

## *Overview*





---

# Contents

<b>Product overview. . . . .</b>	<b>1</b>	Login URL and initial user ID . . . . .	22
What's new in this release . . . . .	1	Definitions for <i>HOME</i> and other directory variables . . . . .	25
Supported languages . . . . .	3	Problems with shared browser sessions . . . . .	26
Features overview . . . . .	3	Password policy for IBM Security Key Lifecycle Manager user. . . . .	27
Key serving. . . . .	4	Changing the password policy . . . . .	28
Encryption-enabled 3592 tape drives and LTO tape drives . . . . .	6	Changing a user password . . . . .	28
Enterprise Storage: DS8000 Storage Controller (2107, 242x). . . . .	7	Changing IBM Security Key Lifecycle Manager user password . . . . .	30
IBM System Storage: DS5000 Storage Controller (1818-51A, 1818-53A, and 1814-20A) . . . . .	7	Resetting password on distributed systems . . . . .	31
Backup and restore . . . . .	7	User roles . . . . .	32
Audit. . . . .	7	Release information . . . . .	38
IBM Security Key Lifecycle Manager automated clone replication . . . . .	8	System requirements . . . . .	38
Master key in Hardware Security Modules . . . . .	8	Software prerequisites . . . . .	39
LDAP integration with IBM Security Key Lifecycle Manager server . . . . .	8	Installation images and fix packs . . . . .	41
Server Configuration Wizard . . . . .	9	<b>Notices . . . . .</b>	<b>43</b>
Technical overview . . . . .	9	Terms and conditions for product documentation..	45
Keys overview. . . . .	9	Trademarks . . . . .	46
Main components . . . . .	18	<b>Index . . . . .</b>	<b>47</b>
Backup and restore . . . . .	20		



---

## Product overview

The Product overview topics describe the IBM Security Key Lifecycle Manager product (formerly called IBM Tivoli Key Lifecycle Manager) and its business and technology context.

They include information about:

- Product features and functions
- Technologies and architecture on which the product is based
- The user model and roles underlying the product features
- The graphical interfaces and tools that support various user roles

---

## What's new in this release

IBM Security Key Lifecycle Manager, Version 2.6.0 provides several usability and interoperability improvements for installing, configuring, migrating IBM Security Key Lifecycle Manager infrastructure and processes to locally create and manage the lifecycle of KMIP objects.

### **Operating system independent UI-based replication configuration**

Provides graphical user interface for automated replication configuration. You can configure the replication program to replicate IBM Security Key Lifecycle Manager critical data across clone servers when new keys are added to the master server.

The automated replication process enables cloning of IBM Security Key Lifecycle Manager environments to multiple servers in a manner that is independent of operating systems and directory structure of the server. For example, you can replicate data from a master server on a Windows system to a clone server on a Linux system. You can clone a master IBM Security Key Lifecycle Manager server with up to 20 copies. For more information, see Replication settings for clone and master servers.

### **Operating system independent backup and restore operations**

Supports cross-platform backup and restore functions to protect IBM Security Key Lifecycle Manager critical information. You can create cross-platform compatible backups and restore the same across operating systems. For example, backups on a Linux system can be restored on a Windows system, and vice versa.

You can use the cross-platform backup utility to run backup operation on earlier versions of IBM Security Key Lifecycle Manager to back up critical data. You can restore these backup files on current version of IBM Security Key Lifecycle Manager to an operating system that is different from the one it was backed up from.

You can also configure IBM Security Key Lifecycle Manager to schedule automatic backup operation. You must configure properties only for the master server to back up data at regular intervals. For more information, see Backup and restore.

### **NSA Suite B compliance**

Supports communication over secure sockets in compliance with the US National Security Agency (NSA) Suite B cryptography guidelines to

provide an enhanced level of security. For more information, see “Compliance for NSA Suite B Cryptography in IBM Security Key Lifecycle Manager” on page 10.

**Debug logging settings through the graphical user interface**

Supports configuration of debug logging settings by using the graphical user interface to collect debug information. Debug log files provide additional information to analyze and troubleshoot IBM Security Key Lifecycle Manager problems. For more information, see Specifying settings for debug information.

**Setup for exporting SSL/KMIP Server certificate through the graphical user interface**

Supports the export of SSL/KMIP server certificate to a file in an encoded format by using the graphical user interface. The exported file facilitates faster deployment of the certificate for secure communication with the server. For more information, see Exporting an SSL/KMIP server certificate.

**Server Configuration Wizard to configure IBM Security Key Lifecycle Manager for SSL/TLS handshake**

Includes the Server Configuration Wizard to configure IBM Security Key Lifecycle Manager server and the client device for SSL/TLS handshake. The SSL handshake enables the server and client devices to establish the connection for secure communication. The wizard offers a guided approach to set up the SSL/TLS handshake process. For more information, see Scenario: Setup for SSL handshake between IBM Security Key Lifecycle Manager server and client device.

**Compliance with KIMP 1.2 and Storage Networking Industry Association Secure Storage Industry Forum (SNIA-SSIF) certification**

Conforms to the testing program for the Key Management Interoperability Protocol (KMIP) and other security-related standards of relevance to the storage industry.

**Faster and simpler configuration of KMIP-compliant clients for key management operations**

IBM Security Key Lifecycle Manager provides graphical user interface to create, configure, and search cryptographic objects. These objects are used to serve encryption keys to the KMIP-compliant client devices. For more information about KMIP objects management, see KMIP objects management.

**Installation improvements**

Several improvements are made to the installer to provide more feedback to the user during installation process by performing environment validation and prerequisite checks.

**Automatic generation of AES 256-bit master key for data encryption**

Generates the AES 256-bit master key automatically for data encryption after a successful installation of IBM Security Key Lifecycle Manager. To conform to the PCI DSS standards and for the increased data security, 256-bit length master key is used for encrypting IBM Security Key Lifecycle Manager sensitive data, such as key material.

**Note:**

- Starting with the IBM Security Key Lifecycle Manager Version 2.6 release, the Solaris operating system is not supported.

- The IBM Security Key Lifecycle Manager command-line interface commands will be deprecated in the future versions of IBM Security Key Lifecycle Manager. Use the REST interfaces instead.
- All references to the **alias** property of cryptographic keys and certificates in the graphical user interface, command-line interface, and REST interface will be deprecated in the later versions of IBM Security Key Lifecycle Manager.

---

## Supported languages

IBM Security Key Lifecycle Manager supports various languages. The user interface labels, messages, and values can be displayed in both English language and in languages other than English. However, IBM Security Key Lifecycle Manager supports only the systems that are localized to a single locale.

IBM Security Key Lifecycle Manager supports the following languages:

- English
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Traditional Chinese

---

## Features overview

Use IBM Security Key Lifecycle Manager to manage the lifecycle of the keys and certificates of an enterprise. You can manage symmetric keys, secret keys, asymmetric key pairs, and certificates.

IBM Security Key Lifecycle Manager has the following key features:

- Role-based access control that provides permissions to do tasks such as create, modify, and delete for specific device groups. Most permissions are associated with specific device groups.
- Extension of support to devices by using industry-standard Key Management Interoperability Protocol (KMIP) for encryption of stored data and the corresponding cryptographic key management.

You can use IBM Security Key Lifecycle Manager graphical user interface to create, configure, and search cryptographic objects. These objects are used to serve encryption keys to the KMIP-compliant client devices.

- Serving symmetric keys to DS5000 storage servers

Provide administration and ongoing maintenance of keys that are served to DS5000 storage servers. Restrict the set of machines with which a device such as a disk drive can be associated. You can associate a device to an existing machine in the IBM Security Key Lifecycle Manager database.

- Encrypted keys to one or more devices to which IBM Security Key Lifecycle Manager server is connected.
- Storage of key materials for the self-signed certificates that you generate, private key, and the key metadata in a database.

- Cross-platform backup and restore to protect critical data and other IBM Security Key Lifecycle Manager data, such as the configuration files and current database information.
- Cross-platform backup utility to run backup operation on IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, 2.0.1, 2.5, and IBM Encryption Key Manager, version 2.1. You can restore these backup files on current version of IBM Security Key Lifecycle Manager across operating systems.
- Migration of IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, 2.0.1, 2.5, and IBM Encryption Key Manager, version 2.1 component during installation.
- Audit records based on selected events that occur as a result of successful operations, unsuccessful operations, or both. Installing or starting IBM Security Key Lifecycle Manager writes the build level to the audit log.
- Support for encryption-enabled 3592 tape drives, LTO tape drives, DS5000 storage servers, DS8000 Turbo drives, and other devices.
- Support for using a Hardware Security Module (HSM) to store the master key that is used to protect all passwords and keys that are stored in the database.
- A set of operations to automatically replicate current active files and data across operating systems. This replication enables cloning of IBM Security Key Lifecycle Manager environments on multiple servers in a manner that is independent of operating systems and directory structure of the server.
- Support for the use of LDAP (Lightweight Directory Access Protocol) server for user authentication. You can configure IBM Security Key Lifecycle Manager users in any of the LDAP repositories, such as IBM Security Directory Server or Microsoft Active Directory.
- Server Configuration Wizard to configure IBM Security Key Lifecycle Manager for SSL/TLS handshake. The SSL handshake enables the server and client devices to establish the connection for secure communication.

## Key serving

IBM Security Key Lifecycle Manager enables definition and serving of keys. IBM Security Key Lifecycle Manager also enables definition of keys or groups of keys that can be associated with a device. Different devices require different key types. After you configure devices, IBM Security Key Lifecycle Manager deploys keys to the devices that request them.

### Key group

An IBM Security Key Lifecycle Manager key group contains keys. A key can be a member of only one key group.

On distributed systems, deleting a key group *also deletes all the keys* in the key group.

### Key metadata

Metadata for an IBM Security Key Lifecycle Manager key includes information such as a key alias, algorithm, and activation date.

Metadata might also include a key description, expiration date, retirement date, destroy date, compromise date, key usage, backup time, and state, such as active. IBM Security Key Lifecycle Manager stores the metadata for a key in the IBM Security Key Lifecycle Manager database.

## Key and certificate states

Cryptographic objects, in their lifetime, transition through several states that are a function of how long the keys or certificates are in existence and whether data is protected. Other factors also affect the state of a cryptographic object, such as whether the key or certificate is compromised.

IBM Security Key Lifecycle Manager maintains these cryptographic object states.

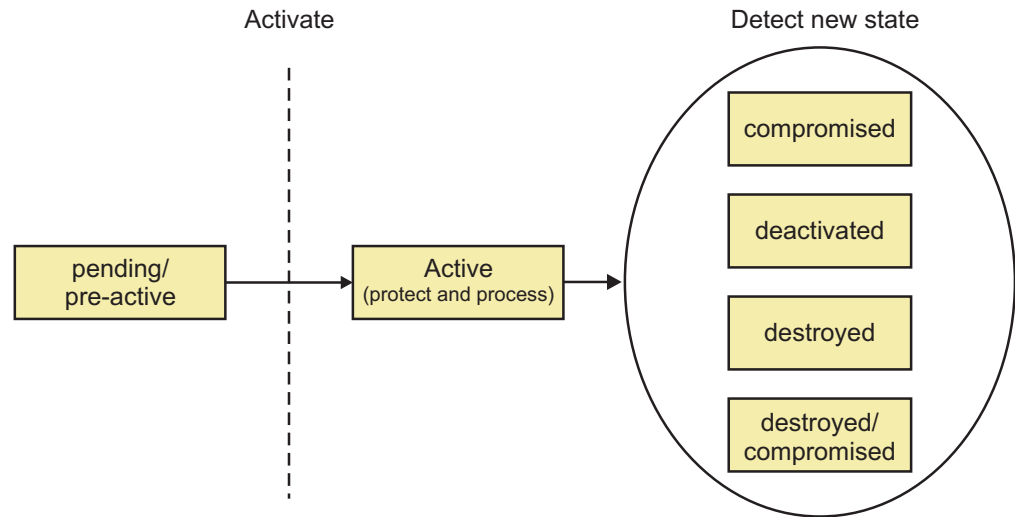


Figure 1. Cryptographic object states

The state of a key or certificate defines the allowed usage:

### pending

A certificate request entry is pending the return of a certificate that is approved and certified by a certificate authority.

### pre-active

Object exists but is not yet usable for any cryptographic purpose, such as migrated certificates with a future use time stamp.

### active

Object is in operational use for protecting and processing data that might use **Process Start Date** and **Protect Stop Date** attributes. For example, protecting includes encryption and signature issue. Processing includes decryption and signature verification.

### compromised

The security of the object is suspect for some reason. A compromised object never returns to an uncompromised state, and cannot be used to protect data. Use the object only to process cryptographically protected information in a client that is trusted to handle compromised cryptographic objects.

IBM Security Key Lifecycle Manager retains the state of the object immediately before it was compromised. To process data that was previously protected, the compromised object might continue to be used.

### deactivated

Object is not to be used to apply cryptographic protection such as encryption or signing. However, if extraordinary circumstances occur, the object can be

used with special permission to process cryptographically protected information. For example, processing includes decryption or verification.

**destroyed**

Object is no longer usable for any purpose. This status causes the object to be removed from the product.

**destroyed-compromised**

Object is no longer usable for any purpose. This status causes the object to be removed from the product.

An object that is no longer active might change states from:

- Deactivated to destroyed.
- Deactivated to compromised.
- Compromised to destroyed-compromised.
- Destroyed to destroyed-compromised.

## **IBM Security Key Lifecycle Manager keystore**

IBM Security Key Lifecycle Manager can store symmetric keys, public keys, private keys, their associated certificate chains, and trusted certificates.

When IBM Security Key Lifecycle Manager generates a new key, the key and the metadata for the key is stored in a key table in the IBM Security Key Lifecycle Manager database. The key material is protected by using a master key. When you create a certificate request, IBM Security Key Lifecycle Manager creates a key entry that is in a pending state.

By using the command-line interface, you can change the information attributes of a key.

## **Encryption-enabled 3592 tape drives and LTO tape drives**

IBM Security Key Lifecycle Manager supports encryption-enabled 3592 tape drives and LTO tape drives. Drives without encryption enablement are not supported.

IBM Security Key Lifecycle Manager supports these drive types:

- 3592 tape drives
  - TS1120 and TS1130 tape drive are enabled to encrypt data.
- LTO tape drives
  - LTO Ultrium 4 tape drive and LTO Ultrium 5 tape drive enabled to encrypt data.

Encryption is run at full line speed in the tape drive after compression.

For information about the devices that IBM Security Key Lifecycle Manager supports, see the Storage Hardware section at <http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html>.

1. Enter IBM Security Key Lifecycle Manager.
2. Select the product version. For example, 2.6.
3. Select the operating system.
4. Click **Submit**.
5. On the Software Product Compatibility Reports page, click **Hardware**.

## Enterprise Storage: DS8000® Storage Controller (2107, 242x)

IBM Security Key Lifecycle Manager supports the DS8000 Storage Controller (IBM System Storage DS8000 Turbo drive).

This support requires the appropriate microcode bundle version on the DS8000 Storage Controller, Licensed Internal Code level 64.20.xxx.0, or higher.

## IBM System Storage®: DS5000 Storage Controller (1818-51A, 1818-53A, and 1814-20A)

IBM Security Key Lifecycle Manager supports the DS5000 storage server (IBM System Storage DS5000).

This support is for DS5000 series storage systems (DS5100, DS5300, and DS5020) with Self-Encrypting Fibre Channel Drives (FDE/SED drives). The optional Full-Disk Encryption Premium Feature must also be purchased and enabled in the storage subsystem. The systems include the following storage controllers:

- 1818-51A, 1818-53A, FC 7358 DS5000 Disk Encryption Activation
- 1814-20A, FC 7410 DS5020 Disk Encryption Activation

See *IBM DS Storage Manager 10.70 Installation and Host Support Guide* for more information in setting the DS5000 storage subsystem to support IBM Security Key Lifecycle Manager.

## Backup and restore

IBM Security Key Lifecycle Manager provides cross-platform backup and restore functions to protect IBM Security Key Lifecycle Manager critical information. You can create cross-platform compatible backups and restore the same across operating systems. For example, backups on a Linux system can be restored on a Windows system, and vice versa.

Use IBM Security Key Lifecycle Manager to protect data with these functions:

### Backup

A backup is a secondary copy of active production information that is used when a recovery copy is needed to get a user back to work. When a disaster occurs, a backup can get the business up and running again. Since backups are focused on constantly changing business information, they are short-term and often overwritten. You might maintain copies of backup files on a secure computer at a geographically separate location.

Depending on your site requirements, you can maintain a replica computer that provides another IBM Security Key Lifecycle Manager server, including a backup of critical data. The replica computer enables quick recovery at times when the primary IBM Security Key Lifecycle Manager server is not available.

### Restore

A restore returns the IBM Security Key Lifecycle Manager server to a known state, by using backed-up production data, such as the IBM Security Key Lifecycle Manager keystore and other critical information.

## Audit

IBM Security Key Lifecycle Manager provides audit records on distributed systems in Common Base Event (CBE) format. The audit records are stored in a flat file in the audit log.

## IBM Security Key Lifecycle Manager automated clone replication

IBM Security Key Lifecycle Manager automated clone replication uses a program to clone a master IBM Security Key Lifecycle Manager server with up to 20 copies.

You can configure the program to replicate keys and also other configuration information, such as when new keys that are rolled over. This program automates the replication of everything that is needed. Automated clone replication ensures continuous key and certificate availability to the encrypting devices.

IBM Security Key Lifecycle Manager provides a set of operations to replicate current active files and data across systems. This replication enables cloning of IBM Security Key Lifecycle Manager environments to multiple servers in a manner that is independent of operating systems and directory structure of the server. For example, you can replicate data from a master server on a Windows system to a clone server on a Linux system. When the automated replication program is run, the following IBM Security Key Lifecycle Manager data is replicated:

- Data in the IBM Security Key Lifecycle Manager database tables.
- All keys materials in the IBM Security Key Lifecycle Manager database.
- IBM Security Key Lifecycle Manager configuration files (except the replication configuration file).

**Note:** This data is taken as part of an IBM Security Key Lifecycle Manager backup. During a replication, the replication configuration file is not backed-up and passed to the clone.

IBM Security Key Lifecycle Manager replication configuration parameters are defined in the `ReplicationSKLMConfig.properties` configuration file. You can use the graphical user interface, command-line interface, or REST interface to change properties of the replication configuration file. You must configure the replication configuration file on all systems that are part of the replication process. Each instance of IBM Security Key Lifecycle Manager is defined as either the *master*, the system that is to be cloned, or a *clone*, the system that the data is being replicated on.

## Master key in Hardware Security Modules

IBM Security Key Lifecycle Manager supports Hardware Security Module (HSM) to store the master key to protect all passwords that are stored in the database.

The HSM adds extra protection to the storage and use of the master key. The master key protects pass phrases that are stored in the product database. The main pass phrase is a password for the keystore that a customer configures in the product to store the keys that are created in IBM Security Key Lifecycle Manager.

## LDAP integration with IBM Security Key Lifecycle Manager server

LDAP (Lightweight Directory Access Protocol) supports the management of user IDs and passwords at an enterprise level instead of management of this data on individual systems. You can integrate IBM Security Key Lifecycle Manager with LDAP user repositories.

You can configure IBM Security Key Lifecycle Manager users in any of the LDAP repositories, such as IBM Security Directory Server or Microsoft Active Directory to

access IBM Security Key Lifecycle Manager server and call server APIs and CLIs. You must add and configure LDAP user repository to the federated repository of WebSphere® Application Server. For more information in LDAP configuration, see LDAP configuration

## Server Configuration Wizard

You can use the Server Configuration Wizard to configure server and the client device for SSL/TLS handshake. The SSL/TLS handshake enables IBM Security Key Lifecycle Manager server and client devices to establish the connection for secure communication.

Immediately after you install IBM Security Key Lifecycle Manager, the only available option is to configure IBM Security Key Lifecycle Manager for SSL/TLS handshake by using the Server Configuration Wizard. To open, click the **Review the configuration parameters and/or create an SSL server certificate** link. The wizard offers a guided approach to set up SSL handshake process. For more information about SSL/TLS handshake, see Scenario: Setup for SSL handshake between IBM Security Key Lifecycle Manager server and client device.

---

## Technical overview

You can use IBM Security Key Lifecycle Manager to create, back up, and manage the lifecycle of keys and certificates that an enterprise uses. You can manage encryption of symmetric keys, asymmetric key pairs, and certificates. IBM Security Key Lifecycle Manager also provides a graphical user interface, command-line interface, and REST interface to manage keys and certificates.

IBM Security Key Lifecycle Manager waits for and responds to key generation or key retrieval requests that arrive through TCP/IP communication. This communication can be from a tape library, tape controller, tape subsystem, device drive, or tape drive.

Major IBM Security Key Lifecycle Manager provides the following features:

- Managing symmetric keys, asymmetric key pairs, and X.509 V3 certificates.
- Managing the creation and lifecycle of keys, which contain metadata on their intended usage.
- For disaster recovery, providing protected backup of critical data. For example, on distributed systems, backup includes cryptographic key data (actual keys and certificates that are managed), metadata about the keys, and configuration files.
- For continuous key and certificate availability to the encrypting devices, providing automated clone replication program to replicate keys and also other configuration information, such as when new keys that are rolled over.
- File-based audit logs that vary, depending on the operating system. On distributed systems, audit logs contain data in a flat file that is based on the Common Base Event (CBE) security event specification. You can also configure IBM Security Key Lifecycle Manager to generate audit records in syslog format and send them to a syslog server.

## Keys overview

An encryption key is typically a random string of bits generated specifically to scramble and unscramble data. Encryption keys are created by using algorithms that are designed to ensure that each key is unique and unpredictable. The longer the key constructed this way, the harder it is to break the encryption code.

IBM Security Key Lifecycle Manager uses two types of encryption algorithms: symmetric algorithms and asymmetric algorithms. Symmetric, or secret key encryption, uses a single key for both encryption and decryption. Symmetric key encryption is used to encrypt large amounts of data efficiently.

Advanced Encryption Standard (AES) keys are symmetric keys that can be three different key lengths (128, 192, or 256 bits). AES is the encryption standard that is recognized and recommended by the US government. The 256-bit keys are the longest allowed by AES. By default, IBM Security Key Lifecycle Manager generates 256-bit AES keys.

Asymmetric, or public/private encryption, uses a pair of keys. Data encrypted using one key can only be decrypted by using the other key in the public/private key pair. When an asymmetric key pair is generated, the public key is typically used to encrypt, and the private key is typically used to decrypt.

IBM Security Key Lifecycle Manager uses both symmetric and asymmetric keys. Symmetric encryption enables high-speed encryption of user or host data. Asymmetric encryption, which is necessarily slower, protects the symmetric key.

### **Federal Information Processing Standard**

The federal government requires all its cryptographic providers to be FIPS 140 certified. This standard is also adopted in a growing private sector community. The certification of cryptographic capabilities by a third party in accordance with government standards are increased value in this security-conscious world.

If you export private keys to a PKCS#12 file, ensure that the file with the key is wrapped by using a FIPS-approved method before the file leaves the computer.

IBM Security Key Lifecycle Manager itself does not provide cryptographic capabilities and therefore does not require or obtain, FIPS 140-2 certification. However, IBM Security Key Lifecycle Manager takes advantage of the cryptographic capabilities of the IBM JVM in the IBM Java Cryptographic Extension component. The capabilities allow the selection and use of the IBMJCEFIPS cryptographic provider, which has a FIPS 140-2 level 1 certification.

For more information about the IBMJCEFIPS provider and its selection and use, see the IBM Security information for Java documentation ([http://www-01.ibm.com/support/knowledgecenter/SSYKE2\\_6.0.0/com.ibm.java.security.component.60.doc/security-component/fips.html](http://www-01.ibm.com/support/knowledgecenter/SSYKE2_6.0.0/com.ibm.java.security.component.60.doc/security-component/fips.html)).

For the procedure on how to configure FIPS, see the following technote: <http://www-01.ibm.com/support/docview.wss?uid=swg21395541>

See the documentation from specific hardware and software cryptographic providers for information about whether their products are FIPS 140-2 certified.

**Note:** Setting the **fips** configuration property to on causes IBM Security Key Lifecycle Manager to use the IBMJCEFIPS provider for all cryptographic functions.

### **Compliance for NSA Suite B Cryptography in IBM Security Key Lifecycle Manager**

You can configure IBM Security Key Lifecycle Manager to comply with standards that are specified by the US National Security Agency (NSA) to define security requirements for encryption.

NSA Suite B requires TLS 1.2 protocol and cipher suites that are configured with a minimum level of security of 128 bits by using ECDSA-256 and ECDSA-384 for client or server authentication. To support the Suite B profile, the following Java system property is provided:

```
com.ibm.jsse2.suiteB=128|192|false
```

When you set the **com.ibm.jsse2.suiteB** system property, IBMJSSE2 ensures adherence to the specified security level. IBMJSSE2 validates that the protocol, keys, and certificates comply with the requested profile. For more information, see [https://www-01.ibm.com/support/knowledgecenter/SSYKE2\\_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/suiteb.html](https://www-01.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/suiteb.html).

To enable Suite B compliance in IBM Security Key Lifecycle Manager, you must configure the SKLMConfig.properties properties file with the following option:

```
suiteB=128|192
```

When you configure **suiteB** with the value 128 or 192, the following properties are added to the properties file or the values are updated if the properties are exist:

```
TransportListener.ssl.protocols=SSL_TLSv2
requireSHA2Signatures=true
autoScaleSignatureHash=true
useThisEKeySize=256(if suiteB is 128)|384(if suiteB is 192)
```

## Configuring IBM Security Key Lifecycle Manager for Suite B compliance

1. Stop the IBM Security Key Lifecycle Manager server. For the instructions see, Starting and stopping the IBM Security Key Lifecycle Manager server on distributed systems.
2. Edit the following property in the *SKLM\_HOME/config/SKLMConfig.properties* file and save the file:

```
suiteB=128|192
```

- The value 128 specifies the 128-bit minimum level of security.
- The value 192 specifies the 192-bit minimum level of security.

You can also use the tklmConfigUpdateEntry CLI command or Update Config Property REST Service to update the SKLMConfig.properties file.

3. Restart the server.

## Key management by using the Key Management Interoperability Protocol

The IBM Security Key Lifecycle Manager server supports Key Management Interoperability Protocol (KMIP) communication with clients for key management operations on cryptographic material. The material includes symmetric and asymmetric keys, certificates, and templates that are used to create and control their use.

The Key Management Interoperability Protocol is part of an Organization for the Advancement of Structured Information Standards (OASIS) standardization project for encryption of stored data and cryptographic key management.

For more information, see Key Management Interoperability Protocol documentation ([http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=kmip](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip)).

You can use the IBM Security Key Lifecycle Manager graphical user interface to manage and control cryptographic materials (objects) that are supported by the server. For more information about how to manage KMIP objects, see KMIP objects management.

## **KMIP profiles supported by IBM Security Key Lifecycle Manager**

IBM Security Key Lifecycle Manager supports the following profiles for KMIP server and client interactions:

- Basic Discover Versions Server Profile
- Basic Baseline Server KMIP Profile
- Basic Secret Data Server KMIP Profile
- Basic Symmetric Key Store and Server KMIP Profile
- Basic Symmetric Key Foundry and Server KMIP Profile
- Basic Asymmetric Key Store Server KMIP Profile
- Basic Asymmetric Key and Certificate Store Server KMIP Profile
- Basic Asymmetric Key Foundry and Server KMIP Profile
- Basic Certificate Server KMIP Profile (except PEM certificate format)
- Basic Asymmetric Key Foundry and Certificate Server KMIP Profile (except PEM certificate format)
- Discover Versions TLS 1.2 Authentication Server Profile
- Baseline Server TLS 1.2 Authentication KMIP Profile
- Secret Data Server TLS 1.2 Authentication KMIP Profile
- Symmetric Key Store and Server TLS 1.2 Authentication KMIP Profile
- Symmetric Key Foundry and Server TLS 1.2 Authentication KMIP Profile
- Asymmetric Key Store Server TLS 1.2 Authentication KMIP Profile
- Asymmetric Key and Certificate Store Server TLS 1.2 Authentication KMIP Profile
- Asymmetric Key Foundry and Server TLS 1.2 Authentication KMIP Profile
- Certificate Server TLS 1.2 Authentication KMIP Profile (except PEM certificate format)
- Asymmetric Key Foundry and Certificate Server TLS 1.2 Authentication KMIP Profile (except PEM certificate format)

For more information about profiles, see KMIP Profiles 1.2 documentation (<http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.pdf>).

## **KMIP attributes for keys and certificates**

IBM Security Key Lifecycle Manager supports the following tasks:

- Following KMIP information about the graphical user interface information:
  - Whether KMIP ports and timeout settings are configured.
  - Current KMIP certificate, indicating which certificate is in use for secure server or server/client communication.
  - Whether SSL/KMIP or SSL is specified for secure communication.
- You can update KMIP attributes for keys and certificates.

For example, you can use the **tklmKeyAttributeUpdate** command to update:

**name**

Specifies the name that is used to identify or locate the object. This attribute is a Key Management Interoperability Protocol attribute.

**applicationSpecificInformation**

Specifies application namespace information as a Key Management Interoperability Protocol attribute.

**contactInformation**

Specifies contact information as a Key Management Interoperability Protocol attribute.

**cryptoParams** *cryptoparameter1, cryptoparameterN*

Specifies the cryptographic parameters that are used for cryptographic operations by using the object. This attribute is a Key Management Interoperability Protocol attribute.

**customAttribute**

Specifies a custom attribute in string format as a Key Management Interoperability Protocol attribute. Client-specific attributes must start with the characters "x-" (x hyphen) and server-specific attributes must start with "y-" (y hyphen).

**link**

Specifies the link from one managed cryptographic object to another, closely related target managed cryptographic object. This attribute is a Key Management Interoperability Protocol attribute.

**objectGroup**

Specifies one or more object group names of which this object might be part. This attribute is a Key Management Interoperability Protocol attribute.

**processStartDate**

Specifies the date on which a symmetric key object can be used for process purposes. You cannot change the value after the date occurs. If you specify a date earlier than the current date, the value is set to the current date. This attribute is a Key Management Interoperability Protocol attribute.

**protectStopDate**

Specifies the date on which an object cannot be used for process purposes. You cannot change the value after the date occurs. If you specify a date earlier than the current date, the value is set to the current date. This attribute is a Key Management Interoperability Protocol attribute.

**usageLimits**

Specifies either total bytes (BYTE) or total objects (OBJECT) as a Key Management Interoperability Protocol attribute. You cannot modify this value once this object is used. For example, **GetUsageAllocation** calls this object.

- List and delete client-registered KMIP templates.

Clients use a template to specify the cryptographic attributes of new objects in a standardized or convenient way. The template is a managed object that contains attributes in operations that the client can set for a cryptographic object. For example, the client can set application-specific information.

**tklmKMIPTemplateList**

List KMIP templates that IBM Security Key Lifecycle Manager provides. For example, you might list all templates.

**tklmKMIPTemplateDelete**

Delete KMIP templates that clients registered with IBM Security Key Lifecycle Manager.

- List and delete secret data such as passwords or a seed that is used to generate keys.

**tklmSecretDataDelete**

Delete secret data that KMIP clients sent to IBM Security Key Lifecycle Manager.

**tklmSecretDataList**

List secret data that KMIP clients sent to IBM Security Key Lifecycle Manager.

- Set default port and timeout properties

**KMIPListener.ssl.port**

Specifies the port on which the IBM Security Key Lifecycle Manager server listens for requests from libraries. The server communicates over the SSL socket by using Key Management Interoperability Protocol.

**TransportListener.ssl.port**

Specifies the port on which IBM Security Key Lifecycle Manager server listens for requests from tape libraries that communicate by using the SSL protocol.

**TransportListener.ssl.timeout**

Specifies how long the socket waits on a read() before closing. This property is used for the SSL socket.

- Enable or disable delete requests from KMIP clients.

An authenticated client can request delete operations that might have a significant impact on the availability of a key, on server performance, and on key security. Specify the `enableKMIPDelete` attribute with either the **tklmDeviceGroupAttributeUpdate** or the **tklmDeviceGroupCreate** command to determine whether IBM Security Key Lifecycle Manager acts on these requests.

**Key serving management**

The IBM Security Key Lifecycle Manager solution assists IBM encryption-enabled devices in generating, protecting, storing, and maintaining encryption keys. You can use keys to encrypt and decrypt information that is written to and read from devices.

IBM Security Key Lifecycle Manager acts as a background process that is waiting for key generation or key retrieval requests sent to it through a TCP/IP communication path between itself and the tape library, tape controller, tape subsystem, device driver, or tape drive. When a drive writes encrypted data, it first requests an encryption key from IBM Security Key Lifecycle Manager.

**AES keys and the 3592 tape drive:**

When a 3592 tape drive writes encrypted data, it first requests an encryption key from IBM Security Key Lifecycle Manager.

On receipt of the request, IBM Security Key Lifecycle Manager generates an Advanced Encryption Standard (AES) key. The key is served to the tape drive in two protected forms:

- Encrypted or wrapped, by using Rivest-Shamir-Adleman (RSA) key pairs. 3592 tape drives write this copy of the key to the cartridge memory and extra places on the tape media in the cartridge for redundancy.
- Separately wrapped for secure transfer to the tape drive where it is unwrapped upon arrival. The key inside is used to encrypt the data that is written to the tape.

When an encrypted tape cartridge is read by a 3592 tape drive, the protected AES key on the tape is sent to IBM Security Key Lifecycle Manager where the wrapped AES key is unwrapped. The AES key is then wrapped with a different key for secure transfer back to the tape drive. The key is unwrapped and used to decrypt the data that is stored on the tape. IBM Security Key Lifecycle Manager also allows protected AES keys to be rewrapped, or rekeyed, by using different RSA keys from the original ones that are used when the tape was written. Rekeying is useful when an unexpected need arises to export volumes to business partners whose public keys were not included. It eliminates rewriting the entire tape and enables the data key of a tape cartridge to be re-encrypted with the public key of a business partner.

### **Asymmetric keys and the 3592 tape drive:**

In addition to 256-bit AES symmetric data keys, IBM Security Key Lifecycle Manager also uses public/private (asymmetric) key cryptography to protect the symmetric data encryption keys. These keys are generated and retrieved as they pass between IBM Security Key Lifecycle Manager and 3592 tape drives.

Public/private key cryptography is also used to verify the identity of the tape drives to which IBM Security Key Lifecycle Manager serves keys.

When a 3592 tape drive requests a key, IBM Security Key Lifecycle Manager generates a random symmetric data encryption key. Use public/private key cryptography to wrap the data encryption key by using a key encryption key, which is the public key of an asymmetric key pair.

The wrapped data key, along with key label information about what private key is required to unwrap the symmetric key, forms a digital envelope, called an externally encrypted data key structure. The structure is stored in the tape header area of any tape cartridge that holds data encrypted by using this method. The key that you use to decrypt the data is stored with the data on the tape itself, protected by asymmetric, public/private key wrapping. The public key that you use to wrap the data key is obtained from one of the following two sources:

- A public key (part of an internally generated public/private key pair) stored in the keystore.
- A certificate (from a business partner, for example) stored in the keystore.

The certificates and keys that are stored in the keystore are the point of control that permits a tape drive or library to decrypt the data on the tape. Without the information in the keystore, the tape cannot be read. It is important to prevent unauthorized users from obtaining the private keys from the keystore. You must always keep the keystore available to you to read the tapes.

The data encryption key is stored *only* on the tape, in a wrapped, protected form. When an encrypted tape is to be read by a 3592 tape drive, the tape drive sends the externally encrypted data key to IBM Security Key Lifecycle Manager. IBM Security Key Lifecycle Manager determines from the alias or key label which

private key encryption key from its keystore to use to unwrap the externally encrypted data key and recover the data encryption key.

After the data encryption key is recovered, it is then wrapped with a different key, which the tape drive can decrypt. The key is then sent back to the tape drive, enabling the tape drive to decrypt the data.

IBM Security Key Lifecycle Manager uses aliases, also known as key labels, to identify the public/private keys that are used to wrap the externally encrypted data key when you encrypt with 3592 tape drives. You can define specific aliases for each tape device by using the IBM Security Key Lifecycle Manager graphical user interface or command-line interface.

IBM Security Key Lifecycle Manager allows the definition of at least two aliases (certificates or key labels) for each encrypting tape drive. The aliases allow access to the encrypted data at another location within your organization or outside it. The private key for one of these aliases must be known. If you do not want to specify two different key labels or aliases, you can define both aliases with the same value.

#### **AES keys and the LTO tape drive:**

When an LTO tape drive writes encrypted data, it first requests an encryption key from IBM Security Key Lifecycle Manager.

Upon receipt of the request, IBM Security Key Lifecycle Manager obtains an existing AES key from a keystore. The key is then wrapped for secure transfer to the tape drive. The key is then unwrapped and used to encrypt the data that is written to the tape.

When an encrypted tape is read by an LTO tape drive, IBM Security Key Lifecycle Manager obtains the required key from the keystore. The key is based on the information in the Key ID on the tape, and serves it to the tape drive wrapped for secure transfer.

#### **Symmetric keys and the LTO tape drive:**

IBM Security Key Lifecycle Manager uses only symmetric data keys for encryption tasks on the LTO tape drive.

When an LTO tape drive requests a key, IBM Security Key Lifecycle Manager uses the alias that is specified for the tape drive. If no alias was specified for the tape drive, IBM Security Key Lifecycle Manager uses an alias from a key group, key alias list, or range of key aliases.

The keys from the key group are used in a round robin fashion to help balance the use of keys more evenly.

The selected alias is associated with a symmetric data key that was preinstalled in the keystore. IBM Security Key Lifecycle Manager sends the data key to the LTO tape drive to encrypt the data. The selected alias is also converted to an entity called data key identifier, which is written to tape with the encrypted data. IBM Security Key Lifecycle Manager can use the data key identifier to identify the correct data key that is required to decrypt the data when the LTO tape is read.

### **AES keys and the DS8000 Turbo drive:**

When the DS8000 Turbo drive starts, the device requests an unlock key from IBM Security Key Lifecycle Manager.

If the DS8000 Turbo drive requests a new key for its unlock key, IBM Security Key Lifecycle Manager generates an Advanced Encryption Standard (AES) key. The key is then served to the drive in the following two protected forms:

- Encrypted (wrapped) by using Rivest-Shamir-Adleman (RSA) key pairs. The DS8000 Turbo drive stores this copy of the key on the array in an unencrypted partition.
- Separately wrapped for secure transfer to the drive where it is unwrapped upon arrival and the key inside is used to unlock the array.

If the DS8000 Turbo drive requests an existing unlock key, the protected AES key on the array is sent to IBM Security Key Lifecycle Manager where the wrapped AES key is unwrapped. The AES key is then wrapped with a different key for secure transfer back to the DS8000 Turbo drive. The key is unwrapped and used to unlock the array.

### **Asymmetric keys and the DS8000 Turbo drive:**

IBM Security Key Lifecycle Manager also uses public/private (asymmetric) key cryptography to protect 256-bit AES symmetric data encryption keys as they pass between IBM Security Key Lifecycle Manager and the DS8000 Turbo drive.

Public/private key cryptography is also used to verify the identity of the tape drives to which IBM Security Key Lifecycle Manager serves keys. When a DS8000 Turbo drive requests a new key, IBM Security Key Lifecycle Manager generates a random symmetric data encryption key. Use public/private key cryptography to wrap the data encryption key by using a key encryption key, which is the public key of an asymmetric key pair.

The wrapped data key, along with key label information about that private key that is required to unwrap the symmetric key, forms a digital envelope, called an externally encrypted data key structure. The structure is stored in the tape header area of any tape cartridge that holds data encrypted using this method. The key that you use to decrypt the data is stored with the data on the tape itself, protected by asymmetric, public/private key wrapping. The public key that is used to wrap the data key is obtained from one of the following two sources:

- A certificate (from a business partner, for example) stored in the keystore.
- A public key (part of an internally generated public/private key pair) stored in the keystore.

The certificates and keys that are stored in the keystore are the point of control that allows a DS8000 Turbo drive to be unlocked. Without the information in the keystore, the DS8000 Turbo drive cannot be unlocked.

You must prevent unauthorized users from obtaining the private keys from the keystore, and to always keep the keystore available to you to unlock the arrays. The data encryption key is stored only on the DS8000 Turbo drive in a wrapped, protected form.

To unlock a DS8000 Turbo drive, the DS8000 Turbo drive sends the externally encrypted data key to IBM Security Key Lifecycle Manager. IBM Security Key

Lifecycle Manager determines from the alias or key label which private key encryption key from its keystore to use to unwrap the externally encrypted data key and recover the data encryption key. After the data encryption key is recovered, it is then wrapped with a different key, which the tape drive can decrypt. The key is sent back to the tape drive to enable the tape drive for data decryption.

IBM Security Key Lifecycle Manager uses aliases, also known as key labels, to identify the public/private keys that you use to wrap the unlocking key. You can define specific aliases for each device. IBM Security Key Lifecycle Manager allows the definition of up to two aliases (certificates or key labels) for each DS8000 Turbo drive to prevent deadlock conditions. IBM Security Key Lifecycle Manager must be on the same system as the DS8000 Turbo drive. The DS8000 Turbo drive must unlock before the IBM Security Key Lifecycle Manager can come up. The private key for one of these aliases must be known. If you do not want to specify two different key labels or aliases, you can define both aliases with the same value.

#### **AES keys and the DS5000 storage server:**

When a DS5000 storage server starts, the device requests a key from IBM Security Key Lifecycle Manager to unlock disk drives.

In response, IBM Security Key Lifecycle Manager obtains an existing AES key from the keystore. IBM Security Key Lifecycle Manager wraps the AES key for secure transfer to the DS5000 storage server, which unwraps and uses the key to unlock disk drives.

#### **Symmetric keys and the DS5000 storage server:**

IBM Security Key Lifecycle Manager uses only symmetric data keys as the unlock key for a DS5000 storage server.

When a DS5000 storage server requests a key, IBM Security Key Lifecycle Manager uses the alias that the request specifies to get the key. If the DS5000 storage server request does not specify an alias, IBM Security Key Lifecycle Manager obtains an alias from the list of keys that are associated with the requesting DS5000 storage server. Keys from the list are served in round robin fashion to balance the use of keys evenly.

The selected alias is associated with a symmetric data key that was preinstalled in the keystore. IBM Security Key Lifecycle Manager sends the symmetric data key to the device to unlock the disk drives of this array. The selected alias is also converted to an entity that is termed a data key identifier, which the DS5000 storage server stores. IBM Security Key Lifecycle Manager can use the data key identifier to identify the correct data key when needed.

## **Main components**

The IBM Security Key Lifecycle Manager solution on distributed systems includes the IBM Security Key Lifecycle Manager server, WebSphere Application Server, and DB2®.

On distributed systems, installing IBM Security Key Lifecycle Manager also installs the prerequisites.

#### **Runtime environment**

- Distributed systems

The WebSphere Application Server runs a Java virtual machine that provides the runtime environment for the application code. The application server provides communication security, logging, messaging, and web services.

#### Database server

IBM Security Key Lifecycle Manager stores key materials in a DB2 relational database. Use IBM Security Key Lifecycle Manager to manage the DB2.

### Deployment on Windows and systems such as Linux or AIX

On Windows systems and other systems such as Linux or AIX, the IBM Security Key Lifecycle Manager installation program deploys the IBM Security Key Lifecycle Manager server and required middleware components on the same computer. You must ensure that the computer has the required memory, speed, and available disk space to meet the workload.

IBM Security Key Lifecycle Manager can run on a member server in a domain controller environment, but is not supported on a primary or backup domain controller.

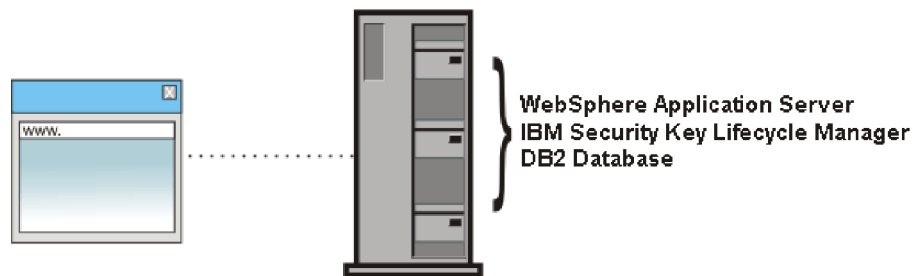


Figure 2. Main components on Windows systems and systems such as Linux or AIX

### Deployment of a primary and replica server

To ensure availability, deploy both a primary IBM Security Key Lifecycle Manager server and, on a separate system, a replica of the primary IBM Security Key Lifecycle Manager server.

On Windows systems and other systems such as Linux or AIX, both computers must have the required memory, speed, and available disk space to meet the workload. The operating system and middleware components must be the same on both computers. The installation paths must also be the same.

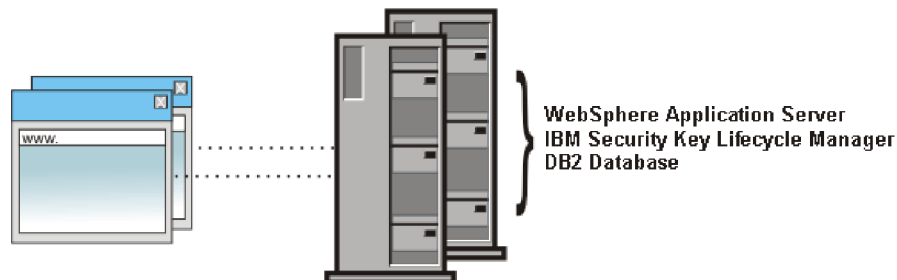


Figure 3. Primary and replica IBM Security Key Lifecycle Manager server

## Replica system requirements

A replica system must have an identical operating system, database, and IBM Security Key Lifecycle Manager application, including critical data from a current IBM Security Key Lifecycle Manager server backup file. The installation paths must also be the same.

Ensure that the same version and fix levels exist on both systems for these requirements:

- Operating system and fixes or patches.
- DB2 and required free disk space. The database must exist on the same system on which the IBM Security Key Lifecycle Manager server runs.
- IBM Security Key Lifecycle Manager server.

You must manually copy the current IBM Security Key Lifecycle Manager server backup file to the replica system. IBM Security Key Lifecycle Manager does not automatically synchronize data between two IBM Security Key Lifecycle Manager servers.

## Backup and restore

Back up and restore tasks provide protection for critical data, and require consideration of your site practices to ensure server availability and runtime capabilities.

IBM Security Key Lifecycle Manager creates backup files in a manner that is independent of operating systems and directory structure of the server. The backup files contain critical data for the current state of the IBM Security Key Lifecycle Manager server. Your site practices must consider how to ensure that key serving is available.

You can use the cross-platform backup utility to run backup operation on earlier versions of IBM Security Key Lifecycle Manager to back up critical data. You can restore these backup files on current version of IBM Security Key Lifecycle Manager to an operating system that is different from the one it was backed up from.

**Note:** Starting with the IBM Security Key Lifecycle Manager version 2.6 release, the Solaris operating system is not supported. If you are using IBM Security Key Lifecycle Manager on Solaris systems, use the cross-platform backup utility to back up the data. You can then run the restore operation to restore data on a IBM Security Key Lifecycle Manager version 2.6 system that is deployed on any of the supported operating systems, such as Windows, Linux, or AIX.

The IBM Security Key Lifecycle Manager backup and restore operations support the use of AES 256-bit key length for data encryption/decryption to conform to the PCI DSS (Payment Card Industry Data Security Standard) standards for increased data security.

The backup and restore operations encrypt or decrypt the data with AES 256-bit length key only when you use AES 256-bit master key for data encryption. You must install Java Cryptography Extension (JCE) unlimited strength jurisdiction policy files if the IBM Security Key Lifecycle Manager backup operation uses AES 256-bit key for data encryption. For installation instructions, see Installing Java Cryptography Extension unlimited strength jurisdiction policy files.

**Note:** In the current version, after you install IBM Security Key Lifecycle Manager, the AES 256-bit master key is generated by default and the JCE unlimited strength jurisdiction policy files are installed in the server.

## **Categories of data in a backup file**

A backup file of IBM Security Key Lifecycle Manager contains critical data. For example, depending on your configuration, it can include the key materials, configuration file, and other information.

The following categories of data require backup protection:

### **IBM Security Key Lifecycle Manager configuration files**

Properties that define selected IBM Security Key Lifecycle Manager activities such as audit settings and other values that you customize for your system configuration.

### **IBM Security Key Lifecycle Manager database**

Data about IBM Security Key Lifecycle Manager objects such as devices, key groups, certificates, key materials, and drives.

## **Backup file security**

Ensure that you do not accidentally corrupt a backup file or misplace its encryption password.

To provide security for backup files:

- Retain a copy of backup files in a location that is not on the IBM Security Key Lifecycle Manager computer, and not in the IBM Security Key Lifecycle Manager directory path. The separate location ensures that other processes cannot remove audit logs and backup files if IBM Security Key Lifecycle Manager is removed.
- Do not edit the files that are in a backup jar file. The files become unreadable.
- Ensure that you retain the password that is used to encrypt a backup file. The same password is required to decrypt and restore the file.

## **Restore**

A restore returns the IBM Security Key Lifecycle Manager server to a known state, by using backed-up production data, such as the IBM Security Key Lifecycle Manager key materials and other critical information.

IBM Security Key Lifecycle Manager supports restore operation across operating systems. You can restore IBM Security Key Lifecycle Manager backup files on an operating system that is different from the one it was backed up from. For example, you can restore a backup that was taken on a Linux system on to a Windows system.

Retrieve a copy of backup files from a location that you specified earlier that is not in the IBM Security Key Lifecycle Manager directory path. You must also know the password that was used to encrypt a backup file. Use the password to decrypt and restore the file on the primary IBM Security Key Lifecycle Manager server.

Before you restore the backup files, ensure that the backup manifest file lists all the IBM Security Key Lifecycle Manager data files in the archive. When you run backup operation, the manifest file is created along with the backup archive.

Before you start a restore task, isolate the system for maintenance. Take a backup of the existing system. You can later use this backup to bring the system back to original state if any issues occur during the restore process. You must restart the

IBM Security Key Lifecycle Manager server immediately after the restore occurs. Verify the environment before you bring the IBM Security Key Lifecycle Manager server back into production.

---

## Login URL and initial user ID

To get started after you install IBM Security Key Lifecycle Manager, obtain the login URL and the initial IBM Security Key Lifecycle Manager administrator user ID and password.

### Access requirements

Install IBM Security Key Lifecycle Manager as an administrator (root user).

You can also install IBM Security Key Lifecycle Manager as a non-root user only on Linux operating system.

### Login URL

Use login URL to access the IBM Security Key Lifecycle Manager web interface. The login URL for the IBM Security Key Lifecycle Manager administrative console is:

`https://ip-address:port/ibm/SKLM/login.jsp`

The value of *ip-address* is an IP address or DNS address of the IBM Security Key Lifecycle Manager server.

The value of *port* is the port number that IBM Security Key Lifecycle Manager server listens on for requests.

If you use an HTTPS address, the default value of the port is 9080:

`https://ip-address:9080/ibm/SKLM/login.jsp`

Do not use a port value greater than 65520.

On Windows systems, the information is on the start menu. Click **Start > All Programs > IBM Security Key Lifecycle Manager 2.6**.

The login URL for the WebSphere Application Server administrative console is:

`https://ip-address:port/ibm/console/logon.jsp`

The value of *ip-address* is an IP address or DNS address of the WebSphere Application Server.

The value of *port* is the port number that WebSphere Application Server listens on for requests.

The default port on the WebSphere Application Server information panel is 9083. During migration, or if the default port has a conflict for other reasons, WebSphere Application Server automatically selects another free port.

The installation complete panel indicates the port that is configured for WebSphere Application Server. The Windows start menu contains an entry to connect to the WebSphere Application Server with the correct port number.

Click **IBM WebSphere > IBM WebSphere Application Server V8.5.5 > Profiles > KLMPProfile > Administrative console**.

## Administrator user IDs and passwords

Installing IBM Security Key Lifecycle Manager provides default administrator user IDs of WASAdmin, SKLMAdmin, and sklmb26.

*Table 1. Administrator user IDs and passwords*

Program	User ID	Password
<b>Distributed systems</b>		
For distributed operating systems, installation must be run by a local administrative ID, which is root for AIX or Linux systems or a member of the Administrators group on Windows systems. Do not use a domain user ID to install IBM Security Key Lifecycle Manager.		
You might have one or more of these user IDs:		
IBM Security Key Lifecycle Manager administrator	<b>SKLMAdmin</b>  As the primary administrator with full access to all operations, this user ID has the klmSecurityOfficer super user role, in the group that is named klmSecurityOfficerGroup. This user ID is not case-sensitive. Alternatively, use <b>sklmbadmin</b> . Use the SKLMAdmin user ID to administer IBM Security Key Lifecycle Manager.  With the SKLMAdmin user ID, you can: <ul style="list-style-type: none"><li>• View and use the IBM Security Key Lifecycle Manager interface.</li><li>• Change the password for the IBM Security Key Lifecycle Manager administrator.</li></ul> However, you cannot: <ul style="list-style-type: none"><li>• Create one or more extra IBM Security Key Lifecycle Manager administrator user IDs.</li><li>• Do WebSphere Application Server administrator tasks such as creating or assigning a role.</li><li>• Start or stop the server.</li></ul>	Specify and securely store a password during installation.

Table 1. Administrator user IDs and passwords (continued)

Program	User ID	Password
WebSphere Application Server administrator	<p><b>WASAdmin</b></p> <p>This user ID is not case-sensitive. Alternatively, use <b>wasadmin</b> or a user ID that you specify during installation.</p> <p>Do not use the:</p> <ul style="list-style-type: none"> <li>• SKLMAdmin user ID to administer WebSphere Application Server.</li> <li>• WASAdmin user ID to administer IBM Security Key Lifecycle Manager. The WASAdmin user ID has no roles to use IBM Security Key Lifecycle Manager.</li> </ul> <p>This administrator user ID is the WebSphere Application Server administrator user ID.</p> <p>With the wasadmin user ID, you can:</p> <ul style="list-style-type: none"> <li>• View and use only the WebSphere Application Server interface.</li> <li>• Create one or more extra IBM Security Key Lifecycle Manager administrator user IDs, groups, and roles.</li> <li>• Reset the password of any IBM Security Key Lifecycle Manager user ID, including the SKLMAdmin administrator.</li> <li>• Start and stop the server.</li> </ul> <p>However, you cannot:</p> <ul style="list-style-type: none"> <li>• Use the IBM Security Key Lifecycle Manager to complete tasks. For example, you cannot create IBM Security Key Lifecycle Manager device groups.</li> <li>• Do other tasks that require access to IBM Security Key Lifecycle Manager data. The wasadmin user ID does <i>not</i> have access to IBM Security Key Lifecycle Manager data as a superuser.</li> </ul>	<p>Specify and securely store a password during installation.</p> <p>Protect the WASAdmin user ID in the same way that you protect the use of the SKLMAdmin user ID. The WASAdmin user ID has authority to reset the SKLMAdmin password and to create and assign permissions to new IBM Security Key Lifecycle Manager users.</p>
The IBM Security Key Lifecycle Manager DB2 database		

Table 1. Administrator user IDs and passwords (continued)

Program	User ID	Password
Instance owner of the database	<p><b>Windows systems and systems such as AIX or Linux:</b> The default value is sk1mdb26. You might specify a different value during installation. The ID is the installation default user ID for the instance owner of the database.</p> <p>Do not specify a user ID greater than eight characters in length.</p> <p>The instance name is also sk1mdb26.</p> <p>If DB2 is on a system such as AIX or Linux, your user ID must be in the bin or root group, or in a separate group in which root is a member.</p> <p>If you use an existing user ID as instance owner of the IBM Security Key Lifecycle Manager database, the user ID cannot own another database instance.</p> <p><b>Note:</b> Do not use a hyphen (-) or underscore character (_) when you specify a user ID for an existing copy of DB2.</p>	<p>Specify and securely store a password during installation. This password is an operating system password. If you change the password on the operating system, you must change this password.</p> <p>For more information, see “Resetting password on distributed systems” on page 31..</p>
Database instance	The administrator ID sk1mdb2 owns a DB2 instance named sk1mdb26.	

## Definitions for *HOME* and other directory variables

You can customize the *HOME* directory for your specific implementation. Make the appropriate substitution for the definition of each directory variable.

The following table contains default definitions that are used in this information to represent the *HOME* directory level for various product installation paths.

The default value of *path* varies for these operating systems, called *distributed systems* for ease in reference. The term “distributed systems” refers to non-mainframe hardware platforms, including personal computers and workstations.

- For Windows systems, the default path is:
  - DB2  
*drive:\Program Files (x86)\IBM*
  - All applications other than DB2  
*drive:\*
- For Linux and AIX systems, /opt is the default path.

Table 2. HOME and other directory variables

Directory variable	Default definition	Description
<i>DB_HOME</i>	<b>Windows systems:</b> <i>drive</i> : \Program Files (x86)\IBM\DB2SKLMV26  <b>AIX and Linux systems:</b> /opt/IBM/DB2SKLMV26	The directory that contains the DB2 application for IBM Security Key Lifecycle Manager.
<i>DB_INSTANCE_HOME</i>	<b>Windows</b> <i>drive</i> \db2adminID  For example, if the value of <i>drive</i> is C: and the default DB2 administrator is sk1mdb26, <i>DB_INSTANCE_HOME</i> is C:\SKLMB26.  <b>Linux and AIX®</b> /home/db2adminID	The directory that contains the DB2 database instance for IBM Security Key Lifecycle Manager.
<i>WAS_HOME</i>	<b>Windows</b> <i>drive</i> : \Program Files (x86)\IBM\WebSphere\AppServer  <b>Linux and AIX</b> <i>path</i> /IBM/WebSphere/AppServer For example: /opt/IBM/WebSphere/AppServer	The WebSphere Application Server home directory.
<i>SKLM_HOME</i>	<b>Windows</b> <i>WAS_HOME</i> \products\sk1m  <b>Linux and AIX</b> <i>WAS_HOME</i> /products/sk1m	The IBM Security Key Lifecycle Manager home directory.
<i>SKLM_INSTALL_HOME</i>	<b>Windows</b> <i>drive</i> : \Program Files (x86)\IBM\SKLMV26  <b>Linux and AIX</b> <i>path</i> /IBM/SKLMV26	The directory that contains the IBM Security Key Lifecycle Manager license and migration files.
<i>IM_INSTALL_DIR</i>	<b>Windows</b> <i>drive</i> : \ProgramData\IBM\Installation Manager  <b>Linux and UNIX</b> /var/ibm/InstallationManager	The directory where IBM Installation Manager is installed.

## Problems with shared browser sessions

You must avoid shared browser sessions that use WebSphere Application Server and IBM Security Key Lifecycle Manager to prevent unpredictable results on the server. When you use multiple browser windows on the same client, the session might be shared.

For example, the session is always shared when you use a Firefox browser. Depending on your registry settings, or how you opened your browser window, the session might also be shared in Internet Explorer.

You must avoid:

- Multiple users who are logged in to the same session.
- Multiple browser windows on the same client to access the same WebSphere Application Server.

## Password policy for IBM Security Key Lifecycle Manager user

The password policy that applies to the password of a new IBM Security Key Lifecycle Manager user is specified by the `SKLM_HOME/config/TKLMPasswordPolicy.xml` file.

The policy does not apply to the initial passwords that are created for default users such as SKLMAdmin. These default users are created during IBM Security Key Lifecycle Manager installation.

The password policy does apply to changes to passwords for default users, and to new and changed passwords for new users. Policy checking is done only when you create or change a user profile. You must assign a role to a new user before that user attempts to log in to IBM Security Key Lifecycle Manager.

The password policy is enabled by default. You can use an XML or ASCII editor to change this file. To disable the policy, change the value of the **enabled** parameter in the policy file to `false`:

```
PasswordPolicy enabled="true"
```

IBM Security Key Lifecycle Manager supports these password rules:

*Table 3. Password rules*

Rule	Default value
Minimum length	6
Maximum length	20
Minimum number of numeric characters	2
Minimum number of alphabetic characters	3
Maximum number of consecutive occurrences of the same character	2
Disallow the presence of the user ID* in the password	Enabled
Disallow the presence of the user name* in the password	Enabled

Table 3. Password rules (continued)

Rule	Default value
<p>* Detection of this value is case-sensitive.</p> <p><b>Note:</b> To specify that the value is not case-sensitive, edit the default password policy and specify <code>CaseInsensitive</code> for the user ID and user name:</p> <pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;PasswordPolicy version="1.0" uuid="" name="Password policy for TKLM" enabled="true"&gt;   &lt;Description/&gt;   &lt;PasswordRules&gt;&lt;![CDATA[&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;PasswordRuleSet version="1.0"&gt;   &lt;MinLengthConstraint Min="6"/&gt;   &lt;MaxLengthConstraint Max="20"/&gt;   &lt;MaxSequentialChars Max="2"/&gt;   &lt;MinAlphabeticCharacters Min="3"/&gt;   &lt;MinDigitCharacters Min="2"/&gt;   &lt;NotUserIDCaseInsensitive/&gt;   &lt;NotUserNameCaseInsensitive/&gt; &lt;/PasswordRuleSet&gt; ]]&gt;&lt;/PasswordRules&gt; &lt;/PasswordPolicy&gt;</pre>	

## Changing the password policy

Use an editor to manually change the password policy that IBM Security Key Lifecycle Manager provides.

### About this task

Ensure that you change only the element and attribute values in the password policy, not the element and attribute names themselves. The password policy applies to changes to passwords for default users, and to new and changed passwords for new users. Policy checking is done only when you create or change a user profile.

### Procedure

1. Before you begin, make a backup copy of the `SKLM_HOME/config/TKLMPasswordPolicy.xml` file in a secure location. If a changed password policy has problems, you can revert to the backup copy.
2. Edit the `TKLMPasswordPolicy.xml` file in a text editor, changing only values of the XML elements and attributes in the password policy.
3. Save the changed file.

The policy change occurs immediately. You do not need to restart the IBM Security Key Lifecycle Manager server.

4. To test the changes, log in to WebSphere Application Server as WASAdmin and create a user profile for a new user.

Confirm that a password that meets the policy is accepted, and that a password that violates the policy is rejected. When done, if necessary, delete the test user profile.

## Changing a user password

The changed password of a user must comply with the password policy that IBM Security Key Lifecycle Manager provides.

## About this task

This task uses the WASAdmin user ID on the WebSphere Integrated Solutions Console to change the password of a user, including the password for the SKLMAdmin user ID.

For more information about the commands that create groups and users, see the IBM WebSphere Application Server documentation ([http://www-01.ibm.com/support/knowledgecenter/SSAW57\\_8.5.5/com.ibm.websphere.nd.iseries.doc/ae/rxml\\_atwimmgt.html](http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.iseries.doc/ae/rxml_atwimmgt.html)).

## Procedure

### 1. Log on to the WebSphere Integrated Solutions Console.

- Graphical user interface:
  - a. On the browser Welcome page, type a user ID of WASAdmin and a password value, such as wasadminpw.
  - b. In the navigation tree, click **Users and Groups > Manage Users**.
- Command-line interface:

In the *WAS\_HOME/bin* directory, start a **wsadmin** session by using Jython. Log on to **wsadmin** with an authorized user ID, such as the WASAdmin user ID. For example, on Windows systems, navigate to the *drive:\Program Files (x86)\IBM\WebSphere\AppServer\bin* directory and type:

  - Windows systems:

```
wsadmin -username WASAdmin -password wasadminpw -lang jython
```
  - Systems such as AIX or Linux:

```
./wsadmin.sh -username WASAdmin -password wasadminpw -lang jython
```

### 2. Change the password for a user.

- Graphical user interface:
  - a. On the **Manage Users > Search for Users** dialog, click **Search**.
  - b. In the search criteria table, double-click a selected user ID. For example, double-click myAdmin as a user ID.
  - c. On the User Properties dialog, change the value of the **Password** and **Confirm password** fields.
  - d. Click **OK**.
- Command-line interface:
  - a. Type updateUser and specify the required values. For example, by using Jython, type on one line:

```
print AdminTask.updateUser('-uniqueName uid=test2,  
o=defaultWIMFileBasedRealm -password secret12 -confirmPassword secret12')
```

Where,
    - uniqueName**  
Specifies the unique name for the user with a password that you want to create. (String, required)  
  
You might use the **searchUsers** command to verify that the name correctly identifies the user before you change the password.
    - password**  
Specifies the password for the user. (String, required)  
  
The new password must comply with the password policy that IBM Security Key Lifecycle Manager provides.

#### **-confirmPassword**

Specifies the password again to validate how it was entered for the password parameter. (String, optional)

### **What to do next**

Next, validate that the user can log in. Log out as WASAdmin. Log in as the user and confirm that the changed password is accepted.

## **Changing IBM Security Key Lifecycle Manager user password**

You can use the IBM Security Key Lifecycle Manager application user ID to change the user password. The changed password must comply with the password policy that IBM Security Key Lifecycle Manager provides.

### **About this task**

For more information about the commands to change passwords, see the IBM WebSphere Application Server documentation ([http://www-01.ibm.com/support/knowledgecenter/SSAW57\\_8.5.5/com.ibm.websphere.nd.iseries.doc/ae/rxml\\_atwimmgt.html](http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.iseries.doc/ae/rxml_atwimmgt.html)).

### **Procedure**

1. Navigate to the appropriate page or directory:
  - Command-line interface:
    - In the *WAS\_HOME/bin* directory, start a wsadmin session by using Jython. Log on to wsadmin with an authorized user ID.

#### **Windows**

Navigate to the C: \Program Files (x86)\IBM\WebSphere\AppServer\bin directory and type:

```
wsadmin.bat -username <SKLM user> -password <SKLM user passwd>
-lang jython
```

#### **AIX or Linux**

Navigate to the /opt/IBM/WebSphere/AppServer/bin directory and type:

```
./wsadmin.sh -username <SKLM user> -password <SKLM user passwd>
-lang jython
```

- Graphical user interface:
    - Log on to the graphical user interface.
2. Change the password for a user.
    - Command-line interface:
      - Run the following command:

#### **Example:**

```
AdminTask.changeMyPassword('[-oldPassword skladmin -newPassword
Ibm12one
-confirmNewPassword Ibm12one]')
```

- Graphical user interface:
  - a. On the header bar, click the **<SKLM User>** link.
  - b. Click **Change Password**.

- c. In the Change Password dialog, type your **Current password**.
- d. Type your **New password**.
- e. Enter the new password again in the **Confirm new password** field.
- f. Click **Change Password**.

## Resetting password on distributed systems

You must be the administrator to reset a password for the IBM Security Key Lifecycle Manager or WebSphere Application Server.

### About this task

You can reset the password on the computer on which IBM Security Key Lifecycle Manager runs. Use these steps only when the password of the user is lost. In all other cases, use the graphical user interface to update the password.

### Procedure

1. Log in with the a local administrator user ID.
2. Back up the *WAS\_HOME/profiles/KLMProfile/config/cells/SKLMCell/fileRegistry.xml* file. Changing the value of the password changes this registry file.
3. Change the password.
  - Windows systems
    - a. Start a **wsadmin** session by using the Jython syntax. For example, type:  
`WAS_HOME/bin/wsadmin -conntype none -profileName KLMProfile -lang jython`
    - b. Reset the password for the SKLMAdmin user ID:  
`wsadmin>print AdminTask.changeFileRegistryAccountPassword ('-userId SKLMAdmin -password newpassword')`
  - Note:
    - Only the WASAdmin user ID or another user ID with WebSphere Application Server administrator authority can change passwords by using the **AdminTask.changeFileRegistryAccountPassword** command.
    - Passwords that you create by using the **AdminTask.changeFileRegistryAccountPassword** command are not validated against the configured password policy that IBM Security Key Lifecycle Manager provides.

After a lost password reset, the user must set the password by using the graphical user interface.
  - c. Save the change and exit:  
`wsadmin>print AdminConfig.save()`  
`wsadmin>exit`
  - Systems such as Linux or AIX
    - a. Start a **wsadmin** session by using the Jython syntax. For example, type on one line:  
`WAS_HOME/bin/wsadmin.sh -conntype none -profileName KLMProfile -lang jython`
    - b. Reset the password for the SKLMAdmin user ID:  
`wsadmin>print AdminTask.changeFileRegistryAccountPassword ('-userId SKLMAdmin -password newpassword')`

**Note:**

- Only the WASAdmin user ID or another user ID with IBM Security Key Lifecycle Manager administrator authority can change passwords by using the **AdminTask.changeFileRegistryAccountPassword** command.
  - Passwords that you create by using the **AdminTask.changeFileRegistryAccountPassword** command are not validated against the configured password policy that IBM Security Key Lifecycle Manager provides.  
After a lost password reset, the user must set the password by using the graphical user interface.
- c. Save the change and exit:
- ```
wsadmin>print AdminConfig.save()
wsadmin>exit
```
4. Stop and start the server.
- Stop
 

**On Windows systems:**

```
stopServer.bat server1
```

**On systems such as Linux or AIX:**

```
./stopServer.sh server1
```
  - Start
 

**On Windows systems:**

```
startServer.bat server1
```

**On systems such as Linux or AIX:**

```
./startServer.sh server1
```
5. Verify that you can log in as the specified administrator with the new password.

## User roles

IBM Security Key Lifecycle Manager provides a super user (klmSecurityOfficer and klmGUICLIAccessGroup) role and the means to specify more limited administrative roles to meet the needs of your organization. By default, the SKLMAAdmin user ID has the klmSecurityOfficer role.

For backup and restore tasks, IBM Security Key Lifecycle Manager also installs the klmBackupRestoreGroup to which no user IDs initially belong. Installing IBM Security Key Lifecycle Manager creates predefined administrator, operator, and auditor groups to manage LTO tape drives.

The WASAdmin user ID has the authority to create and assign these roles, and to change the password of any IBM Security Key Lifecycle Manager administrator. To set administration limits for IBM Security Key Lifecycle Manager, use the WASAdmin user ID on the WebSphere Integrated Solutions Console to create roles, users, and groups. Assign roles and users to a group. For example, you might create a group and assign both users and a role that limits user activities to administer only LTO tape drives. You must assign a role to a new user before that user attempts to log in to IBM Security Key Lifecycle Manager.

Before you begin, complete the following tasks:

- Determine the limits on device administration that your organization requires.  
For example, you might determine that a specific device group has its own administration.

- Estimate how many administrative users might be needed over an interval of time. For ease of use, consider specifying a group and a role to specify their tasks.

For example, you might specify a group that has a limited range of permissions to manage only 3592 tape drives.

### Relations between users, groups, roles, and protected objects

To do useful work on protected objects, an IBM Security Key Lifecycle Manager user must have one or more roles. The role must enable an action such as create an object, such as a device, in the LTO device family.

A user can be a member of a group. A group might have one or more roles. A role specifies authorization for an operation on protected objects. For example, protected objects include devices, device groups, cryptographic objects (certificates, keys, key pairs, and key groups), and rollover settings for certificates and key groups.

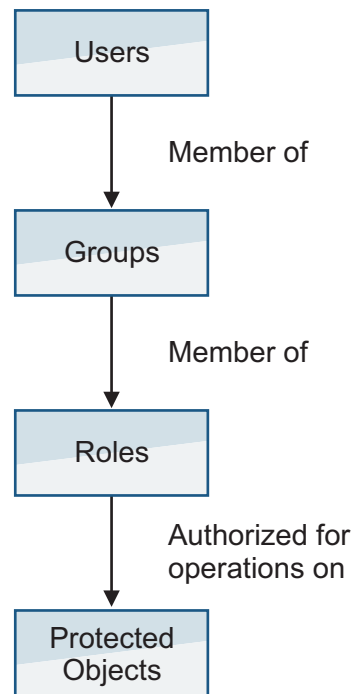


Figure 4. Relations between users, groups, roles, and protected objects

You can use WebSphere Integrated Solutions Console to create child groups with different permissions within a parent group. However, IBM Security Key Lifecycle Manager recognizes the permissions of only the parent group, not the permissions of its child groups.

### Available permissions

Installing IBM Security Key Lifecycle Manager creates the SKLMAdmin user ID, which has the klmSecurityOfficer role as the default super user. The installation process also deploys predefined permissions to the WebSphere Application Server list of administrative roles.

A *permission* from IBM Security Key Lifecycle Manager enables an action or the use of a device group. A *role* in IBM Security Key Lifecycle Manager is one or more

permissions. However, in the WebSphere Application Server graphical user interface, the term *role* includes both IBM Security Key Lifecycle Manager permissions and roles.

**Note:** Installation creates these default groups:

#### **klmSecurityOfficerGroup**

Installation assigns the klmSecurityOfficer role to this group. The klmSecurityOfficer role replaces the previous klmApplicationRole role in the group that was named klmGroup. klmSecurityOfficerGroup replaces klmGroup.

The klmSecurityOfficer role has:

- Root access to the entire set of permissions and device groups that are described in Table 4 and Table 5 on page 35.
- Permission to any role or device group that might be created.
- The suppressmonitor role.

The WebSphere Application Server provides the suppressmonitor role to hide tasks in the left pane of the WebSphere Integrated Solutions Console that an IBM Security Key Lifecycle Manager administrator does not use. Hidden items are associated with the application server, including WebSphere Application Server administrative tasks in the Security, Troubleshooting, and Users and Groups folders.

#### **klmBackupRestoreGroup**

Back up and restore IBM Security Key Lifecycle Manager.

#### **LTOAdmin**

Administer devices in the LTO device family with actions that include create, view, modify, delete, get (export), back up, and configure.

#### **LTOOperator**

Operate devices in the LTO device family with actions that include create, view, modify, and back up.

#### **LTOAuditor**

Audit devices in the LTO device family with actions that include view and audit.

#### **klmGUICLIAccessGroup**

Provides IBM Security Key Lifecycle Manager graphical user interface and command-line interface access to the users. Every product user must be a part of this group.

**Note:** Along with this access to the group, the users must be provided other accesses to be a functional product user.

A user who has any one of the permissions in Table 4 can view:

- IBM Security Key Lifecycle Manager global configuration parameters that are defined in the SKLMConfig.properties file.
- The key server status and last backup date.

*Table 4. Permissions for actions*

| Permission | Enables these actions                           | Unrelated to device groups | Associated with device groups |
|------------|-------------------------------------------------|----------------------------|-------------------------------|
| klmCreate  | Create but not view, modify, or delete objects. |                            | ✓                             |

Table 4. Permissions for actions (continued)

| Permission          | Enables these actions                                                                                                                                                     | Unrelated to device groups | Associated with device groups |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-------------------------------|
| klmDelete           | Delete objects, but not view, modify, or create objects.                                                                                                                  |                            | ✓                             |
| klmGet              | Export a key or certificate for a client device.                                                                                                                          |                            | ✓                             |
| klmModify           | Modify objects, but not view, create, or delete objects.                                                                                                                  |                            | ✓                             |
| klmView             | View objects, but not create, delete, or modify objects. For example, you must have this permission to see the tasks you want to do on the graphical user interface.      |                            | ✓                             |
| klmAdminDeviceGroup | Administer. Create a device group, set default parameters, view, delete an empty device group. This permission does not provide access to devices, keys, or certificates. | ✓                          |                               |
| klmAudit            | View audit data by using the <b>tklmServedDataList</b> command.                                                                                                           | ✓                          |                               |
| klmBackup           | Create and delete a backup of IBM Security Key Lifecycle Manager data.                                                                                                    | ✓                          |                               |
| klmConfigure        | Read and change IBM Security Key Lifecycle Manager configuration properties, or act on SSL certificate. Add, view, update, or delete the keystore.                        | ✓                          |                               |
| klmRestore          | Restore a previous backup copy of IBM Security Key Lifecycle Manager data.                                                                                                | ✓                          |                               |

The klmSecurityOfficer role also has root access to permissions for all device groups.

Table 5. Device groups

| Permission       | Allows actions on these objects |
|------------------|---------------------------------|
| LTO              | LTO device family               |
| TS3592           | 3592 device family              |
| DS5000           | DS5000 device family            |
| DS8000           | DS8000 device family            |
| BRCD_ENCRYPTOR   | BRCD_ENCRYPTOR device group     |
| ONESECURE        | ONESECURE device group          |
| ETERNUS_DX       | ETERNUS_DX device group         |
| XIV              | XIV device group                |
| IBM_SYSTEM_X_SED | IBM_SYSTEM_X_SED device group   |

Table 5. Device groups (continued)

| Permission                         | Allows actions on these objects                                                                                  |
|------------------------------------|------------------------------------------------------------------------------------------------------------------|
| IBM Spectrum Scale (formerly GPFS) | IBM Spectrum Scale device group                                                                                  |
| GENERIC                            | Objects in the GENERIC device family.                                                                            |
| <i>userdevicegroup</i>             | A user-defined instance such as myLT0 that you manually create, based on a predefined device family such as LTO. |

## Multiple permissions

To work on devices, a user must have permissions for one or more actions and one or more device groups.

Errors occur if a user has:

### Action permissions, but no device group permission

For example, the user has the set of action permissions that include view, create, modify, delete. However, the user has no device group permission to receive an action.

### Device group permissions, but no action permission

For example, the user has device group permissions that include LT0 and 3592. However, the user has no action permission to take against a device group.

### A new role for a new device group, but no action permissions

For example, the user has a new role myLT0 that was created for a new device group named myLT0. However, the user has no other action permissions.

Permissions might be:

- Directly assigned.

For example, your role as a user might have view and modify permissions for a specific device group.

- Obtained by group membership.

Permissions are specific to a device group. You might be a member of two user groups. For example, membership in one user group might grant view and modify permissions for use with an LTO device group. A second user group might grant view, create, and modify permissions for use with a 3592 device group. You can view and modify a device in either device group. However, you can complete a create action only for devices in the 3592 device group.

Data such as keys and certificates are associated with a device group. Such data is visible only in graphic user interface pages for the device group to which the data is associated. A user with permissions to several device groups can change the association of data from one device group to another for which the user holds appropriate permissions.

Some properties or attributes in the IBM Security Key Lifecycle Manager database are associated with device groups. For example, the **symmetricKeySet** attribute in the IBM Security Key Lifecycle Manager database is associated with the predefined LTO device group. To change the attribute, your role must have a permission to the modify action and a permission to the LTO device group.

## Predefined groups to manage LTO tape drives

Installing IBM Security Key Lifecycle Manager creates predefined administrative groups to manage LTO tape drives. You can use these groups as a model to define similar administrative groups for other device groups.

### LTOAdmin group:

You can use membership in the LTOAdmin group to administer devices in the LTO device family with actions that include create, view, modify, delete, get (export), back up, and configure.

This group includes the following permissions:

*Table 6. Permissions for actions*

| Permission      | Enables these actions                                                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| LTO             | LTO device family                                                                                                                                    |
| klmCreate       | Create but not view, modify, or delete objects.                                                                                                      |
| klmDelete       | Delete objects, but not view, modify, or create objects.                                                                                             |
| klmGet          | Export a key or certificate for a client device.                                                                                                     |
| klmModify       | Modify objects, but not view, create, or delete objects.                                                                                             |
| klmView         | View objects, but not create, delete, or modify objects.                                                                                             |
| klmAudit        | View audit data by using the <b>tklmServedDataList</b> command.                                                                                      |
| klmBackup       | Create and delete a backup of IBM Security Key Lifecycle Manager data.                                                                               |
| klmConfigure    | Read and change IBM Security Key Lifecycle Manager configuration properties, or act on SSL certificate.                                              |
| suppressmonitor | Hide tasks in the left pane of WebSphere Integrated Solutions Console that an IBM Security Key Lifecycle Manager administrator does not need to use. |

### LTOOperator group:

You can use membership in the LTOOperator group to operate devices in the LTO device family with actions that include create, view, modify, and back up.

This group includes the following permissions:

*Table 7. Permissions for actions*

| Permission | Enables these actions                                    |
|------------|----------------------------------------------------------|
| LTO        | LTO device family.                                       |
| klmCreate  | Create but not view, modify, or delete objects.          |
| klmModify  | Modify objects, but not view, create, or delete objects. |
| klmView    | View objects, but not create, delete, or modify objects. |

Table 7. Permissions for actions (continued)

| Permission      | Enables these actions                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| k1mBackup       | Create and delete a backup of IBM Security Key Lifecycle Manager data.                                                                                   |
| suppressmonitor | Hide tasks in the left pane of the WebSphere Integrated Solutions Console that an IBM Security Key Lifecycle Manager administrator does not need to use. |

### LTOAuditor group:

You can use membership in the LTOAuditor group to audit devices in the LTO device family with actions that include view and audit.

This group includes the following permissions:

Table 8. Permissions for actions

| Permission      | Enables these actions                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| LTO             | LTO device family.                                                                                                                                       |
| k1mView         | View objects, but not create, delete, or modify objects.                                                                                                 |
| k1mAudit        | View audit data by using the <b>tk1mServedDataList</b> command.                                                                                          |
| suppressmonitor | Hide tasks in the left pane of the WebSphere Integrated Solutions Console that an IBM Security Key Lifecycle Manager administrator does not need to use. |

## WebSphere Application Server roles

WebSphere Application Server provides roles that you might need to use. For example, you might need to view or change the WebSphere Application Server configuration. You might assign users and groups to administrative user roles and administrative group roles.

The roles include monitor, configurator, operator, administrator, security manager, and other roles.

For more information, search for *administrative roles* in the WebSphere Application Server documentation ( [http://www-01.ibm.com/support/knowledgecenter/SSAW57\\_8.5.5/com.ibm.websphere.home.doc\\_wasinfo\\_v8r5/welcome\\_ic\\_home.html](http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.home.doc_wasinfo_v8r5/welcome_ic_home.html)).

## Release information

The Release information topics describe information that is specific to this release of IBM Security Key Lifecycle Manager.

## System requirements

Your environment must meet the minimum system requirements to install IBM Security Key Lifecycle Manager.

For information about hardware and software requirements, see the “Installing and configuring” section on IBM Knowledge Center for IBM Security Key Lifecycle Manager. The hardware and software requirements that are published are accurate at the time of publication.

Alternatively, see the detailed system requirements document at <http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html>.

1. Enter IBM Security Key Lifecycle Manager.
2. Select the product version. For example, 2.6.
3. Select the operating system.
4. Click **Submit**.

## Software prerequisites

IBM Security Key Lifecycle Manager has these software prerequisites:

### Java Runtime Environment (JRE) requirements

The IBM Security Key Lifecycle Manager requirement for a version of Java Runtime Environment depends on which operating system is used.

#### On distributed systems:

IBM Java Runtime Environment that is included with WebSphere Application Server.

On all systems, use of an independently installed development kit for Java™, from IBM® or other vendors, is *not* supported.

### Runtime environment requirements

The IBM Security Key Lifecycle Manager requirement for a runtime environment depends on which operating system is used.

#### On distributed systems:

WebSphere Application Server 8.5.5.7 and any applicable fix pack or APAR requirements.

IBM Security Key Lifecycle Manager includes and installs WebSphere Application Server. During installation, IBM Security Key Lifecycle Manager modifies WebSphere Application Server. This modification might cause problems with products that use the same server when you uninstall IBM Security Key Lifecycle Manager. To avoid these issues:

- Do not install IBM Security Key Lifecycle Manager in a WebSphere Application Server instance that another product provides.
- Do not install another product in the instance of WebSphere Application Server that IBM Security Key Lifecycle Manager provides.

### Database authority and requirements

The IBM Security Key Lifecycle Manager requirement for a database depends on which operating system is used.

#### • Distributed systems:

DB2 Workgroup Server Edition on the same computer on which the IBM Security Key Lifecycle Manager server runs:

- Version 10.5.0.6 and the future fix packs on other distributed operating systems that IBM Security Key Lifecycle Manager supports.

**Note:**

- You must use IBM Security Key Lifecycle Manager to manage the database. To avoid data synchronization problems, do not use tools that the database application might provide.
- For improved performance of DB2 Version 10.5.0.6 on AIX systems, ensure that you install and configure the I/O completion ports (IOCP) package that is described in the DB2 documentation ([http://www-01.ibm.com/support/knowledgecenter/SSEPGG\\_10.5.0/com.ibm.db2.luw.admin.perf.doc/doc/t0054518.html](http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.perf.doc/doc/t0054518.html)).
- If an existing copy of DB2 Workgroup Server Edition was installed as the root user at the correct version for the operating system, you can use the existing DB2 Workgroup Server Edition. IBM Security Key Lifecycle Manager installer does not detect the presence of DB2. You must specify the DB2 installation path.

For more information about DB2 prerequisites, see DB2 documentation ([http://www-01.ibm.com/support/knowledgecenter/SSEPGG\\_10.5.0/com.ibm.db2.luw.admin.cmd.doc/doc/r0059710.html](http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.cmd.doc/doc/r0059710.html)).

**DB2 kernel settings**

Ensure that kernel settings are correct for those operating systems, such as the Linux operating system, that requires updating.

Before you install the application, see the DB2 documentation on these web sites for these additional kernel settings:

**AIX systems**

None required.

**Linux systems**

For more information about modifying kernel parameters for DB2 Workgroup Server Edition, version 10.5.0.6 on other supported Linux systems, see DB2 documentation ([http://www-01.ibm.com/support/knowledgecenter/SSEPGG\\_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html](http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html)).

**Window systems**

None required.

**DB2 buffer pool tuning for large-scale environments**

You might need to tune the DB2 buffer pool settings for large-scale environments.

Use these settings:

```
db2 alter bufferpool TKLMBP_LG immediate size 1000 automatic
#---
#--- Use one of the following two statements:
#--- If you migrate from IBM Security Key Lifecycle Manager Version 1,
#--- specify the next statement:
db2 alter bufferpool TKLMBP_4K_IDX immediate size 1000 automatic
#--- Otherwise, omit the statement.

#--- However, if NO migration occurs, specify the next statement:
db2 alter bufferpool TKLMBP_4K_LG_IDX immediate size 1000 automatic
#--- Otherwise, omit the statement.

#---
db2 alter bufferpool TKLMBP_8K_LG immediate size 1000 automatic
db2 alter bufferpool TKLMBP_32K_LG immediate size 1000 automatic
db2 alter bufferpool TKLMBP_SM immediate size 1000 automatic
```

```
db2 alter bufferpool TKLMBP_IDX immediate size 1000 automatic
db2 alter bufferpool TKLMBP_32K_IDX immediate size 1000 automatic
db2 alter bufferpool TKLMBP_SCH immediate size 1000 automatic
```

## Installation images and fix packs

For distributed systems, obtain IBM Security Key Lifecycle Manager installation files and fix packs by using the IBM Passport Advantage® website. You can also obtain the files by another means, such as a DVD as provided by your IBM sales representative.

The Passport Advantage website provides packages, referred to as eAssemblies, for various IBM products.

The Fix Central website provides fixes and updates for software, hardware, and operating system of your system. IBM Security Key Lifecycle Manager fix packs are published on the Fix Central website.

The “Installing and configuring” section on IBM Knowledge Center for IBM Security Key Lifecycle Manager provides instructions for installing and configuring IBM Security Key Lifecycle Manager and the prerequisite middleware products.



---

## Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. \_enter the year or years\_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

---

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

### Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

### Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

### Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

**Rights** Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR

IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

---

## Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



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

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

---

## Index

### Special characters

*DB\_HOME*, default directory 25  
*DB\_INSTANCE\_HOME*, default directory 25  
*SKLM\_HOME*, default directory 25  
*SKLM\_INSTALL\_HOME*, default directory 25  
*WAS\_HOME*, default directory 25

### Numerics

3592  
    device group 33  
    encryption 14, 15

### A

active, state 5  
administrator  
    DB2 22  
    groups 33  
    IBM Security Key Lifecycle Manager 22  
    klmBackupRestoreGroup 32  
    klmGUICLIAccessGroup 32  
    klmSecurityOfficer 32  
    limiting available tasks 32  
    LTOAdmin 33  
    LTOAuditor 33  
    LTOOperator 33  
    password  
        authority to reset 31  
        resetting 31  
    password policy, changing 28  
    password, changing 29  
    predefined groups 32  
    protected objects 33  
    roles 33  
    SKLMAdmin 32  
    SKLMAdmin user ID 32  
    WASAdmin 32  
    WebSphere Application Server 22  
Advanced Encryption Standard 14  
AES keys, encryption 14, 16, 17, 18  
asymmetric keys 15  
audit  
    Common Base Event (CBE) format 8  
    overview 8  
    W7 format 8  
authority  
    SYSADM for database 39  
    SYSCTRL for database 39  
    SYSMAINT for database 39  
automated clone replication 8

### B

backup and restore  
    configuration files 21

backup and restore (*continued*)  
    database 21  
    klmBackupRestoreGroup 32  
    known state 21  
    overview 7, 20  
    security  
        backup file, do not edit 21  
        password 21  
BRCD\_ENCRYPTOR device group 33  
bufferpool settings, DB2 40

### C

change  
    password policy 28  
component  
    DB2 19  
    IBM Security Key Lifecycle Manager server 19  
    replica server 19  
    WebSphere Application Server 19  
components  
    IBM Security Key Lifecycle Manager 18  
compromised, state 5  
configuration files, backup and restore 21  
corruption, backup file 21  
cross-platform  
    backup 8  
    restore 8  
cryptographic 10, 11

### D

database  
    backup and restore 21  
    replica server, same as primary 20  
    requirement, distributed systems 39  
    SYSADM, SYSCTRL, or SYSMAINT authority 39  
DB2  
    bufferpool settings 40  
    documentation website 40  
    kernel settings 40  
    sklmdb2  
        instance name 22  
        instance owner 22  
deployment  
    DB2 19  
    IBM Security Key Lifecycle Manager server 19  
    replica server 19  
    WebSphere Application Server 19  
device groups  
    3592 33  
    BRCD\_ENCRYPTOR 33  
    DS5000 33  
    DS8000 33  
    ETERNUS\_DX 33

device groups (*continued*)  
    LTO 33  
    ONESECURE 33  
    XIV 33  
directory  
    *DB\_HOME* default 25  
    *DB\_INSTANCE\_HOME* default 25  
    *SKLM\_HOME* default 25  
    *SKLM\_INSTALL\_HOME*, default 25  
    *WAS\_HOME* default 25  
    default definitions 25  
domain controller, unsupported for installation 19  
DS5000  
    device group 33  
    encryption 18  
DS8000  
    device group 33  
    encryption 17

### E

encryption  
    3592 tape drive 14, 15  
    AES keys 14  
    key  
        256-bit AES standard 10, 16, 17, 18  
        asymmetric 10, 15  
        symmetric 16, 17, 18  
    LTO tape drive 14  
    management  
        3592 tape drive 14  
        DS5000 18  
        DS8000 17  
        LTO tape drive 16  
ETERNUS\_DX 33  
event  
    Common Base Event (CBE) format 8  
    W7 format 8

### F

features  
    3592 tape drive 6  
    audit 8  
    auto-pending device 3  
    automated clone replication 8  
    backup and restore 7  
    BRCD\_ENCRYPTOR device 3  
    certificate, additional for DS8000 Turbo drives 3  
    concurrent administration 3  
    DS5000 storage servers 3  
    Hardware Security Module 3  
    Hardware Security Modules 8  
    HSM 8  
    key  
        deployment 4  
        group 4

- features (*continued*)
  - key (*continued*)
    - metadata 4
    - states 5
  - Key Management Interoperability Protocol 3
  - keystore 6
  - LDAP 3
  - LTO tape drive 6
  - ONESECURE device 3
  - overview
    - 3592 tape drive 6
    - audit 8
    - backup and restore 7, 20
    - component deployment 19
    - disk drives 7
    - DS5000 storage server 7
    - DS8000 Turbo drive 7
    - encryption, keys 10
    - FIPS 10
    - key deployment 4
    - key group 4
    - key metadata 4
    - key states 5
    - keystore 6
    - KMIP 11
    - LTO tape drive 6
    - replica server 19
    - roles 33, 37
    - Suite B 11
    - tape drives 6
  - replication 3
  - role-based access 3
  - serial number, variable length 3
  - symmetric keys, DS5000 storage servers 3
  - trusted certificate, management 3
  - wizard 3
- FIPS
  - IBMJCECFIPS cryptographic provider 10
  - requirement 10
- fix packs
  - Passport Advantage 41
- fixes, replica server same as primary 20
- free disk space
  - replica server 20

## G

- group
  - LTOAdmin 37
  - LTOAuditor 38
  - LTOOperator 37

## H

- handshake
  - SSL/TSL 9
  - wizard 9
- hardware and software
  - system requirements 39
- Hardware Security Modules
  - master key 8
- HSM 8

## I

- IBM Security Key Lifecycle Manager
  - components 18
- IBM Security Key Lifecycle Manager user
  - password, changing 30
- IBMJCECFIPS cryptographic provider 10
- images
  - installation instructions 41
  - Passport Advantage 41
- initial user ID and password 22
- installation
  - images
    - fix packs 41
    - Passport Advantage 41
- instance
  - name, sklmdb2 22
  - owner, sklmdb2 22

## J

- Java Runtime Environment, requirement 39

## K

- kernel settings for DB2 40
- key
  - deployment overview 4
  - encryption 10
  - group overview 4
  - metadata overview 4
  - states
    - active 5
    - compromised 5
    - pending 5
    - symmetric 10
- keystore
  - overview 6
- klmAdminDeviceGroup permission 33
- klmAudit permission 33
- klmBackup permission 33
- klmBackupRestoreGroup 32, 33
- klmConfigure permission 33
- klmCreate permission 33
- klmDelete permission 33
- klmGet permission 33
- klmGUICLIAccessGroup 33
- klmModify permission 33
- klmRestore permission 33
- klmSecurityOfficer 32
- klmSecurityOfficerGroup 33
- klmView permission 33
- KMIPListener.ssl.port, property 11

## L

- languages support 3
- LDAP integration
  - IBM Security Key Lifecycle Manager 8
  - user repositories LDAP 8
- login
  - multiple browser sessions 26
  - port number 22

login (*continued*)

- URL 22
- user ID and password 22
- WebSphere Application Server
  - port 22
- LTO
  - device group 33
  - encryption 14, 16
- LTOAdmin 33, 37
- LTOAuditor 33, 38
- LTOOperator 33, 37

## M

- master key
  - master key 8
- metadata, key 4
- multiple
  - browser sessions 26

## N

- NSA 11

## O

- ONESECURE device group 33
- operating system
  - replica server, same as primary 20
- overview
  - backup and restore 7
  - features
    - audit 8
    - backup and restore 7, 20
    - component deployment 19
    - FIPS 10
    - key deployment 4
    - key encryption 10
    - key group 4
    - key metadata 4
    - key states 5
    - keystore 6
    - replica server 19
    - roles 33, 37
    - Suite B 11
    - tape drives 6
  - product 1

## P

- Passport Advantage, installation
  - images 41
- password
  - administrator, resetting 31
  - authority to reset 31
  - backup before reset 31
  - backup file 21
  - initial login 22
  - policy 27
  - strength 27
- password change
  - IBM Security Key Lifecycle Manager user 30
- patches, replica server same as primary 20

- pending, state 5
- permissions
  - klmAdminDeviceGroup 33
  - klmAudit 33
  - klmBackup 33
  - klmConfigure 33
  - klmCreate 33
  - klmDelete 33
  - klmGet 33
  - klmModify 33
  - klmRestore 33
  - klmView 33
- port
  - installation default 22
  - number
    - https address 22
- product
  - features
    - auto-pending device 3
    - BRCD\_ENCRYPTOR device 3
    - certificate, additional for DS8000 Turbo drives 3
    - concurrent administration 3
    - DS5000 storage servers 3
    - Key Management Interoperability Protocol 3
    - ONESECURE device 3
    - role-based access 3
    - serial number, variable length 3
    - symmetric keys, DS5000 storage servers 3
    - trusted certificate, management 3
  - overview 1
- property
  - KMIPListener.ssl.port 11
  - TransportListener.ssl.timeout 11

## R

- replica server
  - deployment 19
  - requirements
    - database 20
    - free disk space 20
    - IBM Security Key Lifecycle Manager server 20
    - operating system 20
- replication
  - automated clone replication 8

- replication (*continued*)
  - clone, five copies 8
- requirements
  - cryptographic 10, 11
  - database 39
  - FIPS 10
  - Java Runtime Environment 39
  - runtime environment 39
  - Suite B 11
  - WebSphere Application Server 39
- roles
  - suppressmonitor 33
  - WebSphere Application Server 38

## S

- security
  - audit log Common Base Event (CBE) specification 9
  - backup file
    - corrupt if edited 21
    - password 21
    - restore 21
  - compromised key state 5
  - FIPS 10
  - Suite B 11
- session
  - wsadmin, using Jython 29, 30
- shared
  - browser sessions 26
- SKLMAdmin 22, 32
- sklmdb2
  - instance name 22
  - instance owner 22
- SSL/TSL
  - handshake 9
  - wizard 9
- states
  - active 5
  - compromised 5
  - pending 5
- strength, password 27
- Suite B
  - NSA 11
- support languages 3
- suppressmonitor role 33
- SYSADM authority, database 39
- SYSCTRL authority, database 39
- SYSMAINT authority, database 39

- system requirements
  - hardware and software 39

## T

- tape drives
  - 3592 tape drive 6
  - LTO tape drive 6
  - overview 6
- TransportListener.ssl.timeout, property 11
- Triple DES keys, encryption 16, 17, 18
- TS3592, device family 33

## U

- user groups
  - klmBackupRestoreGroup 33
  - klmGUICLIAccessGroup 33
  - klmSecurityOfficerGroup 33
  - LTOAdmin 33
  - LTOAuditor 33
  - LTOOperator 33
- user ID
  - IBM Security Key Lifecycle Manager administrator 22
  - initial login 22
  - WebSphere Application Server administrator 22

## W

- W7 format, mapping from CBE format 8
- WASAdmin 22, 32
- WebSphere Application Server roles 38
- what is new
  - AES 256-bit master key 1
  - backup, cross-platform 1
  - certificate, export 1
  - debug logging 1
  - replication, cross-platform 1
  - restore, cross-platform 1
  - wizard, SSL/KMIP 1

## X

- XIV 33