkey=`*filename*	`-K`	Specifies a private key file that accompanies the client certificate file.
`--rclientpassword=`*password*	`-P`	Specifies a password (if any) that protects the private key.
`--retries=`*retries*	`-r`	Specifies the number of times that this utility tries to connect to the KMA, if the KMA is busy. The default value is 60.
`--server=`*networkaddress*	`-S`	Specify the network address (IP address or, if DNS is configured, host name) of the remote syslog system.
`--site=`*siteid*	`-S`	Specifies the site ID for the agent being created or modified. This site ID must be between 1 and 64 characters in length, inclusive.
`--startdate`	`-s`	Specifies the start date and time of a performance query in the format: YYYY-MM-DD hh:mm:ss, representing a value in universal coordinated time (UTC) or local time if the localtimezone option is true. The default value is the beginning of data collection.
`--timeout=`*timeout*	`-t`	Specifies the timeout value in seconds between these retries. The default value is 60.
`--usercert=`*filename*	`-u`	Specifies a OKM user's X.509 certificate PEM file for this utility to use to authenticate itself with the OKM. This certificate file must also contain the user's private key. If not specified, then the utility looks for a `clientkey.pem` file in the directory specified by the `--directory` option. This option is mutually exclusive with the `--oper` option.

Long Option Name	Short Name	Description
`--verbose=`*boolean*	`-n`	Indicates that this utility generates verbose output, including progress status during the processing of the request. The boolean value can be "true" or "false."
`--version`	`-v`	Displays command-line usage.

OKM Command Line Filter Parameters

This section list the filter parameters for the OKM Command Line utility.

export and listdu
On the `export` subcommand, this option is mutually exclusive with the `--duids` option.
On the `export` and `listdu` subcommands, the syntax of this filter string is:

```
DUState=state[, Exported=boolean ][, Imported=boolean]
[, DataUnitID=duid][, ExternalTag=tag]
[, ExternalUniqueID=euid]
```

- `DUState=`*state* — Where *state* can be "normal", "needs-rekey", or "normal+needs-rekey." If the `DUState` filter is not specified, then the default is "DUState=normal +needs-rekey."
- `Exported=`*boolean* — Where *boolean* can be "true" or "false." If the `Exported` filter condition is not specified, then data unit selection does not consider the exported state, so both exported data units and data units that have not been exported yet are eligible for selection.
- `Imported=`*boolean* — Where *boolean* can be "true" or "false." If the `Imported` filter condition is not specified, then data unit selection does not consider the imported state, so both imported data units and data units that have not been imported yet are eligible for selection.
- `DataUnitID=`*duid* — Where *duid* is a data unit ID.
- `ExternalTag=`*tag* — Where *tag* is an External Tag (must be padded to 32 characters with spaces for data units created for LTO tape drives).
- `ExternalUniqueID=`*euid* — Where *euid* is an External Unique ID.

listagentperformance
On the `listagentperformance` subcommand, the syntax of this filter string is:

```
AgentID=agentid[, SiteID=siteid][, DefaultKeyGroupID=kgid]
```

- `AgentID=`*agentid* — Where *agentid* is an agent name. The CLI uses the "starts with" operator (instead of equality) when matching on this field as some agents supply trailing blanks to the value for this field.
- `SiteID=`*siteid* — Where *siteid* is a Site ID.
- `DefaultKeyGroupID=`*kgid* — Where *kgid* is a key group ID.

listauditevents
On the `listauditevents` subcommand, the syntax of this filter string is:

```
StartDate=date[, EndDate=date ][, Severity=text]
[, Operation=text][, Condition=text] [, Class=text]
[, RetentionTerm=text] [, KMAName=kmaname]
[, EntityID=entityid][, EntityNetworkAddress=netaddress]
[, SortOrder=order][, ShowShortTerm=boolean]
```

- `StartDate=`*date* — Where *date* has the format: *YYYY-MM-DD hh*:*mm*:*ss* and represents UTC time.
- `EndDate=`*date* — Where *date* has the format: *YYYY-MM-DD hh*:*mm*:*ss* and represents UTC time.
- `Severity=`*text* — Where *text* is an audit severity string (for example, "Error").
- `Operation=`*text* — Where *text* is an audit operation string (for example, "Retrieve Root CA Certificate").
- `Condition=`*text* — Where *text* is an audit condition string (for example, "Success").
- `Class=`*text* — Where *text* is an audit class string (for example, "Security Violation").
- `RetentionTerm=`*text* — Where *text* is an audit retention term string (for example, "MEDIUM TERM RETENTION").
- `KMAName=`*kmaname* — Where *kmaname* is a KMA name.
- `EntityID=`*entityid* — Where *entityid* is an Entity ID.
- `EntityNetworkAddress=`*netaddress* — Where *netaddress* is an IP address or host name.
- `SortOrder=`*order* — Where *order* can be "`asc`" or "`desc`." By default, audit events are displayed in descending order by Created Date.
- `ShowShortTerm=`*boolean* — Where *boolean* can be "true" or "false." By default, audit events that have a short term retention are not displayed.

listkeys

On the listkeys subcommand, the syntax of this filter string is:

```
KeyState=state[, KeyID=keyid][, KeyGroupID=kgid]
              [, Exported=boolean][, Imported=boolean]
              [, Revoked=boolean]
```

- `KeyState=`*state* — Where *state* can be one of the following: gen, ready, pnp, proc, deact, comp, dest
- `KeyID=`*keyid* — Where *keyid* is a Key ID.
- `KeyGroupID=`*kgid* — Where *kgid* is a key group ID.
- `Exported=`*boolean* — Where *boolean* can be "true" or "false".
- `Imported=`*boolean* — Where *boolean* can be "true" or "false".
- `Revoked=`*boolean* — Where *boolean* can be "true" or "false".

listkmaperformance

On the listkmaperformance subcommand, the syntax of this filter string is:

```
KMAName=kmaname[, SiteID=siteid]
```

- `KMAName=`*kmaname* — Where *kmaname* is a KMA name.
- `SiteID=`*siteid* — Where *siteid* is a Site ID.

OKM Command Line Examples

Examples showing a single command line. In some cases, the command line appears on multiple lines for readability. In Solaris examples, backslashes denote the continuation of a command line.

Generating Backups
Generating backup using certificates in the ca.crt and clientkey.pem files in the given directory for authentication:
Solaris:

```
okm backup --kma=mykma1 \
           --directory/export/home/Joe/.sunw/kms/BackupOperatorCertificates \
           --output=/export/home/KMSBackups
```

Windows:

```
okm backup --kma=mykma1
           --directory=D:\KMS\Joe\BackupOperatorCertificates
           --output=D:\KMS\KMSBackups
```

Generating a backup using the user ID and passphrase of a OKM user for authentication:
Solaris:

```
okm backup -k mykma1 -o /export/home/KMSBackups -b Joe
```

Windows:

```
okm backup -k mykma1 -o D:\KMS\KMSBackups -b Joe
```

Exporting Keys
Exporting keys using certificates in the ca.pem and op.pem files in the current working directory for authentication:
Solaris:

```
okm export -k 10.172.88.88 -d "." -a ca.pem -u op.pem \
           -f "DUState = normal+needs-rekey, Exported = false" \
           -o Partner.dat -p Partner
```

Windows:

```
okm export -k 10.172.88.88 -d "." -a ca.pem -u op.pem
           -f "DUState = normal+needs-rekey, Exported = false"
           -o Partner.dat -p Partner
```

Exporting keys using the user ID and passphrase of a OKM user for authentication:
Solaris:

```
okm export --kma=mykma1 --oper=tpFreddy \
           --filter="Exported = false" --output=Partner.dat \
           --partner=Partner
```

Windows:

```
okm export --kma=mykma1 --oper=tpFreddy
           --filter="Exported = false" --output=Partner.dat
           --partner=Partner
```

Importing Keys

Importing keys using certificates in the ca.crt and clientkey.pem files in the current working directory for authentication:

Solaris:

```
okm import --kma=10.172.88.88 --directory="." \
           --input=DRKeys.dat --partner=Partner \
           --keygroup=OpenSysBackupKeyGroup
```

Windows:

```
okm import --kma=10.172.88.88 --directory="."
           --input=DRKeys.dat --partner=Partner
           --keygroup=OpenSysBackupKeyGroup
```

Importing keys using the user ID and passphrase of a OKM user for authentication.

Solaris:

```
okm import --kma=mykma1 --oper=Joe --input=DRKeys.dat \
           --partner=Partner --keygroup=OpenSysBackupKeyGroup
```

Windows:

```
okm import --kma=mykma1 --oper=Joe --input=DRKeys.dat
           --partner=Partner --keygroup=OpenSysBackupKeyGroup
```

Listing Data Units

Listing data units using certificates in the ca.crt and clientkey.pem files in the given directory for authentication:

Solaris:

```
okm listdu --kma=10.172.88.88 \
            --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
            --output=/export/home/KMSDataUnits
```

Windows:

```
okm listdu --kma=10.172.88.88
           --directory=D:\KMS\Joe\OperatorCertificates
           --output=D:\KMS\KMSDataUnits
```

Listing data units using the user ID and passphrase of a OKM user for authentication:

Solaris:

```
okm listdu -k mykma1 -b Joe -f "Exported=false" \
           --output=/export/home/KMSDataUnits
```

Windows:

```
okm listdu -k mykma1 -b Joe -f "Exported=false"
           --output=D:\KMS\KMSDataUnits
```

Listing Audit Events

Listing audit events using certificates in the ca.crt and clientkey.pem files in the given directory for authentication.

Solaris:

```
okm listauditevents --kma=10.172.88.88 \
                    --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
                    --filter=Severity=Error \
                    --output=/export/home/KMSAuditEvents
```

Windows:

```
okm listauditevents --kma=10.172.88.88
                    --directory=D:\KMS\Joe\OperatorCertificates
                    --filter=Severity=Error
                    --output=D:\KMS\KMSAuditEvents
```

Listing audit events using the user ID and passphrase of a OKM user for authentication.
Solaris:

```
okm listauditevents -k mykma1 -b Joe -f "Severity=Error" \
                    --output=/export/home/KMSAuditEvents
```

Windows:

```
okm listauditevents -k mykma1 -b Joe -f "Severity=Error"
                    --output=D:\KMS\KMSAuditEvents
```

Destroying Keys
The following examples destroy all compromised keys using certificates in the ca.crt and clientkey.pem files in the given directory for authentication.
Solaris:

```
okm destroykeys --kma=10.172.88.88 \
                --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
                --all=true --keystate=comp \
                --comment="Joe destroyed compromised keys"
```

Using the user ID and passphrase of a OKM user for authentication:

Windows:

```
okm destroykeys --kma=10.172.88.88
                --directory=D:\KMS\Joe\OperatorCertificates
                --all=true --keystate=comp
                --comment="Joe destroyed compromised keys"
```

The following examples destroy deactivated keys associated with a list of data unit IDs using the user ID and passphrase of a OKM user for authentication.
Solaris:

```
okm destroykeys -k mykma1 -b Joe -i DeactivatedDUIDs.txt \
                -s deact -C "Joe destroyed deactivated keys"
```

Windows:

```
okm destroykeys -k mykma1 -b Joe -i DeactivatedDUIDs.txt
                -s deact -C "Joe destroyed deactivated keys"
```

Backing Up Core Security
The following examples back up core security using certificates in the ca.crt and clientkey.pem files in the given directory for authentication.
Solaris:

```
okm backupcs --kma=10.172.88.88 \
             --directory=/export/home/Joe/.sunw/kms/SecurityOfficerCertificates \
             --output=/export/home/KMSCoreSecurity.xml
```

Windows:

```
okm backupcs --kma=10.172.88.88
             --directory=D:\KMS\Joe\SecurityOfficerCertificates
             --output=D:\KMS\KMSCoreSecurity.xml
```

The following examples back up core security using the user ID and passphrase of a OKM user for authentication.
Solaris:

```
okm backupcs -k mykma1 -b Joe -o /export/home/KMSCoreSecurity.xml
```

Windows:

```
okm backupcs -k mykma1 -b Joe -o D:\KMS\KMSCoreSecurity.xml
```

OKM Command Line Exit Values

This section lists the exit values for the OKM command line utility.

The following exit values are returned:

```
 0    Successful completion
 >0   An error occurred
```

OKM Command Line Sample Perl Scripts

This section provides some basic perl scripts that you can customize and run on either Solaris or Windows.

These examples all use certificate-based authentication and require that the Root CA certificate and user's certificate reside in the current working directory. The perl scripts are not installed with the OKM Command Line utility. If you want to invoke the OKM Command Line utility from a perl script, use a text editor to create one that looks similar to one of the perl scripts shown here.

listdu.pl

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="okm";
$KMA="kma1.example.com";
$FILTER="--filter=Exported=false";
$DIRECTORY=".";
$OUTPUT="listdu.txt";
system("$cmd listdu --verbose=true --directory=$DIRECTORY --kma=$KMA $FILTER
       --output=$OUTPUT")
```

export.pl

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="okm";
$KMA="kma1.example.com";
$TP="DestinationPartner";
```

```
$FILTER="Exported=false";
$OUTPUT="$TP.dat";
system("$cmd export --verbose=true --kma=$KMA --directory=. --filter=$FILTER
       --partner=$TP --output=$OUTPUT");
```

import.pl

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="okm";
$KMA="kma1.example.com";
$TP="SourceTransferPartner";
$KEYGROUP="MyKeyGroup";
$INPUT="../aberfeldy/KeyBundle.dat";
system("$cmd import --verbose=true --kma=$KMA --directory=. --partner=$TP
       --keygroup=$KEYGROUP --input=$INPUT");
```

backup.pl

```
#!/opt/csw/bin/perl
## the following must be in your path
$cmd="okm";
$KMA="kma1.example.com";
$DIRECTORY=".";
$OUTPUT=".";
system("$cmd backup --verbose=true --directory=$DIRECTORY --kma=$KMA
       --output=$OUTPUT")
```

Backup Command Line Utility

Use the Backup Command Line utility to launch or schedule a backup.

Oracle recommends you use the OKM Command Line Utility instead of the Backup Command Line utility. The Backup utility is installed with the OKM Manager GUI using the same installer.

> **Note:**
>
> If you want to enter link-local IPv6 addresses, invoke the Backup Utility and specify the link-local IPv6 address. Include the Zone ID (for example, "%4") at the end of the address. Refer to IPv6 Addresses with Zone IDs to see what steps you must follow for the initial setup.

Solaris Syntax

```
OKM_Backup [-UserID userid] [-Passphrase passphrase]
           -KMAIPAddress IPaddress -BackupFilePath pathname
           [-Retries retries] [-Timeout timeout]
```

Windows Syntax

```
OKMBackupUtility [-UserID userid] [-Passphrase passphrase]
                 -KMAIPAddress IPaddress -BackupFilePath pathname
                 [-Retries retries] [-Timeout timeout]
```

Parameter Descriptions

userid — The Backup Operator user ID. This must be a Backup Operator.

passphrase — The passphrase for the user ID. If the userid or passphrase value is not specified, the utility prompts you for these values.

IPaddress — The KMA Management Network Address on which to launch the backup.

pathname — The location where the backup file and backup key file should be downloaded on your system.

retries — The number of times that this utility tries to connect to the KMA, if the KMA is busy. The default is 60.

timeout — The timeout value in seconds between these entries. The default is 60.

Example 15-1 Backup Command Line Sample

The following example creates a backup file (format: OKM-Backup-backupid-timestamp.dat) and a backup key file (format: OKM-BackupKey-backupid-timestamp.xml).

```
OKM_Backup -UserID MyBackupOperator \
           -KMAIPAddress 10.0.60.172 \
           -BackupFilePath /tmp/MyKMSDownloads
OKM Backup Utility  Version 3.0.0 (build2020)
Copyright (c) 2007, 2013, Oracle and/or its affiliates.  All Rights Reserved.
Enter Passphrase:
```

> **Note:**
>
> The passphrase can optionally be specified on the command line using the -Passphrase parameter.

16
Certificates

A certificate is an electronic document used to prove the ownership of a public key. You can generate, sign, save, and renew certificates.

- Generate and Sign Certificates Using SHA-256
- Ongoing Renewal Policy for the Root CA Certificate
- Save a Client Certificate

Generate and Sign Certificates Using SHA-256

Generate and sign certificates using SHA-256 if you want the cluster to use an X.509v3 certificate for the CA and all subsequently generated entity certificates. Otherwise, the certificate version will remain X.509v1 for legacy compatibility purposes.

To generate new certificates and then sign them using SHA-256, the OKM administrator must perform this procedure. (For OKM 3.3.1 customers, this procedure is necessary only if they want/need X.509v3 certificates, as they have started in production with SHA-256 signed certificates). The cluster must be running OKM 3.3.2 or later at replication version 16 or later.

> **Note:**
>
> Plan this procedure in advance. It impacts the entire cluster's KMAs, agents, and disaster recovery (obsoletes backups). If you have a lot of tape agents, use the Oracle Virtual Operator Panel 2.2 spreadsheet feature to automate the re-enrollment process and reduce downtime.

Complete the tasks listed below in order.

- Renew the Root Certificate
- Create an OKM Backup After Renewing a Certificate
- Retrieve the New Root CA on Peer KMAs (optional)
- Reissue Certificates for Agents (optional)
- Update Users Passphrase (optional)
- Update Disaster Recovery Records

Renew the Root Certificate

Use OKM console to renew the root certificate. This is task 1 of generating a new certificate.

1. Choose the KMA that will renew the root CA certificate.
2. Ensure that the replication version is greater at least 16 for the selected KMA. See Check the Replication Version of the KMA. If the version is less than 16, switch the replication version to 16. See Switch the Replication Version.
3. Launch the OKM Console on the KMA that you will use to renew, and log into it as a Security Officer. Select the menu option to Renew the Root CA Certificate (see Renew the Root CA Certificate).

Create an OKM Backup After Renewing a Certificate

Use OKM Manager to create a backup and destroy all previous backups. This is task 2 of generating a certificate.

Create a backup on the KMA you used to perform the renew certificate operation. Destroy all other backups in the cluster using the OKM Manager GUI with a note that they are obsolete due to a renew. This will prevent these backups from accidentally being selected in a subsequent cluster join with replication acceleration.

1. Launch the Oracle Key Manager GUI and log into this KMA as a Backup Operator.
2. Navigate to the **Backup List** panel.
3. Click **Create Backup** to generate a backup and download it to your workstation.
4. For each previous backup, select it and then click **Confirm Destruction**. Enter a comment that the backup is obsolete due to a Root CA certificate renew.

Retrieve the New Root CA on Peer KMAs (optional)

Retrieve the new Root CA certificate instead of waiting for the certificate to automatically propagate. This is task 3 of generating a new certificate. It is an optional step.

The new certificates will automatically propagate to the other KMAs in the cluster. However, if a KMA has a large replication lag size, you might want to retrieve the new Root CA Certificate and the certificate for this KMA right away instead of waiting for the certificates to propagate.

1. Launch the OKM GUI and log into the KMA that you used for the backup.
2. Navigate to the **KMA List** panel.
3. Log this KMA out of the cluster by modifying the KMA passphrase. See Change a KMA Passphrase (Log the KMA Out of the Cluster).
4. Launch the host console from the ILOM of this KMA.
5. Log the KMA back into the cluster. See Log KMA Back into Cluster .

Reissue Certificates for Agents (optional)

Reissue the certificates for agents to have them use the new certificate. This is task 4 of generating a new certificate. It is an optional step.

After renewing the Root CA certificate, agents will continue to use their existing credentials. The OKM administrator might decide to reissue certificates for the agents and then re-enroll them.

1. Launch the Oracle Key Manager GUI and log into it as an Operator or a Compliance Officer.
2. Navigate to the **Agent List** panel.
3. For each agent:
   a. Bring up the Agent Details dialog (either double-click the agent entry or select an agent and click **Details**).
   b. Select the **Passphrase** tab and change the passphrase to the same value or to a different value if desired.
4. Navigate to the **KMA List** panel.
5. All agents will need to re-enroll into the OKM Cluster. See Enroll Agents. If you have a lot of tape agents, use the VOP 2.2 spreadsheet feature to automate the re-enrollment process.

Update Users Passphrase (optional)

The OKM administrator can reissue certificates for the users by changing their passphrase (OKM users are automatically issued a new certificate when they successfully log in). This is task 5 of generating a new certificate. This is an optional step.

To modify a user's passphrashe, see Modify a User's Details and Set the User's Passphrase.

If there are OKM CLI users, download the new Root CA Certificate and new entity certificate for that user, as described in Save a Client Certificate.

Update Disaster Recovery Records

Update relevant disaster recovery records to reflect the change in the certificate. This is task 6 of generating a new certificate.

1. Update your site's disaster recovery (D/R) records to note that all previous backups will restore the cluster to utilize the former SHA1-based root CA certificate.
2. Replicate the latest backup to D/R sites as soon as possible and in accordance with your site's D/R plans.

Ongoing Renewal Policy for the Root CA Certificate

Adopt a policy of renewing the Root CA certificate in your cluster on a regular basis to decrease the risk of it being compromised.

You can view the age of the current Root CA certificate from the OKM Console, see Show Properties of the Root CA Certificate. You can download the Root CA certificate from the OKM Manager GUI to your workstation, see Save a Client Certificate. When you are ready, you can renew the Root CA certificate, see Renew the Root CA Certificate.

Save a Client Certificate

Save a certificate so that it can be used by the OKM command line utility to authenticate itself as a valid OKM user.

Save the client certificate in either PEM format or PKCS#12 format. Save a certificate in PEM format to use if for Command Line Interface (CLI) operations. The PEM format contains the certificate and the unencrypted private key. The PKCS#12 format is encrypted. You can convert a PKCS#12 format to PEM format if needed (see Convert PKCS#12 Format to PEM Format).

> **Note:**
>
> Store these certificate files in a secure location with sufficient permissions to restrict access by other users.

1. From the System menu, select **Save Certificates**.

   The Save Certificates dialog box is displayed, with automatically-generated filenames for the Root CA Certificate and the Client Certificates. You can edit these filenames directly or click Browse to select a different destination path or edit the filenames.
2. In the Format field, select the format that the certificate should be in when it is exported.
3. If you selected the PKCS#12 format, type a passphrase in the Passphrase field to use for encryption and retype this passphrase in the Confirm Passphrase field.
4. Click **OK** to export these certificates. When these certificates have been exported, a message is displayed, indicating the locations of these files.
5. You can use the openssl utilty to view the contents of the downloaded certificate. For example:

   ```
   openssl x509 -text -noout -in ca.crt
   ```

Convert PKCS#12 Format to PEM Format

Use the `openssl` utility to convert a certificate saved in PKCS#12 format to PEM format. PEM format is used by the OKM command line utility.

1. Locate the `openssl` utility in the directory where the OpenSSL distribution is installed on your workstation.
2. Use the following syntax:

   ```
   openssl pkcs12 -in PKCS12file -out PEMfile -nodes
   ```
   For example:

   ```
   openssl pkcs12 -in KeyTransferOperator.p12 \
   -out KeyTransferOperator.pem -nodes
   Enter Import Password:
   ```

   The `-nodes` argument is necessary to export the private key. Since the private key is not password protected, you should appropriately manage this file. The

Import Password can optionally be specified on the command line using the `-passin` parameter, if required.

A
Disaster Recovery

Disaster recovery is the process for recovering or preventing the loss of business critical information after a natural or human-induced disaster.

Recover a KMA

The cluster allows the system to recover from a KMA failure, as long as there is at least one functioning KMA in the cluster.

OKM uses a cluster of at least two KMAs to reduce the risk of disruptions and assist in recovery. Clustering KMAs allows you to replicate database entries and balance workloads. If a component fails, it can be easily replaced and restored. When designing an encryption and archive strategy, you should ensure that critical data is replicated and vaulted off-site (see Example Scenarios for Recovering Data). If at least one KMA remains operational, you can recover a single KMA without impacting the rest of the cluster.

The following sections address scenarios that require recovery of a single KMA.

KMA Recovery Following a Software Upgrade

Software upgrades do not require a repair or a recovery, however sometimes the KMA will be out of service as the upgrade takes place. The cluster allows the upgrade to occur without interrupting the active encryption agents. You can download the new software concurrently on all KMAs in the cluster, however activating the new software requires the KMA to reboot. Therefore to prevent an interruption, you should stagger rebooting the KMAs in the cluster so that at least one KMA is always active. As each KMA returns to an online status, any database updates done while the KMA was offline will be replicated and all KMAs in the cluster will re-synchronize.

KMA Recovery Following a Network Disconnection

When a KMA disconnects from the management network, such as when activating new software, the remaining KMAs in the cluster attempt to contact it and report communication errors in the audit event log. Agents continue to communicate with other KMAs across the network. Usually these are other KMAs attached to the same service network. However, because agents may be attached to the management network, they first attempt to work with the KMAs in their own configured site; but if need be, they will contact any reachable KMAs within the cluster. When the KMA reconnects to the network, any database updates done while the KMA was disconnected will be replicated and all KMAs in the cluster re-synchronize.

KMA Recovery Following a Hardware Failure

If a hardware failure occurs, you should first delete the KMA from the cluster so that the remaining KMAs stop attempting to communicate with it. If the KMA console is still

accessible, you can reset the KMA. The reset operation returns the unit to its factory defaults. This operation offers the option to scrub the server's hard disk as an extra security precaution. Disposition of the failed server is handled by the customer. Oracle service representative can repair and add a KMA server to the cluster as described in the *Oracle Key Manager 3 Installation and Service Manual*, PN E48395-xx. Once added the cluster, the database replicates, KMAs in the cluster re-synchronize, and the new KMA becomes an active member of the cluster.

Example Scenarios for Recovering Data

An OKM system's ability to recover from a disaster depends on the structure of the cluster.

OKM can span multiple geographically-separated sites to reduce the risk of a disaster destroying the entire cluster. Although unlikely that an entire cluster must be recreated, you can recover most of the key data by re-creating the OKM environment from a recent database backup.

When designing an encryption/archive strategy, you should replicate and vault critical data at a recovery site. If a site is lost, this backup data may be transferred to another operational site. Data units and keys associated with tape volumes will be known to the KMAs at the sister site, and encrypted data required to continue business operations will be available. The damaged portion of the cluster can be restored easily at the same or a different location once site operations resume.

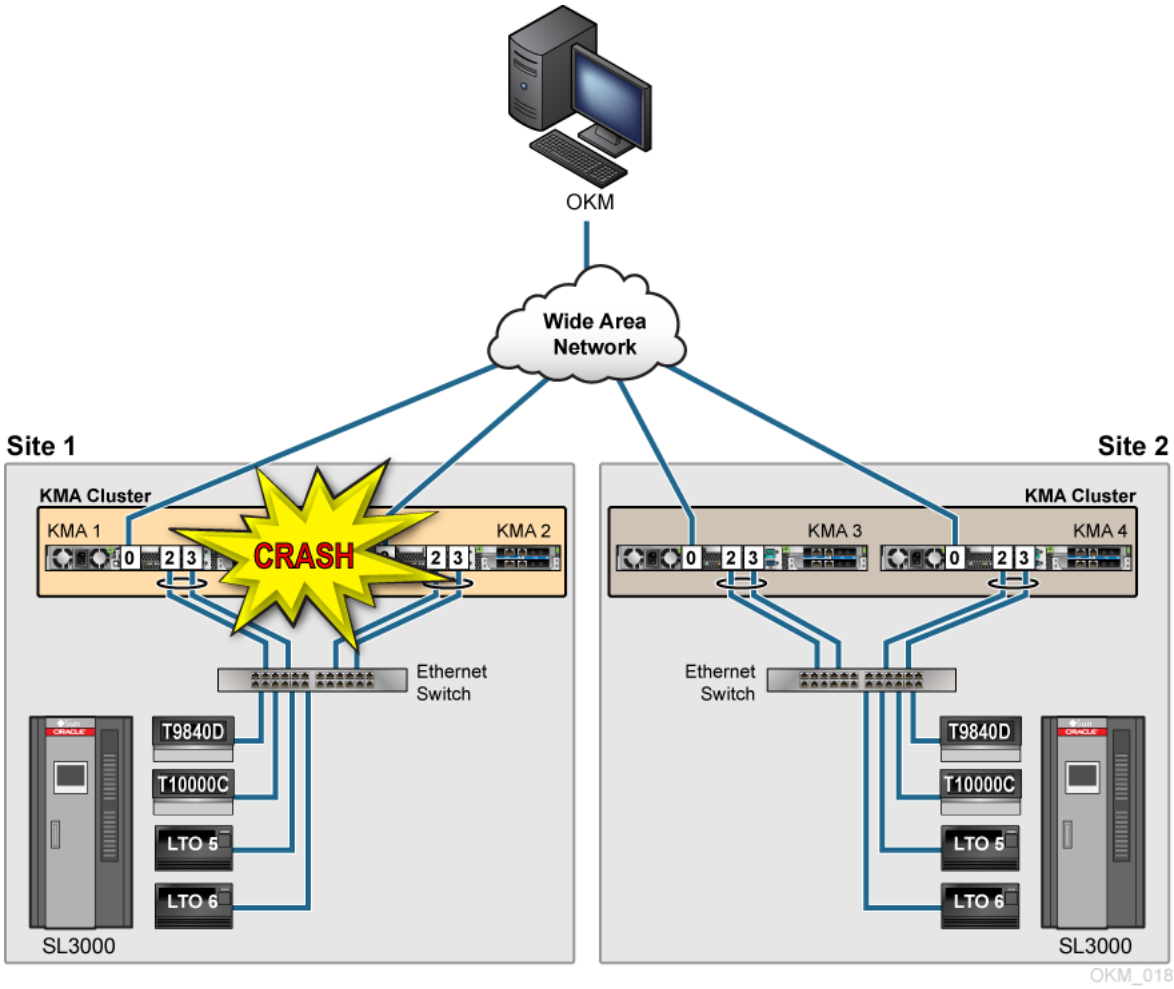
Many companies employ the services of a third-party disaster recovery (DR) site to allow them to restart their business operations as quickly as possible. Periodic unannounced DR tests demonstrate the company's degree of preparedness to recover from a disaster, natural or human-induced.

Replicate from Another Site

Two geographically separate sites (two KMAs at each site) allows recovery of a single KMA to occur with no impact to the rest of the cluster as long as one KMA always remains operational.

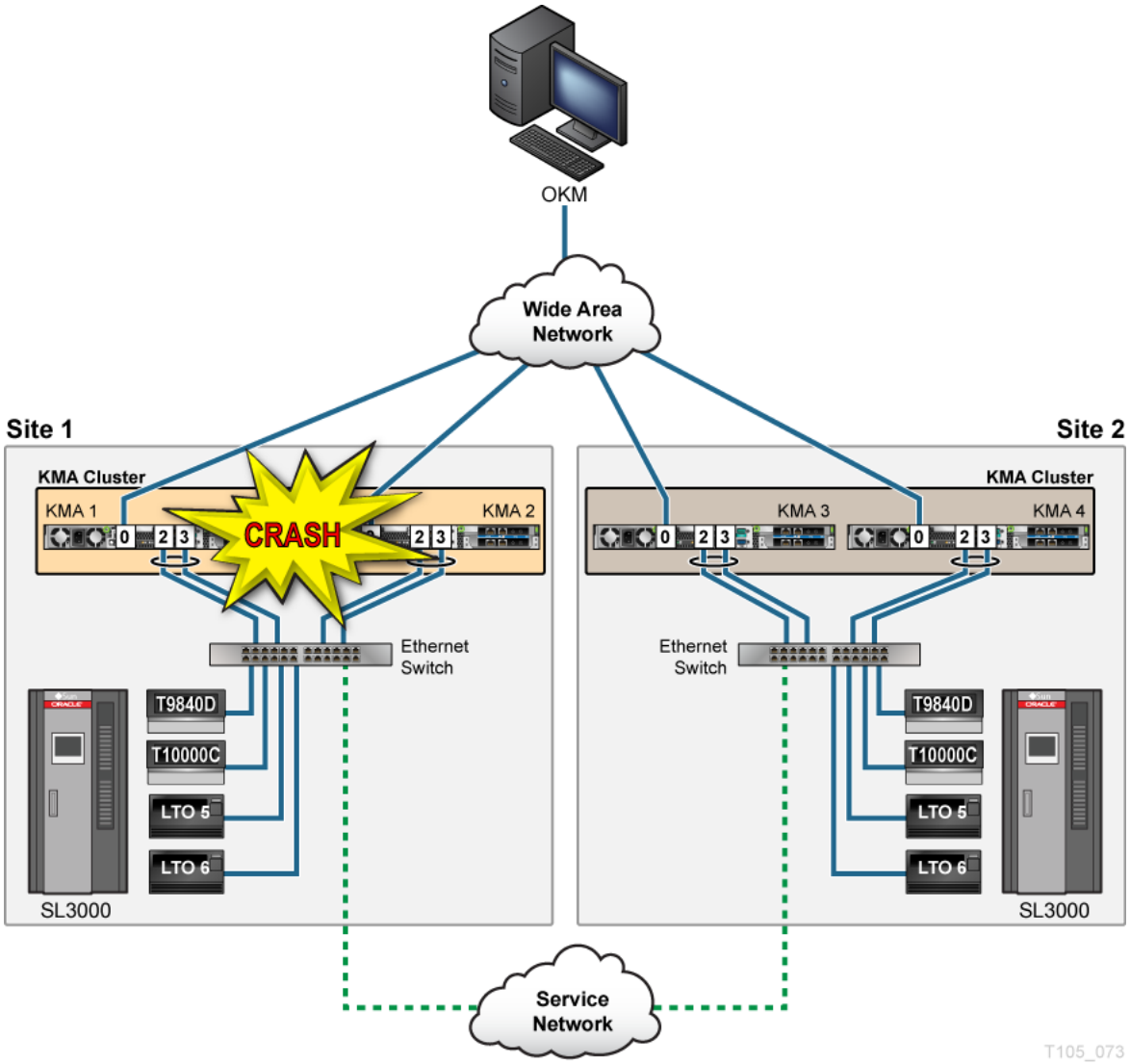
The figure below shows a disaster recover example where the time to recover business continuity to an entire site could take months. If Site 1 were destroyed, the customer must replace all the destroyed equipment to continue tape operations at Site 1. Completely restoring Site 1 would require you to install and create the new KMAs (requires a Security Officer and Quorum), join the existing cluster, and enroll the tape drives. Site 1 then self-replicates from the surviving KMAs at Site 2.

Figure A-1 Replication from Another Site—No WAN Service Network



The figure below shows an disaster recovery example where the amount of time to recover business continuity is a matter of minutes. If the KMAs at Site 1 were destroyed, and the infrastructure at Site 2 is still intact, a WAN used as the Service Network that connects the tape drives between the two sites allows the intact KMAs from Site 2 to continue tape operations between both sites. Once the KMAs are replaced at Site 1, they self-replicate from the surviving KMAs at the intact Site 2.

Figure A-2 Replication from Another Site—WAN Service Network



Dedicated Disaster Recovery Site

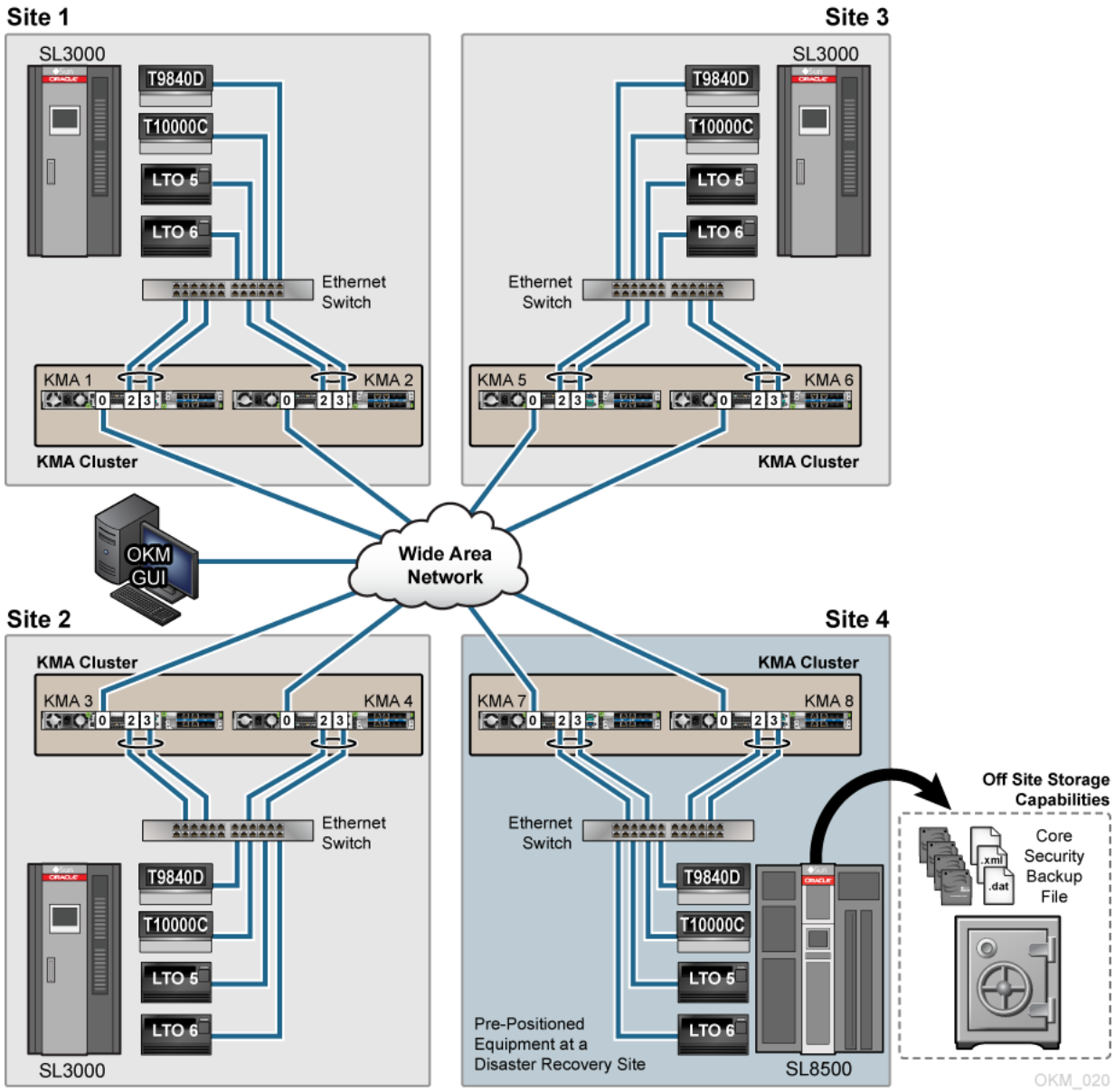
A dedicated disaster recovery site connected to the cluster using a WAN allows recovery to begin immediately in case of a disaster.

A recovery can begin once the customer enrolls the tape drives in the KMAs and joins the OKM cluster. This can be done by connecting the OKM GUI to the KMAs at the DR site. In a true disaster recovery scenario, these may be the only remaining KMAs from the customer's cluster. Drive enrollment can occur within minutes and tape production can begin after configuring the drives.

In the example below, the customer has a big environment with multiple sites. Each site uses a pair of KMAs and the infrastructure to support automated tape encryption and a single cluster where all KMAs share keys. Along with the multiple sites, this customer also maintains and uses equipment at a Disaster Recovery (DR) site that is part of the customer's OKM Cluster.

This customer uses a simple backup scheme that consists of daily incremental backups, weekly differential backups, and monthly full backups. The monthly backups are duplicated at the DR site and sent to an off-site storage facility for 90 days. After the 90-day retention period, the tapes are recycled. Because the customer owns the equipment at the DR site, this site is just an extension of the customer that strictly handles the back-up and archive processes.

Figure A-3 Pre-positioned Equipment at a Dedicated Disaster Recovery Site



Shared Resources for Disaster Recovery

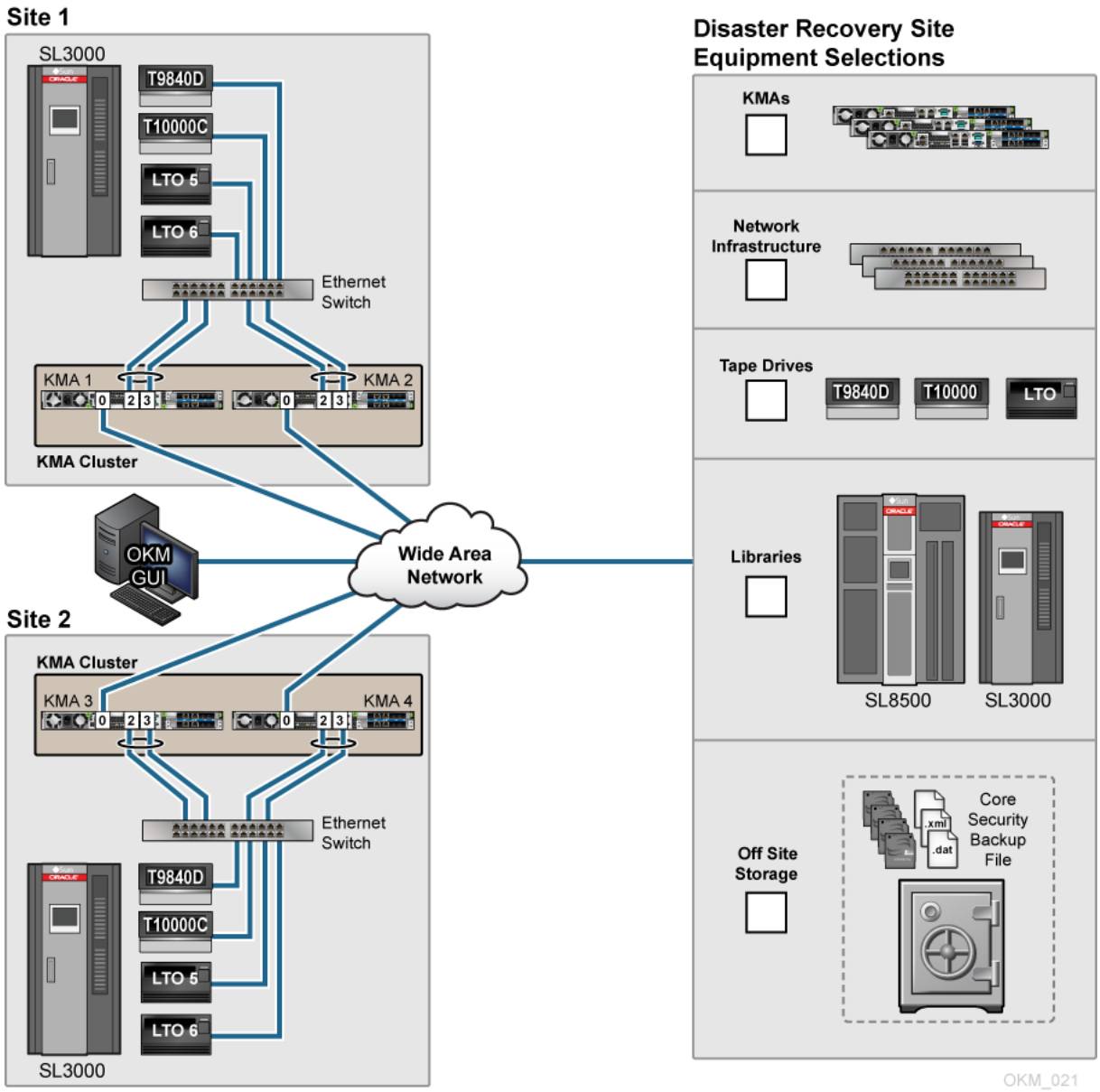
Use shared resources for backup and archive to provide a cost-efficient element for disaster recovery.

Companies that specialize in records management, data destruction, and data recovery, purchase equipment that several customers can use for backup and archive. The customer can restore backups their OKM into KMAs provided by the shared resource site. This avoids the need for a wide area network (WAN) link and the on-site dedicated KMAs, however it requires additional time to restore the database. Restore operations can take about 20 minutes per 100,000 keys.

At the DR site,

- The customer selects the appropriate equipment from the DR site inventory. The DR site configures the equipment and infrastructure accordingly.
- **IMPORTANT**: The customer must provide the DR site with the three OKM back-up files: the Core Security backup file (requires a quorum), .xml backup file, and .dat backup file.
- The customer configures an initial KMA using QuickStart, restores the KMA from the OKM backup files, activates/enables/ switches the drives to encryption-capable, and enrolls the tape drives into the DR site KMA cluster.
- Once the restore completes, the DR site needs to switch-off encryption from the agents, remove the tape drives from the cluster or reset the drives passphrase, reset the KMAs to factory default, and disconnect the infrastructure/network.

Figure A-4 Shared KMAs



Key Transfer Partners for Disaster Recovery

Key Transfer is also called Key Sharing. Transfers allow keys and associated data units to be securely exchanged between partners or independent clusters and is required if you want to exchange encrypted media.

> **Note:**
>
> A DR site may also be configured as a Key Transfer Partner.

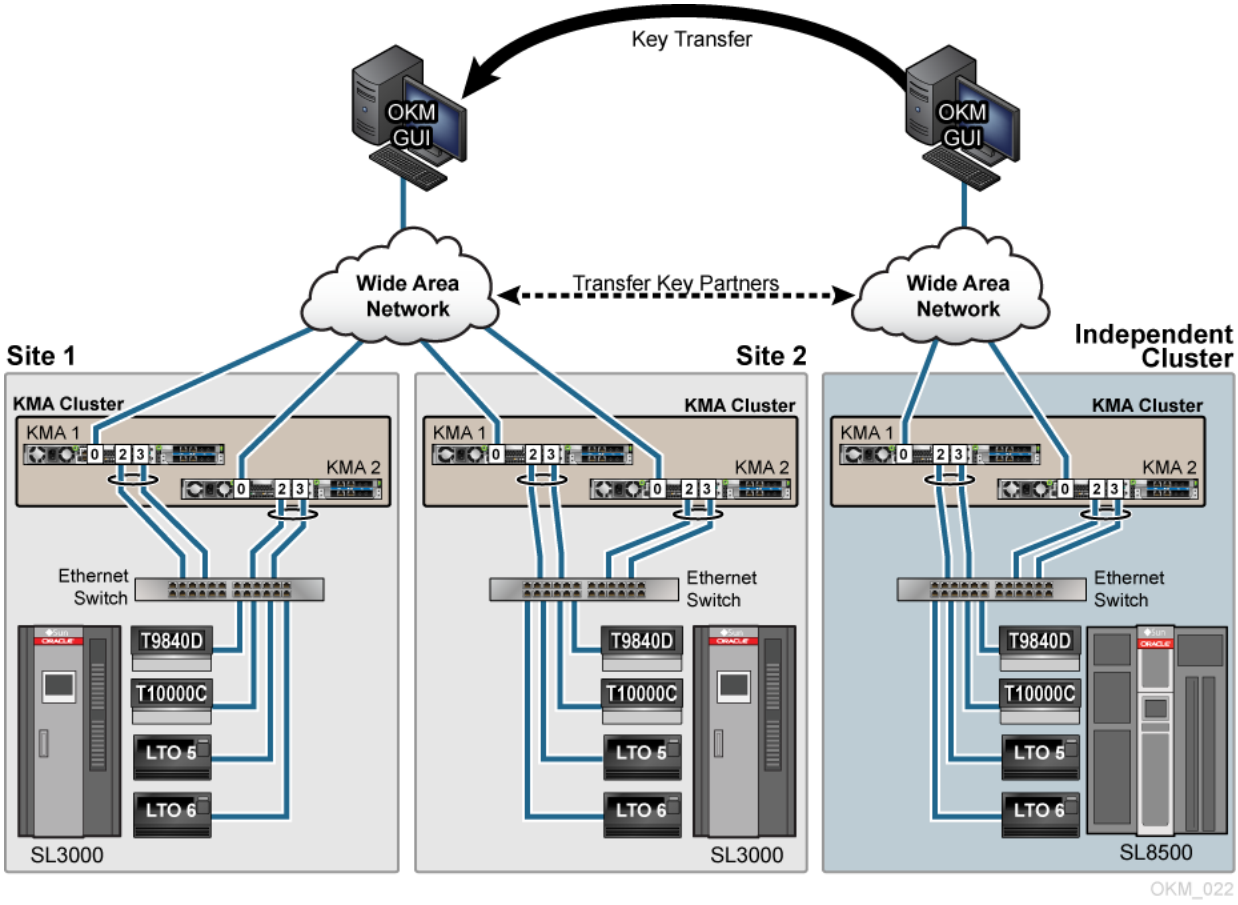
This process requires each party in the transfer to establish a public/private key pair. Once the initial configuration is complete the sending party uses Export Keys to generate a file transfer and the receiving party then uses Import Keys to receive the keys and associated data.

As a practice, it is not recommended to use Key Transfer Partners for Disaster Recovery. However, when DR sites create keys during the backup process, doing a key transfer can incrementally add the DR sites keys to the already existing data base.

The Key Transfer process requires each user to configure a Transfer Partner for each OKM Cluster: one partner *exports* keys from their cluster and the other partner *imports* keys into their cluster. When configuring Key Transfer Partners, administrators must perform tasks in a specific order that requires the security officer, compliance officer, and operator roles.

To configure Key Transfer Partners, see "Transfer Keys Between Clusters".

Figure A-5 Transfer Key Partners



B

Configure the Network for the SL4000

The SL4000 network configuration differs from that of older tape libraries such as the SL8500 and SL3000. This section provides procedures on how to configure the network with an SL4000.

The SL4000 Modular Library System has an internal tape drive network which requires only a single connection to Oracle Key Manager (OKM) rather than individual connections to each encryption-enabled tape drive.

The following devices must be on the same network subnet:

- SL4000 OKM network port
- Key Management Appliances (KMAs) that require network connectivity with the SL4000 tape drives

In the examples provided in this document, `10.80.46.89` is the SL4000 *OkmIpv4Address*.

Configure the SL4000 OKM Network Port

Use the SL4000 GUI to configure the OKM network port on the library.

1. This procedure assumes that you know how to access and use the SL4000 Configuration Wizard (refer to the *SL4000 Modular Library System Library Guide* E76470-xx as necessary).
2. Navigate to the Configure Network Settings section of the Configuration Wizard of the SL4000, and specifically to the screen titled Network Port: OKM (Oracle Key Manager) Network Port.
3. Select in the Protocol field.
4. Enter the IPv4 Address (`10.80.46.89`).
5. Enter the IPv4 Netmask (`255.255.254.0`).
6. Enter the IPv4 Gateway (`10.80.47.254`).
7. The SL4000 library will need to restart.

Configure the KMA to Connect with the SL4000

Setup network routing on the KMAs that reside in the same subnet as the SL4000 OKM network port.

Provide a route between the internal SL4000 drive network and either the Service or Management Network of the OKM appliances. Best practice is to have encrypting tape drives isolated on the service network.

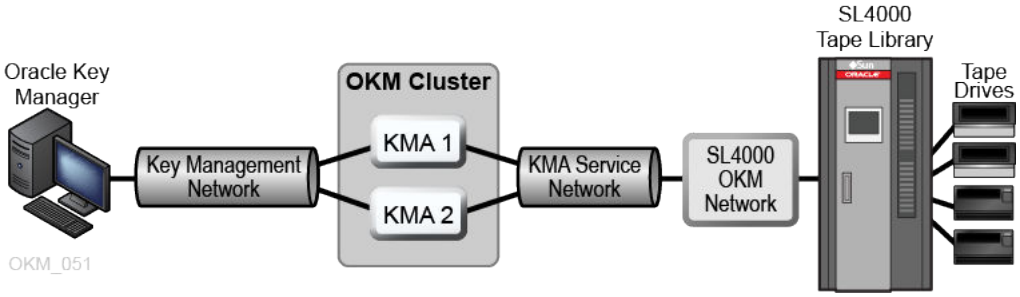
- All SL4000 library base units are assigned an internal drive IP subnet of `192.168.1.0`.
- Drive Expansion Modules (DEMs) are assigned an IP address with a different third octet based upon whether the module is installed to the left or right of the base module.

> **Note:**
>
> You can either add the specific routes to the base drive module, or if you have multiple DEMs adding a route of `192.168.0.0` will enable access to all drives in the base and DEMs.

Refer to the SL4000 documentation for specifics about subnet values.

Familiarity with OKM network topology is very helpful. For example, there may be KMAs at a remote site that may or may not have service network routes between them depending upon customer tape drive failover requirements. The following figure shows a representation of an OKM Cluster and an SL4000 library. There is a Key Management Network between the workstation and the OKM Cluster. The KMA Service network from the cluster connects to the SL4000 OKM Network.

Figure B-1 OKM Connected with an SL4000 Tape Library



1. Identify the KMAs in the same subnet as the SL4000 that need to access the SL4000 internal drive network. Perform the following on only KMAs that reside on that subnet, not all KMAs in the cluster.
2. Log in to the OKM console with the Security Officer role, and open the configuration menu.
3. Enter **5** at the prompt to `Modify Gateway Settings`.

4. Select option **1** `Add a gateway`.
5. Select option **2** `Service` to select the network.
6. Select option **2** `Network` to select the route type.
7. Enter the network values:

   Enter `10.80.46.89` for the Gateway IP Address.
   Enter `192.168.0.0` for the Destination IP Address.
   Enter `255.255.0.0` for the Route Subnet Mask.

   The Gateway IP Address is the IP Address assigned to the SL4000 OKM Network port.
8. Enter **y** to commit the changes.
9. Select option **3** `Exit gateway configuration`.

Repeat this procedure as necessary for any OKM appliance that needs Service Network access to the SL4000 internal drive network.

Enable SL4000 Drive Access Using MDVOP

Use MDVOP to enable OKM access on the drives.

The examples in this section use the SL4000 *OkmIpv4Address* and the 192.168.0.0 address to enable access to all drives in the Base and DEMs.

Windows:

1. Display the current routes

   ```
   route print
   ```
2. Add the route for all modules containing drives in the SL4000 (Base plus the DEMs) in the form:

   route add -p 192.168.0.0 mask 255.255.0.0 *OkmIpv4Address*

   Example:

   ```
   route add -p 192.168.0.0 mask 255.255.0.0 10.80.46.89
   ```
3. Check that the route was added.

   ```
   route print
   ```

Solaris:

1. Display the current routes.

   ```
   netstat -rn
   ```
2. Add the route for all modules containing drives in the SL4000 (Base plus the DEMs) in the form:

   route add 192.168.0.0 *OkmIpv4Address*

   Example:

   ```
   route add 192.168.0.0 10.80.46.89
   ```
3. Check that the route was added.

   ```
   netstat -rn
   ```

Linux:

1. Display the current routes.

   ```
   netstat -rn
   ```

2. Add the route for all modules containing drives in the SL4000 (Base plus the DEMs) in the form:

   route add -net 192.168.0.0 netmask 255.255.0.0 gw *OkmIpv4Address* dev eth1

   Example:

   ```
   route add -net 192.168.0.0 netmask 255.255.0.0 gw 10.80.46.89 dev eth1
   ```

3. Check that the route was added.

   ```
   netstat -rn
   ```

C

OKM-ICSF Integration

The IBM Integrated Cryptography Service Facility (ICSF) is an encryption solution where the external key store resides in an IBM mainframe and is accessed using a TLS/XML protocol.

Key Stores and Master Key Mode

When Master Key Mode is enabled, agents derive keys from a set of externally stored master keys.

In KMS 2.0.x and later, the KMAs in an cluster generate their own keys using either a Hardware Security Module (such as the Sun Cryptographic Accelerator 6000 card) or the Solaris Cryptographic Framework. Some customers prefer to have the KMAs use master keys that are created and stored in an external key store.

KMS 2.2 introduced a Master Key Mode feature. When enabled, the cluster derives tape keys from a set of master keys. The master keys are created and stored in an external key store. Full disaster recovery is possible with just the tapes, the master keys, and factory default OKM equipment.

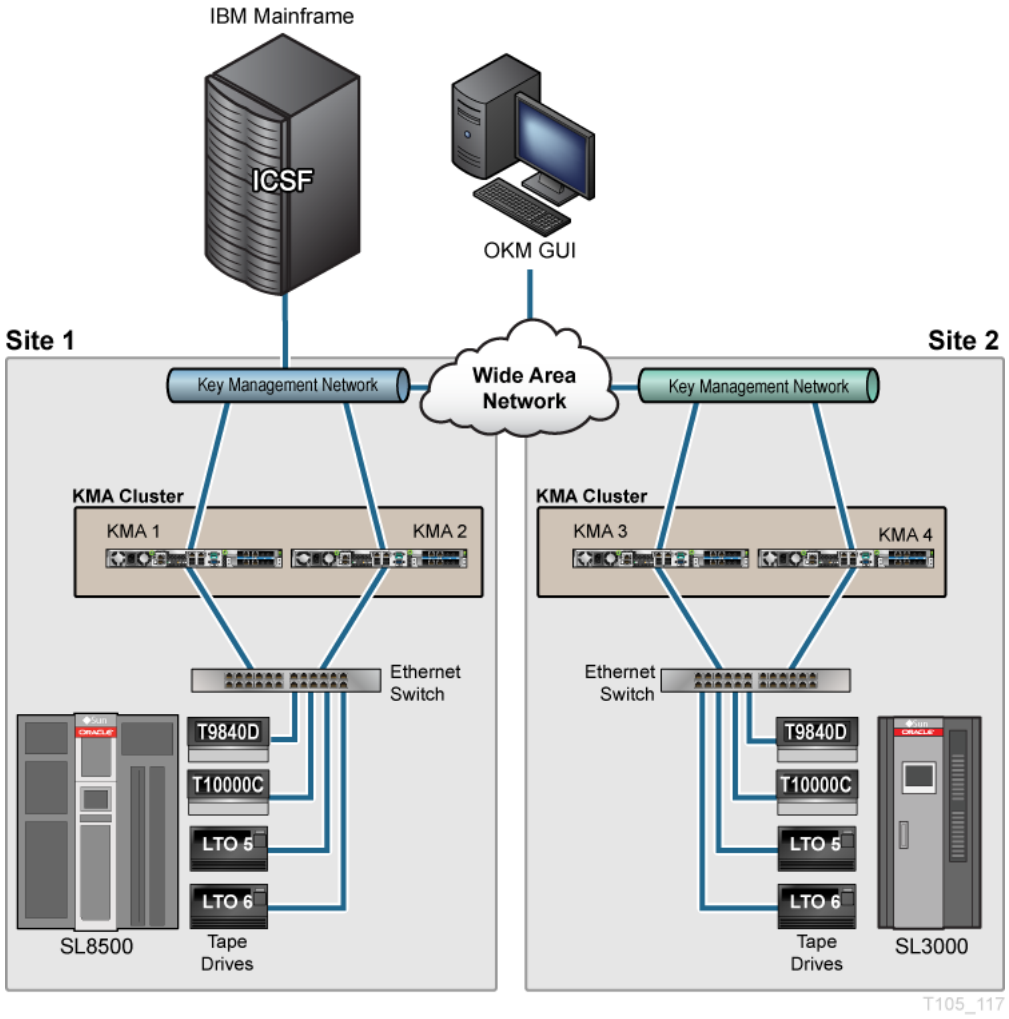
> **Note:**
>
> The original product name, Key Management System (KMS), changed to Oracle Key Manager (OKM) at release 2.3.

Understanding the ICSF Solution

In the ICSF solution and external key store (IBM mainframe) connects to OKM over a WAN.

In this solution, the external key store resides in an IBM mainframe and is accessed using a TLS/XML protocol. This protocol is supported in the IBM mainframe with the keys stored in a Token Data Set in the IBM Integrated Cryptography Service Facility (ICSF). The figure below shows a typical configuration.

Figure C-1 Site Configurations

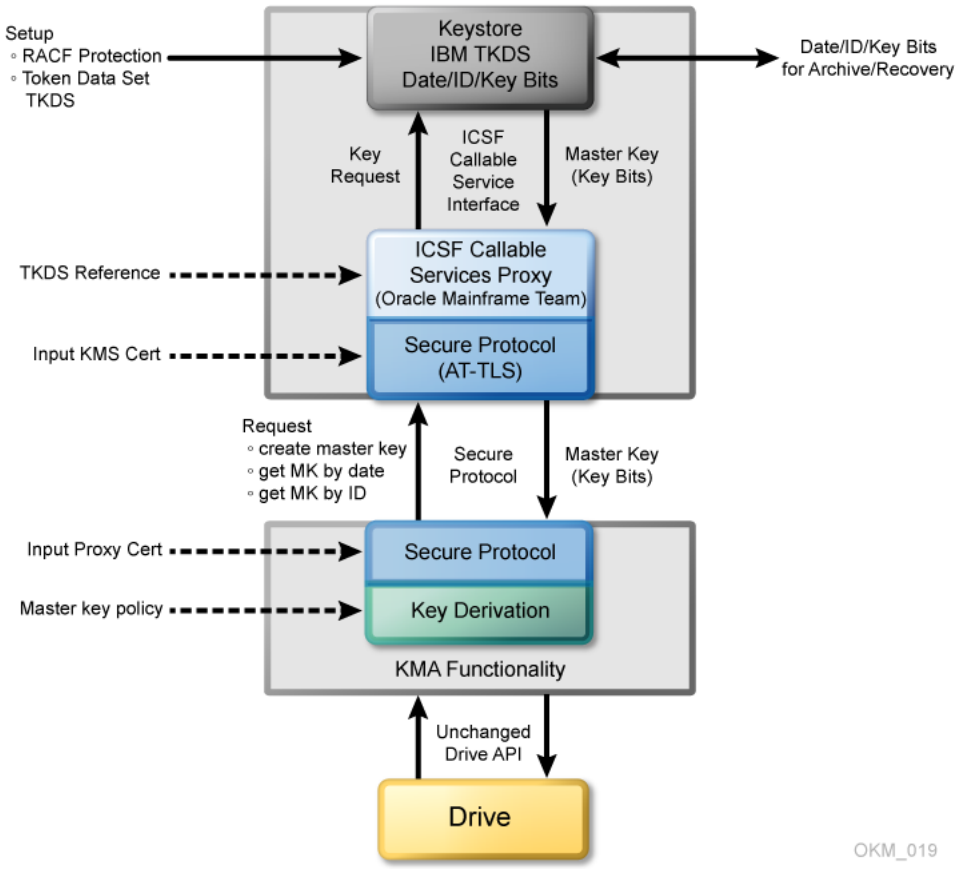


The OKM Cluster periodically issues requests to the IBM mainframe, asking to create new master keys (referred to as application keys in ICSF) and to return them to the OKM Cluster. The KMAs then use these new master keys to derive new tape keys.

Defining the ICSF System Components

The ICSF system components include the keystore, interface, transfer security, key derivation, key policy, and key recovery.

Figure C-2 ICSF Components



KeyStore

Master (application) keys are stored in the Token Data Set (TKDS), as defined in the IBM ICSF documentation. The TKDS is identified in the ICSF installation options data set. The z/OS system programmer can create the TKDS by using the IDCAMS utility.

Keys stored in the TKDS are not encrypted, but access to the data set itself, as well as Callable Services and Tokens (key sets), is controlled by RACF or an equivalent. Access to the TKDS can be defined by the current policy for backup and restore of Master Keys.

Interface

The StorageTek ELS software implements an ICSF Callable Services Proxy. This Proxy allows the OKM Cluster to call PKCS#11 functions to access the KeyStore. Secure communication with the OKM Cluster is implemented using the z/OS Application Transparent - Transport Layer Security (AT-TLS) on the IBM mainframe.

AT-TLS is an encryption solution for TCP/IP applications that is completely transparent to the application client and server. Packet encryption and decryption occur in the z/OS TCPIP address space at the TCP protocol level. The encrypted packet payload is unintelligible when sniffed or traced, but by the time it is delivered to the application the payload is once again readable.

Transfer Security

The OKM Cluster implements a Transport Layer Security (TLS) protocol to communicate with the Proxy on the IBM mainframe.

The z/OS system programmer generates and then exports two self-signed X.509v3 certificates and one RSA 2048-bit public key pair, and then transfers them (using FTP) off the IBM mainframe. The first certificate is a Root Certificate Authority (CA) certificate. The system programmer uses this Root CA certificate to generate the Client Certificate and Key Pair. These certificates and the key pair are manually installed in the IBM mainframe and configured using RACF and AT-TLS so that the Proxy can identify a valid OKM request. The certificates and the private key of the key pair are installed in the OKM Cluster so that it can authenticate the Proxy. As a result, only KMAs in a valid OKM Cluster can issue requests to the Proxy, and they accept a response only from a valid Proxy.

Key Derivation

The OKM Cluster accepts a Master Key Value and 18-byte Master Key ID from the Proxy. It creates a 30-byte Key ID by concatenating a 2-byte header and the 18-byte Master Key ID with an internally generated 10-byte value. It then creates a Derived Key Value by encrypting the Key ID (padded to 32 bytes) with the Master Key Value.

Key management between Drives and the OKM Cluster continue to use the current OKM strategy. Thus, no firmware upgrades are required.

Key Policy

The OKM Cluster controls the Master Key lifecycle. It requests a current Master Key value from the Proxy based on the current date. The Proxy retrieves the current Master Key from the TKDS using a sequence of PKCS#11 function calls. If there is no current Master Key Value, the OKM Cluster issues a Create Master Key request to the Proxy. The OKM can then re-submit the request for a current Master Key Value from the Proxy.

Key Recovery

The OKM Cluster retains all derived Keys and Key IDs it creates. If the Cluster does not have the Key for a specified set of written data, it can re-derive the Key by forming the Master Key ID from the Key ID and then issuing a retrieve request to the Proxy to get the Master Key Value stored in the TKDS. The OKM can then re-derive the Key Value to enable its Agent to read the data.

This key recovery mechanism allows "ground-level up" recovery of all tapes encrypted by this system, based only on availability of archived Master Keys in the TKDS.

System Requirements for ICSF

ICSF requires the IBM mainframe and OKM cluster to be at a minimum level.

IBM Mainframe

The IBM z/OS mainframe must be running ICSF HCR-7740 or *later* and StorageTek ELS 7.0 along with associated PTFs or *later*. A CEX2C cryptographic card must be installed on the IBM mainframe.

OKM Cluster

The OKM Cluster must be running KMS 2.2 or higher and must be using Replication Version 11 or *later*. The FIPS Mode Only security parameter should be set to *off*.

IBM Mainframe Configuration for ICSF

Various steps are required to configure a z/OS system to be used as an external key store for a OKM Cluster.

- Install and Configure the CEX2C Cryptographic Card for ICSF
- StorageTek ELS Setup for OKM-ICSF
- Preparing ICSF
- Configuring AT-TLS

Install and Configure the CEX2C Cryptographic Card for ICSF

Refer to documentation that accompanies this card.

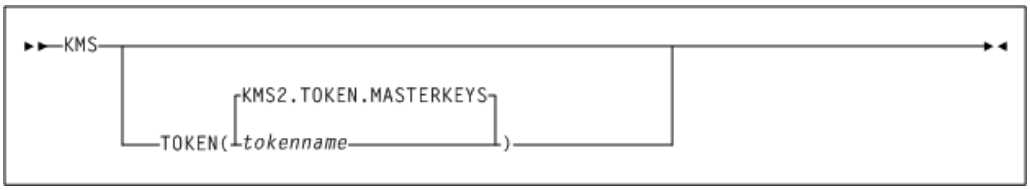
StorageTek ELS Setup for OKM-ICSF

This section describes the ELS command for to setup OKM-ICSF.

For ELS 7.0, the OKM-ICSF function is provided through ELS PTF L1H150P that can be downloaded from:

`http://www.oracle.com/technetwork/indexes/downloads/index.html`

The OKM-ICSF function is in the base code for *subsequent releases*. The OKM-ICSF proxy is an SMC HTTP server CGI routine. The SMC HTTP server must be active on a system with the ICSF PKCS11 function active. The KMS command is valid from the SMCPARMS data set only.



KMS
The command name.

TOKEN
tokenname
Specifies the PKCS11 token name for the OKM-ICSF interface. The first character of the name must be alphabetic or a national character (#, $, or @). Each of the remaining characters can be alphanumeric, a national character, or a period (.). The maximum length is 32 characters.

KMS2.TOKEN.MASTERKEYS
Specifies the default PKCS11 token name.

Preparing ICSF

Verify the system is ready to activate ICSF.

The following items activate the ICSF PKCS#11 function:

- Ensure that ICSF is at HCR7740 or higher.
- Define the Token Data Set (TKDS) in MVS. The TKDS is the repository for the keys used by PKCS#11. The TKDS is a key-sequenced VSAM data set. Keys within the Token Data Set are not encrypted. Therefore, it is important that the security administrator create a RACF profile to protect the Token Data Set from unauthorized access.
- The ICSF installation options data set contains two options related to the Token Data Set:
  - TKDSN(datasetname)

    Identifies the VSAM data set that contains the token data set. It must be specified for ICSF to provide PKCS#11 services.
  - SYSPLEXTKDS(YES|NO,FAIL(YES|NO)

    Specifies whether the token data set should have sysplex-wide data consistency.

See the *IBM z/OS Cryptographic Services ICSF System Programmer's Guide* (SA22-7520) for additional information on ICSF initialization.

ICSF uses profiles in the SAF CRYPTOZ class to control access to PKCS#11 tokens. The user ID of the HTTP Server started task must have the following SAF access level for the defined PKCS#11 token:

- SO.token_name CONTROL
- USER.token_name UPDATE

Configuring AT-TLS

AT-TLS is an encryption solution for TCP/IP applications that is completely transparent to the application server and client. Packet encryption and decryption occurs in the z/OS TCPIP address space at the TCP protocol level.

The document *Using AT-TLS with HSC/SMC Client/Server z/OS Solution, Implementation Example* (http://docs.oracle.com/cd/E21457_01/en/E27193_01/E27193_01.pdf) shows examples for configuring AT-TLS on the IBM mainframe.

To implement AT-TLS encryption for the OKM to NCS/ELS HTTP server connection, the minimum level needed for the Communication Server is z/OS 1.9. The following available IBM PTFs (for APAR PK69048) should be applied for best performance:

- Release 1A0: UK39417 available 08/10/07 z/OS 1.10
- Release 190: UK39419 available 08/10/07 z/OS 1.9

See the following IBM publications for detailed information about the IBM z/OS Communications Server Policy Agent configuration and RACF definitions for AT-TLS:

- *IP Configuration Guide*, SC31-8775
- *IP Configuration Reference*, SC31-8776
- *Security Server RACF Security Administrator's Guide*, SA22-7683
- *Security Server RACF Command Language Reference*, SA22-7687
- *IBM Redbook Communications Server for z/OS V1R7 TCP/IP Implementation*, Volume 4, *Policy-Based Network Security*, SG24-7172

TCPIP OBEY Parameter

Specify this parameter in the TCPIP profile data set to activate the AT-TLS function.

```
TCPCONFIG TTLS
```

This statement may be placed in the TCP OBEY file.

Policy Agent (PAGENT) Configuration

The Policy Agent address space controls which TCP/IP traffic is encrypted. This section provides a sample PAGENT configuration.

PAGENT JCL
PAGENT started task JCL:

```
//PAGENT PROC
//*
//PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
// PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/-d1'
//*
//STDENV DD DSN=pagentdataset,DISP=SHR//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
//*
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

The pagentdataset data set contains the PAGENT environment variables.

PAGENT Environment Variables
This is a sample PAGENT environment variable file:

```
LIBPATH=/lib:/usr/lib:/usr/lpp/ldapclient/lib:.
PAGENT_CONFIG_FILE=/etc/pagent.conf
PAGENT_LOG_FILE=/tmp/pagent.log
PAGENT_LOG_FILE_CONTROL=3000,2
_BPXK_SETIBMOPT_TRANSPORT=TCPIP
TZ=MST7MDT
```

/etc/pagent.conf contains the PAGENT configuration parameters.

PAGENT Configuration
This is a sample PAGENT configuration:

```
TTLSRule           KMS-TO-ZOS
{
   LocalAddr       localtcpipaddress
   RemoteAddr      remotetcpipaddress
   LocalPortRange  localportrange
```

```
   RemotePortRange remoteportrange
   Jobname         HTTPserverJobname
   Direction       Inbound
   Priority        255
   TTLSGroupActionRef gAct1~KMS_ICSF
   TTLSEnvironmentActionRefeAct1~KMS_ICSF
   TTLSConnectionActionRef cAct1~KMS_ICSF
}
TTLSGroupAction    gAct1~KMS_ICSF
{
   TTLSEnabled     On
   Trace           2
}
TTLSEnvironmentAction eAct1~KMS_ICSF
{
   HandshakeRole Server
   EnvironmentUserInstance 0
   TTLSKeyringParmsRef keyR~ZOS
}
TTLSConnectionAction cAct1~KMS_ICSF
{
   HandshakeRole  ServerWithClientAuth
   TTLSCipherParmsRef cipher1~AT-TLS__Gold
   TTLSConnectionAdvancedParmsRefcAdv1~KMS_ICSF
   CtraceClearText Off
   Trace           2
}
TTLSConnectionAdvancedParmscAdv1~KMS_ICSF
{
   ApplicationControlled Off
   HandshakeTimeout      10
   ResetCipherTimer      0
   CertificateLabel      certificatelabel
   SecondaryMap          Off
}
TTLSKeyringParms  keyR~ZOS
{
   Keyring        keyringname
}
TTLSCipherParms   cipher1~AT-TLS__Gold
{
   V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
   V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA
}
```

where:
localtcpipaddress — local TCP/IP address (address of HTTP server)
remotetcpipaddress— remote TCP/IP address (address of OKM client) can be ALL for all TCP/IP addresses
localportrange — local port of HTTP server (specified in the HTTP or SMC startup)
remoteportrange — remote port range (1024-65535 for all ephemeral ports)
HTTPserverJobname — jobname of the HTTP Server
certificatelabel — label from certificate definition
keyringname — name from RACF keyring definition

RACF Definitions
Activate the following RACF classes. Either the RACF panels or the CLI may be used.

- DIGTCERT

- DIGTNMAP
- DIGTRING

The SERVAUTH class must use RACLIST processing to prevent PORTMAP and RXSERV from abending TTLS. See RACF Commands below.

RACF Commands
The RACF commands to achieve the above:

- SETROPTS RACLIST(SERVAUTH)
- RDEFINE SERVAUTH ** UACC(ALTER) OWNER (RACFADM)
- RDEFINE STARTED PAGENT*.* OWNER(RACFADM) STDATA(USER(TCPIP) GROUP(STCGROUP)
- RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE) OWNER(RACFADM)
- RDEFINE FACLITY IRR.DIGTCERT.LIST UACC(NONE) OWNER(RACFADM)
- RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE) OWNER (RACFADM)

RACF Certificate Creation Commands
The IBM Communications Server for z/OS V1R10 TCP/IP Implementation Volume 4: Security and Policy-Based Networking document outlines the procedure required to create and export digital certificates on the z/OS system.
The RACDCERT utility creates and manages digital certificates within RACF. Verify that RACDCERT is in the AUTHCMD section of the IKJTSOxx member in SYS1.PARMLIB.
The following RACF commands to create Keyrings and certificates for use by the AT-TLS function:
RACDCERT ID(*stcuser*) **ADDRING**(*keyringname*)
where:

- *stcuser* — RACF user ID associated with the SMC started task
- *keyringname* — Name of keyring, must match the Keyring specified in the PAGENT configuration

RACDCERT GENCERT CERTAUTH SUBJECTSDN(CN('*serverdomainname*') **O**('*companyname*') **OU**('*unitname*') **C**('*country*')) **WITHLABEL**('*calabel*') **TRUSTSIZE(1024) KEYUSAGE(HANDSHAKE,DATAENCRYPT,CERTSIGN)**
where:

- *serverdomainname* — Domain name of the z/OS server (for example, mvsa.company.com)
- *companyname* — Organization name
- *unitname* — Organizational unit name
- *country* — Country
- *calabel* — Label for certificate authority (for example, CAKMSSERVER). This is the CA certificate for the OKM system.

RACDCERT ID(*stcuser*) **GENCERT SUBJECTSDN(CN**('*serverdomainname*') **O**('*companyname*') **OU**('*unitname*') C('*country*')) **WITHLABEL**('*serverlabel*') **TRUST SIZE(1024) SIGNWITH(CERTAUTH LABEL**('*calabel*'))
where:

- *stcuser* — RACF user ID associated with the SMC started task
- *serverdomainname* — Domain name of the z/OS server (for example, MVSA.COMPANY.COM)
- *companyname* — Organization name
- *unitname* — Organizational unit name
- *country* — Country
- *serverlabel* — Label for the server certificate (for example, KMSSERVER)
- *calabel* — Label for certificate authority, specified in the CA certificate definition. This is the SERVER certificate

RACDCERT ID(*stcuser)* **GENCERT SUBJECTSDN(CN(**'*clientdomainname*') **O**('*companyname*') **OU**('*unitname*') **C**('*country*')) **WITHLABEL**('*clientlabel*') **TRUST SIZE**(1024) **SIGNWITH(CERTAUTH LABEL**('*calabel*'))
where:

- *stcuser* — RACF user ID associated with the SMC started task
- *serverdomainname* — Domain name of the z/OS server (for example, MVSA.COMPANY.COM)
- *companyname* — Organization name
- *unitname* — Organizational unit name
- *country* — Country
- *clientlabel* — Label for the client certificate (for example, KMSCLIENT)
- *calabel* — Label for certificate authority, specified in the CA certificate definition. This is the CLIENT certificate.

The following commands connect the CA, SERVER and CLIENT certificates to the keyring specified in the PAGENT configuration:
RACDCERT ID(*stcuser*) **CONNECT**(**CERTAUTH LABEL**('*calabel*') **RING**('*keyringname*') **USAGE(CERTAUTH)**)
where:

- *stcuser* — RACF user ID associated with the SMC started task.
- *calabel* — Label for certificate authority, specified in the CA certificate definition
- *keyringname* — Name of keyring, must match the Keyring specified in the PAGENT configuration

RACDCERT ID(*stcuser*) **CONNECT(ID**(*stcuser*) **LABEL**('*serverlabel*') **RING**('*keyringname*') **DEFAULT USEAGE(PERSONAL)**
where:

- *stcuser* — RACF user ID associated with the SMC started task
- *serverlabel* — Label for server certificate
- *keyringname* — Name of keyring, must match the Keyring specified in the PAGENT configuration

RACDCERT ID(*stcuser*) **CONNECT(ID**(*stcuser*) **LABEL**('*clientlabel*') **RING**('*keyringname*') **USEAGE(PERSONAL)**
where:

- *stcuser* — RACF user ID associated with the SMC started task

- *clientlabel* — Label for client certificate
- *keyringname* — Name of keyring, must match the Keyring specified in the PAGENT configuration

The following commands export the CA and client certificates for transmission to the OKM:
RACDCERT EXPORT (LABEL('*calabel*')) **CERTAUTH DSN**('*datasetname*') **FORMAT(CERTB64)**
where:

- *calabel* — Label for certificate authority, specified in the CA certificate definition
- *datasetname* — Data set to receive the exported certificate

RACDCERT EXPORT (LABEL('*clientlabel*')) **ID**(*stcuser*) **DSN**('*datasetname*') **FORMAT(PKCS12DER) PASSWORD**('*password*')
where:

- *clientlabel* — Label for the client certificate
- *stcuser* — RACF user ID associated with the SMC started task
- *datasetname* — Data set to receive the exported certificate
- *password* — Password for data encryption. Needed when the certificate is received on the OKM. The password must 8 characters or more.

The export data sets are now transmitted to the OKM, and FTP can be used. The CA certificate is transmitted with an EBCDIC to ASCII conversion. The CLIENT certificate is transmitted as a BINARY file and contains both the client certificate and its private key.

RACF List Commands
The following RACF commands list the status of the various RACF objects:

- RLIST STARTED PAGENT.* STDATA ALL
- RLIST DIGTRING * ALL
- RLIST FACILITY IRR.DIGTCERT.LISTRING ALL
- RLIST FACILITY IRR.DIGCERT.LST ALL
- RLIST FACILITY IRR.DIGCERT.GENCERT ALL
- RACDCERT ID(stcuser) LIST
- RACDCERT ID(stcuser) LISTRING(keyringname)
- RACDCERT CERTAUTH LIST

Update OKM Cluster Information

After configuring the IBM mainframe, the z/OS systems programmer must provide information to the administrator of the OKM Cluster.

The administrator of the OKM Cluster enters the following information as the Master Key Provider settings in the Security Parameters panel of the OKM GUI.

- Host name or IP address of the mainframe
- Port number (such as 9889)
- Web application path (such as "/cgi/smcgcsf")

- File containing the client "user certificate" (exported and transferred off of the mainframe)
- File containing the client private key (exported and transferred off of the mainframe)
- Password that was used when the client private key was created
- File containing the Root CA certificate (exported and transferred off of the mainframe)

The client "user certificate" and the client private key might appear in the same file when they are exported from the IBM mainframe. If so, then the administrator should specify the same file in the OKM Certificate File Name and OKM Private Key File Name fields in the Master Key Provider settings.

The fields and their descriptions are given below:

Master Key Mode
Select "Off," "All Keys," or "Recover Keys Only." A value of "Off" means that the KMAs in this OKM Cluster create their own keys and do not derive keys from a Master Key Provider. A value of "All Keys" means that the KMAs in this OKM Cluster contact the Master Key Provider defined in the settings on this screen in order to create and retrieve master keys, and then use these master keys to derive keys for Agents. A value of "Recover Keys Only" means that the KMAs in this OKM Cluster contact the Master Key Provider defined in the settings on this screen to retrieve (but not create) master keys and then use these master keys to derive keys for Agents. The "All Keys" and "Recover Keys Only" values can be set only if the Replication Version is at least 11.

Master Key Rekey Period
Type the amount of time that defines how often this KMA should contact the Master Key Provider to create and retrieve new master keys. The default is 1 day. The minimum value is 1 day; maximum value is 25,185 days (approximately 69 years).

Master Key Provider Network Address
Type the host name or IP address of the host where the Master Key Provider resides.

Master Key Provider Port Number
Type the port number on which the Master Key Provider listens for requests from the KMAs in this OKM Cluster.

Master Key Provider Web App Path
Type the web application path that forms part of the URL for contacting the Master Key Provider (for example, "/cgi/smcgcsf").

OKM Certificate File Name
Specify the name of the file that contains the OKM certificate that was exported from the Master Key Provider host. The Master Key Provider uses this certificate to verify requests from KMAs in this OKM Cluster.

OKM Private Key File Name
Specify the name of the file that contains the OKM private key that was exported from the Master Key Provider host. The Master Key Provider uses this private key to verify requests from KMAs in this OKM Cluster.

OKM Private Key Password
Type the OKM private key password as it was generated on the Master Key Provider host. The Master Key Provider uses this private key password to verify requests from KMAs in this OKM Cluster.

CA Certificate File Name
Specify the name of the file that contains the CA (Certificate Authority) certificate that was exported from.

D
Switch Configurations

Use these procedures to configure the Brocade, Extreme, and 3COM switches.

- Brocade ICX 6430 Switch Configuration
- Extreme Network Switch Configuration
- 3COM Network Switch Configuration

Brocade ICX 6430 Switch Configuration

Use the Brocade documentation to properly install the switch. See the *Brocade ICX 6430 and ICX 6450 Stackable Switches Hardware Installation Guide*.

Pre-configuration Requirements

Before you configure the switch, follow steps 1 - 4 in the Brocade *ICX 6430 and ICX 6450 Web Management Interface User Guide* and the section on Prerequisite Configuration to attach a PC to the switch and assign an IP address to the management port using its Command Line Interface (CLI). Follow the ICX 6430 instructions in step 3.

Configuring the Brocade Switch

Configure the Brocade switch to use the Rapid Spanning Tree Protocol (RSTP), which was standardized by IEEE 802.1W.

After you perform the following steps, refer to the *Brocade ICX 6430 and ICX 6450 Web Configuration QuickStart Guide* for additional information about configuring Brocade ICX 6430 switches.

1. Start a web browser and connect to the switch at the IP address you established in the pre-configuration requirements above.

   Enable (RSTP) as shown in the following steps.
2. Navigate to `Configuration > System`.
   a. Ensure that Spanning Tree is enabled.
   b. Click `Clock` to set the system clock.
3. Navigate to `Configuration > VLAN`.
   a. Set the VLAN IP address.
   b. Click `Add Port VLAN`.
   c. Ensure that Spanning Tree is Disabled and 802.1W is Enabled.
4. Navigate to `Configuration > RSTP` and view the Ethernet ports.
5. Use ssh to access the management IP address of the switch to launch its CLI. Configure a trunk group for each KMA that should include aggregated service ports.

```
Brocade(config)#show trunk

Brocade(config)#trunk ethernet

Brocade(config)#trunk ethernet 1/1/1 to 1/1/2

Brocade(config)#trunk ethernet 1/1/3 to 1/1/4

< etc. for each KMA that should include aggregated service ports, port
IDs as shown in step 4 >

Brocade(config)#write memory

Brocade(config)#trunk deploy
```

> **Note:**
>
> In this example, the ports had been put into VLAN 1, as indicated by the leading "1/" in the trunk commands. If no VLAN was created on the ports, then the trunk commands should not have the leading "1/". For example:
>
> ```
> Brocade(config)#trunk ethernet 1/1 to 1/2
> ```

6. In the web interface, navigate to `Configuration > Trunk` and view the trunks that you just defined in the CLI.
7. Attach network cables between the pairs of ports on the switch to the service and aggregated service ports on each KMA that should contain aggregated service ports. Port IDs (shown in step 6) are associated with physical ports on the switch.

   To do this:

   a. Inspect the switch and identify the physical ports that are associated with the trunk groups that you created in step 5 and viewed in step 6.
   b. For each KMA, attach a network cable between the first port in the trunk group and the service port on the KMA (labeled LAN 2 or NET 2).
   c. Attach a network cable between the second port in the trunk group and the aggregated service port on the KMA (labeled LAN 3 or NET 3).

Port Mirroring

Mirroring ports can be useful when you want to use a network analyzer in the service network environment. Ports can be mirrored on Brocade ICX 6430 switches as follows:

1. Telnet to the switch management port.
2. On this switch, select a port that is not part of a trunk (for example, port 24 is designated as "1/1/24").
3. Access privileged mode on the switch by entering `enable` (# will be appended to the prompt indicating you are in privileged mode).
4. Enter configuration mode by entering `configure terminal` (you will see (config) appended to the prompt indicating config mode).
5. Configure the mirror-port with the command `mirror-port ethernet 1/1/24`.
6. Determine what port traffic you want to monitor (for example, port 1 designated as 1/1/1).

7. Enter the interface menu for port 1/1/1 by entering interface ethernet 1/1/1 (config-if-e1000-1/1/1 is appended to the prompt indicating you are configuring that port).
8. Enter `monitor ethernet 1/1/24` both to monitor traffic in both directions on port 24.
9. Enter `write` to save the configuration changes.

In Figure 1-8, the service network consists of two *customer-provided* managed switches that are cabled to two unmanaged switches, which contains redundant paths that require a spanning tree configuration. This example may be easily scaled for larger SL8500 drive configurations by adding additional KMAs, switch hardware, and tape drives.

- Managed switches must be enabled for Spanning Tree whenever the cabling includes redundancy.
- Unmanaged switches have two paths to the managed switches for redundancy.
- Unmanaged switches are then cabled for connectivity to the tape drives (agents)
- Each unmanaged switch connects 16 drives. Cabled in groups of four. Ports 1–4, 6–9, 11–14, and 16–19.
- Service Delivery Platform (SDP) connects to each Managed Switch at Port 1.

> **Note:**
>
> The SPARC servers are not currently supported by SDP. Development has not been done on the SDP side.

Extreme Network Switch Configuration

To configure aggregated ports on an Extreme Ethernet switch

1. Log in to the switch using telnet.
2. Enter the following CLI commands:

   ```
   show port sharing

   enable sharing <b> port></b> grouping <b> portlist</b>

   algorithm address-based L3_L4
   ```

   Port specifies the master port for a load sharing group.

   Portlist specifies one or more ports or slots and ports to be grouped to the master port. On a stand-alone switch (this is what is normally supplied), can be one or more port numbers. May be in the form 1, 2, 3, 4, 5.

3COM Network Switch Configuration

1. Use a Web browser to connect to the switch IP.
2. Select port and then link aggregation from the menu.
3. Use the Create tab to create a new port grouping.

E

Advanced Security Transparent Data Encryption (TDE)

Use OKM with Transparent Data Encryption (TDE) to manage encryption or decryption of sensitive database information.

This section assumes familiarity with TDE. See the white paper *Oracle Advanced Security Transparent Data Encryption Best Practices*, available at the following URL:

`http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf`

About Transparent Data Encryption (TDE)

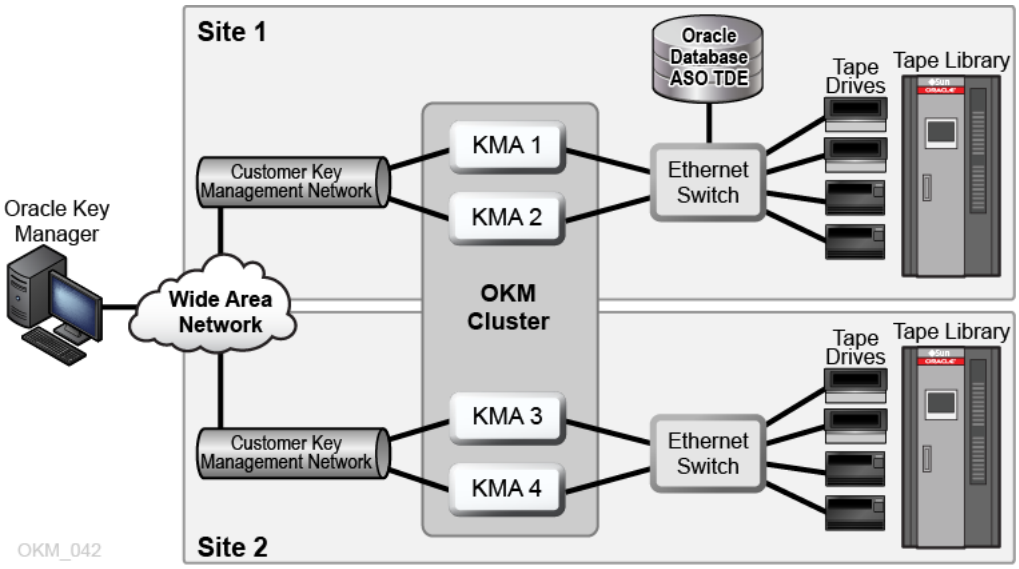
Transparent Data Encryption (TDE), a feature of Oracle Database 11gR2 and higher, provides database encryption and decryption services.

TDE supports the following products:

- Oracle Database
- Oracle Real Application Clusters (Oracle RAC)
- Oracle Data Guard
- Oracle Exadata Database Machine
- Oracle Recovery Manager (RMAN)
- Oracle Data Pump

The figure below shows an OKM cluster featuring an Oracle database with Transparent Data Encryption (TDE). See About Oracle Key Manager for more information about the basic components of the OKM cluster.

Figure E-1 OKM Cluster with TDE



TDE provides encryption services using a two-tiered key approach for TDE column encryption and TDE tablespace encryption. The first tier uses a master encryption key to encrypt the second tier table or tablespace data encryption keys that are stored within the database.

TDE stores the master encryption key in an external security module (Oracle Wallet or hardware security module). This is a recommended security practice and is crucial to maintaining the highest level of security from various threats. Use of OKM for the secure storage of the TDE master encryption keys is the recommended approach.

With TDE configured to use OKM, OKM creates and safely protects the AES256 master encryption key. OKM protects keys through replication (multiple copies across the cluster) and through backups of OKM itself.

Refer to Disaster Recovery for information about disaster recovery planning.

The following minimum versions are supported when using OKM with TDE:

Oracle Key Manager

- Oracle Key Manager 2.4.1 operating with Replication Schema version 13
- Supported OKM management platforms for the GUI and CLI are documented in the OKM product release notes, which include specific considerations for Oracle Solaris and Microsoft Windows platforms.

pkcs11_kms

- Oracle Solaris 11 Express with SRU 12
- Oracle Solaris 11 with x86 or SPARC, 32 bit or 64 bit
- Oracle Solaris 10 Update 10 pkcs11_kms patch 147441-03 for x86 or patch 147159-02 for SPARC, 32 bit or 64 bit
- Oracle Linux Server release 5.5 or higher.

Oracle Database

OKM can be integrated with TDE as the following versions of the Oracle Database server on a supported pkcs11_kms platform:

- Oracle Database 11.2.0.2 with patch 12626642
- Oracle Database 11.2.0.4
- Oracle Database 12.1 and 12.2

OKM PKCS#11 Provider

The pkcs11_kms provider interacts with OKM for key creation and key retrieval operations.

You can configure TDE to use the pkcs11_kms provider through its built-in support for hardware security modules. TDE uses the pkcs11_kms provider to acquire keys to use for encryption and decryption functions. TDE identifies key objects using a unique label that they define. TDE generates this label when the master key is created. The pkcs11_kms provider passes this label to OKM where it is maintained as metadata on the data unit. In OKM, keys are associated with data units and for the pkcs11_kms provider, this relationship should always be 1:1. Each time a new master key is created, a data unit with the key's label is created along with the corresponding key object. The key label name space in OKM is cluster-wide.

Key label naming conflicts can arise with other clients of OKM. Consequently, users of the pkcs11_kms provider should devise a key label naming scheme that insures uniqueness of key labels.

See Locate TDE Master Keys in OKM for more information.

TDE Authentication with OKM

TDE authenticates with OKM through the specific token configured to use the pkcs11_kms provider.

The token uses password-based authentication and X.509 certificates for mutual authentication of each party in the session, specifically the Oracle database instance and the OKM cluster node. You must configure TDE to properly pass these credentials to the PKCS#11 token. The TDE password should be the passphrase of the OKM agent (see Configure Database for TDE), not the AgentID:AgentPassword as suggested in the Oracle TDE documentation. For configuration instructions, refer to the document *Oracle Advanced Security Transparent Data Encryption Best Practices*, referenced at the beginning of this appendix.

Manage Authentication Credentials

OKM allows you to manage authentication credentials for agents using the pkcs11_kms provider. You can reset agent passphrases, and enable, disable or delete agents as your policies dictate. If a security breach is detected, you may disable the specific agent so that key retrievals are denied, while allowing other agents servicing other applications or devices to maintain their access. If you reset an agent passphrase, then remove the profile directory in the directory where the pkcs11_kms provider stores its slot configuration (for example, the location identified by the KMSTOKEN_DIR directory).

Load Balancing and Failover When Using pkcs11_kms

The cluster helps with load balancing and failover when using pkcs11_kms.

The pkcs11_kms provider is aware of the OKM cluster through use of OKM cluster services, a load balancer, and cluster failover logic. The pkcs11_kms provider transparently maintains client-side awareness of the OKM cluster by periodically issuing cluster discovery operations. Network changes and changes in the OKM cluster or KMA availability are handled by the agent on behalf of the pkcs11_kms provider and TDE. PKCS#11 key generation and key retrieval operations are load balanced across KMAs in the OKM cluster.

To further optimize key retrieval performance, agents may be configured to be associated with KMAs through use of OKM sites. This feature allows definition of sites according to network topology. Typically, KMAs and agents within a site would have low network latency as opposed to member KMAs and agents across a WAN.

When a network segment or KMA is unavailable, the failover logic within the agent chooses another KMA to complete the operation. TDE is unaware of any failovers, so key management operations are very reliable. Failover preferences KMAs within the same site as the agent.

You can use the kmscfg(1M) utility to tune the discovery frequency and the failover properties of the agent. See the `kmscfg` man page for more information.

Planning Considerations When Using TDE

There are key planning consideration to take into account when using TDE with OKM.

- Oracle Database Considerations When Using TDE
- OKM Performance and Availability Considerations When Using pkcs11_kms
- Network and Disaster Recovery Planning When Using pkcs11_kms
- Key Management Planning When Using pkcs11_kms

Oracle Database Considerations When Using TDE

OKM is compatible with certain Oracle Database configurations.

OKM is compatible with any of the following:

- Single Instance, Oracle RAC One Node
- Oracle Database High Availability Architectures
  - Oracle Database with Oracle Real Application Clusters (Oracle RAC). Each node of the Oracle RAC system requires a configured pkcs11_kms provider for TDE to use. All nodes must share the same OKM agent ID for authentication. With Oracle RAC, the network topology uses a public and private network. The private network used for Oracle RAC node-node traffic may be shared with the OKM service network for better isolation of key retrieval traffic. Depending on how this private network is configured, this likely precludes agent failover to KMAs outside the private network such as KMAs in a remote site. See Integrate OKM and TDE for shared storage requirements with Oracle RAC and the pkcs11_kms provider configuration files.

  - Oracle RAC Extended Cluster. In this configuration, KMAs within the OKM cluster must be colocated in the network with Oracle RAC nodes to minimize retrieval time.
  - Oracle Exadata Database Machine.
- Oracle Data Guard. All secondary databases access the same OKM cluster used by the primary database.
- Multiple Database Instances. When running multiple independent database instances on a host, a PKCS#11 token must be configured for each instance. This amounts to creating an OKM agent for each database instance, and authenticating the agent to OKM through the token. Use the `kmscfg` tool to complete this task. When running multiple database instances under the same O/S user, but using different OKM agents, you must set the KMSTOKEN_DIR environment variable to a different location each time you invoke the `kmscfg` utility. See Configure Database for TDE for more information about the `kmscfg` utility. For more information about running multiple databases on the same host, refer to the document *Oracle Advanced Security Transparent Data Encryption Best Practices,* referenced at the beginning of this appendix.
- Oracle RMAN
- Oracle Data Pump

OKM Performance and Availability Considerations When Using pkcs11_kms

Some OKM functions should be performed on KMAs that are not servicing Oracle Database to improve performance.

Key retrievals for TDE through the pkcs11_kms token typically take 100-200 milliseconds per KMA access. When failovers occur, the response time is a multiple of the number of failover attempts. OKM backup and key transfer operations are resource-intensive activities that can impact OKM database performance. Plan carefully to determine when and where to perform OKM backups. Since OKM backups are cluster-wide, they can be performed on KMAs that are not servicing Oracle Database instances. Similarly, key transfer operations are also cluster-wide operations and can be performed on any KMA. Therefore, it is recommended that you choose a KMA that is not servicing busy Oracle Database instances.

Network and Disaster Recovery Planning When Using pkcs11_kms

Disaster recovery planning decisions influence the network configuration.

OKM cluster configuration must be planned in accordance with the Oracle Database servers and the enterprise's disaster recovery strategy. OKM networking options are very flexible and include multi-homed interfaces used by the OKM management and service network. Oracle recommends that TDE access be over the OKM service network. The pkcs11 provider's configuration directory is a new consideration for disaster recovery planning. Consider recovery scenarios for this storage area to avoid the need to reconfigure a pkcs11_kms token, especially when it is shared between nodes of an Oracle RAC.

For detailed information about OKM disaster recovery planning, refer to Disaster Recovery along with the Oracle database publications.

Key Management Planning When Using pkcs11_kms

Key management planning must address the key life cycle and security policies of the enterprise.

- See About Key Lifecycles for information about NIST SP-800 key management phases and corresponding OKM key states.
- See Re-Key Due to OKM Policy Based Key Expiration for information about an issue that can occur when a key policy is not set to a long enough time period.

Key Policy Considerations

All TDE master keys are Advanced Encryption Standard (AES) 256 bits generated by OKM. KMAs may contain a FIPS 140-2 Level 3-certified hardware security module, such as an SCA 6000 PCIe card. When KMAs have this hardware security module, their keys are created by the hardware security module. Otherwise, cryptographic operations use the Solaris Crypto Framework's software token provider. See Manage Key Policies for more information.

Key Lifecycle — The key lifecycle is the primary configuration item with respect to key policy planning decisions. The periods for the operational phase of the key's lifecycle should be chosen based upon data retention needs and the frequency with which TDE master keys will be re-keyed. The TDE DDL supports specification of various key sizes for the master key, as does the schema encryption dialogs within OKM. Only AES 256 bit keys can be used with OKM.

Key Policy Encryption Period — The key policy encryption period defines the length of time for the key to be used in the protect and process (encrypt and decrypt) state of the lifecycle. This period should correspond to the time period for use of the master key before it should be re-keyed (for example, maximum one year for PCI).

Key Policy Cyptoperiod — The key policy cryptoperiod is the remaining time allotted for use of the master key to decrypt data during the process only (decrypt only) state of the key lifecycle. The length of this period should conform to the data retention requirements for the data protected by the TDE master key. Typically this value is a number of years corresponding to the enterprise policy for data retention (for example, a seven year retention period for US tax records). The rate at which new keys will be generated should not be a concern with TDE as re-key operations will likely be infrequent. However, if this becomes a concern, then consider lengthening the encryption period on the key policy and re-keying less frequently. You can also increase the OKM key pool size configuration parameter to direct the KMAs to maintain a larger pool of available keys. Multiple key policies may be defined for use with different types of databases as needs dictate.

Key Access Control Through Key Groups

It may be necessary to control access to keys managed by OKM when multiple database instances or multiple agents are accessing the OKM cluster for various purposes.

All OKM agents are assigned to at least one key group (a default key group assignment is required), which authorizes them to have access to the keys within those groups. The agent's default key group is the only key group within which a pkcs11_kms provider's agent will create keys.

Consider using multiple key groups when master keys do not need to be shared across database instances or hosts. An example might be to use one key group for production database instances and another key group for development/test databases, so that isolation is assured. Agents in the test database key group would then be blocked by OKM if they attempt to use a master key for a production database. Such an attempt would also be flagged in the OKM audit log and may be an indicator of a configuration error that could disrupt a production database.

TDE also provides isolation of master keys through their key label naming convention. In the PKCS#11 specification, key labels are not required to be unique. However, OKM enforces unique labels unless the agent includes a default key group attached to a key policy where "Allows Revocation" is true. In this case, OKM relaxes the uniqueness constraints and issues a warning instead of an error for duplicate labels.

If a label conflict occurs between different master keys for different database instances, the first label created is always returned. Any agent attempting to access a key that shares an identical label belonging to another key group will be denied by OKM. This is detected during a re-key operation, and the work around is to re-key until another, non-conflicting, label is generated.

Key and Data Destruction Considerations

Destruction of data to conform to data retention requirements can begin with the destruction of TDE master keys. How and when these keys should be destroyed is an important planning item. OKM provides for this and for tracking of OKM backups, which include these keys. Management of OKM backups is both a Disaster Recovery planning item and key destruction planning item.

Integrate OKM and TDE

This section describes how to install and configure pkcs11_kms and the OKM cluster for use with TDE.

System Requirements for OKM and TDE

Using OKM with TDE requires the system to meet minimum requirements.

Oracle Key Manager

OKM 2.4.1 operating with Replication Schema version 13. Supported OKM management platforms for the GUI and CLI are documented in the OKM product release notes, which include specific considerations for Oracle Solaris and Microsoft Windows platforms.

pkcs11_kms

pkcs11_kms is supported on the following platforms:

- Oracle Solaris 11.x (all SRUs)
- Oracle Solaris 10 Update 10 pkcs11_kms patch 147441-03 for x86 or patch 147159-02 for SPARC, 32 bit or 64 bit
- Oracle Linux Server, release 5.5, 5.6, 5.9, 6.5, and 7

Oracle Database

OKM can be integrated with TDE as the following versions of the Oracle Database server on a supported pkcs11_kms platform:

- Oracle Database 11.2.0.2 with patch 12626642
- Oracle Database 11.2.0.4
- Oracle Database 12.1
- Oracle Database 12.2

Install OKM for TDE

Install OKM using the standard installation instructions, then use the procedures here for TDE.

The OKM cluster installation process is described in the Install the KMA . Typically, OKM installation involves engagement with Oracle Professional Services, to aid in planning, installation, and configuration service choices. Additionally, it is recommended that your security team be involved in the planning process.

After you establish a working OKM cluster, follow the OKM administration steps described in the configuration sections of this appendix.

Install pkcs11_kms

Install and configure the OKM PKCS#11 Provider, pkcs11_kms, on the Oracle database server(s).

A pkcs11_kms distribution is available for each platform.

Oracle Solaris 11

1. Display the version of the pkcs_kms package:

   ```
   #> pkg info -r pkcs11_kms
   ```

2. Enter the following command:

   ```
   #> pkg install system/library/security/pkcs11_kms
   ```

3. Install the provider into the Solaris Crypto Framework. The singel quotes are significant.

   ```
   # cryptoadm install provider='/usr/lib/security/$ISA/pkcs11_kms.so.1'
   ```

4. Enter the following sequence of commands to verify the installation:

```
# cryptoadm list -m -v \
provider='/usr/lib/security/$ISA/pkcs11_kms.so.1'
```

This displays message: 'no slots presented' until kmscfg is run.

Oracle Solaris 10 Update 10

The pkcs distribution is installed as "SUNWpkcs11kms" in Solaris 10 Update 10.

SPARC systems require Solaris patch 147159-03 or later. x86 systems require Solaris patch 147441-03 or later. To download Solaris patches, go to: https://support.oracle.com

1. Enter the following command to install the pkcs11_kms package for the hardware platform.

   ```
   # pkgadd [-d path to parent dir of package] SUNWpkcs11kms
   ```

2. Install the provider into the Solaris Crypto Framework. The single quotes are significant.

   ```
   # cryptoadm install provider='/usr/lib/security/$ISA/pkcs11_kms.so.1'
   ```

Oracle Linux Server

pkcs11_kms is distributed as patch 26093641 for Linux 6 and patch 25979695 for Linux 7 on the My Oracle Support site at https://support.oracle.com

1. Log in and click the **Patches & Updates** tab and search for the specific patch ID directly.
2. pkcs11_kms is distributed as an RPM package. Use RPM package manager commands to install this software.
   For example: `rpm -i pkcs11kms-1.3.0-1.x86_64.rpm`

Uninstall pkcs11_kms

The procedures for unistalling pkcs11_kms depend on the platform.

Oracle Solaris 11

Enter the following commands:

```
# cryptoadm uninstall \
provider='/usr/lib/security/$ISA/pkcs11_kms.so.1'
# pkg uninstall system/library/security/pkcs11_kms
```

Oracle Solaris 10 Update 10

Enter the following command:

```
# pkgrm SUNWpkcs11kms
```

Oracle Linux Server

When packaged with Oracle Database, the pkcs11_kms provider will be uninstalled through the steps used to uninstall the Oracle Database product. If installed through another means, then follow the inverse procedures of the install using rpm.

For example:

```
# rpm -e pkcs11kms-1.3.0-1.x86_64.rpm
```

Configure Database for TDE

Configure the shared library file (pkcs_kms.so) for TDE access.

Each Oracle Database server must be running on a supported pkcs11_kms platform. For Oracle Database 12.2.0.2, mandatory patch 12626642 must be installed. This patch is available at the following URL:

`https://updates.oracle.com/download/12626642.html`

Once installed, the shared library file (pkcs_kms.so) must be configured for TDE access. The library path is OS-specific:

- `/usr/lib/security/pkcs11_kms.so.1` (Solaris only, 32-bit)
- `/usr/lib/security/amd64/pkcs11_kms.so.1` (Solaris only, 64-bit)
- `/usr/lib64/pkcs11_kms.so.1` (Linux only, 64-bit)

Configure the OKM Cluster for TDE

Configure an already functional OKM cluster for TDE.

These tasks assume a functioning OKM cluster configured with appropriate administrative users and roles. All KMAs in the OKM cluster must be running a minimum of OKM 2.4.1 and Replication Version 13.

1. Define the key policy. See:
   - Manage Key Policies
   - Key Management Planning When Using pkcs11_kms
2. Define the group definition. Assign the key policy to the key group and a handy name for the group. See:
   - Manage Key Groups
   - Key Access Control Through Key Groups
3. Configure agent(s). See:
   - OKM PKCS#11 Provider
   - Manage Agents
4. Associate each agent with a default key group. See Assign Agents to Key Groups.
   - Agent ID — The agent ID can be anything meaningful to the configuration, and should correspond to the Oracle user for the database instance to be associated with the agent.
   - Passphrase — Choose a strong passphrase as this passphrase will also be configured on the Oracle host for authenticating with OKM through the DDL statements that open the wallet (for example, the pkcs11_kms token). See Create an Agent for information about passphrase requirements. OneTimePassphrase flag should be set to "false" to allow password-based authentication any time the TDE "wallet" must be opened, as well as from multiple Oracle RAC nodes sharing a common agent ID. For maximum

security this can be set to the default value of "true," but will only work in a single node Oracle Database configuration and not in Oracle RAC. When OneTimePassphrase is true, the agent's X.509 certificate is returned only when the agent successfully authenticates the first time. The pkcs11_kms provider securely stores the X.509 certificate's private key in a PKCS#12 file that is protected by a passphrase. The X.509 certificate and corresponding private key are then used for agent transactions with OKM. See kmscfg(1M) for other information that the pkcs11_kms provider stores.

- Key Group — Assign the agent to the key group(s) defined for TDE. The pkcs11_kms provider only supports the default key group for key creation operations, including re-key operations. Any additional, non-default key groups associated with the agent will only allow key retrievals from keys in those groups. This capability could be leveraged in read-only/decryption-only database scenarios such as in support of a secondary database that will never generate a master key, but only needs the ability to access the master keys.

Configure kcs11_kms

Configure the pkcs11_kms provider on the Oracle Database nodes that will require TDE master keys.

1. Configure the agent and pkcs11_kms provider using the Oracle Database user account. This does not require special privileges for the O/S user. When a host supports "Multiple Oracle Homes," then the pkcs11_kms token configuration must be in accordance with each Oracle Database software owner's user account. Refer to the *Oracle Database Installation Guide 11g Release 2* for more information.
2. The kmscfg utility creates one slot configuration per user at a time. It is possible to define additional slot configurations for an individual user, but only one will be active per process.

> **Caution:**
>
> The default location of the slot configuration directory for the KMS PKCS#11 provider is `/var/kms/$USER` on Solaris 11 Express and is `/var/user/$USER/kms` on Solaris 11. If you plan to upgrade your Solaris 11 Express system to Solaris 11, then you should first save your slot configuration elsewhere.
>
> For example:
>
> ```
> # cd /var/kms/$USER
> # tar cvf ~/save_my_okm_config.tar .
> ```
>
> After the upgrade, restore your slot configuration to the new location. For example:
>
> ```
> # mkdir -p /var/user/$USER/kms
> # cd /var/user/$USER/kms
> # tar xvf ~/save_my_okm_config.tar
> ```
>
> **If you do not back up pcks11_kms data before you upgrade, your data will be lost and the master key used by the Oracle data base for encrypted data will not be available.**

The kmscfg utility stores configuration and run-time data in a KMS configuration directory at one of the following paths:

- `/var/user/$USER/kms (Solaris 11)`
- `/var/kms/$USER` (Solaris 10u10 and Solaris 11 Express)
- `/var/opt/kms/$USER` (Oracle Linux Server)

This directory is overridden by the $KMSTOKEN_DIR environment variable to the location of the customer's choosing.

When kmscfg runs, a "profile" name is provided. This name is used for the agent-specific run-time subdirectory created within the configuration directory described above.

3. Refer to the kmscfg man page for the default location of its slot configurations. Slot configurations may be controlled using the KMSTOKEN_DIR environment variable to define an alternate slot configuration and file system location.

   For Oracle RAC, where the agent profile must be shared between Oracle RAC nodes, use the KMSTOKEN_DIR environment variable to direct kmscfg to create the profile using the appropriate shared filesystem path. If the KMSTOKEN_DIR environment variable is set, it must be set persistently for the shell in a shell configuration file (such as `.bashrc`) so that it is always set before the database performing any PKCS#11 operations.

4. Allocate file system storage space for the slot's configuration and run-time information. If you plan to use Oracle RAC, define the profile in a shared file system location with permissions that are readable and writable by each of the Oracle RAC node users.

5. Allocate space requirements to allow for growth in each agent log. The log file is automatically created and is a helpful troubleshooting tool. The space consumed

by the KMSAgentLog.log file can be managed using a tool like logadm(1M) on Solaris or logrotate(8) on Oracle Linux Server. Allocating 10 MB for each agent's profile directory is adequate for most configurations.

6. Initialize a pkcs11_kms provider using the `kmscfg` utility. In this step, you define a profile for the OKM agent that will later be associated with a pkcs11_kms token.

```
# kmscfg
Profile Name: oracle
Agent ID: oracle
KMA IP Address: kma1
```

7. Verify authentication with OKM.

   a. On Solaris systems, verify authentication using the cryptoadm(1M) command. Note that the flag field shows `CKF_LOGIN_REQUIRED` in the following example, indicating that the slot is not yet configured with an authenticated token.

```
solaris> cryptoadm list -v \
provider='/usr/lib/security/$ISA/pkcs11_kms.so.1'
Provider: /usr/lib/security/$ISA/pkcs11_kms.so.1
...
Flags: CKF_LOGIN_REQUIRED
```

   b. Verify that the pkcs11_kms token can authenticate with the OKM cluster. This example uses Oracle Solaris pktool(1), a utility that is not available for Linux platforms. The SO (PKCS#11 abbreviation for a security officer) prompt is for the agent's secret passphrase as established in a previous step by the OKM administrator who created the agent.

```
solaris> pktool inittoken currlabel=KMS
Enter SO PIN:
Token KMS initialized.
```

   c. On Solaris systems, verify that the token is initialized by using the Solaris Crypto Framework cryptoadm(1M) command or the pktool(1) utility. Note that the token's flag shown by output from cryptoadm is now `CKF_TOKEN_INITIALIZED`:

```
solaris> cryptoadm list -v \
provider='/usr/lib/security/$ISA/pkcs11_kms.so.1'
 ...
 PIN Max Length: 256
 Flags: CKF_LOGIN_REQUIRED CKF_TOKEN_INITIALIZED
```

   d. On Solaris systems, use the pktool(1) utility to verify the status of PKCS#11 visible tokens:

```
glengoyne> pktool tokens
Flags: L=Login required  I=Initialized  X=User PIN expired  S=SO PIN expired
Slot ID  Slot Name     Token Name                  Flags
-------  ---------     ----------                  -----
1        Sun Crypto    Softtoken      Sun Software PKCS#11 softtoken
2        Oracle Key Management System              KMS  L
glengoyne>
```

   This shows that Login to the token is still required. The meaning of the Flags in the pktool output can be shown as follows:

```
glengoyne> pktool tokens -h
Usage:
   pktool -?    (help and usage)
```

```
   pktool -f option_file
   pktool subcommand [options...]
```

where subcommands may be:

```
   tokens
   * flags shown as: L=Login required  I=Initialized
     E=User PIN expired  S=SO PIN expired
glengoyne>
```

e. On Solaris systems, use the pktool(1) utility to log in to the token and authenticate with the OKM cluster's KMA specified in the kmscfg(1) step and the passphrase created by an OKM administrator for the agent. This passphrase is supplied with the SO PIN prompt:

```
glengoyne> pktool inittoken currlabel=KMS
Enter SO PIN:
Token KMS initialized.
```

f. On Solaris systems, use the pktool(1) utility to verify the tokens status and that it is now initialized:

```
glengoyne> pktool tokens
Flags: L=Login required  I=Initialized  X=User PIN expired  S=SO PIN expired
Slot ID  Slot Name   Token Name                    Flags
-------  ---------   ----------                    -----
1        Sun Crypto  Softtoken         Sun Software PKCS#11 softtoken
2        Oracle Key Management System              KMS   LI
```

g. On Solaris systems, use the cryptoadm(1M) command to verify that the pkcs11_kms token is initialized by requesting to see the mechanisms that it supports:

```
glengoyne> cryptoadm list -m -p  provider=/usr/lib/security/'$ISA'/
pkcs11_kms.so.1
Mechanisms:
CKM_AES_KEY_GEN
CKM_AES_CBC
CKM_AES_CBC_PAD
glengoyne>
```

On Solaris systems, use the pktool(1) utility to create and list keys through the pkcs11_kms provider as follows:

```
 # pktool genkey token=KMS keytype=aes keylen=256
   label=MyKey-test1
 # pktool list token=KMS objtype=key
 # pktool list token=KMS objtype=key label=MyKey-test1
```

You can see the keys in the OKM system through the OKM Manager GUI or OKM CLI.

> **Note:**
>
> For Solaris, kmscfg(1) by default creates just one slot configuration per user at a time. You can define additional slot configurations, but only one will be active per process. You can do this by using the KMSTOKEN_DIR variable to define an alternate slot configuration and file system location.
>
> The Solaris 11 default is `/var/user/$USERNAME/kms`, but you can create your own naming schemes. A best practice might be `/var/user/$USERNAME/$AGENTID-$CLUSTER/` This naming convention allows Solaris to have multiple slot-agent-cluster combinations based on various usage scenarios.
>
> For some PKCS#11 configurations, an alternate location is recommended, for example, TDE with Oracle RAC (see the TDE configuration section above), so that each node shares the pkcs11_kms provider's metadata).

8. To configure TDE to use auto-open wallets, follow the instructions described in the document *Oracle Advanced Security Transparent Data Encryption Best Practices*, referenced at the beginning of this appendix.

Migrate Master Keys from the Oracle Wallet

Retain the old wallet and have OKM generate a new master key.

Refer to the document *Oracle Advanced Security Transparent Data Encryption Best Practices*, referenced at the beginning of this appendix. The Oracle Database Administrator must perform re-key operations before the key's lifecycle dictates. Otherwise, the database will not start. Refer to the various Oracle Database and TDE documents for the DDL used to perform this operation. Re-keying may also be performed using Oracle Enterprise Manager.

Re-Key Due to OKM Policy Based Key Expiration

The Oracle Database Administrator must perform re-key operations before the key's lifecycle dictates, otherwise the database will not start.

Once a key reaches the post-operational state, each key retrieval by TDE will trigger a warning in the OKM audit logs indicating that a post-operational key has been retrieved. Presence of these audit messages is an indication that it is time to re-key the database instance's master encryption key. The OKM audit message identifies the specific agent and key that is being retrieved to facilitate identification of the Oracle Database instance and master encryption key that has reached the post-operational state. Notification through SNMP v3 informs or SNMP v2 traps may be configured in OKM to support automation of this process.

The pkcs11_kms provider will attempt to inform its PKCS#11 consumers that the key has reached the post-operational state. This is done by setting the PKCS#11 "CKA_ENCRYPT" attribute to false for the master key.

All released versions of Oracle Database 11 and 12 will try to use a key to encrypt data after its encryption period has expired. TDE will never automatically re-key the TDE master key.

On Solaris, you may see errors similar to the following in the database alert logs:

```
HSM heartbeat died. Likely the connection has been lost.
PKCS11 function C_EncryptInit returned
PKCS11 error code: 104
HSM connection lost, closing wallet
```

If this error is encountered, the Database Administrator must perform the following actions:

1. Set an environment variable for the user associated with the pkcs11_kms token (typically the Oracle user's profile). This allows the deactivated key to continue to be used for encryption:

   ```
   # export PKCS11_KMS_ALLOW_ENCRYPT_WITH_DEACTIVATED_KEYS=1
   ```

2. Restart the database.
3. Rekey the master key for the database instance, following the instructions in your Oracle Database administration documentation.

On Oracle Linux, the default for the pkcs11_kms provider allows use of deactivated keys, however, you will see errors similar to the following in the /var/log/messages file:

```
pkcs11_kms:  Encrypting with key which does not support encryption (check to see if
key is expired or revoked
```

If this message is encountered, the database administrator should re-key the TDE master key as described in the Oracle Database administration documentation.

In spite of this, TDE will continue to use the key and not perform an automatic re-key operation. OKM administrators observing the post-operational key retrieval audit warnings must inform a Database Administrator that it is time to re-key their database instance's master key.

Convert from Another Hardware Security Module Solution

Contact Oracle technical support for specific steps required to convert from another vendor's hardware security module solution to OKM.

Key Destruction When Using TDE

Verify the key is not being used before destroying keys that have reached the post-operational phase.

OKM administrators are responsible for the regular destruction of keys in the post-operational phase. Deletion of keys through the pkcs11_kms provider is not supported with OKM and is a restricted operation reserved for OKM users that have been assigned the role of Operator. Once a key has been destroyed, any attempt to retrieve it will fail, including PKCS#11 C_FindObjects requests.

Key Transfer in Support of Oracle RMAN and Oracle Data Pump

Oracle RMAN and/or Oracle Data Pump may require the ability to supply the master key to another OKM cluster.

OKM key transfer operations readily support key transfer using the secure key export and key import services. See Transfer Keys Between Clusters for more information.

1. Establish key transfer partners between the source and destination OKM clusters.
2. Identify the TDE master keys to be exported in support of Oracle RMAN backups or encrypted data exported using Oracle Data Pump.
3. Export the keys from the source OKM cluster. This will create a secure key export file.
4. Transmit the exported key file to the transfer partner.
5. The destination transfer partner imports the keys into their OKM cluster.

Run Oracle RMAN restore or Oracle Data Pump import to re-create the database instance that requires the keys. This requires the configuration steps necessary to use TDE with OKM at the importing location. The restore or import operation then accesses the OKM for the universal master keys required to decrypt the column or tablespace keys used by the database instance.

Attestation, Auditing, and Monitoring for TDE

Oracle recommends the following:

- Review and monitor the OKM active history of the TDE agent to help detect problems.
- Auditors can use OKM audit events to attest that TDE is accessing its master keys from the OKM cluster.
- Configure an SNMP manager for OKM.
- Explore the use of OKM CLI to generate enterprise specific reports.

Locate TDE Master Keys in OKM

You can locate the TDE master keys within OKM using either the GUI or CLI. TDE generates the master key labels and OKM uses a data unit's External Tag attribute to store this value. TDE master key generation (including re-key operations) always creates a new data unit object and key object within the OKM cluster.

1. Perform a query on the OKM data units and filter the list using an ExternalTag filter: "ExternalTag" begins with "ORACLE.TDE". All TDE key labels begin with this string so this will generate a list of OKM data units that were created by TDE. Each OKM data unit will have a single TDE master key associated with it. These keys can be viewed using the OKM GUI to examine their lifecycle state and other properties, such as key group, export/import status, and which OKM backups contain destroyed keys. These keys can also be viewed using the OKM CLI. For example:

```
>okm listdu --kma=acme1 --user=joe \
--filter="ExternalTag=ORACLE.TDE"
```

2. When multiple Oracle Database instances share an OKM cluster, an OKM administrator can identify which keys correspond to a particular database by using a query against the audit events for the agent that corresponds to that database instance. These audit events can be viewed using the Oracle GUI. Filter the agent's audit history using the filter: "Operation equals CreateDataUnit". This produces a list of the audit events corresponding to TDE master key creations. The audit event details provide the necessary information to identify the specific data units for the master keys. These audit events can also be viewed using the OKM CLI. For example:

```
>okm listauditevents --kma=acme1 --user=joe \
--filter="Operation=CreateDataUnit"
```

Troubleshoot pkcs11_kms Issues

Use these procedures to troubleshoot error conditions that may be encountered when using OKM with pkcs11_kms.

Cannot Retrieve the Master Key When Using pkcs11_kms

Use these steps to correct when the Oracle Database reports the master key cannot be retrieved (error ORA-28362 & ORA-06512).

1. Examine the `$ORACLE_BASE/diag/rdbms/$SID/$SID/trace/alert_$SID.log` file. This file logs success/fail messages related to "alter" DDL statements used to access the encryption wallet.
2. Examine the `KMSAgentLog.log` file in the pkcs11_kms configuration directory (`$KMSTOKEN_DIR/KMSAgentLog.log`).
3. Verify the general status of OKM. Check the following:
   - Are KMAs active?
   - Are KMAs locked?
   - Is the key pool depleted?
   - KMA ILOM faults
   - KMA console messages
4. Verify the status of the pkcs11_kms token as demonstrated earlier.
5. Verify the status of the agent by examining OKM audit events for that agent to ensure that it enrolled and is enabled.
6. Verify network connectivity from the Oracle Database host to OKM nodes.

7. Contact Oracle Technical Support. You may be asked to provide one or more KMA System Dumps.

Loss of the pkcs11_kms Configuration Directory

Use this procedure to recover a lost or corrupted pkcs11_kms token profile.

1. Perform the configuration steps described in Configure Database for TDE.
2. **Solaris Only** - Repopulate the token's metadata, using the following data unit filter with the OKM: "ExternalTag" begins with "ORACLE.TDE".
3. **Solaris Only** - Save the results of this listing to a file (for example "du.lst") and then execute the following shell script:

```
for label in `awk '{print $2}' < du.lst `
do
pktool list token=KMS objtype=key label="${label}"
done
```

No Slots Available Error When Using pkcs11_kms

Use this procedure when the client gets "No Slots Available" errors when issuing any PKCS#11 operation.

1. Ensure that the kmscfg utility has run successfully.
2. Ensure that the pkcs11_kms provider has been properly installed and configured.

CKA_GENERAL_ERROR Error When Using pkcs11_kms

Use this procedure when the client gets the CKA_GENERAL_ERROR error when trying to retrieve keys.

1. Verify that the agent has a default key group in the OKM cluster.
2. Review the $KMSTOKEN_DIR/KMSAgentLog.log file for more information.

Could Not Open PKCS#12 File Error

Use this procedure when the "Could not open PKCS#12 file" error appears in the $KMSTOKEN_DIR/KMSAgentLog.log file.

1. Select audit events in the OKM cluster to determine whether the agent passphrase has recently changed.
2. Remove the <profile-name> directory under $KMSTOKEN_DIR.

F

Solaris ZFS Encryption

Use OKM with Oracle Solaris 11 ZFS to manage encryption and decryption of files in ZFS storage pools.

- Use pkcs11_kms with ZFS
- Considerations When Using ZFS
- Integrate OKM and ZFS

This section assumes familiarity with Solaris 11 and Oracle Solaris ZFS.

- Refer to the Oracle Solaris 11 publications for more information about Oracle Solaris 11.
- Refer to the publication *Oracle Solaris Administration: ZFS File Systems* for more information about Oracle Solaris ZFS.

Use pkcs11_kms with ZFS

Configure ZFS to use the PKCS#11 provider (pkcs11_kms) to retrieve encryption keys from an OKM cluster.

This requires a configured OKM cluster and a Solaris 11 system with established connectivity to KMAs in this OKM cluster. Once a Solaris 11 administrator installs and configures pkcs11_kms, the administrator can request that pkcs11_kms create a key, and then direct ZFS to use it.

See the following sections for more information about pkcs11_kms:

- OKM PKCS#11 Provider
- Manage Authentication Credentials
- Load Balancing and Failover When Using pkcs11_kms

Considerations When Using ZFS

There are key planning considerations when using OKM with ZFS.

See the following sections for considerations that may apply as you plan for this integration:

- OKM Performance and Availability Considerations When Using pkcs11_kms
- Network and Disaster Recovery Planning When Using pkcs11_kms
- Key Management Planning When Using pkcs11_kms

Integrate OKM and ZFS

Use these procedures for integrating OKM with ZFS.

- Configure the OKM Cluster for ZFS
- Install pkcs11_kms on Solaris 11
- Configure pkcs11_kms on Solaris 11
- Configure ZFS to use pkcs11_kms

> **Note:**
>
> Much of the information for these tasks also applies in OKM configurations using Transparent Data Encryption (TDE). Where appropriate, the following sections include references to additional information described in the TDE section.

Configure the OKM Cluster for ZFS

Use the procedures provided for configuring a standard OKM cluster to configure the cluster for ZFS.

1. Ensure that all KMAs in the OKM cluster are running OKM 2.4.1 or later and that the OKM cluster uses Replication Schema version 13. Supported OKM management platforms for the GUI and CLI are documented in the OKM product release notes, which include specific considerations for Oracle Solaris and Microsoft Windows platforms.
2. Create a key policy and key group, configure an agent, and associate that agent with the key group as its default key group. For more information, see Configure the OKM Cluster for TDE.

> **Note:**
>
> The agent should be configured to disable the **One Time Passphrase** property. See Create an Agent or View and Modify Agents.

Install pkcs11_kms on Solaris 11

Install pkcs11_kms for ZFS using the same procedures used for TDE.

To install Oracle's PKCS#11 provider, pkcs11_kms, on the Solaris 11 system, perform the steps described in Install pkcs11_kms.

Configure pkcs11_kms on Solaris 11

Configure pkcs11_kms for ZFS by using the same procedures as TDE.

To configure pkcs11_kms on the Solaris 11 system, perform Steps 2 and 3 as described in Configure kcs11_kms. Disregard references to Oracle RAC, as they do not apply in an OKM/ZFS integration.

Configure ZFS to use pkcs11_kms

Generate a key in the pkcs11_kms provider and configure ZFS to use this key when encrypting files in file systems contained in a particular ZFS pool.

Use the Solaris pktool genkey command to create an AES 256-bit key.

1. At the "Enter PIN for KMS" prompts, enter the passphrase of the agent that was provided to the kmscfg utility when you configured pkcs11_kms.

   For example:

   ```
   # pktool list token=KMS objtype=key
   Enter PIN for KMS:
   # pktool genkey keystore=pkcs11 token=KMS keytype=aes keylen=256
   label=zfscrypto_key_256
   Enter PIN for KMS:
   # pktool list token=KMS objtype=key label=zfscrypto_key_256
   Enter PIN for KMS:
   ```

2. Use the `zfs create` command to configure ZFS to use this key.

   In the "keysource" argument of the zfs create command, specify the label of key that you generated above.

   At the "Enter 'KMS' PKCS#11 token PIN" prompts, enter the passphrase of the agent.

   For example:

   ```
   # zfs create -o encryption=aes-256-ccm -o
   keysource="raw,pkcs11:token=KMS;object=zfscrypto_key_256" cpool_nd/cfs
   Enter 'KMS' PKCS#11 token PIN for 'cpool_nd/cfs':
   ```

Troubleshoot pkcs11_kms Issues with ZFS

Use the same troubleshooting procedures as when using pkcs11_kms and TDE.

See Troubleshoot pkcs11_kms Issues for troubleshooting information.

G

Upgrade and Configure Integrated Lights Out Manager (ILOM)

Use these procedures to upgrade and configure the Service Processor (ILOM) of your KMA.

See Also: For initial configuration of a newly installed KMA, see Initial ILOM Configuration.

About ILOM (Integrated Lights Out Manager)

The ILOM contains a separate service processor from the main server, which provides a remote connection between a terminal emulator (usually on a laptop) and the KMA. ILOM allows you to perform server functions such as the QuickStart program.

The setup of a SPARC T8-1, SPARC T7-1, Netra SPARC T4-1, or Sun Fire X4170 M2 KMAs requires access to the ILOM.

> **Note:**
>
> SunFire X2100 M2 or X2200 M2 servers use Embedded Lights Out Manager (ELOM). Refer to the OKM 2.5 documentation for information on ELOM.

Connect to the KMA through the ILOM using either:

- Network connection—NET MGT ILOM interface—(recommended)
- Keyboard and monitor attached to the KMA (Sun Fire servers only). On KMS 2.x KMAs, an alternate method to the network connection is to use a keyboard connected to one of the USB ports and a monitor connected to the VGA connector.

Related Documentation

ILOM 4.0 (for SPARC T7-1 or T8-1)

Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0

Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 4.0

Oracle ILOM Quick Reference for CLI Commands Firmware Release 4.0

Oracle ILOM Security Guide Firmware Release 3.x and 4.x

https://docs.oracle.com/cd/E81115_01/index.html

ILOM 3.2 (for Netra SPARC T4-1)

Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2

Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.1

Oracle ILOM Quick Reference for CLI Commands Firmware Release 3.2.1

Oracle ILOM Security Guide Firmware Release 3.0, 3.1, and 3.2

http://docs.oracle.com/cd/E37444_01/index.html

ILOM 3.1 (for Sun Fire X4170 M2)

Oracle ILOM 3.1 Configuration and Maintenance Guide

http://docs.oracle.com/cd/E24707_01/index.html#tooltipjtvrspan

ILOM Upgrade Overview

T8-1, T7-1, T4-1, and X4170 M2 KMAs are manufactured with the latest ILOM firmware level that was available at the time. However, you may need to upgrade the ILOM over time.

> **Note:**
>
> SunFire X4170 M2 KMAs run ILOM 3.1 or later, while SPARC T8-1, SPARC T7-1, and Netra SPARC T4-1 KMAs run ILOM 3.2 or later. ILOM 3.2 is included in server firmware 8.3 or later. You can view the current server firmware from the ILOM.

This information describes the procedures that should be used with the firmware upgrade procedures documented in the following guides:

- For the Sun Fire X4170 M2 server: *Oracle Integrated Lights Out Manager (ILOM) 3.1 Configuration and Maintenance Guide*.
- For the SPARC T8-1, SPARC T7-1 and Netra SPARC T4-1 servers: *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2*

Oracle recommends configuring specific, non-default, OpenBoot/BIOS settings that prevent changes to the BIOS that may compromise security. These settings are saved in the CMOS. In a default CMOS configuration, a remote user can use the ILOM to change BIOS settings and then start the KMA from a network device. To minimize this security risk, access to the BIOS settings must be limited. Following the procedures in this document will ensure that these settings are retained.

> **Note:**
>
> SPARC T8-1, SPARC T7-1 and Netra SPARC T4-1 servers do not include a BIOS. There are no BIOS procedures for users to follow. Follow the OBP procedures, instead.

This appendix assumes familiarity with the Oracle Key Manager solution, in particular, the Shutdown the KMA procedure with the ILOM web-based interface and the BIOS Setup Utility.

Verify ILOM and OBP or BIOS Levels

Log in to the ILOM and verify BIOS/OpenBoot levels match the latest levels documented for your server type.

SPARC servers do not have a BIOS they have an OpenBoot level instead. The firmware versions can be used to determine what type of KMA server you're connected to through the ILOM.

1. Log into the ILOM web GUI.
2. Navigate to **System Information > Firmware**.
3. Look for the values in the ILOM Version and BIOS/OpenBoot Version fields.

   Expected ILOM and OpenBoot or BIOS firmware levels vary across OKM releases. Use the following table for the latest levels.

Table G-1 Server Firmware Levels

Server	Server Firmware	ILOM Firmware	OpenBoot PROM/BIOS Firmware	OKM Release
SPARC T8-1	9.9.2.a	4.0.4.3.a	4.43.2	3.3.2
SPARC T7-1	9.8.5.c	4.0.2.2.c	4.42.4	3.3.2
Netra SPARC T4-1	8.4.2.d	3.2.1.7.f	4.35.5.a	3.0, 3.0.2[1]
Sun Fire X4170 M2	1.7.2	3.1.2.20.b	08.14.01.03	2.x, 3.0.2[2]
Sun Fire X4170 M2	1.6.1	3.0.16.10.d	08.12.01.04	2.5.x
Sun Fire X4170 M2	1.3	3.0.14.11.a	08.06.01.08	2.3.1, 2.4, 2.5
Sun Fire X4170 M2	1.2	3.0.9.27	08.04.01.10	2.3

[1] Oracle recommends that customers with OKM 3.0 KMAs upgrade these servers to server firmware 8.4.2.d. Clear the web browser cache before upgrading the server firmware.For OKM 3.0.2 KMAs or Netra SPARC T4-1 KMAs that have been upgraded to OKM 3.1, customers may choose to upgrade these servers to server firmware 8.8.3.b.

[2] Oracle requires that customers who want to migrate their OKM 2.x KMAs to OKM 3.0.2 must first upgrade their server firmware to 1.7.2.

Download ILOM Server Firmware

Use My Oracle Support to download the latest ILOM server firmware.

1. Go to My Oracle Support at: `http://support.oracle.com` and sign in.
2. Click the **Patches & Updates** tab.
3. Click **Product or Family (Advanced)**.
4. In the **Start Typing...** field, type in the product information (for example, "Netra" or "X4170"), and click **Search** to see the latest firmware for each release.

   The firmware distribution is packaged as a zip file. After you download this file, extract it and then extract the firmware package.zip file that it contains (if any). The firmware package is in a pkg file. You upload this file during the upgrade procedure outlined below.

Upgrade the ILOM Server Firmware

Upgrade the ILOM firmware by uploading a new version using the ILOM web GUI.

The firmware update process takes several minutes to complete. During this time, do not perform any other ILOM tasks. When the firmware update process completes, the system will reboot. Be sure you have met the initial requirements for the upgrade. Refer to "Before You Begin the Firmware Update" in the *Oracle ILOM Administrator's Guide for Configuration and Maintenance*. The process for upgrading the firmware is discussed in detail in "Update the Server SP or CMM Firmware Image" in the *Oracle ILOM Administrator's Guide for Configuration and Maintenance*.

1. Log in to the ILOM using the Web based interface. You must have administrator privileges to perform the firmware upgrades.
2. To avoid trouble with service processors that may be in an error state begin by resetting the service processor.
   a. Click **ILOM Administration > Maintenance > Reset SP** and then click **Reset SP**.
   b. Log out and then log back into the ILOM Web based interface. If necessary, the reset can be performed using the serial interface and CLI to the ILOM, then log back into the ILOM Web based interface.
3. Set the **Session Time-out** value to 3 hours (**System Information** tab, then **Session Timeout** tab).
4. Shut down the server.

   For new installs, or FRU situations, before QuickStart you should power down using the **ILOM Web Interface's Remote Control** tab, select the **Remote Power Control** tab and then choose the **Graceful Shutdown** and **Power Off** action. Save this choice to have the server shut down.

   For KMAs that have already been configured (QuickStart procedure), log in to the OKM Console as an Operator and select the `Shutdown KMA` menu option to shut down the KMA.
5. Click **ILOM Administration > Maintenance > Firmware Upgrade**.

6. Click **Enter Firmware Upgrade Mode**, then click **OK**.
7. In the Firmware Upgrade page, either click **Browse** to specify the firmware to upload or enter a URL to upload the firmware.
8. Click **Upload**.
9. In the Firmware Verification page, enable the **Preserve Configuration** option.
10. Click **Start**.
11. Click **OK** to proceed through a series of prompts. The system automatically reboots when the Update Status is 100 percent complete.
12. To verify that the updated firmware has been installed, click **System Information > Firmware**.

Set the Boot Mode for OpenBoot from the ILOM - SPARC KMAs Only

Boot into the OpenBoot firmware so that it can be secured. Securing the OpenBoot firmware can mitigate an attack where the KMA could be booted using an alternate device.

1. Log in to the ILOM web-based interface .Navigate to **Remote Control > Redirection** and click **Launch Redirection**.
2. Navigate to **Host Management > Boot Mode**. In the Script text box enter "setenv auto-boot? false" and click **SAVE**.
3. Navigate to **Host Management > Power Control**. Select **Power On** and click **SAVE** to boot up the host.
4. Switch to the Remote Host Console window and monitor the boot process, where it should stop at the OpenBoot firmware prompt.
5. Proceed to Configure OpenBoot Firmware (SPARC KMAs Only) to verify and update OBP settings.

Launch the BIOS Setup Utility from the ILOM - Sun Fire X4170 M2 Only

Use the ILOM web interface to launch the BIOS.

1. Log in to the ILOM web-based interface. Navigate to **Remote Control > Redirection** and click **Launch Redirection** to launch the Remote Host Console.
2. Navigate to **Host Management >Host Control** for next boot device. Select **BIOS** and then click **Save**.
3. Navigate to **Host Management > Power Control**. Select **Power On** and click **SAVE**. To reboot the system, **Remote Control > Remote Power Control**.
4. In the Remote Host Console, monitor the normal boot messages. When the American Megatrends screen appears, press the **F2** key to launch the BIOS Setup Utility.
5. Proceed to Configure the BIOS (Sun Fire X4170 Server Only) to verify and update BIOS settings.

Use ILOM Security Hardening when you want to harden the ILOM. The table below is organized as displayed in the ILOM Web Interface using ":" to delimit the tab names presented by the ILOM web interface.

ILOM Security Hardening

Take steps to secure the ILOM by following certain configuration guidelines.

Follow the *Oracle ILOM Security Guide* for security hardening of the ILOM (see https://docs.oracle.com/cd/E37444_01/html/E37451/index.html.)

To further secure the KMA, customers may choose to update some ILOM settings (see Configure ILOM FIPS Mode - SPARC KMAs Only).

Use of ILOM FIPS mode is recommended and supported, with or without use of the HMP feature of OKM. Use of HMP enables IPMI 2.0 which does expose the ILOM to some types of attacks, see https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4786.

Configure ILOM FIPS Mode - SPARC KMAs Only

Configure the ILOM to operate in FIPS mode to increase security.

1. Be sure you can physically access the ILOM as network connectivity to the ILOM management port will be removed.
2. To verify Oracle ILOM Remote Host Console client firmware, as instructed in the ILOM FIPS information section of the Security Guide or the *Administrator's Guide for Configuration and Maintenance Firmware*, use Help > About from the Remote Host Console.

   When connected to ILOM 4.0 you see that it supports the newer Remote Host Console client firmware, such as the Plus version:
3. Log in to the ILOM web-based interface. Navigate to **ILOM Administration > Configuration Management**. Perform a backup of the current configuration. This is necessary since the subsequent step for enabling FIPS resets the configuration. The backup will then be used to restore your configuration. Save the password that you assign to the ILOM backup for use during the subsequent restore operation.
4. Enable FIPS mode by navigating to ILOM **Administration > Management Access** then the **FIPS** tab, enable **FIPS** and click **SAVE**.
5. Navigate to ILOM **Administration > Maintenance** and the **Reset SP** tab. Click the **Reset SP** button. You will now lose network connectivity to the ILOM management port. Use a physical console connection to reconfigure the ILOM management connectn.
6. Locate the ILOM backup file saved from the first step of this procedure. Use an editor to change the XML backup files' setting of the FIPS mode from "disabled" to "enabled". The restore operation will fail without this update.
7. Once ILOM network connectivity is configured, log in to the ILOM web-based interface. You should now see that FIPS mode enabled by observing the yellow "F" badge in the upper-right corner of the web interface.

   Navigate to **ILOM Administration > Configuration Management**. Perform a restore of the configuration using the ILOM backup.

8. Verify configuration settings were properly restored.

Table G-2 ILOM Configuration and Security Hardening for ILOM 3.1, 3.2, and 4.0

Navigation Point	Recommended Changes
Remote Control: Redirection	Launch Remote Host Console - This is the typical means for accessing the KMA console. Select the "Use serial redirection" option before launching the Remote Host Console. Once the console launches, the default Devices, Keyboard, and Video settings should be used.
Remote Control: KVMS	KVMS Settings - Use the default settings. Host Lock Settings - Leave this disabled.
Remote Control: Host Storage Device (ILOM 4.0)	Change the Mode setting to "Disabled" to prevent booting from NFS, SAMBA or supplying a Solaris Miniroot package.
Host Management: Power Control	Reset - Whenever possible, it is preferable to use the corresponding OKM console option to reboot the KMA as this provides an OKM audit event. Graceful Reset - Whenever possible, it is preferable to use the corresponding OKM console option to reboot the KMA as this provides an OKM audit event. Immediate Power Off - Whenever possible, it is preferable to use the corresponding OKM console option to shut down the KMA as this provides an OKM audit event. Graceful Shutdown and Power Off - Whenever possible, it is preferable to use the corresponding OKM console option to shut down the KMA as this provides an OKM audit event. Power On - As needed. Power Cycle - As needed. In some cases, a power cycle is necessary for recovery of the hardware security module.
Host Management: Host Control	Use the default settings. For ILOM 4.0, the DIMM sparing feature is irrelevant due to the DIMM configuration. For ILOM 3.1 (4170 KMAs) see ILOM Security Hardening where this setting is manipulated.
Host Management: Keyswitch (ILOM 3.2 only)	The Keyswitch setting may be changed to "Locked" to prevent unauthorized updates to flash devices.
Host Management: TPM (ILOM 3.2 only)	Not yet tested by OKM.
Host Management: Verified Boot (ILOM 4.0)	The Boot Policy may be changed to "Warning" to enable boot verification. See *Securing Systems and Attached Devices in Oracle Solaris 11.3* https://docs.oracle.com/cd/E53394_01/html/E54828 for more information. The following messages may appear on the console on each verified startup, if an SCA 6000 card or Thales nShield Solo module is installed. These messages can be safely ignored: WARNING: Signature verification of module/kernel/drv/sparcv9/mca failed. WARNING: Signature verification of module /kernel/drv/sparcv9/mcactl failed. WARNING: Signature verification of module /kernel/drv/sparcv9/nfp failed.
Host Management: Diagnostics	Use the default settings.
Host Management: Host Domain (ILOM 3.2 only)	Auto Boot should be enabled. Boot Guests may be changed to disabled since OKM does not support hosting guest virtual machines.
Host Management: Host Boot Mode (ILOM 3.2 only)	See Set the Boot Mode for OpenBoot from the ILOM - SPARC KMAs Only. Use the default settings.

Table G-2 (Cont.) ILOM Configuration and Security Hardening for ILOM 3.1, 3.2, and 4.0

Navigation Point	Recommended Changes
System Management: Policy	Use the default settings.
System Management:Diagnostics (ILOM 4.0)	You may change the "HW Change" setting to "Min" to save some time during cold boots.
System Management: Miniroot - (ILOM 4.0)	Use the default setting,
Power Management	Use defaults for all items.
ILOM Administration: Identification	SP Hostname - assign an appropriate host name per customer policy SP System Identifier - assign a meaningful name per customer policy SP System Contact - customer contact information SP System Location - physical rack or other description of location of this server The "Physical Presence Check" should be enabled (default setting) Customer FRU Data: optional but can be used to record existence of a hardware security module in this KMA.
ILOM Administration:Logs	No specific recommendations.
ILOM Administration: Management Access: Web Server	No specific changes are recommended for KMAs, although a security best practice is to change the default port number for HTTPS. Disable use of SSLv2 and SSLv3.
ILOM Administration: Management Access: SSL Certificate	The ILOM uses a default certificate but supports loading an alternate certificate with its corresponding private key for stronger authentication.
ILOM Administration: Management Access: SNMP	For "Settings" the use of SNMPv3 protocol is recommended (v1 and v2c can be disabled) and "Set Requests" can be disabled to prevent configuration changes from happening through SNMP. Refer to the *Oracle ILOM Protocol Management Reference SNMP and IPMI* document for details.
ILOM Administration: Management Access: SSH Server	No specific changes are recommended for KMAs.
ILOM Administration: Management Access: IPMI	This service should be disabled if there are no plans to use IPMI. Leaving this interface open exposes the KMA to attackers knowledgeable of the WS-Management protocols. If the Hardware Management Pack will be enabled in OKM then IPMI must also be enabled.
ILOM Administration: Management Access: CLI	Configure the session timeout as the default allows CLI sessions to remain open indefinitely.
ILOM Administration:Management Access:WS-MAN (ILOM 3.1 only)	The State setting can be disabled.
ILOM Administration: Management Access: Banner Messages	Changing the banner setting to contain the product name is recommended so that users of the ILOM are aware that the key management appliance is not a generic server. Add a connect message. For example: "Oracle Key Manager ILOM Connect" Add a login message. For example: "Oracle Key Manager ILOM"
ILOM Administration:Management Access:FIPS (ILOM 3.2 only)	See Configure ILOM FIPS Mode - SPARC KMAs Only.

Table G-2 (Cont.) ILOM Configuration and Security Hardening for ILOM 3.1, 3.2, and 4.0

Navigation Point	Recommended Changes
ILOM Administration: User Management: Active Sessions	No KMA-specific changes are prescribed.
ILOM Administration: User Management: User Accounts	Use of user accounts and roles is recommended over the default root account. Refer to the "Setting Up and Maintaining User Accounts" section in the *Oracle ILOM Administrator's Guide for Configuration and Maintenance* document.
ILOM Administration: User Management: LDAP, LDAP/SSL, RADIUS, Active Directory	No KMA-specific changes are prescribed. These services can all remain disabled.
ILOM Administration: Connectivity: Network	No KMA-specific changes are prescribed. If HMP will be enabled then see the section HMP Prerequisites for the Local Host Interconnect settings.
ILOM Administration: Connectivity: DNS	No KMA-specific changes are prescribed.
ILOM Administration: Connectivity: Serial Port	No KMA-specific changes are prescribed.
ILOM Administration:Configuration Management	Backups of the ILOM configuration are recommended following this hardening procedure and whenever the configuration is changed.
ILOM Administration:Notifications	No specific OKM recommendations other than if HMP will be enabled then see the section HMP Prerequisites for the Alerts settings.
ILOM Administration: Date and Time: Clock	The ILOM SP clock is not synchronized with the host clock on the server. So that ILOM events can be correlated with server events, the ILOM date and time should be set manually to UTC/GMT time or configured to synchronize with external NTP servers — preferably the same NTP servers used for the KMA server during or after QuickStart.
ILOM Administration: Date and Time: Timezone	The ILOM time zone should be "GMT".
ILOM Administration:Maintenance	No specific OKM guidelines.

Configure the BIOS (Sun Fire X4170 Server Only)

Ensure that the BIOS has specific settings defined to limit access to the KMA.

Launch the BIOS Setup Utility and check the settings whenever you deploy Sun Fire X4170 M2 KMA or upgrade the ILOM firmware on the KMA. If you need to configure the BIOS for a KMA, perform the procedure below. For more information, refer to the *Sun Fire X4170 M2 Server Service Manual*.

1. Launch the BIOS Setup Utility. If the password prompt appears, enter the BIOS password. If you do not know the password, you press Enter to access the BIOS Setup Utility with limited privileges.
2. In the Main menu, verify the UTC time.
3. In the Main menu, set the BIOS supervisor password.
4. In the Security Menu, verify user access.
5. In the Boot Menu, verify boot order.
6. In the Boot menu, select the "Boot Device Priority" using the up and down arrow keys, then press enter.

Look for the name of the KMA's single disk device, such as: HDD:P0-SEAGATE ST95000NSSUN500G102.All other devices listed should be individually selected using arrow keys and disabled.

7. In the Boot menu, select "Option ROM Enable" using the up and down arrow keys and hit enter.
8. In the Boot menu, Select each "Net Option ROM" device (there are 4 numbered Net0 to Net3) using the up and down arrow keys and press enter.
9. In the Boot menu, disable the ability to boot from this device by selecting "Disable" and pressing enter.
10. **Optional**: Disable PCI-E Option ROM for each of the 3 PCI-E slots to mitigate possibility of booting from PCI-E devices. The KMA does not ship with any PCI-E devices that support booting so there is marginal benefit from making this change.
11. Save the BIOS changes.
12. Navigate to the Exit menu.
13. Verify that the system boots correctly and that the supervisor password works for reentering the BIOS Setup Utility.
14. Go to Initial ILOM Configuration to continue the installation.

    Refer to the *Sun Fire X2100 M2 Server Product Notes*, the *Sun Fire X2200 M2 Server Product Notes* for the ILOM, or the *Sun Fire X4170 M2 and X4270 M2 Servers Installation Guide* as appropriate for the server type of the KMA.

> **Note:**
>
> A connection to the NET MGT interface is required to initially configure the servers. Never use the manual procedure for clearing CMOS NVRAM after a KMA has been Quick Started because it resets the clock.

Configure OpenBoot Firmware (SPARC KMAs Only)

Ensure that the OpenBoot firmware has specific settings defined to secure firmware variables.

Boot into the OpenBoot firmware and check settings under whenever you deploy a T8-1, T7-1 or T4-1 KMA or upgrade the ILOM firmware on the KMA. If you need to configure the OpenBoot firmware for a KMA, perform the procedure below. For more information, refer to the SPARC T7 or T8 Series Security Guide section on "Restricting Access(OpenBoot)" or to the OpenBoot™ 4.x Command Reference Manual, and the section on "Setting Security Variables". When you boot into the OpenBoot firmware, a password prompt may appear if you have a password already defined.

1. To display variables:

   ```
   ok printenv
   ```

2. Set a security password to restrict the set of operations that users are allowed to perform:

   ```
   ok password
   ```

> **Caution:**
>
> It is important to remember your security password and to set the security password before setting the security mode. If you forget this password, you cannot use your system; you must then use an ILOM account with sufficient privileges to reset the NVRAM.

You will then be prompted to supply a secure password. The security password you assign must be between zero and eight characters. Any characters after the eighth are ignored. You do not have to reset the system; the security feature takes effect as soon as you type the command.

3. Specify the security mode to either "command" or "full". Full security is the most restrictive and will require the password for any operation, including each time the system boots. For this reason the "command" mode is recommended.

   ```
   ok.setenv security-mode command

   ok
   ```

4. It is recommended that you also specify the number of password attempts:

   ```
   ok setenv security-#badlogins 10
   ```

5. Now boot the system and verify that it boots correctly:

   ```
   ok boot
   ```

6. Log in to the ILOM web-based interface. **Navigate to Host Management>Boot Mode**. In the Script text box enter "setenv auto-boot? true" and click **SAVE**. This configures the host to automatically boot off the default boot device without entering OpenBoot firmware each time it is booted.

7. Go to Initial ILOM Configuration to continue the installation.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z