Overview

Contents

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 2.5.0, Fix Pack 3 provides new infrastructure and processes to locally create, distribute, backup, and manage the lifecycle of keys and certificates.

IBM Security Key Lifecycle Manager, Version 2.5.0, Fix Pack 3 provides the following capabilities:

IBM Security Key Lifecycle Manager audit messages in syslog format
Supports the generation of IBM Security Key Lifecycle Manager audit messages in syslog format to send them to a syslog server. Syslog is a standard for computer message logging and is supported by a wide variety of devices and receivers across multiple operating systems. Syslog is now standardized by IETF in RFC 5424.

You can configure syslog for the audit messages either for writing to a file or to a syslog server. For more information, see Generating audit records in syslog format.

AES 256 key for backup and restore operations
Uses the AES 256-bit length key for IBM Security Key Lifecycle Manager backup and restore operations to conform to the PCI DSS (Payment Card Industry Data Security Standard) standards for increased data security. For more information, see "Backup and restore" on page 35.

AES 256-bit master key for data encryption
Supports AES 256-bit length for the IBM Security Key Lifecycle Manager master key.

You can now change the IBM Security Key Lifecycle Manager master key length from AES 128-bit to 256-bit length. To conform to the PCI DSS standards and for the increased data security, use 256-bit length master key for encrypting IBM Security Key Lifecycle Manager sensitive data, such as key material. By using **Master Key REST Service**, you can create 256-bit master key. For more information, see Master Key REST Service documentation.

IBM Security Key Lifecycle Manager user change password
Supports the password change for IBM Security Key Lifecycle Manager user through the graphical user interface. For more information about how to change the password, see Changing IBM Security Key Lifecycle Manager user password.

Last used date of keys, certificates, or key groups

Includes the last used date of keys, certificates, or key groups in the deletion confirmation message. When you delete a key, certificate, or key group through IBM Security Key Lifecycle Manager graphical user interface, the deletion confirmation message contains the following additional information:

- Date that the key or certificate last used.
- Date that the recently served key of the key group last used.

Proof of encryption

Tracks the information whether IBM Security Key Lifecycle Manager Server served the key to a storage device for data encryption through the IBM proprietary protocol (IPP) or KMIP protocol. See the **tklmServedDataList** CLI command and **Served Data List REST Service** documentation for the details.

REpresentational State Transfer (REST) interfaces

Includes the following new REST services to access the IBM Security Key Lifecycle Manager server functions:

- **Master Key REST Service**
- **Pending Client Certificate Accept REST Service**
- **Pending Client Certificate List REST Service**
- **Pending Client Certificate Reject REST Service**
- **Served Data List REST Service**

For more information, see the REST documentation in the Reference section.

Note:

- The IBM Security Key Lifecycle Manager command-line interface commands will be deprecated in the later 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

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.

On Windows systems, the information is on the start menu. Click **Start** > **All Programs** > **IBM Security Key Lifecycle Manager 2.5**.

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.

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

`https://localhost:9083/ibm/console/logon.jsp`

On Windows systems, the information is on the start menu. Click **IBM WebSphere** > **IBM WebSphere Application Server V8.5** > **Profiles** > **KLMProfile** > **Administrative console**.

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.

Administrator user IDs and passwords

Installing IBM Security Key Lifecycle Manager provides default administrator user IDs of WASAdmin, SKLMAdmin, and `sklmdb2`.

Table 1. Administrator user IDs and passwords

Program	User ID	Password
Distributed systems 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	**SKLMAdmin** 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 **sklmadmin**. Use the SKLMAdmin user ID to administer IBM Security Key Lifecycle Manager. With the SKLMAdmin user ID, you can: • View and use the IBM Security Key Lifecycle Manager interface. • Change the password for the IBM Security Key Lifecycle Manager administrator. However, you cannot: • Create one or more extra IBM Security Key Lifecycle Manager administrator user IDs. • Do WebSphere Application Server administrator tasks such as creating or assigning a role. • Start or stop the server.	Specify and securely store a password during installation.

Table 1. Administrator user IDs and passwords (continued)

Program	User ID	Password
WebSphere Application Server administrator	**WASAdmin** This user ID is not case-sensitive. Alternatively, use **wasadmin** or a user ID that you specify during installation. Do not use the: • SKLMAdmin user ID to administer WebSphere Application Server. • WASAdmin user ID to administer IBM Security Key Lifecycle Manager. The WASAdmin user ID has no roles to use IBM Security Key Lifecycle Manager. This administrator user ID is the WebSphere Application Server administrator user ID. With the wasadmin user ID, you can: • View and use only the WebSphere Application Server interface. • Create one or more extra IBM Security Key Lifecycle Manager administrator user IDs, groups, and roles. • Reset the password of any IBM Security Key Lifecycle Manager user ID, including the SKLMAdmin administrator. • Start and stop the server. However, you cannot: • Use the IBM Security Key Lifecycle Manager to complete tasks. For example, you cannot create IBM Security Key Lifecycle Manager device groups. • Do other tasks that require access to IBM Security Key Lifecycle Manager data. The wasadmin user ID does *not* have access to IBM Security Key Lifecycle Manager data as a superuser.	Specify and securely store a password during installation. 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.
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	**Windows systems and systems such as AIX or Linux:** The default value is `sklmdb2`. You might specify a different value during installation. The ID is the installation default user ID for the instance owner of the database. Do not specify a user ID greater than eight characters in length. The instance name is also `sklmdb2`. 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. 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. **Note:** Do not use a hyphen (-) or underscore character (_) when you specify a user ID for an existing copy of DB2.	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. For more information, see "Resetting password on distributed systems" on page 12..
Database instance	The administrator ID `sklmdb2` owns a DB2 instance named `sklmdb2`.	

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, Solaris, and AIX systems, `/opt` is the default path.

Table 2. HOME and other directory variables

Directory variable	Default definition	Description
DB_HOME	**Windows systems:** *drive*:\Program Files (x86)\IBM\DB2SKLMV25 **AIX and Linux systems:** /opt/IBM/DB2SKLMV25	The directory that contains the DB2 application for IBM Security Key Lifecycle Manager.
DB_INSTANCE_HOME	**Windows** *drive**db2adminID* For example, if the value of *drive* is C: and the default DB2 administrator is sklmdb2, *DB_INSTANCE_HOME* is C:\SKLMDB2. **Linux and AIX®** /home/*db2adminID* **Solaris** /export/home/*db2adminID*	The directory that contains the DB2 database instance for IBM Security Key Lifecycle Manager.
WAS_HOME	**Windows** *drive*:\Program Files (x86)\IBM\WebSphere\AppServer **Linux, AIX, and Solaris** *path*/IBM/WebSphere/AppServer For example: /opt/IBM/WebSphere/AppServer	The WebSphere Application Server home directory.
SKLM_HOME	**Windows** *WAS_HOME*\products\sklm **Linux, AIX, and Solaris** *WAS_HOME*/products/sklm	The IBM Security Key Lifecycle Manager home directory.
SKLM_INSTALL_HOME	**Windows** *drive*:\Program Files (x86)\IBM\SKLMV25 **Linux, AIX, and Solaris** *path*/IBM/SKLMV25	The directory that contains the IBM Security Key Lifecycle Manager license and migration files.
IM_INSTALL_DIR	**Windows** *drive*:\ProgramData\IBM\Installation Manager **Linux and UNIX** /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

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

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).

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).

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:

       ```
       AdminTask.changeMyPassword('[-oldPassword <oldpasswordvalue>
       -newPassword
       <newpasswordvalue> -confirmNewPassword <newpasswordvalue>]')
       ```

       Example:

       ```
       AdminTask.changeMyPassword('[-oldPassword sklmadmin -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 WASAdmin 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) role and the means to specify more limited administrative roles to meet the needs of your organization. By default, the SKLMAdmin 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.

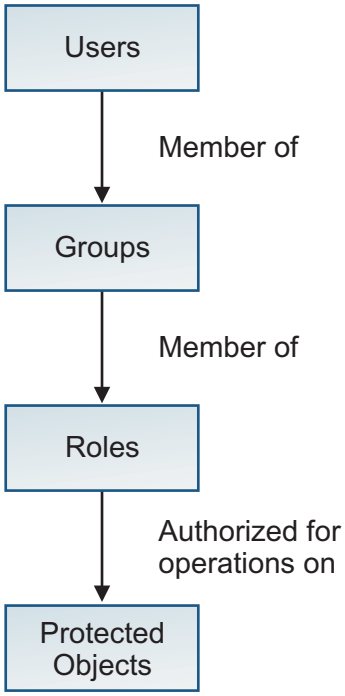

Figure 1. Relations between users, groups, roles, and protected objects

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 16.
- 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 **tklmServedDataList** 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
GENERIC	Objects in the GENERIC device family.

Table 5. Device groups (continued)

Permission	Allows actions on these objects
userdevicegroup	A user-defined instance such as myLTO 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 LTO 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 myLTO that was created for a new device group named myLTO. 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 **`tklmServedDataList`** 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.
`klmBackup`	Create and delete a backup of IBM Security Key Lifecycle Manager data.

Table 7. Permissions for actions (continued)

Permission	Enables these actions
`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.
`klmView`	View objects, but not create, delete, or modify objects.
`klmAudit`	View audit data by using the **`tklmServedDataList`** 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).

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, asymmetric key pairs, and certificates.

IBM Security Key Lifecycle Manager has the following 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.
- 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.
- A graphical user interface, command-line interface, and REST interface to manage keys, certificates, and devices.

  Note:
  - The IBM Security Key Lifecycle Manager command-line interface commands will be deprecated in the later 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.
- 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.
- Backup and restore to protect critical data and other IBM Security Key Lifecycle Manager data, such as the configuration files and current database information.
- Migration of IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, 2.0.1, 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 systems. This replication enables cloning of IBM Security Key Lifecycle Manager environments on multiple servers in a fully automated fashion.

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.

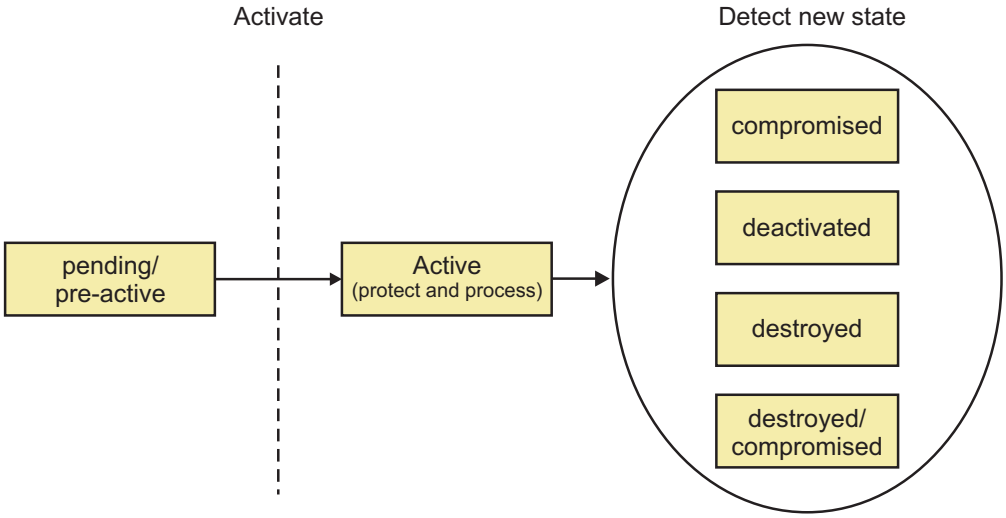

Figure 2. Cryptographic object states

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, `2.5`.
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 backup and restore functions to protect critical IBM Security Key Lifecycle Manager information.

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 with up to five copies.

You can configure the program to replicate the 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.

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.

You can replicate the following data:

- Tables in the IBM Security Key Lifecycle Manager database.
- All keys materials in the IBM Security Key Lifecycle Manager database.
- IBM Security Key Lifecycle Manager configuration files apart from 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.

You can configure IBM Security Key Lifecycle Manager replication with the `ReplicationSKLMgrConfig.properties` configuration file. You must specify the replication configuration file on all systems that are involved in 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. The master and clone systems must be identical. The operating system, directory structures, and DB2 admin user must be same on the systems. Not having them identical might lead to unpredictable results.

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.

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.
- File-based audit logs that vary, depending on the operating system:
  - Distributed systems

    Contain data in a flat file that is based on the Common Base Event (CBE) security event specification.

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).

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.

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).

IBM Security Key Lifecycle Manager can listen for connection requests from KMIP clients that send requests to locate, store, and manage cryptographic material on the IBM Security Key Lifecycle Manager server. IBM Security Key Lifecycle Manager supports KMIP secret data and symmetric key interoperability profiles for KMIP server and client interactions.

KMIP profiles supported by IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Manager supports the following KMIP profiles:

- 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.

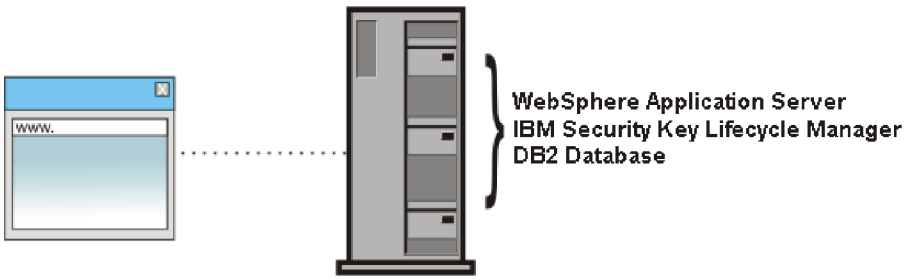

Figure 3. Main components on Windows systems and systems such as Linux or AIX

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 4. 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 that 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.

The IBM Security Key Lifecycle Manager backup and restore operations use 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.

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.

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 restore and decrypt the file on the primary IBM Security Key Lifecycle Manager server.

Before you start a restore task, isolate the system for maintenance. 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.

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, `2.5`.
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 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 10.1 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 10.1 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_10.1.0/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_10.1.0/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 Solaris 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 10.1 on other supported Linux systems, see DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html).

Solaris systems

For more information about modifying kernel parameters, see DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0006476.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.

Known limitations, problems, and workaround

There are known IBM Security Key Lifecycle Manager limitations, problems, and workaround.

Product migration, installation, and removal problems and workaround

You might encounter the migration, IBM Security Key Lifecycle Manager server installation, or product removal problems, and use workaround that are described in this topic.

- **Problem:** Migration from Encryption Key Manager to IBM Security Key Lifecycle Manager fails if the Encryption Key Manager keystore contains a certificate with a key that has an Elliptic Curve (EC) public key algorithm.

  Workaround: Delete the key that has the EC algorithm and run the migration script that IBM Security Key Lifecycle Manager provides. For example, to delete a key from an Encryption Key Manager JCEKS keystore, type on one line:

  ```
  JAVA_INSTALL_DIR/bin/keytool -keystore keystore_path_and_filename
   -storetype jceks -delete -alias EC_keyname
  ```

- **Problem:** Installation fails on a computer that has insufficient space and also does not remove files that the installation process created.

  Workaround: Provide enough free disk space on the computer to allow successful completion of the product installation. You must manually remove the files that the failed installation created.

- **Problem:** You cannot use the graphical user interface to delete a migrated rollover that you added with the command-line interface by using the **tklmCertDefaultRolloverAdd** or the **tklmKeyGroupDefaultRolloverAdd** command.

  Workaround: Use the command-line interface to delete a migrated rollover that you created by using the command-line interface.

- **Problem:** During migration on distributed systems, the correct path and file are not dependably located if you click **Browse** to locate an Encryption Key Manager properties file. You also cannot dependably select a folder and press **Enter**.

  Workaround: Manually enter the path to the Encryption Key Manager properties file.

- **Problem:** During IBM Security Key Lifecycle Manager installation on distributed systems, if you omit a forward slash when you type the value of the DB2 home directory, you might see an error message that indicates that the specified administrative user ID cannot be created. The message indicates that you must ensure that the password meets system requirements and that the home directory has adequate disk space.

  Workaround: Ensure that a forward slash is the first character when you specify the DB2 home directory. For example, type:

  ```
  /mydb2home
  ```

- **Problem:** If you install IBM Security Key Lifecycle Manager by Exceed on a local system while you export the display from a Linux system to the local system, you cannot decline the license agreement. If you decline the license agreement, the installation program becomes unresponsive.

  Workaround: Accept the license agreement, or use the Cygwin X Server or a Virtual Network Connection (VNC) instead.

- **Problem:** When you migrate or restore devices from Encryption Key Manager Version 2.1 to IBM Security Key Lifecycle Manager Version 2, the device serial numbers can appear in lists for all device groups in the graphical user interface. For example, the serial number for a migrated LTO tape drive is displayed in a list of LTO tape drives, and also in lists for 3592 tape drives.

  Workaround: Ensure that the device is the correct type before you start an operation that alters the device.

- **Problem:** Migration might cause a drive of a specific type to appear with an `UNKNOWN` label in the IBM Security Key Lifecycle Manager graphical user interface.

  Limitation: Migration from Encryption Key Manager does not resolve the device group for all drives. The current migration result is shown in the following table:

Table 9. Device group assignment after migration from Encryption Key Manager

Drive characteristic	Assigned device group
Drives with an alias or aliases defined	3592 tape drive
Drives that follow the serial number specification for 3592 tape drives	3592 tape drive
Drives with `symAlias` defined	LTO tape drive
Other drives that do not define an alias, a `symAlias`, or follow a serial number specification for 3592 tape drives	UNKNOWN After a drive of an unknown type makes a request to IBM Security Key Lifecycle Manager, its type might change to a known device group. Alternatively, you can modify the device group by the IBM Security Key Lifecycle Manager graphical user interface.

- **Problem:** Migration from Encryption Key Manager to IBM Security Key Lifecycle Manager fails when the system locale is set as non-English language. The Encryption Key Manager component supports only the English locale.

  Workaround: Perform migration with English language locale set.
- **Problem:** IBM Security Key Lifecycle Manager might not work as expected if you uninstall WebSphere Application Server or DB2.

  Workaround: Uninstall IBM Security Key Lifecycle Manager and reinstall all the components.
- **Problem:** You might see the following output when you install IBM Security Key Lifecycle Manager on AIX platform:

```
Could not load SWT library. Reasons:
        /tmp/sw/disk1/im/configuration/org.eclipse.osgi/bundles/631/1/.cp/
libswt-pi-gtk-4234.a (No such file or directory)
        swt-pi-gtk (Not found in java.library.path)
        /.swt/lib/aix/ppc/libswt-pi-gtk-4234.a (No such file or directory)
        /.swt/lib/aix/ppc/libswt-pi-gtk.a (No such file or directory)
  java.lang.UnsatisfiedLinkError: Could not load SWT library. Reasons:
        /tmp/sw/disk1/im/configuration/org.eclipse.osgi/bundles/631/1/.cp/
libswt-pi-gtk-4234.a (No such file or directory)
        swt-pi-gtk (Not found in java.library.path)
        /.swt/lib/aix/ppc/libswt-pi-gtk-4234.a (No such file or directory)
        /.swt/lib/aix/ppc/libswt-pi-gtk.a (No such file or directory)

  java.lang.UnsatisfiedLinkError: Could not load SWT library. Reasons:
        /tmp/sw/disk1/im/configuration/org.eclipse.osgi/bundles/631/1/.cp/
libswt-pi-gtk-4234.a (No such file or directory)
        swt-pi-gtk (Not found in java.library.path)
        /.swt/lib/aix/ppc/libswt-pi-gtk-4234.a (No such file or directory)
        /.swt/lib/aix/ppc/libswt-pi-gtk.a (No such file or directory)

    at org.eclipse.swt.internal.Library.loadLibrary(Library.java:331)
    at org.eclipse.swt.internal.Library.loadLibrary(Library.java:240)
    at org.eclipse.swt.internal.gtk.OS.<clinit>(OS.java:22)
    at java.lang.J9VMInternals.initializeImpl(Native Method)
   ...
The displayed failed to initialize. See the log /tmp/sw/disk1/im/
configuration/1374569112557.log for details.
```

  Workaround: To fix this issue, see the workaround information at: http://www-01.ibm.com/support/docview.wss?uid=swg21631478
- **Problem:** You might see the following output when you install IBM Security Key Lifecycle Manager on Red Hat Enterprise Linux platform:

```
[root@zahar-rhel64 IMinstallKit]# ./install
bash: ./install: /lib/ld-linux.so.2: bad ELF interpreter: No such file or
directory

[root@c01bmp02 IM]# ./install
JVMJ9VM011W Unable to load j9dmp24: libstdc++.so.5: cannot open shared
object file: No such file or directory
JVMJ9VM011W Unable to load j9jit24: libstdc++.so.5: cannot open shared
object file: No such file or directory
JVMJ9VM011W Unable to load j9gc24: libstdc++.so.5: cannot open shared
object file: No such file or directory
JVMJ9VM011W Unable to load j9vrb24: libstdc++.so.5: cannot open shared
object file: No such file or directory
```

Workaround: To fix this issue, see the workaround information at: https://www-304.ibm.com/support/docview.wss?uid=swg21459143

- **Problem:** You might see the following output when you install IBM Security Key Lifecycle Manager on 64-bit Red Hat Enterprise Linux platform:

```
InstallError
================================================================================
eclipse.buildId=unknownjava.fullversion=JRE 1.6.0 IBM J9 2.4 Linux x86-32
jvmxi3260sr9-20110203_74623 (JIT enabled, AOT enabled)J9VM -
20110203_074623JIT - r9_20101028_17488ifx3GC - 20101027_AABootLoader
constants: OS=linux, ARCH=x86, WS=gtk, NL=enFramework arguments: -toolId
install -accessRights admin input @osgi.install.area/install.xmlCommand-
line arguments: -os linux -ws gtk -arch x86 -toolId install -accessRights
admin input @osgi.install.area/install.xml!ENTRY com.ibm.cic.agent.ui 4 0
2013-07-09 14:11:47.692!MESSAGE Could not load SWT library.
Reasons:/home/tklm-v3/disk1/im/configuration/org.eclipse.osgi/bundles/207/1/
.cp/libswt-pi-gtk-4234.so (libgtk-x11-2.0.so.0: cannot open shared object
file: No such file or directory)
swt-pi-gtk (Not found in java.library.path)/root/.swt/lib/linux/x86/libswt-
pi-gtk-4234.so (libgtk-x11-2.0.so.0: cannot open shared object file: No
such file or directory)
/root/.swt/lib/linux/x86/libswt-pi-gtk.so (/root/.swt/lib/linux/x86/liblib
swt-pi-gtk.so.so:cannot open shared object file: No such file or directory)"
```

Workaround: To fix this issue, see the workaround information at: https://www-304.ibm.com/support/docview.wss?uid=swg21459143

- **Problem:** Silent installation of IBM Security Key Lifecycle Manager on 64-bit Linux for System z fails with the following error:

```
 wrong ELF class: ELFCLASS64
```

Workaround: To fix this issue, see the workaround information at: http://www-01.ibm.com/support/docview.wss?uid=swg21645797

- **Problem:** Not possible to proceed with the IBM Security Key Lifecycle Manager installation as a non-root user.

  If you are logged in to the UNIX system as a root user, you cannot install IBM Security Key Lifecycle Manager as a non-root user.

  Workaround: Restart the system, log in as a non-root user, start the VNC server, and start the IBM Security Key Lifecycle Manager installer.

- **Problem:** The data source connection and restore operation fails when you install IBM Security Key Lifecycle Manager as a non-root user. After the installation, you might see these messages:

```
SQL2044N An error occurred while accessing a message queue.  Reason code:
 "1"." in db2_config.log
SQL2043N Unable to start a child process or thread" in db2restore.log after
restore operation failed.
```

  Workaround: Modify the following kernel parameter on Linux system and try again:

```
sysctl -w kernel.msgmni=16384
sysctl -w kernel.sem="250 32000 100 1024"
echo "kernel.msgmni=16384" ))/etc/sysctl.conf
echo "kernel.sem=\"250 32000 100 1024\"" ))/etc/sysctl.conf
```

For the detailed information to troubleshoot this issue, see http://www-01.ibm.com/support/docview.wss?uid=swg21365583.

- **Problem:** When you install IBM Security Key Lifecycle Manager, the Prerequisite Scanner for non-root installation fails with the error message in the `results.txt` file located under `%temp%/sklmPRS`.

```
KLM - IBM Security Key Lifecycle Manager [03000000]:
Property                Result          Found              Expected
========                ======          =====              =========
user.isAdmin         FAIL             False              True
```

  Workaround: In the following directories, create a `sklmInstall.properties` file with the property **SKIP_PREREQ=true** to skip the Prerequisite Scanner:

  Windows
  `%TEMP%`

  UNIX `/tmp`

- **Problem:** You cannot install IBM Security Key Lifecycle Manager when a system has multiple partitions and if you:
  - You choose to install on the partition other than the `/opt` directory.
  - Less space on the `/opt` directory.

  The installer displays the following error:

```
One or more prerequisite failed to meet the requirement.
```

  Workaround: To fix this issue, use any of the following solutions:
  - Increase space in the `/opt` directory to meet the requirement.
  - In the following directories, create a `sklmInstall.properties` file with the property **SKIP_PREREQ=true** to skip the Prerequisite Scanner:

    Windows
    `%TEMP%`

    UNIX `/tmp`

- **Problem:** When you install IBM Security Key Lifecycle Manager, the Prerequisite Scanner incorrectly displays low disk space in the "`/opt`" directory even if the disk space is low in the "/" directory.

  Workaround: Ensure that the required disk space (12 GB) is available in the `/opt` directory.

- **Problem:** The description that is specified in **Tivoli Integrated Portal** > **Users and Groups** > **Manage Groups** cannot be migrated from IBM Security Key Lifecycle Manager earlier version 2.0, or 2.0.1 to version 2.5. However, the group itself is migrated.

  Workaround: You can add the descriptions in WebSphere Integrated Solutions Console for each user group. Click **WebSphere Integrated Solutions Console** > **Users and Groups** > **Manage Groups** to update or specify the description.

- **Problem:** When IBM Security Key Lifecycle Manager earlier version 1.0 is migrated to version 2.5, on the welcome page, the link that shows the time stamp of the backup file is not displayed.

  Workaround: To resolve this issue, run the IBM Security Key Lifecycle Manager backup operation.

- **Problem:** When you migrate earlier version of IBM Security Key Lifecycle Manager to version 2.5 in graphical mode, keystore password of the earlier version is not validated.

  This issue is a known limitation.
- **Problem:** Installation of IBM Security Key Lifecycle Manager can fail if the Windows User Account Control (UAC) setting is set to `Always notify`.

  Workaround: To fix this issue, see the workaround information at: http://www-01.ibm.com/support/docview.wss?uid=swg21665207
- **Problem:** IBM Security Key Lifecycle Manager installation fails on Windows 2012 R2 operating system with the following error message:

  ```
  CTGKM9103E Unable to find the location of prerequisite scanner tool.
  ```

  Workaround: To fix this issue, run the following steps:

  1. Update the Windows UAC setting as described in this technote: http://www-01.ibm.com/support/docview.wss?uid=swg21665207
  2. Go to the IBM Security Key Lifecycle Manager installation files directory.
  3. Right-click on the `launchpad.exe` file.
  4. Click **Run as administrator**.
  5. Continue with the steps to install IBM Security Key Lifecycle Manager.
- **Problem:** On Windows operating system, the `%temp%/sklmPRS/results.txt` file contains the following warning message for Prerequisite Scanner.

  ```
  WARNING: [KLM 03000000] The syntax for the following section title is
  not valid: risc.cpu. The prerequisite property in the section title is not
  supported. The section check is evaluated to FALSE. Prerequisite properties
  in this section are not checked. Review the documentation for the valid
  prerequisite properties and update the section title.
  ```

  Workaround: You can ignore this message. This message is displayed because Prerequisite Scanner looks for the `risc.cpu` property on Windows. This property does not exists for Windows.

IBM Security Key Lifecycle Manager server limitations, problems, and workaround

The IBM Security Key Lifecycle Manager server problems, workaround, and limitations are described in this topic.

- **Problem:** For DS5000 storage servers, IBM Security Key Lifecycle Manager erroneously returns an error code of `EE31` when a key group runs out of keys and the **`stopRoundRobinKeyGrps`** property is enabled. The error can also occur for an LTO device group.

  Note: Occurs only when the **`StopRoundRobinKeyGrps`** property is set to true.

  Workaround: The event is not a keystore error. To correct the problem, add more keys to the key group that is documented in the audit event.
- **Problem:** IBM Security Key Lifecycle Manager operations take significant amounts of time to complete when you add or update a large number of keys in the IBM Security Key Lifecycle Manager keystore, such as more than 50,000 keys.

  Workaround: Periodically perform database maintenance. For example, when you add or update a large number of keys, take these steps:

  1. Perform a backup of IBM Security Key Lifecycle Manager.
  2. Stop the IBM Security Key Lifecycle Manager server by using the **`stopServer`** command.

     Alternatively on Windows systems, stop the IBM Security Key Lifecycle Manager server by using Windows Computer Management:

a. Open the Control Panel and click **Administrative Tools** > **Computer Management** > **Services**.
b. Stop the IBM Security Key Lifecycle Manager server service, which has a name like `IBMWAS85Service - SKLMServer`

3. From a DB2 command window, run these DB2 commands, each on one line:

```
db2 reorg indexes all for table kmt_device_type allow no access
db2 runstats on table sklmdb2.kmt_device_type and indexes all
db2 reorg indexes all for table sklmdb2.kmt_certstr_rn allow no access
db2 runstats on table sklmdb2.kmt_certstr_rn and indexes all
db2 reorg indexes all for table sklmdb2.kmt_keystr_rn allow no access
db2 runstats on table sklmdb2.kmt_keystr_rn and indexes all
db2 reorg indexes all for table sklmdb2.kmt_group allow no access
db2 runstats on table sklmdb2.kmt_group and indexes all
db2 reorg indexes all for table sklmdb2.kmt_devaudit allow no access
db2 runstats on table sklmdb2.kmt_devaudit and indexes all
db2 reorg indexes all for table sklmdb2.kmt_kmip_attr_appinfo allow no access
db2 runstats on table sklmdb2.kmt_kmip_attr_appinfo and indexes all
db2 reorg indexes all for table sklmdb2.kmt_kmip_attr_cryptoparams allow no access
db2 runstats on table sklmdb2.kmt_kmip_attr_cryptoparams and indexes all
db2 reorg indexes all for table sklmdb2.kmt_kmip_attr_custom allow no access
db2 runstats on table sklmdb2.kmt_kmip_attr_custom and indexes all
db2 reorg indexes all for table sklmdb2.kmt_kmip_attr_digest allow no access
db2 runstats on table sklmdb2.kmt_kmip_attr_digest and indexes all
db2 reorg indexes all for table sklmdb2.kmt_kmip_attr_link allow no access
db2 runstats on table sklmdb2.kmt_kmip_attr_link and indexes all
db2 reorg indexes all for table sklmdb2.kmt_kmip_global_names allow no access
db2 runstats on table sklmdb2.kmt_kmip_global_names and indexes all
db2 reorg indexes all for table sklmdb2.kmt_kmip_attr_name allow no access
db2 runstats on table sklmdb2.kmt_kmip_attr_name and indexes all
db2 reorg indexes all for table sklmdb2.kmt_kmip_attr_objectgroup allow no access
db2 runstats on table sklmdb2.kmt_kmip_attr_objectgroup and indexes all
```

4. Start the IBM Security Key Lifecycle Manager server by using the **`startServer`** command.

   Alternatively on Windows systems, start the IBM Security Key Lifecycle Manager server by using Windows Computer Management:

   a. Open the Control Panel and click **Administrative Tools** > **Computer Management** > **Services**.
   b. Start the IBM Security Key Lifecycle Manager server service, which has a name like - `IBMWAS85Service - SKLMServer`.

5. Perform another backup of IBM Security Key Lifecycle Manager.

- **Problem:** On systems where there are large numbers of keys, an operation such as creating a key group might time out.

  Workaround: Change the value of `com.ibm.SOAP.requestTimeout` in `/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/properties/soap.client.props` to a larger value. For example, set the value to `3600` and restart WebSphere Application Server.

- **Problem:** After an IBM Security Key Lifecycle Manager session times out, your first attempt to log in fails with a message like this example:

  ```
  Your session has become invalid. This is due to a session timeout,
  an administrator has logged you out, or another user has invalidated
  your session by logging on with the same User ID.
  ```

  Workaround: Ignore the message and log in again.

- **Problem:** If you create a 10-character serial number for a new device that uses KMIP in the LTO device family, IBM Security Key Lifecycle Manager pads the serial number with leading zeros to a length of 12 characters. Later, a KMIP client is unable to locate the device.

Workaround: Create a 12-character serial number for a new device that uses KMIP. Do not create serial numbers that are less than 12 characters in length.

- **Problem:** On the Sun Solaris operating system, backing up IBM Security Key Lifecycle Manager occasionally fails with an SQL error of SQL1125N. For example:

  ```
  SQL1225N  The request failed because an operating system process, thread, or
  swap space limit was reached.
  ```

  The error might be caused by a lack of resources available to perform the backup. Examining the sklmdb2/sqllib/db2dump/db2diag.log file might indicate that system resources such as DB2 processes are not able to acquire semaphores.

  Workaround: Restart the system and try to run the backup again.

- **Problem:** If a problem occurs, you might require to change the maximum number of values that can be used in a multi-valued KMIP attribute.

  Workaround: Update this property only if a problem occurs in reaching the maximum limit for a multi-valued attribute. Use the **tklmConfigUpdateEntry** command to change the mv.attribute.max.values property in the SKLMConfig.properties file.

  mv.attribute.max.values=*maxvaluesinteger*
  Determines the maximum number of values that can be used in a multi-valued KMIP attribute.

  Required
  Yes

  Default

  The default value is 32.

  Example

  ```
  mv.attribute.max.values=40
  ```

- **Problem:** You might require to change the maximum number of values that can be used in a KMIP custom attribute.

  Workaround: Use the **tklmConfigUpdateEntry** command to change the value of the **custom.attribute.max.values** property in the SKLMConfig.properties file.

  custom.attribute.max.values=*maxvaluesinteger*
  Determines the maximum number of values that can be used in a KMIP custom attribute.

  Required
  Yes

  Default

  The default value is 32.

  Example

  ```
  custom.attribute.max.values=40
  ```

- **Problem:** A WebSphere Application Server startup problem occurs with transaction logs. The problem report is that the server cannot recover a transaction from the log. The IBM Security Key Lifecycle Manager server then fails to initialize.

  Workaround: When the WebSphere Application Server starts, the server attempts to recover a failed transaction that is written to the log and the startup fails. Remove the WebSphere Application Server logs from the *WAS_HOME*/profiles/KLMProfile/tranlog/SKLMCell/SKLMNode/server1/transaction/ directory. Then, restart the WebSphere Application Server.

- **Problem:** On a page that has a date field with a short date format of dd/MM/yyyy, an example entry might be 20/04/2009. However, if you change the entry to a value such as 20/04/**09**, more help appears. When you submit the entry, the value changes to 20/04/**0**009, rather than **2**009.

  Workaround: You can successfully submit the entry by typing the value with the expected format of yyyy for the year. For example, type `2010`.
- **Problem:** After you cancel an in-progress installation of IBM Security Key Lifecycle Manager, the cleanup function might not remove some files in WebSphere Application Server directories.

  Workaround: If you cancel an in-progress installation of IBM Security Key Lifecycle Manager, ensure that you manually delete the *WAS_HOME* directory.
- **Problem:** If an asterisk (*) is the last (trailing) character in the name of more than one certificate or key group, IBM Security Key Lifecycle Manager cannot associate the certificate or key group to a device. The device name might end with an asterisk, or end with other characters.

  Workaround: To successfully associate certificates or key groups with devices, do not use a trailing asterisk to name certificates or key groups.
- **Problem:** In silent mode, installation and the uninstallation processes fail or exit without completion if the command that starts the process does not specify a response file. IBM Security Key Lifecycle Manager provides both installation response files and uninstall response files. For example, typing this command causes the uninstallation process to fail or to exit without completion:

  ```
  ./uninstall -i silent
  ```

  Limitation: You must specify a response file in an installation or uninstallation statement. For example, type:

  ```
  ./imcl -input full_path_to_response_file -silent
  ```
- **Problem:** In interactive mode, some commands print inaccurate syntax statements to the console. The statements omit two brackets for the attribute flag.

  Limitation: Interactive console displays of command syntax incorrectly specify several delimiters.

  For example, a **tklmDeviceAdd** command entry with the correct command syntax might be:

  ```
  AdminTask.tklmDeviceAdd
   ('[-type 3592 -serialNumber 123456789012
    -attributes "{worldwideName ww_name} {aliasOne cert1} "]')
  ```

  However, the interactive mode has this result:

  1. Run the **tklmDeviceAdd** command in interactive mode.

     ```
     wsadmin>AdminTask.tklmDeviceAdd('-interactive')
     ```
  2. The resulting statement is missing the correct brackets for the attribute flag.

     ```
     WASX7278I: Generated command line: AdminTask.tklmDeviceUpdate('[-uuid
     DEVICE-8f8f2acf-4bb4-4150-8672-8f809382bef5 -attributes [ [symAlias sym]
     [description desc] ]]')
      'CTGKM0001I: Command succeeded.'
     ```

  A **tklmDeviceUpdate** command entry with the correct command syntax might be:

  ```
  AdminTask.tklmDeviceUpdate
   ('[-uuid DEVICE-3c2617ec-0f65-445d-9323-a909512fa973
    -attributes "{description old_desc}"]')
  ```

  However, the interactive mode has this result:

  1. Run the **tklmDeviceUpdate** command in interactive mode.

     ```
     wsadmin>AdminTask.tklmDeviceUpdate('-interactive')
     ```

2. After more interactive activities, the resulting statement is missing the correct delimiters (in **boldface**) for the attribute flag.

```
WASX7278I: Generated command line: AdminTask.tklmDeviceUpdate
 ('[-uuid DEVICE-8f8f2acf-4bb4-4150-8672-8f809382bef5
  -attributes "[ [symAlias sym] [description desc]]"]')
```

- **Problem:** You might click the IBM Security Key Lifecycle Manager help prompt (?) to obtain more information in a browser instance, and then allow the current IBM Security Key Lifecycle Manager session to time out. The timeout message and an attempt to obtain a new login window appears in a help browser instance that remains open.

  Using the help browser instance, you can log in again. However, required navigation buttons are unavailable. Clicking the help prompt causes help information to appear, closing the IBM Security Key Lifecycle Manager graphical user interface without any means of return.

  Workaround: If your IBM Security Key Lifecycle Manager session times out and you also have a help browser instance open, close the help browser instance. Then, again log in to IBM Security Key Lifecycle Manager.

- **Problem:** Installing IBM Security Key Lifecycle Manager on a distributed system creates a user ID for IBM Security Key Lifecycle Manager with a password that expires according to the local policy on the system, which might set a short span of time, such as 90 days. If the user ID does not exist, the user ID is the same as the DB2 instance name.

  After the password expires, a correctly configured system fails and the user who attempts an operation such as listing a keystore, or listing keys in a group, might see these messages:

  ```
  CTGKM0506E Internal Database Operation error.
  CTGKM0900E Database connection failed on data source java:comp/env/jdbc/sklmDS
  ```

  Workaround: Use these steps if the DB2 password expires, or you want to reset the password for other reasons, such as a change of administrator:

  – Verify that database server is up and running. Type

    ```
    set DB2INSTANCE=slkminstance
    db2start
    ```

    where *sklminstance* is a value such as `sklmdb2`.

    The database returns an informational message such as:

    ```
    SQL1026N The database manager is already active.
    ```

  – Resolve the problem:

    1. Change the password for the IBM Security Key Lifecycle Manager instance owner.
       a. On Windows systems, click **Start** > **Control Panel** > **Administrative Tools** > **Computer Management** > **System Tools** > **Local Users and Groups** > **Users**.
       b. Change the password for the IBM Security Key Lifecycle Manager instance owner.
    2. Stop related services and change the password. On Windows systems, navigate to the services panel by clicking **Start** > **Control Panel** > **Administrative Tools** > **Computer Management**.

       Stop the following services

       ```
       DB2 - DBSKLMV25 - SKLMDB2
       DB2 Governor (DBSKLMV25)
       DB2 Remote Command Server (DBSKLMV25)
       ```

    3. Restart the instances that you stopped.

4. Additionally, stop and restart these services, which run as a local system account. You must not change their password.

   ```
   DB2 License Server (DBSKLMV25)
   DB2 Management Service (DBSKLMV25)
   ```

5. Log in as WASAdmin to a **wsadmin** session.
6. Use the **wsadmin** command to change the password of the WebSphere Application Server data source:
   a. The following command lists JAASAuthData entries:

      ```
      wsadmin>print AdminConfig.list('JAASAuthData')
      ```

      The result might be:

      ```
      (cells/SKLMCell|security.xml#JAASAuthData_1379859888963)
      ```

   b. Identify the data source ID with the alias that matches the string sklm_db. Also, identify the data source ID with the alias that matches the string sklmdb:

      ```
      print AdminConfig.showAttribute('JAASAuthData_list_entry', 'alias')
      ```

      For example, type on one line:

      ```
      print AdminConfig.showAttribute
      ('(cells/SKLMCell|security.xml#JAASAuthData_1379859888963)', 'alias')
      ```

      The result is:

      ```
      sklm_db
      ```

   c. Change the password of the sklm_db alias, entering this command on one line:

      ```
      print AdminConfig.modify('JAASAuthData_list_entry',
        '[[password newpassword]]'
      ```

      If you specify special characters in the password, use quotation marks as delimiters when you specify the password value.

      For example, type on one line:

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1379859888963)',
      '[[password tucs0naz]]')
      ```

   d. Save the changes:

      ```
      print AdminConfig.save()
      ```

   e. Stop and restart the IBM Security Key Lifecycle Manager server by using the **stopServer** and **startServer** commands.

      Alternatively, stop and restart the IBM Security Key Lifecycle Manager server by using Windows Computer Management.

      1) Open the Control Panel and click **Administrative Tools** > **Computer Management** > **Services and Applications** > **Services**.
      2) Stop and start the IBM Security Key Lifecycle Manager server service, which has a name like IBMWAS85Service - SKLMServer.

   f. Verify that you can connect to the database by using the WebSphere Application Server data source.

      1) First, type:

         ```
         print AdminConfig.list('DataSource')
         ```

         The result might be:

         ```
         "Default Datasource(cells/SKLMCell/nodes/SKLMNode/servers/server1|
         resources.xml#DataSource_1183122153625)"
         "SKLM DataSource(cells/SKLMCell/nodes/SKLMNode/servers/server1|
         resources.xml#DataSource_1379859893896)"
         "SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/servers/
         ```

```
server1|resources.xml#DataSource_1379859896273)"
DefaultEJBTimerDataSource(cells/SKLMCell/nodes/SKLMNode/servers/
server1|resources.xml#DataSource_1000001
```

2) Test the connection on the first data source. For example, type:

```
print AdminControl.testConnection('SKLM DataSource(cells....)')
```

For example, type on one line:

```
print AdminControl.testConnection
('(SKLM DataSource(cells/SKLMCell/nodes/SKLMNode/servers/server1|
resources.xml#DataSource_1379859893896)')
```

3) Test the connection on the remaining data source. For example, type:

```
print AdminControl.testConnection
('(SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/
servers/server1|resources.xml#DataSource_1379859896273)')
```

4) In both cases, you receive a message that the connection to the data source was successful. For example:

```
WASX7217I: Connection to provided datasource was successful.
```

Now you can run an IBM Security Key Lifecycle Manager operation.

- **Problem:** At a **wsadmin** command prompt on a Solaris operating system, a limit to the length of a command-line entry can prevent typing a long IBM Security Key Lifecycle Manager command. For example, you cannot complete the entry of this **tklmCertGenRequest** command:

```
print AdminTask.tklmCertGenRequest('[-alias sklmsslcertificate_008
-cn sklmsslcertificate_008  -ou sklmcertification006_ou -o IBM
-locality sklmLOC_008 -state NC -valid
ity 365 -keyStoreName defaultKeyStore  -fileName sklmcert8_fileName.csr
-usage SSLSERVER]')
```

Workaround: Write the long command as one line in a file, and run the file as a script, in a session similar this example:

```
-bash-3.00# ./wsadmin.sh -f createCert.py
Realm/Cell Name: <default>
Username: wasadmin
Password:
WASX7209I: Connected to process "server1" on node SKLMNode using SOAP
connector;  The type of process is: UnManagedProcess
CTGKM0001I Command succeeded.
/opt/IBM/WebSphere/AppServer/products/sklm/sklmcert8_fileName.csr

-bash-3.00# cat createCert.py
print AdminTask.tklmCertGenRequest('[-alias sklmsslcertificate_008
-cn sklmsslcertificate_008  -ou sklmcertification006_ou -o IBM
-locality sklmLOC_008 -state NC -valid
ity 365 -keyStoreName defaultKeyStore  -fileName sklmcert8_fileName.csr
-usage SSLSERVER]')

-bash-3.00# ls -l createCert.py
-rw-r--r--   1 root     root         262 Sep 15 13:31 createCert.py

-bash-3.00#
```

- **Problem:** Although IBM Security Key Lifecycle Manager allows you to specify a key label that is up to 256 characters in length, a label that exceeds 64 characters is too long for use with encryption-capable tape drives or RAID controllers. For example, the 64–character limit applies to the key label for a certificate that is used by a 3592 tape drive, LTO tape drive, or DS8000 Turbo drive.

  Workaround: Specify key labels that are 64 characters or less in length for a 3592 tape drive, LTO tape drive, or DS8000 Turbo drive.

- **Problem:** On a field that accepts date input, typing a value in the field might display bubble help that states the date format is not valid, until the full date is entered.

  Workaround: The temporary appearance of help information is because validation occurs as you type the date. Use the pop-up calendar, or ignore the bubble help until the full date is entered.
- **Problem:** The **tklmVersionInfo** command-line interface might report unknown version numbers on the Windows systems with system locale set to a non-English language.
- **Problem:** The **tklmReplicationStatus** CLI command creates the following message even if the replication configuration file exists and has entries in it.

  ```
  CTGKM2222E No valid replication config file exists.
  ```

  Workaround: This message is displayed whenever there is an issue with an entry in the replication configuration file or when the file does not exist. Check the replication audit log or the main product audit log to determine which entry(s) is having the issue. Correct the issue, restart IBM Security Key Lifecycle Manager, and try again.
- **Problem:** You might not see the desired device to be added in the IBM Security Key Lifecycle Manager GUI. However, the device is listed in the command-line interface output.

  Workaround: Because the device is partially added in the IBM Security Key Lifecycle Manager database, delete the device from the database and then add it manually by using the graphical user interface. For the detailed workaround information, see the technote at: http://www.ibm.com/support/docview.wss?uid=swg21608874
- **Problem:** The IBM Security Key Lifecycle Manager backup operation might fail with the following errors in the `sklm_audit.log` file:

  ```
  outcome=[result=successful]
  ...
  resource=[name=
  CTGKS0040E Socket timed out.
  ```

  Or

  ```
  CTGKS0040E Internal Error: Process Message failed
  ```

  Workaround: The error CTGKS0040E indicates the occurrence of socket timeout. The following technote describes the problem and the workaround: http://www-01.ibm.com/support/docview.wss?uid=swg21610328
- **Problem:** When you start IBM Security Key Lifecycle Manager, an error like this example might occur:

  ```
  ADM6023I The table space "table space name"
  (ID "number") is in state 0x"2001100".
  The table space cannot be accessed. Refer to the documentation
  for SQLCODE -290
  ```

  Workaround: You might experience this error because of the missing table space. To fix this issue, see the workaround information at: http://www-01.ibm.com/support/docview.wss?uid=swg21609130
- **Problem:** After the installation of IBM Security Key Lifecycle Manager on the Russian native environment, the error messages `CTGKM0100E` and `CTGKM0900E` are displayed when you open the Configuration page.

  This problem is because of this known DB2 issue:

  ```
  IC87668 CONNECTION FAILS WITH SQLCODE -4220 WHEN CHARACTERS IN CLIENTUSER
  ACCOUNT CAN NOT BE CONVERTED TO EBCDIC 500
  ```

Workaround: Replace the `db2jcc.jar` file in your existing WebSphere Application Server environment with the DB2, version 10.5 `db2jcc.jar` file. You can download the DB2 JDBC driver from the following location and the driver is supported for the DB2 versions 9.5 – 10.5: http://www-01.ibm.com/support/docview.wss?uid=swg21363866

- **Problem:** You cannot use the IBM Security Key Lifecycle Manager REST services to delete the certificate default rollovers that are added by using the IBM Security Key Lifecycle Manager CLI commands.

  You cannot use **`Certificate Default Rollover Delete REST Service`** to delete the certificate default rollovers that are added by using the **`tklmCertDefaultRolloverAdd`** CLI command

  Workaround: Use the CLI commands to delete certificate default rollovers that are added through CLI commands. For example, you must use the **`tklmCertDefaultRolloverDelete`** command to delete the certificate default rollovers that are added by using the **`tklmCertDefaultRolloverAdd`** command.
- **Problem:** On the graphical user interface, the description is not correctly displayed if you use the "<" and ">" special characters in the certificate description field.

  Workaround: Do not use the "<" and ">" characters for a certificate description.
- **Problem:** On the graphical user interface, when you click on any menu (other than the **Welcome** menu) and then a quick succession click on the **Welcome** menu, the welcome page does not open.

  Workaround: To resolve this issue, do any of the following tasks:

  – Click the **Return home** link on the page.

  – Click some other menu. After the page is loaded, click the **Welcome** menu.
- **Problem:** The KMIP **`Recertify()`** operation cannot be used for a certificate request.

  This issue is a known limitation.
- **Problem:** If the size of backup files that are created by using the backup operation exceeds 4 GB, the restore operation fails when these backed-up files are used.

  This issue is a known limitation.
- **Problem:** The IBM Security Key Lifecycle Manager backup operation fails with the following error message:

  ```
  Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy
   Files are required. For more information, see the "Backup and restore"
  section of IBM Security Key Lifecycle Manager documentation on IBM Knowledge
  Center.
  ```

  Workaround: You must install Java Cryptography Extension (JCE) unlimited strength jurisdiction policy files if IBM Security Key Lifecycle Manager backup operation uses the AES 256-bit key for data encryption. For the instructions, see the "Installing Java Cryptography Extension unlimited strength jurisdiction policy files" topic in the Administering section of IBM Security Key Lifecycle Manager documentation on IBM Knowledge Center.
- **Problem:** On Windows 2012 R2, the IBM Security Key Lifecycle Manager backup operation fails with the following error message:

  ```
  wsadmin>print AdminTask.tklmBackupRun("[-backupDirectory tklmbackup
  -password password]")
  (1) Backup operation fails.
  CTGKM0910E  I/O error while creating backup jar file tklmbackup\sklm_v2.5.0.3_
  20140721182309+0530_backup.jar
  Error message: C:\SKLM\SKLMDB.0.SKLMDB2.DBPART000.20140721182309.001 (Access
  is denied.)
  ```

Workaround: Restart WebSphere Application Server as an Administrator:

1. Click **Start** > **All Programs** > **Accessories**.
2. Right-click **Command Prompt**.
3. Click **Run as administrator**.
4. Change to the `%WAS_HOME%\profiles\KLMProfile\bin` directory. This directory contains the `startServer.bat` file.
5. Run the following command:

```
C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\KLMProfile\
bin>startServer.bat server1
```

WebSphere Application Server limitations, problems, and workaround

You might encounter the WebSphere Application Server problems, limitations, and workaround that are described in this topic.

- **Problem:** As the WASAdmin administrator, you might specify a lowercase name such as `user_lto` when you create a user. Then, you might create a role with an uppercase name such as `user_LTO` that is intended for the user. When the user later logs in, the role does not provide the expected role-based access, and errors occur.

  Workaround: The matching process is case-sensitive. Specify the names of a user and a user role with a case that matches for all characters.

- **Problem:** On Windows systems, the mapped drives are not displayed in the drop-down lists on the graphical user interface when you browse for a file. For example, on a page to back up files, the mapped drives are not visible when you browse for the backup repository location.

  Workaround: Use the command-line interface if you use a mapped drive. For example, to back up files, use the **tklmBackupRun** command. You can also find more workaround information in the technote that describes mapped network drives in Windows that are not visible to WebSphere Application Server. For more information, refer to this site:

  http://www.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg21316456&loc=en_US&cs=utf-8&lang=en

- **Problem:** Selecting the Back arrow fails to sequence through previous portlets that are visited within the WebSphere Application Server. For example, after a sequence of pages is viewed, selecting the Back arrow returns instead to the Welcome page.

  Limitation: The Back arrow does not cycle back through a sequence of pages. Use the choices in the left pane to navigate to a target page.

- **Problem:** You cannot access IBM Security Key Lifecycle Manager graphical user interface for the following conditions:
  - When WebSphere Application Server is already installed on the default port and is used by another application.
  - The same port is specified during IBM Security Key Lifecycle Manager installation.

  The IBM Security Key Lifecycle Manager installer cannot detect the port that is in use if the other application is down.

  Workaround: Ensure that the port you are specifying during installation is not used by another application on the same system.

- **Problem:** On AIX operating system, the restore operation fails if the WebSphere Application Server installation path differs from /opt/IBM/WebSphere/AppServer. The restore operation fails with the following error message when you run the **tklmBackupRunRestore** command.

  ```
  "CTGKM0850E An exception occurred during the restore operation.
  Examine the db2restore.log for exception information. Complete the restore
  operation before attempting any other IBM Security Key Lifecycle Manager
  tasks."
  ```

  The IBM Security Key Lifecycle Manager installer cannot detect the port that is in use if the other application is down.

  Workaround: Set the execute permission for the files under <*WAS_INSTALL_DIR*>/products/sklm/bin/db.

  ```
  chmod -Rf 755/<WAS_HOME>/products/sklm/bin/db
  ```

  For example:

  ```
  chmod -Rf 755/usr/IBM/WebSphere/AppServer/products/sklm/bin/db
  ```

Browser limitations, problems, and workaround

You might encounter the browser limitations, problems, and workaround that are described in this topic.

- **Problem:** Depending on the browser that you use, error results vary when you attempt to accept a pending LTO device and specify an incorrect key name.
  - Internet Explorer

    This error message appears:

    ```
    CTGKM0201E Cannot modify device.
    CTGKM0245E The key name specified is not known.
    ```

  - Firefox

    No error message appears. The device remains in the pending device list. Additional help appears on the pending device table.

  Workaround: Use either message format to recognize your need to correct the key name and try again.
- **Problem:** If you add a DS5000 storage server by using IBM Security Key Lifecycle Manager and Internet Explorer Version 8, you might be unable to close the Add Device dialog.

  Workaround: Ensure that the browser has enabled the Binary and script behaviors scripting setting under ActiveX controls and plug-ins. Take these steps:

  1. Open the browser and click **Tools > Internet Options > Security**.
  2. On the Security tab, click **Custom level**.
  3. Scroll the list of security settings to the ActiveX controls and plug-ins options and ensure that the Binary and script behaviors setting is enabled.
  4. Click **OK**.
- **Problem:** When you attempt to add a self-signed certificate, the cursor might not appear, depending on the browser that you use. With some browsers, the cursor might initially appear in fields such as a required text field for character entry. However, when additional help appears for the field, the cursor no longer displays or blinks to show which field has focus.

  Workaround: Ignore the missing cursor. You can successfully complete the entry by typing characters in the field.

- **Problem:** For an internal WebSphere Application Server certificate, the Internet Explorer browser reports a certificate error after you install and then first log on to IBM Security Key Lifecycle Manager.

  Workaround: The error occurs because the owner of the internal certificate is not in the list of trusted signing authorities. Install the certificate into each browser that you use to access IBM Security Key Lifecycle Manager.

  To install the certificate on a browser, take these steps:

  1. When you see a security alert that indicates that the company signing the certificate is not in the list of trusted companies, click **View Certificate**.
  2. An additional dialog displays the host name of the IBM Security Key Lifecycle Manager server as both `issued to` and `issues by name`.
  3. Install the certificate on the browser by clicking **Install Certificate**. Then, complete the instructions that the browser provides to install the certificate.
- **Problem:** On the Create Backup page, you cannot type the value for a path in the field that appears when you click **Browse**, in a browser session by using Internet Explorer version 6.0 with Service Pack 2. For example, you cannot type `/opt` as a value.

  Workaround: Use the drop-down arrow on the Browse File dialog to select the directory path.
- **Problem:** The IBM Security Key Lifecycle Manager console is not loading on the Internet Explorer, version 9.0 browser.

  Workaround: To load the IBM Security Key Lifecycle Manager console, you must change the **Document Mode** in the Internet Explorer browser:

  1. Click **Internet Explorer** > **Tools** > **Developer Tools**.
  2. Click **Developer Tools** > **Document Mode**.
  3. Select **Internet Explorer 9 Standards**.
  4. Refresh the page.

Documentation limitations, problems, and workaround

You might encounter documentation problems and use the workaround that is described in this topic.

- **Problem:** The content of error message CTGKM0583E does not describe the problem when you attempt to create a new key group with same name as an existing key group.

  Currently, you receive these messages:

  ```
  CTGKM0215E Cannot create key group.
  CCTGKM0583E You specified an existing key group name. Specify a different,
  unique key group name.
  ```

  No problem exists in matching the family type. The problem is that you attempted to specify an existing key group name.

  A corrected message might read:

  ```
  CTGKM1129E You specified an existing key group name. Specify a different,
  unique key group name.
  ```

  Limitation: The message content is incorrect.
- **Problem:** Accessibility software such as the Freedom Scientific JAWS screen reader application cannot read some tables of information in the IBM Security Key Lifecycle Manager Documentation. Similar tables in the graphical user interface help might have the same problem. For example, a screen reader cannot read the content of a table of status icons and their meanings in a topic about administering DS8000 storage images.

Limitation: The accessibility reader provides no additional information about the text or graphical content of some tables.

- **Problem:** An additional message would provide increased clarity after you run a successful migration from IBM Security Key Lifecycle Manager, version 1 to version 2 and then run the migration script again.

  Currently, you receive these messages:

  ```
  CTGKS0220I: The Security Key Lifecycle Manager migration started at <timestamp>
  CTGKS0153I The migration program succeeded during the previous run.
  ```

  However, an additional message could be provided. For example, the message might read:

  ```
  Examine the TKLM_HOME/migration/migrate.log file for more information.
  ```

  Limitation: No additional message is provided.

Problem determination

Problem determination topics describe error locations, diagnostic steps, and other information that you can use to identify problems and provide solutions with IBM Security Key Lifecycle Manager.

Error information locations

Several locations provide error information for IBM Security Key Lifecycle Manager:

IBM Security Key Lifecycle Manager audit log
The audit log contains most of the error messages. In the `SKLMConfig.properties` file, the location and file name are set in the **`Audit.handler.file.name`** property.

Errors reported in IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Manager reports error messages that are returned in the drive sense data. The error messages are typically called fault symptom codes or FSCs and are stored in the IBM Security Key Lifecycle Manager audit log.

Table 10. Errors that are reported by IBM Security Key Lifecycle Manager

Error Number	Description	Action
EE02	Encryption Read Message Failure, DriverErrorNotifyParameterError, Bad ASC & ASCQ received. ASC & ASCQ does not match with either of Key Creation/Key Translation or Key Acquisition operation.	The tape drive requested an unsupported action.
EE0F	Encryption logic error, Internal error, Unexpected error, Internal programming error.	
EE23	Encryption Read Message Failure: Internal error, Unexpected error.	The message received from the drive or proxy server cannot be parsed because of a general error.
EE25	Encryption Configuration Problem, Errors that are related to the drive table occurred.	Verify the contents of the IBM Security Key Lifecycle Manager drive table by using the key management panels on the IBM Security Key Lifecycle Manager graphical user interface, or by running the **tklmDeviceList()** command to verify whether the drive is correctly configured. For example, verify that the drive serial number, alias, and certificates are correct.

Table 10. Errors that are reported by IBM Security Key Lifecycle Manager (continued)

Error Number	Description	Action
EE29	Encryption Read Message Failure: Invalid signature	The message received from the drive or proxy server does not match the signature on it.
EE2B	Encryption Read Message Failure, Internal error, Either no signature in DSK or the signature in DSK cannot be verified.	
EE2C	Encryption Read Message Failure, QueryDSKParameterError, Error parsing a QueryDSKMessage from a device. Unexpected dsk count or unexpected payload.	The tape drive requested an unsupported function.
EE2D	Encryption Read Message Failure, Invalid Message Type	The IBM Security Key Lifecycle Manager server received a message out of sequence or received a message that it does not know how to handle.
EE2E	Encryption Read Message Failure, Internal error, Invalid signature type	The message received from the drive or proxy server does not have a valid signature type.
EE31	Encryption Configuration Problem, Errors that are related to the keystore occurred.	Check the key labels that you are trying to use or that are configured for the defaults. You can list the certificates that are available to IBM Security Key Lifecycle Manager by using the **tklmKeyList()** command. If you know that you are trying to use the defaults, then run the **tklmDeviceList()** command on the IBM Security Key Lifecycle Manager server to verify whether the drive is correctly configured (for example, the drive serial number, and associated aliases/key labels are correct). If the drive without associated aliases or key labels, check the values of the drive.default.alias1 and drive.default.alias2 table entry for the device group in the IBM Security Key Lifecycle Manager database. Use the **tklmDeviceGroupAttributeList** and **tklmDeviceGroupAttributeUpdate** commands to view and change the table value. **Note:** For DS5000 storage servers, IBM Security Key Lifecycle Manager erroneously returns an error code of `EE31` when a key group runs out of keys and the **`stopRoundRobinKeyGrps`** property is enabled. The error can also occur for an LTO device group. The event is not a keystore error. To correct the problem, add more keys to the key group that is documented in the audit event.
EE32	IBM Security Key Lifecycle Manager was unable to locate the key that is requested on a key for a read request by an LTO device.	Use the LTO management panel or **tklmKeyList()** command to verify the existence of the requested key.

Table 10. Errors that are reported by IBM Security Key Lifecycle Manager (continued)

Error Number	Description	Action
EE34	The key group that is configured as the system default or is assigned as a device default is run out of keys. This error can also occur if: • A device requests for a key that the device does not have permission to receive. • The requested key is assigned to a different device group. For example, an LTO device requests a key from a key group that is assigned to a user-defined LTO device group or to the DS5000 device family.	IBM Security Key Lifecycle Manager is configured to not reuse keys in key groups and one of the key groups is run out of keys. Use the LTO management panel to add more keys to this group.
EE35	This error can occur if you do not make a backup after keys or certificates are created. See the reference topic on the backup.keycert.before.serving property.	Back up newly created keys or certificates.
EEE1	Encryption logic error, Internal error, Unexpected error: EK/EEDK flags conflict with subpage.	
EF01	Encryption Configuration Problem, Drive not configured.	The drive that is trying to communicate with the IBM Security Key Lifecycle Manager server is not present in the drive table. Run the **tklmDeviceList()** command to check whether the drive is in the list. If not, configure the drive manually by using the **tklmDeviceAdd()** command with the correct drive information or set the device.AutoPendingAutoDiscovery attribute to an appropriate value by using the **tklmDeviceGroupAttributeUpdate** command.

Error codes and messages for common error scenarios in REST services

IBM Security Key Lifecycle Manager REST services might return error messages when you access IBM Security Key Lifecycle Manager server functions.

The following table lists the error scenarios that you might encounter when you work with IBM Security Key Lifecycle Manager REST services:

Error scenario	HTTP status code	IBM Security Key Lifecycle Manager application code	IBM Security Key Lifecycle Manager application message
Invalid request parameter was specified in the service request.	400	CTGKM0630E	`CTGKM0630E Validation error: \"Invalid name \" for parameter \"userId\"`
After the user is logged in to the server, authorization header was not specified for other REST services.	400	CTGKM6002E	`CTGKM6002E Bad Request: Invalid user authentication ID or invalid request format.`

Error scenario	HTTP status code	IBM Security Key Lifecycle Manager application code	IBM Security Key Lifecycle Manager application message
Incorrect user name or password was specified.	401	CTGKM6003E	`CTGKM6003E Authentication Failure: Incorrect userid or password.`
After the user is logged in to the server, an invalid authentication ID was specified in the authorization header for other REST services.	401	CTGKM6004E	`CTGKM6004E User is not authenticated or has already logged out`
An incorrect or unsupported HTTP operation was used for REST services. For example, POST operation was used instead of GET operation.	405	NA	NA
REST service request was sent with an empty HTTP request body.	500	NA	`Error 500: javax.servlet.ServletException: java. io.IOException: Expecting '{' on line 1, column 0 instead, obtained token: 'Token: EOF'`

Audit files

IBM Security Key Lifecycle Manager has a default directory for audit data. The location depends on which operating system is used.

Distributed systems

In the *SKLM_HOME*/config/SKLMConfig.properties file, edit the **Audit.handler.file.name** property to set this directory. The default is value is:

```
Audit.handler.file.name=logs/audit/sklm_audit.log
```

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.

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 “Copyright and trademark information” at 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

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

O

P

R

S

T

U

W

X