Troubleshooting and support for IBM Security Key Lifecycle Manager V2.7

Contents

Troubleshooting and support

Troubleshooting and support information for IBM Security Key Lifecycle Manager helps you understand, isolate, and resolve problems.

The troubleshooting section includes descriptions of the events that generated the problems, the symptoms, the environment, the possible causes, and suggestions for recovery actions.

The support section provides information about the tools and options that you can use to connect to the service and support organization. The support section also includes general information about searching knowledge bases, getting fixes, and contacting IBM® support, as well as product-specific topics.

To resolve a problem on your own, you can find out how to identify the source of a problem, how to gather diagnostic information, where to get fixes, and which knowledge bases to search. If you need to contact IBM Support, you can find out what diagnostic information the service technicians need to help you address a problem.

General information

To get started with troubleshooting, familiarize yourself with the basic techniques for troubleshooting and on how to contact and exchange information with IBM Support. You can also use tools such as IBM knowledge base, Fix Central, and Support Portal.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it

down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multisite installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running in an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the IBM Security Key Lifecycle Manager documentation. However, sometimes you need to look beyond the documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Search for content by using the IBM Support Assistant (ISA).

  ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
- Find the content that you need by using the IBM Support Portal.

  The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one

place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

- Search for content about IBM Security Key Lifecycle Manager.
  - IBM Security Key Lifecycle Manager Support website.
- Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the **Search** field at the top of any ibm.com® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

  Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Getting fixes from Fix Central

You can use Fix Central to find the fixes that are provided by IBM Support for various products, including IBM Security Key Lifecycle Manager. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A IBM Security Key Lifecycle Manager product fix might be available to resolve your problem.

About this task

Procedure

To find and install fixes:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from Fix Central. This site provides download, installation, and configuration instructions for the update installer.
2. Select IBM Security Key Lifecycle Manager as the product, and select one or more check boxes that are relevant to the problem that you want to resolve. For details, see: http://www.ibm.com/systems/support/fixes/en/fixcentral/help/faq_sw.html.
3. Identify and select the fix that is required.
4. Download the fix.
   a. Open the download document and follow the link in the "Download Package" section.
   b. When you download the file, ensure that the name of the maintenance file is not changed. This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. Apply the fix.
   a. Follow the instructions in the "Installation Instructions" section of the download document.
   b. For more information, see the "Installing fixes with the Update Installer" topic in the product documentation.

6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates. See "Subscribing to Support updates" on page 7.

Contacting IBM Support

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM *maintenance contract name*, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

For information about the types of available support, see the Support portfolio topic in the *Software Support Handbook*.

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. See the Contacting IBM Support topic in the *Software Support Handbook*. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
     a. Download and install the ISA tool from the ISA website. See www.ibm.com/software/support/isa/.
     b. Open ISA.
     c. Click **Collection and Send Data**.
     d. Click the **Service Requests** tab.
     e. Click **Open a New Service Request**.

     Using ISA in this way can expedite the analysis and reduce the time to resolution.
   - Online through the IBM Support Portal: You can open, update, and view all of your service requests from the **Service Request** portlet on the Service Request page.
   - By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page. You can also see the Contacts page in the *Software Support Handbook*.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit

from the same resolution. See "Exchanging information with IBM."

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:
   - Collect the data manually.
   - Collect the data automatically.
3. Compress the files by using the `.zip` or `.tar` file format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
   - IBM Support Assistant
   - The Service Request tool
   - Standard data upload methods: FTP, HTTP
   - Secure data upload methods: FTPS, SFTP, HTTPS
   - Email

   All of these data exchange methods are explained on the IBM Support website.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:
   a. Change to the `/fromibm` directory.
      ```
      cd fromibm
      ```
   b. Change to the directory that your IBM technical-support representative provided.
      ```
      cd nameofdirectory
      ```

3. Enable binary mode for your session.

   ```
   binary
   ```

4. Use the **get** command to download the file that your IBM technical-support representative specified.

   ```
   get filename.extension
   ```

5. End your FTP session.

   ```
   quit
   ```

Subscribing to Support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

About this task

By subscribing to receive updates about IBM Security Key Lifecycle Manager, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to updates by using one of two approaches:

RSS feeds

For information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds site.

My Notifications

With **My Notifications**, you can subscribe to Support updates for any IBM product. **My Notifications** replaces **My Support**, which is a similar tool that you might have used in the past. With **My Notifications**, you can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). **My Notifications** enables you to customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

Procedure

To subscribe to Support updates:

1. Subscribe to My Notifications by going to the IBM Support Portal and click **My Notifications** in the **Notifications** portlet.
2. Sign in using your IBM ID and password, and click **Submit**.
3. Identify what and how you want to receive updates.
   a. Click the **Subscribe** tab.
   b. Select the appropriate software brand or type of hardware.
   c. Select one or more products by name and click **Continue**.
   d. Select your preferences for how to receive updates, whether by email, online in a designated folder, or as an RSS or Atom feed.
   e. Select the types of documentation updates that you want to receive, for example, new information about product downloads and discussion group comments.
   f. Click **Submit**.

Results

Until you modify your **RSS feeds** and **My Notifications** preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Related information

- IBM Software Support RSS feeds
- Subscribe to My Notifications support content updates
- My Notifications for IBM technical support
- My Notifications for IBM technical support overview

Problem determination

Problem determination topics describe error locations, diagnostic steps, and other information that you can use to identify problems and to provide solutions to resolve the problems.

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.

For more information about log files and locations, see the "Important log files and locations" on page 12 topic.

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 1. 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.

Table 1. Errors that are reported by IBM Security Key Lifecycle Manager (continued)

Error Number	Description	Action
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.
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.

Table 1. Errors that are reported by IBM Security Key Lifecycle Manager (continued)

Error Number	Description	Action
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.
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.	

Table 1. Errors that are reported by IBM Security Key Lifecycle Manager (continued)

Error Number	Description	Action
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.`
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

Error scenario	HTTP status code	IBM Security Key Lifecycle Manager application code	IBM Security Key Lifecycle Manager application message
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'`

Installation and migration log files

If the installation or migration encounters an unexpected error condition, use the log files to determine the cause of the problem.

Background information

The installation program uses several subprograms, components, and subsystems during installation. Many error conditions occur because a subprogram fails.

Installation subprograms, components, and systems

You might see these names or abbreviations in the log files:

- DB2®
- IBM Installation Manager

Installation phases

Error conditions that occur and the log files available to you depend on the phase in which the error occurred:

1. Introductory that includes panels for language selection, details of the packages to be installed, and the license agreement. The installation program also runs a system prerequisites check to verify the minimum requirements to install the product.
2. DB2 installation that includes panels to gather information for installing DB2. After you enter the information, the installation program installs DB2.
3. Middleware installation that includes panels that gather information to install WebSphere® Application Server middleware. After you enter the information, the installation program installs the middleware.

   IBM Security Key Lifecycle Manager is installed during this phase.

Important log files and locations

The installation of IBM Security Key Lifecycle Manager and its components generates log files that you can read to ensure that the installation is completed successfully. The installation error logs provide critical information.

The following table list the log files and the file locations that are generated when you use the default installation settings.

Table 2. Location of installation log files

Log File	Description	Location
`db2_install.log`	DB2 installation log file.	**Windows systems** `drive:\<IM App Data Dir>\logs\sklmLogs\` `C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\` **Linux systems** `/<IM App Data Dir>/logs/sklmLogs/` `/var/ibm/InstallationManager/logs/sklmLogs/`
`db_config.log`	Contains information about IBM Security Key Lifecycle Manager database creation and table creation.	**Windows systems** `drive:\<IM App Data Dir>\logs\sklmLogs\` `C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\` **Linux systems** `/<IM App Data Dir>/logs/sklmLogs/` `/var/ibm/InstallationManager/logs/sklmLogs/`
Various `*.xml` and `*.log` files	IBM Security Key Lifecycle Manager installation log files. You can verify the installation, modification, or uninstallation of IBM Security Key Lifecycle Manager by checking the log file that the IBM Installation Manager creates.	**Windows systems** `drive:\<IM App Data Dir>\logs\` `C:\ProgramData\IBM\Installation Manager\logs\` **Linux systems** `/<IM App Data Dir>/logs/` `/var/ibm/InstallationManager/logs/`
Various `*.out` and `*.err` files	STDOUT and STDERR files that are generated during installation. The **.err** file sizes are zero bytes if the operation they represent was successful. Examine error files with sizes greater than zero.	**Windows** *WAS_HOME*`\logs\` `C:\Program Files\IBM\WebSphere\AppServer\logs\` **Linux** *WAS_HOME*`/logs/` `/opt/IBM/WebSphere/AppServer/log/`

Table 2. Location of installation log files (continued)

Log File	Description	Location
`migration.log`	After you migrate existing data (earlier version) into the new installation, you can review the migration log file to verify whether the process was successful, or for troubleshooting purposes.	**Windows systems** `drive:\<IM App Data Dir>\logs\sklmLogs\` `C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\` **Linux systems** `/<IM App Data Dir>/logs/sklmLogs/` `/var/ibm/InstallationManager/logs/sklmLogs/`
`sklmInstall*.log`	IBM Security Key Lifecycle Manager installer log files. The log files are created when each step of the installation is run. You can read these log fines to verify whether the product is installed successfully.	**Windows** `%temp%/sklmInstaller*.log*` **Linux** `${TMPDIR}/sklmInstaller*.log`
Log files in `sklmPRS`	The `sklmPRS` folder contains log files for detailed output of the prerequisite scan activity (`precheck.log`) and for the results of the scan (`results.txt`).	**Windows** `%temp%/sklmPRS/` **Linux** `${TMPDIR}/PRS/`

Log files to troubleshoot problems

The timing of an error can provide an idea of which log file to use first. The two places an error might occur are immediately after the DB2 phase, and immediately after the middleware phase. Use this list to determine where to start.

During or immediately after the DB2 installation phase

1. If the error occurs early enough, you might want to check the `db2_install.log`, `prsResults.xml`, and `sklmInstaller*.log` files.
2. If the error occurs later during this phase, the `sklmV27properties` directory might contain results of some of the DB2 configuration, or results from the other subprograms that run during this phase.
3. The location of the error log file can vary depending on whether the error occurs during the DB2 phase, or at the end of the DB2 phase.

   At the end of the DB2 phase, the log files are copied from the `sklmV27properties` directory to the `<IM App Data Dir>\logs\sklmLogs` directory. See Table 2 on page 13 for the location of the files.

During or immediately after WebSphere Application Server installation phase

The log files to examine for errors are `db_config.log` and `sklmInstaller*.log` files.

Migration log file names and location

During the migration process, the migration program creates log files when it calls other programs or tools.

After you upgrade IBM Security Key Lifecycle Manager, and migrate your existing data into the new installation, you can review the `migration.log` file to verify whether the process was successful, or for troubleshooting purposes.

Windows systems

`drive:\<IM App Data Dir>\logs\sklmLogs`

For example: `C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\migration.log`

Linux systems

`/<<IM App Data Dir>>/logs/sklmLogs`

For example: `/var/ibm/InstallationManager/logs/sklmLogs/migration.log`

Examining an error log file

IBM Security Key Lifecycle Manager generates several log files that you can use to troubleshoot problems that occur when you install and configure IBM Security Key Lifecycle Manager.

Procedure

1. Review the list of log files. The log file to start with depends on the operating system and the phase of the installation. The list in "Log files to troubleshoot problems" on page 14 can provide a starting point. You might examine several log files before you find the one with the error messages.
2. Go to the directory with the log file, and open it with a text editor. On a Windows system, use a text editor that can process UNIX-style newline characters, such as Microsoft WordPad.
3. The most recent log entries are at the end of the file. Starting at the last entry in the log file, examine each entry. Take note of the program that is involved and the time stamp of the entry if it has one.

   After the final entry is reviewed, look at the entry before it. Review this entry as you did the previous entry. Scan for anything that is mentioned in both places such as file names or error conditions.

   Repeat the previous step, moving upward in the log file. There might be several entries with information that is related to the error condition. If the information in this log file is insufficient, look for more information in another log file.

   If there are no messages about an error, go to another log file.

Other information to gather

You must run several actions that might provide more information to verify installation.

- Check your free disk space. See Hardware requirements for minimum space requirements.

- See whether the DB2 instance is created. If so, this validates the DB2 installation.

  To verify that the DB2 instance was created, log in as the IBM Security Key Lifecycle Manager DB2 instance owner, go to the *DB_INSTANCE_HOME* directory, and run:

  ```
  db2ilist
  ```

  A list of the configured instances is displayed. The instance name for IBM Security Key Lifecycle Manager such as `sklmdb27` is typically in the list.
- Start and stop the IBM Security Key Lifecycle Manager database server by using the instance owner user ID. This validates the database creation.

  To start and stop the database, log in as the IBM Security Key Lifecycle Manager DB2 instance owner, go to the *DB_INSTANCE_HOME* directory, and run the **db2start** and **db2stop** commands on the database.
- Display a list of the tables in the DB2 database. This validates the Dynamic Data Language process.

  To display the list of tables, log in as the IBM Security Key Lifecycle Manager DB2 instance owner, go to the *DB_INSTANCE_HOME* directory, and run these commands:

  ```
  db2 connect to sklm_database user sklm_instance_owner_userid \
  using sklm_instance_owner_passwd

  db2 list tables

  db2 describe table table_name
  ```
- Determine whether the Java process for WebSphere Application Server is running. A running process validates the WebSphere Application Server installation.

  To determine whether the Java process is running, stop and restart the server by going to the *WAS_HOME*`/bin` directory and running these commands:

  ```
  stopServer.sh server1
  startServer.sh server1
  ```

  If global security is enabled, add these parameters to the commands to stop and restart your server:

  ```
  -username was_admin_id -password was_admin_passwd
  ```

  On Windows systems, you can also open the Windows Services console and verify that the service for the `KLMProfile` is started.
- Start the IBM Security Key Lifecycle Manager application to validate the IBM Security Key Lifecycle Manager installation and the overall installation.

  To start the IBM Security Key Lifecycle Manager application, start the WebSphere Application Server, and look for the IBM Security Key Lifecycle Manager task.

Product installation problems and workaround

Use the information in this section to troubleshoot problems that you might encounter during IBM Security Key Lifecycle Manager installation, uninstallation, or migration process.

Migration fails if keystore contains a certificate with a key that has Elliptic Curve public key algorithm

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.

To resolve tis problem, 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
```

Installation fails on a system that has insufficient disk space

IBM Security Key Lifecycle Manager installation fails on a computer that has insufficient disk space and also does not remove files that the installation process created.

Provide enough free disk space on the system according to the requirements to allow successful completion of the product installation. You must manually remove the files that the failed installation created.

Unable to delete a migrated rollover

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.

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

Correct path not displayed to locate Encryption Key Manager file

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**.

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

Unable to create specified administrative user ID for DB2

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 error message indicates that you must ensure that the password meets system requirements and that the home directory has adequate disk space.

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

```
/mydb2home
```

Installation program becomes unresponsive if you use Exceed

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.

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

Incorrect display of device serial numbers

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.

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

Migration might cause a drive of a specific type to appear with an `UNKNOWN` label

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.

Migration from Encryption Key Manager does not resolve the device group for all drives. It is a limitation.

The current migration result is shown in the following table:

Table 3. 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.

Migration fails when the system locale is set as non-English language

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. It is a limitation.

Perform migration with English language locale set.

Uninstallation of WebSphere Application Server or DB2 might cause problems

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.

Error when you install IBM Security Key Lifecycle Manager on AIX operating system

You might see the error message when you install IBM Security Key Lifecycle Manager on AIX operating system.

```
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.
```

To fix this issue, see the workaround information at: http://www-01.ibm.com/support/docview.wss?uid=swg21631478

Error when you install IBM Security Key Lifecycle Manager on Linux operating system

You might see the error message when you install IBM Security Key Lifecycle Manager on Red Hat Enterprise Linux operating system.

```
[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
```

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

Error when you install IBM Security Key Lifecycle Manager on 64-bit Linux operating system

You might see the error message when you install IBM Security Key Lifecycle Manager on 64-bit Red Hat Enterprise Linux operating system.

```
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

Silent installation fails on 64-bit Linux for System z

Silent installation of IBM Security Key Lifecycle Manager on 64-bit Linux for System z fails with the error message.

```
wrong ELF class: ELFCLASS64
```

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

Unable to install IBM Security Key Lifecycle Manager as a non-root user

Unable 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.

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

Data source connection and restore operation fails

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.
```

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.

Prerequisite Scanner for non-root installation fails

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 under `%temp%/sklmPRS`.

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

This problem is a known limitation.

As a workaround for this limitation, create a `sklmInstall.properties` file in the following directories with the property **`SKIP_PREREQ=true`** to skip the Prerequisite Scanner:

Windows
`%TEMP%`

UNIX `/tmp`

Unable to install IBM Security Key Lifecycle Manager when a system has multiple partitions

You cannot install IBM Security Key Lifecycle Manager when a system has multiple partitions.

Installation fails when:

- You choose to install on the partition other than the `/opt` directory.
- Less space on the `/opt` directory.

The installer displays the following error message:

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

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`

Incorrect display disk space usage in "/opt" directory

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.

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

Unable to migrate description specified for the user group

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

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.

Time stamp of the backup file is not displayed

When IBM Tivoli Key Lifecycle Manager, 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.

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

Unable to validate keystore password

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.

Installation fails if UAC setting is set to Always notify

Installation of IBM Security Key Lifecycle Manager can fail if the Windows User Account Control (UAC) setting is set to Always notify.

To fix this issue, see the workaround information at: http://www-01.ibm.com/support/docview.wss?uid=swg21665207

Installation fails on Windows 2012 R2 operating system

IBM Security Key Lifecycle Manager installation fails on Windows 2012 R2 operating system with the error message:

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

To fix this issue, run the following steps:

1. Update the Windows UAC setting as described in the 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.

Warning message in %temp%/sklmPRS/results.txt file

On Windows operating system, the %temp%/sklmPRS/results.txt file contains the 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.
```

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

Installation and uninstallation processes fail or exit without completion in silent mode

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
```

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

```
./imcl -input full_path_to_response_file -silent
```

Keys are added to a newly created key group during Encryption Key Manager migration to IBM Security Key Lifecycle Manager, Version 2.6

During IBM Security Key Lifecycle Manager, Version 2.6 installation, when you migrate Encryption Key Manager, some of the keys that are not part of any key groups in Encryption Key Manager are added to a newly created key group DefaultMigrateGroup.

This issue is a known limitation and has no impact on serving keys to the devices.

File handles are not closed properly if the upgrade task fails

Applying Fix Pack 5 on IBM Security Key Lifecycle Manager, Version 2.5 fails and throws Java error with exit code 1.

When the upgrade task to IBM Security Key Lifecycle Manager, Version 2.5, Fix Pack 05 fails, the file handles are not cleaned up properly. Because of this problem, the Java error is thrown when you retry the installation process. To resolve this issue, restart the system or increase the number of file handles. After you restart the system, ensure that DB2 comes up before you retry the upgrade process.

Error when installing IBM Security Key Lifecycle Manager using the launchpad.sh command

On some versions of the Linux operating system, you might see the error message when you start the installation program by using the **launchpad.sh** command from the DVD.

```
-bash: ./launchpad.sh: /bin/sh: bad interpreter: Permission denied
```

This problem occurs when the default automount settings have `-noexec` permission. Change the permissions before you run the installation program. For example, type:

```
mount -o remount,exec /media/SKLM_LINUX_Base
```

Unexpected messages are displayed when installing IBM Security Key Lifecycle Manager in silent mode

On Windows operating system, when you are installing IBM Security Key Lifecycle Manager in silent mode, unexpected warning messages might get displayed.

```
InstallRegistry.xml file not found at location :
C:\ProgramData\IBM\Installation Manager\installRegistry.xml
```

You can ignore the messages and continue with the installation task.

Uninstallation of IBM Security Key Lifecycle Manager does not remove the application start link

On Red Hat Enterprise Linux systems, the application start link is not removed even after you uninstall IBM Security Key Lifecycle Manager.

This is a known limitation. You can safely remove the link by manually deleting it according to the procedure provided by the operating system.

Error message about missing DB2 installation location after IBM Security Key Lifecycle Manager uninstallation

On all the operating systems, an error message about missing DB2 installation location might display after you uninstall IBM Security Key Lifecycle Manager that was installed by using existing DB2.

For example, the following error message on the uninstallation panel is displayed for Linux operating system.

```
The "IBM DB2" package group's "/opt/IBM/DB2SKLMV27" install location
is missing or empty.
```

This is a known limitation. You can ignore this error message.

Problems during cross-migration of IBM Tivoli Key Lifecycle Manager, Version 2.0.1 data

After the cross-migration of data from IBM Tivoli Key Lifecycle Manager, Version 2.0.1 to IBM Security Key Lifecycle Manager, Version 2.7, device type attributes such as `machine affinity`, `auto pending`, and `auto accept` of various device types might not get migrated.

This issue is a known limitation. To resolve this problem, reset those device attributes in the corresponding device type UI pages.

Error message during Encryption Key Manager to IBM Security Key Lifecycle Manager migration

Error message is displayed when you are migrating Encryption Key Manager data to IBM Security Key Lifecycle Manager, Version 2.7 if the data contains any certificate (Subject Name or Common Name) with length more than 512 characters.

The restore.log file shows the following error message.

```
error:value=nullcolumn=LENGTHjavatype=class
java.lang.Integervalue=nullcolumn=ORIGINAL_CREATION_DATEjavatype=class
javax.xml.datatype.XMLGregorianCalendarvalue=nullcom.ibm.db2.jcc.am.SqlDataException:
DB2 SQL Error: SQLCODE=-302, SQLSTATE=22001, SQLERRMC=null, DRIVER=3.70.4Ending Restore at
Thu Sep 15 02:47:45 EDT 2016
```

This issue is a known limitation. In IBM Security Key Lifecycle Manager, the length of the certificate (Subject Name or Common Name) must not exceed 512 characters.

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

You might encounter some issues and limitations during the deployment or usage of IBM Security Key Lifecycle Manager. This section describes the IBM Security Key Lifecycle Manager server problems, workaround, and limitations.

An error code of EE31 is returned when a key group runs out of keys

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.

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.

IBM Security Key Lifecycle Manager operations take significant amounts of time

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.

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 - `IBM WebSphere Application Server V8.5 - SKLM26Server`.

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

Key group creation might time out

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

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.

Login fails with an error message

After a IBM Security Key Lifecycle Manager session times out, your first attempt to log in fails with an error message.

For 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.
```

Ignore the message and log in again.

KMIP client is unable to locate the device

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.

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

Problem in reaching the maximum limit for a multi-valued KMIP attribute

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

Use the **tklmConfigUpdateEntry** command or **Update Config Property REST Service** to change the `mv.attribute.max.values` property in the `SKLMConfig.properties` file. Update this property only if a problem occurs in reaching the maximum limit for a multi-valued attribute.

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
```

You might require to change values for a KMIP custom attribute

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

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
```

IBM Security Key Lifecycle Manager server fails to initialize

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.

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.

Format for date field

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**0009, rather than **2**009.

You can successfully submit the entry by typing the value with the expected format of yyyy for the year. For example, type 2010.

Unable to remove some files in WebSphere Application Server directories

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.

If you cancel an in-progress installation of IBM Security Key Lifecycle Manager, ensure that you manually delete the *WAS_HOME* directory.

Unable to associate certificate or key group to a device

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.

To successfully associate certificates or key groups with devices, do not use a trailing asterisk to name certificates or key groups.

Some commands print inaccurate syntax statements

In interactive mode, some commands print inaccurate syntax statements to the console. The statements omit two brackets for the attribute flag.

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]]"]')
   ```

IBM Security Key Lifecycle Manager session times out

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.

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.

Database connection fails

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
```

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.
  ```

- Change the password for the IBM Security Key Lifecycle Manager instance owner.
  1. On Windows systems, click **Start** > **Control Panel** > **Administrative Tools** > **Computer Management** > **System Tools** > **Local Users and Groups** > **Users**.
  2. Change the password for the IBM Security Key Lifecycle Manager instance owner.

- 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)
  ```
- Restart the instances that you stopped.
- 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)
  ```
- Log in as WASAdmin to a **wsadmin** session.
- Use the **wsadmin** command to change the password of the WebSphere Application Server data source:
  1. The following command lists JAASAuthData entries:

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

     The result might be:

     ```
     (cells/SKLMCell|security.xml#JAASAuthData_1379859888963)
     ```
  2. 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
     ```
  3. 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]]')
     ```
  4. Save the changes:

     ```
     print AdminConfig.save()
     ```
  5. 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.

     a. Open the Control Panel and click **Administrative Tools** > **Computer Management** > **Services and Applications** > **Services**.

     b. Stop and start the IBM Security Key Lifecycle Manager server service, which has a name like IBM WebSphere Application Server V9.0 - SKLM27Server.
  6. Verify that you can connect to the database by using the WebSphere Application Server data source.

a. 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
   ```

b. 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)')
   ```

c. 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)')
   ```

d. 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.

Limit to length of key labels

Although in IBM Security Key Lifecycle Manager you can 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.

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

Invalid date format

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.

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.

Error message when you run `tklmReplicationStatus` CLI command

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.
```

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 entries are having the issue. Correct the issue, restart IBM Security Key Lifecycle Manager, and try again.

Problems adding device by using graphical user interface

You might not see the device to be added in the IBM Security Key Lifecycle Manager GUI. However, the device is listed in the command-line interface output.

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 athttp://www.ibm.com/support/docview.wss?uid=swg21608874.

IBM Security Key Lifecycle Manager backup operation might fail

The IBM Security Key Lifecycle Manager backup operation might fail with the errors in the `sklm_audit.log` file.

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

Or

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

The error `CTGKS0040E` indicates the occurrence of socket timeout. The technote describes the problem and the workaround http://www-01.ibm.com/support/docview.wss?uid=swg21610328.

Error occurs because of missing table space

The IBM Security Key Lifecycle Manager backup operation might fail with the errors in the `sklm_audit.log` file.

```
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
```

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

Error message when you open Configuration page on Russian native environment

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
```

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

Unable to use REST services to delete certificate default rollovers

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

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.

Incorrect display of certificate description if you use special characters

On the graphical user interface, the description is not correctly displayed if you use the "<" and ">" special characters in the certificate description field.

Do not use the "<" and ">" characters for a certificate description.

IBM Security Key Lifecycle Manager welcome page does not appear

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.

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.

KMIP `Recertify()` operation cannot be used

The KMIP **Recertify()** operation cannot be used for a certificate request.

This issue is a known limitation.

IBM Security Key Lifecycle Manager restore operation fails

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 problem is a known limitation.

Backup operation fails if JCE policy files are not installed

The IBM Security Key Lifecycle Manager backup operation fails with the 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.
```

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.

Backup operation fails on Windows 2012 R2

On Windows 2012 R2, the IBM Security Key Lifecycle Manager backup operation fails with the 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.)
```

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
   ```

Cross-platform backup and restore operation for earlier versions of IBM Security Key Lifecycle Manager fails

Backup and restore operation fails when you use the cross-platform backup and restore utility to back up and restore data of earlier versions (10, 2.0, 2.0.1, and 2.5) of IBM Security Key Lifecycle Manager and Encryption Key Manager.

Before you run the cross-platform backup and restore operations, you must configure the `backup.properties` and `restore.properties` files. On Windows system, if the values in these files contain leading or trailing spaces, the backup and restore operations might fail.

To resolve the problem, ensure that there are no leading or trailing spaces in the `backup.properties` and `backup.properties` files.

Data is not populated on the Automated Clone Replication Configuration page

After configuring and saving the IBM Security Key Lifecycle Manager instance as Replication Master, if you immediately access the Automated Clone Replication Configuration page for any updates, data is not populated for the **Replication backup encryption passphrase** and **Confirm replication backup encryption passphrase** fields.

To resolve this problem, wait for a while and refresh the page before you save the data again.

Synchronization issues between WebSphere Application Server and DB2 on Linux systems

On Linux systems, there might be problems with the sequence in which WebSphere Application Server and DB2 starts up after a system restart. WebSphere Application Server might start before DB2.

To resolve this problem, see details in this technote: http://www-01.ibm.com/support/docview.wss?uid=swg21969891

Error changing user password for IBM Security Key Lifecycle Manager

On windows system, when `SKLMAdmin` user tries to change the password by using the `Change Password` option, which is available in IBM Security Key Lifecycle Manager graphical user interface, the password gets changed, but the error message is displayed on the screen.

The following error message is displayed when you are changing the password.

```
com.ibm.websphere.wim.exception.WIMApplicationException: com.ibm.websphere.wim.e
xception.WIMApplicationException: CWWIM4508E  Virtual member manager failed to w
rite to the 'C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\KLMProfile\
config\cells\SKLMCell\fileRegistry.xml' file: 'CWWIM4508E  Virtual member manage
r failed to write to the 'C:\Program Files (x86)\IBM\WebSphere\AppServer\profile
s\KLMProfile\config\cells\SKLMCell\fileRegistry.xml' file: 'Caller is not in the
required role to access restricted document(s)'.'.
```

The password is changed according to your requirements, and you can ignore the error message.

Error creating user-defined device group on a migrated system

Error message is displayed when you try to create a user-defined device group on some of the systems with IBM Security Key Lifecycle Manager, Version 2.7 that has migrated data.

To create a user-defined device group on such systems with migrated data, you must run the following steps.

Windows

1. Open a command-prompt and run the following command.

   ```
   d2cmd
   set DB2INSTANCE=sklmdb27
   db2 connect to sklmdb27 user username using password
   ```

   Where,

   sklmdb27
   Identified by the **DB2DBNAME** property.

   username
   Identified by the **DB2ADMIN** property

   password
   Password for the database.

2. Drop the identity.

```
db2 "alter table KMT_DEVICE_TYPE alter column UUID drop identity"
```

3. Start the identity with number higher than the existing user-defined group with highest uuid value.

```
db2 "alter table KMT_DEVICE_TYPE alter column UUID  set GENERATED BY DEFAULT AS IDENTITY
(START WITH 10100 INCREMENT BY 1 MINVALUE 1 MAXVALUE 32767 CYCLE CACHE 20)"
```

4. Run the following command to exit the session.

```
db2 terminate
```

Linux

1. Open a command-prompt and run the following command.

```
. ~sklmdb2/sqllib/db2profile
db2 connect to sklmdb27 user username using password
```

Where,

sklmdb27
Identified by the **DB2DBNAME** property.

username
Identified by the **DB2ADMIN** property

password
Password for the database.

2. Drop the identity.

```
db2 "alter table KMT_DEVICE_TYPE alter column UUID drop identity"
```

3. Start the identity with number higher than the existing user-defined group with highest uuid value.

```
db2 "alter table KMT_DEVICE_TYPE alter column UUID  set GENERATED BY DEFAULT AS IDENTITY
(START WITH 10100 INCREMENT BY 1 MINVALUE 1 MAXVALUE 32767 CYCLE CACHE 20)"
```

4. Run the following command to exit the session.

```
db2 terminate
```

WebSphere Application Server limitations, problems, and workaround

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

User role does not provide the expected role-based access

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.

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

Mapped drives are not displayed in the drop-down lists

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.

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

Selecting the Back arrow fails to sequence through previous portlets

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.

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.

Cannot access IBM Security Key Lifecycle Manager graphical user interface

You cannot access IBM Security Key Lifecycle Manager graphical user interface if the specified port information is incorrect.

- 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.

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

Restore operation fails on AIX operating system

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.

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
```

Cannot run the backup operation on a system with large data objects

With the default setting of WebSphere Application Server transaction timeout of 600 seconds, if you run the backup operation on a system with large data objects, a Java exception occurs.

To resolve this problem, you must set the higher transaction timeout value, such as 7200 seconds (2 hours). To modify the settings, run the following steps:

1. Using the WASAdmin user ID, log in to the WebSphere Integrated Solutions Console.

   `https://localhost:9083/ibm/console/logon.jsp`
2. Go to the Transaction service page by clicking **Servers** > **Server Types** > **WebSphere application servers** > **[Application servers] server1** > **[Container Settings] Container Services** > **Transaction Service**.
3. In the **Total transaction lifetime timeout** and **Maximum transaction timeout** fields, specify a higher value, for example `7200`.
4. Click **Apply**.
5. Click **OK**.

Browser limitations, problems, and workaround

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

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.

Error results vary when you attempt to accept a pending LTO device

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.

Use either message format to recognize your need to correct the key name and try again.

Unable to close Add Device dialog

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.

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**.

Cursor might not appear when you add a self-signed certificate

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 flashes to show which field has focus.

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

Internet Explorer browser reports a certificate error

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.

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.

Cannot type value for a path in the field that appears when you click Browse

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.

Use the drop-down arrow on the Browse File dialog to select the directory path.

Unable to load IBM Security Key Lifecycle Manager console

The IBM Security Key Lifecycle Manager console is not loading on the Internet Explorer, version 9.0 browser.

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.

Error message when assigning a role to the user

In the WebSphere Integrated Solutions Console, an error message is displayed for selecting a role even after a role is assigned to the user.

This message is displayed because of using an unsupported version of Internet Explorer. To resolve this problem, in the browser, you must enable compatibility mode for the host name or domain on which IBM Security Key Lifecycle Manager is running.

1. Open Internet Explorer.
2. Click **Tools** > **Compatibility View settings**
3. Add the domain or host name listed in the window.
4. Click **Add**.
5. Refresh the page.

Replication problems and resolution

You must consider possible issues on the clone and master systems when you run the IBM Security Key Lifecycle Manager replication task.

Incomplete replication

- Ensure that the SSL certificate and private key that is specified in the **backup.TLSCertAlias** parameter are available on both the master and clone servers.
- Ensure that the port numbers specified for replication communication are not currently in use by other software products.
- Check the server names or IP addresses specified in the replication configuration file are correct and accessible from the master server.
- Check whether the replication task is up on each server by running the **tklmReplicationStatus** command, **Replication Status REST Service**, or the status on the **Replication** section of IBM Security Key Lifecycle Manager welcome page.
- For DB2 replication, ensure that date/time of master and clone servers are closely synchronized. Large discrepancies can lead to restore failure.
- Check the replication configuration file to ensure that the minimum required parameters are defined, without typographical error.
- Define a maximum of one master and 20 associated clones. At least one clone must be defined.
- Check the replication audit file to get more information about replication failure.

Replication is not taking place at scheduled time

- Scheduled replications take place only when you create **new** key material.
- When both specific replication time and a check interval are set in the master replication configuration file, the time overrides the check interval.

Clone system replication

- The clone system restarts after replication.
- Maintain the availability of your clone servers. You can specify a specific time-of-day to complete the replication with the **restore.DailyStartReplicationRestoreTime** parameter. For example, to run restores only at 11 p.m., regardless of when the backup file is received, code the following property in the configuration file:

  ```
  restore.DailyStartReplicationRestoreTime=23:00
  ```

Accessibility limitations, problems, and workarounds

You might encounter some IBM Security Key Lifecycle Manager accessibility limitations or accessibility problems.

JAWS screen reader reads Configuration page element incorrectly

On the **Configuration** > **SSL/KMIP** page, warning icon on the message box is read as **Close** button.

This problem is a known limitation of using Dojo widget for displaying the warning message. This problem occurs when you create a self-signed certificate in the **Configuration** page.

1. Log on to the graphical user interface.
2. On the Welcome page, click **Configuration** > **SSL/KMIP**.
3. Select **Create self-signed certificate**.
4. Complete the required and optional fields, and then click **OK**.

   A warning message box for taking the backup is displayed. The screen reader reads the warning icon on the message box as **Close** button.

JAWS screen reader reads warning message incorrectly

On the **Configuration** > **SSL/KMIP** page, the warning message is read as document.

This problem is a known limitation of using Dojo widget for displaying the warning message. This problem occurs when you create a self-signed certificate in the Configuration page.

1. Log on to the graphical user interface.
2. On the Welcome page, click **Configuration** > **SSL/KMIP**.
3. Select **Create self-signed certificate**.
4. Complete the required and optional fields, and then click **OK**.

   A warning message box for taking the backup is displayed. The screen reader reads this warning message as document.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

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

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

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

Index

M

N

P

R

S

T

U

V

W