Installing and configuring

IBM

Contents

Overview of the environment

IBM Security Key Lifecycle Manager delivers simplified key lifecycle management capabilities in a solution that is easy to install, deploy, and manage.

This document focuses on the tasks that you must complete to install and configure IBM Security Key Lifecycle Manager.

Features overview

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

IBM Security Key Lifecycle Manager has the following features:

- Role-based access control that provides permissions to do tasks such as create, modify, and delete for specific device groups. Most permissions are associated with specific device groups.
- Extension of support to devices by using industry-standard Key Management Interoperability Protocol (KMIP) for encryption of stored data and the corresponding cryptographic key management.
- Serving symmetric keys to DS5000 storage servers

  Provide administration and ongoing maintenance of keys that are served to DS5000 storage servers. Restrict the set of machines with which a device such as a disk drive can be associated. You can associate a device to an existing machine in the IBM Security Key Lifecycle Manager database.
- A graphical user interface, command-line interface, and REST interface to manage keys, certificates, and devices.

  Note:

  – The IBM Security Key Lifecycle Manager command-line interface commands will be deprecated in the later versions of IBM Security Key Lifecycle Manager. Use the REST interfaces instead.

  – All references to the **`alias`** property of cryptographic keys and certificates in the graphical user interface, command-line interface, and REST interface will be deprecated in the later versions of IBM Security Key Lifecycle Manager.
- Encrypted keys to one or more devices to which IBM Security Key Lifecycle Manager server is connected.
- Storage of key materials for the self-signed certificates that you generate, private key, and the key metadata in a database.
- Backup and restore to protect critical data and other IBM Security Key Lifecycle Manager data, such as the configuration files and current database information.
- Migration of IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, 2.0.1, and IBM Encryption Key Manager, version 2.1 component during installation.
- Audit records based on selected events that occur as a result of successful operations, unsuccessful operations, or both. Installing or starting IBM Security Key Lifecycle Manager writes the build level to the audit log.
- Support for encryption-enabled 3592 tape drives, LTO tape drives, DS5000 storage servers, DS8000 Turbo drives, and other devices.

- Support for using a Hardware Security Module (HSM) to store the master key that is used to protect all passwords and keys that are stored in the database.
- A set of operations to automatically replicate current active files and data across systems. This replication enables cloning of IBM Security Key Lifecycle Manager environments on multiple servers in a fully automated fashion.

Deployment

Deployment of IBM Security Key Lifecycle Manager consists of an installation process that gathers information for database preparation, user ID configuration, and optional data migration from the Encryption Key Manager.

Deployment on Windows and systems such as Linux or AIX

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

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

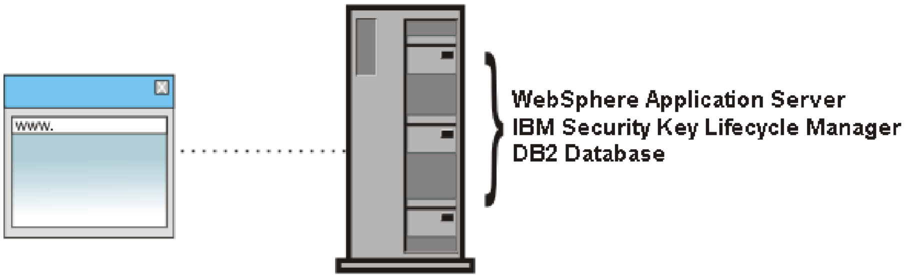
www.
WebSphere Application Server
IBM Security Key Lifecycle Manager
DB2 Database

Figure 1. Main components on Windows systems and systems such as Linux or AIX

Installation overview

The IBM Security Key Lifecycle Manager installation involves preparing the software and then running the installation program.

The major steps to install IBM Security Key Lifecycle Manager are:

1. Plan your installation and fill in the installation worksheet. See “Planning the installation” on page 7.
2. Install and configure IBM Security Key Lifecycle Manager. The installation falls into these phases:
   a. Introductory that includes the language selection and introduction panel, and the license agreement panel.
   b. DB2® and WebSphere® Application Server middleware installations that include panels for gathering information to install DB2 and WebSphere Application Server. After you enter the information, the installation program installs DB2 and the middleware. IBM Security Key Lifecycle Manager is installed during this phase.
3. Log in and verify the installation, resolving any problems. See “Login URL and initial user ID” on page 14 and “Installation verification” on page 90 for details.

Note: Installation might take more than half an hour.

Installation images and fix packs

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

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

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

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

Installation package preparation

For distributed systems, the installation package is available on a DVD, or as one or more compressed files that you download.

Installing from a DVD

To install from a DVD for distributed systems, take these steps:

1. Insert or mount the DVD, as required by the operating system.
2. Locate the installation scripts in the root directory of the DVD.

Installing from downloaded packages

The installation package files for distributed systems are archive files that contain the files that are used in the installation. Packages that are labeled "eImage <*integer*>" require assembly into a temporary installation directory on your computer. For example, a package label might be `eImage 1`. Paths to temporary installation directories cannot contain spaces or special characters.

To install from eImage images, follow these assembly steps:

1. Download the eImage package files to a convenient temporary directory.
2. Expand all the compressed files from the eImage packages into a different temporary directory.

   Windows systems:

   Extract the first eImage package into a temporary subdirectory that matches the first eImage package name. Extract subsequent packages into the subdirectory that matches the first eImage package name, not the subsequent package name.

   For example, by using temporary directory `C:\mysklmV25download`, take these steps:

   a. First, extract eImage package 1 into a subdirectory such as `C:\mysklmV25download\CZJF3ML`.
   b. Next, extract package 2 into the same subdirectory that eImage package 1 created, which in this example is `C:\mysklmV25download\CZJF3ML`.

   c. Extract subsequent packages into the eImage package 1 subdirectory, which in this example is `C:\mysklmV25download\CZJF3ML`.

Linux systems:

On Linux systems, the compressed files are expanded directly into the temporary directory without the addition of package names.

AIX

On AIX systems, the compressed files are expanded directly into the temporary directory without the addition of package names.

You must use a GNU `tar` utility to extract the eImage packages. Take these steps:

a. Download and install the GNU `tar` utility from this address:

   ftp://ftp.software.ibm.com/aix/freeSoftware/aixtoolbox/RPMS/ppc/tar/tar-1.22-1.aix6.1.ppc.rpm

b. Extract each package. For example, to extract a first eImage named `CZJD7ML.tar`, run this command:

```
/usr/bin/gtar -xvf CZJD7ML.tar
```

c. Repeat the command by specifying each of the additional eImages.

Solaris

On Solaris systems, the compressed files are expanded directly into the temporary directory without the addition of package names.

You must use a GNU `tar` utility to extract the eImage packages. Take these steps:

a. You might already have the GNU `tar` package installed. Determine whether the utility is located here: `/usr/sfw/bin/gtar`

   To obtain more information about the package, run this command:

```
 pkginfo -l SUNWgtar
```

   If you want to download and install the GNU `tar` utility, access this website:

   http://www.sunfreeware.com/

b. Extract each package. For example, to extract a first eImage named `CZJE9ML.tar`, run this command:

```
/usr/sfw/bin/gtar -xvf CZJE9ML.tar
```

c. Repeat the command by specifying each of the additional eImages.

3. Locate and run the installation files in the temporary directory into which you expanded the installation packages. For example, locate:
   - Windows systems: `launchpad.exe`
   - Other systems: `launchpad.sh`

     On some versions of the Linux operating system, you might see this 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
```

To update from fix pack images, follow the readme file instructions on the IBM Fix Central website at http://www.ibm.com/support/fixcentral. Use the following details to access the website:

- Product Group: Security Systems
- Product Name: IBM Security Key Lifecycle Manager

Planning the installation

Before you can install the necessary software, you must plan your environment and understand the requirements of IBM Security Key Lifecycle Manager.

Before you install IBM Security Key Lifecycle Manager, follow these steps:

- Use the worksheet in "Preinstallation worksheets" on page 93 to assist with your planning.
- Determine the IBM Security Key Lifecycle Manager topology, described in "Deployment" on page 2.
- Ensure that the system meets hardware requirements. For more information, see
  - "Hardware requirements for distributed systems" on page 9
- Ensure that the operating system is at the correct level, with all the required patches in place. See "Operating system requirements" on page 10 for information on required operating system versions.
- Ensure that kernel settings are correct for those operating systems, such as the Solaris operating system, that requires updating. See "DB2 kernel settings" on page 13 for details.
- If you intend to use your own previously installed version of DB2, ensure that the copy of DB2 is at the required software level. See "Software prerequisites" on page 12 for information on supported versions of DB2.
- Determine whether you want to migrate the configuration from an earlier version of Encryption Key Manager. For more migration information, see "Migration planning" on page 23.

  Note: The only opportunity to migrate an Encryption Key Manager configuration to IBM Security Key Lifecycle Manager is during installation.
- Decide what installation mode you want to use to install IBM Security Key Lifecycle Manager: graphical mode or silent mode. See "Types of installation" on page 43 for a description of the installation modes.

Definitions for *HOME* and other directory variables

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

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

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

- For Windows systems, the default path is:
  - DB2

    `*drive*:\Program Files (x86)\IBM`
  - All applications other than DB2

    `*drive*:\`
- For Linux, Solaris, and AIX systems, `/opt` is the default path.

Table 1. HOME and other directory variables

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

Hardware and software requirements

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

The hardware and software requirements that are published are accurate at the time of publication.

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

1. Enter `IBM Security Key Lifecycle Manager`.
2. Select the product version. For example, `2.5`.
3. Select the operating system.
4. Click **Submit**.

Hardware requirements for distributed systems

You must ensure that the computer has the required memory, processor speed, and available disk space to meet the workload.

Table 2. Hardware requirements

System components	Minimum values*	Suggested values**
System memory (RAM)	4 GB	8 GB
Processor speed	**Linux and Windows systems** 3.0 GHz single processor **AIX and Sun Solaris systems** 1.5 GHz (2-way)	**Linux and Windows systems** 3.0 GHz dual processors **AIX and Sun Solaris systems** 1.5 GHz (4-way)
Disk space free for IBM Security Key Lifecycle Manager and prerequisite products such as DB2	5 GB	20 GB
Disk space free in `/tmp` or `C:\temp`	2 GB	2 GB
Disk space free in `/home` directory for DB2	5 GB	20 GB
Disk space free in `/var` directory for DB2	512 MB on Linux and UNIX operating systems	512 MB on Linux and UNIX operating systems

Table 2. Hardware requirements (continued)

System components	Minimum values*	Suggested values**
All file systems must be writable. * Minimum values: These values enable a basic use of IBM Security Key Lifecycle Manager. ** Recommended values: You must use larger values that are appropriate for your production environment. The most critical requirements are to provide adequate system memory, and free disk and swap space. Processor speed is less important. On Linux and UNIX operating systems, you must install your DB2 product in an empty directory. If the directory that you specify as the installation path contains subdirectories or files, your DB2 installation might fail. On Linux and UNIX operating systems, 4 GB of free space is required in the `$HOME` directory. On Windows operating systems, the following free space is required in addition to that of your DB2 product: • 40 MB in the system drive • 60 MB in the `/temp` folder that is specified by the *temp* environment variable Installing into mapped network drives/mounted partitions is not supported. If installation locations of more than one system component fall on the same Windows drive/UNIX partition, the cumulative space to contain all those components must be available in that drive/partition.		

Operating system requirements

For each operating system that IBM Security Key Lifecycle Manager server runs on, there is a minimum version level required.

The “Operating system requirements” table identifies the operating systems requirements for installation:

Table 3. Operating system requirements

Operating system	Use DB2 Workgroup Server Edition Version 10.1 with
AIX version 6.1 and version 7.1 in 32-bit mode. POWER7 processor-based servers are supported. • A 64-bit AIX kernel is required. • Use AIX 6.1 Technology Level 2. The minimum C++ runtime level requires the xlC.rte 9.0.0.8 and xlC.aix61.rte 9.0.0.8 (or later) files. These files are included in the June 2008 IBM C++ Runtime Environment Components for AIX package.	✓
Sun Server Solaris 10 (SPARC 64–bit in 32-bit mode) If raw devices are used, apply patch 125100-07. **Note:** IBM Security Key Lifecycle Manager runs in a 32–bit JVM.	✓
Windows Server 2008 **R2** (64-bit in 32-bit mode for all Intel and AMD processors), which includes these editions: • Standard Edition • Enterprise Edition	✓
Windows Server 2012 (64-bit in 32-bit mode for all Intel and AMD processors) for: • Standard Edition	✓

Table 3. Operating system requirements (continued)

Operating system	Use DB2 Workgroup Server Edition Version 10.1 with
Windows Server 2012 **R2** (64-bit in 32-bit mode for all Intel and AMD processors) for: • Standard Edition	✓
Red Hat Enterprise Linux Version 5.0 Update 6.0 and Version 6.0 Update 3 on x86 64-bit in 32-bit mode	✓
Red Hat Enterprise Linux Version 5.0 Update 6.0 and Version 6.0 Update 3 (System z) on x86 64–bit mode	✓
SuSE Linux Enterprise Server Version 10 on x86 64–bit mode and Version 11 on x86 64–bit mode	✓
SuSE Linux Enterprise Server Version 11 (System z) on x86 64–bit mode	✓

Before you install IBM Security Key Lifecycle Manager on Red Hat Enterprise Linux operating system, ensure that the required libraries described in this technote are installed: https://www-304.ibm.com/support/docview.wss?uid=swg21459143

Before you install IBM Security Key Lifecycle Manager on AIX operating system, ensure that the required libraries described in this technote are installed: http://www-01.ibm.com/support/docview.wss?uid=swg21631478

Linux packages

On Linux operating systems, IBM Security Key Lifecycle Manager requires the `compat-libstdc++` package, which contains `libstdc++.so.6`. It also requires the `libaio` package, which contains the asynchronous library that is required for DB2 database servers.

- `libstdc` package

  To determine whether you have the package, run this command:

  ```
  rpm -qa  | grep -i "libstdc"
  ```

  If the package is not installed, locate the `rpm` file on your original installation media and install it.

  ```
  find installation_media -name compat-libstdc++*
  rpm -ivh full_path_to_compat-libstdc++_rpm_file
  ```

- `libaio` package

  To determine whether you have the package, run this command:

  ```
  rpm -qa  | grep -i "libaio"
  ```

  If the package is not installed, locate the `rpm` file on your original installation media and install it.

  ```
  find installation_media -name libaio*
  rpm -ivh full_path_to_libaio_rpm_file
  ```

On Red Hat Enterprise Linux 64-bit systems, DB2 installation requires that two separate `libaio` packages must be installed before running **`db2setup`**. These packages are both named `libaio`. However, there are two different RPM files to install: one of which is an i386 RPM file, and the other is an x86_64 RPM file.

Disabling Security Enhanced Linux

IBM Security Key Lifecycle Manager problems occur on Linux operating systems if the Security Enhanced Linux (SELINUX) setting is enabled.

About this task

For example, a problem might occur with TCP/IP connections on IBM Security Key Lifecycle Manager server ports. To disable Security Enhanced Linux, do these steps after you install the Linux operating system:

Procedure

1. Edit the `/etc/selinux/config` file and set `SELINUX=disabled`.
2. Restart the system.
3. Run **`sestatus`** from the command line to ensure that SELinux is disabled.

   ```
   [root@localhost ~]$ sestatus
   SELinux status: disabled
   ```
4. Install IBM Security Key Lifecycle Manager.

Software prerequisites

IBM Security Key Lifecycle Manager uses several support and middleware programs.

- "Java Runtime Environment (JRE) requirements"
- "Runtime environment requirements" on page 13
- "Database authority and requirements"
- A supported browser, which is not included with the product installation

On distributed systems, IBM Security Key Lifecycle Manager installs the middleware that it uses. If you have DB2 already installed on the system, see the details in "Database authority and requirements."

Ensure that Bash Shell is installed before you install IBM Security Key Lifecycle Manager on UNIX operating systems.

Java Runtime Environment (JRE) requirements

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

On distributed systems:
IBM Java Runtime Environment that is included with WebSphere Application Server.

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

Database authority and requirements

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

- Distributed systems:

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

  - Version 10.1 and the future fix packs on other distributed operating systems that IBM Security Key Lifecycle Manager supports.

Note:

- You must use IBM Security Key Lifecycle Manager to manage the database. To avoid data synchronization problems, do not use tools that the database application might provide.
- For improved performance of DB2 Version 10.1 on AIX systems, ensure that you install and configure the I/O completion ports (IOCP) package that is described in the DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.admin.perf.doc/doc/t0054518.html).
- If an existing copy of DB2 Workgroup Server Edition was installed as the root user at the correct version for the operating system, you can use the existing DB2 Workgroup Server Edition. IBM Security Key Lifecycle Manager installer does not detect the presence of DB2. You must specify the DB2 installation path.

For more information about DB2 prerequisites, see DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.admin.cmd.doc/doc/r0059710.html).

DB2 kernel settings:

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

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

AIX systems
None required.

Linux systems
For more information about modifying kernel parameters for DB2 Workgroup Server Edition, version 10.1 on other supported Linux systems, see DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html).

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

Window systems
None required.

Runtime environment requirements

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

On distributed systems:
WebSphere Application Server 8.5.5 and any applicable fix pack or APAR requirements.

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

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

Browser requirements

You must enable the session cookies and JavaScript in the browser to establish a session with IBM Security Key Lifecycle Manager.

Supported browsers are not included with the product installation. You must deploy a browser on the same computer on which IBM Security Key Lifecycle Manager runs.

Table 4. Supported browsers

Browser	**Fix pack**	**AIX**	**Sun Server Solaris SPARC**	**Windows Server 2008 R2**	**Windows Server 2012**	**Red Hat Enterprise Linux**	**SuSE Linux Enterprise Server**
Microsoft Internet Explorer, Version 9.0	None			✓	✓		
Microsoft Internet Explorer, Version 10.0	None			✓	✓		
Firefox ESR, version 17.0	None	✓	✓	✓	✓	✓	✓

Key size requirements

You must consider the requirements for key sizes before you install and configure IBM Security Key Lifecycle Manager.

Supported key sizes and import and export restrictions

IBM Security Key Lifecycle Manager can serve either 2048 or 1024-bit keys to devices. Older keys that were generated as 1024-bit keys can continue to be used.

Table 5 lists the supported key sizes that IBM Security Key Lifecycle Manager supports.

Table 5. Supported key sizes

Import PKCS#12 file	**Export PKCS#12 file**	**Key Generation Size in Bits**
Yes	Yes	2048

Login URL and initial user ID

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

Access requirements

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

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

Login URL

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

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

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

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

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

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

Do not use a port value greater than 65520.

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

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

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

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

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

Administrator user IDs and passwords

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

Table 6. Administrator user IDs and passwords

Program	User ID	Password
Distributed systems For distributed operating systems, installation must be run by a local administrative ID, which is root for AIX or Linux systems or a member of the Administrators group on Windows systems. Do not use a domain user ID to install IBM Security Key Lifecycle Manager. You might have one or more of these user IDs:		

Table 6. Administrator user IDs and passwords (continued)

Program	**User ID**	**Password**
IBM Security Key Lifecycle Manager administrator	**SKLMAdmin** As the primary administrator with full access to all operations, this user ID has the `klmSecurityOfficer` super user role, in the group that is named `klmSecurityOfficerGroup`. This user ID is not case-sensitive. Alternatively, use **sklmadmin**. Use the SKLMAdmin user ID to administer IBM Security Key Lifecycle Manager. With the SKLMAdmin user ID, you can: • View and use the IBM Security Key Lifecycle Manager interface. • Change the password for the IBM Security Key Lifecycle Manager administrator. However, you cannot: • Create one or more extra IBM Security Key Lifecycle Manager administrator user IDs. • Do WebSphere Application Server administrator tasks such as creating or assigning a role. • Start or stop the server.	Specify and securely store a password during installation.

Table 6. Administrator user IDs and passwords (continued)

Program	**User ID**	**Password**
WebSphere Application Server administrator	**WASAdmin** This user ID is not case-sensitive. Alternatively, use **wasadmin** or a user ID that you specify during installation. Do not use the: • SKLMAdmin user ID to administer WebSphere Application Server. • WASAdmin user ID to administer IBM Security Key Lifecycle Manager. The WASAdmin user ID has no roles to use IBM Security Key Lifecycle Manager. This administrator user ID is the WebSphere Application Server administrator user ID. With the wasadmin user ID, you can: • View and use only the WebSphere Application Server interface. • Create one or more extra IBM Security Key Lifecycle Manager administrator user IDs, groups, and roles. • Reset the password of any IBM Security Key Lifecycle Manager user ID, including the SKLMAdmin administrator. • Start and stop the server. However, you cannot: • Use the IBM Security Key Lifecycle Manager to complete tasks. For example, you cannot create IBM Security Key Lifecycle Manager device groups. • Do other tasks that require access to IBM Security Key Lifecycle Manager data. The wasadmin user ID does *not* have access to IBM Security Key Lifecycle Manager data as a superuser.	Specify and securely store a password during installation. Protect the WASAdmin user ID in the same way that you protect the use of the SKLMAdmin user ID. The WASAdmin user ID has authority to reset the SKLMAdmin password and to create and assign permissions to new IBM Security Key Lifecycle Manager users.
The IBM Security Key Lifecycle Manager DB2 database		

Table 6. Administrator user IDs and passwords (continued)

Program	User ID	Password
Instance owner of the database	**Windows systems and systems such as AIX or Linux:** The default value is `sklmdb2`. You might specify a different value during installation. The ID is the installation default user ID for the instance owner of the database. Do not specify a user ID greater than eight characters in length. The instance name is also `sklmdb2`. If DB2 is on a system such as AIX or Linux, your user ID must be in the bin or root group, or in a separate group in which root is a member. If you use an existing user ID as instance owner of the IBM Security Key Lifecycle Manager database, the user ID cannot own another database instance. **Note:** Do not use a hyphen (-) or underscore character (_) when you specify a user ID for an existing copy of DB2.	Specify and securely store a password during installation. This password is an operating system password. If you change the password on the operating system, you must change this password. For more information, see "Resetting password on distributed systems" on page 59..
Database instance	The administrator ID `sklmdb2` owns a DB2 instance named `sklmdb2`.	

Audit files

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

Distributed systems

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

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

User roles

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

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

The WASAdmin user ID has the authority to create and assign these roles, and to change the password of any IBM Security Key Lifecycle Manager administrator. To set administration limits for IBM Security Key Lifecycle Manager, use the

WASAdmin user ID on the WebSphere Integrated Solutions Console to create roles, users, and groups. Assign roles and users to a group. For example, you might create a group and assign both users and a role that limits user activities to administer only LTO tape drives. You must assign a role to a new user before that user attempts to log in to IBM Security Key Lifecycle Manager.

Before you begin, complete the following tasks:

- Determine the limits on device administration that your organization requires.

  For example, you might determine that a specific device group has its own administration.
- Estimate how many administrative users might be needed over an interval of time. For ease of use, consider specifying a group and a role to specify their tasks.

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

Available permissions

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

A *permission* from IBM Security Key Lifecycle Manager enables an action or the use of a device group. A *role* in IBM Security Key Lifecycle Manager is one or more permissions. However, in the WebSphere Application Server graphical user interface, the term *role* includes both IBM Security Key Lifecycle Manager permissions and roles.

Note: Installation creates these default groups:

klmSecurityOfficerGroup

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

The `klmSecurityOfficer` role has:

- Root access to the entire set of permissions and device groups that are described in Table 7 on page 20 and Table 8 on page 21.
- Permission to any role or device group that might be created.
- The `suppressmonitor` role.

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

klmBackupRestoreGroup

Back up and restore IBM Security Key Lifecycle Manager.

LTOAdmin

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

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

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

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

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

A user who has any one of the permissions in Table 7 can view:

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

Table 7. Permissions for actions

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

Table 7. Permissions for actions (continued)

Permission	Enables these actions	Unrelated to device groups	Associated with device groups
klmRestore	Restore a previous backup copy of IBM Security Key Lifecycle Manager data.	✓	

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

Table 8. Device groups

Permission	Allows actions on these objects
LTO	LTO device family
TS3592	3592 device family
DS5000	DS5000 device family
DS8000	DS8000 device family
BRCD_ENCRYPTOR	BRCD_ENCRYPTOR device group
ONESECURE	ONESECURE device group
ETERNUS_DX	ETERNUS_DX device group
XIV	XIV device group
GENERIC	Objects in the GENERIC device family.
userdevicegroup	A user-defined instance such as myLTO that you manually create, based on a predefined device family such as LTO.

IBM Security Key Lifecycle Manager integration with LDAP

You can integrate IBM Security Key Lifecycle Manager with LDAP user repositories. You must configure LDAP repositories to access IBM Security Key Lifecycle Manager server, server APIs, and CLIs.

You can configure IBM Security Key Lifecycle Manager users in any of the LDAP repositories, such as IBM Security Directory Server or Microsoft Active Directory to access IBM Security Key Lifecycle Manager server and call server APIs and CLIs. You must add and configure LDAP user repository to the federated repository of WebSphere Application Server. IBM Security Key Lifecycle Manager uses application groups to enforce the role-based authorization for IBM Security Key Lifecycle Manager functions. For an IBM Security Key Lifecycle Manager user to run IBM Security Key Lifecycle Manager functions in an LDAP user repository, the user must be member of a specific IBM Security Key Lifecycle Manager application groups.

When you install IBM Security Key Lifecycle Manager, the application groups and users are created in a default file based repository in the WebSphere Application Server federated repository. When an LDAP user repository is added to the WebSphere Application Server federated repository, you must make LDAP user as a member of IBM Security Key Lifecycle Manager application groups. You cannot make LDAP users as member of the groups in the default file based repository.

Cross repository group membership is not possible between a file-based repository and an LDAP repository. However, cross repository group membership is possible across an LDAP repository and a database-based repository. So, create a database-based repository and create all the IBM Security Key Lifecycle Manager application groups in this repository. The application groups that existed in file based repository are removed.

Once the database-based repository is created and the IBM Security Key Lifecycle Manager application groups are added to this repository, the user in an LDAP repository can be made members of IBM Security Key Lifecycle Manager application groups in the database-based repository. Then, the user can log on to IBM Security Key Lifecycle Manager application and run IBM Security Key Lifecycle Manager application functions.

For information about LDAP configuration tasks, see the Administering section.

Migration planning

Before you install IBM Security Key Lifecycle Manager at this version, determine whether you migrate a previous version of IBM Security Key Lifecycle Manager, or previous configuration data from IBM Encryption Key Manager component for the Java platform.

Note: The Encryption Key Manager component supports only the English locale. Therefore, you must do the migration from Encryption Key Manager to IBM Security Key Lifecycle Manager in the English locale.

- IBM Security Key Lifecycle Manager, version 2.0.1 or later fix packs.

  Installing IBM Security Key Lifecycle Manager, version 2.5 detects an earlier version of IBM Security Key Lifecycle Manager. The installation automatically migrates its data.

  A failed migration of IBM Security Key Lifecycle Manager, version 2.0.1 retains a record of successful migration steps. Running the migration recovery script starts at the point in the migration process where the error occurred.
- IBM Security Key Lifecycle Manager, version 2 at fix pack 4 or later.

  Installing IBM Security Key Lifecycle Manager, version 2.5 detects an earlier version of IBM Security Key Lifecycle Manager. The installation automatically migrates its data.

  A failed migration of IBM Security Key Lifecycle Manager, version 2.0 retains a record of successful migration steps. Running the migration recovery script starts at the point in the migration process where the error occurred.
- IBM Security Key Lifecycle Manager, version 1 at fix pack 3 or later.

  Installing IBM Security Key Lifecycle Manager, version 2.5 detects an earlier version of IBM Security Key Lifecycle Manager. The installation automatically migrates its data.

  A failed migration of IBM Security Key Lifecycle Manager, version 1 retains a record of successful migration steps. Running the migration recovery script starts at the point in the migration process where the error occurred.
- Encryption Key Manager, version 2.1

  Migration is enabled for version 2.1, but not for earlier versions of Encryption Key Manager. The only opportunity to migrate the configuration is during the installation of IBM Security Key Lifecycle Manager, or immediately afterward, before you change the IBM Security Key Lifecycle Manager configuration.

  If Encryption Key Manager, version 2.1 migration fails, no data is migrated to the IBM Security Key Lifecycle Manager database. Any changes that are made are reversed.

If migration fails from the installer, you can manually run the IBM Security Key Lifecycle Manager, version 2.5 migration utility from the `*SKLM_HOME*\migration\bin` directory after you exit the installation.

- Run **`migrate.bat`** or **`migrate.sh`** to migrate Encryption Key Manager, version 2.1 to IBM Security Key Lifecycle Manager. On systems such as Linux or AIX, ensure that you are logged in as the root user before you run **`migrate.sh`**.
- Run **`migrateToSKLM.bat`** or **`migrateToSKLM.sh`** in the *SKLM_HOME*`\migration` directory to migrate IBM Security Key Lifecycle Manager earlier version to

version 2.5. On systems such as Linux or AIX, ensure that you are logged in as the root user before you run **migrateToSKLM.sh**.

Do not run other ***.bat** utilities that you might see in this directory. The utilities are for use only by the automatic installation process.

Before migration

Before you begin, ensure that your enterprise allows a time interval for a temporary halt to key serving activity.

A window of time for testing is also required to ensure that the new IBM Security Key Lifecycle Manager has the expected keys and other configuration attributes that you intended to migrate.

Complete these preliminary tasks:

Disk space requirements

Before you migrate IBM Security Key Lifecycle Manager earlier versions to IBM Security Key Lifecycle Manager, version 2.5, verify that there is sufficient disk space on your system.

These disk space requirements are in addition to disk space requirements identified by the installer for installing IBM Security Key Lifecycle Manager, version 2.5 and its prerequisite software; WebSphere Application Server and DB2, version 10.1.

The additional disk space is required because the migration program runs the following tasks:

- Moves users from the earlier version to version 2.5.
- Moves data from the older version database to the new IBM Security Key Lifecycle Manager database.
- Moves all keys from the keystore into the IBM Security Key Lifecycle Manager database.

If you determine that disk space is not available, increase the disk space on the partitions or the drive letters. You must identify the disk space requirements, which include identifying the number of keys and served data.

Identify disk space requirements

To identify disk space requirements, take these steps:

Windows systems

1. Identify the following properties in your IBM Security Key Lifecycle Manager, version 1.0, 2.0, or 2.0.1 installation by typing the contents of the file `%SYSTEMDRIVE%\tklmtemp\db2srcit.txt`. For example:

   ```
   DB2ADMIN=tklmdb2
   DB2DBNAME=tklmdb
   DB2ADMINID=tklmdb2
   DB2PORTSTART=50010
   DB2INSTALLDIR=C:\IBM\tklmV2db2\
   INSTANCEHOME=C:
   ```

2. Identify the drive letter where the IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, or 2.0.1 installation database is located. That is,

the value of the INSTANCEHOME property. Using Windows Explorer, identify the size of the folder that is named TKLMDB2.

Note: Calculate that the additional space required for migration in the drive with the database is three times the size of the TKLMDB2 folder.

3. Identify the number of keys and device audit data by using the steps in "Identify the number of keys and served data." The migration of keys and served data generates the log in the <*IM App Data Dir*>/logs/sklmLogs folder.

   Note: Calculate that the additional space required on the Windows drive on which IBM Security Key Lifecycle Manager, version 2.5 is installed is the sum of the following two operations:

   - Number of keys that are multiplied by 5 KB
   - Number of served data that is multiplied by 1 KB

   In a typical installation, the migration of other entities such as devices and groups does not result in extra disk space requirements.

Systems such as Linux or AIX

1. Identify the following properties in your IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, or 2.0.1 installation by typing the contents of the file /tklmtemp/db2unix.srcit.

   A typical file might contain these entries:

   ```
   export DB2ADMIN=tklmdb2
   export DB2DBNAME=tklmdb
   export INSTANCEHOME=/home/tklmdb2
   ```

2. Identify the home directory of the database owner by examining the value of the **INSTANCEHOME** property. Type this command to determine the disk space in the home directory:

   ```
   du –k /home/sklmdb2/sklmdb2
   ```

   Note:
   Calculate that the additional space required for migration in the disk partition with the database is three times the size of the /home/sklmdb2/sklmdb2 folder.

3. Identify the number of keys and device audit data by using the steps in "Identify the number of keys and served data." The migration of keys and served data generates the log in the <*IM App Data Dir*>/logs/sklmLogs folder.

   Note: Calculate that the additional space required in the disk partition on the computer on which IBM Security Key Lifecycle Manager, version 2.5 is installed is the sum of the following two operations:

   - Number of keys that are multiplied by 5 KB
   - Number of served data that is multiplied by 1 KB

   In a typical installation, the migration of other entities such as devices and groups does not result in extra disk space requirements.

Identify the number of keys and served data

To identify the number of keys and served data, take these steps:

Windows systems

1. Type:

```
d2cmd
set DB2INSTANCE=sklmdb2
db2 connect to tklmdb user sklmdb2 using password
```

where:

tklmdb Identified by the **DB2DBNAME** property.

sklmdb2
Identified by the **DB2ADMIN** property

password
Password for the database.

2. Identify the number of keys to be migrated. Type:

```
db2 "SELECT COUNT(UUID) FROM KMT_KEY"
```

3. Identify the number of served data to be migrated. Type:

```
db2 "SELECT COUNT(*) FROM KMT_DEVAUDIT"
```

4. Exit the session. Type:

```
db2 terminate
```

Systems such as Linux or AIX

1. Type:

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

where:

tklmdb Identified by the **DB2DBNAME** property.

sklmdb2
Identified by the **DB2ADMIN** property

password
Password for the database.

2. Identify the number of keys to be migrated. Type:

```
db2 "SELECT COUNT(UUID) FROM KMT_KEY"
```

3. Identify the number of served data to be migrated. Type:

```
db2 "SELECT COUNT(*) FROM KMT_DEVAUDIT"
```

4. Exit the session. Type:

```
db2 terminate
```

Example calculation

Assume that IBM Security Key Lifecycle Manager, version 2.5 is installed in the default location /opt/IBM/WebSphere/AppServer and that the disk partition is /opt. The home directory of the database instance owner is /home/sklmdb2 and the disk partition is /home.

You identify these values:

- Keys in the database = 84000
- Served data list = 100000
- Typing the command du -k /home/sklmdb2/sklmdb2 returns a value of 173712.

You calculate the required additional disk space:

- In the /opt partition

```
(84000 * 5) + (100000 * 1) = 520000 KB
```

- In the /home partition

  ```
  (3 * 173712) = 521136 KB
  ```

Data quantity

Determine whether a large quantity of data requires migration. Migrating an existing database can require up to four times the current disk space usage during the migration activity.

Most of this disk space is released after migration succeeds. You might also change the memory settings that are described in “Hardware requirements for distributed systems” on page 9.

Encryption Key Manager configuration

Before migration, the Encryption Key Manager configuration must be correctly configured and must be a working configuration.

Take these steps:

- Refresh and stop the Encryption Key Manager server to ensure that there is no data loss.
- Back up the server that has the configuration data that you intend to migrate. Migrated data includes the following files:
  - A configuration properties file
  - Keys and certificates that are referenced by the configuration properties file
  - Drive tables
  - An optional metadata file pointed at by the configuration properties file
  - An optional key groups file
- Stop Encryption Key Manager. Key serving cannot be active during migration.

IBM Security Key Lifecycle Manager, version 2.5 requirements

Before migration, ensure that IBM Security Key Lifecycle Manager, version 2.5 has the prerequisites.

Before you migrate, take these steps:

- Ensure that you applied the most current fix pack for IBM Security Key Lifecycle Manager for the version that you are migrating.
- Back up IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, or 2.0.1. Also, back up any replica. If migration fails, you might restore IBM Security Key Lifecycle Manager earlier version from a backup copy.

  Note: After you successfully migrate IBM Security Key Lifecycle Manager to version 2.5, earlier version backup files cannot be used to restore IBM Security Key Lifecycle Manager at version 2.5.
- Verify that you have a functioning IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, or 2.0.1 system with a configured keystore. Migration fails if a keystore is not configured.
- Migration does not remove the previous version backup directory when the version 2.5 installation process removes the IBM Security Key Lifecycle Manager previous version.

However, if the IBM Security Key Lifecycle Manager earlier version backup directory is a subfolder in the Tivoli Integrated Portal Server directory path, uninstalling Tivoli Integrated Portal also removes the IBM Security Key Lifecycle Manager backup directory.

- Migration does not remove the previous version of IBM Security Key Lifecycle Manager. To remove, follow the uninstall instructions for the version of IBM Security Key Lifecycle Manager you have migrated from.

  Note: Because the IP ports are shared between the two versions, do not run both versions at the same time.
- Stop IBM Security Key Lifecycle Manager and any replica server. Key serving cannot be active during migration.
- You cannot use passwords with special characters for the IBM Security Key Lifecycle Manager database. You can use only alphabetical characters (A-Z and a-z), numeric characters (0-9), the underscore (_), and hyphen (-). If you previously modified a password, change the password before migration to use only the character set that migration allows. After migration, you can reset the password to use special characters.
- During migration, examine the `<IM App Data Dir>/logs/sklmLogs/migration.log` file frequently to determine how far migration is progressed. If migration fails, run the migration utility to print messages to the `migration.log` file and to the command-line interface.
- To avoid errors while migration is in progress, do not start or stop the DB2 server or the Tivoli Integrated Portal Server outside of the migration process. Do not interrupt the migration process.
- The Tivoli Integrated Portal Server, Tivoli Key Lifecycle Manager server, and the Tivoli Key Lifecycle Manager DB2 database server must be running during the migration process for both silent and graphical mode of installations.

Migration requirements for Encryption Key Manager

There are certain requirements before you can migrate from Encryption Key Manager to IBM Security Key Lifecycle Manager. You can migrate only version 2.1 of Encryption Key Manager.

- Migrate only one Encryption Key Manager server to one IBM Security Key Lifecycle Manager server. To migrate a second Encryption Key Manager, use a second IBM Security Key Lifecycle Manager server.
- Both the Encryption Key Manager server and the IBM Security Key Lifecycle Manager server that receives migrated data must be on the same host. After migration, IBM Security Key Lifecycle Manager server uses the keystore, TCP port, and SSL port that Encryption Key Manager server previously used.
- Two properties are required for migration:
  - **`config.keystore.file`**
  - **`TransportListener.ssl.keystore.name`**
- To migrate key groups, if your Encryption Key Manager was configured with key groups to work with LTO tape drives, ensure that the **`config.keygroup.xml.file`** property exists in the Encryption Key Manager properties file and is specified as an absolute path.

  This property might not be in the properties file because Encryption Key Manager might use the file from a default directory from which the Encryption Key Manager was started.

Migration for Encryption Key Manager from IBM i systems

You might require to relocate Encryption Key Manager from a system such as IBM i to a different operating system before you can migrate Encryption Key Manager to IBM Security Key Lifecycle Manager.

Take these steps:

1. On an IBM i system, the keys must be in a JCEKS keystore. Otherwise, you must first move the keys to a JCEKS keystore.
2. Move the JCEKS keystore and Encryption Key Manager properties file, which you must update for the new operating system, from the IBM i system to a system that IBM Security Key Lifecycle Manager, Version 2.5 supports.
3. Use the keystore and modified properties file that you moved to set up Encryption Key Manager on the system that IBM Security Key Lifecycle Manager, Version 2.5 supports.
4. Ensure that Encryption Key Manager is functional on the new system.
5. Migrate from the new Encryption Key Manager to IBM Security Key Lifecycle Manager, Version 2.5 as part of installing IBM Security Key Lifecycle Manager, Version 2.5. You can migrate only Version 2.1 of Encryption Key Manager.

Note: Use this website to obtain Encryption Key Manager for an IBM operating system: Encryption Key Manager component

Migration from unsupported Linux operating systems

Use the Migration Backup Tool utility to migrate IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 that is running on the operating systems Red Hat Enterprise Linux Version 4.0 and SuSE Linux Enterprise Server Version 9.0, which version 2.5 does not support.

Migration process

You must run the following steps to migrate to IBM Security Key Lifecycle Manager, version 2.5:

1. Ensure that the earlier version 2.0 or 2.0.1 is installed and running on an unsupported operating system.
2. Run Migration Backup Tool. See “Running Migration Backup Tool” on page 30.

   This step creates a migration backup JAR file.
3. Install IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 on a supported operating system Red Hat Enterprise Linux, version 5.0 or SuSE Linux Enterprise Server, version 10. You must have the setup that is similar to that on the unsupported operating system about users, passwords, and install location.
4. Copy the migration backup JAR file to the system on the supported operating system.
5. Carry out the restore operation of the migration backup JAR file by using the graphical user interface or command-line interface. See “Restoring the migration backup file” on page 31.
6. The installation of IBM Security Key Lifecycle Manager, version 2.5 detects earlier versions 2.0 or 2.0.1, which is preinstalled in this system and runs the migration process.

Migration Backup Tool location

You can locate Migration Backup Tool in the /disk1/UnsupportedPlatformMig folder when you extract the IBM Security Key Lifecycle Manager installer image **sklm_v25_linux_64.tar.gz**. Copy the **UnsupportedPlatMig_1.0.0.jar** and **dbmigbackup.sh** files to the system on unsupported operating system. Copy the **dbtklmrestore.sh** file to the system on supported operating system.

Return codes from Migration Backup Tool

Migration Backup Tool returns one of the following return codes:

Return code	Description
0	success
1	The backup file specified is null, a directory or does not exist.
2	Unable to create temp directory.
3	IO error extracting file from backup jar. The password may be incorrect.
4	Error reading the manifest in the backup file. File may not be a backup file.
5	TIP properties could not be read.
6	Error running the migration database backup script. Check the dbmigbackup.log file for the issue.
80	Error deleting the temp directory.
99	Usage was not correct. The parameters are (backup file name and path) (password for backup) and optional (WAS_HOME, that is, directory where TKLM is installed).
100	Unexpected exception occurred.

Migration Backup Tool creates a migration backup JAR file in the same location where the original backup JAR file is present when the return code 0 is returned, for example:

```
tklm_v2.0.1.0_20130318223754+0530_backup_mig.jar.
```

If the return code is other than 0, contact the services team for support. You must send the following log files to the support team:

debug Generated in the /UnsupportedPlatformMig/logs directory.

dbmigbackup
Generated in the /UnsupportedPlatformMig directory.

Running Migration Backup Tool

You must run the Migration Backup Tool in the system where IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 is installed on an unsupported operating system. A migration backup JAR file is generated when you run this tool.

About this task

You must specify the values for the following parameters:

- Backup file name and path
- Password for backup file

- `WAS_HOME`, the directory where earlier version of IBM Security Key Lifecycle Manager is installed (optional parameter).

Procedure

1. Download the IBM Security Key Lifecycle Manager Linux installer image and extract it.
2. Copy the **`UnsupportedPlatMig_1.0.0.jar`** and **`dbmigbackup.sh`** files to the system where IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 is installed on an unsupported operating system.
3. Set the `JAVA_HOME` and `CLASSPATH` environment variables and run the tool.

   ```
   export JAVA_HOME=/opt/ibm/java2-i386-50
   export PATH=$JAVA_HOME/bin:$PATH
   export CLASSPATH=/UnsupportedPlatformMig/UnsupportedPlatMig_1.0.0.jar:
   $CLASSPATH
   ```

Example

```
[root@sourceRHL4U8 /]# cd /UnsupportedPlatformMig/
[root@sourceRHL4U8 UnsupportedPlatformMig]#
java com.ibm.tklm.migration.unsupportedplatmig.MigrationBackup
/Backup/tklm_v2.0.1.0_20130318223754+0530_backup.jar passw0rd
/opt/IBM/tivoli/tiptklmV2/
0
```

What to do next

Run the restore operation. See "Restoring the migration backup file."

Restoring the migration backup file

You must restore the migration backup JAR file on the system where IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 is installed on a supported operating system.

Before you begin

Ensure that the migration backup JAR file is created when you run Migration Backup Tool on the system where IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 is installed on an unsupported operating system.

Procedure

1. Download the IBM Security Key Lifecycle Manager Linux installer image and extract it.
2. Rename **`db2tklmrestore.sh`** to **`db2tklmrestore.sh.bkup`**

   You can locate the **`db2tklmrestore.sh`** file at: `/disk1/UnsupportedPlatformMig`
3. Copy **`db2tklmrestore.sh.bkup`** to the `<tip_home>/products/tklm/bin/db` directory.
4. Copy the migration backup JAR file to the system where IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 is installed on a supported operating system.
5. Run the restore operation by using the graphical user interface or command-line interface.

   Note:

   - If you are using version 1.0 on unsupported operating systems (Red Hat Enterprise Linux Version 4.0, SuSE Linux Enterprise Server Version 9.0, AIX

5.3, Solaris 9, and Windows 2003), you must first migrate to IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1.

- If version 2.0 or 2.0.1 is installed on the supported operating systems, the IBM Security Key Lifecycle Manager installer detects it and runs the migration task.

Migration from unsupported Windows, AIX, and Solaris operating systems

Use backup and restore operations to migrate IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 that is running on operating systems that version 2.5 does not. The unsupported operating systems are Windows 2003 R2, Windows 2008, AIX 5.3, and Sun Server Solaris, version 9.0.

Note: Use the backup and restore operations to migrate IBM Security Key Lifecycle Manager versions only across the same operating systems.

For more information about backup and restore operations, see the “Backup and restore” topic in the Administering section of IBM Security Key Lifecycle Manager documentation.

Migration process

You must run the following steps to migrate to IBM Security Key Lifecycle Manager, version 2.5:

1. Ensure that IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 is installed and running on an unsupported operating system.
2. Run the backup operation on the unsupported operating system to generate the backup files of the earlier version by using the graphical user interface or command-line interface.
3. Install IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1 on a supported operating system, Windows Server 2008 R2, or Sun Server Solaris, version 10. You must have the setup that is similar to that on the unsupported operating system about users, passwords, and install location.

   Note: Operating system on the target system (where the operating system version is supported) must be the same operating system (unsupported version of the operating system) as of the source system. For example, if the source system is running on Windows, the target system must also be running on Windows.
4. Copy the backup files to the system on the supported operating system.
5. Run the restore operation of the backup files on the supported operating system by using the graphical user interface or command-line interface.
6. The installation of IBM Security Key Lifecycle Manager, version 2.5 on the supported operating system detects earlier versions 2.0 or 2.0.1, which is preinstalled in this system and runs the migration process.

Note:

- If you are using IBM Security Key Lifecycle Manager earlier version 1.0 on unsupported operating systems (Red Hat Enterprise Linux Version 4.0, SuSE Linux Enterprise Server Version 9.0, AIX 5.3, Solaris 9, Windows 2003 R2, and Windows 2008), you must first migrate to IBM Security Key Lifecycle Manager earlier version 2.0 or 2.0.1.

- If version 2.0 or 2.0.1 is installed on the supported operating systems, the IBM Security Key Lifecycle Manager installer detects it and runs the migration task.

Operating system matrix for migration

The following table lists the supported operating systems for various versions of IBM Security Key Lifecycle Manager and Encryption Key Manager, version 2.1:

Operating system	Encryption Key Manager, version 2.1	Tivoli Key Lifecycle Manager, version 1.0	Tivoli Key Lifecycle Manager, version 2.0	Tivoli Key Lifecycle Manager, version 2.0.1	IBM Security Key Lifecycle Manager, version 2.5
Windows Server 2003 R2 32–bit	✓	✓	✓	✓	
Windows Server 2003 R2 64-bit (32-bit mode application)	✓	✓	✓	✓	
Windows Server 2008 32-bit	✓	✓	✓	✓	
Windows Server 2008 64-bit (32-bit mode application)	✓	✓	✓	✓	
Windows Server 2008 R2 64-bit (32-bit mode application)	✓		✓	✓	✓
Windows Server 2012 64-bit (32-bit mode application)					✓
Windows Server 2012 R2 64-bit (32-bit mode application)					✓
AIX 5.3 64–bit	✓	✓ Use technology level 5300-04 and Service Pack 5300-04-02	✓ Use technology level 9 and Service Pack 2. The minimum C++ runtime level requires the xlC.rte 9.0.0.8 and xlC.aix50.rte 9.0.0.8 (or later) filesets. These filesets are included in the June 2008 IBM® C++ Runtime Environment Components for AIX package.	✓ Use technology level 9 and Service Pack 2. The minimum C++ runtime level requires the xlC.rte 9.0.0.8 and xlC.aix50.rte 9.0.0.8 (or later) filesets. These filesets are included in the June 2008 IBM® C++ Runtime Environment Components for AIX package.	

Operating system	Encryption Key Manager, version 2.1	Tivoli Key Lifecycle Manager, version 1.0	Tivoli Key Lifecycle Manager, version 2.0	Tivoli Key Lifecycle Manager, version 2.0.1	IBM Security Key Lifecycle Manager, version 2.5
AIX 6.1 64–bit	✓	✓	✓ Use AIX 6.1 technology level 2. The minimum C++ runtime level requires the xlC.rte 9.0.0.8 and xlC.aix61.rte 9.0.0.8 (or later) filesets. These filesets are included in the June 2008 IBM C++ Runtime Environment Components for AIX package.	✓ Use AIX 6.1 technology level 2. The minimum C++ runtime level requires the xlC.rte 9.0.0.8 and xlC.aix61.rte 9.0.0.8 (or later) filesets. These filesets are included in the June 2008 IBM C++ Runtime Environment Components for AIX package.	✓
AIX 7.1 64–bit	✓		✓	✓	✓
Sun Server Solaris 9 (SPARC 64–bit)	✓	✓	✓ Apply patches 111711-12 and 111712-12 If raw devices are used, apply patch 122300-11.	✓ Apply patches 111711-12 and 111712-12 If raw devices are used, apply patch 122300-11.	
Sun Server Solaris 10 (SPARC 64–bit)	✓	✓	✓ If raw devices are used, apply patch 125100-07.	✓ If raw devices are used, apply patch 125100-07.	✓
SuSE Linux Enterprise Server Version 9 on x86 (32–bit)	✓	✓	✓	✓	
SuSE Linux Enterprise Server Version 10 on x86 (32–bit)	✓	✓	✓ SLES10 SP2	✓ SLES10 SP2	
SuSE Linux Enterprise Server Version 10 x86_64 (32-bit mode application)	✓	✓	✓ Use Service Pack 2	✓ Use Service Pack 2	✓
SuSE Linux Enterprise Server Version 11 on x86	✓		✓	✓	

Operating system	Encryption Key Manager, version 2.1	Tivoli Key Lifecycle Manager, version 1.0	Tivoli Key Lifecycle Manager, version 2.0	Tivoli Key Lifecycle Manager, version 2.0.1	IBM Security Key Lifecycle Manager, version 2.5
SuSE Linux Enterprise Server Version 11 (System z) on x86_64	✓		✓	✓	✓
Red Hat Enterprise Linux AS 4.0 on x86	✓	✓	✓	✓	
Red Hat Enterprise Linux 5.0 on x86	✓	✓	✓ Use Update 2	✓	
Red Hat Enterprise Linux 5.0 on x86_64 (32-bit mode application)	✓	✓	✓ Use Update 2	✓	✓
Red Hat Enterprise Linux 5.0 (System z) on x86_64	✓		✓	✓ Use Update 1	✓
Red Hat Enterprise Linux 6 on x86	✓				
Red Hat Enterprise Linux 6 on x86_64	✓				✓
Red Hat Enterprise Linux 6 (System z) on x86_64	✓				✓
To migrate from unsupported Linux operating systems, see the “Migration from unsupported Linux operating systems” on page 29 topic.					

Obtaining Encryption Key Manager

You can migrate only version 2.1 of Encryption Key Manager to IBM Security Key Lifecycle Manager, version 2.5.

About this task

If you are using earlier versions of Encryption Key Manager, upgrade to version 2.1. To obtain Encryption Key Manager, version 2.1, contact IBM Software Support at: http://www.ibm.com/software/support

Migration restrictions for Encryption Key Manager

There are certain restrictions on what you can migrate from Encryption Key Manager.

- Migration of Administrator SSL keystores and truststores is not supported. IBM Security Key Lifecycle Manager server does not support Administrator sync capability.
- Migration of PKCS11Impl keystores and truststores is not supported. IBM Security Key Lifecycle Manager server does not support PKCS11Impl keystores.

- IBM Security Key Lifecycle Manager does not support the use of a key in multiple groups, unlike Encryption Key Manager, which supports the use of a key in multiple groups.

  When you migrate key data in KeyGroup.xml from Encryption Key Manager to IBM Security Key Lifecycle Manager, each key is attached to one group. A key that was previously in multiple groups in Encryption Key Manager is created in only one group in IBM Security Key Lifecycle Manager.

  The migration process logs the event that the key is not created in multiple groups, and continues. If the symmetricKeySet property specifies a list or range or keys, and not a group, all keys that are specified by symmetricKeySet are migrated into a key group named DefaultMigrateGroup. If the keys from symmetricKeySet are created as a part of other groups, and the key group named DefaultMigrateGroup is empty, IBM Security Key Lifecycle Manager does not create the DefaultMigrateGroup key group, and also does not migrate the symmetricKeySet property.

  To work around the problem, use the IBM Security Key Lifecycle Manager graphical or command-line interface to define a default key group, for example, for LTO tape drives.

After migration of Encryption Key Manager

After Encryption Key Manager is migrated, you must validate the configuration and protect data.

- Do not run Encryption Key Manager. After migration, the Encryption Key Manager retains its ability to serve keys.
- Resolve possible problems with certificates and keys.

  Encryption Key Manager does not restrict device groups to which a certificate and its keys can be associated. Certificates and keys that belong to multiple device types are marked as CONFLICTED after migration to IBM Security Key Lifecycle Manager Version 2.5. You cannot change their device group to another device group. IBM Security Key Lifecycle Manager can use a certificate or key that is marked as CONFLICTED for both read and write operations.

  Migration might also cause a certificate to appear with an UNKNOWN label in the IBM Security Key Lifecycle Manager graphical user interface.

  - Unknown certificates can be used as rollover certificates. Once scheduled as a rollover, the unknown certificate is updated to the specific device group of the rollover. An SSL server certificate with an UNKNOWN label is updated to be an SSL certificate.
  - Pending certificates might be listed on the graphical user interface with a device group that has an UNKNOWN status. First, accept the pending certificate, which then has an UNKNOWN status. Next, use the **tklmCertUpdate** command to update the certificate usage to a specific device group. The update changes the certificate status to a state such as active.
  - After migration completes, one or more devices might be associated with the `UNKNOWN` device group. You can assign the device group for `UNKNOWN` devices to a new group, or allow the group to be determined when the devices make a first key service request.

  Use the **`tklmCertList`** command to find certificates that are marked as `CONFLICTED` or `UNKNOWN`. Specify no value for the **`-usage`** parameter, or specify a parameter value of 3592, DS8000, or `SSLSERVER`. For example, this Jython-formatted command lists all certificates for the 3592 device group:

  ```
  print AdminTask.tklmCertList('[-usage 3592 -v y]')
  ```

- Verify that the migrated Encryption Key Manager configuration is in the state that you expect before making any updates or any configuration changes to IBM Security Key Lifecycle Manager.

  The Encryption Key Manager configuration keystore becomes the IBM Security Key Lifecycle Manager keystore after migration is complete. You cannot migrate Encryption Key Manager server data a second time to the same IBM Security Key Lifecycle Manager server.

  If migration fails and you choose to complete the remaining IBM Security Key Lifecycle Manager installation process, there is a stand-alone migration-recovery script that you can start only if you are not made any updates or changes to the IBM Security Key Lifecycle Manager configuration. For more information, see “Recovery from migration failure” on page 73.

After migrating IBM Security Key Lifecycle Manager

After IBM Security Key Lifecycle Manager is migrated, you must validate the configuration and protect data.

- Immediately after you install IBM Security Key Lifecycle Manager, version 2.5, perform a backup of IBM Security Key Lifecycle Manager, version 2.5. A backup of earlier version cannot be restored to a version 2.5 environment.

  Migration to version 2.5 does not remove the earlier version of IBM Security Key Lifecycle Manager. You must not run two versions simultaneously to avoid port conflict.

  Note: On Windows platform, after you migrate IBM Security Key Lifecycle Manager earlier version (1.0, 2.0, or 2.0.1) to version 2.5, DB2 associated with the earlier version might not start if you uninstall IBM Security Key Lifecycle Manager version 2.5 before uninstalling the earlier version.

  If migration fails and you choose to complete the remaining IBM Security Key Lifecycle Manager installation process, there is a stand-alone migration-recovery script that you can start only if you have not made any updates or changes to the IBM Security Key Lifecycle Manager configuration. For more information, see “Recovery from migration failure” on page 73. You must complete the migration recovery process before you can use IBM Security Key Lifecycle Manager, version 2.5.
- Retain and do not run a replica of IBM Security Key Lifecycle Manager previous version to ensure that you have a environment and data for the previous version in case validation determines that there is a problem with version 2.5.
- Resolve possible problems with certificates and keys.

  IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, or 2.0.1 does not restrict device groups to which a certificate and its keys can be associated. Certificates and keys that belong to multiple device types at version 1.0, 2.0, or 2.0.1 are marked as CONFLICTED at version 2.5. You cannot change their device group to another device group. IBM Security Key Lifecycle Manager can use a certificate or key that is marked as CONFLICTED for both read and write operations.
- After migration completes, one or more devices might be associated with the `UNKNOWN` device group. You can assign the device group for `UNKNOWN` devices to a new group, or allow the group to be determined when the devices make a first key service request.

- After you complete migration of IBM Security Key Lifecycle Manager earlier version to version 2.5, the migration program will not remove the previous version. To remove, follow the uninstall instructions for the version of the product you have migrated from.

  Note: Because the IP ports are shared between the two versions, do not run both versions at the same time. If migration cannot complete these steps, migration process issues a warning and a successful completion message. Examine the `<`*`IM App Data Dir`*`>/logs/sklmLogs/migration.log` file for messages and take the appropriate manual action.
- For future administrative use in IBM Security Key Lifecycle Manager previous version, you might have marked a certificate for use as a 3592 rollover or a key group as an LTO rollover. If the scheduled future date for rollover is earlier than the time of migration, the migration program adds an appropriate message and does not migrate these rollover entries. After successfully installing IBM Security Key Lifecycle Manager, version 2.5, use the command-line interface or graphical user interface to manually add these rollover entries.
- 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.
- After you ensure that the primary IBM Security Key Lifecycle Manager at version 2.5 is configured and running correctly, back up the version 2.5 IBM Security Key Lifecycle Manager server and install the backup on a replica computer.
  - Validate that the version 2.5 replica computer is configured and running correctly.
  - Retain a copy of version 2.5 backup files in a location that is not in the IBM Security Key Lifecycle Manager version 2.5 directory path. The separate location ensures that other processes cannot remove backup files if IBM Security Key Lifecycle Manager is removed.

    Additionally, retain the `<`*`IM App Data Dir`*`>/logs/sklmLogs/migration.log` files for future reference.

Data objects and properties migrated from Encryption Key Manager

The data objects and properties are also migrated from Encryption Key Manager.

Properties that must be in the Encryption Key Manager configuration file include:

- Audit.metadata.file.name

  File must exist in the same directory as the configuration file itself and must be read enabled.
- config.drivetable.file.url

  File must exist in the same directory as the configuration file itself and must be read enabled.
- config.keystore.file

  File must exist in the same directory as the configuration file itself and must be read and write enabled.
- config.keystore.password.obfuscated
- config.keystore.type

  The keystore type must not be PKCS11IMPLKS.

- TransportListener.ssl.keystore.name

  File must exist in the same directory as the configuration file itself and must be read enabled.
- TransportListener.ssl.keystore.password.obfuscated
- TransportListener.ssl.keystore.type

  The keystore type must not be PKCS11IMPLKS.
- TransportListener.ssl.port

  The value must be a positive integer between 1 and 65535 and must not be identical to the value for TransportListener.tcp.port.
- TransportListener.ssl.truststore.type

  The truststore type must not be PKCS11IMPLKS.
- TransportListener.tcp.port

  The value must be a positive integer between 1 and 65535 and must not be identical to the value for TransportListener.ssl.port.

Migration includes the following data objects:

Keystores

IBM Security Key Lifecycle Manager stores all keys and certificates in the database. During migration, the keys and certificates from the two Encryption Key manager keystores, `Config`, and `TransportListner` are all copied to the IBM Security Key Lifecycle Manager database. Keys and certificates are copied from the `Config` keystore. The certificates are copied from the `TransportListner` truststore.

A certificate from the `TransportListener` keystore is set as the SSL certificate for IBM Security Key Lifecycle Manager. The **`config.keystore.ssl.certalias`** property is updated with the alias of this certificate.

Other Encryption Key Manager keystores are not used.

Devices

All the device information is read from the drive table pointed at by the config.drivetable.file.url property, and is entered in an IBM Security Key Lifecycle Manager database. If the drive has the symalias property that is defined, the drive type is set to LTO. If the drive has aliases that are defined, the drive type is set to 3592. Migration sets a type of UNKNOWN for a drive that has none of these properties that are defined and that has no type that can be determined.

Keygroups

The keygroup.xml file that is pointed at by the config.keygroup.xml.file property, is parsed, and the keygroup information is stored in an IBM Security Key Lifecycle Manager database. All the group members and group relationships are also migrated.

If the symmetricKeySet property has a list of aliases or range of aliases, a default key group named DefaultMigrationGroup is created with all the aliases as members of the group. In this case, the symmetricKeySet property is set to DefaultMigrationGroup. If the symmetricKeySet property is already a group alias, the default migration group is not created.

Metadata

All the metadata information that is pointed at by the Audit.metadata.file.name property is migrated into an IBM Security Key Lifecycle Manager database.

The properties that are migrated from the Encryption Key Manager configuration file to the SKLMConfig.properties file might include:

- Audit.eventQueue.max
- Audit.handler.file.size
- Audit.event.outcome
- Audit.event.types
- config.keystore.name (set to `defaultKeyStore`)
- cert.valiDATE
- drive.acceptUnknownDrives is migrated to the database as the default entry in the specified device group.
- fips
- TransportListener.ssl.ciphersuites
- TransportListener.ssl.clientauthentication
- TransportListener.ssl.port
- TransportListener.ssl.protocols
- TransportListener.ssl.timeout
- TransportListener.tcp.port
- TransportListener.tcp.timeout
- useSKIDefaultLabels
- zOSCompatibility

These properties **are** migrated from the Encryption Key Manager configuration file to the IBM Security Key Lifecycle Manager database:

- **`drive.default.alias1`**
- **`drive.default.alias2`**
- **`symmetricKeySet`** (set to an already-specified group alias, otherwise set to **`DefaultMigrationGroup`**)

Data objects and properties migrated from IBM Security Key Lifecycle Manager

The data objects and properties are also migrated from IBM Security Key Lifecycle Manager earlier versions 1.0, 2.0, and 2.0.1.

Keystore

The keystore, including all certificates and metadata from earlier versions, are added to the IBM Security Key Lifecycle Manager, version 2.5 database. The keystore is identified by the **`config.keystore.name`** property in the SKLMConfig.properties file.

Devices

All the device information is read from the IBM Security Key Lifecycle Manager database.

Keygroups

The key group information is read from the IBM Security Key Lifecycle Manager database.

Rollover certificates and keygroups

Certificates and keygroups from the earlier versions might be marked for future 3592 administration. The migration program detects and marks these rollovers for future administration with IBM Security Key Lifecycle Manager, version 2.5.

Metadata

All the metadata information is migrated from earlier version database and made usable by the IBM Security Key Lifecycle Manager, version 2.5 database.

Properties

Properties in the SKLMConfig.properties file are migrated from the IBM Security Key Lifecycle Manager database. The `datastore.properties` file is migrated.

These properties are replaced in the version 2.5 SKLMConfig.properties file:

- **`ds8k.acceptUnknownDrives`**

  The **`device.AutoPendingAutoDiscovery`** property replaces this property.
- **`drive.acceptUnknownDrives`**

  The **`device.AutoPendingAutoDiscovery`** attribute in the IBM Security Key Lifecycle Manager database replaces this property.

These IBM Security Key Lifecycle Manager, version 2.0.1 properties are obsolete and are not migrated:

- **`tklm.internal.gui.jagworkflow`**
- **`tklm.internal.gui.lto4workflow`**

These properties are migrated from the version 2.5 SKLMConfig.properties file to the IBM Security Key Lifecycle Manager database:

- **`drive.default.alias1`**
- **`drive.default.alias2`**
- **`symmetricKeySet`** (removed from the SKLMConfig.properties file and replaced with an entry for the device group in the IBM Security Key Lifecycle Manager database)

Types of installation

You have several options for installing IBM Security Key Lifecycle Manager.

On distributed systems, you can use one of these modes of installation:

- A graphical user interface-based installation that is driven by a wizard.
- A silent installation that runs unattended, using response files for the configuration options.

Note: IBM Security Key Lifecycle Manager does not support a console mode installation.

Installing required libraries on Red Hat Enterprise Linux systems

Before you run the installation commands for graphical or silent mode installation, you must install the required libraries on x86-64-bit Red Hat Enterprise Linux Version 6.0 and Red Hat Enterprise Linux Version 6.1 systems.

Procedure

1. Mount the Red Hat Enterprise Linux 6.0/6.1 distribution DVD to the system. Insert the DVD into the DVD drive.
2. Select open a terminal window as a root.
3. Execute the commands:
   ```
   [root@localhost]# mkdir /mnt/cdrom
   [root@localhost]# mount -o ro /dev/cdrom /mnt/cdrom
   ```
4. Create the text file `server.repo` in the `/etc/yum.repos.d` directory.

   Note: To use gedit:

   a. execute the command:
      ```
      [root@localhost]# gedit /etc/yum.repos.d/server.repo
      ```
   b. Add the following text to the file:
      ```
      [server]
      name=server
      baseurl=file:///mnt/cdrom/Workstation
      enabled=1
      ```

      Where `baseurl` depends on the mounting point and the Red Hat Enterprise Linux distribution.

      In the example, the mounting point is `cdrom` and the Red Hat Enterprise Linux distribution is `Workstation`, but can be `sever`.
5. Execute the command:
   ```
   [root@localhost]# yum clean all
   ```
6. Execute the command to import related public keys:
   ```
   [root@localhost]# rpm --import /mnt/cdrom/*GPG*
   ```
7. Execute the commands to install the required libraries:
   ```
   [root@localhost]# yum install gtk2.i686
   [root@localhost]# yum install libXtst.i686
   ```

   If you received the missing libstdc++ message above, install the libstdc++ library:

```
[root@localhost]# yum install compat-libstdc++
```

During the install you might receive prompts similar to the example. Answer with `'y'`.

Example:

```
Total download size: 15 M
Installed size: 47 M
Is this ok [y/N]: y
```

Note: The package name extension (.i686) might change in the command depending on the hardware platform that you use. The table lists valid values for the package name extension. Red Hat Enterprise Linux 6.0 package names on different platforms:

Platform	32-bit	64-bit
x86/x86_64	i686	x86_64
ppc/ppc64	ppc	ppc64
s390/s390x	s390	s390x

Syntax and parameters for the installation program

You must use the installation commands to install IBM Security Key Lifecycle Manager.

Silent installation

`silent_install.sh` *`full_path_to_response_file`*

`silent_install.bat` on Windows systems.

`silent_install.sh` on systems such as Linux or AIX.

Graphical mode installation

`install_program`

Where *install_program* is

`launchpad.exe` on Windows systems.

`launchpad.sh` on systems such as Linux, Linux for System z, AIX, or Solaris.

Note: Do not install from a network drive or mounted drive. For example, do not specify either of these **net use** statements as the directory location and attempt installation:

```
net use z: \\server\share
net use \\server\share
```

Graphical mode installation

IBM Security Key Lifecycle Manager provides a graphical user interface installation program. IBM Installation Manager is used to install IBM Security Key Lifecycle Manager and its components. It presents a series of panels that prompt for the information that is required for installation.

These steps install IBM Security Key Lifecycle Manager in graphical mode.

- Start the installation wizard.
- Complete the installation wizard pages, entering the configuration options. For details, see “Installation on distributed systems” on page 49.

- Verify that the IBM Security Key Lifecycle Manager server is operational. For details, see "Installation verification" on page 90.

Command to start a graphical installation

To start the installation wizard, navigate to the directory where you stored the installation files, and run the installation command.

```
install_program
```

Where *install_program* is:

launchpad.exe on Windows systems.

launchpad.sh on systems such as Linux, Linux for System z, AIX, or Solaris.

For details about the syntax and flags for the installation program, see "Syntax and parameters for the installation program" on page 44.

Installation and migration panels

Installing IBM Security Key Lifecycle Manager in graphical mode requires you to start the installation wizard, navigate through a series of installation panels, and supply the requisite information.

You might see these panels during installation:

1. Language selection and introduction
2. Installation Manager window with installation packages such as IBM Installation Manager, IBM DB2, IBM WebSphere Application Server, and IBM Security Key Lifecycle Manager
3. Software license agreement
4. Installation directory selection for IBM Installation Manager and the other installation packages.
5. Language selection for package translation
6. Package features selection for installation
7. DB2 configuration options
8. IBM Security Key Lifecycle Manager configuration options
9. Installation progress for IBM Security Key Lifecycle Manager
10. Installation summary

Notes:

- When you install IBM Security Key Lifecycle Manager, retain the default path for **Shared Resources Directory**. IBM Installation Manager uses this location to download artifacts and to store information about the installed packages.
- When the installation is complete, a page displays the status of the installation and the list of packages that are installed. You must select **None** to instruct the installer not to create a profile and click **Finish**.

You might see these panels when migration occurs during installation:

1. Language selection
2. Introduction
3. Software license agreement
4. DB2 directory
5. **Migration information**
6. **Migration summary**

7. Summary of prerequisites
8. Installation progress for DB2
9. Beginning IBM Security Key Lifecycle Manager installation
10. Installation directory for IBM Security Key Lifecycle Manager and WebSphere Application Server
11. WebSphere Application Server information
12. SKLMAdmin password
13. Pre-installation summary
14. Migration progress for IBM Security Key Lifecycle Manager
15. Installation summary

Silent installation

A silent installation is a noninteractive installation, which is driven by a response file that provides installation settings.

No user input is required during a silent installation. This type of installation is useful in environments where IBM Security Key Lifecycle Manager is to be installed on multiple identical systems, such as in a data center.

Note: Silent mode installation uses a response file that might contain password information. For more security, delete the response file immediately after the installation of IBM Security Key Lifecycle Manager.

You must add the encrypted passwords to the relevant elements of the response file. Use the IBM Installation Manager utility to create an encrypted password.

Windows

For example, if you extract the IBM Security Key Lifecycle Manager product image to the `C:\SKLM\disk1` directory, run the following command to create an encrypted password.

```
cd C:\SKLM\disk1\im\tools
imcl.exe encryptString password
```

Add the encrypted password that you created in the response file as shown in the following example.

```
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.ofng'
value='<encrypted password>'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.ofng'
value='<encrypted password>'/>
...
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.win32'
value='<encrypted password>'/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.win32'
value='<encrypted password>'/>
...
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.win32'
value='<encrypted password>'/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.win32'
value='<encrypted password>'/>
```

Linux For example, if you extract the IBM Security Key Lifecycle Manager product image to the `/SKLM/disk1` directory, run the following command to create an encrypted password.

```
cd /SKLM/disk1/im/tools
./imcl encryptString password
```

Add the encrypted password that you created in the response file as shown in the following example.

```
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.aix.ofng'
value='<encrypted password>'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.aix.ofng'
value='<encrypted password>'/>
...
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.aix'
value='<encrypted password>'/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.aix'
value='<encrypted password>'/>
...
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.aix'
value='<encrypted password>'/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.aix'
value='<encrypted password>'/>
```

You can create a different encrypted password for each user.

To start the installation program in `silent` mode by using a response file, enter this command:

```
silent_install.sh full_path_to_response_file
```

`silent_install.bat` on Windows systems.

`silent_install.sh` on systems such as Linux or AIX.

Note: If you enter an invalid value for the *full_path_to_response_file* parameter, such as an incomplete path, the installation program exits. No error message is displayed or logged.

Sample response files

IBM Security Key Lifecycle Manager includes sample response files that you can use as a template for creating your own response file. The sample file must be modified for the specifics of your environment before it can be used.

The sample response files are in the directory in which your installation package is located.

- "New installation of version 2.5 on Windows systems" on page 95
- "New installation of version 2.5 on systems such as Linux or AIX systems" on page 96
- "Earlier version to version 2.5 migration on Windows systems" on page 98
- "Earlier version to version 2.5 migration on Linux systems" on page 99
- "Earlier version to version 2.5 migration on AIX systems" on page 101
- "Earlier version to version 2.5 migration on Solaris systems" on page 103
- "Uninstallation on Windows systems" on page 104
- "Uninstallation on systems such as Linux or AIX" on page 105

Installation on distributed systems

During graphical mode installation, you are prompted for the configuration information that is required to install IBM Security Key Lifecycle Manager and the prerequisite software it uses.

Notes: There are several important considerations to keep in mind:

- Installation can take more than an hour.
- Do not install from a network drive or mounted drive. For example, do not specify either of these *net use* statements as the directory location and attempt installation:

  ```
  net use z: \\server\share
  net use \\server\share
  ```

- Ensure that you select the correct language at prompts during installation. Correcting a locale error requires uninstalling and reinstalling IBM Security Key Lifecycle Manager and DB2.
- When you install IBM Security Key Lifecycle Manager, the DB2 password that you specify must comply with the password policy of the underlying operating system.
- When you install IBM Security Key Lifecycle Manager on a system such as Solaris, certain DB2 configuration changes made during installation might require that you restart the system. Close any other applications before you restart the system. After the system restarts, run the installation program again.
- Entries for all fields are restricted to alphabetical characters (A-Z and a-z), numeric characters (0-9), and the underscore character (_). The restriction also applies to the values in the response file that is used for silent installations.
- Ensure that the installation path does not contain Unicode characters.
- Ensure that there are no non-ASCII characters in the installation path.
- If you have IBM Security Key Lifecycle Manager earlier version in your environment before you install and migrate to version 2.5:
  - Obtain the administrative passwords for your earlier version of IBM Security Key Lifecycle Manager.
  - Apply the most current fix pack to your earlier version of IBM Security Key Lifecycle Manager.
  - On Windows systems, ensure that the IBM ADE Service is started.

    On Windows systems, open the Services console. Verify that the IBM ADE Service is started. If the service is not started, select and start the service.

DB2 configuration during installation

IBM Security Key Lifecycle Manager requires DB2 Workgroup Server Edition at a Version 10.1 level that depends on the operating system.

The installation program runs one of the following actions:

- If an existing copy of DB2 Workgroup Server Edition is installed as the root user at the correct version for the operating system, you can use the existing DB2 Workgroup Server Edition. IBM Security Key Lifecycle Manager installer does not detect the presence of DB2. You must specify the DB2 installation path.

You can also install a new copy of DB2 Workgroup Server Edition. An existing DB2 must be locally installed on the system and not on a network or shared drive.

On a Windows system, if a new copy of DB2 is installed, the `DB2_COPY_NAME` is set to `DBSKLMV25`.

- If IBM Security Key Lifecycle Manager earlier version and an earlier version of DB2 exist on the system, the process installs DB2 Workgroup Server Edition at a version 10.1 level that depends on the operating system. You can also use another existing, installed version of DB2 10.1 that is at the correct level.

  The process also migrates data from the previous version of IBM Security Key Lifecycle Manager to the new version. For example:

  - The new copy of DB2 Workgroup Server Edition uses the previous `db2admin` user ID and password.
  - On a Windows system, if a new copy of DB2 is installed, the `DB2_COPY_NAME` is set to `DBSKLMV25`.
- If no IBM Security Key Lifecycle Manager exists on the system and there is either no copy or an earlier version of DB2, the installation process installs DB2 Workgroup Server Edition at a version 10.1 level that depends on the operating system.

  No DB2 upgrade occurs.

During DB2 configuration, you are prompted for the following information, which might differ from this list, depending on the operating system and on whether IBM Security Key Lifecycle Manager is installing DB2 or by using an existing copy:

DB2 Selection

The directory for the DB2 installation.

On systems such as AIX or Linux, the entry must start from the root directory. The first character in the entry must be a forward slash ('/').

The installation process provides a default value. See “Definitions for *HOME* and other directory variables” on page 7.

DB2 Administrator ID

The local DB2 administrator user ID. The installation process provides a default Administrator user ID with the necessary permissions. Do not use a domain user ID as the DB2 administrator. Do not specify a user ID greater than eight characters in length.

Note: Do not use a hyphen (-) or underscore character (_) when you specify a user ID for an existing copy of DB2.

On a Windows system, the DB2 Administrator user ID must be a member of the Administrator group. The user ID is subject to the security policy active on the Windows system.

On a system such as Linux or AIX, the user ID of the IBM Security Key Lifecycle Manager DB2 instance owner must be a member of a group in which the root user ID is also a member. If it is available, use bin as the group. If `bin` is not available, ask the system administrator for the name of a general-purpose group to use.

Note: The Administrator ID cannot be a DB2 reserved word, such as `db2`, `users`, `admins`, `guests`, `public`, `private`, `properties`, `local`, or `root`.

DB2 Administrator Password

The password for the administrator. The maximum length is 20 characters.

The password for the DB2 Administrator user ID is subject to the security policy active on the system. In addition, the login password for the DB2 Administrator user ID and the DB2 password for the user ID must be the same. When you change one, you must change the other.

Database Name
The name of the IBM Security Key Lifecycle Manager database, which is `sklmdb`.

DB2 Port
The port that DB2 uses.

Administrator's Group
Access group in which the Administrator user ID exists. If DB2 is on a system such as AIX or Linux, your user ID must be in the bin or root group, or in a separate group in which root is a member.

Administrator / Database Home
The directory (AIX or Linux systems) or drive (Windows systems) in which the database instance and the formatted tables that are used by IBM Security Key Lifecycle Manager are created.

Notes:

1. Entries for all fields are restricted to alphabetical characters (A-Z and a-z), numeric characters (0-9), and the underscore character (_). The restriction also applies to the values in the response file that is used for silent installations.
2. Do not specify spaces in any of the directory paths or file names.
3. The name of the computer on which you install DB2 cannot start with "ibm," "sql," or "sys," in lowercase or uppercase. The name of the computer also cannot contain the underscore character (_).

DB2 password security issues on Windows systems

On Windows systems, the DB2 Administrator user ID and password are subject to the security policy that is active on the system.

If there is a password expiration restriction in effect, you must change the login password and DB2 password for the Administrator user ID before the expiration period expires.

In addition, the login password for the DB2 Administrator user ID and the DB2 data source password that is used by WebSphere Application Server must be the same. When you change one, you must change the other.

To change the DB2 database password, take these steps:

1. Stop the WebSphere Application Server and *all* Windows services that are related to DB2.
2. Open the Windows user management tool by opening the Control Panel and clicking **Administrative tools** > **Computer Management** > **Local Users and Groups** > **Users**.
3. Change the password for the IBM Security Key Lifecycle Manager database owner.
4. Open the Windows Services console by opening the Control Panel and clicking **Administrative Tools > Computer Management**.
5. On the following services, change the password by using the **Logon** tab of the **Properties** dialog box:

- DB2 - DBSKLMV25 - *sklminstance*

  For example, the value of *sklminstance* might be:

  ```
  DB2 - DBSKLMV25 - DBSKLM25
  DB2 - DBSKLMV25 - SKLMDB2
  ```

  For example, with the default instance name, the value of *sklminstance* is:

  ```
  DB2 - DBSKLMV25 - SKLMDB2
  ```

- DB2 Governor (DBSKLMV25)
- DB Remote Command Server (DBSKLMV25)
- DB2DAS - DB2DAS00

When the passwords are changed for all the services, restart the services.

The following services must be stopped and restarted. Password change is not required:

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

6. Start the WebSphere Application Server.
7. Using the **wsadmin** interface that the WebSphere Application Server provides, specify the Jython syntax.

   ```
   wsadmin -username WASAdmin -password mypwd -lang jython
   ```

8. Use the **wsadmin** command to change the password of the WebSphere Application Server data source:

   a. The following command lists JAASAuthData entries:

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

   The result might be:

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

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

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

   For example, type on one line:

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

   The result is:

   ```
   sklm_db
   ```

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

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

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

   For example, type on one line:

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

   d. Save the changes:

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

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

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

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

2) Stop and start the IBM Security Key Lifecycle Manager server service, which has a name like `IBMWAS85Service - SKLMServer`.

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

1) First, type:

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

The result might be:

```
"Default Datasource(cells/SKLMCell/nodes/SKLMNode/servers/server1|
resources.xml#DataSource_1183122153625)"
"SKLM DataSource(cells/SKLMCell/nodes/SKLMNode/servers/server1|
resources.xml#DataSource_1379859893896)"
"SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/servers/
server1|resources.xml#DataSource_1379859896273)"
DefaultEJBTimerDataSource(cells/SKLMCell/nodes/SKLMNode/servers/
server1|resources.xml#DataSource_1000001
```

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

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

For example, type on one line:

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

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

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

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

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

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

DB2 password security issues on systems such as Linux or AIX

On systems such as Linux or AIX, you might want to change the password for the DB2 Administrator user ID. The login password for the DB2 Administrator user ID and the DB2 password for the user ID must be the same.

The IBM Security Key Lifecycle Manager installation program installs DB2 and prompts the installing person for a password for the user named `sklmdb2`. Additionally, the DB2 application creates an operating system user entry named `sklmdb2`. For example, the password for this user might expire, requiring you to resynchronize the password for both user IDs.

Before you can change the password of the DB2 Administrator user ID, you must change the password for the system user entry. Take these steps:

1. Log on to IBM Security Key Lifecycle Manager server as root.
2. Change user to the `sklmdb2` system user entry. Type:

   ```
   su sklmdb2
   ```

3. Change the password. Type:

   ```
   passwd
   ```

   Specify the new password.

4. Exit back to root.

   ```
   exit
   ```

5. In the *WAS_HOME*/bin directory, use the **wsadmin** interface that the WebSphere Application Server provides to specify the Jython syntax.

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

6. Change the password for the WebSphere Application Server data source:

   a. The following command lists the JAASAuthData entries:

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

      The result might like this example:

      ```
      (cells/SKLMCell|security.xml#JAASAuthData_1228871756187)
      (cells/SKLMCell|security.xml#JAASAuthData_1228871757843)
      ```

   b. Type the **AdminConfig.showall** command for each entry to locate the alias sklm_db. For example, type on one line:

      ```
      print AdminConfig.showall
        ('(cells/SKLMCell|security.xml#JAASAuthData_1228871756187)')
      ```

      The result is like this example:

      ```
      {alias sklm_db}
      {description "SKLM database user j2c authentication alias"}
      {password *****}
      {userId sklmdb2}
      ```

      And also type on one line:

      ```
      print AdminConfig.showall
        ('(cells/SKLMCell|security.xml#JAASAuthData_1228871757843)')
      ```

      The result is like this example:

      ```
      {alias sklmdb}
      {description "SKLM database user J2C authentication alias"}
      {password *****}
      {userId sklmdb2}
      ```

   c. Change the password for the sklm_db alias that has the identifier JAASAuthData_**1228871756187**:

      ```
      print AdminConfig.modify('JAASAuthData_list_entry', '[[password passw0rdc]]'
      ```

      For example, type on one line:

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1228871756187)',
      '[[password tucs0naz]]')
      ```

   d. Change the password for the sklmdb alias that has the identifier JAASAuthData_**1228871757843**:

      ```
      print AdminConfig.modify('JAASAuthData_list_entry', '[[password passw0rdc]]'
      ```

      For example, type on one line:

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1228871757843)',
      '[[password tucs0naz]]')
      ```

   e. Save the changes:

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

   f. Exit back to root.

      ```
      exit
      ```

   g. In the *WAS_HOME*/bin directory, stop the WebSphere Application Server application. For example, as WASAdmin, type on one line:

      ```
      stopServer.sh server1 -username wasadmin -password passw0rd
      ```

      The result is like this example:

```
ADMU0116I: Tool information is being logged in file
//opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the WASProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.
```

h. Start the WebSphere Application Server application. As the WebSphere Application Server administrator, type on one line:

```
startServer.sh server1
```

i. In the *WAS_HOME*/bin directory, use the **wsadmin** interface that the WebSphere Application Server provides to specify the Jython syntax.

```
./wsadmin.sh -username wasadmin -password mypwd -lang jython
```

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

1) First, query for a list of data sources. Type:

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

The result might be like this example:

```
"SKLM DataSource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1228871762031)"
"SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1228871766562)"
"Tivoli Common Reporting Data Source(cells/SKLMCell|resources.xml#
  DataSource_1227211230078)"
DefaultEJBTimerDataSource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1000001)
ttssdb(cells/SKLMCell|resources.xml#DataSource_1227211144390)
```

2) Type:

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

For example, type on one line:

```
print AdminControl.testConnection
  ('SKLMDataSource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1228871762031)')
```

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

```
print AdminControl.testConnection
 ('SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1228871766562)')
```

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

```
WASX7217I: Connection to provided data source was successful.
```

Middleware configuration during installation

The installation wizard gathers configuration information for IBM Security Key Lifecycle Manager and for the WebSphere Application Server runtime environment.

The installation requires answers for the following fields:

- Use only alphabetical characters (A-Z and a-z), numeric characters (0-9), and the underscore character (_). The restriction also applies to the values in the response file during silent installations.

  The name string cannot contain leading and trailing spaces, and cannot contain these characters:

/	forward slash
\	backslash
*	asterisk

,	comma
:	colon
;	semi-colon
=	equal sign
+	plus sign
?	question mark
|	vertical bar
<	left angle bracket
>	right angle bracket
&	ampersand (and sign)
%	percent sign
'	single quotation mark
"	double quotation mark
]]>	No specific name exists for this character combination.
.	period (not valid if first character; valid if a later character)
#	Hash mark
$	Dollar sign
~	Tilde
(	Left parenthesis
)	Right parenthesis

- Select a new location when you respond to a request for a location to install WebSphere Application Server.

  If WebSphere Application Server is already installed on the system, ***do not*** use an existing Key Lifecycle Manager profile.

WebSphere Application Server Directory Name
Specifies the directory where you want to install WebSphere Application Server. Do not use spaces in the directory path.

User ID
Specifies the WebSphere Application Server login user ID for the Key Lifecycle Manager Administrator profile.

Password
Specifies the WebSphere Application Server password for the Key Lifecycle Manager profile.

Port Number
Specifies the WebSphere Application Server port for the Key Lifecycle Manager profile. Do not use a port value greater than 65520.

Migration of Encryption Key Manager configuration

Installation provides the only opportunity to migrate an existing Encryption Key Manager configuration to IBM Security Key Lifecycle Manager.

Before you begin, obtain the password to log in to the Encryption Key Manager server.

To migrate an existing configuration, select this option:

Migrate Encryption Key Manager
Check this box if you have an old Encryption Key Manager properties file to migrate to IBM Security Key Lifecycle Manager. If you select the check box, you must specify the properties file from the previous Encryption Key Manager system.

You can migrate from Version 2.1 of Encryption Key Manager.

Encryption Key Manager must not be active when you are doing the migration. To stop a running Encryption Key Manager process, complete these steps:

1. Start an administrative session. At Version 2.1, enter this command:

   ```
   java com.ibm.keymanager.KMSAdminCmd KeyManagerConfig.properties -i
   ```

2. After the administrative session starts, complete these steps:

   a. Authenticate to the Encryption Key Manager server by using the login command. Type:

      ```
      login -ekmuser EKMAdmin -password password
      ```

   b. Stop the server. Type:

      ```
      stopekm
      ```

3. Exit the session.

For restrictions on migration, see “Migration planning” on page 23.

Installing IBM Security Key Lifecycle Manager on Linux systems as a non-root user

You can install IBM Security Key Lifecycle Manager as a non-root user on Linux operating system. Non-root installation of IBM Security Key Lifecycle Manager installs both DB2 and WebSphere Application Server as a non-root user.

About this task

Note:

- If you install IBM Security Key Lifecycle Manager as a non-root user, you cannot migrate IBM Security Key Lifecycle Manager earlier version 1.0, 2.0, 2.0.1 and Encryption Key Manager to version 2.5.
- You cannot install IBM Security Key Lifecycle Manager as a non-root user in silent mode.

Procedure

1. Ensure that your target environment meets IBM Security Key Lifecycle Manager installation prerequisites. See “Planning the installation” on page 7.
2. Create a non-root User ID. Ensure that the User ID must have a primary group other than `guests`, `admins`, `users`, and `local`.
3. Run **launchpad.sh**.
4. Specify DB2 configuration parameters. See “DB2 configuration during non-root installation” on page 58.
5. Specify WebSphere Application Server configuration parameters.
6. Open `/home/username/sklmV25properties/scripts` and run the following command.

   Non-root DB2 installation requires root access to configure DB2 instance with a specific port number and service name.

   ```
   sudo nonrootconfig.sh <instance_home> <user_name> <port_number>
   ```

What to do next

In the *SKLM_HOME*`/config/SKLMConfig.properties` file, update the SSL port number higher than 1024. For example:

```
TransportListener.ssl.port property =4411
```

After the installation, you must log in as a non-root user to start or stop the IBM Security Key Lifecycle Manager sever and the DB2 server.

DB2 configuration during non-root installation

IBM Security Key Lifecycle Manager requires DB2 Workgroup Server Edition at a Version 10.1 level that depends on the operating system.

During DB2 configuration, you are prompted for the following information:

DB2 Administrator ID
The local DB2 administrator user ID. Because non-root DB2 user can have a single instance, the DB2 administrator ID must be same as the User ID who is logged on the system.

User IDs have the following restrictions and requirements:

- Must have a primary group other than `guests`, `admins`, `users`, and `local`.
- Can include lowercase letters (a-z), numbers (0-9), and the underscore character (_).
- Cannot be longer than eight characters.
- Cannot begin with IBM, SYS, SQL, or a number
- Cannot be a DB2 reserved word (USERS, ADMINS, GUESTS, PUBLIC, or LOCAL), or an SQL reserved word
- Cannot use any User IDs with root privilege for the DB2 instance ID, DAS ID or fenced ID.
- Cannot include accented characters.

DB2 Administrator Password
The password for the administrator. The maximum length is 20 characters.

The password for the DB2 Administrator user ID is subject to the security policy active on the system. In addition, the login password for the DB2 Administrator user ID and the DB2 password for the user ID must be the same. When you change one, you must change the other.

Database Name
The name of the IBM Security Key Lifecycle Manager database, which is `sklmdb`.

DB2 Port
The port that DB2 uses.

Administrator's Group
Access group in which the Administrator user ID exists. User ID must not be in the `bin` or `root` group.

Administrator / Database Home
The directory in which the database instance and the formatted tables that are used by IBM Security Key Lifecycle Manager are created.

Notes:

1. Entries for all fields are restricted to alphabetical characters (A-Z and a-z), numeric characters (0-9), and the underscore character (_). The restriction also applies to the values in the response file that is used for silent installations.
2. Do not specify spaces in any of the directory paths or file names.
3. The name of the computer on which you install DB2 cannot start with “ibm”, “sql”, or “sys” in lowercase or uppercase. The name of the computer also cannot contain the underscore character (_).

For more information about how to modify kernel parameters and non-root installation, see DB2 documentation.

- http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
- http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0050571.html

Resetting password on distributed systems

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

About this task

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

Procedure

1. Log in with the WASAdmin user ID.
2. Back up the `WAS_HOME/profiles/KLMProfile/config/cells/SKLMCell/fileRegistry.xml` file. Changing the value of the password changes this registry file.
3. Change the password.
   - Windows systems
     a. Start a **wsadmin** session by using the Jython syntax. For example, type:
     ```
     WAS_HOME/bin/wsadmin -conntype none -profileName KLMProfile -lang jython
     ```
     b. Reset the password for the SKLMAdmin user ID:
     ```
     wsadmin>print AdminTask.changeFileRegistryAccountPassword
      ('-userId SKLMAdmin -password newpassword')
     ```

     Note:
     - Only the WASAdmin user ID or another user ID with WebSphere Application Server administrator authority can change passwords by using the **AdminTask.changeFileRegistryAccountPassword** command.
     - Passwords that you create by using the **AdminTask.changeFileRegistryAccountPassword** command are not validated against the configured password policy that IBM Security Key Lifecycle Manager provides.

       After a lost password reset, the user must set the password by using the graphical user interface.

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

Note:

- Only the WASAdmin user ID or another user ID with IBM Security Key Lifecycle Manager administrator authority can change passwords by using the **AdminTask.changeFileRegistryAccountPassword** command.
- Passwords that you create by using the **AdminTask.changeFileRegistryAccountPassword** command are not validated against the configured password policy that IBM Security Key Lifecycle Manager provides.

  After a lost password reset, the user must set the password by using the graphical user interface.

c. Save the change and exit:

```
wsadmin>print AdminConfig.save()
wsadmin>exit
```

4. Stop and start the server.
   - Stop

     On Windows systems:
     ```
     stopServer.bat server1
     ```

     On systems such as Linux or AIX:
     ```
     ./stopServer.sh server1
     ```
   - Start

     On Windows systems:
     ```
     startServer.bat server1
     ```

     On systems such as Linux or AIX:
     ```
     ./startServer.sh server1
     ```
5. Verify that you can log in as the specified administrator with the new password.

Uninstallation on distributed systems

On distributed systems, uninstalling IBM Security Key Lifecycle Manager has these considerations:

- The default uninstallation mode is the same as the mode used to install IBM Security Key Lifecycle Manager. You can also uninstall by using a different mode. For more information, see “Syntax and parameters for the uninstallation program.”
- Uninstalling IBM Security Key Lifecycle Manager does not uninstall DB2 if it is installed before you install IBM Security Key Lifecycle Manager. This task a separate, optional step. For information, see “DB2 uninstallation” on page 67.

  In addition, although uninstalling IBM Security Key Lifecycle Manager disassociates the DB2 database instance from the user ID used for the IBM Security Key Lifecycle Manager DB2 instance owner, the deletion of the user ID is a separate step. For information, see “Removal of user ID from the DB2 instance owner” on page 69.

  Unsuccessful uninstallation might indicate the need to return to a known state of IBM Security Key Lifecycle Manager, version 2.0.1. For more information, see “Reinstalling previous version if migration repeatedly fails” on page 65.

Syntax and parameters for the uninstallation program

You must use the uninstallation commands to uninstall IBM Security Key Lifecycle Manager.

Silent unstallation

```
imcl -input full_path_to_response_file -silent
```

-input Specifies the full path and file name for the response file with the uninstallation options to use during the silent uninstallation.

-silent
Specifies that the IBM Installation Manager installer must run in silent mode.

Graphical mode unstallation

```
uninstall_program
```

Where *uninstall_program* is:

***<IM_INSTALL_DIR>*/IBMIM.exe** on Windows systems.

***<IM_INSTALL_DIR>*\IBMIM** on systems such as Linux or AIX.

Uninstalling on Windows systems

Use IBM Installation Manager to uninstall IBM Security Key Lifecycle Manager, DB2, and the WebSphere Application Server.

Before you begin

Stop WebSphere Application Server before you uninstall IBM Security Key Lifecycle Manager. If WebSphere Application Server is not stopped before you uninstall IBM Security Key Lifecycle Manager, the following false message is displayed after Step 4:

```
Running processes have been detected that may interfere with the current
operation. Stop all WebSphere and related processes before continue.
```

Click **Recheck Status** to proceed with the uninstallation task.

Procedure

1. Browse to <*IM_INSTALL_DIR*> and double-click **IBMIM** to start IBM Installation Manager in GUI mode.
2. In IBM Installation Manager, click **Uninstall**. The Uninstall Packages window opens.
3. Select the check boxes to uninstall IBM Security Key Lifecycle Manager, DB2, and the WebSphere Application Server.
4. Click **Next**. Type the WebSphere Application Server Administrator user ID and the password.
5. Click **Next**. The Summary panel window opens.
6. Review the software packages to be uninstalled and their installation directories; click **Uninstall**.

What to do next

Note: After you uninstall IBM Security Key Lifecycle Manager, delete the `C:\Program Files (x86)\IBM\WebSphere` and `C:\Program Files (x86)\DB2SKLMV25` directories if not already removed.

Recovering from a failed uninstallation on Windows systems

You must recover a failed attempt to uninstall IBM Security Key Lifecycle Manager on a Windows system.

About this task

This task assumes that the uninstallation program failed to complete successfully. Take these recovery steps:

Procedure

1. Stop the WebSphere Application Server service.
   a. Open the Windows Services Console by opening the Control Panel and clicking **Administrative Tools** > **Services**.
   b. Locate the WebSphere Application Server service.

      For example: `IBM WebSphere Application Server V8.5 - SKLMServer`
   c. Open the **Properties** dialog box for the service. If the **Service status** is not `Stopped`, click **Stop**.
   d. Click **OK** to close the dialog box and exit the Windows Services Console.

   If you cannot stop the service from inside the Windows Service Console, open a command prompt window and enter these commands to stop the service manually:

   ```
   cd WAS_HOME\bin
   WASService -stop SKLMServer
   ```
2. Remove the WebSphere Application Server service, if it is not already removed. Open a command prompt window and enter these commands:

   ```
   cd WAS_HOME\bin
   WASService -remove SKLMServer
   ```

3. Uninstall WebSphere Application Server, if exists and other products are not using it.

   For uninstallation instructions, see the following links:

   Graphical user interface

   http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_gui.html

   Command-line interface

   http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_cl.html

   If the `*WAS_HOME*` or `*WAS_HOME*\bin` directories are already removed, skip Steps 1, 2, and 3.
4. Uninstall DB2, if exists and other products are not using it.

   For uninstallation instructions, see "Optional removal of DB2" on page 67.
5. Open the `C:\ProgramData\IBM\Installation Manager\installRegistry.xml` file in a text editor.

   Note: Back up the `installRegistry.xml` file.
6. Remove the entries that are relating *only* to IBM Security Key Lifecycle Manager. For example:

   ```
   <profile id='IBM Security Key Lifecycle Manager v2.5' kind='product'>
     ....
   </profile>
   ```
7. Remove the installation log files in this directory:

   `\<*IM App Data Dir*>\logs`
8. Remove **Control Panel** > **Add or remove programs** > **IBM Installation Manger**.
9. Remove the following folders, if exists:
   - `C:\Program Files (x86)\IBM\DB2SKLMV25`
   - `C:\Program Files (x86)\IBM\WebSphere`
   - `C:\Program Files (x86)\IBM\SKLMV25`
   - `C:\Program Files (x86)\IBM\Installation Manager`
   - `C:\Program Files (x86)\IBM\IBMIMShared`
10. Restart the computer.

Uninstalling on systems such as Linux and AIX

You must stop WebSphere Application Server before you uninstall IBM Security Key Lifecycle Manager.

Before you begin

To uninstall IBM Security Key Lifecycle Manager on a system such as Linux or AIX, take these steps.

Procedure

1. Browse to <*IM_INSTALL_DIR*> and run **IBMIM**.
2. In IBM Installation Manager, click **Uninstall**. The Uninstall Packages window opens.

3. Select the check boxes to uninstall IBM Security Key Lifecycle Manager, DB2, and the WebSphere Application Server.
4. Click **Next**. Type the WebSphere Application Server Administrator user ID and the password.
5. Click **Next**. The summary panel opens.
6. Review the software packages to be uninstalled and their installation directories.
7. Click **Uninstall**.

Recovering from a failed uninstallation on systems such as Linux and AIX

You might want to recover a failed attempt to uninstall IBM Security Key Lifecycle Manager on a system such as Linux or AIX.

About this task

This task assumes that the uninstallation program failed to complete successfully. Take these recovery steps:

Procedure

1. Log in as root.
2. Stop the WebSphere Application Server processes if they are running.
   ```
   cd WAS_HOME/profiles/KLMProfile/bin
   ./stopServer.sh server1
   ```
3. Uninstall WebSphere Application Server, if exists and other products are not using it.

   For uninstallation instructions, see the following links:

   Graphical user interface
      http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_gui.html

   Command-line interface
      http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_cl.html

   If the *WAS_HOME* or *WAS_HOME*/bin directories are already removed, skip Steps 2 and 3.
4. Uninstall DB2, if exists and other products are not using it.

   For uninstallation instructions, see "Optional removal of DB2" on page 67.
5. Open the /var/ibm/InstallationManager/installRegistry.xml file.

   Note: Back up the installRegistry.xml file.
6. Remove the entries that are relating **only** to IBM Security Key Lifecycle Manager. For example:
   ```
   <profile id='IBM Security Key Lifecycle Manager v2.5' kind='product'>
     ....
   </profile>
   ```
7. Remove the installation log files from the /var/ibm/InstallationManager/logs directory by using the following command:
   ```
   rm -rf /var/ibm/InstallationManager/logs
   ```

8. Uninstall IBM Installation Manger.
9. Remove the following folders, if exist:
   - `opt/IBM/DB2SKLMV25`
   - `opt/IBM/WebSphere`
   - `opt/IBM/SKLMV25`
   - `opt/IBM/Installation Manager`
   - `opt/IBM/IBMIMShared`
10. Restart the computer.

Reinstalling previous version if migration repeatedly fails

Migration process does not affect the earlier version of IBM Security Key Lifecycle Manager. If the migration continues to fail, uninstall IBM Security Key Lifecycle Manager version 2.5 and continue to run the pervious version.

Note: On Windows platform, after you migrate IBM Security Key Lifecycle Manager earlier version (1.0, 2.0, or 2.0.1) to version 2.5, DB2 associated with the earlier version might not start if you uninstall IBM Security Key Lifecycle Manager version 2.5 before uninstalling the earlier version.

You can uninstall IBM Security Key Lifecycle Manager, version 2.5 by following the steps in “Uninstallation on distributed systems” on page 61.

Optional removal of DB2

After you uninstall IBM Security Key Lifecycle Manager, you have the option of leaving DB2 installed or uninstalling the program.

Uninstalling IBM Security Key Lifecycle Manager does not uninstall DB2 if it is installed before you install IBM Security Key Lifecycle Manager. DB2 is uninstalled when you uninstall IBM Security Key Lifecycle Manager if it is installed by the IBM Security Key Lifecycle Manager installer. You might also ensure that related automatic startup services are disabled.

DB2 uninstallation

After uninstalling IBM Security Key Lifecycle Manager, you have the option of leaving DB2 installed or uninstalling the program.

If you choose to leave DB2 installed, you have the option of keeping or removing the IBM Security Key Lifecycle Manager DB2 instance owner. Unless you have a specific reason for keeping the instance owner, such as keeping a connection to a database, disassociate the user ID from the DB2 database instance. For more information, see "Disassociation of a user ID from the DB2 instance" on page 68.

If you choose to uninstall DB2, follow these steps:

Windows systems:

Open the Control Panel.

Windows Server 2008: Click **Programs and Features**. Locate the entry for DB2, and click **Remove** to uninstall it.

Note: After uninstalling DB2, extra steps might be required to finish removing DB2 artifacts.

1. To delete the user ID that was used for the IBM Security Key Lifecycle Manager DB2 instance owner, open the Control Panel and click **Administrative tools > Computer Management > Local Users and Groups > Users**.

   Review the list of user IDs. If the user ID for the IBM Security Key Lifecycle Manager DB2 instance owner still exists, delete it.

   Close the Computer Management console.
2. Review the entries and verify that the entries for the DB2 ports are removed from the `C:\WINDOWS\system32\drivers\etc\services` file. Edit the file and search for the port numbers that are used by DB2. If any are found, remove the entries from the file.
3. Open the Control Panel and click **Administrative Tools > Computer Management > Services**. Review the list of services and verify that the DB2 related service entries are removed. Close the Services console when you are finished.
4. Remove the DB2 installation directory if the directory is not already removed.

For more information on uninstalling DB2 on Windows systems, see DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0007436.html).

AIX and Linux systems:

1. Log in as the root user.
2. Remove the user ID of the IBM Security Key Lifecycle Manager DB2 instance owner:
   a. Change to the user ID of the IBM Security Key Lifecycle Manager DB2 instance owner, run the **db2istop** command for the instance owner user ID and exit back to the root user ID:
      ```
      su - sklm_instance_owner_userid

      cd DB_HOME/instance
      ./db2istop sklm_instance_owner_userid /home/sklm_instance_owner_userid

      exit
      ```
   b. Run the **db2idrop** command on the instance owner user ID:
      ```
      cd DB_HOME/instance
      ./db2idrop sklm_instance_owner_userid
      ```
   c. Remove the user ID from the system:
      ```
      userdel -r sklm_instance_owner_userid
      ```
3. Remove DB2 from the system:
   ```
   cd DB_HOME/install/
   ./db2_deinstall -a
   ```
4. Edit the services file:
   ```
   vi /etc/services
   ```

   Locate the port numbers that are used by DB2, and remove the entries from the file.
5. Remove the DB2 installation directory if it is not removed.

For more information on uninstalling DB2 on systems such as Linux and AIX, see DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0007439.html).

The following example shows the steps that are involved, by using the default DB2 instance owner user ID, sklmdb2, and the default DB2 directory, /opt/IBM/DB2SKLMV25.

Starting as root, type:

```
su - sklmdb2
cd /opt/IBM/DB2SKLMV25/instance
./db2istop sklmdb2/home/sklmdb2
exit
# Exit back to root.
cd /opt/IBM/DB2SKLMV25/instance
./db2idrop sklmdb2
userdel -r sklmdb2
cd /opt/IBM/DB2SKLMV25/install
./db2_deinstall -a
vi /etc/services
# Locate and remove the DB2 port entries in the services file.
rm -rf /opt/IBM/DB2SKLMV25
```

Disassociation of a user ID from the DB2 instance

You can disassociate a user ID from the IBM Security Key Lifecycle Manager DB2 instance.

If the user ID is already disassociated from the DB2 instance, a step might return a message that the user was not found. If you get this message, continue with the next step.

- **Windows systems:**
  1. Open the Windows Services console, and stop the DB2 service for the IBM Security Key Lifecycle Manager instance owner.

     To locate the DB2 instance service, search the list of services for services whose names begin with "DB2." The entry for the instance service contains the user ID of the IBM Security Key Lifecycle Manager DB2 instance owner as part of the service name. For example, **DB2 - DBSKLMV25 - SKLMDB2**.

     Open the properties dialog for the service and set the **Service status** to `Stopped`, and the **Startup type** to `Manual`.
  2. Click **Start > Programs > IBM DB2 >** ***instance_owner*** **> Command Line Tools > Command Window** to open the DB2 Command Window, and enter:
     ```
     db2idrop db databasename
     db2idrop sklm_instance_owner_userid
     ```
  3. If the C:\sklm_instance_owner_user_id directory still exists, remove it:
     ```
     del /s /q  C:\sklm_instance_owner_user_id
     ```
- **AIX and Linux systems:**

  Log in as the root user, and follow these steps.
  1. Change to the user ID of the IBM Security Key Lifecycle Manager DB2 instance owner, run the **db2istop** command for the instance owner user ID and exit back to the root user ID:
     ```
     su - sklm_instance_owner_userid

     cd DB_HOME/instance
     ./db2istop sklm_instance_owner_userid /home/sklm_instance_owner_userid

     exit
     ```
  2. Run the **db2idrop** command on the instance owner user ID:
     ```
     cd DB_HOME/instance
     ./db2idrop sklm_instance_owner_userid
     ```
  3. If the *`sklm_instance_owner_user_id`*`/sqllib` directory still exists, remove it:
     ```
     rm -rf sklm_instance_owner_user_id/sqllib
     ```

Removal of user ID from the DB2 instance owner

To remove the user ID that was used as the IBM Security Key Lifecycle Manager DB2 instance owner, use the user management utilities of the operating system to delete the user ID.

Before you delete a user ID that is used as the instance owner for the IBM Security Key Lifecycle Manager databases, ensure that the user ID is no longer associated with the DB2 instance.

Follow the steps in “Disassociation of a user ID from the DB2 instance” on page 68. If the user ID is already disassociated from the DB2 instance, a step might return a message that the user was not found. If this message, continue with the next step.

After verifying that the user ID is not associated with the DB2 database instance, follow these steps to remove the user ID from the system:

- **Windows systems:**

Use the user management tool for the version of Windows you are running to delete the DB2 administrative user from the system. For example, on some versions of Windows, carry out these steps:

1. Open the Control Panel.
2. Click **Administrative tools > Computer Management > Local Users and Groups > Users**.
3. Delete the user from the system.

- **AIX and Linux systems:**

  Log in as the root user, and enter this command to remove the user ID:

  ```
  userdel -r sklm_instance_owner_userid
  ```

Disablement of automatic services

The IBM Security Key Lifecycle Manager uninstall process disables the DB2 and WebSphere Application Server services that are associated with IBM Security Key Lifecycle Manager. To correct error conditions, you might also want to ensure that these services are disabled.

Windows systems

On Windows systems, use the Windows Services console to prevent the DB2 and WebSphere Application Server services that are associated with IBM Security Key Lifecycle Manager from starting automatically.

Open the Windows Services console and locate the services in the following list. For each service in the list, open the Properties dialog box for the service, and ensure that the **Startup Type** is set to `Disabled`, and the **Service status** field is set to `Stopped`.

DB2 - *db2 copy name - SKLM_INSTANCE_OWNER*
For example, **DB2 - DBSKLMV25 - SKLMDB2**

DB2 Governor (*db2 copy name***)**
For example, **DB2 Governor (DBSKLMV25)**

DB2 License Server (*db2 copy name***)**
For example, **DB2 License Server (DBSKLMV25)**

DB2 Management Service (*db2 copy name***)**
For example, **DB2 Management Service (DBSKLMV25)**

DB2 Remote Command Server (*db2 copy name***)**
For example, **DB2 Remote Command Server (DBSKLMV25)**

DB2DAS - *DB2DAS_entry*
For example, **DB2DAS - DB2DAS00**

Note: Disable DB2 Administration Server (DAS) only if DAS service is hosted in Windows service.

AIX and Linux systems

On AIX or Linux systems, enter the following commands to configure the IBM Security Key Lifecycle Manager DB2 instance owner so that it does not start automatically:

```
. ~sklmdb2/sqllib/db2profile
DB_HOME/instance/db2iauto -off sklmdb2
```

Where sklmdb2 is the default instance owner user ID. If you changed it during installation, use that user ID instead.

Next, edit the /etc/inittab file and remove the entry that autostarts the WebSphere Application Server server:

```
/opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
```

Recovery from migration failure

You can take migration recovery steps for failure to migrate either Encryption Key Manager or IBM Security Key Lifecycle Manager.

Recovery from migration failure for Encryption Key Manager

Errors might occur during migration for Encryption Key Manager.

The installation process completes the installation step for IBM Security Key Lifecycle Manager and starts a migration process to migrate data from Encryption Key Manager to IBM Security Key Lifecycle Manager.

- As migration starts, an error might occur when the installation program is validating the values in the Encryption Key Manager properties file for the following conditions:
  - The properties file cannot be read because of inadequate access permissions.
  - A required property does not exist or does not have a value.
  - The value of a property is malformed.
  - The file that a property points to does not exist or cannot be read because of inadequate access permissions.
- An error might occur after the migration operation completes significant activities. In this case, review the error log file:

  Windows systems:

  ```
  <IM App Data Dir>\logs\sklmLogs\migration.log
  ```

  AIX and Linux systems:

  ```
  <IM App Data Dir>/logs/sklmLogs/migration.log
  ```

If Encryption Key Manager migration fails and you choose to complete the remaining migration process, you can start a migration-recovery script if you do not make changes or otherwise configure IBM Security Key Lifecycle Manager server before you run the script.

If Encryption Key Manager migration fails, and no data was migrated, remove the `tklmKeystore.jceks` file to start the migration process again. You can locate the file in the `WAS_HOME\products\sklm\keystore` directory.

Migration recovery script for Encryption Key Manager

You can start a migration-recovery script for Encryption Key Manager if you do not make any changes or otherwise configure IBM Security Key Lifecycle Manager server before you run the script. For example, do not significantly change the available disk space on the system.

The migration script is in the *SKLM_HOME*`\migration\bin` directory. The commands to run the script are:

Windows systems:

```
cd SKLM_HOME\migration\bin
.\migrate.bat sklm_instance_owner_password
```

Linux and AIX systems:

```
cd SKLM_HOME/migration/bin
./migrate.sh sklm_instance_owner_password
```

On systems such as Linux or AIX, ensure that you are logged in as the root user before you run `migrate.sh`.

Where the *sklm_instance_owner_password* parameter is the password for the IBM Security Key Lifecycle Manager server DB2 instance owner.

The *SKLM_HOME* parameter is only used on Windows systems and must be enclosed in quotation marks.

Windows systems:

```
cd "C:\Program File\IBM\SKLMV25\migration\bin"

.\bin\migrate.bat password
echo %ERRORLEVEL%
```

Note:

- If you do not want to specify the password as an argument, omit the password. The recovery script prompts you for the value. The password is not in clear text. For example:

  ```
  migrate.bat
  echo $?
  ```

- During its runtime progress, the migration recovery script creates a `migration.log` file.
- If `migrate.bat` or `migrate.sh` is not available,
  1. Copy `migrate.bat.template` or `migrate.sh.template` to `migrate.bat` or `migrate.sh`.
  2. Specify the required parameters.
  3. Run the file.

Linux and AIX systems:

```
cd /opt/IBM/SKLMV25/migration/bin
./bin/migrate.sh password
echo $?
```

On systems such as Linux or AIX, ensure that you are logged in as the root user before you run `migrate.sh`.

Recovery from migration failure for IBM Security Key Lifecycle Manager

These error scenarios might occur during migration for IBM Security Key Lifecycle Manager:

- As migration starts, an error message might be caused by one or more of the following conditions:
  - Inadequate access permissions prevent reading required files, or properties or files are missing.
  - Other applications are using a required file.
  - During DB2 server migration, WebSphere Application Server unexpectedly stopped running.
- After migration is complete, or has performed significant activities, An error might occur after the migration operation has begun.

The installation program displays an error message. In this case, review the error log file:

Windows systems:

```
<IM App Data Dir>\logs\sklmLogs\migration.log
```

AIX and Linux systems:

```
<IM App Data Dir>/logs/sklmLogs/migration.log
```

If repeated running of the migration program fails and you choose to go back to earlier version, complete these tasks for a new version of DB2:

– Uninstall IBM Security Key Lifecycle Manager earlier version. On systems such as AIX or Linux, navigate to the home directory of the instance owner such as `/home/sklmdb2`. If the `sqllib_v91` directory exists, remove the directory.

– Restart the computer.

– Reinstall IBM Security Key Lifecycle Manager previous version and restore the most recent backup. Apply the most recent fix pack.

Migration recovery script for IBM Security Key Lifecycle Manager

You can start a migration-recovery script for IBM Security Key Lifecycle Manager if you do not make any changes or otherwise configure IBM Security Key Lifecycle Manager server before you run the script. For example, do not significantly change the available disk space on the system.

The migration utility creates a `migration.log` file in the *<IM App Data Dir>\logs\sklmLogs* directory.

The migration script is in the *SKLM_HOME*`\migration` directory. Before you run the migration script ensure that `JAVA_HOME` is set correctly. Following example shows the path for `JAVA_HOME`:

Windows systems

```
C:\Program Files (x86)\IBM\WebSphere\AppServer\java\jre
```

Linux and AIX systems

```
/opt/IBM/WebSphere/AppServer/java/jre
```

The commands to run the migration script are:

Windows systems

```
cd SKLM_HOME\migration
.\migrateToSKLM.bat
```

Note: You must specify value for the migration parameters in the `migration.properties` file, which exists under the *SKLM_HOME*`\migration` directory.

For example:

```
cd "C:\Program Files (x86)\IBM\SKLMv25\migration"
.\migrateToSKLM.bat
```

Linux and AIX systems

```
cd SKLM_HOME/migration
./migrateToSKLM.sh
```

Note: You must specify value for the migration parameters in the `migration.properties` file, which exists under the *SKLM_HOME*`/migration` directory.

For example:

```
cd /opt/IBM/SKLMV25/migration
./migrateToSKLM.sh
```

On systems such as Linux or AIX, ensure that you are logged in as the root user before you run **`migrateToSKLM.sh`**.

Note: After you run the migration recovery script, restart WebSphere Application Server manually.

Parameters in the migration.properties file

WAS_HOME
The directory where WebSphere Application Server for IBM Security Key Lifecycle Manager, version 2.5 is installed.

TKLM_TIP_HOME
The directory where Tivoli Integrated Portal for IBM Security Key Lifecycle Manager, earlier version 1.0, 2.0, or 2.0.1 is installed.

WAS_ADMIN_ID
The Tivoli Integrated Portal administrator user name for the earlier version.

WAS_ADMIN_PASSWORD
Password for the Tivoli Integrated Portal administrator user name.

SKLM_INSTALL_PATH
The directory where IBM Security Key Lifecycle Manager is installed.

SKLM_ADMIN_USER
Administrator user name, for the earlier version of IBM Security Key Lifecycle Manager. The user name must be `TKLMAdmin`.

MIG_LOG_PATH
The file path where the `migration.log` is stored.

TKLM_VERSION
The earlier version number IBM Security Key Lifecycle Manager that is installed on the system.

TKLM_DB_PWD
The DB2 administrator password for the earlier version of IBM Security Key Lifecycle Manager.

KEYSTORE_PWD
The key store password for the earlier version of IBM Security Key Lifecycle Manager.

IM_INSTALL_DIR
The directory where IBM Installation Manager is installed.

Note: All the values except passwords are pre-filled in the properties file. Do not modify any values except for the fields that are blank.

Automatic start enablement for DB2

If you completed a failed migration by running the migration script in recovery mode, you must enable DB2 to start automatically when the computer restarts.

Windows systems

On Windows systems, take these steps to start DB2 automatically:

1. Open the Control Panel and click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click the **DB2 - DB2SKMV3 - SKLMDB2** service and right-click **Properties**.
3. On the Properties dialog, on the **General** tab, change the **Startup Type** to **Automatic** and click **Apply**.
4. Restart the system to verify that the database server starts automatically.

AIX and Linux systems

If you enabled crontab in IBM Security Key Lifecycle Manager Version 1, type this command to enable DB2 to start automatically:

```
. <DB_home_dir>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb2
```

Where `sklmdb2` is the default instance owner user ID. If you changed the value during installation, use that user ID instead.

Solaris systems

On Solaris systems, enter the following commands to configure the IBM Security Key Lifecycle Manager DB2 instance owner to start automatically:

```
. <DB_home_dir>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb2
```

Where `sklmdb2` is the default instance owner user ID. If you changed it during installation, use that user ID instead.

Migration properties file

The IBM Security Key Lifecycle Manager server migration utility maintains a *SKLM_HOME*/`migration/migratestatus.properties` file to track completed tasks.

If migration fails, the properties file is retained for debugging purposes. The migration utility also uses the retained file to determine at what point to start a new migration process. If you accidentally run migration again, the utility uses the properties file to determine whether migration already succeeded.

Post-installation steps

After you install IBM Security Key Lifecycle Manager, ensure that the DB2 and WebSphere Application Server services are correctly configured.

On a system that is Internet Protocol version 6 (IPv6) only, the Universal Resource Locator that is displayed at the end of installation is an IPv4 URL. Change the URL to your known IPv6 URL before you access IBM Security Key Lifecycle Manager.

Services, ports, and processes

After you install IBM Security Key Lifecycle Manager server, validate that required services, ports, and processes are running.

Windows systems:

- Services
  - WebSphere Application Server: IBMWAS85Service - SKLMServer
  - DB2: DBSKLMV25 - SKLMDB2
- Ports

  Note: All the following ports must be open and not used by any other processes.
  - HTTPS port to access IBM Security Key Lifecycle Manager graphical user interface and REST services: **9080**
  - HTTPS port to access WebSphere Integrated Solutions Console: **9083**
  - DB2: **50010** as the default.

    This is the default for DB2. You can configure this port at the time of IBM Security Key Lifecycle Manager installation. This value might be another port number, depending on the installation settings. There are other ports, which are associated with the default port number.
  - Default installation time SSL port that listens for KMIP messages: **5696**
  - SSL port for device messages: **441**
  - TCP port for device messages: **3801**
  - WebSphere Application Server: **9080 - 9099**

    WebSphere Application Server installation requires these ports for various services it provides.
  - User configured replication ports in the replication configuration file for master and clone servers. If a firewall is used between the master and clone servers, the firewall must be configured to pass Internet Control Message Protocol (ICMP).
- Processes
  - IBM Security Key Lifecycle Manager: `WASService.exe` `java.exe`
  - DB2: `db2fmp64.exe` `db2syscs.exe`

If version 2.5 is migrated from version 1.0, 2.0, or 2.0.1:

- Services
  - Tivoli Integrated Portal: TIPProfile_Port_16340

  - DB2: DB2TKLMV2 - TKLMDB2
- Ports
  - IBM Security Key Lifecycle Manager: 16340, 16341, 16342, 16343, 16345, 16346, 16350, 16352, 16353
  - DB2: The port number is the same as the DB2 port number at IBM Security Key Lifecycle Manager Version 1. There are other ports, which are associated with the default port number.
- Processes
  - IBM Security Key Lifecycle Manager: `WASService.exe` `java.exe`
  - DB2: `db2fmp.exe` `db2syscs.exe`

Systems such as AIX or Linux:

- Ports

  Note: All the following ports must be open and not used by any other processes.
  - HTTPS port to access IBM Security Key Lifecycle Manager graphical user interface and REST services: **9080**
  - HTTPS port to access WebSphere Integrated Solutions Console: **9083**
  - DB2: **50010** as the default.

    This is the default for DB2. You can configure this port at the time of IBM Security Key Lifecycle Manager installation. This value might be another port number, depending on the installation settings. There are other ports, which are associated with the default port number.
  - Default installation time SSL port that listens for KMIP messages: **5696**
  - SSL port for device messages: **441**
  - TCP port for device messages: **3801**
  - WebSphere Application Server: **9080 - 9099**

    WebSphere Application Server installation requires these ports for various services it provides.
  - User configured replication ports in the replication configuration file for master and clone servers. If a firewall is used between the master and clone servers, the firewall must be configured to pass Internet Control Message Protocol (ICMP).
- Processes
  - IBM Security Key Lifecycle Manager: WebSphere Application Server and Java
  - DB2: `db2fmp64` `db2syscs`

Post-installation security

After you install IBM Security Key Lifecycle Manager, you must take several steps to ensure certificate recognition by your browser, and protect sensitive user IDs and passwords.

Specifying a certificate for browser access

All browsers trigger a certificate error that you must overwrite to gain access to WebSphere Application Server.

About this task

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. You can use the WebSphere Application Server user interface to overwrite the certificate.

To configure the certificate, follow these steps:

Procedure

1. Using the WASAdmin user ID, log in to the IBM Security Key Lifecycle Manager server.
2. On the Security tab, click **SSL certificate and key management**.
3. On the SSL certificate and key management page, click **Manage endpoint security configuration -> server1**. In the local topology tree, you might need to click **SKLMCell > nodes > SKLMNode > servers > server1** to expand the tree and locate server1 in the outbound branch.
4. To set the specific SSL configuration for this endpoint, click **Manage Certificates**.
5. *Extract* the certificate.

   The browser needs only the certificate. Extract retrieves the certificate (the public key) and stores it into a file. Do not export the certificate, which obtains both the public and the private key.
6. Import the certificate into your browser.
   - Firefox
     a. Click **Tools > Options > Advanced > Encryption**.
     b. Select **View Certificates > Import** buttons.
     c. Navigate to the directory from which the certificate is exported. Select the certificate and click **Open**.
     d. On the Certificate Manager dialog, select the imported certificate and click **Edit**.
     e. On the Edit website certificate trust settings dialog, select **Trust the authenticity of this certificate** and click **OK**.
     f. On the Certificate Manager dialog, click **OK**.
     g. On the Options dialog, click **OK**.
   - Internet Explorer
     a. Click **Tools > Internet Options**.
     b. Select the **Content** tab and click the **Certificates** button.
     c. Select the **Trusted Root Certification Authorities** tab and click the **Import** button.
     d. On the Certificate Import Wizard dialog, click **Next**.
     e. Browse to locate the certificate and click **Next**.
     f. Type the password for the certificate and click **Next**.
     g. Complete the remaining steps that the wizard provides.
     h. On the Security Warning dialog, read the warning. If you agree, click **Yes**.
7. On the browser address field, enter the fully qualified Universal Resource Locator to point to the IBM Security Key Lifecycle Manager server. Press **Enter**.

Changing the WebSphere Application Server keystore password

SSL certificates for the browser are stored in WebSphere Application Server keystores. On WebSphere Application Server, these keystore passwords are public and must be changed.

About this task

When you install the application server, each server creates a keystore and truststore for the default SSL configuration with the default password value of `WebAS`.

Procedure

1. Change the password by using the graphical user interface:
   a. Using the WASAdmin user ID, log in to the WebSphere Integrated Solutions Console.
      ```
      https://localhost:9083/ibm/console/logon.jsp
      ```
   b. On the Security tab, click **SSL certificate and key management**.
   c. On the SSL certificate and key management page, click **Key stores and certificates** > **NodeDefaultKeyStore**.
   d. Change the keystore password.
   e. On the SSL certificate and key management page, click **Key stores and certificates** > **NodeDefaultTrustStore**.
   f. Change the truststore password.
2. Save the password in a secure location.

WebSphere Application Server security

You must take several steps to ensure WebSphere Application Server security for sensitive information.

Support might determine that tracing is required to debug an issue in a function that the **WASService.exe** command runs. Turning on tracing for this function writes potentially sensitive trace information to the `WASService.Trace` file in the Windows root directory. Use information protection steps that are appropriate for your site to protect the `WASService.Trace` file.

Additionally, use caution when you run the **stopServer** command. Do not put the password directly on the command line. Instead, enter the user name and password for the WebSphere Application Server administrator when prompted.

For example, to stop all processes that are bound to *WAS_HOME*, type:

```
stopServer server1
```

Enter the user name and password at the prompts.

Avoid including the user ID and password in the command. For example, do not type:

On Windows systems:

```
stopServer.bat server1 -username wasadmin -password mypwd
```

On systems such as Linux or AIX:

```
./stopServer.sh server1  -username wasadmin -password mypwd
```

After the **ps -aef** command is run to display information about the active process, can potentially display the WebSphere Application Server password.

Installation errors during installation

Errors that you must correct can occur during installation. Many error messages contain enough information to correct the situation that caused the error. However, some error conditions require more information.

Silent installation might exit with no error message displayed, but errors do exist in the log file.

If silent installation exits with a zero return code, also check the log file for error messages.

Windows systems:

`\<IM App Data Dir>\logs`

Systems such as AIX or Linux:

`/<IM App Data Dir>/logs`

If you get an error message about a disk or file system not having enough disk space available:

Remove files to free up space, or add storage to the system to expand the size of the file system.

Do not correct the problem while the installation program is running. Exit the installation program before you make the corrections, and restart the program after the corrections are made.

See "Hardware requirements for distributed systems" on page 9 for information about disk space and other hardware requirements.

If you install IBM Security Key Lifecycle Manager using an Exceed X Server on a local machine while exporting the display from a Linux system to the local machine, do not decline the license agreement.

If you decline the license agreement, the installation program can be rendered unresponsive. Accept the license agreement, or use a Cygwin X Server or a Virtual Network Connection instead.

Removing the sklmdb2 administrator using Windows user and group management tool requires removing the previous sklmdb2 subdirectory before reinstalling IBM Security Key Lifecycle Manager and DB2.

During IBM Security Key Lifecycle Manager installation, you might encounter a problem if you used the Windows user and group management tool to previously delete the sklmdb2 user ID as the DB2 administrator. Reinstalling IBM Security Key Lifecycle Manager then fails to install DB2.

To fix the problem, take these steps:

1. Change to the appropriate subdirectory:
   - Windows Server 2003: *drive*:\Documents and Settings
   - Windows Server 2008: *drive*:\Users
2. Remove the sklmdb2 subdirectory.
3. Reinstall IBM Security Key Lifecycle Manager. The `sklmdb2` subdirectory is not automatically removed when you use the Windows user and group management tool to delete the user account `sklmdb2`.

Automatic services enablement

The IBM Security Key Lifecycle Manager installation process starts the DB2 and WebSphere Application Server services that IBM Security Key Lifecycle Manager requires. The installation process also sets the services to start automatically. However, you might want to correct error conditions with the automatic starting of services.

Windows systems

On Windows systems, use the Windows Services console to configure the services to start automatically.

Locate the services in the following list. For each service in the list, open the Properties dialog box for the service, and ensure that the **Startup Type** is set to `Automatic`. If the **Service status** field has a value of `Stopped`, click **Start** to start the service.

DB2 - *db2 copy name - SKLM_INSTANCE_OWNER*
For example, **DB2 - DBSKLMV25 - SKLMDB2**

DB2 Governor (*db2 copy name***)**
For example, **DB2 Governor (DBSKLMV25)**

DB2 License Server (*db2 copy name***)**
For example, **DB2 License Server (DBSKLMV25)**

DB2 Management Service (*db2 copy name***)**
For example, **DB2 Management Service (DBSKLMV25)**

DB2 Remote Command Server (*db2 copy name***)**
For example, **DB2 Remote Command Server (DBSKLMV25)**

DB2DAS - *DB2DAS_entry*
For example, **DB2DAS - DB2DAS00**

Note: Disable DB2 Administration Server (DAS) only if DAS service is hosted in Windows service.

WAS Service- IBM Security Key Lifecycle Manager
For example, **IBM WebSphere Application Server V8.5 - SKLMServer**

Linux systems

On Linux systems, enter the following commands to configure the IBM Security Key Lifecycle Manager DB2 instance owner to start automatically:

```
<DB_home_dir>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb2
```

Where `sklmdb2` is the default instance owner user ID. If you changed the value during installation, use that user ID instead.

Installing IBM Security Key Lifecycle Manager on Linux systems adds command to start the WebSphere Application Server to the `/etc/inittab` file. On Linux systems, the installer creates the `SecurityKeyLifecycleManager_was.init` file in `/etc/init.d`. You can add similar command into the `/etc/initttab` file:

```
slp:2345:wait:/bin/sleep 60
tt:23456789:wait:WAS_HOME/bin/startServer.sh server1
```

Solaris and AIX systems

On Solaris and AIX systems, enter the following commands to configure the IBM Security Key Lifecycle Manager DB2 instance owner to start automatically:

```
<DB_home_dir>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb2
```

Where sklmdb2 is the default instance owner user ID. If you changed it during installation, use that user ID instead.

Installing IBM Security Key Lifecycle Manager on Solaris and AIX systems adds commands to start the WebSphere Application Server to the /etc/inittab file. You might edit these commands in the /etc/inittab file:

```
sl:2345:wait:/bin/sleep 60
tt:23456:wait:WAS_HOME/bin/startServer.sh server1
```

To configure the WebSphere Application Server to start automatically, follow the steps that are described in the section that describes creating an SMF service definition, in the *IBM WebSphere Application Server V6.1 on the Solaris 10 Operating System* Redbooks publication. This document is available at: http://www.redbooks.ibm.com/abstracts/sg247584.html.

Adapt the information from the web page with values based on your IBM Security Key Lifecycle Manager installation. For example, use the directories from your system in the script:

```
WAS_DIR="//opt/IBM/WebSphere/AppServer/profiles/KLMProfile"
```

On some systems, it might be necessary to increase the timeout value in the manifest file from 60 to 300.

Setting the session timeout interval

The IBM Security Key Lifecycle Manager user interface session can be configured to time out after thirty minutes of inactivity or to stay alive with no time restriction.

Procedure

1. You can set the session timeout interval by using the graphical user interface:
   a. Using the WASAdmin user ID, log in to the WebSphere Integrated Solutions Console.

      ```
      https://localhost:9083/ibm/console/logon.jsp
      ```
   b. On the **Applications** tab, click **Application Types** > **WebSphere enterprise applications**.
   c. On the Enterprise Applications page, click **sklm_kms**.
   d. In the Web Module Properties section, click **Session management**.
   e. In the General Properties section, select **Override session management** .
   f. In the Session timeout section, select **No timeout** to stay alive with no timeout.
   g. To set the inactivity timeout in minutes, select **Set timeout** and specify the desired inactivity timeout value.
2. Click **Apply**.
3. Click **OK**.

Setting the maximum transaction timeout

The total transaction timeout value is set to 600 seconds. Depending on the setting, some long running IBM Security Key Lifecycle Manager operations might timeout.

About this task

Long running IBM Security Key Lifecycle Manager operations might timeout with an error message like this example:

```
[10/21/08 14:28:41:693 CDT] 00000020 TimeoutManage I
WTRN0006W: Transaction 00000110001 has timed out after xxx seconds.
```

To configure the transaction timeout interval to a larger value, take these steps:

Procedure

1. Stop the server.
   - Windows systems:

     In the *WAS_HOME*`\bin` directory, type:

     ```
     stopServer.bat server1
     ```
   - AIX, Linux, and Solaris systems:

     In the *WAS_HOME*`/bin` directory, type:

     ```
     ./stopServer.sh server1
     ```
2. Edit this file:

   ```
   ..\profiles\KLMProfile\config\cells\SKLMCell\nodes\SKLMNode\
     servers\server1\server.xml
   ```
3. Change the **`propogatedOrBMTTranLifetimeTimeout`** parameter to a larger value.
4. Save the file.
5. Start the server.
   - Windows systems:

     In the *WAS_HOME*`\bin` directory, type:

     ```
     startServer.bat server1
     ```
   - AIX, Linux, and Solaris systems:

     In the *WAS_HOME*`/bin` directory, type:

     ```
     ./startServer.sh server1
     ```

Ensuring the correct version of DB2 after migration

Before you connect to the IBM Security Key Lifecycle Manager database, ensure that you use the correct version of DB2.

About this task

After migrating IBM Security Key Lifecycle Manager from version 1.0, 2.0, or 2.0.1 to version 2.5, both obsolete version 10.1 and a later version of DB2 are available.

Take these steps:

Procedure

1. Log in as the database instance owner on systems such as AIX or Linux, or the DB2 administrator on Windows systems.
2. Ensure that the correct version of DB2 is available. Take these steps:

Windows systems:

- Click **Start > IBM DB2 > DB2SKLMV25 > Command Line Tools > Command Line Processor**. Specify:

  ```
  set DB2INSTANCE=sklmdb2
  ```

- Navigate to the *drive*:\Program Files (x86)\IBM\DB2SKLMV25\bin directory and ensure that you can successfully run a DB2 command. For example, type:

  ```
  db2cmd
  db2stop
  db2start
  ```

Systems such as AIX or Linux:

- Navigate to the /opt/IBM/DB2SKLMV25/bin directory.
- Ensure that you can successfully run a DB2 command. For example, type:

  ```
  <DB_home_dir>/sqllib/db2profile
  db2stop
  db2start
  ```

3. Start IBM Security Key Lifecycle Manager, version 2.5.

Changing the DB2 server host name

After you change the IBM Security Key Lifecycle Manager system host name, you might want to change the host name of the DB2 server.

About this task

Obtain the current steps to change the host name for your level of the DB2 server from the technote at this web address: http://www.ibm.com/support/docview.wss?rs=71&context=SSEPGG&context=SSEPDU&context=SSVGXH&context=SSVGZB&context=SSFHEG&context=SSYK8P&context=SSTLZ9&q1=db2+change+hostname&uid=swg21258834&loc=en_US&cs=utf-8&lang=en

Changing an existing WebSphere Application Server host name

You must change the host name of WebSphere Application Server before you change the system host name.

Procedure

1. Change the host name of WebSphere Application Server. For more information about how to change the host name, see IBM WebSphere Application Server documentation (http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.base.iseries.doc/ae/tagt_hostname.html).
2. When this task succeeds, change the host name of the DB2 server. For more information, see "Changing the DB2 server host name."

Stopping the DB2 server

To stop the database server, stop the WebSphere Application Server and stop the DB2 server.

About this task

You must be the database instance owner on systems such as AIX or Linux, or the Local Administrator on Windows systems.

To stop the database server, take these steps:

Procedure

1. Log in as the database instance owner on systems such as AIX or Linux, or log in as Local Administrator on Windows systems.
2. Stop the WebSphere Application Server. Type this command:

   Windows systems:

   ```
   cd C:\Program Files (x86)\IBM\WebSphere\AppServer\bin
   .\stopServer.bat server1 -username wasadmin -password mysecretpwd
   ```

   Systems such as AIX or Linux:

   ```
   /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1 -username wasadmin
    -password mysecretpwd
   ```
3. Stop the DB2 server. Type these commands:

   Windows systems:

   ```
   set DB2INSTANCE=sklmdb2
   db2stop
   ```

   Systems such as AIX or Linux:

   ```
   su -sklmdb2
   db2stop
   ```

Configuring SSL

After you install IBM Security Key Lifecycle Manager, you might configure secure communication by using SSL.

About this task

This option is controlled by the **config.keystore.ssl.certalias** property in the *SKLM_HOME*/config/SKLMConfig.properties file.

If transport ports are specified, this alias points at an existing certificate that is used for SSL authentication for secure communication between a drive and the IBM Security Key Lifecycle Manager server.

If you migrate data from Encryption Key Manager, all the certificates from the TransportListener truststore are imported into the IBM Security Key Lifecycle Manager keystore.

A certificate from the TransportListener *keystore* is set as the SSL certificate for IBM Security Key Lifecycle Manager. The **config.keystore.ssl.certalias** property is updated with the alias of this certificate.

To configure SSL for secure communication, follow these steps:

Procedure

1. Navigate to the appropriate page or directory.
   - Graphical user interface:

     Log on to the graphical user interface. You can select either of these paths:
     - Click **IBM Security Key Lifecycle Manager > Configuration > SSL/KMIP**.
     - **IBM Security Key Lifecycle Manager > Advanced Configuration > Server Certificates**.
   - Command-line interface:

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

- Windows systems:

  ```
  wsadmin -username SKLMAdmin -password mypwd -lang jython
  ```

- Systems such as AIX or Linux:

  ```
  ./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
  ```

2. Specify the certificate that is used for SSL communication.
   - Graphical user interface:

     Specify a certificate as the SSL certificate:

     - On the SSL/KMIP for Key Serving page, select the option to use an existing certificate from the keystore as the SSL certificate. Select a certificate and click **OK**.
     - Alternatively, on the Administer Server Certificates page, select an existing certificate and click **Modify**. Specify that the certificate is the currently used certificate and click **Modify Certificate**.
   - Command-line interface:
     - To see the value of the property, use the **tklmConfigGetEntry** command. For example, you might want to validate that a migrated certificate is set as the SSL certificate.

       This Jython-formatted command obtains the current value of the **config.keystore.ssl.certalias** property.

       ```
       wsadmin>print AdminTask.tklmConfigGetEntry
        ('[-name config.keystore.ssl.certalias]')
       ```
     - To change the value of the property, use the **tklmConfigUpdateEntry** command to specify the certificate that the IBM Security Key Lifecycle Manager server uses.

     For example, this Jython-formatted command example changes the value of the **config.keystore.ssl.certalias** property.

     ```
     print AdminTask.tklmConfigUpdateEntry
       ('[-name config.keystore.ssl.certalias
        -value mycert]')
     ```
3. A success indicator varies, depending on the interface:
   - Graphical user interface:

     On the Success page, under Next Steps, click a related task that you want to carry out.
   - Command-line interface:

     A completion message indicates success.

Determining the current port number

After IBM Security Key Lifecycle Manager server installation, you might want to determine the secure port numbers for the IBM Security Key Lifecycle Manager server and the WebSphere Integrated Solutions Console.

About this task

The value of the port numbers is specified by the **WC_defaulthost_secure** or the **WC_adminhost_secure** property in the *WAS_HOME*/profiles/KLMProfile/properties/portdef.props file. For example, the file might specify these values:

```
WC_defaulthost_secure=9080
WC_adminhost_secure=9083
```

The **`WC_defaulthost_secure`** property value corresponds to the IBM Security Key Lifecycle Manager server secure port and the **`WC_adminhost_secure`** property value corresponds to the WebSphere Integrated Solutions Console secure port.

Installation verification

After the installation on distributed systems, verify that the IBM Security Key Lifecycle Manager installation was successful.

Perform these actions to verify the installation on distributed systems:

1. Start and stop the server. See “Starting and stopping the IBM Security Key Lifecycle Manager server on distributed systems” on page 91 for details.
2. Open IBM Security Key Lifecycle Manager in a web browser and log in.
   a. Open a web browser and direct it to the administrative console. For more information, see “Login URL and initial user ID” on page 14.
   b. Log in to WebSphere Application Server.
   c. Click the IBM Security Key Lifecycle Manager link in the navigation panel on the left side of the page to expand the IBM Security Key Lifecycle Manager section and click the **Welcome** link.
   d. IBM Security Key Lifecycle Manager opens in the main panel, displaying the IBM Security Key Lifecycle Manager Welcome page.
3. Use the command-line interface to list the IBM Security Key Lifecycle Manager command group. For example, from *`WAS_HOME`*`/bin`, enter:

   ```
    ./wsadmin.sh -username <sklmadmin id> -password <sklmadmin passwd> -lang jython
   ```

   When the **wsadmin** tool prompts you, enter this command:

   ```
   wsadmin>print AdminTask.help("-commandGroups")
   ```

   The IBM Security Key Lifecycle Manager command groups are displayed. For example, the list contains backup commands and other command groups:

   ```
   TKLMBackupCommands - IBM Security Key Lifecycle Manager backup/restore commands
   ```

Enabling scripting settings for Internet Explorer, version 9 and 10

Ensure that scripting settings for Internet Explorer, version 9.0 and 10.0 are enabled.

About this task

Unless some scripting settings are enabled for Internet Explorer, version 9.0 and 10.0, you might later be unable to create an IBM Security Key Lifecycle Manager user.

Ensure that these browser settings are enabled:

- Allow status bar updates through scripts
- Active Scripting
- Scripting of Java applets

Procedure

1. Open the browser and click **Tools** > **Internet Options** > **Security**.

2. Scroll the list of security settings to the Scripting options and ensure that these settings are enabled:
   - Allow status bar updates through scripts
   - Active Scripting
   - Scripting of Java applets
3. Click **OK**.

Starting and stopping the IBM Security Key Lifecycle Manager server on distributed systems

You might want to use the **startServer** or **stopServer** command to start or stop the IBM Security Key Lifecycle Manager server. For example, after a restore task completes, restart the IBM Security Key Lifecycle Manager server.

About this task

The IBM Security Key Lifecycle Manager server automatically restarts after a backup file is restored when the **autoRestartAfterRestore** property value is `true` (default value) in the `SKLMConfig.properties` file.

Scripts to start and stop the IBM Security Key Lifecycle Manager server are in the *WAS_HOME*/bin directory.

Procedure

1. Navigate to the *WAS_HOME*/bin directory.
2. Start or stop the server.
   - Start

     On Windows systems:
     ```
     startServer.bat server1
     ```
     On systems such as Linux or AIX:
     ```
     ./startServer.sh server1
     ```
   - Stop

     On Windows systems:
     ```
     stopServer.bat server1
     ```
     On systems such as Linux or AIX:
     ```
     ./stopServer.sh server1
     ```

   Global security is enabled by default. Enter the user ID and password of the WebSphere Application Server administrator as parameters to the `stopServer` script. The script prompts for these parameters when they are omitted, but you can specify them on the command line:

   On Windows systems:
   ```
   stopServer.bat server1 -username wasadmin -password mypwd
   ```
   On systems such as Linux or AIX:
   ```
   ./stopServer.sh server1  -username wasadmin -password mypwd
   ```

What to do next

Determine whether IBM Security Key Lifecycle Manager is running. For example, open IBM Security Key Lifecycle Manager in a web browser and log in.

Enabling global security

Conditions might occur in which you must enable global security.

About this task

Do not disable global security when you use IBM Security Key Lifecycle Manager.

Procedure

1. To enable global security, log in as the WebSphere Application Server administrator WASAdmin.
2. In the navigation bar, click **Security**.
3. Click **Secure administration, applications and infrastructure**.
4. Check the **Enable administrative security** check box.

   Ensure that **Enable application security** is also selected and that **Use Java 2 security to restrict application access to local resources** is *not* selected.
5. Click **Apply**.
6. Click **Save** in the Messages box. Click **Logout**.
7. Stop and restart the server.
8. Reload the IBM Security Key Lifecycle Manager login page. Verify that the page requires a password.

Disabling global security

Conditions might occur in which you must disable global security.

About this task

Do not disable global security when you use IBM Security Key Lifecycle Manager.

Procedure

1. To disable global security, log in as the WebSphere Application Server administrator WASAdmin.
2. In the navigation bar, click **Security**.
3. Click **Secure administration, applications and infrastructure**.
4. Clear the **Enable administrative security** check box.
5. Click **Apply**.
6. Click **Save** in the Messages box. Click **Logout**.
7. Stop and restart the server.
8. Reload the IBM Security Key Lifecycle Manager login page. Verify that the page does *not* require a password.

Preinstallation worksheets

Before you begin to install and configure IBM Security Key Lifecycle Manager, you can complete these worksheets to identify the configuration parameters that are required to complete the IBM Security Key Lifecycle Manager installation.

General installation parameters

Use the worksheet to record general installation parameters.

Table 9. General installation parameters

Option	Description	Default or example value	Your value

Installation mode	Mode in which to run the installation program.	`gui (default)`
		`silent`	

Important Step: Check your free disk space	Ensure that you have enough free disk space available.	See "Hardware requirements for distributed systems" on page 9 for values.	

DB2 configuration parameters

Use the worksheet to record your entries that are related to the installation and configuration of DB2.

Table 10. DB2 configuration parameters

Field name	Description	Default or example value	Your value

DB2 Destination	Directory in which to install DB2	**Windows systems:**
		`*drive*:\Program Files (x86)\IBM\DB2SKLMV25`
		AIX and Linux systems:
		`/opt/IBM/DB2SKLMV25`	

DB2 Administrator ID	User ID for the IBM Security Key Lifecycle Manager database administrator (also called the instance owner)	`sklmdb2`	
DB2 Administrator Password	Password for the database administrator user ID		

Table 10. DB2 configuration parameters (continued)

Field name	Description	Default or example value	Your value
Database name	Name of the IBM Security Key Lifecycle Manager database	`sklmdb`	
DB2 Port	DB2 service listening port	`50010`	
Administrator / Database Home	Directory where the database instance and formatted tables are created	C:	
Administrator group	Group in which the instance owner of the database is a member.	If DB2 is on a system such as AIX or Linux, your user ID must be in the bin or root group, or in a separate group in which root is a member.	
Instance Drive Letter	Drive where DB2 is to be installed (Windows systems only)	C:	

Sample response files

You might want to use sample response files for Windows and other systems. Before installation, you must also read and agree to the license terms for this product. To locate the response files and license term files, look in the root directory of the installation image files. The `/license` subdirectory has the license files in text format.

Installation fails unless you take these steps.

In the response file, make following changes to the line that specifies the license:

- Set the default value to `true` to indicate that you agree with the terms of the license.
- Uncomment the line by removing the pound sign (#) character at the beginning of the line.

New installation of version 2.5 on Windows systems

The example response file contains responses for an installation of IBM Security Key Lifecycle Manager, version 2.5 onto a Windows system or an installation in which Encryption Key Manager migration occurs.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense="true">
<server>
<repository location='C:\disk1\im'/>
<repository location='C:\disk1\'/>
</server>
<profile id="IBM Installation Manager" installLocation="C:\Program Files
<x86>\IBM\Installation Manager\eclipse" kind="self">
<data key="eclipseLocation" value="C:\Program Files <x86>\IBM\Installation
Manager\eclipse"/>
<data key="user.import.profile" value="false"/>
<data key="cic.selector.os" value="win32"/>
<data key="cic.selector.arch" value="x86_64"/>
<data key="cic.selector.ws" value="win32"/>
</profile>
<install modify="false">
<offering id="com.ibm.cic.agent"  profile="IBM Installation Manager"
features="agent_core,agent_jre" installFixes="none"/>
<offering id="com.ibm.db2.ofng"  profile="IBM DB2" features="com.ibm.db2.ofng"
installFixes="none"/>
<offering id="com.ibm.websphere.BASE.v85"  profile="IBM WebSphere Application
Server V8.5" features="core.feature,ejbdeploy,thinclient,embeddablecontainer,
com.ibm.sdk.6_32bit" installFixes="none"/>
<offering id="com.ibm.sklm.win32"  profile="IBM Security Key Lifecycle Manager
v2.5" features="main.feature" installFixes="none"/>
</install>
<profile id="IBM DB2" installLocation="C:\Program Files <x86>\IBM\DB2SKLMV25">
<data key="eclipseLocation" value="C:\Program Files <x86>\IBM\DB2SKLMV25"/>
<data key="user.import.profile" value="false"/>
<data key="cic.selector.os" value="win32"/>
<data key="cic.selector.arch" value="x86"/>
<data key="cic.selector.ws" value="win32"/>
<data key="user.DB2_ADMIN_ID,com.ibm.db2.ofng" value="sklmdb2"/>
<data key="user.DB2_ADMIN_PWD,com.ibm.db2.ofng" value="SwIhGBTDHcJok80Ux4Sb3g
=="/>
<data key="user.CONFIRM_PASSWORD,com.ibm.db2.ofng" value="SwIhGBTDHcJok80Ux4Sb3g
=="/>
<data key="user.DB2_DB_HOME,com.ibm.db2.ofng" value="C:"/>
<data key="user.DB2_DB_NAME,com.ibm.db2.ofng" value="SKLMDB"/>
<data key="user.DB2_DB_PORT,com.ibm.db2.ofng" value="50010"/>
<data key="user.DB2_EXISTS,com.ibm.db2.ofng" value="false"/>
<data key="user.DB2_LOCATION,com.ibm.db2.ofng" value="C:\\Program Files <x86>\\
IBM\\DB2SKLMV25"/>
<data key="cic.selector.nl" value="en"/>
</profile>
<profile id="IBM WebSphere Application Server V8.5" installLocation="C:\Program
Files <x86>\IBM\WebSphere\AppServer">
<data key="eclipseLocation" value="C:\Program Files <x86>\IBM\WebSphere\
AppServer"/>
<data key="user.import.profile" value="false"/>
<data key="cic.selector.os" value="win32"/>
<data key="cic.selector.arch" value="x86"/>
<data key="cic.selector.ws" value="win32"/>
<data key="cic.selector.nl" value="en"/>
</profile>
<profile id="IBM Security Key Lifecycle Manager v2.5" installLocation=
"C:\Program Files <x86>\IBM\SKLMV25">
<data key="eclipseLocation" value="C:\Program Files <x86>\IBM\SKLMV25"/>
<data key="user.import.profile" value="false"/>
<data key="cic.selector.os" value="win32"/>
<data key="cic.selector.arch" value="x86"/>
<data key="cic.selector.ws" value="win32"/>
<data key="user.EKM_PROPFILE,com.ibm.sklm.win32" value="C:\KeyManagerConfig.
properties"/>
<data key="user.EKM_MIGRATION,com.ibm.sklm.win32" value="false"/>
<data key="user.PROFILE_NAME,com.ibm.sklm.win32" value="KLMProfile"/>
<data key="user.WAS_ADMIN_ID,com.ibm.sklm.win32" value="wasadmin"/>
<data key="user.WAS_ADMIN_PASSWORD,com.ibm.sklm.win32"
value="zN39fpCc9SqIryGJM7+02A=="/>
<data key="user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.win32"
value="zN39fpCc9SqIryGJM7+02A=="/>
<data key="user.SKLM_ADMIN_USER,com.ibm.sklm.win32" value="SKLMAdmin"/>
<data key="user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.win32"
value="94FrH/Ll220hVIYc9TflNQ=="/>
<data key="user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.win32"
value="94FrH/Ll220hVIYc9TflNQ=="/>
<data key="user.SKLM_APP_PORT,com.ibm.sklm.win32" value="9080"/>
<data key="cic.selector.nl" value="en"/>
</profile>
<preference name="com.ibm.cic.common.core.preferences.eclipseCache"
value="C:\Program Files <x86>\IBM\IBMIMShared"/>
<preference name="com.ibm.cic.common.core.preferences.connectTimeout"
value="30"/>
<preference name="com.ibm.cic.common.core.preferences.readTimeout"
value="45"/>
<preference name="com.ibm.cic.common.core.preferences.downloadAutoRetryCount"
value="0"/>
<preference name="offering.service.repositories.areUsed" value="true"/>
<preference name="com.ibm.cic.common.core.preferences.ssl.nonsecureMode"
value="false"/>
<preference name="com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication" value="false"/>
<preference name="http.ntlm.auth.kind" value="NTLM"/>
<preference name="http.ntlm.auth.enableIntegrated.win32" value="true"/>
<preference name="com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts" value="true"/>
<preference name="com.ibm.cic.common.core.preferences.keepFetchedFiles"
value="false"/>
<preference name="PassportAdvantageIsEnabled" value="false"/>
<preference name="com.ibm.cic.common.core.preferences.searchForUpdates"
value="false"/>
<preference name="com.ibm.cic.agent.ui.displayInternalVersion" value="false"/>
<preference name="com.ibm.cic.common.sharedUI.showErrorLog" value="true"/>
<preference name="com.ibm.cic.common.sharedUI.showWarningLog" value="true"/>
<preference name="com.ibm.cic.common.sharedUI.showNoteLog" value="true"/>
</agent-input>
```

New installation of version 2.5 on systems such as Linux or AIX systems

The example response file contains responses for an installation of IBM Security Key Lifecycle Manager, version 2.5 onto a system such as Linux or AIX or an installation in which Encryption Key Manager migration occurs.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--
The "acceptLicense" attribute has been deprecated. Use "-acceptLicense" command line
option to accept license agreements.
  -->
```

```
- <agent-input acceptLicense="true">
- <server>
  <repository location="/disk1/im" />
  <repository location="/disk1/" />
  </server>
- <profile id="IBM DB2" installLocation="/opt/IBM/DB2SKLMV25">
  <data key="eclipseLocation" value="/opt/IBM/DB2SKLMV25" />
  <data key="user.import.profile" value="false" />
  <data key="cic.selector.os" value="linux" />
  <data key="cic.selector.arch" value="x86" />
  <data key="cic.selector.ws" value="gtk" />
  <data key="user.DB2_ADMIN_ID,com.ibm.db2.linux.ofng" value="sklmdb2" />
  <data key="user.DB2_ADMIN_GRP,com.ibm.db2.linux.ofng" value="root" />
  <data key="user.DB2_ADMIN_PWD,com.ibm.db2.linux.ofng" value="SwIhGBTDHcJok80Ux4Sb3g==" />
  <data key="user.CONFIRM_PASSWORD,com.ibm.db2.linux.ofng" value="SwIhGBTDHcJok80Ux4Sb3g=="/>
  <data key="user.DB2_DB_LHOME,com.ibm.db2.linux.ofng" value="/home/sklmdb2" />
  <data key="user.DB2_DB_NAME,com.ibm.db2.linux.ofng" value="SKLMDB" />
  <data key="user.DB2_DB_PORT,com.ibm.db2.linux.ofng" value="50010" />
  <data key="user.DB2_EXISTS,com.ibm.db2.linux.ofng" value="false" />
  <data key="user.DB2_LOCATION,com.ibm.db2.linux.ofng" value="/opt/IBM/DB2SKLMV25" />
  <data key="cic.selector.nl" value="en" />
  </profile>
- <install modify="false">
  <offering id="com.ibm.cic.agent" profile="IBM Installation Manager" features="agent_core,
agent_jre" installFixes="none" />
  <offering id="com.ibm.db2.linux.ofng" profile="IBM DB2" features=
"com.ibm.com.ibm.db2.linux" installFixes="none" />
  <offering id="com.ibm.websphere.BASE.v85" profile="IBM WebSphere Application Server V8.5"
features="core.feature,ejbdeploy,thinclient,embeddablecontainer,com.ibm.sdk.6_32bit"
installFixes="none" />
  <offering id="com.ibm.sklm.linux" profile="IBM Security Key Lifecycle Manager v2.5"
features="main.feature" installFixes="none" />
  </install>
- <profile id="IBM Installation Manager" installLocation="/opt/IBM/InstallationManager/
eclipse" kind="self">
  <data key="eclipseLocation" value="/opt/IBM/InstallationManager/eclipse" />
  <data key="user.import.profile" value="false" />
  <data key="cic.selector.os" value="linux" />
  <data key="cic.selector.arch" value="x86" />
  <data key="cic.selector.ws" value="gtk" />
  </profile>
- <profile id="IBM WebSphere Application Server V8.5" installLocation="/opt/IBM/WebSphere/
AppServer">
  <data key="eclipseLocation" value="/opt/IBM/WebSphere/AppServer" />
  <data key="user.import.profile" value="false" />
  <data key="cic.selector.os" value="linux" />
  <data key="cic.selector.arch" value="x86" />
  <data key="cic.selector.ws" value="gtk" />
  <data key="cic.selector.nl" value="en" />
  </profile>
- <profile id="IBM Security Key Lifecycle Manager v2.5" installLocation="/opt/IBM/SKLMV25">
  <data key="eclipseLocation" value="/opt/IBM/SKLMV25" />
  <data key="user.import.profile" value="false" />
  <data key="cic.selector.os" value="linux" />
  <data key="cic.selector.arch" value="x86" />
  <data key="cic.selector.ws" value="gtk" />
  <data key="user.EKM_PROPFILE,com.ibm.sklm.linux" value="/opt/IBM/KeyManagerConfig.
properties" />
  <data key="user.EKM_MIGRATION,com.ibm.sklm.linux" value="false" />
  <data key="user.PROFILE_NAME,com.ibm.sklm.linux" value="KLMProfile" />
  <data key="user.WAS_ADMIN_ID,com.ibm.sklm.linux" value="wasadmin" />
  <data key="user.WAS_ADMIN_PASSWORD,com.ibm.sklm.linux" value="zN39fpCc9SqIryGJM7+02A==" />
  <data key="user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.linux" value="zN39fpCc9SqIryGJM7+02A==" />
  <data key="user.SKLM_ADMIN_USER,com.ibm.sklm.linux" value="SKLMAdmin" />
  <data key="user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.linux" value="94FrH/Ll220hVIYc9TflNQ==" />
  <data key="user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.linux" value="94FrH/Ll220hVIYc9TflNQ==" />
  <data key="user.SKLM_APP_PORT,com.ibm.sklm.linux" value="9080" />
  <data key="cic.selector.nl" value="en" />
  </profile>
  <preference name="com.ibm.cic.common.core.preferences.eclipseCache" value="/opt/IBM/
IBMIMShared" />
  <preference name="com.ibm.cic.common.core.preferences.connectTimeout" value="30" />
  <preference name="com.ibm.cic.common.core.preferences.readTimeout" value="45" />
  <preference name="com.ibm.cic.common.core.preferences.downloadAutoRetryCount" value="0" />
  <preference name="offering.service.repositories.areUsed" value="true" />
  <preference name="com.ibm.cic.common.core.preferences.ssl.nonsecureMode" value="false" />
  <preference name="com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication" value="false" />
  <preference name="http.ntlm.auth.kind" value="NTLM" />
  <preference name="http.ntlm.auth.enableIntegrated.win32" value="true" />
  <preference name="com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts"
value="true" />
  <preference name="com.ibm.cic.common.core.preferences.keepFetchedFiles" value="false" />
  <preference name="PassportAdvantageIsEnabled" value="false" />
  <preference name="com.ibm.cic.common.core.preferences.searchForUpdates" value="false" />
  <preference name="com.ibm.cic.agent.ui.displayInternalVersion" value="false" />
  <preference name="com.ibm.cic.common.sharedUI.showErrorLog" value="true" />
  <preference name="com.ibm.cic.common.sharedUI.showWarningLog" value="true" />
  <preference name="com.ibm.cic.common.sharedUI.showNoteLog" value="true" />
  </agent-input>
```

Earlier version to version 2.5 migration on Windows systems

The example response file contains responses for an installation onto a Windows system in which IBM Security Key Lifecycle Manager earlier version to version 2.5 migration occurs.

Note: To determine whether IBM Security Key Lifecycle Manager earlier version exists and requires migration, use the **tklmVersionInfo** command. For example, type this command in a Jython session:

```
print AdminTask.tklmVersionInfo()
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
<server>
<repository location='C:\disk1\im'/>
<repository location='C:\disk1\'/>
</server>
<profile id='IBM Installation Manager' installLocation='C:\Program Files <x86>\
IBM\Installation Manager\eclipse' kind='self'>
<data key='eclipseLocation' value='C:\Program Files <x86>\IBM\Installation
Manager\eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='win32'/>
<data key='cic.selector.arch' value='x86_64'/>
<data key='cic.selector.ws' value='win32'/>
</profile>
<install modify='false'>
<offering id='com.ibm.cic.agent'  profile='IBM Installation Manager'
features='agent_core,agent_jre' installFixes='none'/>
<offering id='com.ibm.db2.ofng'  profile='IBM DB2' features='com.ibm.db2.ofng'
installFixes='none'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
com.ibm.sdk.6_32bit' installFixes='none'/>
<offering id='com.ibm.sklm.win32'  profile='IBM Security Key Lifecycle Manager
v2.5' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM DB2' installLocation='C:\Program Files <x86>\IBM\DB2SKLMV25'>
<data key='eclipseLocation' value='C:\Program Files <x86>\IBM\DB2SKLMV25'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='win32'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='win32'/>
<data key='user.DB2_ADMIN_ID,com.ibm.db2.ofng' value='sklmdb2'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.ofng' value='SwIhGBTDHcJok80Ux4Sb3g==
'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=
='/>
<data key='user.DB2_DB_HOME,com.ibm.db2.ofng' value='C:'/>
<data key='user.DB2_DB_NAME,com.ibm.db2.ofng' value='SKLMDB'/>
<data key='user.DB2_DB_PORT,com.ibm.db2.ofng' value='50010'/>
<data key='user.DB2_EXISTS,com.ibm.db2.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.db2.ofng' value='C:\\Program Files <x86>\\
IBM\\DB2SKLMV25'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM WebSphere Application Server V8.5' installLocation='C:\Program
Files <x86>\IBM\WebSphere\AppServer'>
<data key='eclipseLocation' value='C:\Program Files <x86>\IBM\WebSphere\
AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='win32'/>
```

```
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='win32'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v2.5' installLocation=
'C:\Program Files <x86>\IBM\SKLMV25'>
<data key='eclipseLocation' value='C:\Program Files <x86>\IBM\SKLMV25'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='win32'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='win32'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm.win32' value='C:\KeyManagerConfig.
properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm.win32' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm.win32' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm.win32' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.win32' value=
'L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.win32' value=
'L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm.win32' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.win32' value=
'now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.win32' value=
'now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm.win32' value='9080'/>
<data key='user.TKLM_VERSION,com.ibm.sklm.win32' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm.win32' value=
'C:\IBM\tivoli\tiptklmV2'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm.win32' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm.win32' value=
'/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm.win32' value=
'fufgZbY47EfxLYarBAIxeQ=='/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='C:\Program Files <x86>\IBM\IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout'
value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout'
value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount'
value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode'
value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles'
value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates'
value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Earlier version to version 2.5 migration on Linux systems

The example response file contains responses for an installation Linux system in which IBM Security Key Lifecycle Manager earlier version to version 2.5 migration occurs.

Note: To determine whether IBM Security Key Lifecycle Manager earlier version exists and requires migration, use the **tklmVersionInfo** command. For example, type this command in a Jython session:

```
print AdminTask.tklmVersionInfo()
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
<server>

<repository location='/disk1/im'/>
<repository location='/disk1/'/>

</server>
<profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV25'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV25'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.db2.linux.ofng' value='sklmdb2'/>
<data key='user.DB2_ADMIN_GRP,com.ibm.db2.linux.ofng' value='root'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.linux.ofng' value=
'SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.linux.ofng' value=
'SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.DB2_DB_LHOME,com.ibm.db2.linux.ofng' value=
'/home/sklmdb2'/>
<data key='user.DB2_DB_NAME,com.ibm.db2.linux.ofng' value='SKLMDB'/>
<data key='user.DB2_DB_PORT,com.ibm.db2.linux.ofng' value='50010'/>
<data key='user.DB2_EXISTS,com.ibm.db2.linux.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.db2.linux.ofng' value=
'/opt/IBM/DB2SKLMV25'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<install modify='false'>
<offering id='com.ibm.cic.agent'  profile='IBM Installation Manager'
features='agent_core,agent_jre' installFixes='none'/>
<offering id='com.ibm.db2.linux.ofng'  profile='IBM DB2' features=
'com.ibm.com.ibm.db2.linux' installFixes='none'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
com.ibm.sdk.6_32bit' installFixes='none'/>
<offering id='com.ibm.sklm.linux'  profile='IBM Security Key Lifecycle Manager
v2.5' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/
InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='x86_64'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/WebSphere/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v2.5' installLocation=
'/opt/IBM/SKLMV25'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV25'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm.linux' value='/opt/IBM/
KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm.linux' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm.linux' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm.linux' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.linux' value=
'L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.linux' value=
'L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm.linux' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.linux' value=
'now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.linux' value=
'now6wpN1MFAVFGfIB1r9+Q=='/>
```

```
<data key='user.SKLM_APP_PORT,com.ibm.sklm.linux' value='9080'/>
<data key='user.TKLM_VERSION,com.ibm.sklm.linux' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm.linux' value=
'/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm.linux' value=
'true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm.linux' value=
'/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm.linux' value=
'fufgZbY47EfxLYarBAIxeQ=='/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout'
value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout'
value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount'
value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode'
value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles'
value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates'
value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value=
'false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value=
'true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value=
'true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Earlier version to version 2.5 migration on AIX systems

The example response file contains responses for an installation on AIX system in which IBM Security Key Lifecycle Manager earlier version to version 2.5 migration occurs.

Note: To determine whether IBM Security Key Lifecycle Manager earlier version exists and requires migration, use the **tklmVersionInfo** command. For example, type this command in a Jython session:

```
print AdminTask.tklmVersionInfo<>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
<server>

<repository location='/disk1/im'/>
<repository location='/disk1/'/>

</server>
<profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV25'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV25'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='motif'/>
<data key='user.DB2_ADMIN_ID,com.ibm.db2.aix.ofng' value='sklmdb2'/>
<data key='user.DB2_ADMIN_GRP,com.ibm.db2.aix.ofng' value='bin'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.aix.ofng' value=
'SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.aix.ofng' value=
'SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.DB2_DB_HOME,com.ibm.db2.aix.ofng' value='/home/sklmdb2'/>
<data key='user.DB2_DB_NAME,com.ibm.db2.aix.ofng' value='SKLMDB'/>
<data key='user.DB2_DB_PORT,com.ibm.db2.aix.ofng' value='50010'/>
<data key='user.DB2_EXISTS,com.ibm.db2.aix.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.db2.aix.ofng' value=
'/opt/IBM/DB2SKLMV25'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<install modify='false'>
<offering id='com.ibm.cic.agent'  profile='IBM Installation Manager'
features='agent_core,agent_jre' installFixes='none'/>
<offering id='com.ibm.db2.aix.ofng'  profile='IBM DB2' features='main.feature'
installFixes='none'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
com.ibm.sdk.6_32bit' installFixes='none'/>
<offering id='com.ibm.sklm.aix'  profile='IBM Security Key Lifecycle Manager
v2.5' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM Installation Manager' installLocation=
'/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='motif'/>
</profile>
<profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/WebSphere/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='motif'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v2.5' installLocation=
'/opt/IBM/SKLMV25'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV25'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='motif'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm.aix' value='/opt/IBM/KeyManagerConfig.
properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm.aix' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm.aix' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm.aix' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.aix' value=
'L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.aix' value=
'L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm.aix' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.aix' value=
'now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.aix' value=
'now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm.aix' value='9080'/>
<data key='user.TKLM_VERSION,com.ibm.sklm.aix' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm.aix' value='/opt/IBM/tivoli/
tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm.aix' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm.aix' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm.aix' value=
'fufgZbY47EfxLYarBAIxeQ=='/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout'
value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout'
value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount'
value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode'
value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.
```

```
disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles'
value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates'
value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Earlier version to version 2.5 migration on Solaris systems

The example response file contains responses for an installation on Solaris system in which IBM Security Key Lifecycle Manager earlier version to version 2.5 migration occurs.

Note: To determine whether IBM Security Key Lifecycle Manager earlier version exists and requires migration, use the **tklmVersionInfo** command. For example, type this command in a Jython session:

```
print AdminTask.tklmVersionInfo<>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
<server>

<repository location='/disk1/im'/>
<repository location='/disk1/'/>

</server>
<profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV25'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV25'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='solaris'/>
<data key='cic.selector.arch' value='sparc'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.db2.solaris.ofng' value='sklmdb2'/>
<data key='user.DB2_ADMIN_GRP,com.ibm.db2.solaris.ofng' value='root'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.solaris.ofng' value=
'SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.solaris.ofng' value=
'SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.DB2_DB_HOME,com.ibm.db2.solaris.ofng' value=
'/export/home/sklmdb2'/>
<data key='user.DB2_DB_NAME,com.ibm.db2.solaris.ofng' value='SKLMDB'/>
<data key='user.DB2_DB_PORT,com.ibm.db2.solaris.ofng' value='50010'/>
<data key='user.DB2_EXISTS,com.ibm.db2.solaris.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.db2.solaris.ofng' value=
'/opt/IBM/DB2SKLMV25'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<install modify='false'>
<offering id='com.ibm.cic.agent'  profile='IBM Installation Manager' features=
'agent_core,agent_jre' installFixes='none'/>
<offering id='com.ibm.db2.solaris.ofng'  profile='IBM DB2' features=
'main.feature' installFixes='none'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none
<offering id='com.ibm.sklm.solaris'  profile='IBM Security Key Lifecycle Manager
 v2.5' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/
InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='solaris'/>
<data key='cic.selector.arch' value='sparc'/>
<data key='cic.selector.ws' value='gtk'/>
```

```
</profile>
<profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/WebSphere/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='solaris'/>
<data key='cic.selector.arch' value='sparc'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v2.5' installLocation=
'/opt/IBM/SKLMV25'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV25'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='solaris'/>
<data key='cic.selector.arch' value='sparc'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm.solaris' value='/opt/IBM/
KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm.solaris' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm.solaris' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm.solaris' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.solaris' value=
'L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.solaris' value=
'L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm.solaris' value=
'TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.solaris' value=
'now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.solaris' value=
'now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm.solaris' value='9080'/>
<data key='user.TKLM_VERSION,com.ibm.sklm.solaris' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm.solaris' value='/opt/IBM/tivoli/
tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm.solaris' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm.solaris' value='/6vJK3fcU3QxHY+RVfCFVw
=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm.solaris' value=
'fufgZbY47EfxLYarBAIxeQ=='/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout'
value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout'
value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount'
value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode'
value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles'
value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates'
value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Uninstallation on Windows systems

The example response file contains responses for uninstall on Windows systems.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<profile id="IBM Security Key Lifecycle Manager v2.5">
<data key="user.WAS_ADMIN_ID,com.ibm.sklm.win32" value="wasadmin"/>
```

```
<data key="user.WAS_ADMIN_PASSWORD,com.ibm.sklm.win32"
value="zN39fpCc9SqIryGJM7+02A=="/>
</profile>
<uninstall modify="false">
<offering id="com.ibm.sklm.win32"  profile="IBM Security Key Lifecycle Manager
v2.5" features="main.feature"/>
<offering id="com.ibm.websphere.BASE.v85"  profile="IBM WebSphere Application
Server V8.5" features="core.feature,ejbdeploy,thinclient,embeddablecontainer,
samples,com.ibm.sdk.6_32bit,com.ibm.sdk.6_64bit"/>
<offering id="com.ibm.db2.ofng"  profile="IBM DB2" features="com.ibm.db2.ofng"/>
</uninstall>
</agent-input>
```

Uninstallation on systems such as Linux or AIX

The example response file contains responses for uninstall on a system such as Linux or AIX.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<profile id='IBM Security Key Lifecycle Manager v2.5'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm.linux' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.linux' value=
'zN39fpCc9SqIryGJM7+02A=='/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm.linux'  profile='IBM Security Key Lifecycle Manager
v2.5' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
samples,com.ibm.sdk.6_32bit,com.ibm.sdk.6_64bit'/>
<offering id='com.ibm.db2.linux.ofng'  profile='IBM DB2' features=
'com.ibm.com.ibm.db2.linux'/>
</uninstall>
</agent-input>
```

Installation error messages

Depending on the outcome of an operation, IBM Security Key Lifecycle Manager might provide an informational, warning, or error message.

Message format

Messages that are logged by IBM Security Key Lifecycle Manager adhere to the Tivoli Message Standard. Each message consists of a message identifier (ID) and accompanying message text.

Messages have the following syntax:

```
CTGUUXXXXZ
```

where:

CTG Identifies the IBM Security Key Lifecycle Manager product.

UU Identifies the component or subsystem of IBM Security Key Lifecycle Manager. For example:

KM IBM Security Key Lifecycle Manager server messages.

KO Password policy messages.

KS IBM Security Key Lifecycle Manager key server messages.

XXXX Indicates serial or message number, such as 0001.

Z One-character type code indicates the severity of the message:

- `I` for informational message
- `W` for warning message
- `E` for error message
-

For example:

```
CTGKM0545E: An error occurred exporting a certificate.
```

Error and warning messages

IBM Security Key Lifecycle Manager generates error and warning messages that are based on the action you take.

CTGKM9002E The administrator ID must be eight characters or less.

Explanation: The user ID is restricted to a maximum length of eight characters.

System action: Installation cannot continue until you correct the error.

User response: Select a different user ID that is eight characters or less.

CTGKM9003E The administrator ID must begin with an alphabetic character.

Explanation: The user ID must start with a letter.

Additionally, the user ID can only use alphabetical characters, numeric characters, and the underscore (A-Z, a-z, 0–9, and _).

System action: Installation cannot continue until you correct the error.

User response: Select a different user ID that starts with a letter.

CTGKM9004E The administrator ID cannot begin with: ibm, sql, or sys.

Explanation: The administrator user ID cannot start with ibm, sql, or sys.

System action: Installation cannot continue until you correct the error.

User response: Select a different user ID that does not start with one of the restricted strings.

CTGKM9005E The administrator ID cannot be: db2, users, admins, guests, public, private, properties, local, or root.

Explanation: DB2 reserved keywords cannot be used as an administrator user ID.

System action: Installation cannot continue until you correct the error.

User response: Select a different user ID that is not a DB2 keyword.

CTGKM9006E The administrator ID is a required field.

Explanation: You must specify an administrator user ID.

System action: Installation cannot continue until you enter a value in the field.

User response: Enter a user ID in the Administrator ID field.

CTGKM9007E The password is a required field.

Explanation: You must specify a password.

System action: Installation cannot continue until you enter a value in the field.

User response: Enter a password for the user ID.

CTGKM9010E The password confirmation field is required.

Explanation: You must specify a password.

System action: Installation cannot continue until you enter a value in the field.

User response: Enter a password for the user ID.

CTGKM9011E The database home is a required field.

Explanation: You must specify the database home directory.

System action: Installation cannot continue until you enter a value in the field.

User response: Enter the directory in which to store the database files.

CTGKM9012E The database name is a required field.

Explanation: You must specify a name for the database.

System action: Installation cannot continue until you enter a value in the field.

User response: Enter a name for the database.

CTGKM9037E The port value should be a positive integer between 1024 and 65536.

Explanation: Port numbers must be between 1024 and 65536.

System action: Installation cannot continue until you correct the error.

User response: Enter a port number that is between 1024 and 65536.

CTGKM9038E The port is a required field.

Explanation: You must specify a port.

System action: Installation cannot continue until you enter a value in the field.

User response: Enter a port number.

CTGKM9041E The password and password confirmation fields do not match. Reenter matching passwords for these two fields.

Explanation: The passwords in both fields must match.

System action: Installation cannot continue until you correct the error.

User response: Re-enter the values in the fields.

CTGKM9042I Passwords cannot contain spaces.

Explanation: Passwords can only contain alphanumeric characters and the underscore (a-z, A-Z, 0–9, and _).

System action: Installation cannot continue until you correct the error.

User response: Enter a different password that conforms to the rules.

CTGKM9044I The Administrator ID cannot be an SQL reserved word.

Explanation: The Administrator ID cannot be an SQL reserved word.

System action: Installation cannot continue until you correct the error.

User response: Enter a different value for the Administrator ID.

CTGKM9049I The Windows DB2 DB Home field must be a drive letter [A-Z] followed by a colon.

Explanation: On Windows systems, you must select the drive on which to install the IBM Security Key Lifecycle Manager database. A Windows drive indicator is a letter, following by a colon (:). For example, C:.

System action: Installation cannot continue until you correct the error.

User response: Enter a correctly formatted drive letter.

CTGKM9050E The DB Name must be 8 characters or less.

Explanation: The DB Name must be 8 characters or less.

System action: Installation cannot continue until you correct the error.

User response: Select a different name.

CTGKM9050I The Windows DB2 DB Home field must be a drive letter that can be written to.

Explanation: The drive must be writable for installation to proceed.

System action: Installation cannot continue until you correct the error.

User response: Use the operating system utilities to make the drive writable, or select a different drive.

CTGKM9051E The DB Name cannot contain special characters.

Explanation: The name contains one or more incorrect characters.

User response: Reenter the name and try again.

CTGKM9052E The DB Name must begin with an alphabetic character.

Explanation: The DB Name can only use alphabetical characters, numeric characters, and the underscore (A-Z, a-z, 0–9, and _).

System action: Installation cannot continue until you correct the error.

User response: Select a different name.

CTGKM9053E The DB2 version currently selected for use is not supported. The supported version is 10.1 and above.

Explanation: IBM Security Key Lifecycle Manager requires a supported version of DB2.

System action: The installation task fails.

User response: Obtain a supported version of DB2. Try again.

CTGKM9054E The location specified is not a valid DB2 installation directory

Explanation: The specified directory does not contain the existing DB2 installation.

User response: Select a valid DB2 installation directory.

CTGKM9055E The user name/password fields cannot have more than {0} characters.

Explanation: The value you specified exceeds the maximum length.

System action: Installation cannot continue until you correct the error.

User response: Specify a value that does not exceed the limit. Then, try the operation again.

CTGKM9056E Password and the confirmation does not match for {0}.

Explanation: The Password and Confirm Password fields must have the same value.

System action: Installation cannot continue until you correct the error.

User response: Specify the same value for the Password and Confirm Password fields, and try the operation again.

CTGKM9057E The Application Server Administrator Confirm Password field is empty.

Explanation: User has not specified the password confirmation value.

System action: Installation cannot continue until you correct the error.

User response: Enter a value in the Confirm Password field. Try again.

CTGKM9058E The Application Server Administrator User field is empty.

Explanation: This message is displayed when the Application Server Administrator User field is empty.

System action: Installation cannot continue until you correct the error.

User response: Specify a value and try again.

CTGKM9059E The IBM Security Key Lifecycle Manager Administrator User field is empty.

Explanation: This message is displayed when the IBM Security Key Lifecycle Manager Administrator User field is empty.

System action: Installation cannot continue until you correct the error.

User response: Specify a value and try again.

CTGKM9060E The user name field cannot contain any special characters.

Explanation: The user name contains one or more incorrect characters.

System action: Installation cannot continue until you correct the error.

User response: Reenter the user name with valid characters and try again.

CTGKM9061E The port specified is already in use.

Explanation: The port number that is entered must be available for use. The port number is already in use.

System action: Installation cannot continue until you correct the error.

User response: Select another port number. Ensure that the specified port number is available.

CTGKM9062E The IBM Security Key Lifecycle Manager Administrator Password field is empty.

Explanation: This message is displayed when the IBM Security Key Lifecycle Manager Administrator Password field is empty.

System action: Installation cannot continue until you correct the error.

User response: Specify a value and try again.

CTGKM9063E The Application Server Administrator Password field is empty.

Explanation: This message is displayed when the Application Server Administrator Password field is empty.

System action: Installation cannot continue until you correct the error.

User response: Specify a value and try again.

CTGKM9064E The Encryption Key Manager Property File field is empty.

Explanation: This message is displayed when the Encryption Key Manager Property File field is empty.

System action: Installation cannot continue until you correct the error.

User response: Specify a value.

CTGKM9065E The IBM Security Key Lifecycle Manager Administrator Confirm Password field is empty.

Explanation: User has not specified the password confirmation value.

System action: Installation cannot continue until you correct the error.

User response: Specify a value and try again.

CTGKM9066E IBM Security Key Lifecycle Manager Application Port Number is empty.

Explanation: This message is displayed when the IBM Security Key Lifecycle Manager Application Port Number field is empty.

System action: Installation cannot continue until you correct the error.

User response: Specify a value and try again.

CTGKM9067E The password for Database Administrator field is empty.

Explanation: This message is displayed when the password field for Database Administrator field is empty.

System action: Installation cannot continue until you correct the error.

User response: Specify a value and try again.

CTGKM9068E The password for keystore is empty.

Explanation: You must specify a password for the keystore.

User response: Specify a password for the keystore and try again.

CTGKM9069E The user name {0} or password is not valid.

Explanation: The operation requires a valid user name and password.

System action: The operation fails.

User response: Specify a valid user name and password. Then, try again.

CTGKM9070E The credentials could not be validated at the moment.

Explanation: The specified credentials might be incorrect.

System action: Installation cannot continue until you correct the error.

User response: Refer to the WebSphere Application Server logs for more information and correct the problem.

CTGKM9071E The WebSphere Application Server instance could not be started.

Explanation: The WebSphere Application Server instance could not be started.

System action: Installation cannot continue until you correct the error.

User response: Refer to the WebSphere Application Server logs for more information and correct the problem.

CTGKM9072E The DB2 installation details file {0} cannot be found.

Explanation: The DB2 instance data file was not found.

System action: Installation cannot continue until you correct the error.

User response: Ensure that the following files exist.

Windows systems

The `db2srcit.txt` file under the following directories:

- `C:\tklmv2properties`
- `C:\tklmtemp`
- `C:\sklmV25properties`

Linux and AIX systems

Check for the missing properties in the `db2unix.srcit` file under the following directories:

- `/tklmv2properties`
- `/tklmtemp`
- `/root/sklmV25properties`

CTGKM9073E DB2InstallResponseUpdater requires minimum {0} parameters. Only had {1} parameters.

Explanation: The installer is not passing in the correct parameters for a binary which it is trying to execute. This is an internal error which cannot be resolved by the Installation Manager.

System action: The installation fails.

User response: Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter S on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9074E File {0} does not exist.

Explanation: A binary which the installer is executing is attempting to access a file which does not exist. This is an internal error which cannot be resolved by the Installation Manager.

System action: The installation fails.

User response: Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter `S` on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9075E File {0} is not writable.

Explanation: A binary which the installer is executing is attempting to modify a read-only file. This is an internal error which cannot be resolved by the Installation Manager.

System action: The installation fails.

User response: Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter `S` on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9076E The specified path for existing DB2 installation is not valid.

Explanation: The specified path for existing DB2 installation is incorrect.

System action: Installation cannot continue until you correct the error.

User response: Specify the correct path. Then, try again.

CTGKM9077E The response file object is null.

Explanation: You must specify the response file.

User response: Specify a value. Then, try again.

CTGKM9078E {0} requires {1} parameters. Only had {2} parameters.

Explanation: The installer is not passing in the correct parameters for a binary which it is trying to execute. This is an internal error which cannot be resolved by the Installation Manager.

System action: The installation fails.

User response: Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter `S` on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9079E The file/folder specified by the path {0} does not exist on the file system.

Explanation: A binary which the installer is executing is attempting to access a file which does not exist. This is an internal error which cannot be resolved by the Installation Manager.

System action: The installation fails.

User response: Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter `S` on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9081E Error while executing the command {0}

Explanation: There was a problem when running the specified command.

System action: The installation fails.

User response: Check the Installation Manager log files and take necessary corrective actions. Then, try again.

CTGKM9082E Cannot find a running process for the server.

Explanation: There was a problem when trying to stop WebSphere Application Server.

System action: The installation fails.

User response: Manually start the server and try again.

CTGKM9083E Unable to determine the install location for WebSphere Application Server v8.5.

Explanation: The Installer could not identify the location of WebSphere Application Server, version 8.5.

System action: The installation fails.

User response: Uninstall Installation Manager and rerun the installation process.

CTGKM9084E Invalid DB2 installation details file. Cannot find an entry for {0}.

Explanation: The details present in the DB2 instance data file is incorrect.

System action: The installation fails.

User response:

Windows systems

Check for the missing properties in the `db2srcit.txt` file under the following directories:

- `C:\tklmv2properties`
- `C:\tklmtemp`
- `C:\sklmV25properties`

Linux and AIX systems

Check for the missing properties in the `db2unix.srcit` file under the following directories:

- `/tklmv2properties`
- `/tklmtemp`
- `/root/sklmV25properties`

CTGKM9086E No WebSphere Application Server installation found in the registry.

Explanation: Instance of the WebSphere Application Server, version 8.5 was not found in the install registry.

System action: Installation cannot continue until you correct the error.

User response: Uninstall Installation Manager and rerun the installation program.

CTGKM9087E Could not load data from the ports definition file {0}.

Explanation: The ports definition file for the WebSphere Application Server could not be read.

System action: Installation cannot continue until you correct the error.

User response: Clean up any existing installation and rerun the installation program.

CTGKM9088E The ports definition file {0} does not contain the required keys - {1}.

Explanation: Details in the ports definition file is incorrect.

System action: Installation cannot continue until you correct the error.

User response: Clean up any existing installation and rerun the installation program.

CTGKM9089E Could not get the key store file location.

Explanation: Keystore location was not found.

System action: Installation fails.

User response: Make sure that the Tivoli Key Lifecycle Manager database is up and running and rerun the installation program.

CTGKM9090E IBM DB2 and IBM WebSphere Application Server offerings must be selected for IBM Security Key Lifecycle Manager installation to proceed. Go back to the previous screen and select IBM DB2 v10.1 and IBM WebSphere Application Server v8.5 offerings.

Explanation: The details that you specified are incorrect.

User response: Specify the correct values.

CTGKM9091E IBM DB2 and IBM WebSphere Application Server offerings associated with IBM Security Key Lifecycle Manager must be selected for IBM Security Key Lifecycle Manager uninstallation to proceed. Go back to the previous screen and select IBM DB2 v10.1 and IBM WebSphere Application Server v8.5 offerings.

Explanation: The details that you specified are incorrect.

System action: Uninstallation cannot continue until you correct the error.

User response: Specify the correct values.

CTGKM9092E One or more prerequisites failed to meet the requirements. The report is given below.

Explanation: The prerequisite requirements for the installation are not met. All prerequisites must be satisfied for the installation.

System action: Installation cannot continue until you correct the error.

User response: Take corrective actions to meet the requirements. Then, try again.

CTGKM9093E None of the drives on the system has the required space ({0}) to install the product.

Explanation: The minimum space to install the product is not available in the system.

System action: Installation cannot continue until you correct the error.

User response: Increase the amount of space available on the specified drive to the minimum required. Then, try again.

CTGKM9094E Unable to read the prerequisite scanner results.

Explanation: The prerequisite output file was not found after Prerequisite Scanner is run.

System action: Installation cannot continue until you correct the error.

User response: Rerun the installation without deleting any files from the system.

CTGKM9096E The credentials provided for WebSphere Application Server Administrator is not valid.

Explanation: Incorrect credentials are specified for the WebSphere Application Server administrator.

System action: Installation cannot continue until you correct the error.

User response: Specify the correct user name and password for WebSphere Application Server administrator. Then, try again.

CTGKM9099E WebSphere Administrator credentials are required to proceed with uninstallation.

Explanation: The user name or password for WebSphere Application Server is not specified or incorrect.

User response: Specify the correct user name and password for the WebSphere Application Server administrator and then try again.

CTGKM9101E The path "<Variable formatSpec="{0}">VALUE_0</Variable>" is either on a network file system or not writable. Select a local file system path for installation.

Explanation: The installation is attempted on a location that is not on the local hard disk of the system.

System action: Installation cannot continue until you correct the error.

User response: Change the installation path and specify a local path on the system.

CTGKM9102E The path "<Variable formatSpec="{0}">VALUE_0</Variable>" is either on a network drive or not writable. Select a local drive for installation.

Explanation: The installation is attempted on a location that is not on the local hard disk of the system.

System action: Installation cannot continue until you correct the error.

User response: Change the installation path and specify a local path on the system.

CTGKM9103E Unable to find the location of prerequisite scanner tool.

Explanation: Location of Prerequisite Scanner was not found.

System action: Installation cannot continue until you correct the error.

User response: Rerun the installation without deleting any files from the system.

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 (IM)

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 the Language Selection panel, the Introduction panel, and the License Agreement panel.
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.

Error reports are most likely to occur immediately after the DB2 phase and middleware installation phase.

Important log files

The installation error logs provide critical information.

db2_install.log
DB2 installation log file.

db_config.log
Contains information about IBM Security Key Lifecycle Manager database creation and table creation.

***.out and *.err**
The `.err` file sizes are zero bytes if the operation they represent was successful. Examine error files with sizes greater than zero.

Log files to be used first

The timing of an error can provide an idea of which log file to use first. The two main 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, the only log file available might be `db2_install.log`.
2. If the error occurs later during this phase, the `sklmV25properties` 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 `sklmV25properties` directory to the <*IM logs*>`\sklmLogs` directory. See Table 11 for the location of the files.

During or immediately after the middleware installation phase

The first log file to examine for errors is `db_config.log`.

Log file names and locations

After installation, most error logs are in the *WAS_HOME*`\logs` directory.

For the approximate order in which you use error files during installation, see Table 11.

If migration occurs, there are also files in the <*IM App Data Dir*>`\logs\sklmLogs\migration.log` directory.

Table 11. Location of installation log files

Log file	Description	Location
`db2_install.log`	DB2 installation log.	Early in the installation, this file is here: **Windows systems:** `C:\<`*IM App Data Dir*`>\logs\sklmLogs` **AIX and Linux systems:** `/<`*IM App Data Dir*`>/logs/sklmLogs`
`db_config.log`	Contains information about database creation and table creation.	**Windows systems:** `C:\<`*IM App Data Dir*`>\logs\sklmLogs` **AIX and Linux systems:** `/<`*IM App Data Dir*`>/logs/sklmLogs`
Various `*.xml` and `*.log` files	IBM Security Key Lifecycle Manager installation log files.	**Windows systems:** `C:\<`*IM App Data Dir*`>\logs` **AIX and Linux systems:** `/<`*IM App Data Dir*`>/logs`
Various `*.out` and `*.err` files	STDOUT and STDERR files that are generated during installation.	*WAS_HOME*`\logs`
`migration.log`	Migration events.	`<`*IM App Data Dir*`>\logs\sklmLogs\migration.log`
`results.txt`	Contains the results for Prerequisite Scanner.	`%temp%/sklmPRS/results.txt`

Migration log file names and location

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

If migration fails, examine the migration log files in the `<IM App Data Dir>\logs\sklmLogs\migration.log` directory.

Examining an error log file

You must review the log files to examine an error log file.

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 be used first” on page 115 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 carry out several actions that might provide more information to verify installation.

- Check your free disk space. See “Hardware requirements for distributed systems” on page 9 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, navigate 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 `sklmdb2` 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, navigate 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, navigate 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 navigating 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.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

Index