IBM Security Key Lifecycle Manager
Version 4.0

Installing

Note

Before you use this information and the product it supports, read the information in “Notices” on page 145.

Contents

Chapter 1. Installing

IBM Security Key Lifecycle Manager installation process involves planning activities, installation steps, and postinstallation tasks.

Installation process overview

Complete the following steps to plan, install, and configure IBM Security Key Lifecycle Manager.

1. Complete the preinstallation tasks.
2. Install IBM Security Key Lifecycle Manager.
3. Complete the postinstallation tasks.

Note: Installation might take more than half an hour.

Preinstallation tasks

Before you install IBM Security Key Lifecycle Manager, understand the prerequisites and plan your environment accordingly.

Complete the following prerequisite tasks:

- Ensure that the system meets the minimum hardware and software requirements. For more information, see IBM Security Key Lifecycle Manager Support Matrix.
- Use the preinstallation worksheets for planning.
- Determine the IBM Security Key Lifecycle Manager topology.
- Decide the installation mode you want to use to install IBM Security Key Lifecycle Manager: graphical mode or silent mode.

Preinstallation worksheets

Before you install and configure IBM Security Key Lifecycle Manager, you can complete the preinstallation worksheets to define the configuration parameters that are required to complete the IBM Security Key Lifecycle Manager installation.

The preinstallation worksheets list all of the values that you must specify during an IBM Security Key Lifecycle Manager installation process. Completing the preinstallation worksheets before you install the components can help you plan your installation, save time, and enforce consistency during the installation and configuration process.

General installation parameters

Use the worksheet to record general installation parameters.

Table 1. 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 the available free disk space.	Ensure that you have enough free disk space available.	For values, see https://www.ibm.com/support/pages/ibm-security-key-lifecycle-manager-support-matrix.	

Table 1. General installation parameters (continued)			
Option	**Description**	**Default or example value**	**Your value**
Installation Directory - IBM Installation Manager	Directory in which to install IBM Installation Manager.	**Windows** *drive*:\Program Files\IBM\Installation Manager\eclipse **AIX and Linux** /opt/ibm/InstallationManager/eclipse	
Installation Directory - IBM DB2	Directory in which to install IBM DB2.	**Windows** *drive*:\Program Files\IBM\DB2SKLMV40 **AIX and Linux** /opt/ibm/DB2SKLMV40	
Installation Directory - IBM WebSphere® Application Server	Directory in which to install WebSphere Application Server.	**Windows** *drive*:\Program Files\IBM\WebSphere\AppServer **AIX and Linux** /opt/IBM/WebSphere/AppServer/bin	
Installation Directory - IBM Security Key Lifecycle Manager	Directory in which to install IBM Security Key Lifecycle Manager.	**Windows** C:\Program Files\IBM\SKLMV40 **AIX and Linux** /opt/IBM/SKLMV40	

Db2 configuration parameters

Use the worksheet to record your entries that are related to the installation and configuration of Db2®.

Table 2. Db2 configuration parameters			
Field name	**Description**	**Default or example value**	**Your value**
Installation Directory - Db2	Directory in which to install Db2.	**Windows** *drive*:\Program Files\IBM\DB2SKLMV40 **AIX and Linux** /opt/IBM/DB2SKLMV40	
Install DB2 or Use an existing installation of DB2	Specify whether to use an existing DB2 instance or a new DB2 installation.	If an existing DB2 instance is used, you must specify the DB2 installation location and the other details.	

Table 2. Db2 configuration parameters (continued)			
Field name	**Description**	**Default or example value**	**Your value**
Db2 Administrator ID	User ID for the IBM Security Key Lifecycle Manager database administrator (also called the instance owner).	`SKLMDB40`	
Db2 Administrator Password	Password for the database administrator user ID.		
Database Name	Name of the IBM Security Key Lifecycle Manager database.	`SKLMDB40`	
Db2 Port	Db2 service listening port.	`50060`	

Administrator / Database Home	Directory where the database instance and formatted tables are created.	**Windows**
		`C:`
		Linux and AIX
		`/home/sklmdb40`	

Administrator group	Operating system user group in which the instance owner of the database is a member on Linux or AIX systems.	-	

WebSphere Application Server and IBM Security Key Lifecycle Manager server configuration parameters

Use the configuration worksheet to record your entries for installation and configuration of the application server, which is used to host your IBM Security Key Lifecycle Manager server.

Table 3. WebSphere Application Server configuration parameters			
Field name	**Description**	**Default or example value**	**Your value**
User Name	Specifies the WebSphere Application Server login user ID for the IBM Security Key Lifecycle Manager Administrator profile.	`wasadmin`	
Password	Specifies the WebSphere Application Server password for the IBM Security Key Lifecycle Manager profile.		

Table 3. WebSphere Application Server configuration parameters (continued)			
Field name	**Description**	**Default or example value**	**Your value**
HTTPS Admin Port	Specifies the WebSphere Application Server port for the IBM Security Key Lifecycle Manager profile.	9083	

Table 4. IBM Security Key Lifecycle Manager configuration parameters			
Field name	**Description**	**Default or example value**	**Your value**
User Name	Specifies the user ID to administer IBM Security Key Lifecycle Manager.	SKLMAdmin	
Password	Specifies the password for the IBM Security Key Lifecycle Manager administrator.		
HTTPS Port Number	Specifies the secure port to access IBM Security Key Lifecycle Manager.	9443	
HTTP Port Number	Specifies the non-secure port to access IBM Security Key Lifecycle Manager.	9080	

Types of installation

You can install IBM Security Key Lifecycle Manager in graphical user interface or silent mode.

- 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.

Notes:

- IBM Security Key Lifecycle Manager does not support a console mode installation.
- Do not install IBM Security Key Lifecycle Manager 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.

Run the following steps to install IBM Security Key Lifecycle Manager in graphical mode.

- Start the installation wizard.
- Complete the installation wizard pages by entering the configuration options. For details, see “Installing IBM Security Key Lifecycle Manager in graphical mode” on page 10.

- Verify that IBM Security Key Lifecycle Manager server is operational.

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 must select the locale that you want to use for the installation process. The locale determines the language that the installer runs in. Type the number that is displayed next to your locale and press Enter.

You might see these panels during installation:

1. Installation Manager window with installation packages such as IBM Installation Manager, IBM DB2, IBM WebSphere Application Server, and IBM Security Key Lifecycle Manager
2. Software license agreement
3. Installation directory selection for IBM Installation Manager and the other installation packages.
4. Language selection for package translation
5. Package features selection for installation
6. Db2 configuration options
7. IBM Security Key Lifecycle Manager configuration options
8. Encryption Key Manager migration selection
9. Installation package preview
10. Installation progress for IBM Security Key Lifecycle Manager
11. 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. Introduction
2. Software license agreement
3. Db2 directory
4. **Migration information**
5. **Migration summary**
6. Summary of prerequisites
7. Installation progress for Db2
8. Beginning IBM Security Key Lifecycle Manager installation
9. Installation directory for IBM Security Key Lifecycle Manager and WebSphere Application Server
10. WebSphere Application Server information
11. SKLMAdmin password
12. Pre-installation summary
13. Migration progress for IBM Security Key Lifecycle Manager
14. 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 needed 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. For more information about silently installing IBM Security Key Lifecycle Manager, see "Installing IBM Security Key Lifecycle Manager in silent mode" on page 11.

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

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.

Stand-alone deployment of IBM Security Key Lifecycle Manager server

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, processor speed, and available disk space to meet the workload.

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

Figure 1. Main components of IBM Security Key Lifecycle Manager server

Default users

When you install IBM Security Key Lifecycle Manager, some default administrator users are created with the necessary permissions to administer the product.

Installation of IBM Security Key Lifecycle Manager provides default administrator user IDs of `WASAdmin`, `SKLMAdmin`, and `sklmdb40`.

The 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.

The following table provides the default user IDs and guidance on specifying their passwords. Also, see "Password policy" on page 70.

Table 5. Administrator user IDs and passwords

User	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 5. Administrator user IDs and passwords (continued)

User	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 5. Administrator user IDs and passwords (continued)		
User	**User ID**	**Password**
Instance owner of the database	**Windows, Linux, or AIX systems:** The default value is `sklmdb40`. 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 `sklmdb40`. 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 a password" on page 40. .
Database instance	The administrator ID `sklmdb40` owns a Db2 instance named `sklmdb40`.	

Installing IBM Security Key Lifecycle Manager

The IBM Security Key Lifecycle Manager installer can run in two modes, such as graphical mode and silent mode. Select a mode that suits your requirements when you install or migrate IBM Security Key Lifecycle Manager.

Installation guidelines

For a successful installation, ensure that you understand and follow the rules and guidelines to install IBM Security Key Lifecycle Manager.

- On a Linux or AIX operating system, ensure that Bash shell (bash) and C shell (sch) are installed. Also, ensure that bash is the default shell.
- On a Linux operating system, ensure that SELinux is disabled and umask is set to `022`.
- Installation can take more than an hour.
- Do not install from a network drive or mounted drive.
- 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.
- If you are using an existing user as Db2 Administrator, ensure that the password is correctly specified.
- When you install IBM Security Key Lifecycle Manager on Linux, 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.
- Ensure that the host name of the system is set correctly.

- Entries for all fields are restricted to alphabetical characters (A-Z and a-z), numeric characters (0-9), and , and the underscore character (_). Additionally, the password fields allow selected special characters. For more information, see Supported special characters in passwords.

  The restriction also applies to the values in the response file that is used for silent installation.
- Ensure that the installation path does not contain Unicode characters.
- Ensure that there are no non-ASCII characters in the installation path.
- 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.
- Do not install IBM Security Key Lifecycle Manager on systems with hardened operating system.

  In a hardened system, you might have restricted access to the specific directories, or you might not be a part of the administrator group. On Windows, you might not have access to certain directories in the system even if you are part of the administrator group. To install IBM Security Key Lifecycle Manager, you must have access to all the installation directories with Read, Write, and Execute permissions.

Installing IBM Security Key Lifecycle Manager in graphical mode

Use the IBM Installation Manager installation wizard to install IBM Security Key Lifecycle Manager and its components in a graphical user interface mode.

Before you begin

- Complete the planning tasks.
- Download and extract the files for IBM Security Key Lifecycle Manager to a directory. These files are available for download from the IBM Passport Advantage website.
- Review the considerations and restrictions for installing and configuring IBM Security Key Lifecycle Manager.

About this task

When you start the installation process from the Launchpad program, IBM Installation Manager is automatically installed if it is not already on your system. When the installation task is complete, IBM Security Key Lifecycle Manager is installed along with the installation of required middleware components, such as WebSphere Application Server and DB2 on the same system.

Procedure

1. Go to the directory of your installation package and open `disk1`. For example: *`download_path`*`/disk1`
2. Start the installation program.

Operating system	Command to run
Windows	**`launchpad.bat`**
Linux or AIX	**`launchpad.sh`**

3. Select the locale that you want to use for the installation process. The locale determines the language that the installer runs in. Type the number that is displayed next to your locale and press Enter. The Installation Manager wizard is displayed.
4. In the **Install Packages** window, click each of the product packages to highlight them. The description of the package is displayed in the **Details** section at the bottom of the window. To fully understand the package that you are installing, review all information.
5. Select the product packages to install. All the packages are selected for installation by default.
6. Click **Next**.

   The prerequisite checks verify the prerequisite requirements for the installation.

7. Select **I accept the terms in the license agreements** and click **Next**.
8. Select a location for the shared resources directory and click **Next**.

   Note: Retain the default path for shared resources directory, for example, `C:\Program Files\IBM\IBMIMShared`. IBM Installation Manager uses this location to download artifacts and to store information about the installed packages.
9. On the **Location** page, review the installation location for each package group, and click **Next**.

   Note: You can change the installation locations of the package groups. Ensure that the non-administrator or non-root user account has access to the locations that you specify.
10. Select the translation packages to install and click **Next**.
11. On the **Features** page, select the package features to install.
    a. To see the dependency relationships between features, select **Show dependencies**.
    b. Click a feature to view its brief description under **Details**.
    c. When you are finished selecting features, click **Next**.
12. On the **Configuration for IBM DB2** page, specify the database configuration information and click **Next**.

    For more details about DB2 configuration, see DB2 configuration parameters and DB2 configuration during installation.
13. On the **Configuration for IBM Security Key Lifecycle Manager** page, specify the configuration information for IBM Security Key Lifecycle Manager and WebSphere Application Server. Then, click **Next**.

    For more configuration details, see WebSphere Application Server and IBM Security Key Lifecycle Manager server configuration parameters and Configuration during installation.
14. Click **Next**.
15. On the **Summary** page, review your choices before you install the product package. To change a selection, click **Back** to return to your selections.
16. To begin the installation, click **Install**.

    A progress indicator shows the percentage of the installation that is completed. When the installation process is complete, a message confirms the completion of the process.
17. Click **View Log File** to open the installation log file and to verify that all of the components were installed properly.
18. In the Install Package wizard, select **None** to instruct the installer not to create a profile.
19. Click **Finish** to complete the installation task and to close the wizard.

What to do next

Before you use IBM Security Key Lifecycle Manager, run the postinstallation tasks that are described in Postinstallation steps.

Installing IBM Security Key Lifecycle Manager in silent mode

You can install IBM Security Key Lifecycle Manager in silent installation mode. This installation method is useful if you want identical installation configurations on multiple workstations. Silent installation requires a response file that defines the installation configuration.

Before you begin

- Complete the planning tasks.
- Download and extract the files for IBM Security Key Lifecycle Manager to a directory. These files are available for download from the IBM Passport Advantage website.
- Review the considerations and restrictions for installing and configuring IBM Security Key Lifecycle Manager.

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

  The response files are available in the root directory of the installation image files.

  Note: You can change the installation locations (**installLocation** parameter in the response file) of the package groups. Ensure that the non-administrator or non-root user account has access to the locations that you specify.

Procedure

1. Edit the repository location information and other details in the response file. The sample response files are in the directory in which your installation package is located.

   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.

   You must update the response file with the correct repository location. The repository location is the place where your installation package is located.

   ```
   <repository location='<user repository location>\im'/>
   <repositoryima location='<user repository location>\'/>
   ```

   If you have extracted the installation package in `C:\sklm40`, update repository location in the `SKLM_install_Win_Resp.xml` response file as shown in the following example.

   ```
   <repository location='<C:\sklm40\disk1\im'>\im'/>
   <repository location='<C:\sklm40\disk1\'/>
   ```

2. To add the encrypted passwords to the relevant elements of the response file, use the IBM Installation Manager utility to create encrypted passwords.

   For information about how to encrypt the password, see Encrypted password for response file elements.

3. Open a command prompt and run the silent installation command.

   Windows
   Go to the *<installation package directory>*`\disk1` directory and run the following command.

   ```
   silent_install.bat SKLM_Silent_Win_Resp.xml -acceptLicense
   ```

   Linux
   Go to the *<installation package directory>*`/disk1` directory and run the following command.

   ```
   silent_install.sh SKLM_Silent_Linux_Resp.xml -acceptLicense
   ```

4. Verify that the installation was successful by reviewing the log files. You can view the Installation Manager logs at the following locations.

   Windows
   `drive:\`*<IM_DATA_DIR>*`\logs\native`.

   For example, `C:\ProgramData\IBM\Installation Manager\logs\native`.

   `drive:\`*<IM_DATA_DIR>*`\logs\sklmLogs\`.

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

   Linux
   /<*IM_DATA_DIR*>`/logs/native`.

   For example, `/var/ibm/installationmanager/logs/native`.

   /<*IM_DATA_DIR*>`/logs/sklmLogs/`.

For example, `/var/ibm/InstallationManager/logs/sklmLogs/`.

For the definition of *<IM_DATA_DIR>*, see "Definitions for HOME and other directory variables" on page 71.

What to do next

Before you use IBM Security Key Lifecycle Manager, run the postinstallation tasks that are described in "Postinstallation tasks" on page 22.

Encrypted password for response file elements

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.

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.sklm40.db2.win.ofng'
value='<encrypted password>'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm40.db2.win.ofng'
value='<encrypted password>'/>
...
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm40.win'
value='<encrypted password>'/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm40.win'
value='<encrypted password>'/>
...
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm40.win'
value='<encrypted password>'/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm40.win'
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.sklm40.db2.lin.ofng'
value='<encrypted password>'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm40.db2.lin.ofng'
value='<encrypted password>'/>
...
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm40.linux'
value='<encrypted password>'/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm40.linux'
value='<encrypted password>'/>
...
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm40.linux'
value='<encrypted password>'/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm40.linux'
value='<encrypted password>'/>
```

You can create a different encrypted password for each user.

Db2 configuration during installation

The IBM Security Key Lifecycle Manager installation process installs and configures Db2 Advanced Workgroup Server Edition.

Review the following scenarios and suggested actions before you configure Db2 during installation:

- If an existing copy of Db2 Advanced Workgroup Server Edition is installed as the root user at the correct version for the operating system, you can use the existing Db2 Advanced 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 Advanced 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 `DBSKLMV40`.
- If an earlier version of IBM Security Key Lifecycle Manager and an earlier version of Db2 exist on the system, the installation process does not auto-detect the existing version, and installs Db2 Advanced Workgroup Server Edition at a version that depends on the operating system.

  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 Advanced 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 `DBSKLMV40`.
- If no IBM Security Key Lifecycle Manager, no copy or earlier version of Db2 exist on the system, the installation process installs Db2.

  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 Linux or AIX systems, 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 71.

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 Linux or AIX system, 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.

Db2 Administrator Password
The password for the administrator.

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 a password, ensure that the other one is changed too.

Note: If you are using an existing user as Db2 Administrator, ensure that the password is correctly specified during installation.

Database Name
Name of the IBM Security Key Lifecycle Manager database, SKLMDB40.

Db2 Port
The port that Db2 uses.

Administrator's Group
Access group in which the Administrator user ID exists.

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:

- Entries for all fields are restricted to alphabetical characters (A-Z and a-z), numeric characters (0-9), and , and the underscore character (_). Additionally, the password fields allow selected special characters. For more information, see Supported special characters in passwords.

  The restriction also applies to the values in the response file that is used for silent installation.
- Do not specify spaces in any of the directory paths or file names.
- 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 (_).
- If you are using an existing user as Db2 Administrator, ensure that the password is correctly specified during installation.
- The Db2 admin group name cannot be longer than 8 characters.

Db2 user ID restrictions and requirements

You must ensure that the DB2 administrator user ID meets the specific requirements and restrictions.

- 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.

WebSphere Application Server and IBM Security Key Lifecycle Manager server configuration during installation

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

Application Server Administration

User Name
Specifies the WebSphere Application Server login user ID for the IBM Security Key Lifecycle Manager administrator profile.

Password
Specifies the WebSphere Application Server password for the IBM Security Key Lifecycle Manager profile. For more information about the supported special characters, see https://www.ibm.com/support/pages/supported-special-characters-ibm-security-key-lifecycle-manager-passwords.

HTTPS Admin Port
Specifies the HTTPS port to access WebSphere Integrated Solutions Console for the IBM Security Key Lifecycle Manager profile.

Default value is 9083.

IBM Security Key Lifecycle Manager Application Administration

User Name
Specifies the user ID to administer IBM Security Key Lifecycle Manager.

Password
Specifies the password for the IBM Security Key Lifecycle Manager administrator. For more information about the supported special characters, see https://www.ibm.com/support/pages/supported-special-characters-ibm-security-key-lifecycle-manager-passwords.

HTTPS Port Number
Specifies the secure port to access IBM Security Key Lifecycle Manager.

Default value is 9443.

HTTP Port Number
Specifies the non-secure port to access IBM Security Key Lifecycle Manager.

Default value is 9080.

Note:

The **User Name** string cannot contain leading and trailing spaces, and cannot contain the following 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

Setting up Multi-Master cluster on a cross-migrated IBM Security Key Lifecycle Manager server

You can set up a Multi-Master cluster on an IBM Security Key Lifecycle Manager server that is cross-migrated from any of the earlier versions.

Before you begin

Ensure that the IBM Security Key Lifecycle Manager server on which you want to set up the Multi-Master cluster is cross-migrated to version 4.0.

Procedure

1. In the SKLMConfig.properties file, update the **TransportListener.ssl.protocols** property to the value: TLSv1.2.

   ```
   TransportListener.ssl.protocols=TLSv1.2
   ```

   You can use the "Update Config Property REST Service" on page 43 or the "tklmConfigUpdateEntry" on page 48 CLI command to update the property.
2. Stop the IBM Security Key Lifecycle Manager Agent.
3. Restart the IBM Security Key Lifecycle Manager server.
4. During the restore process, if you specified the **RESTORE_USER_ROLES** property as RESTORE_USER_ROLES=y in the restoreV*version* utility (For example, restoreV25.bat), refresh the user credentials on the IBM Security Key Lifecycle Manager server:
   a) Log on to the IBM Security Key Lifecycle Manager graphical user interface.
   b) Click **Administration** > **Multi-Master**.
   c) On the page, click the **Multi-Master** link and in the **Confirm** dialog box, click **OK**.
   d) In the **Masters** table, select the master server and click **Modify Master**.
   e) In the **Multi-Master Configuration - Modify Master** window, specify the values for the **IBM Security Key Lifecycle Manager password** and **WebSphere Application Server password**.
   f) Click **Accept host certificate automatically** and click **Update**.
   g) In the information message dialog box with the message Successfully modified the master, click **Close**.
   h) Click **Cancel**.

   The IBM Security Key Lifecycle Manager master server is setup as the primary master.

What to do next

You can now add standby and non-HADR master servers to the cluster. For more information, see "Adding a standby master server to a cluster" on page 51 and "Adding a master server to a cluster" on page 49.

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

```
\<IM_DATA_DIR>\logs
```

Linux or AIX

```
/<IM_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.

For more information, see https://www.ibm.com/support/pages/ibm-security-key-lifecycle-manager-support-matrix.

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 `sklmdb40` administrator using Windows user and group management tool requires removing the previous `sklmdb40` 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 `sklmdb40` 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 2012: *drive*`:\Users`
2. Remove the `sklmdb40` subdirectory.
3. Reinstall IBM Security Key Lifecycle Manager. The `sklmdb40` subdirectory is not automatically removed when you use the Windows user and group management tool to delete the user account `sklmdb40`.

Non-root installation of IBM Security Key Lifecycle Manager on Linux systems

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

Best practices and guidelines for a non-root installation of IBM Security Key Lifecycle Manager on Linux systems

When you plan your non-root installation of IBM Security Key Lifecycle Manager on Linux systems, there are a number of best practices to consider. Review these best practices before you start your installation.

- Ensure that the non-root user belongs to a non-root primary group. The non-root user must have a primary group other than `guests`, `admins`, `users`, and `local`.
- The home directory for non-root user ($HOME) must point to the correct location. For example: `/home/<user_name>`
- Verify that the previous installation (if any) of IBM Security Key Lifecycle Manager and Db2 in the system are removed without any remnants.
- When you install IBM Security Key Lifecycle Manager, Prerequisite Scanner for non-root installation might fail. Ensure that all the prerequisites that are indicated in the Prerequisite Scanner check are met except for the requirement for Administrator privileges before you proceed with the installation.

  To continue with the installation, skip running Prerequisite Scanner. To skip the prerequisite scan, create `sklmInstall.properties` file in the `/tmp` directory with the following property.

```
SKIP_PREREQ=true
```

- Ensure that the kernel settings at the operating-system level are correct for Db2 installation. For more information about Db2 kernel settings, see Db2 documentation at: http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
- During the installation, ensure that the database Administrator ID is the same as the non-root user who is logged on to the system for running the installation process. Ensure the following requirements for the database Administrator ID:
  - Maximum length of the database Administrator ID is 8 characters.
  - Password for the database Administrator ID is the same as the operating system level password for the non-root user.
  - Database Administrator group is the same as the primary group of the non-root user at the operating system level.
  - Database home points to the home directory of the non-root user.
- You cannot install IBM Security Key Lifecycle Manager as a non-root user in silent mode.
- Migration from the earlier versions of IBM Security Key Lifecycle Manager (1.0, 2.0, 2.0.1, 2.5, 2.6, 2.7, and Encryption Key Manager) to non-root installation of version 4.0 is not supported.
- Db2 might not start on system boot when installed as a non-root user. Correct by starting Db2 before WebSphere Application Server starts. Run the `nonrootconfig.sh` script after installer completed the installation.
- The Db2 admin group name cannot be longer than 8 characters.
- After you run the nonrootconfig.sh command, and when WebSphere Application Server is started, you might get the error message `No DB connected` on IBM Security Key Lifecycle Manager user interface. To resolve this issue, restart Db2 and WebSphere Application Server.

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.

Before you begin

- Configure the WebSphere Application Server (WAS), and other ports to be greater than 1024. For example, 1180. You cannot use privileged ports (ports < 1024).
- Ensure that the non-root user belongs to a non-root primary group. The non-root user must have a primary group other than guests, admins, users, and local.
- See Non-root Db2 installation.

About this task

Before you install IBM Security Key Lifecycle Manager on Linux systems as a non-root user, review the best practices information in the "Non-root installation of IBM Security Key Lifecycle Manager on Linux systems" on page 18 topic.

Procedure

1. Ensure that your target environment meets the IBM Security Key Lifecycle Manager installation prerequisites. See "Preinstallation tasks" on page 1.
2. Create a non-root User ID. Ensure that the User ID has a primary group other than `guests`, `admins`, `users`, and `local`.
3. Skip running Prerequisite Scanner by creating `sklmInstall.properties` file in the `/tmp` directory with the following property.

   ```
   SKIP_PREREQ=true
   ```

4. Go to the directory of your installation package and open `disk1`.

For example, *download_path*/disk1.

5. Open a command line window and run **launchpad.sh**.
6. Specify the Db2 configuration parameters. See “Db2 configuration during non-root installation” on page 21.
7. Specify the WebSphere Application Server configuration parameters.
8. After the IBM Security Key Lifecycle Manager installation process is complete, open the command line window.
9. Stop WebSphere Application Server and Db2.

   Note: Ensure that you perform this step as the non-root user that you created in step 2.

   Run the following command to stop WebSphere Application Server.

   ```
   cd <WAS_HOME>/bin
   ./stopServer.sh <server name> -username <WAS Admin User ID> -password <WAS Admin password>
   ```

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

   Run the following command to stop Db2.

   ```
   cd ~/sqllib/adm
   ./db2stop
   ```

10. Open a new shell and run the following command under /home/username/sklm40properties/scripts.

    Non-root Db2 installation requires root access to configure Db2 instance with a specific port number and service name.

    ```
    sudo nonrootconfig.sh <DB_INST_HOME> <DB_INST_NAME> <PORT> <DB_USER> <DB_PASSWORD>
    <WAS_HOME> <WAS_USER> <WAS_PASSWORD>
    ```

    For example, **sudo nonrootconfig.sh /home/testuser testuser 50060 testuser mydbpwd /home/testuser/IBM/WebSphere/AppServer wasadmin mypwd** .

    Where,

    <DB_INST_HOME> - the directory that contains the Db2 database instance. For example, /home/testuser.

    <DB_INST_NAME> - the Db2 instance name. For example, testuser.

    <PORT> - Db2 service listening port. For example, 50060.

    <DB_USER> - Db2 user name. For example, testuser.

    <DB_PASSWORD> - Db2 password. For example, mydbpwd.

    <WAS_HOME> - the WebSphere Application Server home directory. For example, /home/testuser/IBM/WebSphere/AppServer.

    <WAS_USER> - WebSphere Application Server user name. For example, wasadmin.

    <WAS_PASSWORD> - WebSphere Application Server password. For example, mypwd.

    When you run the script, you are prompted to provide password for the Db2 user name to continue with installation.

11. Restart WebSphere Application Server.

    Note: Ensure that you perform this step as the non-root user that you created in step 2.

    ```
    cd WAS_HOME/bin
    ./startServer.sh server name
    ```

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

What to do next

- In the *SKLM_HOME*/config/SKLMConfig.properties file, update the SSL port number to be greater than 1024 by using the graphical user interface, command-line interface, or REST interface. For example,

```
TransportListener.ssl.port=1441
```

- Restart the IBM Security Key Lifecycle Manager server.

  After the installation, you must log in as a non-root user to start or stop IBM Security Key Lifecycle Manager server and Db2 server.

Db2 configuration during non-root installation

IBM Security Key Lifecycle Manager requires Db2 Advanced Workgroup Server Edition at a version 11.1.2.2 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 the same as the User ID who is logged on to the system. Ensure that the maximum length of the ID is 8 characters.

Db2 Administrator Password
: The password for the administrator. Ensure that the maximum length of the password is 20 characters.

  The password for the Db2 Administrator user ID is subject to the security policy active on the system. Password for Db2 Administrator ID must be same as the operating system level password for the non-root user who is logged on to the system. When you change one, you must change the other.

Database Name
: The name of the IBM Security Key Lifecycle Manager database, which is SKLMDB40.

Db2 Port
: The port that Db2 uses.

Administrator's Group
: Access group in which the Administrator user ID exists. Database Administrator group must be same as the primary group for the non-root user at operating system level.

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. Database home must point to the home directory of the non-root user.

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 (_).
4. The Db2 admin group name cannot be longer than 8 characters.

For more information about how to modify kernel parameters and non-root installation, see Db2 documentation.

- http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
- http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0050571.html

Postinstallation tasks

Complete the following postinstallation tasks in the given order to verify the installation and to ensure that the product is functional.

Validating services, ports, and processes

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

Note: From IBM Security Key Lifecycle Manager 4.0, the IBM Security Key Lifecycle Manager processes now run under a non-administrator or non-root user account even when you install the product under an administrator or root user account.

Ensure that clients or devices that use IPP to communicate with the IBM Security Key Lifecycle Manager server use the same IPP port number (Default: 1441) that is configured on the server.

Windows

Services

Component	Service Name
WebSphere Application Server	`IBM WebSphere Application Server V9.0 - SKLM40Server`
Db2	`DB2SKLMV40 - SKLMDB40`

Note: The processes run under the Db2 Administrator user account. User credentials for this account are specified during installation. For more information, see "Db2 configuration during installation" on page 14.

Ports

The following ports must be open for communication and not used by any other processes.

Note: If you changed the ports during installation, you can determine the port number. See "Checking the current port number" on page 24.

Description	Port Number
FCM (Fast Communication Manager) port. You cannot configure this port. Its value is fixed. IBM Security Key Lifecycle Manager requires this port for Db2 installation.	60060
Default HTTPS port to access IBM Security Key Lifecycle Manager graphical user interface and REST services. You can configure this port at the time of IBM Security Key Lifecycle Manager installation.	9443
Default HTTP port to access IBM Security Key Lifecycle Manager graphical user interface. You can configure this port at the time of IBM Security Key Lifecycle Manager installation.	9080
Default HTTPS port to access WebSphere Integrated Solutions Console. You can configure this port at the time of IBM Security Key Lifecycle Manager installation.	9083

Description	Port Number
Default port 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.	50060
Default installation time SSL port that listens for KMIP messages.	5696
SSL port for device messages.	1441
TCP port for device messages.	3801
WebSphere Application Server installation requires these ports for various services it provides.	9080 - 9099
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).	-
Default port for IBM Security Key Lifecycle Manager agent.	60015

Processes

Name	Process
IBM Security Key Lifecycle Manager	`WASService.exe` and `java.exe`
Db2	`db2fmp64.exe` and `db2syscs.exe`

Linux

Ports

The following ports must be open for communication and not used by any other processes.

Note: If you changed the ports during installation, you can determine the port number. See "Checking the current port number" on page 24.

Description	Port Number
FCM (Fast Communication Manager) port. You cannot configure this port. Its value is fixed. IBM Security Key Lifecycle Manager requires this port for Db2 installation.	60060
Default HTTPS port to access IBM Security Key Lifecycle Manager graphical user interface and REST services. You can configure this port at the time of IBM Security Key Lifecycle Manager installation.	9443
Default HTTP port to access IBM Security Key Lifecycle Manager graphical user interface. You can configure this port at the time of IBM Security Key Lifecycle Manager installation.	9080

Description	Port Number
Default HTTPS port to access WebSphere Integrated Solutions Console. You can configure this port at the time of IBM Security Key Lifecycle Manager installation.	9083
Default port 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.	50060
Default installation time SSL port that listens for KMIP messages.	5696
SSL port for device messages.	1441
TCP port for device messages.	3801
WebSphere Application Server installation requires these ports for various services it provides.	9080 - 9099
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).	-
Default port for IBM Security Key Lifecycle Manager agent.	60015

Processes

Component	Process
IBM Security Key Lifecycle Manager	WebSphere Application Server and Java
Db2	`db2fmp64` and `db2syscs`

Checking the current port number

Use the property values that are available in the *WAS_HOME*`/profiles/KLMProfile/properties/portdef.props` file to determine the current secure and non-secure port numbers for the IBM Security Key Lifecycle Manager server and the WebSphere Integrated Solutions Console.

About this task

The following table provides the property details:

Table 6. Properties in `WAS_HOME/profiles/KLMProfile/properties/portdef.props` file for secure and non-secure port numbers

Property	Description	Default value
`WC_adminhost_secure`	WebSphere Integrated Solutions Console secure port	9083
`WC_adminhost`	WebSphere Integrated Solutions Console non-secure port	9443
`WC_defaulthost_secure`	IBM Security Key Lifecycle Manager server secure port	9061

Table 6. Properties in WAS_HOME/profiles/KLMProfile/properties/portdef.props file for secure and non-secure port numbers (continued)		
Property	**Description**	**Default value**
WC_defaulthost	IBM Security Key Lifecycle Manager server non-secure port	9080

Logging in to IBM Security Key Lifecycle Manager and WebSphere Application Server

Obtain the login URL and use the default administrator user credentials to log in to the product web interface.

Default administrative users

Use information from the following topic: "Default users" on page 6

Login URL for IBM Security Key Lifecycle Manager

To access the IBM Security Key Lifecycle Manager web interface, use the following login URL:

```
https://hostname or IP address:port/ibm/SKLM/login.jsp
```

The value of *hostname* or *ip-address* is the name of the host system or IP address or DNS address of the IBM Security Key Lifecycle Manager server.

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

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL. For example:

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

Do not use a port value greater than 65520.

On Windows systems, the information is on the Start screen:

1. On the desktop, hover the mouse cursor in the lower left corner of the screen, and click when the thumbnail of the Start screen appears.
2. Click the down arrow in the lower-left corner of the **Start** screen.
3. Click **IBM Security Key Lifecycle Manager** > **Launch IBM Security Key Lifecycle Manager Application**.

Short login URL for IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Manager has a short login URL that you can easily remember.

Short login URL to access IBM Security Key Lifecycle Manager when default port 9080 (HTTP) or 9443 (HTTPS) is used:

```
http://hostname or ip-address:9080
```

```
https://hostname or ip-address:9443
```

Short login URL to access IBM Security Key Lifecycle Manager when you use custom ports instead of the default ports:

```
http://hostname or ip-address:port/
```

```
https://hostname or ip-address:port/
```

Login URL for WebSphere Application Server

To log in to WebSphere Application Server, enter the following login URL for the WebSphere Application Server administrative console in a browser:

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

The value of *hostname* or *ip-address* is the name of the host system or IP address or DNS address of the WebSphere Application Server.

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

The default port on the WebSphere Application Server information pane is 9083. You can modify the default port during IBM Security Key Lifecycle Manager installation. During migration, or if the default port has a conflict for other reasons, WebSphere Application Server automatically selects another free port.

The Windows start menu contains an entry to connect to the WebSphere Application Server with the correct port number.

Click **KLMProfile - Administrative console**.

For information about IBM Security Key Lifecycle Manager administrator user ID and password, see "Default users" on page 6.

Enabling scripting settings for Internet Explorer, Version 9, 10, and 11

Ensure that scripting settings for Internet Explorer, version 9, 10, and 11 are enabled.

About this task

Unless some scripting settings are enabled for Internet Explorer, version 9, 10, and 11, 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**.

Backing up critical data

Create a backup of the critical data for future reference.

Back up the data in the following directories and ensure that they are stored in a safe place.

- *WAS_HOME*\configuration
  For example, `C:\Program Files\IBM\WebSphere\AppServer\configuration`
- *WAS_HOME*\products
  For example, `C:\Program Files\IBM\WebSphere\AppServer\products`

- *SKLM_DATA*
  For example, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`

Creating a server certificate

You can specify the self-signed certificate to be used as server communication certificate. Alternatively, you can create requests for certificates and manually send the request to a certificate authority (CA) for signing.

About this task

For example, you can use certificates to secure the communication between IBM Security Key Lifecycle Manager and a tape library. The generated certificate request files reside in the *<SKLM_HOME>* directory. A sample certificate request file: `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\171029122037-sslcert001.csr`.

Your role must have the permission to the configure action to create an SSL or KMIP certificate.

Before you begin, consider the following points:

- Whether you can use self-signed certificates during a phase in your project such as a test phase.
- The time interval that is needed to receive a CA-issued certificate after a request is sent. You must manually send a certificate request to the issuing authority.
- Whether your site requires partner certificates for use with business partners, vendors, or for disaster recovery purposes.
- The customary setting in days for a certificate validity interval.

Procedure

- Using graphical user interface
  a) Log in to the graphical user interface. Click **IBM Security Key Lifecycle Manager** > **Configuration** > **SSL/KMIP**.
  b) Select whether to generate a self-signed certificate, request a certificate from a third-party provider, or use an existing certificate from the keystore.
  c) Specify values for the required and optional fields, and click **OK**.

  Review and complete the steps under the **Next steps** section.
- Using REST interface
  a) Open a REST client.
  b) Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.
  c) Run **`Certificate Generate Request REST Service`**.

  Example 1: Create a self-signed certificate:

  ```
  POST https://localhost:<port>/SKLM/rest/v1/certificates
  {"type":"selfsigned","alias":"sklmCertificate","cn":"sklm","ou":"sales",
  "o":"myCompanyName","usage":"3592","country":"US","validity":"999", "
  algorithm ": " RSA "  }
  ```

  Example 2: Obtain a certificate from a certificate authority:

  ```
  POST https://localhost:<port>/SKLM/rest/v1/certificates
  {"type":"certreq","alias":"sklmCert","cn":"sklm","ou":"sales","o":
  "myCompanyName","usage":"3592","country":"US","validity":"999","fileName":
  "myCertRequest1.crt","algorithm":"ECDSA"}
  ```
- Using command-line interface
  a) Go to the *<WAS_HOME>*`/bin` directory.

For example:

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b) Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin.

For example,

Windows

```
wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
```

Linux

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

c) Run the **tklmCertCreate** command.

Example 1: Create a self-signed certificate:

```
print AdminTask.tklmCertCreate ('[-type selfsigned
    -alias sklmSSLCertificate -cn sklmssl -ou accounting -o myCompanyName
         -country US -keyStoreName defaultKeyStore
                -usage SSLSERVER -validity 999]')
```

Example 2: Obtain a certificate from a certificate authority:

```
print AdminTask.tklmCertGenRequest('[-alias sklmSSLCertificate1
    -cn sklm -ou sales -o myCompanyName -locality myLocation
        -country US -validity 999 -keyStoreName defaultKeyStore
            -fileName mySSLCertRequest1.crt -usage SSLSERVER]')
```

If you select a certificate request for a third-party provider, the certificate request file in `.csr` format is generated in the <SKLM_HOME> directory. For example, `C:\Program Files\IBM\WebSphere \AppServer\products\sklm\171029122037-sslcert001.csr`. Manually send the certificate request to a certificate authority. You must then import the signed certificate to IBM Security Key Lifecycle Manager.

Uninstalling IBM Security Key Lifecycle Manager

Review the following considerations before you uninstall IBM Security Key Lifecycle Manager.

Before you begin

- The default uninstallation mode is the same as the mode used to install IBM Security Key Lifecycle Manager.
- Uninstalling IBM Security Key Lifecycle Manager does not uninstall Db2 if it is installed before you install IBM Security Key Lifecycle Manager. This task is a separate, optional step. For more information, see “Db2 uninstallation” on page 33.

  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 more information, see “Removal of user ID from the Db2 instance owner” on page 35.

  Unsuccessful uninstallation might indicate the need to return to a known state of IBM Security Key Lifecycle Manager, see “Reinstalling previous version if migration repeatedly fails” on page 48.
- On Linux systems, when you uninstall IBM Security Key Lifecycle Manager, the Db2 user, for example, `sklmdb40`, is not removed. The users created by IBM Security Key Lifecycle Manager installer or existing users are not removed by the uninstaller. If needed, you can manually remove such users.

However, the `klmfcuser` is removed during IBM Security Key Lifecycle Manager uninstallation.

- In graphical mode of uninstallation, if WebSphere Application Server is not stopped before you uninstall IBM Security Key Lifecycle Manager, the following false message is displayed.

```
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.

Uninstalling on Windows systems

Uninstall IBM Security Key Lifecycle Manager and its components when you no longer need them on your Windows systems.

Uninstalling in graphical mode

Uninstall IBM Security Key Lifecycle Manager and its components when you no longer need them on your Windows systems in graphical mode.

Procedure

1. From the command prompt, go to the `disk1` directory of your installation package. For example, *download_path*`/disk1`.
2. Run the following command.

```
uninstallSKLM.bat IM_INSTALL_LOCATION WAS_INSTALL_LOCATION SKLM_INSTALL_HOME
WAS_ADMIN WAS_PASSWORD
```

IM_INSTALL_LOCATION - Installation Manager directory for IBM Security Key Lifecycle Manager.

WAS_INSTALL_LOCATION - WebSphere Application Server directory for IBM Security Key Lifecycle Manager.

SKLM_INSTALL_HOME - IBM Security Key Lifecycle Manager installation directory.

WAS_ADMIN - User name of WebSphere Application Server for IBM Security Key Lifecycle Manager.

WAS_PASSWORD - Password of WebSphere Application Server user name.

For example:

```
uninstallSKLM.bat "C:\Program Files\IBM\Installation Manager"
"C:\Program Files\IBM\WebSphere\AppServer"
"C:\Program Files\IBM\SKLMV40" wasadmin WAS@admin123
```

3. In IBM Installation Manager, click **Uninstall**.
4. Select the check boxes to uninstall IBM Security Key Lifecycle Manager, Db2, and WebSphere Application Server.

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

```
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.
5. Click **Next**. Type the WebSphere Application Server Administrator user ID and the password.
6. Click **Next**.

   The **Summary panel** window opens.
7. Review the software packages to be uninstalled and their installation directories.
8. Click **Uninstall**.

After IBM Security Key Lifecycle Manager uninstallation, if DB2 services are still running, manually uninstall DB2 and its components. For more information about DB2 uninstallation, see http://www-01.ibm.com/support/docview.wss?uid=swg21104569.

What to do next

Verify the uninstallation summary and the log files that are at `C:\ProgramData\IBM\InstallationManager\logs\sklmLogs\`.

After you uninstall IBM Security Key Lifecycle Manager, delete the `C:\Program Files\IBM\WebSphere` and `C:\Program Files\DB2SKLMV40` directories if not already removed.

Uninstalling in silent mode

Uninstall IBM Security Key Lifecycle Manager and its components when you no longer need them on your Windows systems in silent mode.

Procedure

1. Edit the response file to add encrypted passwords to the relevant elements of the file. The sample response files are in the directory in which your installation package is located.

   You can use the IBM Installation Manager utility to create encrypted passwords. For information about how to encrypt the password, see Encrypted password for response file elements.
2. From the command prompt, go to the `disk1` directory of your installation package. For example, *download_path*`/disk1`.
3. Run the following command.

   ```
   silent_uninstallSKLM.bat IM_INSTALL_LOCATION WAS_INSTALL_LOCATION SKLM_INSTALL_HOME
   WAS_ADMIN WAS_PASSWORD
   ```

   IM_INSTALL_LOCATION - Installation Manager directory for IBM Security Key Lifecycle Manager.

   WAS_INSTALL_LOCATION - WebSphere Application Server directory for IBM Security Key Lifecycle Manager.

   SKLM_INSTALL_HOME - IBM Security Key Lifecycle Manager installation directory.

   WAS_ADMIN - User name of WebSphere Application Server for IBM Security Key Lifecycle Manager.

   WAS_PASSWORD - Password of WebSphere Application Server user name.

   For example:

   ```
   silent_uninstallSKLM.bat "C:\Program Files\IBM\Installation Manager"
   "C:\Program Files\IBM\WebSphere\AppServer"
   "C:\Program Files\IBM\SKLMV40" wasadmin WAS@admin123
   ```

   After IBM Security Key Lifecycle Manager uninstallation, if DB2 services are still running, manually uninstall DB2 and its components. For more information about DB2 uninstallation, see http://www-01.ibm.com/support/docview.wss?uid=swg21104569.

What to do next

Verify the uninstallation summary and the log files that are at `C:\ProgramData\IBM\InstallationManager\logs\sklmLogs\`.

After you uninstall IBM Security Key Lifecycle Manager, delete the `C:\Program Files\IBM\WebSphere` and `C:\Program Files\DB2SKLMV40` directories if not already removed.

Uninstalling on Linux and AIX systems

Uninstall IBM Security Key Lifecycle Manager and its components when you no longer need them on your Linux or AIX systems.

Uninstalling in graphical mode

Uninstall IBM Security Key Lifecycle Manager and its components when you no longer need them on your Linux or AIX systems in graphical mode.

Procedure

1. Open a terminal window.
2. Go to the `disk1` directory of your installation package. For example, *`download_path`*`/disk1`.
3. Run the following command.

   ```
   uninstallSKLM_linux.sh IM_INSTALL_LOCATION WAS_INSTALL_LOCATION
   SKLM_INSTALL_HOME WAS_ADMIN WAS_PASSWORD
   ```

   `IM_INSTALL_LOCATION` - Installation Manager directory for IBM Security Key Lifecycle Manager.

   `WAS_INSTALL_LOCATION` - WebSphere Application Server directory for IBM Security Key Lifecycle Manager.

   `SKLM_INSTALL_HOME` - IBM Security Key Lifecycle Manager installation directory.

   `WAS_ADMIN` - User name of WebSphere Application Server for IBM Security Key Lifecycle Manager.

   `WAS_PASSWORD` - Password of WebSphere Application Server user name.

   For example:

   ```
   uninstallSKLM_linux.sh /opt/IBM/Installation Manager /opt/IBM/WebSphere/AppServer
   /opt/IBM/SKLMV40 wasadmin WAS@admin123
   ```

4. In the IBM Installation Manager uninstallation wizard, click **Uninstall**.
5. Select the packages to uninstall, IBM Security Key Lifecycle Manager, Db2, and WebSphere Application Server.

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

   ```
   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.
6. Click **Next**.
7. Type the WebSphere Application Server Administrator user ID and the password.
8. Click **Next**.
9. Review the software packages to be uninstalled and their installation directories.
10. Click **Uninstall**.

What to do next

Verify the uninstallation summary and the log files that are at `/var/ibm/InstallationManager/logs/sklmLogs/`.

After you uninstall IBM Security Key Lifecycle Manager, delete the `/opt/IBM/WebSphere` and `/opt/DB2SKLMV40` directories if not already removed.

Uninstalling in silent mode

Uninstall IBM Security Key Lifecycle Manager and its components when you no longer need them on your Linux and AIX systems in silent mode.

Procedure

1. Edit the response file to add encrypted passwords to the relevant elements of the file. The sample response files are in the directory in which your installation package is located.

   You can use the IBM Installation Manager utility to create encrypted passwords. For information about how to encrypt the password, see Encrypted password for response file elements.
2. From the terminal window, go to the `disk1` directory of your installation package. For example, *download_path*`/disk1`.
3. Run the following command.

   Linux

   ```
   silent_uninstallSKLM_linux.sh IM_INSTALL_LOCATION WAS_INSTALL_LOCATION
   SKLM_INSTALL_HOME WAS_ADMIN WAS_PASSWORD
   ```

   ```
   silent_uninstallSKLM_linux.sh /opt/IBM/InstallationManager /opt/IBM/WebSphere/AppServer
   /opt/IBM/SKLMV40 wasadmin WAS@admin123
   ```

   AIX

   ```
   silent_uninstallSKLM_AIX.sh IM_INSTALL_LOCATION WAS_INSTALL_LOCATION
   SKLM_INSTALL_HOME WAS_ADMIN WAS_PASSWORD
   ```

   ```
   silent_uninstallSKLM_AIX.sh /opt/IBM/InstallationManager /opt/IBM/WebSphere/AppServer
   /opt/IBM/SKLMV40 wasadmin WAS@admin123
   ```

   IM_INSTALL_LOCATION - Installation Manager directory for IBM Security Key Lifecycle Manager.

   WAS_INSTALL_LOCATION - WebSphere Application Server directory for IBM Security Key Lifecycle Manager.

   SKLM_INSTALL_HOME - IBM Security Key Lifecycle Manager installation directory.

   WAS_ADMIN - User name of WebSphere Application Server for IBM Security Key Lifecycle Manager.

   WAS_PASSWORD - Password of WebSphere Application Server user name.

What to do next

Verify the uninstallation summary and the log files that are at `/var/ibm/InstallationManager/logs/sklmLogs/`.

After you uninstall IBM Security Key Lifecycle Manager, delete the `/opt/IBM/WebSphere` and `/opt/DB2SKLMV40` directories if not already removed.

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 34.

If you choose to uninstall Db2, follow these steps:

Windows

Open the Control Panel.

Windows Server 2012: 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 **Server Manager** and click **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 **Server Manager** and click **Tools > 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 Db2 uninstallation on Windows systems, see DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0007436.html).

AIX and Linux

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 **db2stop** command for the instance owner user ID and exit back to the root user ID:

   ```
   su - sklm_instance_owner_userid

   cd DB_HOME/instance
   ./db2stop 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 Linux and AIX systems, see Db2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/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, `sklmdb40`, and the default Db2 directory, `/opt/IBM/DB2SKLMV40`.

Starting as root, type:

```
su - sklmdb40
cd /opt/IBM/DB2SKLMV40/instance
./db2stop sklmdb40/home/sklmdb40
exit
# Exit back to root.
cd /opt/IBM/DB2SKLMV40/instance
./db2idrop sklmdb40
userdel -r sklmdb40
cd /opt/IBM/DB2SKLMV40/install
./db2_deinstall -a
vi /etc/services
# Locate and remove the Db2 port entries in the services file.
rm -rf /opt/IBM/DB2SKLMV40
```

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 - DBSKLMV40 - SKLMDB40**.

   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 **db2stop** command for the instance owner user ID and exit back to the root user ID:

```
su - sklm_instance_owner_userid

cd DB_HOME/instance
./db2stop 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 34. 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 - DBSKLMV40 - SKLMDB40**

Db2 Governor (*db2 copy name*)
For example, **Db2 Governor (DB2SKLMV40)**

Db2 License Server (*db2 copy name*)
For example, **Db2 License Server (DB2SKLMV40)**

Db2 Management Service (*db2 copy name*)
For example, **Db2 Management Service (DB2SKLMV40)**

Db2 Remote Command Server (*db2 copy name*)
For example, **Db2 Remote Command Server (DB2SKLMV40)**

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 sklmdb40
```

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/bin/startServer.sh server1
```

Encrypted password for response file elements

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.WAS_ADMIN_ID,com.ibm.sklm40.win' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm40.win' value='e9PjN93MeQxwnSs9VXJFMw==/>
```

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.WAS_ADMIN_ID,com.ibm.sklm40.linux' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm40.linux' value='e9PjN93MeQxwnSs9VXJFMw==/>
```

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 V9.0 - SKLM40Server`
   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.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_gui.html

   Command-line interface
   http://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_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 32.
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 v2.7' 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\IBM\DB2SKLMV40
- C:\Program Files\IBM\WebSphere
- C:\Program Files\IBM\SKLMV40
- C:\Program Files\IBM\Installation Manager
- C:\Program Files\IBM\IBMIMShared

10. Restart the computer.

Recovering from a failed uninstallation on Linux or AIX systems

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

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.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_gui.html

   Command-line interface
   http://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_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 32.
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 v3.0' 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/DB2SKLMV40
   - opt/IBM/WebSphere

- `opt/IBM/SKLMV40`
- `opt/IBM/Installation Manager`
- `opt/IBM/IBMIMShared`

10. Restart the computer.

Installation error messages

Messages indicate events that occur during the operation of the system. Depending on the outcome of an operation, IBM Security Key Lifecycle Manager provides an informational, warning, or error message.

Supported upgrade paths and migration methods

Steps to upgrade IBM Security Key Lifecycle Manager depend on the existing version that is installed on the host system.

Upgrade process overview

IBM Security Key Lifecycle Manager does not support a direct upgrade from the existing version (installed on the host system) to the target version (to which you want to upgrade).

To upgrade, you must complete the following high-level operations:

I. Install the target version.
You can install the product by using the graphical user interface or silently.

You can install the target version on the same system that hosts the existing version, or on another host system. For example, when the system configuration of the host of the existing version does not meet the requirements of the target version, or when you need to upgrade IBM Security Key Lifecycle Manager on to a different operating system, you need to install the target version on another host system.

II. Migrate data from the existing version to the target version.
There are two methods of data migration:

Inline migration
When the host system of the target version is the same as the existing version, use inline migration of data.

Cross migration
When the host system of the target version is different than the host system of the existing version, use cross migration of data. IBM Security Key Lifecycle Manager provides sample response files that you can use to cross migrate data.

Note: Migration does not remove the earlier version of IBM Security Key Lifecycle Manager.

Supported upgrade paths and migration methods

Use the following table to understand the supported upgrade paths and migration methods.

Table 7. Supported upgrade paths and migration methods				
Existing version	**Minimum required level**	**Supported?**		**Notes**
		Inline migration	**Cross migration**	
3.0.1	General availability (GA)	✓	✓	"Upgrading IBM Security Key Lifecycle Manager to Version 4.0" on page 73
3.0	General availability (GA)	✓	✓	
2.7	General availability (GA)	✓	✓	
2.6	Fix pack 2	✓	✓	
2.5**	Fix pack 3	✓	✓	
IBM Tivoli Key Lifecycle Manager V 2.0.1**	Fix pack 5			Upgrade path: (→ V2.7 → V4.0)* "Upgrading IBM Tivoli Key Lifecycle Manager to IBM Security Key Lifecycle Manager 4.0" on page 73
IBM Tivoli Key Lifecycle Manager V 2.0**	Fix pack 6			
IBM Tivoli Key Lifecycle Manager V 1.0**	Fix pack 7			
Encryption Key Manager V 2.1**	-	✓	✓	"Upgrading Encryption Key Manager to IBM Security Key Lifecycle Manager 4.0" on page 73

* - Cross-migration of IBM Tivoli Key Lifecycle Manager data to IBM Security Key Lifecycle Manager, Version 4.0 consists of the following two stages:

1. Migrating the IBM Tivoli Key Lifecycle Manager data to a system where IBM Security Key Lifecycle Manager, Version 2.7 is installed.
2. Migrating IBM Security Key Lifecycle Manager, Version 2.7 data to a system where IBM Security Key Lifecycle Manager, Version 4.0 is installed.

** - End of support (EOS) version. For more information, see IBM Support - Software lifecycle.

Resetting a password

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

About this task

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

Procedure

1. Log in with the a local administrator user ID.

2. Back up the *WAS_HOME*/profiles/KLMProfile/config/cells/SKLMCell/fileRegistry.xml file. Changing the value of the password changes this registry file.
3. Change the password.
   - Windows
     a. Start a **wsadmin** session by using the Jython syntax. For example, type:

     ```
     WAS_HOME/bin/wsadmin.bat -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
     ```

   - Linux
     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

Windows

```
stopServer.bat server1
```

Linux

```
./stopServer.sh server1
```

- Start

Windows

```
startServer.bat server1
```

Linux

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

5. Verify that you can log in as the specified administrator with the new password.

Updating Db2 password on a Windows system

On Windows systems, the Db2 Administrator user ID and password are subject to the security policy that is active on the system. If a password expiration restriction is in effect, you must change the login password and Db2 password for the Administrator user ID before the expiration period ends.

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. For information about the supported special characters in a password, see https://www.ibm.com/support/pages/supported-special-characters-ibm-security-key-lifecycle-manager-passwords.

Run the following steps to change the Db2 database password:

1. Open the Windows user management tool by opening the Control Panel and clicking **Administrative tools** > **Computer Management** > **Local Users and Groups** > **Users**.
2. Change the password for the IBM Security Key Lifecycle Manager database owner.
3. Open the Windows Services console by opening the Control Panel and clicking **Administrative Tools > Computer Management**.
4. Change the password for the following services from the **Logon** tab of the **Properties** dialog box.
   - DB2® - DB2SKLMV40 - *sklminstance*

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

     ```
     DB2 - DBSKLMV40 - SKLMDB40
     ```

   - `IBM WebSphere Application Server V9.0 - SKLM40Server`
5. Stop and restart the following services:
   - Db2 License Server (DBSKLMV40)
   - Db2 Management Service (DBSKLMV40)
   - DB Remote Command Server (DBSKLMV40)
   - Db2 Governor (DBSKLMV40)
   - WAS Service - IBM Security Key Lifecycle Manager (`IBM WebSphere Application Server V9.0 - SKLM40Server`)

   Db2 password is updated on the system.

Updating Db2 password on a Linux or AIX system

On Linux or AIX systems, 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 `sklmdb40`. Additionally, the Db2 application creates an operating system user entry named `sklmdb40`. For example, the password for this user might expire, requiring you to resynchronize the password for both user IDs.

Note: Run all the Db2 specific commands as a **`sklmdb`** user, and run the WebSphere Application Server commands as a **`root`** user.

Before you can change the password for the Db2 Administrator user ID, you must change the password for the user at the operating system level.

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. For information about the supported special characters in a password, see https://www.ibm.com/support/pages/supported-special-characters-ibm-security-key-lifecycle-manager-passwords.

1. Log in to the IBM Security Key Lifecycle Manager server as root.
2. Change user to the `sklmdb40` system user entry. Type:

   ```
   su sklmdb40
   ```

3. Change the password. Type:

   ```
   passwd
   ```

   Specify the new password.
4. Exit back to root.

   ```
   exit
   ```

   Db2 password is updated on the system.

Update Config Property REST Service

Use **`Update Config Property REST Service`** to update one or more properties in one of the following IBM Security Key Lifecycle Manager configuration files: `SKLMConfig.properties` (controls the IBM Security Key Lifecycle Manager server operations), `MMConfig.properties` (controls the Multi-Master cluster operations).

Operation
PUT

URL
`https://`*`host`*`:`*`port`*`/SKLM/rest/v1/configProperties`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body	
JSON property name	**Description**
Property names	Specify the configuration property that you want to update in the configuration file. You can specify multiple comma-separated properties. For example, `{"fips" : "on", "KMIPListener.ssl.port" : "5678"}`
type	Optional. Specify the value `MM` when you want to update properties in the `MMConfig.properties` file. When this parameter is not specified, the REST API updates properties in the `SKLMConfig.properties` file.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification:	
JSON property name	**Description**
property	Returns the name of the property that is updated.
status	Returns the status to indicate the configuration file updates.

Note: The success response code 200 OK is returned even if the property you requested is not found. An appropriate message is returned in the response body.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request to update a single server configuration property

```
PUT https://localhost:<port>/SKLM/rest/v1/configProperties
{ "KMIPListener.ssl.port" : "10000"}
```

Success response

```
Status Code : 200 OK
[{"property":"KMIPListener.ssl.port","status":"CTGKM0607I Update
successful, server restart required for change to take effect"}]
```

Error response

```
Status Code : 400 Bad Request
{"code" : "CTGKM6002E", "message" : "CTGKM6002E Bad Request:
Invalid user authentication ID or invalid request format"}
```

Service request to update multiple server configuration properties

```
PUT https://localhost:<port>/SKLM/rest/v1/configProperties
 {"fips" : "on", "KMIPListener.ssl.port" : "5678"}
```

Success response

```
Status Code : 200 OK
[{"property":"KMIPListener.ssl.port","status":"CTGKM0607I Update
successful, server restart required for change to take effect"},{"
property":"fips","status":"CTGKM0606I Update successful, change will
take effect immediately"}]
```

Error response

```
Status Code : 400 Bad Request
Content-Language: en
{"code" : "CTGKM6002E", "message" : "CTGKM6002E Bad Request:
Invalid user authentication ID or invalid request format"}
```

Service request to update the Db2 password change in Multi-Master configuration (`MMConfig.properties`) file

```
PUT https://localhost:port/SKLM/rest/v1/configProperties
{ "Db2PasswordChangeActivity" : "true", "type" : "MM"}
```

Success response

```
Status Code : 200 OK
[{"property":"Db2PasswordChangeActivity","status":"CTGKM0607I Update
successful, change will take effect immediately"}]
```

Error response

```
Status Code : 400 Bad Request
{"code" : "CTGKM6002E", "message" : "CTGKM6002E Bad Request:
Invalid user authentication ID or invalid request format"}
```

Supported special characters in passwords

The following special characters are supported in the Db2 administrator password, WebSphere Application Server administrator (WASadmin) password, and IBM Security Key Lifecycle Manager administrator (SKLMAdmin) password.

Supported special characters in passwords on Linux systems

The following table provides the list of special characters that are supported in the passwords on Linux systems:

Name of the special character	Special character
tilde	~
at sign	@
hash mark	#
underscore	_
caret	^
asterisk	*
percent sign	%
slash	/
period	.
plus sign	+
colon	:
semicolon	;
equal sign	=

Supported special characters in passwords on Windows systems

The following table provides the list of special characters that are supported in the passwords on Windows systems:

Name of the special character	Special character
tilde	~
at sign	@
underscore	_
slash	/

Name of the special character	Special character
plus sign	+
colon	:

Guidelines for using the supported special characters in passwords

Consider the following guidelines while using the supported special characters in passwords. These guidelines are not applicable when you specify passwords on the graphical user interface.

- Enclose the password in quotes when you use the operating system shells for connecting to WebSphere Application Server wsadmin interface, or Db2 command line, or to run a fix pack installation. Use single quotes for Linux and double quotes for Windows. For example:

  Linux

  ```
  [root@sklm bin]# ./wsadmin.sh -username sklmadmin -password '~@_ABc12/+:' -lang jython
  WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector; The type
  of process is: UnManagedProcess
  WASX7031I: For help, enter: "print Help.help()"
  wsadmin>
  ```

  Windows

  ```
  C:\Program Files\IBM\WebSphere\AppServer\bin>wsadmin.bat -username sklmadmin -password
  "~@_ABc12/+:" -lang jython
  WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector;
    The type of process is: UnManagedProcess
  WASX7031I: For help, enter: "print Help.help()"
  wsadmin>
  ```

- Add encrypted passwords to the relevant elements of response file when you run the IBM Security Key Lifecycle Manager installation or upgrade (fix pack or main release) process in silent mode.

  To create an encrypted password, use the `imcl` utility, as shown here:

  Linux

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

  Ensure that you use backslash (\) as an escape character for the special characters in the password. For example:

  ```
  cd /SKLM/disk1/im/tools
  ./imcl encryptString \~\@\_ABc12\/\+\:
  ```

  The encrypted string (for example, pABm1rqy66jAykrhBtpM6Q==) is returned.

  Windows

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

  Ensure that you enclose the complete password in double quotes. For example:

  ```
  cd C:\SKLM\disk1\im\tools
  C:\SKLMV40\disk1\im\tools>imcl.exe encryptString "~@_ABc12/+:"
  ```

  The encrypted string (for example, pABm1rqy66jAykrhBtpM6Q==) is returned.

For more information, see “Encrypted password for response file elements” on page 36.

tklmConfigUpdateEntry

Use the **tklmConfigUpdateEntry** command to change an existing entry or to add an entry in the SKLMConfig.properties file.

Note: The IBM Security Key Lifecycle Manager command-line interface commands will be deprecated in a later version of IBM Security Key Lifecycle Manager. Use the REST interfaces instead.

Purpose

Changes an existing entry or adds an entry in the SKLMConfig.properties file.

To change an attribute of a device group in the IBM Security Key Lifecycle Manager database, use the "tklmDeviceGroupAttributeUpdate" on page 59 CLI command.

Note: If you use the graphical user interface, or command-line interface, you can change the IBM Security Key Lifecycle Manager configuration file while the server is running. Depending on the change, you might see a message that indicates you to restart the IBM Security Key Lifecycle Manager server for the change to take effect.

Permissions

Your role must have the permission to the configure action.

Syntax

tklmConfigUpdateEntry -name *attributename* -value *attributevalue*

Parameters

-name
Required. Specify the name of the attribute.

-value
Required. Specify the value of an attribute. Depending on the attribute, you can specify multiple values, by using commas to separate the values. For more information, see the SKLMConfig.properties file.

Examples

This Jython-formatted command example changes the types of events that are audited, specifying an Audit.event.types property to have two values (runtime and audit_management) in the SKLMConfig.properties file.

```
print AdminTask.tklmConfigUpdateEntry ('[-name Audit.event.types
 -value runtime,audit_management]')
```

This example specifies a different TCP port number.

```
print AdminTask.tklmConfigUpdateEntry
    ('[-name TransportListener.tcp.port -value 3802]')
```

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 4.0 and continue to run the previous version.

Note: On Windows platform, after you migrate from the earlier version of IBM Security Key Lifecycle Manager to version 4.0, DB2 associated with the earlier version might not start if you uninstall IBM Security Key Lifecycle Manager, Version 4.0 before uninstalling the earlier version.

You can uninstall IBM Security Key Lifecycle Manager, Version 4.0 by following the steps in "Uninstalling IBM Security Key Lifecycle Manager" on page 28.

Adding a master server to a cluster

In IBM Security Key Lifecycle Manager, high-availability solution is implemented by using Multi-Master cluster configuration. Adding a master server to a cluster is part of setting up a Multi-Master environment.

Before you begin

Complete the following tasks:

- Review the considerations and restrictions that are listed in the Requirements and considerations for Multi-Master configuration topic.
- Before you add a non-HADR master to the Multi-Master cluster, ensure that at least one standby master is added in the cluster. For more information, see "Adding a standby master server to a cluster" on page 51.

About this task

When you create a Multi-Master cluster, the server from which you add a master server or standby server to the cluster becomes the primary master. After the cluster is created with a minimum of one primary and standby master servers each, you can add master servers to the cluster from any of the master servers. Your role must have the permission to add master server to the Multi-Master cluster.

You cannot add a master server to the cluster by using the **Multi-Master Configuration - Add Master** page when a standby or master server in the cluster is out of network or not reachable. To add a master server in this scenario, you must use the **`Add Master REST Service`** with additional parameters. For more information, see "REST service for adding a master when other master in the cluster is not reachable" on page 65.

Procedure

1. Go to the appropriate page or directory.

   Graphical user interface

   a. Log in to the graphical user interface.

   b. On the **Welcome** page, click **Administration** > **Multi-Master** > **Masters** > **Add Master**.

   REST interface

   Open a REST client.

2. Add a master to the cluster.

   Graphical user interface

   a. Click the **Basic Properties** tab.

   b. On the **Basic Properties** dialog, specify information for the master that you are adding.

Host name / IP address	Specify the host name of the IBM Security Key Lifecycle Manager instance that is added to the cluster.
IBM Security Key Lifecycle Manager user name	Specify the name of the IBM Security Key Lifecycle Manager administrator. The administrator name is displayed by default.
IBM Security Key Lifecycle Manager password	Specify the password for the IBM Security Key Lifecycle Manager server administrator.

WebSphere Application Server user name	Specify the WebSphere Application Server login user ID for the IBM Security Key Lifecycle Manager server administrator profile. The WebSphere Application Server login ID is displayed by default.
WebSphere Application Server password	Specify the password for the WebSphere Application Server login user ID.
UI port	Specify the HTTPS port to access IBM Security Key Lifecycle Manager graphical user interface and REST services. The port number is displayed by default.

c. If you want the primary master to automatically accept the certificate of the master that you are adding, select **Accept host certificate automatically**. Otherwise, manually add the certificate to the truststore of the primary master. For instructions, see "Adding a certificate to the truststore" on page 68.

Note: By default, the certificate is not automatically accepted.

d. Click **Check Prerequisites**. The master server performs some checks. For example, communication between the standby master server that you are adding and the current primary master is successful, user login credentials are valid, and so on.

e. Click **Add**.

REST interface

a. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.

b. Run "Check Prerequisites REST Service" on page 62 to ensure that the master server that you want to add meets all requirements and conditions that are defined for a Multi-Master configuration.

c. Run the **Add Master REST Service**. For example:

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/config/nodes/addNodes
[
{
"clusterName" : "multimaster",
"primaryHadrPort" : "60020"
},
{
"type" : "Node",
"ipHostname": "cimkc2b151",
"httpPort": "9443",
"sklmUsername": "sklmadmin",
"sklmPassword": "SKLM@admin123",
"wasUsername": "wasadmin",
"wasPassword": "WAS@admin123",
"autoAccept": "Yes"
}
]
```

What to do next

The primary master restarts, and is temporarily unavailable during this process after you add a master to the cluster. Verify whether the master with its health status information is listed in the Masters table, and also on the IBM Security Key Lifecycle Manager welcome page.

Preinstallation tasks

Before you install IBM Security Key Lifecycle Manager, understand the prerequisites and plan your environment accordingly.

Complete the following prerequisite tasks:

- Ensure that the system meets the minimum hardware and software requirements. For more information, see IBM Security Key Lifecycle Manager Support Matrix.
- Use the preinstallation worksheets for planning.
- Determine the IBM Security Key Lifecycle Manager topology.
- Decide the installation mode you want to use to install IBM Security Key Lifecycle Manager: graphical mode or silent mode.

Adding a standby master server to a cluster

In IBM Security Key Lifecycle Manager, high-availability solution is implemented by using Multi-Master cluster configuration. IBM Security Key Lifecycle Manager Multi-Master cluster must contain a primary master server and a standby master server. Add a standby master server to the cluster for setting up a Multi-Master environment.

Before you begin

Before you add a standby master server to the cluster, review the considerations and restrictions that are listed in the Requirements and considerations for Multi-Master configuration topic.

About this task

To provide continuous data availability to all the IBM Security Key Lifecycle Manager instances in a Multi-Master cluster, Db2 high-availability disaster recovery (HADR) configuration is used. Db2 HADR is a database replication feature that provides a high-availability solution. HADR protects against data loss by replicating data changes from a source database, called primary, to a target database, called the standby. Db2 HADR supports up to three standby databases in your Multi-Master setup.

When you create an IBM Security Key Lifecycle Manager Multi-Master cluster, the server from which you add a master or standby to the cluster becomes the primary master. Once the cluster is created with a minimum of one primary master and standby master, you can then add masters to the cluster from any of the masters in the cluster. Use the **Multi-Master Configuration - Add Master** dialog or **`Add Master REST Service`** to add a master to the cluster. Your role must have a permission to add standby master to the IBM Security Key Lifecycle Manager Multi-Master cluster.

You cannot add a standby master to the cluster by using the **Multi-Master Configuration - Add Master** page when a standby or master server in the cluster is out of network or not reachable. To add a standby master in this scenario, you must use **`Add Master REST Service`** with additional parameters. For more information about the REST service, see “REST service for adding a master when other master in the cluster is not reachable” on page 65.

Procedure

1. Go to the appropriate page or directory.

   Graphical user interface

   a. Log in to the graphical user interface.

   b. On the **Welcome** page, click **Administration** > **Multi-Master** > **Masters** > **Add Master**.

   REST interface

   Open a REST client.

2. Add a standby master server to the cluster.

Graphical user interface

a. Click the **Basic Properties** tab.

b. On the **Basic Properties** dialog, specify information for the standby master that you are adding.

Host name / IP adress	Specify the host name of the IBM Security Key Lifecycle Manager standby master that is added to the cluster.
IBM Security Key Lifecycle Manager user name	Specify the name of the IBM Security Key Lifecycle Manager administrator. The administrator name is displayed by default.
IBM Security Key Lifecycle Manager password	Specify the password for the IBM Security Key Lifecycle Manager server administrator.
WebSphere Application Server user name	Specify the WebSphere Application Server login user ID for the IBM Security Key Lifecycle Manager server administrator profile. The WebSphere Application Server login ID is displayed by default.
WebSphere Application Server password	Specify the password for the WebSphere Application Server login user ID.
UI port	Specify the HTTPS port to access IBM Security Key Lifecycle Manager graphical user interface and REST services. The port number is displayed by default.

c. Click the **Advanced Properties** tab.

d. On the **Advanced Properties** dialog, specify information for the standby master that you are adding.

Do you want to set this master as standby database?	Select **Yes** to add the current instance of IBM Security Key Lifecycle Manager as a standby master to the cluster.
HADR port	Specify the port number for the standby HADR database to communicate with the primary HADR database.
Standby priority index	Specify the priority index value for the standby database to takeover when the primary database is down. You can set the priority index to any value in the range 1-3. The standby server with a higher priority index level (lower number) takes precedence over the lower-priority databases.

e. If you want the primary master to automatically accept the certificate of the master that you are adding, select **Accept host certificate automatically**. Otherwise, manually add the certificate to the truststore of the primary master. For instructions, see "Adding a certificate to the truststore" on page 68.

Note: By default, the certificate is not automatically accepted.

f. Click **Check Prerequisites**. The master server performs some checks. For example, communication between the standby master server that you are adding and the current primary master is successful, user login credentials are valid, and so on.

g. Click **Add**.

REST interface

a. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.

b. Run “Check Prerequisites REST Service” on page 62 to ensure that the master server that you want to add meets all requirements and conditions that are defined for IBM Security Key Lifecycle Manager Multi-Master configuration.

c. Run **Add Master REST Service**. For example:

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/config/nodes/addNodes
[
{
"clusterName" : "multimaster",
"hadrPort" : "60020"
},
{
"type" : "Standby",
"ipHostname"    :  "cimkc2b151",
"httpPort"      :  "9443",
"sklmUsername" :  "sklmadmin",
"sklmPassword" :  "SKLM@admin123",
"wasUsername"  :  "wasadmin",
"wasPassword"  :  "WAS@admin123",
"standbyPriorityIndex" : "1",
"autoAccept"    : "Yes"
}
]
```

What to do next

The primary master server restarts, and is temporarily unavailable during this process after you add a standby master server to the cluster. Verify that the standby master server is listed in the Masters table, and also on the IBM Security Key Lifecycle Manager Welcome page.

Migrating data from Encryption Key Manager

You can use the cross-platform backup utility of the current version of IBM Security Key Lifecycle Manager to migrate data from its earlier version.

Note: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

To migrate data:

1. Back up Encryption Key Manager data.
2. Restore the backup to IBM Security Key Lifecycle Manager.

Update Client Name REST Service

Use **Update Client Name REST Service** to update the name of a client.

Operation
PUT

URL
`https://host:port/SKLM/rest/v1/clients/updateClientName`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON object with the following specification:	
Property name	**Description**
clientName	Required. Specify the name of the client that you want to update.
newClientName	Required. Specify the new name of the client.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification:	
JSON property name	**Description**
messageId	Returns the message identifier.
message	Returns the message to indicate the operation is successful.

Error response body JSON object with the following specification.	
JSON property name	**Description**
messageId	Returns the message identifier.
error	Returns a message that describes the error.

Example

Update the name of a client

```
PUT https://localhost:port/SKLM/rest/v1/clients/updateClientName
```

Success response

```
  {
    "message": "CTGKM3420I Client name updated successfully.",
    "messageId": "CTGKM3420I"
}
```

Error response

```
{
    "messageId": "CTGKM3408E",
    "error": "CTGKM3408E Client with CLIENT_KMIP name not found."
}
```

Restarting the IBM Security Key Lifecycle Manager server

Restart of the server causes the server to read its configuration and accept the configuration changes, if any. To restart the IBM Security Key Lifecycle Manager server, you can use the graphical user interface, REST service, or run the server restart scripts.

About this task

To restart server, use the *<IBM Security Key Lifecycle Manager User>* link on welcome page header bar, **Restart Server REST Service**, or run the **stopServer** and **startServer** scripts.

Procedure

- **Using graphical user interface**
  a) Log on to the graphical user interface.
  b) On the Welcome page header bar, click the *<IBM Security Key Lifecycle Manager User>* link.
  For example, click the **SKLMAdmin** link.
  c) Click **Restart Server**.
  d) Click **OK**.

Note: The IBM Security Key Lifecycle Manager server is unavailable for a few minutes while the restart operation is in progress.

- **Using REST interface**
  a) Open a REST client.
  b) Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST APIs. For more information about the authentication process, see "Authentication process for REST services" on page 69.
  c) Run the "Restart Server REST Service" on page 75.
  Sample request:

```
POST https://localhost:port/SKLM/rest/v1/ckms/servermanagement/restartServer
```

- **Using scripts**
  a) Go to the *WAS_HOME*\bin directory.

  Windows

```
C:\Program Files\IBM\WebSphere\AppServer\bin
```

  Linux

```
/opt/IBM/WebSphere/AppServer/bin
```

  b) Stop the server.

  Windows

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

  Linux

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

  Because the administrative security for WebSphere Application Server is enabled, you must specify the user ID and password of the WebSphere Application Server administrator as parameters to the stopServer script. If these parameters are omitted, you are prompted to specify the values.

  c) Start the server.

  Windows

```
startServer.bat server1
```

  Linux

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

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.

Updating Db2 password for a stand-alone IBM Security Key Lifecycle Manager server

After you change or reset the Db2 password on the computer that hosts the IBM Security Key Lifecycle Manager server, you must update the password in IBM Security Key Lifecycle Manager so that IBM Security Key Lifecycle Manager can continue to connect to the Db2 database.

About this task

The password of the Db2 Administrator user must be the same as that of the Db2 data source password in WebSphere Application Server.

You need to change the Db2 password at the operating system level in accordance with the password expiration policy as defined by your organization. If the password expires, the IBM Security Key Lifecycle Manager graphical user interface displays a data-loading error. You must then reset the Db2 password and update it in IBM Security Key Lifecycle Manager. To update the password on the operating system, you must be the database instance owner on an AIX or Linux system, or the Local Administrator on a Windows system.

Procedure

1. Update the Db2 password on the operating system.
   For more information, see:
   - "Updating Db2 password on a Windows system" on page 42
   - "Updating Db2 password on a Linux or AIX system" on page 43
2. Change the Db2 data source password that is configured in WebSphere Application Server:
   - **Using graphical user interface**
     a. Log in to the graphical user interface.
     b. On the header bar, click ***SKLM User*** and select **Change Database Password**.
        SKLM User is the user with which you have logged into the graphical user interface.
     c. In the **Change Database Password** window, type the new password.
     d. Click **Submit**.
   - **Using REST interface**
     a. Open a REST client.
     b. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.
     c. Run "Update Db2 Password on Standalone Server REST Service" on page 77.

Results

Db2 password is updated and IBM Security Key Lifecycle Manager server agent can connect to the Db2 database.

Migrating data from an earlier version of IBM Security Key Lifecycle Manager

You can use the cross-platform backup utility of IBM Security Key Lifecycle Manager V4.0 (target) to migrate data from its earlier version.

Note: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Updating Db2 password for IBM Security Key Lifecycle Manager Multi-Master cluster

The Db2 password on the computers that host the IBM Security Key Lifecycle Manager master servers in a Multi-Master cluster must be the same. After you change or reset this password at the operating system level, you must update it in IBM Security Key Lifecycle Manager as well so that IBM Security Key Lifecycle Manager can continue to connect to the Db2 database.

About this task

The password of the Db2 Administrator user must be the same as that of the Db2 data source password in WebSphere Application Server.

You need to change the Db2 password at the operating system level in accordance with the password expiration policy as defined by your organization. If the password expires, the IBM Security Key Lifecycle Manager graphical user interface displays a data-loading error. You must then reset the Db2 password and update it in IBM Security Key Lifecycle Manager. To update the password on the operating system, you must be the database instance owner on an AIX or Linux system, or the Local Administrator on a Windows system.

Note: The password of the Db2 Administrator user must be the same on all the master servers of the IBM Security Key Lifecycle Manager Multi-Master cluster.

Procedure

On every master server (HADR and non-HADR)

1. Set the **Db2PasswordChangeActivity** property in the `MMConfig.properties` file to `true`.
   For instructions, see "Update Config Property REST Service" on page 43.
2. Update the Db2 password on the operating system.
   For more information, see:
   - "Updating Db2 password on a Windows system" on page 42
   - "Updating Db2 password on a Linux or AIX system" on page 43

On any master server

3. Change the Db2 data source password that is configured in WebSphere Application Server:
   - **Using graphical user interface**
     a. Log in to the graphical user interface.
     b. On the header bar, click ***SKLM User*** and select **Change Database Password**.
        SKLM User is the user with which you have logged into the graphical user interface.
     c. In the **Change Database Password** window, type the new password.
     d. Click **Submit**.
   - **Using REST interface**
     a. Open a REST client.
     b. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.
     c. Run "Update Db2 Password in Multi-Master Cluster REST Service" on page 79.

On every master server (HADR and non-HADR)

4. Set the **Db2PasswordChangeActivity** property in the `MMConfig.properties` file to `false`.
   For instructions, see "Update Config Property REST Service" on page 43.

Results
Db2 password is updated and IBM Security Key Lifecycle Manager server agent can connect to the Db2 database.

tklmDeviceGroupAttributeUpdate

Use the **tklmDeviceGroupAttributeUpdate** command to update the attributes of a device group such as myLTO.

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.

Purpose
Use this command to update the attributes of a device group such as myLTO.

To change an existing entry or to add an entry in the SKLMConfig.properties file, use the "tklmConfigUpdateEntry" on page 48 command.

Permissions

Your role must have permissions to the modify action and to the appropriate device group.

Syntax

tklmDeviceGroupAttributeUpdate [**-name** {LTO | 3592 | DS5000 | DS8000® | GPFS | PEER_TO_PEER | BRCD_ENCRYPTOR | ONESECURE | GENERIC | *userdevicegroup*} **-attributes** {*attributevaluepair*} {*attributevaluepair*}]

Parameters

-attributes
Specify one or more user-defined attribute-value pairs. Use the **tklmDeviceGroupAttributeList** command to view the current value.

drive.default.alias1
Specifies the system default certificate that a 3592 device uses if the device is not associated with another certificate.

drive.default.alias2
Specifies the system partner certificate that a 3592 device uses if the device is not associated with another certificate.

enableKMIPDelete
Enables or disables KMIP delete requests. The klmAdminDeviceGroup permission permits administration (create, view, delete) of a device group. Disabling this attribute when you create a device group prevents KMIP clients from deleting keys in the device group. The default is disabled (false). Use the **tklmDeviceGroupAttributeUpdate** command to modify this attribute.

symmetricKeySet
Specifies a key group to be used for a device group.

shortName
This property specifies a short label that is usually a drive type such as LTO. This is used for any additional attributes that are required by an original equipment manufacturer.

longName
This property specifies an extended descriptive name of a drive type, such as my division LTO. For example, this information might include business information.

AddNewCertsToPending
Specifies whether to add a certificate to the list of pending certificates that you can accept or reject before key serving occurs, or to add a certificate automatically to the certificate table for

immediate key service upon request. The attribute applies to the GPFS and PEER_TO_PEER device groups and their extended device groups.

-name
Required. Specify an existing device group, such as myLTO.

LTO
Specifies the LTO device group.

3592
Specifies the 3592 device group.

DS5000
Specifies the DS5000 device group.

DS8000
Specifies the DS8000 device group.

GPFS
Specifies the IBM Spectrum Scale (previously known as GPFS) device group.

PEER_TO_PEER
Specifies the PEER_TO_PEER device group.

BRCD_ENCRYPTOR
Specifies the BRCD_ENCRYPTOR device group that is in the LTO device family.

ONESECURE
Specifies the ONESECURE device group that is in the DS5000 device family.

GENERIC
Specifies a device family that uses the Key Management Interoperability Protocol to interact with IBM Security Key Lifecycle Manager. The GENERIC device group enables management of KMIP objects.

Do not use the command-line interface to add a device to the GENERIC device group, or to change a GENERIC device group attribute.

userdevicegroup
Specifies a user-defined group that is based on a supported device family.

Example

This Jython-formatted command updates an attribute for a 3592 device group.

```
print AdminTask.tklmDeviceGroupAttributeUpdate
('[-name 3592 -attributes "{longName 3592}"]')
```

This Jython-formatted command updates an attribute for an LTO device group.

```
print AdminTask.tklmDeviceGroupAttributeUpdate
('[-name LTO -attributes "{symmetricKeySet LTO}"]')
```

Requirements and considerations for Multi-Master configuration

Before you set up IBM Security Key Lifecycle Manager Multi-Master environment, review the requirements and considerations to ensure a successful configuration.

Operating system and database requirements

- Ensure that the master servers with primary and standby Db2 HADR database host systems have the same operating system version and fix pack levels. The non-HADR master servers can have a different operating system.
- IBM Security Key Lifecycle Manager Multi-Master architecture is based on Db2 High Availability Disaster Recovery (HADR) technology to implement high-availability solution. Therefore, all the Db2 HADR

configuration rules and guidelines are applicable for IBM Security Key Lifecycle Manager Multi-Master configuration.

- Db2 user name and password must be same on all the master servers of the IBM Security Key Lifecycle Manager Multi-Master cluster.

Port requirements

- Ensure that the agent port (60015) and HADR port (60027) that are used for Multi-Master configuration are not blocked by the firewall.

  Default agent port is 60015, which you can update through UI. Default HADR port is 60027, which is assigned during the Multi-Master setup. It is configurable.
- Ensure that the KMIP, SSL, TCP, and agent ports are not blocked for communication before you set up IBM Security Key Lifecycle Manager masters for Multi-Master configuration.
- A TCP/IP interface must be available between primary and standby Db2 HADR database host systems with a dedicated, high speed, and high capacity network bandwidth.

Other requirements and considerations

- If you want to add an existing IBM Security Key Lifecycle Manager server to the cluster, use the device group export and import feature. For more information, see "Adding an existing IBM Security Key Lifecycle Manager instance with data to the Multi-Master cluster" on page 81.
- The IBM Security Key Lifecycle Manager server that you want to add to a Multi-Master cluster must not contain any data. Adding of server with data results in loss of data that was previously created.
- For IBM Security Key Lifecycle Manager Multi-Master deployment, the cluster must contain a minimum of one primary master server and one standby master server. When you set up a Multi-Master cluster, the server from which you add a master server or standby master server to the cluster becomes the primary master server. You must add at least one standby master server to the cluster before you add other master servers.
- Server certificate must be created in the IBM Security Key Lifecycle Manager server before you add it to the cluster as the primary master.
- IBM Security Key Lifecycle Manager Multi-Master cluster supports up to three standby master servers. When you add a standby master server to the cluster, the priority index value must be in the range of 1-3.
- After the Multi-Master cluster is configured, you must avoid running manual backup and restore operations on any of the master servers in the cluster.
- Run the IBM Security Key Lifecycle Manager Multi-Master configuration operations only from the primary master server of the cluster to avoid any problems.
- Before you add a server that runs the Linux operating system, to a cluster, the permissions for the `/tmp` directory must be set to 777 that is full execute, read, and write permissions.
- If you want to configure the Multi-Master cluster to use HSM to store the master key, you must configure all the master servers in the cluster to use the same HSM.
- Before you add a master server to the cluster through the migrated system, modify the IBM Security Key Lifecycle Manager administrator user name and the password in the following situations:

  1. When users and groups are migrated from previous version to version 4.0 through cross-migration process.
  2. IBM Security Key Lifecycle Manager administrator user name and the password are different than that of the credentials specified during version 4.0 installation.
- You cannot remove a standby master server from the Multi-Master cluster if a standby server is down.
- Ensure that the master servers are *not* configured to back up large amount of data. So in the `SKLMConfig.properties` configuration file on every master server, ensure that the **`enableHighScaleBackup`** property does not exist or is set to `false`.

- If you plan to integrate LDAP with the Multi-Master setup for user authentication, you must configure LDAP on all master servers before configuring the Multi-Master cluster. Ensure that all the master servers use the same LDAP, and have the same users as IBM Security Key Lifecycle Manager Administrator.

  Best practice: If you plan to use IBM Security Key Lifecycle Manager REST services to connect to the IBM Security Key Lifecycle Manager server for key management operations, integrate with LDAP for user authentication and management.
- The `MMConfig.properties` file contains the Multi-Master configuration properties.

  Note: Do not update the configuration file manually.

Check Prerequisites REST Service

Use **`Check Prerequisites REST Service`** to verify whether the master server that you want to add to the cluster meets all requirements and conditions that are defined for IBM Security Key Lifecycle Manager multi-master configuration.

You can use **`Check Prerequisites REST Service`** to check whether the following conditions are met:

- Db2 and operating system levels are the same as that of the primary master.
- Database name and password are same on both the systems.
- Ports of the master server that you want to add are valid and accessible.
- The system has permission to read-write-execute on the `/tmp` folder.
- IBM Security Key Lifecycle Manager master server is freshly installed.
- Remote agent is accessible.
- The specified IBM Security Key Lifecycle Manager user credentials are valid.

Operation

POST

URL

`https://<host>:<port>/SKLM/rest/v1/ckms/nodes/checkPreRequisite`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
`host`	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
`port`	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
`Content-Type`	`application/json`
`Accept`	`application/json`

Request Headers (continued)	
Header name	**Value**
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON object with the following specification:	
Property name	**Description**
ipHostname	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server master server that you are adding.
clusterName	Specify the name for the multi-master cluster to which the master to be added. Possible value: `multimaster`
sklmUsername	Specify the name of the IBM Security Key Lifecycle Manager server administrator.
sklmPassword	Specify the password for the IBM Security Key Lifecycle Manager server administrator.
standbyPriorityIndex	Specify the priority index value for the standby database to takeover when the primary database is down.
wasUsername	Specify the WebSphere Application Server login user ID for the IBM Security Key Lifecycle Manager server administrator profile.
wasPassword	Specify the password for the WebSphere Application Server login user ID.
sklmUIPort	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests from devices that communicate by using the SSL protocol.
standbyHadrPort	Specify the HADR port of the standby server.
autoaccept	Specify whether the cluster must automatically accept the certificate of the master server that is being added. This property has two values: `true`, `false`. The default value is `false` to indicate that the cluster does not automatically accept the certificate of the master server that is being added.
hadrType	Specify the role of the master server. Possible values are: `Standby`, `Node` Use `Node` to indicate a non-HADR master server.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	application/json
Content-Language	Locale for the response message.

Success response body JSON object with the following specification:	
JSON property name	**Description**
code	Returns the code that is specified by the status property.
status	Returns the status to indicate whether the configuration of masters in the cluster you specify was successful.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request to check whether the master server meets all the configuration conditions

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/nodes/checkPreRequisite
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{
  "ipHostname" : "civ4cez199",
  "clusterName" : "multimaster",
  "sklmUsername" : "sklmadmin",
  "sklmPassword" : "SKLM@admin123",
  "wasUsername" : "wasadmin",
  "wasPassword" : "WAS@admin123",
   "sklmUIPort" : "9443",
  "standbyHadrPort" : "60020"
}
```

Success response

```
Status Code: 200 OK
{"code":"0","status":"CTGKM3002I civ4cez199 met all the pre requisites and can be added
into the cluster."}
```

Error response

```
{"code":"CTGKM6002E",
"message":"CTGKM6002E Bad Request: Invalid user authentication ID or invalid request
format."}
```

REST service for adding a master when other master in the cluster is not reachable

To add a standby or master server to the cluster when a standby or master server in the cluster is out of network or not reachable, use the **Add Master REST Service** with additional parameters, **ignoreStandbys** and **ignoreNodes**.

Operation
POST

URL
`https://<host>:<port>/SKLM/rest/v1/ckms/config/nodes/addNodes`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON object with the following specification:	
Property name	**Description**
clusterName	Specify a name for the multi-master cluster to which the masters to be added.

Request body JSON object with the following specification: *(continued)*	
Property name	**Description**
primaryHadrPort	Specify the port number for the HADR primary database. You must specify the value for this property for the first time only when stand-alone IBM Security Key Lifecycle Manager server instance is configured as "Primary" along with "Standby" or "Node".
type	Specify the IBM Security Key Lifecycle Manager server instance type. For example, `Primary`, `Standby`, or `Node`.
ipHostname	Specify the host name of the IBM Security Key Lifecycle Manager server server.
standbyPriorityIndex	Specify the priority index value for the standby database to takeover when the primary database is down. You can set the priority index to any value in the range 1-3. The standby server with a higher priority index level (lower number) takes precedence over the lower-priority databases.
httpPort	Specify the port number on which the IBM Security Key Lifecycle Manager server server listens for requests from devices that communicate by using the SSL protocol.
sklmUsername	Specify the name of the IBM Security Key Lifecycle Manager server administrator.
sklmPassword	Specify the password for the IBM Security Key Lifecycle Manager server administrator.
wasUsername	Specify the WebSphere Application Server login user ID for the IBM Security Key Lifecycle Manager server administrator profile.
wasPassword	Specify the password for the WebSphere Application Server login user ID.
ignoreStandbys	Specify the host name of standby server that is not reachable.
ignoreNodes	Specify the host name of master server that is not reachable.
autoAccept	Specify whether the cluster automatically accepts the certificate of the master server that is being added. This property has two values: `Yes`, `No`. The default value is `No`, which indicates that the cluster does not automatically accept the certificate of the master server that is being added.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification:	
JSON property name	**Description**
code	Returns the code that is specified by the `status` property.
status	Returns the status to indicate whether the master is added to the multi-master cluster.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request to add master to the cluster when a master or standby server is not reachable

Example for adding a standby.

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/config/nodes/addNodes
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
[
{
"clusterName" : "multimaster",
"primaryHadrPort" : "60027"
"ignoreStandbys" : "cimkc2b151",
"ignoreNodes" : "cimkc2b152"
},
{
"type" : "Standby",
"ipHostname" :  "cimkc2b150",
"httpPort" :  "9443",
"sklmUsername" :  "sklmadmin",
```

```
"sklmPassword" :  "SKLM@admin123",
"wasUsername" :  "wasadmin",
"wasPassword" :  "WAS@admin123",
"standbyPriorityIndex" : "2",
"autoAccept" : "Yes"
}
]
```

Example for adding a master.

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/config/nodes/addNodes
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
[
{
"clusterName" : "multimaster"
"ignoreStandbys" : "cimkc2b151",
"ignoreNodes" : "cimkc2b152"
},
{
"type" : "Node",
"ipHostname" :  "cimkc2b153",
"httpPort" :  "9443",
"sklmUsername" :  "sklmadmin",
"sklmPassword" :  "SKLM@admin123",
"wasUsername" :  "wasadmin",
"wasPassword" :  "WAS@admin123",
"autoAccept" : "Yes"
}
]
```

Success response

```
Status Code: 200 OK
{"code":"0","status":"CTGKM3002I Successfully added the master in Multi-Master cluster."}
```

Error response

```
{"code":"CTGKM6002E",
"message":"CTGKM6002E Bad Request: Invalid user authentication ID or invalid request
format."}
```

Adding a certificate to the truststore

You might add a certificate from a certificate file that is in DER or base64 format to the IBM Security Key Lifecycle Manager internal truststore. The certificate is used for communication between IBM Security Key Lifecycle Manager and the device that identifies itself by using this certificate or the root certificate for this certificate.

About this task

You can use the **Add Certificate** dialog, **tklmTrustStoreCertAdd** command, or **Truststore Certificate Add REST Service** to add a certificate to the IBM Security Key Lifecycle Manager truststore. Your user ID must have the klmSecurityOfficer role.

Procedure

1. Go to the appropriate page or directory.
   - Graphical user interface
     a. Log on to the graphical user interface.
     b. Click **IBM Security Key Lifecycle Manager** > **Configuration** > **Truststore**.
     c. On the **Truststore** page, click **Add**.
   - Command-line interface

a. Go to the *<WAS_HOME>*/bin directory. For example,

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

```
wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
```

Linux

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

- REST interface

  – Open a REST client.

2. Add a certificate from a certificate file that is in DER or base64 format to the truststore.

- Graphical user interface

  a. In the **Certificate alias** field, specify alias name for the certificate.

  b. Click **Browse** to specify the certificate file location under *<SKLM_DATA>* directory, for example, C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data. For the definition of *<SKLM_DATA>*, see "Definitions for HOME and other directory variables" on page 71.

  c. Select the certificate file format such as DER or base64.

  d. Click **Add Certificatre**.

- Command-line interface

  Type **tklmTrustStoreCertAdd** to add a certificate file to the truststore. For example, to add a certificate file in DER format, run the following command.

```
print AdminTask.tklmTrustStoreCertAdd
    ('[-fileName d:\\mypath\\mycertfilename.der
        -format DER -alias myCertAlias]')
```

- REST interface

  Use **Truststore Certificate Add REST Service** to add a certificate. For example, you can send the following HTTP request.

```
PUT https://localhost:<port>/SKLM/rest/v2/trustStoreCertificates/addCertToTrustStore
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"certFile":"C:\\Program Files\\IBM\\WebSphere\\AppServer\\products\\sklm\\data\
\clientsslcert.cer",
"certFormat":"DER","certAlias":"myCert"}
```

Authentication process for REST services

Before you access IBM Security Key Lifecycle Manager REST services, authenticate to the IBM Security Key Lifecycle Manager server by using your user name and password.

You can use a REST client to access the IBM Security Key Lifecycle Manager REST services. To access a REST service, you must complete the following process:

1. Log in to the IBM Security Key Lifecycle Manager server with your login credentials. You can use "Login REST Service" on page 81 to access the server. The "Login REST Service" on page 81 accepts user name and password and returns a unique user authentication identifier.

2. Access the IBM Security Key Lifecycle Manager REST services that provide the required server functions. To access an IBM Security Key Lifecycle Manager REST service, pass the user authentication identifier that you obtained in Step 1 along with the request message.
3. Log out of the IBM Security Key Lifecycle Manager server by using "Logout REST Service" on page 83. To log out, you must pass the user authentication identifier that you obtained in Step 1.

Password policy

The password policy applies to all passwords in IBM Security Key Lifecycle Manager. For example, passwords for users, export files, backup files, replication backup files, and so on. The policy is specified in the `SKLM_DATA/config/TKLMPasswordPolicy.xml` file.

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

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

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

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

IBM Security Key Lifecycle Manager supports these password rules:

Table 8. Password rules. Password policy rules

Rule	**Default value**
Minimum length	6
Maximum length	20 **Note:** Ensure that the value does not exceed 127.
Minimum number of numeric characters	2
Minimum number of alphabetic characters	3
Maximum number of consecutive occurrences of the same character	2
Upper-case characters	At least 1
Lower-case characters	At least 1
Special characters The special character requirement is not enforced when **imcl** tool is used for silent installation. For more information, see https://www.ibm.com/support/pages/supported-special-characters-ibm-security-key-lifecycle-manager-passwords.	At least 1
Disallow the presence of the user ID* in the password	Enabled
Disallow the presence of the user name* in the password	Enabled

* Detection of this value is case-sensitive.

Note: To specify that the value is not case-sensitive, edit the default password policy and specify `CaseInsensitive` for the user ID and user name:

```
<?xml version="1.0" encoding="UTF-8"?>
<PasswordPolicy enabled="true" name="Password policy for TKLM"
    uuid="" version="1.0">
    <Description />
  <PasswordRules><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
      <PasswordRuleSet version="1.0">
        <MinLengthConstraint Min="6"/>
        <MaxLengthConstraint Max="20"/>
        <MaxSequentialChars Max="2"/>
        <MinAlphabeticCharacters Min="3"/>
        <MinDigitCharacters  Min="2"/>
        <NotUserID/>
        <NotUserName/>
     </PasswordRuleSet>
  ]]></PasswordRules>
</PasswordPolicy>
```

Installation images and fix packs

Obtain IBM Security Key Lifecycle Manager installation files from the IBM Passport Advantage® website and fix packs from Fix Central. 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 at http://www-01.ibm.com/software/passportadvantage/pao_customer.html.

You can use Fix Central to find the fixes that are provided by IBM Support for various products, including IBM Security Key Lifecycle Manager at https://www-945.ibm.com/support/fixcentral. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A IBM Security Key Lifecycle Manager product fix might be available to resolve your problem.

Definitions for *HOME* and other directory variables

You can customize the *HOME* directory for your specific implementation. Substitute the definition of the directory variable appropriately.

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

Table 9. HOME and other directory variables

Directory variable	Default definition	Description
DB_HOME	**Windows systems** *drive*:\Program Files\IBM\DB2SKLMV40 **AIX and Linux systems** /opt/IBM/DB2SKLMV40	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 sklmdb40, *DB_INSTANCE_HOME* is C:\SKLMDB40. **Linux and AIX®** /home/*db2adminID*	The directory that contains the Db2 database instance for IBM Security Key Lifecycle Manager.

Table 9. HOME and other directory variables (continued)

Directory variable	Default definition	Description
WAS_HOME	**Windows** *drive*:\Program Files\IBM\WebSphere\AppServer **Linux and AIX** *path*/IBM/WebSphere/AppServer For example: /opt/IBM/WebSphere/AppServer	The WebSphere Application Server home directory.
SKLM_HOME	**Windows** *WAS_HOME*\products\sklm **Linux and AIX** *WAS_HOME*/products/sklm	The IBM Security Key Lifecycle Manager home directory.
SKLM_INSTALL_HOME	**Windows** *drive*:\Program Files\IBM\SKLMV40 **Linux and AIX** *path*/IBM/SKLMV40	The directory that contains the IBM Security Key Lifecycle Manager license and migration files.
SKLM_DATA	**Windows** *WAS_HOME*\products\sklm\data C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data **Linux and AIX** *WAS_HOME*\products\sklm/data /opt/IBM/WebSphere/AppServer/products/sklm/data	The directory that contains the files that are exported from IBM Security Key Lifecycle Manager such as backup files, exported certificates, and device group export files. Also, you must save the files that you want to import into IBM Security Key Lifecycle Manager in this directory.
IM_INSTALL_DIR	**Windows** *drive*:\Program Files\IBM\Installation Manager **Linux and UNIX** /opt/ibm/InstallationManager	The directory where IBM Installation Manager is installed.
IM_DATA_DIR	**Windows** *drive*:\ProgramData\IBM\Installation Manager **Linux and UNIX** /var/ibm/InstallationManager	The data directory, which is used to store information about products that are installed with Installation Manager. **Note:** ProgramData\ is a hidden folder, and to see it you must modify your view preferences in Explorer to show hidden files and folders.

Upgrading IBM Security Key Lifecycle Manager to Version 4.0

Complete the following steps to upgrade earlier versions of IBM Security Key Lifecycle Manager to IBM Security Key Lifecycle Manager 4.0.

1. Review the supported upgrade path and determine the migration method. If the existing version is not at the minimum fix pack level, apply the latest fix pack for the version.
2. Review and complete pre-upgrade tasks.
3. Install IBM Security Key Lifecycle Manager Version 4.0.
4. If you installed the target version on another host server, or if you installed the target version silently, migrate the data.
5. Complete the post-upgrade tasks.

Upgrading IBM Tivoli Key Lifecycle Manager to IBM Security Key Lifecycle Manager 4.0

Upgrading IBM Tivoli Key Lifecycle Manager requires an interim upgrade to IBM Security Key Lifecycle Manager version 2.5, 2.6, or 2.7 before you can upgrade to version 4.0.

Note: The procedure in this documentation considers interim upgrade to IBM Security Key Lifecycle Manager version 2.7.

Procedure

Complete the following steps:

1. Review the supported upgrade path and determine the migration method. If the existing version is not at the minimum fix pack level, apply the latest fix pack for the version.
2. To complete interim upgrade, install IBM Security Key Lifecycle Manager version 2.7.
3. Review and complete the pre-upgrade tasks.
4. Install IBM Security Key Lifecycle Manager V4.0.
5. Migrate the data.

   You need to migrate the data from IBM Tivoli Key Lifecycle Manager to IBM Security Key Lifecycle Manager V2.7, and then from the IBM Security Key Lifecycle Manager V2.7 to IBM Security Key Lifecycle Manager V4.0.
6. Complete the post-upgrade tasks.

Upgrading Encryption Key Manager to IBM Security Key Lifecycle Manager 4.0

You can upgrade Encryption Key Manager to IBM Security Key Lifecycle Manager version 4.0 (target).

Complete the following steps:

1. Review the upgrade path and determine the migration method.
2. Review the restrictions and requirements.
3. Complete the pre-upgrade tasks.
4. Install the target version.
5. If you installed the target version on another host server, or if you skipped data migration during installation, migrate data.
6. Complete post-upgrade tasks.

Applying a fix pack

To apply a fix pack, follow the readme file instructions on the IBM Fix Central website at http://www.ibm.com/support/fixcentral.

To access the website:

1. Go to IBM Fix Central website at http://www.ibm.com/support/fixcentral.
2. Click **Select product**.
3. From the **Product Group** list, select `IBM Security`.
4. From the **Select from IBM Security** list, select `IBM Security Key Lifecycle Manager`.

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.

Installation and migration problems and workarounds

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

Pre-upgrade restrictions and requirements for Encryption Key Manager

You must follow certain rules and guidelines before you can upgrade Encryption Key Manager to IBM Security Key Lifecycle Manager V4.0.

Pre-upgrade requirements

You can upgrade to IBM Security Key Lifecycle Manager V4.0 from Encryption Key Manager, version 2.1 only.

Note: If you are using earlier versions of Encryption Key Manager, upgrade to V2.1. To obtain Encryption Key Manager, V2.1, contact IBM Support at: https://www.ibm.com/mysupport/s/

Pre-upgrade restrictions

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

- Migrate only one Encryption Key Manager server to one IBM Security Key Lifecycle Manager server. To migrate another Encryption Key Manager server, use a separate IBM Security Key Lifecycle Manager server.
- 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.

Restart Server REST Service

Use **`Restart Server REST Service`** to restart the IBM Security Key Lifecycle Manager server. Restart of the server causes the server to read its configuration and accept the configuration changes, if any.

Operation

POST

URL

`https://<host>:<port>/SKLM/rest/v1/ckms/servermanagement/restartServer`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
`host`	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
`port`	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
`Content-Type`	`application/json`
`Accept`	`application/json`
`Authorization`	`SKLMAuth userAuthId=<authIdValue>`
`Accept-Language`	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	application/json
Content-Language	Locale for the response message.

Success response body JSON object with the following specification:	
JSON property name	**Description**
code	Returns the value that is specified by the **message** property.
message	Returns the status message that indicates success or failure of the server restart operation.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request to restart the IBM Security Key Lifecycle Manager server

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/servermanagement/restartServer
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

Success response

```
Status Code : 200 OK
{"code": "CTGKM2936I","message": "CTGKM2936I IBM Security Key Lifecycle Manager Server
restarted successfully.
After restarting the SKLM server, it will be unavailable for few minutes."}}
```

Error response

```
Status Code : 200 OK
{"code": "CTGKM2937E","message": "CTGKM2937E Error restarting IBM Security Key Lifecycle
```

```
Manager Server,
plesae check logs for more information."}
```

Update Db2 Password on Standalone Server REST Service

After the Db2 password is updated at the operating system level, use **Update Db2 Password on Standalone Server REST Service** to update the password on the standalone IBM Security Key Lifecycle Manager server so that Db2 continues to be connected to the IBM Security Key Lifecycle Manager server agent.

Before you begin

Before you use this REST service, ensure that you update the Db2 database password at the operating system level. For more information about the instructions, see "Updating Db2 password on a Windows system" on page 42, "Updating Db2 password on a Linux or AIX system" on page 43.

Operation

PUT

URL

`https://localhost:port/SKLM/rest/v1/ckms/changePassword/db2/standalone`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON object with the following specification:	
Property name	**Description**
newDb2Password	Specify the new Db2 password.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification:	
JSON property name	**Description**
code	Returns the code that is specified by the `status` property.
status	Returns the status of the operation.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Update database password on IBM Security Key Lifecycle Manager server standalone server

```
PUT https://localhost:port/SKLM/rest/v1/ckms/changePassword/db2/standalone
{
"newDb2Password" : "SKLM@db2"
}
```

Success response

```
{"code":"0",
"status":"CTGKM3012I DB2 password for IBM Security Key Lifecycle Manager instance updated
successfully."}
```

Error response

```
{"code":"CTGKM0630E",
"status":"CTGKM0630E Validation error: Invalid name for parameter newDb2Password."}
```

Update Db2 Password in Multi-Master Cluster REST Service

After you update the Db2 password on the operating system of each master server, use **Update Database Password in Multi-Master Cluster REST Service** to update the password in the Multi-Master cluster so that Db2 continues to be connected to the IBM Security Key Lifecycle Manager server agent.

Before you begin

Before you use this REST service, ensure that you update the Db2 database password on the operating system of each master server.

Operation

PUT

URL

`https://localhost:port/SKLM/rest/v1/ckms/changePassword/db2/multimaster`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON object with the following specification:	
Property name	**Description**
newDb2Password	Specify the new Db2 password.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification:	
JSON property name	**Description**
code	Returns the code that is specified by the `status` property.
status	Returns the status of the operation.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Update database password on Multi-Master cluster

```
PUT https://localhost:port/SKLM/rest/v1/ckms/changePassword/db2/multimaster
{
"newDb2Password" : "SKLM@db2"
}
```

Success response

```
{
    "code": "CTGKM3448I",
    "status": "CTGKM3448I Db2 password changed successfully.
Services on the IBM Security Key Lifecycle Manager servers will resume shortly."
}
```

Error response

```
{"code":"CTGKM0630E",
"status":"CTGKM0630E Validation error: Invalid name for parameter newDb2Password."}
```

Adding an existing IBM Security Key Lifecycle Manager instance with data to the Multi-Master cluster

You can use the export and import feature of IBM Security Key Lifecycle Manager to add data from an existing IBM Security Key Lifecycle Manager instance to the Multi-Master cluster. You must import the data that was exported from the existing stand-alone instance to the Primary master server that is configured with DB2 HADR.

About this task

You cannot directly add an existing stand-alone instance with data into the cluster. You must first import data from the existing IBM Security Key Lifecycle Manager instance to the primary master. Then, add a master server into the cluster separately.

After data is imported, the data is available on all instances in the cluster. It is up to you to decide whether to add a master separately.

Procedure

1. Export device group data from the existing IBM Security Key Lifecycle Manager instance. For more information about how to export device group data, see "Exporting a device group" on page 102.
2. Import the data that was exported from the existing stand-alone instance to the primary master server that is configured with DB2 HADR. For more information about how to import device group data, see "Importing a device group" on page 103.
3. After you successfully import data to the primary server, you can access data from all the masters in the cluster. If you need a dedicated IBM Security Key Lifecycle Manager master to access the imported data, add a master to the cluster. For more information about adding a master, see "Adding a master server to a cluster" on page 49.

What to do next

You might want to decommission the existing stand-alone IBM Security Key Lifecycle Manager instance after you successfully exported the data.

Login REST Service

Use **`Login REST Service`** to log in to the IBM Security Key Lifecycle Manager server with valid user credentials. The REST service validates the credentials and returns a unique user authentication identifier for all subsequent service requests.

Operation

POST

URL

`https://<host>:<port>/SKLM/rest/v1/ckms/login`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
`host`	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.

Request Parameters (continued)	
Parameter	**Description**
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`

Request body JSON Object with the following specification:	
Parameter	**Description**
userid	Specify the user ID to access the IBM Security Key Lifecycle Manager server.
password	Specify the password that is associated with the user ID.

Response

Response headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`

Success response body JSON object with the following specification:	
JSON property name	**Description**
userAuthId	Returns a unique identifier for the authenticated user.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.

Error Response Body JSON object with the following specification. *(continued)*	
JSON property name	**Description**
message	Returns a message that describes the error.

Examples

Service request for user authentication

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/login
Content-Type: application/json
Accept : application/json
{"userid" : "admin1", "password" : "pswd"}
```

Success response

```
Status Code : 200 OK
{"userAuthId" : "37ea1939-1374-4db7-84cd-14e399be2d20"}
```

Error response

```
Status Code : 401 Unauthorised
{"code" : "CTGKM6001E", "message" : "Authentication Failure :
Incorrect user ID/password combination"}
```

Logout REST Service

Use **Logout REST Service** to stop the user session and log out of the IBM Security Key Lifecycle Manager server. The server automatically logs out the user after 15 minutes of inactivity.

Operation
DELETE

URL
https://<*host*>:<*port*>/SKLM/rest/v1/ckms/logout

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request headers	
Header name	**Value**
Content-Type	application/json

Request headers (continued)	
Header name	**Value**
Accept	`application/json`

Request body JSON Object with the following specification:	
JSON property name	**Description**
userAuthId	Specify the user authentication identifier that you must use to log out from the IBM Security Key Lifecycle Manager server.

Response

Response headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`

Success response body JSON object with the following specification:	
JSON property name	**Description**
userId	Returns the user identifier.
logout	Indicates whether the user is logged out of the server. Valid values are `true` or `false`.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request for user logout

```
DELETE https://localhost:<port>/SKLM/v1/ckms/logout
Content-Type: application/json
Accept : application/json
{"userAuthId" : "37ea1939-1374-4db7-84cd-14e399be2d20"}
```

Success response

```
Status Code : 200 OK
{"userid" : "admin","logout" : "true”}
```

Error response

```
Status Code : 400 Bad Request
{"code" : ""CTGKM6002E"", "message" : "Invalid Request: Invalid user
authentication ID or invalid request format"}
```

Pre-upgrade tasks for IBM Security Key Lifecycle Manager

Complete the required tasks before you upgrade IBM Security Key Lifecycle Manager.

1. Download and extract the installation files for the target version. See “Software download instructions” on page 105.
2. Review the system requirements to ensure that your host system meets the minimum requirements. See the technote: IBM Security Key Lifecycle Manager Support Matrix.
3. Obtain the administrative passwords for the existing version of IBM Security Key Lifecycle Manager.
4. Review the following considerations:
   - 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 server has the expected keys and other configuration attributes that you intended to migrate.
   - Ensure that there is sufficient disk space on your system. These disk space requirements are in addition to disk space requirements that are identified by the installer for installing the target version, and its prerequisite software.

     The additional disk space is required for the migration process to move users, keys, and other metadata in the database of the existing version of the IBM Security Key Lifecycle Manager server to version 4.0 of the server.
   - Stop IBM Security Key Lifecycle Manager and any replica server. Key serving cannot be active during migration.
   - During the inline migration process, examine the *IM_DATA_DIR*`/logs/sklmLogs/migration.log` file frequently to determine the progress of migration.
   - Ensure that the migration process is not interrupted. Do not start or stop the Db2 server or the WebSphere Application Server outside of the migration process.

What to do next

Depending on the mode that you want to use for installing the target version of IBM Security Key Lifecycle Manager, see the topic:

- “Upgrading: Installing IBM Security Key Lifecycle Manager in graphical mode” on page 86
- “Upgrading: Installing IBM Security Key Lifecycle Manager silently” on page 87

Upgrading: Installing IBM Security Key Lifecycle Manager in graphical mode

Use the IBM Installation Manager installation wizard to install IBM Security Key Lifecycle Manager in a graphical mode.

About this task

When you start the install process from the Launchpad program, IBM Installation Manager is automatically installed if it is not already available on your system. Also, the install process detects the existing (source) version of IBM Security Key Lifecycle Manager or Encryption Key Manager that is installed on the host system. If you are installing on another host system, the install process performs a fresh installation of IBM Security Key Lifecycle Manager.

Procedure

1. Go to the directory of your installation package and open `disk1`. For example: *download_path*`/disk1`
2. Start the installation program.

Operating system	Command to run
Windows	**`launchpad.bat`**
Linux or AIX	**`launchpad.sh`**

3. Select the locale that you want to use for the installation process. The locale determines the language that the installer runs in. Type the number that is displayed next to your locale and press Enter. The Installation Manager wizard is displayed.
4. In the **Install Packages** window, click each of the product packages to highlight them. The description of the package is displayed in the **Details** section at the bottom of the window. To fully understand the package that you are installing, review all information.
5. Select the product packages to install. All the packages are selected for installation by default.
6. Click **Next**.

   The prerequisite checks verify the prerequisite requirements for the installation.
7. Select **I accept the terms in the license agreements** and click **Next**.
8. Select a location for the shared resources directory and click **Next**.

   Note: Retain the default path for shared resources directory, for example, `C:\Program Files\IBM\IBMIMShared`. IBM Installation Manager uses this location to download artifacts and to store information about the installed packages.
9. On the **Location** page, the location of the package group into which each product is installed is displayed. Click each product to see its package group location. Click **Next**.
10. On the next page, select the translation packages to install and click **Next**.
11. On the **Features** page, select the package features to install.
    a. To see the dependency relationships between features, select **Show dependencies**.
    b. Click a feature to view its brief description under **Details**.
    c. When you are finished selecting features, click **Next**.
12. On the **Configuration for IBM DB2** page, specify the database configuration information and click **Next**.

    For more information, see DB2 configuration parameters and DB2 configuration during installation.
13. **If you are installing IBM Security Key Lifecycle Manager on the same host system on which the existing version is installed**: Specify configuration details of the existing version.
    - (**For IBM Security Key Lifecycle Manager version 2.5 or later**):

On the **Configuration for IBM Security Key Lifecycle Manager** page, based on the source version from where you are upgrading, specify the configuration information for the following components: IBM Security Key Lifecycle Manager and WebSphere Application Server. Then, click **Next**.

For more information, see WebSphere Application Server and IBM Security Key Lifecycle Manager server configuration parameters and Configuration during installation.

- (**For Encryption Key Manager version 2.1**):

  Select **Migrate Encryption Key Manager**, specify the property file location, click **Next**.

14. On the **Summary** page, review your choices before you install the product package. To change a selection, click **Back** to return to your selections.
15. To begin the installation, click **Install**.

    A progress indicator shows the percentage of the installation that is completed. When the installation process is complete, a message confirms the completion of the process.
16. Click **View Log File** to open the installation log file and to verify that all of the components were installed properly.
17. In the Install Package wizard, select **None** to instruct the installer not to create a profile.
18. Click **Finish** to complete the installation task and to close the wizard.

What to do next

Depending on the version that you are upgrading from, go to the next step from the topic:

- Upgrading Encryption Key Manager
- Upgrading IBM Tivoli Key Lifecycle Manager
- Upgrading IBM Security Key Lifecycle Manager

Upgrading: Installing IBM Security Key Lifecycle Manager silently

You can choose to migrate data during the installation of IBM Security Key Lifecycle Manager V 4.0 (target) or migrate the data as a separate step.

Before you begin

- Read the license terms for the product. To locate the license term files, in the root directory in which the installation package is located, navigate to the `disk1/im/license` subdirectory. The`/license` subdirectory has the license files in text format.
- Select the appropriate sample response file to create the response file to be used for the installation.

  IBM Security Key Lifecycle Manager includes platform-specific sample response files that you can use as a template for creating your own response file. A separate response file is available depending on the operating system of the host system and the data migration approach.

Table 10. Response files

Approach	**Sample response file name**	**Example: Install target version on a host system that is running Linux with existing (source) version as 3.0**
Install IBM Security Key Lifecycle Manager target version with inline data migration	`SKLM_Silent_`*`platform`*`_Mig_`*`version`*`_Resp.xml`	`SKLM_Silent_Linux_Mig_30_Resp.xml`

Table 10. Response files (continued)		
Approach	**Sample response file name**	**Example: Install target version on a host system that is running Linux with existing (source) version as 3.0**
Install IBM Security Key Lifecycle Manager target version only (Skip data migration during installation)	SKLM_Silent_*platform*_Resp.xml	SKLM_Silent_Linux_Resp.xml

Where,

– *platform* is the operating system that is running on the host system.

– *version* is the existing (source) version of IBM Security Key Lifecycle Manager or Encryption Key Manager.

The response files are available in the root directory of the installation image files.

- If you are upgrading from Encryption Key Manager, use the SKLM_Silent_*platform*_Resp.xml response file.
- Obtain the encrypted values of the passwords for following administrators of the source version: IBM Security Key Lifecycle Manager, WebSphere Application Server, and database.

  Also, create an encrypted password for the database administrator of the target version.

  These passwords are used in the silent inline migration procedure.

  To create the encrypted password, use the IBM Installation Manager utility. For more information, see Encrypted password for response file elements.
- Ensure that the correct administrator password is specified in the response file.

Procedure

1. Open the sample response file in edit mode and update the following parameters:

   repository location
   Specify the full path to the directory in which the installation package is located.

   Note: If you enter an invalid value for this parameter, the installation program exits without an error message. Also, the error is not logged.

   The file has two instances of this parameter and both must be updated. Specify the values as shown here:

   ```
   <repository location='myRepositoryLocation\im'/>
   <repository location='myRepositoryLocation\'/>
   ```

   where *myRepositoryLocation* is the full path to the installation package directory.

   For example, if the installation package exists in the *C:\SKLM40* directory, update this parameter as follows:

   ```
   <repository location='/SKLM40/disk1/im'/>
   <repository location='/SKLM40/disk1/'/>
   ```

   user.DB2_ADMIN_PWD,com.ibm.sklm40.db2.*platform*.ofng
   Specify the encrypted password for the database administrator of the target version.

   For example:

   ```
   <data key='user.DB2_ADMIN_PWD,com.ibm.sklm40.db2.linux.ofng' value='QTh/
   0AiFacssjhs9gnOYkGA=='/>
   ```

user.CONFIRM_PASSWORD,com.ibm.sklm40.db2.*platform*.ofng
Specify the same password that you provided in the **user.DB2_ADMIN_PWD,com.ibm.sklm40.db2.*platform*.ofng** parameter.

For example:

```
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm40.db2.linux.ofng' value='QTh/
0AiFacssjhs9gnOYkGA==' />
```

user.WAS_HOME,com.ibm.sklm40.*platform*
Specify the *WAS_HOME* directory path for WebSphere Application Server of the target version. For the definition of *WAS_HOME*, see "Definitions for HOME and other directory variables" on page 71.

For example:

```
<data key='user.WAS_HOME,com.ibm.sklm40.linux' value='/opt/IBM/WebSphere/AppServer' />
```

user.WAS_ADMIN_ID,com.ibm.sklm40.*platform*
Specify the user ID for the WebSphere Application Server administrator of the source version.

For example:

```
<data key='user.WAS_ADMIN_ID,com.ibm.sklm40.linux' value='wasadmin' />
```

user.WAS_ADMIN_PASSWORD,com.ibm.sklm40.*platform*
Specify the encrypted password for the WebSphere Application Server administrator of the source version. This password is used for the target WebSphere Application Server administrator.

For example:

```
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm40.linux'
value='e9PjN93MeQxyzSs9VXJFMw==' />
```

user.WAS_ADMIN_CONF_PWD,com.ibm.sklm40.*platform*
Specify the same password that you provided in the **user.WAS_ADMIN_CONF_PWD,com.ibm.sklm40.***platform* parameter.

For example:

```
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm40.linux'
value='e9PjN93MeQxyzSs9VXJFMw==' />
```

user.SKLM_ADMIN_USER,com.ibm.sklm40.*platform*
Specify the user ID for the IBM Security Key Lifecycle Manager administrator of the source version.

For example:

```
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm40.linux' value='sklmadmin' />
```

user.SKLM_ADMIN_PASSWORD,com.ibm.sklm40.*platform*
Specify the encrypted password for the IBM Security Key Lifecycle Manager administrator of the source version. This password applies to the IBM Security Key Lifecycle Manager administrator of the target version.

For example:

```
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm40.linux'
value='9YTRJMRIydDSdfhaHPs1mn==' />
```

user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm40.*platform*
Specify the same password that you provided in the **user.SKLM_ADMIN_PASSWORD,com.ibm.sklm40.***platform* parameter.

For example:

```
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm40.linux'
value='9YTRJMRIydDSdfhaHPs1mn==' />
```

user.TKLM_VERSION,com.ibm.sklm40.*platform*
Specify the source IBM Security Key Lifecycle Manager version.

For example, if you are upgrading from version 3.0 on a server that is running on Linux, update this parameter as follows:

```
<data key='user.TKLM_VERSION,com.ibm.sklm40.linux' value='3.0.0.0'/>
```

user.TKLM_TIP_HOME,com.ibm.sklm40.*platform*
For IBM Security Key Lifecycle Manager 2.5 and later, specify the *WAS_HOME* directory path for the WebSphere Application Server of the source version. For the definition of *WAS_HOME*, see "Definitions for HOME and other directory variables" on page 71.

For example:

```
<data key='user.TKLM_TIP_HOME,com.ibm.sklm40.linux' value='/opt/IBM/WebSphere/
AppServer'/>
```

user.TKLM_INSTALLED,com.ibm.sklm40.*platform*
Ensure that the value is `true`, which indicates that an earlier version of IBM Security Key Lifecycle Manager is already installed on the server.

For example:

```
<data key='user.TKLM_INSTALLED,com.ibm.sklm40.linux' value='true'/>
```

user.TKLM_DB_PWD,com.ibm.sklm40.*platform*
Specify the encrypted password for the database of the source version.

For example:

```
<data key='user.TKLM_DB_PWD,com.ibm.sklm40.linux' value='SwIhGBTDHcJok80Ux4Sb3g==''/>
```

user.SKLM_APP_PORT,com.ibm.sklm40.*platform*
Specify the port number that the IBM Security Key Lifecycle Manager server of the target version listens on for HTTPS requests.

For example:

```
<data key='user.SKLM_APP_PORT,com.ibm.sklm40.linux' value='8443'/>
```

user.WAS_ADMIN_PORT,com.ibm.sklm40.*platform*
Specify the port number that the WebSphere Application Server of the target version listens on for requests.

For example:

```
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm40.linux' value='8083'/>
```

user.SKLM_APP_NS_PORT,com.ibm.sklm40.*platform*
Specify the port number that the IBM Security Key Lifecycle Manager server of the target version listens on for HTTP requests.

For example:

```
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm40.linux' value='8080'/>
```

2. **Only when upgrading from Encryption Key Manager with inline migration**: Set the following properties in the response file.

user.EKM_PROPFILE,@OFFERINGIDPREFIX@.linux
Specify the properties file name.

For example:

```
<data key='user.EKM_PROPFILE,@OFFERINGIDPREFIX@.linux' value='/opt/IBM/
KeyManagerConfig.properties'/>
```

user.EKM_MIGRATION,@OFFERINGIDPREFIX@.linux
Specify `false` to indicate that data is to be migrated inline.

For example:

```
<data key='user.EKM_MIGRATION,@OFFERINGIDPREFIX@.linux' value='false'/>
```

3. Save the response file and close it.
4. Check whether the Db2 JAR file `db2jcc.jar` exists in the installation directory. If not, copy the file from the installation package into the installation directory.

   For example, copy the file from `disk1/im/jre_7.0.9040.20160504_1613/jre/lib/ext` into `/opt/IBM/InstallationManager/eclipse/jre_7.0.9040.20160504_1613/jre/lib/ext`.
5. Open command line and run the silent installation command as follows:

   ```
   ./silent_install.sh myResponseFile -acceptLicense
   ```

   Where, *myResponseFile* is the response file that you want to use. For example, `SKLM_Silent_Linux_30_Resp.xml`.

   By specifying the **-acceptLicense** parameter, you agree to and accept the license terms for this product.
6. Verify that the installation was successful by reviewing the log files. You can view the IBM Installation Manager logs at the following locations.

   Windows
   `drive:\<IM_DATA_DIR>\logs\native`.

   For example, `C:\ProgramData\IBM\Installation Manager\logs\native`.

   `drive:\<IM_DATA_DIR>\logs\sklmLogs\`.

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

   Linux
   `/<IM_DATA_DIR>/logs/native`.

   For example, `/var/ibm/installationmanager/logs/native`.

   `/<IM_DATA_DIR>/logs/sklmLogs/`.

   For example, `/var/ibm/InstallationManager/logs/sklmLogs/`.

   For the definition of *<IM_DATA_DIR>*, see "Definitions for HOME and other directory variables" on page 71.

What to do next
Depending on the version that you are upgrading from, go to the next step from the topic:

- Upgrading Encryption Key Manager
- Upgrading IBM Tivoli Key Lifecycle Manager
- Upgrading IBM Security Key Lifecycle Manager

Post-upgrade tasks for IBM Security Key Lifecycle Manager

Validate the configuration and protect the data by completing the post-upgrade tasks on the target version of IBM Security Key Lifecycle Manager.

General

1. For IBM Security Key Lifecycle Manager on Linux or AIX:

a. Manually update the IPP port number in the IBM Security Key Lifecycle Manager server. Ensure that the value is greater than 1024.

b. Reconfigure the IPP port number in all the clients or devices that are connected to the IBM Security Key Lifecycle Manager server.

2. Validate that the required services, ports, and processes are running.
3. Add rollover entries, if any, by using the graphical user interface or command-line interface.

   This task is required only if in the earlier version of IBM Security Key Lifecycle Manager, you have marked a certificate as a 3592 rollover or a key group as an LTO rollover for future administrative use. If the scheduled future date for rollover is earlier than the time of upgrade, the upgrade process adds an appropriate message and does not migrate these rollover entries automatically. Hence, you need to add these rollover entries manually.

   Rollovers that are configured for LTO key groups and 3592 certificates are not automatically restored from the earlier versions of IBM Security Key Lifecycle Manager. You must manually set the rollover for certificates and key groups.
4. Immediately after the upgrade, back up IBM Security Key Lifecycle Manager, Version 4.0.

   Retain a copy of version 4.0 backup files in a location that is not in the IBM Security Key Lifecycle Manager, Version 4.0 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_DATA_DIR>*`/logs/sklmLogs/migration.log` files for future reference.
5. Review the following considerations:

   - The upgrade process creates clients and associates them with certificates that did not have associated clients before upgrade. Objects that are associated with the certificates are also automatically added to the new clients.

     Certificate names are used as client names. If two clients have the same name, a random string is appended to each of them. If you want, you can modify the client name as per your requirement.
   - 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.
   - IBM Security Key Lifecycle Manager stores information about data served to clients in a database table. If the number of records is equal to or greater than 100000, the data is archived during the cross-migration operation.
   - Retain a replica of the earlier version of IBM Security Key Lifecycle Manager to ensure that you have a working environment and data in case data validation post upgrade determines that there is a problem with version 4.0.

     The upgrade process does not remove the earlier version of IBM Security Key Lifecycle Manager.

     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_DATA_DIR>*`/logs/sklmLogs/migration.log` file for messages and take the appropriate manual actions.
   - 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.
6. Ensure that the paths for properties in the `SKLMConfig.properties`, `datastore.properties`, and `ReplicationSKLMConfig.properties` files are correct.
7. Remove the earlier version of IBM Security Key Lifecycle Manager. For instructions, use the procedure from the respective version's topic in the IBM Knowledge Center.
8. Resolve possible problems with certificates and keys.

Earlier versions of IBM Security Key Lifecycle Manager do not restrict device groups to which a certificate and its keys can be associated. Certificates and keys that belong to multiple device types in the earlier IBM Security Key Lifecycle Manager versions are marked as `CONFLICTED` at version 4.0. 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.

LDAP configuration

If the earlier version of IBM Security Key Lifecycle Manager was configured with LDAP, add users by running the **addLDAPUserToGroup** LDAP configuration script.

All the LDAP users from the earlier version are not migrated to V4.0 during data migration. Only the LDAP user that is used for the IBM Security Key Lifecycle Manager Administrator role during the installation process is migrated. You must explicitly add all other LDAP users after the upgrade process completes.

Inline migration

During inline migration, if the IBM Security Key Lifecycle Manager V4.0 is installed but the data migration task fails, start the stand-alone migration-recovery script.

Note: Use the migration-recovery script before you make any updates or changes to the IBM Security Key Lifecycle Manager configuration post upgrade.

Multi-Master configuration

If you performed cross-migration and had Multi-Master cluster in the earlier version of IBM Security Key Lifecycle Manager, set up the Multi-Master cluster in the upgraded version.

Migration failure

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.

What to do next

From the **Welcome** page, configure the drive types, keys, and certificates that your organization requires, or get started with using the product.

Cross-migrating IBM Tivoli Key Lifecycle Manager, Version 1.0 data

Use the IBM Security Key Lifecycle Manager backup and restore utilities to cross-migrate IBM Tivoli Key Lifecycle Manager, Version 1.0 data.

About this task

Cross-migration of IBM Tivoli Key Lifecycle Manager, Version 1.0 data to IBM Security Key Lifecycle Manager, Version 4.0 consists of the following two stages:

1. Migrating IBM Tivoli Key Lifecycle Manager, Version 1.0 data to a system where IBM Security Key Lifecycle Manager, Version 2.7 is installed by following steps that are described in the IBM Security Key Lifecycle Manager, Version 2.7 documentation.

   Backing up IBM Tivoli Key Lifecycle Manager, Version 1.0 data

   Restoring IBM Tivoli Key Lifecycle Manager Version 1.0 backup files
2. Migrating IBM Security Key Lifecycle Manager, Version 2.7 data on a system where IBM Security Key Lifecycle Manager, Version 4.0 is installed by using steps that are described in the following topics.

   “Backing up data of an earlier version of IBM Security Key Lifecycle Manager” on page 108

"Restoring the backup file of an earlier version of IBM Security Key Lifecycle Manager" on page 111

What to do next
Complete the post-upgrade tasks

Cross-migrating IBM Tivoli Key Lifecycle Manager, Version 2.0 data

Use the IBM Security Key Lifecycle Manager backup and restore utilities to cross-migrate IBM Tivoli Key Lifecycle Manager, Version 2.0 data.

About this task
Cross-migration of IBM Tivoli Key Lifecycle Manager, Version 2.0 data to IBM Security Key Lifecycle Manager, Version 4.0 consists of the following two stages:

1. Migrating IBM Tivoli Key Lifecycle Manager, Version 2.0 data to a system where IBM Security Key Lifecycle Manager, Version 2.7 is installed by following steps that are described in the IBM Security Key Lifecycle Manager, Version 2.7 documentation.

   Backing up IBM Tivoli Key Lifecycle Manager, Version 2.0 data

   Restoring IBM Tivoli Key Lifecycle Manager Version 2.0 backup files
2. Migrating IBM Security Key Lifecycle Manager, Version 2.7 data on a system where IBM Security Key Lifecycle Manager, Version 4.0 is installed by using steps that are described in the following topics.

   "Backing up data of an earlier version of IBM Security Key Lifecycle Manager" on page 108

   "Restoring the backup file of an earlier version of IBM Security Key Lifecycle Manager" on page 111

What to do next
Complete the post-upgrade tasks

Cross-migrating IBM Tivoli Key Lifecycle Manager, Version 2.0.1 data

Use the IBM Security Key Lifecycle Manager backup and restore utilities to cross-migrate IBM Tivoli Key Lifecycle Manager, Version 2.0.1 data.

About this task
Cross-migration of IBM Tivoli Key Lifecycle Manager, Version 2.0.1 data to IBM Security Key Lifecycle Manager, Version 4.0 consists of the following two stages:

1. Migrating IBM Tivoli Key Lifecycle Manager, Version 2.0.1 data to a system where IBM Security Key Lifecycle Manager, Version 2.7 is installed by following steps that are described in the IBM Security Key Lifecycle Manager, Version 2.7 documentation.

   Backing up IBM Tivoli Key Lifecycle Manager, Version 2.0.1 data

   Restoring IBM Tivoli Key Lifecycle Manager Version 2.0.1 backup files
2. Migrating IBM Security Key Lifecycle Manager, Version 2.7 data on a system where IBM Security Key Lifecycle Manager, Version 4.0 is installed by using steps that are described in the following topics.

   "Backing up data of an earlier version of IBM Security Key Lifecycle Manager" on page 108

   "Restoring the backup file of an earlier version of IBM Security Key Lifecycle Manager" on page 111

What to do next
Complete the post-upgrade tasks

Backing up Encryption Key Manager data

Use the IBM Security Key Lifecycle Manager, Version 4.0 backup utility to create Encryption Key Manager, Version 2.1 backup files.

Before you begin

- You must install IBM Security Key Lifecycle Manager, Version 4.0 on a system.
- Ensure that the Encryption Key Manager folder contains the configuration file, keystore files, other data files and folders that are related to drivetable, key groups, and metadata.

About this task

You can use the backup utility to create cross-platform backup files in a manner that is independent of operating systems and directory structure of the server. You can restore these cross-platform compatible backup files on a system with IBM Security Key Lifecycle Manager, Version 4.0 across operating systems.

Note: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedure

1. Copy the Encryption Key Manager folder and all other necessary files to a system where IBM Security Key Lifecycle Manager, Version 4.0 is installed.
2. Ensure that the `KeyManagerConfig.properties` file and the following files that are mentioned in the `KeyManagerConfig.properties` file are copied.

   Note: You must edit the `KeyManagerConfig.properties` configuration file in Encryption Key Manager folder to specify absolute paths of keystore and other data files as shown in the following example.

   ```
   Admin.ssl.keystore.name=C\:/EKM21/test.keys.ssl
   Admin.ssl.truststore.name=C\:/EKM21/test.keys.ssl
   TransportListener.ssl.truststore.name=C\:/EKM21/test.keys.ssl
   TransportListener.ssl.keystore.name=C\:/EKM21/test.keys.ssl
   config.keystore.file=C\:/EKM21/test.keys.jceks
   config.drivetable.file.url=FILE\:C\:/EKM21/filedrive.table
   Audit.handler.file.directory=C\:/audit
   Audit.metadata.file.name=C\:/EKM21/metadata/EKMData.xml
   config.keygroup.xml.file=FILE\:C\:/EKM21/KeyGroups.xml
   ```

3. Locate backup utilities folder in the system where version 4.0 is installed.

   Windows

   `<SKLM_INSTALL_HOME>\migration\utilities\ekm21`

   Default location is `C:\Program Files\IBM\SKLMV40\migration\utilities\ekm21`.

   Linux

   `<SKLM_INSTALL_HOME>/migration/utilities/ekm21`

   Default location is `/opt/IBM/SKLMV40/migration/utilities/ekm21`.

4. Edit `backup.properties` in the backup utilities folder to configure properties as shown in the following example. You must set values for all the properties, except for the `BACKUP_DIR` property (optional).

   If you do not specify the value for `BACKUP_DIR`, the backup file is created in the `backup` subfolder under the same directory from where you run the backup utility.

   Note: On Windows operating system, the `backup.properties` file that you use for backup operations must not contain the property keys and values with leading or trailing spaces.

Windows

```
KLM_VERSION=2.1
BACKUP_DIR=C:\\ekm_backup
EKM_HOME=C:\\EKM21
BACKUP_PASSWORD=passw0rd123
JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0
```

Linux

```
KLM_VERSION=2.1
BACKUP_DIR=/ekm_backup
EKM_HOME=/EKM21
BACKUP_PASSWORD=passw0rd123
JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0
```

Note: On Windows system, when you specify path in the properties file, use either "/ " or "\\ " as path separator as shown in following example.

```
C:\\ekm_backup
```

Or

```
C:/ekm_backup
```

5. Open a command prompt and run the backup utility.

   Windows

   Go to the *<SKLM_INSTALL_HOME>*\migration\utilities\ekm21 directory and run the following command:

   ```
   backupEKM21.bat
   ```

   Linux

   a. Go to the ekm21 directory (see Step b).

   b. Check whether the backupEKM21.sh file has executable permissions. If not, give permissions by running the following command:

   ```
   chmod 755 backupEKM21.sh
   ```

   c. Run the backup utility:

   ```
   backupEKM21.sh
   ```

6. Verify the backup operation:

   - Review the directory that contains backup files to ensure that the backup file exists. The backup files are created in the location that you specified for BACKUP_DIR in the backup.properties file.
   - Check the backup.log file for errors or exceptions. The backup.log file is created in the same directory where you run the backup utility. For a successful backup operation, ensure that there are no errors or exceptions in the log file.
   - Retain the backup password for future use in case you restore the backup.
   - Do not edit a file in the backup archive. The file that you attempt to edit becomes unreadable.

What to do next

“Restoring the Encryption Key Manager backup to IBM Security Key Lifecycle Manager” on page 97

Restoring the Encryption Key Manager backup to IBM Security Key Lifecycle Manager

You can restore the Encryption Key Manager, Version 2.1 cross-platform backup files on a system with IBM Security Key Lifecycle Manager, Version 4.0 by using graphical user interface, command-line interface, REST interface, or the migration restore script.

Before you begin

Install IBM Security Key Lifecycle Manager, Version 4.0 on a system. You must have the Encryption Key Manager backup file and ensure that you have the password that you used when the backup file was created.

Note: You must have IBM Security Key Lifecycle Manager User role to run the backup and restore operations.

About this task

You can restore Encryption Key Manager cross-platform compatible backup files on a system with IBM Security Key Lifecycle Manager, Version 4.0 across operating systems.

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

Note: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedure

1. Log on to the system where IBM Security Key Lifecycle Manager, Version 4.0 is installed.
2. Copy the backup file, for example `sklm_vEKM21_20170420113253+0530_backup.jar`, from Encryption Key Manager, Version 2.1 system to a folder of your choice under *<SKLM_DATA>* directory, for example, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. For the definition of *<SKLM_DATA>*, see "Definitions for HOME and other directory variables" on page 71.
3. Restore the backup file by using any of the following methods.
   - **Graphical user interface**
     a. Log on to the graphical user interface as an authorized user, for example, `SKLMAdmin`.
     b. On the **Welcome** page, click **Administration** > **Backup and Restore**.
     c. Click **Browse** to specify the Encryption Key Manager backup file location under *<SKLM_DATA>* directory.
     d. Click **Display Backups** to display the backup files that you want to restore.
     e. In the **Backup and Restore** table, select a backup file.
     f. Click **Restore From Backup**.
     g. On the **Restore Backup** page, specify the backup password that you used to create the backup file.
     h. Click **Restore Backup**.
     i. Restart IBM Security Key Lifecycle Manager server.
   - **Command-line interface**
     a. Go to the *<WAS_HOME>*`/bin` directory. For example,

     Windows

     ```
     cd drive:\Program Files\IBM\WebSphere\AppServer\bin
     ```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

```
wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
```

Linux

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

c. Run the **tklmBackupRunRestore** CLI command by specifying the parameters such as the backup file name with its full path and backup password that you used to create the backup as shown in the following example.

```
print AdminTask.tklmBackupRunRestore
    ('[-backupFilePath <SKLM_DATA>/sklm_vEKM21_20170420113253+0530_backup.jar
        -password myBackupPwd]')
```

d. Restart IBM Security Key Lifecycle Manager server.

- **REST interface**

a. Open a REST client.

b. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.

c. To invoke **Backup Run Restore REST Service**, send the HTTP POST request with backup file name with its full path and backup password as parameters. Pass the user authentication identifier that you obtained in Step b along with the request message as shown in the following example.

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/restore
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
{"backupFilePath":"<SKLM_DATA>/sklm_vEKM21_20170420113253+0530_backup.jar
backup.jar","password":"myBackupPwd"}
```

d. Restart IBM Security Key Lifecycle Manager server.

- **Migration restore script**

a. Locate the IBM Security Key Lifecycle Manager restore utilities.

Windows

<*SKLM_INSTALL_HOME*>\migration\utilities\ekm21

Default location is C:\Program Files\IBM\SKLMV30\migration\utilities\ekm21.

Linux

<*SKLM_INSTALL_HOME*>/migration/utilities/ekm21

Default location is /opt/IBM/SKLMV40/migration/utilities/ekm21.

b. Edit restore.properties in the ekm21 folder to configure properties as shown in the following example:

Note: On Windows operating system, the restore.properties file that you use for restore operations must not contain the property keys and values with leading or trailing spaces.

Window

```
WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer
JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0
BACKUP_PASSWORD=passw0rd123
DB_PASSWORD=db2_password
```

```
RESTORE_FILE=<SKLM_DATA>\\sklm_vEKM21_20170424024117-0400_backup.jar
WAS_USER_PWD=wasadmin_password
RESTORE_USER_ROLES=n
```

Linux

```
WAS_HOME=/opt/IBM/WebSphere/AppServer
JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0
BACKUP_PASSWORD=passw0rd123
DB_PASSWORD=db2_password
RESTORE_FILE=<SKLM_DATA>/20170424024117-0400_backup.jar
WAS_USER_PWD=wasadmin_password
RESTORE_USER_ROLES=n
```

To log in to IBM Security Key Lifecycle Manager by using the user credentials that are specified during product installation, set the **RESTORE_USER_ROLES** property set as "n ". Setting the property to "n " ensures that user ID and the password are not overwritten with the user credentials of the older version.

Note: On Windows operating system, when you specify path in the properties file, use either "/ " or "\\ " as path separator as shown in the following example.

```
C:\\ekm_restore
```

Or

```
C:/ekm_restore
```

c. Open a command prompt and run the restore utility.

Windows

Go to the <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 directory and run the following command:

```
restoreEKM21.bat
```

Linux

1) Go to the <*SKLM_INSTALL_HOME*>/migration/utilities/ekm21 directory.
2) Check whether the restoreEKM21.sh file has executable permissions. If not, give permissions by running the following command:

```
chmod 755 restoreEKM21.sh
```

3) Run the following command:

```
restoreEKM21.sh
```

d. Restart IBM Security Key Lifecycle Manager server.

Note: After data restoration, ensure that the path for the properties in the SKLMConfig.properties, datastore.properties, and ReplicationSKLMConfig.properties files are correct before you proceed with your next task.

What to do next

"Post-upgrade tasks for Encryption Key Manager" on page 99

Post-upgrade tasks for 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, 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 4.0. 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 the Encryption Key Manager migration fails, see:

- “Recovery from Encryption Key Manager migration failure” on page 100
- “Migration recovery script for Encryption Key Manager” on page 101

What to do next

From the **Welcome** page, configure the drive types, keys, and certificates that your organization requires, or get started with using the product.

Recovery from Encryption Key Manager migration failure

During inline migration process for Encryption Key Manager, you might encounter migration failure. If the migration failure occurs, run the migration recovery steps.

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.

- When the migration process starts, an error might occur during 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

  ```
  <IM_DATA_DIR>\logs\sklmLogs\migration.log
  ```

  AIX and Linux

  <*IM_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. For information about how to run the script, see Migration recovery script for Encryption Key Manager.

If Encryption Key Manager migration fails, and no data were 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.

For the definition of <*IM_DATA_DIR*> and <*WAS_HOME*>, see "Definitions for HOME and other directory variables" on page 71.

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_INSTALL_HOME*>\migration\bin directory. The commands to run the script are:

Windows systems:

```
cd <SKLM_INSTALL_HOME>\migration\bin
.\migrate.bat sklm_instance_owner_password
```

Linux and AIX systems:

```
cd <SKLM_INSTALL_HOME>/migration/bin
./migrate.sh sklm_instance_owner_password
```

On Linux or AIX systems, 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_INSTALL_HOME*> parameter is only used on Windows systems and must be enclosed in quotation marks.

Windows systems:

```
cd "C:\Program Files\IBM\SKLMV40\migration\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/SKLMV40/migration/bin
./migrate.sh password
echo $?
```

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

Exporting a device group

You can export device group data for the selected device group to an encrypted archive. Then, you can import this device group data into another instance of IBM Security Key Lifecycle Manager across operating systems.

About this task

You can use the **Export Device Group** dialog box to export a device group. Alternatively, you can use **`Device Group Export REST Service`**.

Your role must have a permission to export device groups.

Note: During data migration from previous versions of IBM Security Key Lifecycle Manager, some of the certificates might not be associated with the correct device group. As a result, it is possible that a few certificates are falsely shown (in UI, REST, or CLI) for a device group, such as 3592 or DS8000, even though the certificates do not belong to the device group. When you export such device groups, only the certificates of the device group are exported. The falsely shown certificates are not exported.

Procedure

1. Go to the appropriate page or directory.

   Graphical user interface

   a. Log in to the graphical user interface.

   b. On the **Welcome** page, click **Administration** > **Export and Import**. The **Export/Import Device Groups** page is displayed.

   Alternatively, in the **Key and Device Management** section, right-click a device group, and select **Export**.

   REST interface

   Open a REST client.

2. Export the device group data for the selected device group to the directory you specified.

   Graphical user interface

   a. On the **Export/Import Device Groups** page, click **Export**.

   b. On the **Export Device Group** dialog box, the **Device Group** field specifies the selected device group.

   c. To change the device group, click **Select**.

   d. The **Export repository location** field displays the default *<SKLM_DATA>* directory path, where the export file is saved, for example, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. For the definition of *<SKLM_DATA>*, see "Definitions for HOME and other directory variables" on page 71. Click **Browse** to specify a export repository location under *<SKLM_DATA>* directory.

Directory path in the **Export repository location** field changes based on the value that is set for the **browse.root.dir** property in the SKLMConfig.properties file.

e. In the **Password** field, specify a value for the encryption password. Ensure that you retain the encryption password for future use.

f. In the **Retype password** field, retype the password that you entered in the **Password** field.

g. In the **Description** field, specify additional information that indicates the purpose of the device group export file.

h. Click **Export**.

REST interface

a. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.

b. Run the **Device Group Export REST Service**. For example:

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/deviceGroupsExport
{"name": "3592", "exportDirectory": "/opt/IBM/WebSphere/AppServer/products/sklm/
data/",
"password": "mypassword"}
```

When the export process is complete, a message box is displayed to indicate that the export operation is complete.

What to do next

Ensure that you retain this password for use when you later import and decrypt the device group export file into another instance of IBM Security Key Lifecycle Manager. Review the directory that contains the export archive to ensure that the export file exists. You can also verify whether the archive is listed in the table on the **IBM Security Key Lifecycle Manager** > **Administration** > **Export and Import** > **Export/Import** page.

Importing a device group

You can import device group data that were exported from another IBM Security Key Lifecycle Manager server if you want to move data across IBM Security Key Lifecycle Manager servers.

Before you begin

You must have the export file and ensure that you have the password that you used when the export file was created. Save the export files in the default *<SKLM_DATA>* directory, for example, C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data. For the definition of *<SKLM_DATA>*, see "Definitions for HOME and other directory variables" on page 71.

The *<SKLM_DATA>* directory path changes based on the value that is set for the **browse.root.dir** property in the SKLMConfig.properties file.

Version of the IBM Security Key Lifecycle Manager instance where the device group export data is being imported must be same as the IBM Security Key Lifecycle Manager instance from which the device group data were exported.

About this task

At times, the device group data that is imported might conflict with an existing data in the database. For example, a key in the imported device group might be a key with same alias name of a device group in the current instance of IBM Security Key Lifecycle Manager where the data is being imported. When conflicts occur, they must be resolved before the import process can continue.

You can use the **Export and Import** page. Alternatively, you can use Device Group Import REST Service to import device groups.

Your role must have a permission to import device groups. For more information about device group export and import operations, see “Overview of device group export and import” on page 115.

Procedure

1. Go to the appropriate page or directory.

   Graphical user interface

   a. Log in to the graphical user interface.

   b. On the **Welcome** page, click **Administration** > **Export and Import**.

   REST interface

   Open a REST client.

2. Import a selected export file. Only one export or import task can run at a time. If you want import a file to an IBM Security Key Lifecycle Manager instance on a different system, copy the export file to that system by using media such as a disk, or electronic transmission.

   Graphical user interface

   a. Click **Browse** to specify the export file location under <SKLM_DATA> directory, for example, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`.

   b. Click **Display Exports** to display the export files.

   c. In the table, select an export file.

   d. Click **Import**.

   e. Alternatively, double-click or right-click the export file and select **Import**.

   f. On the **Import from Export Archive** dialog, specify the encryption password that you used to create the export file.

   g. Click **Import** to start the import operation.

   h. If any conflicts arise during the import process, the **Conflicts while Importing** dialog appears. For more information, see “Resolving the import conflicts” on page 116.

   Else, the progress dialog box appears. When the import process is complete, a message box is displayed to indicate that the import operation is complete.

   i. Click **Close**.

   REST interface

   a. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see “Authentication process for REST services” on page 69.

   b. To run **`Device Group Import REST Service`**, send the HTTP POST request. Pass the user authentication identifier that you obtained in `Step a` along with the request message as shown in the following example.

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/deviceGroupsImport
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"importFilePath": "C:\\Program Files\\IBM\\WebSphere\\AppServer\\products\\sklm\\data
\\sklm_v4.0.0.0_20160728040703-1200_export.exp",
"password": "passw0rd123"}
```

   c. If any conflicts arise during the import process, obtain the list of conflicts.

   For more information, see “Resolving the import conflicts” on page 116.

3. Restart the server. For instructions about how to stop and start the server, see “Restarting the IBM Security Key Lifecycle Manager server” on page 55.

Software download instructions

You can download the IBM Security Key Lifecycle Manager installation files (eImage) from the IBM Passport Advantage website and fix packs from the Fix Central website.

IBM Passport Advantage website

http://www-01.ibm.com/software/lotus/passportadvantage/pao_customer.html.

To prepare files for installation:

1. Download the installation files depending on your operating system.
   - "Installation images for Windows systems" on page 116
   - "Installation images for Linux systems" on page 117
   - "Installation images for AIX systems" on page 117
2. Unpack the eImage into a temporary directory on your system.
3. Select a different temporary directory to use as a base directory for the installation.

Fix Central website

http://www.ibm.com/support/fixcentral

Search, select, order, and download fixes for your system with a choice of delivery options.

Pre-upgrade considerations

Before you migrate data from an earlier version of IBM Security Key Lifecycle Manager to the current version, consider the following guidelines, restrictions, and requirements.

- 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 server has the expected keys and other configuration attributes that you intended to migrate.
- Ensure 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, V4.0, and its prerequisite software.

  The additional disk space is required for the migration process to move users, keys, and other metadata in the database of the earlier version of IBM Security Key Lifecycle Manager server to version 4.0 of the server.
- Ensure that the minimum required fix pack is applied to earlier version of IBM Security Key Lifecycle Manager from which you are upgrading. For information about minimum required fix pack level, see "Supported upgrade paths and migration methods" on page 39.
- Migration does not remove the earlier version of IBM Security Key Lifecycle Manager.
- Stop IBM Security Key Lifecycle Manager and any replica server. Key serving cannot be active during migration.
- During the inline migration process, examine the *IM_DATA_DIR*`/logs/sklmLogs/migration.log` file frequently to determine the progress of upgrade.
- To avoid errors when upgrade is in progress, do not start or stop the Db2 server or the WebSphere Application Server outside of the migration process. Do not interrupt the migration process.

Backing up critical data

Create a backup of the critical data for future reference.

Back up the data in the following directories and ensure that they are stored in a safe place.

- *WAS_HOME*\configuration
  For example, C:\Program Files\IBM\WebSphere\AppServer\configuration
- *WAS_HOME*\products
  For example, C:\Program Files\IBM\WebSphere\AppServer\products
- *SKLM_DATA*
  For example, C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data

Running the LDAP configuration scripts

Run the LDAP configuration scripts to easily integrate IBM Security Key Lifecycle Manager with LDAP for configuring IBM Security Key Lifecycle Manager users in any of the LDAP repositories, such as IBM Security Directory Server or Microsoft Active Directory.

About this task

Procedure

1. Open the config.py properties file and update the values for the properties as per your requirements.

   Note: To run the scripts with default configuration, you must set the following properties:

   - **ip**
   - **port**
   - **LDAP_server_type**
   - **backupPassword**

   For a description of all the properties, see LDAP integration by using configuration scripts.

   Windows
   SKLM_INSTALL_HOME\bin\LDAPIntegration\config.py
   C:\Program Files\IBM\SKLMV40\bin\LDAPIntegration\config.py

   Linux
   SKLM_INSTALL_HOME/bin/LDAPIntegration/config.py
   /opt/IBM/SKLMV40/bin/LDAPIntegration/config.py
2. Create the database for LDAP configuration.
   a. Open the DB2 command window.
   b. Run the following command to create the database.

   ```
   db2  create database USERDB40 using codeset UTF-8 territory US
   ```
3. Update the data source from the WebSphere Integrated Solutions Console with jndi name jdbc/wimXADS. For the instructions, see “Updating a data source from WebSphere Integrated Solutions Console” on page 119.
4. Create database-based repository to hold all the IBM Security Key Lifecycle Manager application groups.
   a. Go to the <*WAS_HOME*>\bin folder.

   Windows
   C:\Program Files\IBM\WebSphere\AppServer\bin

Linux
/opt/IBM/WebSphere/AppServer/bin

b. Open a command prompt and run the following commands.

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
<SKLM_INSTALL_HOME>\bin\LDAPIntegration\createDBRepos.py <WAS_HOME> <LDAP_DBNAME>
<SKLM_DBUSER> <SKLM_DBUSERPASSWD> <SKLM_DBPORT#>
```

Notes: On Linux platforms, use **wsadmin.sh** instead of **wsadmin.bat**

During IBM Security Key Lifecycle Manager installation, if you use the defaults,

```
LDAP_DBNAME = USERDB40
SKLM_DBUSER = sklmdb40
SKLM_DBPORT# = 50060
```

SKLM_DBUSERPASSWD is the IBM Security Key Lifecycle Manager database password that you specified during the installation.

5. Run the configuration scripts sklmLDAPConfigure and addLDAPUserToGroup.

Windows
Go to the *SKLM_INSTALL_HOME*\bin\LDAPIntegration directory and run the following scripts:

```
sklmLDAPConfigure.bat WAS_HOME SKLM_INSTALL_HOME WAS_ADMIN WASAdmin_PASSWORD SKLM_ADMIN
SKLM_ADMIN_PASS DB2_install_directory
addLDAPUserToGroup.bat WAS_HOME SKLM_INSTALL_HOME WAS_ADMIN WASADMIN_PASS
USER_UNIQUE_NAME SKLM_ADMIN SKLM_ADMIN_PASS
```

For example:

```
sklmLDAPConfigure.bat "c:\Program Files\IBM\WebSphere\AppServer" "c:\Program Files\IBM
\SKLMV40" wasadmin WAS@admin123 sklmadmin SKLM@admin123 "c:\Program Files\IBM\DB2SKLMV40"
addLDAPUserToGroup.bat "c:\Program Files\IBM\WebSphere\AppServer" "c:\Program Files\IBM
\SKLMV40" wasadmin WAS@admin123 "uid=001,c=in,ou=bluepages,o=ibm.com" sklmadmin
SKLM@admin123
```

Linux
Go to the *SKLM_INSTALL_HOME*/bin/LDAPIntegration directory and run the following scripts:

```
sklmLDAPConfigure.sh WAS_HOME SKLM_INSTALL_HOME WAS_ADMIN WASAdmin_PASSWORD SKLM_ADMIN
SKLM_ADMIN_PASS DB2_install_directory
addLDAPUserToGroup.sh WAS_HOME SKLM_INSTALL_HOME WAS_ADMIN WASADMIN_PASS
USER_UNIQUE_NAME SKLM_ADMIN SKLM_ADMIN_PASS
```

For example:

```
sklmLDAPConfigure.sh "/opt/IBM/WebSphere/AppServer" "/opt/IBM/SKLMV40" wasadmin
WAS@admin123 sklmadmin SKLM@admin123 "/opt/IBM/DB2SKLMV40"
addLDAPUserToGroup.sh "/opt/IBM/WebSphere/AppServer" "/opt/IBM/SKLMV40" wasadmin
WAS@admin123 "uid=001,c=in,ou=bluepages,o=ibm.com" sklmadmin SKLM@admin123
```

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

Windows
drive:\Program Files\IBM\WebSphere\AppServer

Linux
path/IBM/WebSphere/AppServer

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

Windows
drive:\Program Files\IBM\SKLMV40

Linux

WAS_ADMIN
User name of WebSphere Application Server for IBM Security Key Lifecycle Manager.

WAS_PASS
Password of WebSphere Application Server for IBM Security Key Lifecycle Manager.

USER_UNIQUE_NAME
The LDAP user for whom you want to assign IBM Security Key Lifecycle Manager administrator role.

SKLM_ADMIN
Administrator for IBM Security Key Lifecycle Manager.

SKLM_ADMIN_PASS
Password for IBM Security Key Lifecycle Manager administrator.

DB2_install_directory
The directory where DB2 is installed.

Windows
drive:\Program Files\IBM\DB2SKLMV40

Linux
path/IBM/DB2SKLMV40

For non-root installation on Linux , the path is: *<non_root_user_home _directory>*/sqllib

What to do next
After the LDAP configuration, you must run the subsequent tasks. For more information, see "Post-LDAP configuration tasks to support LDAP integration" on page 119

Recovery from migration failure

During inline migration process for Encryption Key Manager or IBM Security Key Lifecycle Manager earlier versions to version 4.0, you might encounter migration failure. You can run the migration recovery steps in case of a migration failure.

If migration fails from the installer, you can manually run the IBM Security Key Lifecycle Manager, Version 4.0 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 Linux or AIX systems, ensure that you are logged in as the root user before you run **migrate.sh**.
- Run **migrateToSKLM.bat** or **migrateToSKLM.sh** in the *<SKLM_INSTALL_HOME>*\migration directory to migrate IBM Security Key Lifecycle Manager earlier version to version 4.0. On Linux or AIX systems, 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.

Backing up data of an earlier version of IBM Security Key Lifecycle Manager

The first step to migrate data from your existing IBM Security Key Lifecycle Manager version to V4.0 is to back up the data of the existing version. The next and final step is to restore this backup file to the system where IBM Security Key Lifecycle Manager V4.0 is installed.

Before you begin

- Ensure that the system from which you want to migrate data and create backup has the minimum required level of IBM Security Key Lifecycle Manager version already installed.

Note: You must have the required IBM Security Key Lifecycle Manager user role to run the backup and restore operations.

- Ensure that IBM Security Key Lifecycle Manager, V4.0 is installed on the system to which you want to restore the backed-up file.

About this task

Use the IBM Security Key Lifecycle Manager backup utility to create the backup file. The backup file is independent of the operating system and directory structure of the server. You can restore this cross-platform-compatible backup file to a system with IBM Security Key Lifecycle Manager, version 4.0 across operating systems.

IBM Security Key Lifecycle Manager stores the transactional data of keys that are served to clients in a database table. If the number of records in the table is equal to or greater than 100,000, IBM Security Key Lifecycle Manager automatically purges the database table and archives or stores the transactional data in a comma-separated values (CSV) file.

The CSV file and a checksum file are included in an archive (JAR) file that is saved in the SKLM_DATA \ServedDataListArchives folder.

Note: The archive file is not included in the cross-platform backup files. If you want the transactional data of served keys to be backed up and restored, then select the inline migration method.

The directory names and `.bat` and `.sh` file names vary depending on the version of IBM Security Key Lifecycle Manager that you are backing up.

IBM Security Key Lifecycle Manager version	Directory with backup utility (*sklmv##*)	Backup utility file name (backupV##.bat/ backupV##.sh
3.0.1	sklmv301	• backupV301.bat • backupV301.sh
3.0	sklmv30	• backupV30.bat • backupV30.sh
2.7	sklmv27	• backupV27.bat • backupV27.sh
2.6	sklmv26	• backupV26.bat • backupV26.sh
2.5	sklmv25	• backupV25.bat • backupV25.sh

Procedure

1. Run the followings steps on the system where the IBM Security Key Lifecycle Manager version 4.0 is installed.
   a. Log in to the system with your user credentials.
   b. Locate the backup utilities folder.

      Windows

      <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv##

      Default location is C:\Program Files\IBM\.SKLMV40\migration\utilities\sklmv##

Linux

<*SKLM_INSTALL_HOME*>/migration/utilities/sklmv##

Default location is /opt/IBM/SKLMV40/migration/utilities/sklmv##.

2. Run the followings steps on the system where the earlier version of IBM Security Key Lifecycle Manager, from where you want to migrate the data, is installed.

   a. Log in to the system with your user credentials.

   b. Copy sklmv## folder from the system where IBM Security Key Lifecycle Manager, Version 4.0 is installed to a local directory of your choice.

   c. Edit the backup.properties file in the sklmv## directory to configure the properties. You must set values for all the properties, except for the BACKUP_DIR property (optional).

   If you do not specify the value for BACKUP_DIR, the backup file is created in the backup subdirectory under the same directory from where you run the backup utility.

   Note: On Windows operating system, the backup.properties file that you use for backup operations must not contain the property keys and values with leading or trailing spaces.

   The content in the following examples is from the backup.properties file for IBM Security Key Lifecycle Manager V2.5 with sample password values:

   Windows

```
WAS_HOME=C:\\Program Files (x86)\\IBM\\WebSphere\\AppServer
BACKUP_PASSWORD=passw0rd123
DB_PASSWORD=sklmdb2_password
WAS_USER_PWD=wasadmin_password
BACKUP_DIR=C:\\sklmv25_backup
```

   Linux

```
WAS_HOME=/opt/IBM/WebSphere/AppServer
BACKUP_PASSWORD=passw0rd123
DB_PASSWORD=sklmdb2_password
WAS_USER_PWD=wasadmin_password
BACKUP_DIR=/sklmv25_backup
```

   Note: On Windows operating system, when you specify path in the properties file, use either "/ " or "\\ " as path separator as shown in following example:

```
C:\\sklmv25_backup
```

   Or

```
C:/sklmv25_backup
```

   d. Open a command prompt and run the backup utility.

   Windows

   Go to the sklmv## directory (see Step b) and run the following command:

```
backupV##.bat
```

   For example: The command for IBM Security Key Lifecycle Manager V2.5:

```
backupV25.bat
```

   Linux

   1) Go to the sklmv## directory (see Step b).

   2) Check whether the backupV##.sh file has executable permissions. If not, give permissions by running the following command:

```
chmod 755 backupV##.sh
```

For example: The command for IBM Security Key Lifecycle Manager V2.5:

```
chmod 755 backupV25.sh
```

3) Run the backup utility:

```
backupV##.sh
```

For example: The command for IBM Security Key Lifecycle Manager V2.5:

```
backupV25.sh
```

3. Complete the following verification tasks:
   - Review the directory that contains backup files to ensure that the backup file exists. The backup files are created in the location that you specified for BACKUP_DIR in the `backup.properties` file.
   - Check the `backup.log` file for errors or exceptions. The `backup.log` file is created in the same directory where you run the backup utility. For a successful backup operation, ensure that there are no errors or exceptions in the log file.
   - Retain the backup password for future use in case you restore the backup.
   - Do not edit a file in the backup archive. The file that you attempt to edit becomes unreadable.

Restoring the backup file of an earlier version of IBM Security Key Lifecycle Manager

Use the graphical user interface, command-line interface, REST interface, or the migration restore script to restore the backup file of IBM Security Key Lifecycle Manager version 2.5 or later to a system with IBM Security Key Lifecycle Manager version 4.0, across operating systems. After restoring the file, data migration to the system with IBM Security Key Lifecycle Manager V4.0 is complete.

Before you begin

- Ensure that you have the backup file of the IBM Security Key Lifecycle Manager version from which you want to migrate the data, and ensure that you have the password that was used to create the backup file.

  Note: You must have the required IBM Security Key Lifecycle Manager user role to run the backup and restore operations.
- Ensure that IBM Security Key Lifecycle Manager, V4.0 is installed on the system to which you want to restore the backed up file.

About this task

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

The directory names and `.bat` and `.sh` file names vary depending on the version of IBM Security Key Lifecycle Manager that you are restoring from.

IBM Security Key Lifecycle Manager version	**Directory with restore utility (*sklmv##*)**	**Restore utility file name (`restoreV##.bat`/ `restoreV##.sh`**
3.0.1	`sklmv301`	• `restoreV301.bat` • `restoreV301.sh`

IBM Security Key Lifecycle Manager version	Directory with restore utility (*sklmv##*)	Restore utility file name (**restoreV##.bat/ restoreV##.sh**
3.0	sklmv30	• restoreV30.bat • restoreV30.sh
2.7	sklmv27	• restoreV27.bat • restoreV27.sh
2.6	sklmv26	• restoreV26.bat • restoreV26.sh
2.5	sklmv25	• restoreV25.bat • restoreV25.sh

Note: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedure

1. Log in to the system where IBM Security Key Lifecycle Manager V4.0 is installed as the non-administrator or non-root user who is the owner of the Db2 and WebSphere Application Server services (For example, sklmdb40).
2. Copy the backup file from the system from which you want to migrate the data in the *SKLM_DATA* directory.

   You can copy the backup file to any directory in the *SKLM_DATA* directory as well. In the following example, the backup file for IBM Security Key Lifecycle Manager V2.5 is stored directly in the *SKLM_DATA* directory:

   ```
    C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data
   \sklm_v2.5.0.3_20170429013250-0400_migration_backup.jar
   ```

3. Restore the backup file by using any of the following methods:
   - **Graphical user interface**
     a. Log in to the graphical user interface as an authorized user, for example, SKLMAdmin.
     b. On the **Welcome** page, click **Administration** > **Backup and Restore**.
     c. Click **Browse** to specify the backup file location under *<SKLM_DATA>* directory.
     d. Click **Display Backups** to display the backup files that you want to restore.
     e. In the **Backup and Restore** table, select a backup file.
     f. Click **Restore From Backup**.
     g. On the **Restore Backup** page, specify the backup password that you used to create the backup file.
     h. Click **Restore Backup**.
     i. Restart IBM Security Key Lifecycle Manager server.
   - **Command-line interface**

     Note: By using the graphical user interface, you cannot restore roles, users, and groups from IBM Security Key Lifecycle Manager backup file.

     a. Go to the *<WAS_HOME>*/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

```
wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
```

Linux

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

c. Run the **tklmBackupRunRestore** CLI command by specifying the parameters such as the backup file name with its full path and backup password that you used to create the backup as shown in the following example.

```
print AdminTask.tklmBackupRunRestore
    ('[-backupFilePath <SKLM_DATA>/
sklm_v2.5.0.3_20170429013250-0400_migration_backup.jar
        -password myBackupPwd]')
```

d. Restart IBM Security Key Lifecycle Manager server.

Note: By using the command-line interface, you cannot restore roles, users, and groups from IBM Security Key Lifecycle Manager backup file.

- **REST interface**

a. Open a REST client.

b. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services.

c. Run the **Backup Run Restore REST Service**. For example.

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/restore
{"backupFilePath":"<SKLM_DATA>/sklm_v2.5.0.3_20170429013250-0400_migration_backup.jar",
"password":"myBackupPwd"}
```

d. Restart IBM Security Key Lifecycle Manager server.

Note: By using the REST interface, you cannot restore roles, users, and groups from IBM Security Key Lifecycle Manager backup file.

- **Migration restore script**

a. Locate the IBM Security Key Lifecycle Manager restore utilities.

Windows

<*SKLM_INSTALL_HOME*>\migration\utilities*sklmv##*

For example: Default location of IBM Security Key Lifecycle Manager V2.5 is `C:\Program Files\IBM\SKLMV40\migration\utilities\sklmv25`.

Linux

<*SKLM_INSTALL_HOME*>/migration/utilities/*sklmv##*

For example: Default location of IBM Security Key Lifecycle Manager V2.5 is `/opt/IBM/SKLMV40/migration/utilities/sklmv25`.

b. Edit the `restore.properties` file in the *sklmv##* directory to configure its properties.

Note: On Windows operating system, the `restore.properties` file that you use for restore operations must not contain the property keys and values with leading or trailing spaces.

The following example shows the updated file for IBM Security Key Lifecycle Manager V2.5:

Windows

```
WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer
JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0
BACKUP_PASSWORD=passw0rd123
```

```
DB_PASSWORD=db2_password
RESTORE_FILE=<SKLM_DATA>\\sklm_v2.5.0.3_20170429013250-0400_migration_backup.jar
WAS_USER_PWD=wasadmin_password
RESTORE_USER_ROLES=y
#pkcs11_config=C:\\luna.cfg
```

Linux

```
WAS_HOME=/opt/IBM/WebSphere/AppServer
JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0
BACKUP_PASSWORD=passw0rd123
DB_PASSWORD=db2_password
RESTORE_FILE=<SKLM_DATA>/sklm_v2.5.0.3_20170429013250-0400_migration_backup.jar
WAS_USER_PWD=wasadmin_password
RESTORE_USER_ROLES=y
#pkcs11_config=/luna.cfg
```

Note:

- To log in to IBM Security Key Lifecycle Manager by using the user credentials that are specified during product installation, set the **RESTORE_USER_ROLES** property as "n ". Setting the property to "n " ensures that user ID and the password are not overwritten with the user credentials of the earlier version.
- If IBM Security Key Lifecycle Manager is configured with HSM, uncomment the **#pkcs11_config** property and specify the correct path of `luna.cfg` file as the value.
- On Windows operating system, when you specify path in the properties file, use either "/ " or "\\ " as a path separator. The following example shows the path in IBM Security Key Lifecycle Manager V2.5 properties file:

  ```
  C:\\sklmv25_restore
  ```

  Or

  ```
  C:/sklmv25_restore
  ```

c. Open a command prompt and run the restore utility.

Windows

Go to the <*SKLM_INSTALL_HOME*>\migration\utilities*sklmv##* directory and run the following command:

```
restoreV##.bat
```

For example, for V2.5, run the following command:

```
restoreV25.bat
```

Linux

1) Go to the <*SKLM_INSTALL_HOME*>/migration/utilities/*sklmv##* directory.
2) Check whether the `restoreV##.sh` file has executable permissions. If not, give permissions by running the following command:

   ```
   chmod 755 restoreV##.sh
   ```

   For example, for IBM Security Key Lifecycle Manager v2.5:

   ```
   chmod 755 restoreV25.sh
   ```

3) Run the following command:

   ```
   restoreV##.sh
   ```

For example, for IBM Security Key Lifecycle Manager v2.5:

```
restoreV25.sh
```

d. Restart the IBM Security Key Lifecycle Manager server.

Note: By using the migration restore script, you can restore users, groups, and roles from IBM Security Key Lifecycle Manager backup file. Ensure that the value of the **WAS_USER_PWD** parameter for WebSphere Application Server administrator password in the `restore.properties` is correctly specified. If the password value is incorrect, restore of users, groups, and roles fails.

Note: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Overview of device group export and import

When multiple IBM Security Key Lifecycle Manager instances are maintained across operating systems, you might need to move device group data from one instance to another according to your business requirements. You can use the device group export and import operations to export and import data across IBM Security Key Lifecycle Manager instances with the same version as of the source IBM Security Key Lifecycle Manager instance, on the same or different operating systems, while maintaining data integrity. The exported device group data is encrypted and protected through a password.

Device groups for all the default device types are created during installation of IBM Security Key Lifecycle Manager. When you add a device type by using the graphical user interface, command-line interface, or REST interface, the corresponding device group is created in the database. Name of the device group is same as the device type that you created.

Device group export

You can export device group by using the IBM Security Key Lifecycle Manager graphical user interface or REST interface. The export device group operation creates a compressed archive with the extension `.exp` in a location that you specify. Except for the `manifest` and `summary.json` files, all the following files of the archive are encrypted by the password that was specified during device group export operation.

- Manifest file, which lists all the device group data files in the archive
- `summary.json`, which contains summary information for the device group
- Files specific to devices
- Files specific to keys
- Files specific to certificates

Device group import

You can import device group data to an IBM Security Key Lifecycle Manager instance from an encrypted archive that was exported from another IBM Security Key Lifecycle Manager instance. During device group import operation, you must specify the password that was used for device group export operation to import and decrypt data. Use the IBM Security Key Lifecycle Manager graphical user interface or REST interface to import device group.

Note: You must restart the server after you run the device group import operation.

Device group import conflicts

At times, the device group data that is imported might conflict with an existing data in the database. For example, a key in the imported device group might be a duplicate key of a device group in the current instance of IBM Security Key Lifecycle Manager where the data is being imported. When conflicts occur, they must be resolved before the import process can continue.

The device group import operation includes the following tasks:

- Saving export file in the target IBM Security Key Lifecycle Manager server where the device group is being imported. You must have the same encryption password that was used for creating the export file to extract and decrypt data
- Evaluating duplicates between the data that is imported and the data in the target server
- Resolving the conflicts
- Importing device group data to the target server

You can view the list of conflicting items, if any, during device group import operation. Then, you can export the conflict information to a file in comma-separated values (CSV) format for further analysis.

Resolving the import conflicts

When the device group data is imported from an export file, its content is analyzed for conflicts with the data that is stored in the database. The conflicts must be resolved before the data can be imported. You can view the list of conflicts to analyze and resolve the problems.

About this task

When you import device group data from an export file into an IBM Security Key Lifecycle Manager server, you might detect conflicts. You can also use **Device Group Import Conflicts REST Service** to obtain the list of the data conflicts, if any.

You must resolve the conflicts before the data can be imported.

Procedure

1. Open a REST client.
2. Use the following REST APIs to resolve the import conflicts:
   - **Change Name REST Service**
   - **Change Certificate Alias REST Service**
   - **Change History REST Service**
   - **Renew Key Alias REST Service**

Related tasks

"Importing a device group" on page 103
You can import device group data that were exported from another IBM Security Key Lifecycle Manager server if you want to move data across IBM Security Key Lifecycle Manager servers.

Installation images for Windows systems

You can download the IBM Security Key Lifecycle Manager installation files (eImages) for Windows systems from the IBM Passport Advantage website.

Table 11. eImages for Windows systems

eImage	Description
CC49YML	IBM Security Key Lifecycle Manager, Version 4.0 for Windows systems eImage 1.
CC49ZML	IBM Security Key Lifecycle Manager, Version 4.0 for Windows systems eImage 2.

Installation images for Linux systems

You can download the IBM Security Key Lifecycle Manager installation files (eImages) for Linux systems from the IBM Passport Advantage website.

Table 12. eImages for Linux (Red Hat and SuSE) systems

eImage number	Description
CC4A0ML	IBM Security Key Lifecycle Manager, Version 4.0 for Linux (Red Hat and SuSE) systems eImage 1.
CC4A1ML	IBM Security Key Lifecycle Manager, Version 4.0 for Linux (Red Hat and SuSE) systems eImage 2.

Table 13. Linux System z eImages

eImage	Description
CC4A4ML	IBM Security Key Lifecycle Manager, Version 4.0 for Linux System z eImage 1.
CC4A5ML	IBM Security Key Lifecycle Manager, Version 4.0 for Linux System z eImage 2.

Table 14. Linux PowerPC eImages

eImage	Description
CC4A6ML	IBM Security Key Lifecycle Manager, Version 4.0 for Linux PowerPC eImage 1.
CC4A7ML	IBM Security Key Lifecycle Manager, Version 4.0 for Linux PowerPC eImage 2.

Installation images for AIX systems

You can download the IBM Security Key Lifecycle Manager installation files (eImages) for AIX systems from the IBM Passport Advantage website.

Table 15. eImages for AIX systems

eImage	Description
CC4A2ML	IBM Security Key Lifecycle Manager, Version 4.0 for AIX systems eImage 1.
CC4A3ML	IBM Security Key Lifecycle Manager, Version 4.0 for AIX systems eImage 2.

LDAP integration by using configuration scripts

You can run the configuration scripts from a command-line to integrate IBM Security Key Lifecycle Manager with LDAP by using the default configuration settings that are defined in the `config.py` properties file.

The following example shows the properties that are defined in the `config.py` file.

```
import string, sys
LDAP_server_type="IDS"
```

```
login_id="uid"
ip="9.x.x.x"
port="389"
gr_name="Group"
pr_name="PersonAccount"
gr_obj_class="groupOfUniqueNames"
pr_obj_class="person"
mem_name="uniqueMember"
mem_obj_class="groupOfUniqueNames"
base_entry="o=ibm.com"
scope="direct"
backupPassword="<changeit>"
```

The following table provides description for the `config.py` file properties.

Property	Description
LDAP_server_type	Type of the LDAP server that is being used. By default, IDS is specified.
login_id	Property name that is used for login. For example, `uid` and `mail`.
ip	IP address or host name for the primary LDAP server.
port	Port number for the LDAP server.
gr_name	Name of the group entity type.
pr_name	Name of the entity type.
gr_obj_class	Object class for the entity type.
pr_obj_class	Object class for the entity type.
mem_name	Name of the LDAP attribute that is used as the group member attribute. For example, `member` or `uniqueMember`.
mem_obj_class	Group object class that contains the member attribute. For example, `groupOfNames` or `groupOfUniqueNames`. If you do not define this parameter, the member attribute applies to all group object classes.
base_entry	LDAP base entity
scope	Scope of the member attribute. Specify any of the following values for the parameter. **direct** Member attribute that contains only the direct members. Therefore, this value refers to the member directly contained by the group and not contained through the nested group. For example, if `Group1` contains `Group2` and `Group2` contains `User1`, then `Group2` is a direct member of `Group1` but `User1` is not a direct member of `Group1`. Both `member` and `uniqueMember` are direct member attributes. **nested** Member attribute that contains direct members and the nested members.
backupPassword	Password to encrypt the backup key that is used to back up the IBM Security Key Lifecycle Manager data. By default, `<changeit>` is specified. You must modify this value before you run the LDAP configuration scripts. You must specify this password to decrypt and restore the backup files.

If you discover problems during LDAP integration when the scripts are used to run the configuration task, you might need to review the following log files that are at *<SKLM_INSTALL_HOME>*/bin/LDAPIntegration to diagnose the problems.

- sklmldapconf.log
- ldaplog.out

For more information about how to run the configuration scripts, see Running the LDAP configuration scripts.

Updating a data source from WebSphere Integrated Solutions Console

You must update data source for the database-based repository to hold IBM Security Key Lifecycle Manager application groups. The database-based repository uses the tables that are created in the IBM Security Key Lifecycle Manager application database.

Procedure

1. Log on to update the data source from WebSphere Integrated Solutions Console (https://localhost:9083/ibm/console/logon.jsp) as a wasadmin user.
2. In the navigation bar, click **Resources** > **JDBC** > **Data sources**.
3. Click **WIM Data Source** to edit the database values.
4. Update the database name with USERDB40 under the **Common and required data source properties** section.
5. Click **OK**.
6. Click **Save** to save the configuration.

Post-LDAP configuration tasks to support LDAP integration

After LDAP configuration, you might need to complete extra tasks to ensure successful integration of IBM Security Key Lifecycle Manager with LDAP user repositories.

Important notes after the LDAP configuration

1. After the LDAP configuration, sklmadmin user that existed in the default file-based user repository cannot access IBM Security Key Lifecycle Manager application.
2. After the LDAP configuration, you must use **wsadmin** commands to create groups and to assign IBM Security Key Lifecycle Manager roles. You cannot use WebSphere Integrated Solutions Console. Run the following steps to add a group and assign a role to the group:
   a. Go to *<WAS_HOME>*/bin.
   b. Log on to wsadmin by using the following command:

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

   c. To create a group and assign the role, run the following command:

```
AdminTask.createGroup<'[-cn <groupname> -parent "o=sklmrepdb.ibm"]'>
AdminTask.mapGroupsToAdminRole<'[-roleName <role> -groupids
<groupname>]'>
```

3. After the LDAP configuration, you might want to restore the IBM Security Key Lifecycle Manager configuration in WebSphere Application Server to the state as before the LDAP configuration. To restore the configuration, run the following steps:
   a. Stop WebSphere Application Server.
   b. Stop WebSphere Application Server related processes, if any.

c. Restore WebSphere Application Server profile configuration that was taken before the LDAP configuration:

1) Manually delete the KLMProfile folder at *<WAS_HOME>*/profiles/KLMProfile.

2) Run the **-validateAndUpdateRegistry** option of the **manageProfiles** command.

Windows

<WAS_HOME>\bin\manageProfiles.bat -validateAndUpdateRegistry

For example: C:\Program Files\IBM\WebSphere\AppServer\bin \manageProfiles.bat -validateAndUpdateRegistry

Linux

<WAS_HOME>/bin/manageprofiles.sh -validateAndUpdateRegistry

For example: /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -validateAndUpdateRegistry

3) Restore the profile:

Windows

<WAS_HOME>\bin\manageProfiles.bat -restoreProfile -backupFile *<path to profile backup file>*

For example: C:\Program Files\IBM\WebSphere\AppServer\bin \manageProfiles.bat -restoreProfile -backupFile C:\SKLM_WAS_ProfileBackup

Linux

<WAS_HOME>/bin/manageprofiles.sh -restoreProfile -backupFile *<path to profile backup file>*

For example: /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -restoreProfile -backupFile /root/SKLM_WAS_ProfileBackup

For information about the **manageProfiles** command, see http://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/rxml_manageprofiles.html.

4) Start WebSphere Application Server.

5) Restore IBM Security Key Lifecycle Manager backup that was taken before the LDAP configuration, if needed.

4. You must not restore IBM Security Key Lifecycle Manager application backup that is taken before the LDAP configuration after the LDAP configuration is done unless Step 3 in the **Important notes after the LDAP configuration** section is followed.
5. After the LDAP configuration, the tables are created in the IBM Security Key Lifecycle Manager database for the database-based repository. The IBM Security Key Lifecycle Manager groups are stored in these tables. If the IBM Security Key Lifecycle Manager server is configured for the replication and the replication happens to the configured clones, the groups in the database-based repository are also replicated on the clone. This is because the database tables of the database-based repository are also replicated to the clones.
6. If the IBM Security Key Lifecycle Manager server (master) that is configured to integrate with LDAP repositories and replication is enabled, when replication happens to the configured clones where LDAP is not configured, you can configure LDAP on the clone or not. If LDAP configuration must be done on the clone, run the following steps on the clone:

a. Copy db2jcc.jar,db2jcc4.jar and db2jcc_license_cu.jar from the DB2SKLMV40 folder to the *<WAS_HOME>*/lib folder.

Default definition of *<WAS_HOME>* variable is typically:

Windows

C:\Program Files\IBM\WebSphere\AppServer

Linux
/opt/IBM/WebSphere/AppServer

b. Go to *<WAS_HOME>*/bin.

1) Log on to wsadmin by using the following command:

```
wsadmin.bat -user <WASADMIN_USER> -password <WASADMIN_PASSWORD>
-lang jython
```

2) Run the following command:

```
AdminTask.deleteIdMgrDBTables<'[-schemaLocation "<WAS_HOME>/etc/wim/set
up" -databaseType db2 -dbURL "jdbc:db2://localhost:<SKLMDB_PORT>/
<LDAPDB_NAME>" -dbDriver com.ibm.db2.jcc.DB2Driver -dbAdminId
<SKLMDBADMIN_USER> -dbAdminPassword <SKLMDBADMIN_PASSWORD>
-reportSqlError true]'>
```

c. Follow the procedure to setup/configure LDAP integration as was done on the master IBM Security Key Lifecycle Manager server. For the integration steps, see "Integrating LDAP by using WebSphere Integrated Solutions Console" on page 142.

7. After the replication between an IBM Security Key Lifecycle Manager server that is configured for LDAP integration and a clone that is not configured for LDAP integration, if you inadvertently run the normal LDAP integration configuration on the clone, the Step 5 in "Integrating LDAP by using WebSphere Integrated Solutions Console" on page 142 fails. You must run these steps:

a. Go to *<WAS_HOME>*/bin.

1) Log on to wsadmin:

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

2) Run the following command:

```
AdminTask.deleteIdMgrDBTables<'[-schemaLocation "<WAS_HOME>/etc/wim/set
up" -databaseType db2 -dbURL "jdbc:db2://localhost:<SKLMDB_PORT>/
<LDAP_DBNAME>" -dbDriver com.ibm.db2.jcc.DB2Driver -dbAdminId
<SKLMDB2ADMINUSER> -dbAdminPassword <SKLMDB2ADMINUSER_PASSWORD>
-reportSqlError true]'>
```

b. Run steps 5 - 9 in "Integrating LDAP by using WebSphere Integrated Solutions Console" on page 142.

Backup Run Restore REST Service

Use **Backup Run Restore REST Service** to restore from an existing backup file. Before you begin, obtain the password that was used to create the backup the file that you intend to use.

Only one backup or restore task can run at a time. Before you start a restore task, isolate the system for maintenance. IBM Security Key Lifecycle Manager server automatically restarts after the restore process is complete. Verify the environment before you bring the IBM Security Key Lifecycle Manager server back into production.

Operation
POST

URL
https://*<host>*:*<port>*/SKLM/rest/v1/ckms/restore

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON Object with the following specification.	
JSON property name	**Description**
backupFilePath	Required parameter. Specify the full path and file name that contains backup data. To determine this directory, examine the value of the **sklm.backup.dir** property in the `SKLMgrConfig.properties` file.
password	You must specify the password to restore data from the backup file if IBM Security Key Lifecycle Manager uses a password-based encryption method. **Note:** You need not specify the password to restore the data if IBM Security Key Lifecycle Manager is configured to use Hardware Security Module (HSM) to store the master encryption key. For more information about hsm-based encryption, see "HSM-based encryption for backups" on page 132. To restore a backup file, you must provide the password that was used to encrypt the data in that file during the backup operation.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the value that is specified by the **status** property.
status	Returns the status message to indicate whether the restore task was successful. **-1** State is unknown. The task is not run since the last time the IBM Security Key Lifecycle Manager server started. **0** The restore succeeded. **1** The restore task failed.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Note: Backup Run Restore REST Service returns the `500 Internal Server Error` response when a restore operation fails. In the response body, you can see only the status message without status code 1.

Examples

Service request to run a backup restore task

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/restore
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{"backupFilePath":"/opt/mysklmbackups/sklm_v2.7.0_20160705235417-1200_
backup.jar","password":"passw0rd"}
```

Success response

```
Status Code : 200 OK
Content-Language: en
{"code":"0","status":"Restore operation succeeded. Restart the server."}
```

Error response

```
Status Code : 400 Bad Request
Content-Language: en
{"code":"CTGKM6002E","message":"CTGKM6002E Bad Request: Invalid user
authentication ID or invalid request format."}
```

Change Name REST Service

Use **`Change Name REST Service`** to change the serial number of a storage device.

Note: The import conflict REST services make significant changes to the IBM Security Key Lifecycle Manager instance that might impact its operation and the communication with the storage device. You must carefully plan and evaluate the changes that are required on both IBM Security Key Lifecycle Manager and the storage device. The changes must be atomic; that is the changes must be done both on the IBM Security Key Lifecycle Manager system and the devices. The import conflict resolution REST services handle the changes for IBM Security Key Lifecycle Manager. For the complete process handling, you must take the guidance of your IBM support representative.

Operation

POST

URL

`https://<host>:<port>/SKLM/rest/v1/ckms/conflictResolution/changeName`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
`host`	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
`port`	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
`Content-Type`	`application/json`

Request Headers (continued)	
Header name	**Value**
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON object with the following specification	
Property name	**Description**
type	Specifies that the user can change the name of a device serial number. You can provide the value `Device`, `Client`, or `LTOKeyGroup`.
oldName	Specifies the existing value of the storage device serial number.
newName	Specifies the new value to be set for the storage device serial number.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification	
JSON property name	**Description**
code	Returns the value that is specified by the **status** property.
status	Returns the status to indicate whether the serial number of the storage device is changed with an appropriate message.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request to change the serial number of a storage device

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/conflictResolution/changeName
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"type" : "Device" , "oldName" : "device1", "newName" : "newdevice1"}
```

Success response

```
Status Code : 200 OK
 {"code":"0","status”:”Change of Name successfull.”}
```

Error response

```
Status Code: 500 Internal Server Error
{"code":"CTGKM2923E","message":"CTGKM2923E  Device with Serial number newdevice1 already
exists."}
```

Change Certificate Alias REST Service

Use **Change Certificate Alias REST Service** to change the alias of a certificate present in the IBM Security Key Lifecycle Manager instance.

Note: The import conflict REST services make significant changes to the IBM Security Key Lifecycle Manager instance that might impact its operation and the communication with the storage device. You must carefully plan and evaluate the changes that are required on both IBM Security Key Lifecycle Manager and the storage device. The changes must be atomic; that is the changes must be done both on the IBM Security Key Lifecycle Manager system and the devices. The import conflict resolution REST services handle the changes for IBM Security Key Lifecycle Manager. For the complete process handling, you must take the guidance of your IBM support representative.

Operation

POST

URL

`https://<host>:<port>/SKLM/rest/v1/ckms/conflictResolution/changeCertificateAlias`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON object with the following specification	
Property name	**Description**
oldAlias	Specifies the existing value of the alias for the certificate present in IBM Security Key Lifecycle Manager system.
newAlias	Specifies the new value to be set for the alias of the certificate. This value must be unique in the IBM Security Key Lifecycle Manager system.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification	
JSON property name	**Description**
code	Returns the value that is specified by the **status** property.
status	Returns the status to indicate whether the certificate alias is changed with an appropriate message.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request to change certificate alias

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/conflictResolution/changeCertificateAlias
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"oldAlias" : "3592cert2" ,"newAlias" : "3592cert3"}
```

Success response

```
Status Code : 200 OK
 {"code":"0","status":"Certificate alias successfully changed"}
```

Error response

```
Status Code: 500 Internal Server Error
{"code":"CTGKM2919E","message":"CTGKM2919E  Certificate with Alias name 3592cert3
already exists."}
```

Change History REST Service

Use **Change History REST Service** to get information about the historical changes that are done to different cryptographic objects such as key alias, certificate alias, device serial number, and UUID in the IBM Security Key Lifecycle Manager instance.

Note: The import conflict REST services make significant changes to the IBM Security Key Lifecycle Manager instance that might impact its operation and the communication with the storage device. You must carefully plan and evaluate the changes that are required on both IBM Security Key Lifecycle Manager and the storage device. The changes must be atomic; that is the changes must be done both on the IBM Security Key Lifecycle Manager system and the devices. The import conflict resolution REST services handle the changes for IBM Security Key Lifecycle Manager. For the complete process handling, you must take the guidance of your IBM support representative.

Operation

GET

URL

`https://<host>:<port>/SKLM/rest/v1/ckms/conflictResolution/getChangeHistory`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can

modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON Object with the following specification:	
JSON property name	**Description**
getChangeHistory	Returns the JSON object that contains the information about the historical changes done to the different cryptographic objects in the IBM Security Key Lifecycle Manager instance.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request to get history information

```
GET https://localhost:<port>/SKLM/rest/v1/ckms/conflictResolution/getChangeHistory
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
```

Success response

```
Status Code : 200 OK
Content-Language: en

[{"objectType":"CERTIFICATE","changeType":"ALIAS","oldValue":"cert1","newValue":"cert1_updat
ed","changeTime":"10\/16\/16, 5:26:32 PM GMT-12:00"},
….
{"objectType":"KEY","changeType":"ALIAS","oldValue":"abc0074a5aa0000000001","newValue":"fri0
074a5aa0000000000","changeTime":"10\/17\/16, 12:48:06 AM GMT-12:00"},
……
{"objectType":"DEVICE","changeType":"SERIALNUMBER","oldValue":"DEV1LTO12345”,”newValue":"DEV
1LTO1234U","changeTime":"10\/17\/16, 6:13:07 AM GMT-12:00"},
…
]
```

Error response

```
Status Code : 400 Bad Request
{"code":"CTGKM6002E","message":"CTGKM6002E Bad Request: Invalid user authentication ID or
invalid request format."}
```

Renew Key Alias REST Service

Use **Renew Key Alias REST Service** to change the alias of a key present in the IBM Security Key Lifecycle Manager instance.

Note: The import conflict REST services make significant changes to the IBM Security Key Lifecycle Manager instance that might impact its operation and the communication with the storage device. You must carefully plan and evaluate the changes that are required on both IBM Security Key Lifecycle Manager and the storage device. The changes must be atomic; that is the changes must be done both on the IBM Security Key Lifecycle Manager system and the devices. The import conflict resolution REST services handle the changes for IBM Security Key Lifecycle Manager. For the complete process handling, you must take the guidance of your IBM support representative.

Operation

POST

URL

`https://<host>:<port>/SKLM/rest/v1/ckms/conflictResolution/renewKeyAlias`

By default, IBM Security Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Key Lifecycle Manager installation, you can modify these default ports. If you are using the default port for HTTP or HTTPS, the port is an optional part of the URL.

Request

Request Parameters	
Parameter	**Description**
host	Specify the IP address or host name of the IBM Security Key Lifecycle Manager server.
port	Specify the port number on which the IBM Security Key Lifecycle Manager server listens for requests.

Request Headers	
Header name	**Value**
Content-Type	`application/json`
Accept	`application/json`
Authorization	`SKLMAuth userAuthId=<authIdValue>`
Accept-Language	Any valid locale that is supported by IBM Security Key Lifecycle Manager. For example: en or de

Request body JSON object with the following specification	
Property name	**Description**
oldAlias	Specifies the existing value of the alias for the key that is present in the IBM Security Key Lifecycle Manager system.
newAliasPrefix	Specifies the value to be set for the alias of the key.

Response

Response Headers	
Header name	**Value and description**
Status Code	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request** The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
Content-Type	`application/json`
Content-Language	Locale for the response message.

Success response body JSON object with the following specification	
JSON property name	**Description**
code	Returns the value that is specified by the **status** property.
status	Returns the status to indicate whether the key alias is changed with an appropriate message.

Error Response Body JSON object with the following specification.	
JSON property name	**Description**
code	Returns the application error code.
message	Returns a message that describes the error.

Examples

Service request to renew key alias

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/conflictResolution/renewKeyAlias
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"oldAlias" : "fri004a19372000000000" ,"newAliasPrefix" : "fri"}
```

Success response

```
Status Code : 200 OK
 {"code":"0","status":"Renew of Key alias successfull."}
```

Error response

```
Status Code: 500 Internal Server Error
{"code":"CTGKM2918E","message":"CTGKM2918E Key with Alias name fri004a19372000000000
doesn't exists."}
```

HSM-based encryption for backups

You can configure IBM Security Key Lifecycle Manager to use Hardware Security Module (HSM) for storing the master encryption key, which protects the key materials that are stored in the database.

When you run the IBM Security Key Lifecycle Manager backup operation, a backup archive is created. The backup key in the archive encrypts backup contents. The master key in HSM encrypts the backup key. During the restore process, master key, which is stored in HSM, decrypts the backup key. Then, the backup key is used to restore backup contents.

If you use HSM to store the master key, the backup archive contains the following files:

- Manifest file, which lists all the IBM Security Key Lifecycle Manager data files in the archive.
- IBM Security Key Lifecycle Manager configuration files
- IBM Security Key Lifecycle Manager data dumps

HSM-based encryption is the default method for the backups when HSM is configured to store the master key. You can also use the password-based encryption for the backups when HSM is configured by setting the following property in the `SKLMConfig.properties` file.

```
enablePBEInHSM=true
```

Note:

- If HSM is not configured, you can only use password-based encryption for the backups.
- If the value for **enablePBEInHSM** is not set or set to any other value than `true`, the value is assumed as `false`.
- You can restore the backup file that is created by using either password-based or HSM-based encryption irrespective of the value set for **enablePBEInHSM**.

Backing up data with password-based encryption when HSM is configured

You must set the **enablePBEInHSM=true** property in the SKLMConfig.properties file to back up data with password-based encryption when Hardware Security Module (HSM) is configured.

Before you begin

Ensure that IBM Security Key Lifecycle Manager is configured to use HSM for storing the master key by using steps in the "Configuring HSM parameters" on page 137 topic.

About this task

When HSM is configured, during the backup process, the master key in HSM encrypts the backup key. HSM-based encryption is the default method for the backups when HSM is configured to store the master key. For information about HSM-based encryption, see "HSM-based encryption for backups" on page 132. Your role must have the permission to back up files.

Note: Backup success messages are system wide. Two administrators might run backup tasks that overlap in time. During this interval, the administrator who starts a second task that fails might see a false success message from the first backup task.

Procedure

1. Set the **enablePBEInHSM=true** property in the *<SKLM_HOME>*/config/SKLMConfig.properties file.

   Command-line interface

   a. Go to the WAS_HOME/bin directory. For example,

   Windows

   ```
   cd drive:\Program Files\IBM\WebSphere\AppServer\bin
   ```

   Linux

   ```
   cd /opt/IBM/WebSphere/AppServer/bin
   ```

   b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

   Windows

   ```
   wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
   ```

   Linux

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

   c. Run the **tklmConfigUpdateEntry** CLI command to set **enablePBEInHSM** property in the SKLMConfig.properties configuration file.

   ```
   print AdminTask.tklmConfigUpdateEntry ('[-name enablePBEInHSM
    -value true]')
   ```

   REST interface

   a. Open a REST client.

b. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.

c. Run **Update Config Property REST Service** to set **enablePBEInHSM** property in the SKLMConfig.properties configuration file. Pass the user authentication identifier that you obtained in Step b along with the request message as shown in the following example.

```
PUT https://localhost:<port>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "enablePBEInHSM" : "true"}
```

2. Go to the appropriate page or directory for backing up data.

Graphical user interface

a. Log on to the graphical user interface.

b. On the **Welcome** page, click **Administration** > **Backup and Restore**.

Command-line interface

a. Go to the WAS_HOME/bin directory.

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin.

REST interface

Open a REST client.

3. Create a backup file.

You can run only one backup or restore task at a time.

Graphical user interface

a. On the **Backup and Restore** table, the **Backup repository location** field displays the default *<SKLM_DATA>* directory path, where the backup file is saved, for example, C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data. For the definition of *<SKLM_DATA>*, see "Definitions for HOME and other directory variables" on page 71. Click **Browse** to specify a backup repository location under *<SKLM_DATA>* directory.

Directory path in the **Backup repository location** field changes based on the value that you set for the **tklm.backup.dir** property in the SKLMConfig.properties file.

b. Click **Create Backup**.

c. On the **Create Backup** page, specify information such as a value for the encryption password and backup description. A read-only backup file location is displayed in the **Backup location** field. Ensure that you retain the encryption password for future use in case you restore the backup.

d. Click **Create Backup**.

Command-line interface

Type **tklmBackupRun**, the backup location, password, and any other necessary information to create a backup file as shown in the following example.

```
print AdminTask.tklmBackupRun
    ('[-backupDirectory C:\\sklmbackup1 -password myBackupPwd]')
```

REST interface

Run **Backup Run REST Service** by sending the HTTP POST request as shown in the following example.

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/backups
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
```

```
Accept-Language : en
{"backupDirectory":"/sklmbackup1","password":"myBackupPwd"}
```

4. A message indicates that the backup file was created, or that the backup operation succeeded.

   The time stamp on a backup file has a Greenwich Mean Time (GMT) offset represented in RFC 822 format. The file name contains a *+hhmm* or *-hhmm* element to specify a timezone ahead of or behind GMT. For example, a file name might be `sklm_v3.0.1.0_20170123144220-0800_backup.jar`, where -0800 indicates that the timezone is eight hours behind GMT.

What to do next

Do not edit a file in the backup JAR file. The file that you attempt to edit becomes unreadable. You must connect to the same HSM and the master key for backup and restore operations irrespective of whether you use HSM-based encryption or password-based encryption.

Backing up data with HSM-based encryption

When IBM Security Key Lifecycle Manager is configured with Hardware Security Module (HSM) for storing the master encryption key, you can use HSM-based encryption for creating secure backups.

Before you begin

Ensure that IBM Security Key Lifecycle Manager is configured to use HSM for storing the master key before you back up data with HSM-based encryption. For the configuration steps, see "Configuring HSM parameters" on page 137.

You must consider the following guidelines for HSM-based encryption

- The same HSM partition must be present with all its key entries on the system where the backup file is restored.
- Master key that you used for the backup key encryption must be intact to restore the backup file. If the master key is refreshed, all the older backups are inaccessible or unusable.
- You must connect to the same HSM and the master key for backup and restore operations irrespective of whether you use HSM-based encryption or password-based encryption.

About this task

When you run the IBM Security Key Lifecycle Manager backup operation, a backup archive is created. The backup key in the archive encrypts backup contents. The master key in HSM encrypts the backup key. During the restore process, master key, which is stored in HSM, decrypts the backup key. Then, the backup key is used to restore backup contents. For information about HSM-based encryption, see "HSM-based encryption for backups" on page 132. Your role must have the permission to back up files.

IBM Security Key Lifecycle Manager creates backup files in a manner that is independent of operating systems and directory structure of the server. You can restore the backup files to an operating system that is different from the one it was backed up from.

Note: Backup success messages are system wide. Two administrators might run backup tasks that overlap in time. During this interval, the administrator who starts a second task that fails might see a false success message from the first backup task.

Procedure

1. Go to the appropriate page or directory.

   Graphical user interface

   a. Log on to the graphical user interface.

   b. On the **Welcome** page, click **Administration** > **Backup and Restore**.

Command-line interface

a. Go to the WAS_HOME/bin directory. For example,

Windows

```
cd drive:\Program Files (x86)\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

```
wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
```

Linux

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

REST interface

Open a REST client.

2. Create a backup file.

You can run only one backup or restore task at a time.

Graphical user interface

a. On the **Backup and Restore** table, the **Backup repository location** field displays the default *<SKLM_DATA>* directory path, where the backup file is saved, for example, C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data. For the definition of *<SKLM_DATA>*, see "Definitions for HOME and other directory variables" on page 71. Click **Browse** to specify a backup repository location under *<SKLM_DATA>* directory.

Directory path in the **Backup repository location** field changes based on the value that you set for the **tklm.backup.dir** property in the SKLMConfig.properties file.

b. Click **Create Backup**.

c. On the **Create Backup** page, specify a description. A read-only backup file location is displayed in the **Backup location** field.

d. Click **Create Backup**.

Command-line interface

Type **tklmBackupRun**, the backup location, and any other necessary information to create a backup file. For example:

```
print AdminTask.tklmBackupRun
    ('[-backupDirectory C:\\sklmbackup1]')
```

REST interface

a. Obtain a unique user authentication identifier to access IBM Security Key Lifecycle Manager REST services. For more information about the authentication process, see "Authentication process for REST services" on page 69.

b. To run **Backup Run REST Service**, send the HTTP POST request. Pass the user authentication identifier that you obtained in Step a along with the request message as shown in the following example.

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/backups
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
{"backupDirectory":"/sklmbackup1"}
```

3. A message indicates that the backup file was created, or that the backup operation succeeded.

The time stamp on a backup file has a Greenwich Mean Time (GMT) offset represented in RFC 822 format. The file name contains a *+hhmm* or *-hhmm* element to specify a timezone ahead of or behind GMT. For example, a file name might be `sklm_v3.0.1.0_20170123144220`**`-0800`**`_backup.jar`, where -0800 indicates that the timezone is eight hours behind GMT.

What to do next

Do not edit a file in the backup JAR file. The file that you attempt to edit becomes unreadable. Master key that was used for the backup key encryption must be intact to restore the backup file. If the master key is refreshed, all the older backups are inaccessible or unusable.

Configuring HSM parameters

You must define the **pkcs11.pin**, **pkcs11.config**, and **useMasterKeyInHSM** configuration parameters to configure Hardware Security Module.

Procedure

1. Set up the HSM as per the instructions from HSM manufacturers.
2. Add the **pkcs11.pin**, **pkcs11.config**, and **useMasterKeyInHSM** parameters to the IBM Security Key Lifecycle Manager configuration file. You can use the following CLI command or REST interface to add the parameter:

   REST interface

   ```
   PUT https://localhost:<port>/SKLM/rest/v1/configProperties
   { "pkcs11.pin" : "<hsm pin>"}
   ```

   ```
   PUT https://localhost:<port>/SKLM/rest/v1/configProperties
   { "pkcs11.config" : "<hsm config file>"}
   ```

   ```
   PUT https://localhost:<port>/SKLM/rest/v1/configProperties
   { "useMasterKeyInHSM" : "<true | false>"}
   ```

   Note: <*hsm pin*> is the PIN for HSM. <*hsm config file*> is the full path and file name to the HSM configuration file. For example: `C:\Program Files\IBM\WebSphere\AppServer\sklm\config\LunaSA.cfg`.

   Command-line interface

   ```
   print AdminTask.tklmConfigUpdateEntry('[-name pkcs11.pin -value
   <hsm pin>]')
   ```

   ```
   print AdminTask.tklmConfigUpdateEntry('[-name pkcs11.config -value
   <hsm config file>]')
   ```

   ```
   print AdminTask.tklmConfigUpdateEntry('[-name useMasterKeyInHSM -value
   <true | false>]')
   ```

3. Restart IBM Security Key Lifecycle Manager.

LDAP configuration

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.

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 a member of a specific IBM Security Key Lifecycle Manager application group.

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.

When 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.

To integrate LDAP with IBM Security Key Lifecycle Manager, use any of the following configuration methods:

- By using WebSphere Integrated Solutions Console. For more information, see Integrating LDAP by using WebSphere Integrated Solutions Console.
- By running the LDAP configuration scripts. For more information, see Running the LDAP configuration scripts.

Adding LDAP repository to the federated repository

You must add LDAP repository to the federated repository to configure an LDAP repository, such as IBM Security Directory Server or Microsoft Active Directory in the federated repository.

About this task

For more information about configuring LDAP settings in a federated repository configuration, see http://www-01.ibm.com/support/knowledgecenter/api/redirect/wasinfo/v8r5/topic/com.ibm.websphere.base.doc/ae/twim_ldap_settings.html.

Procedure

1. Log on to WebSphere Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`) as `wasadmin` user.
2. In the navigation bar, click **Security** > **Global security**.
3. Under **User account repository**, select **Federated repositories** from the **Available realm definitions** drop-down list.
4. Click **Configure**.
5. In the **Global security** > **Federated repositories** page, click **Add Repositories (LDAP, custom,etc...)**.
6. In the **Global security** > **Federated repositories** > **Repository reference** page, select **LDAP Repository** from the **New Repository** drop-down list.
7. In the **Global security** > **Federated repositories** > **Repository reference** > **New** page, specify name of the LDAP repository and other details according to your requirements.
8. Click **OK**.
9. Click **Save** to save the configuration.
10. In the **Global security** > **Federated repositories** > **Repository reference** page, specify the value for **Unique distinguished name of the base (or parent) entry in federated repositories**.

11. Click **OK**.
12. In the **Global security** > **Federated repositories** page, select the link to the LDAP repository that you created.
13. In the **Global security** > **Federated repositories** > **<LDAP Repository Name>** page, under Additional Properties, select `Federated repositories` entity types to LDAP object classes mapping link.

    In the **Global security** > **Federated repositories** > **<LDAP Repository Name>** > **Federated repositories entity types to LDAP object classes mapping** page, ensure that each entity type listed is mapped to the correct object classes. Modify the values according to your requirements.
14. In the **Global security** > **Federated repositories** page, select the link to the LDAP repository that you created. Under Additional Properties, select **Group attribute definition**.
15. In the **Global security** > **Federated repositories** > **<LDAP Repository Name>** > **Group attribute definition** page, under Additional Properties, select **Member Attributes**.
16. In the **Global security** > **Federated repositories** > **<LDAP Repository Name>** > **Group attribute definition** > **Member attributes** page, ensure that `uniqueMember` member attribute is mapped to the correct object class. If this attribute is not present, create an attribute and map it to the correct object class.

What to do next
Create a data source from WebSphere Integrated Solutions Console.

Creating a database-based repository

Create a database-based repository to hold all the IBM Security Key Lifecycle Manager application groups and to remove all the IBM Security Key Lifecycle Manager application groups from file-based repository. You must add the IBM Security Key Lifecycle Manager application groups to database-based repository and update the WebSphere Application Server federated repository with LDAP repository.

Procedure

1. Go to the *<WAS_HOME>*`\bin` folder.
2. Run the following commands:

```
wsadmin.bat -user wasadmin user -password wasadmin passwd -lang jython -f
SKLM_INSTALL_HOME\bin\LDAPIntegration\createDBRepos.py WAS_HOME LDAP_DBNAME
SKLM_DBUSER SKLM_DBUSERPASSWD SKLM_DBPORT#
```

Notes:

- On Linux platforms, use **`wsadmin.sh`** instead of **`wsadmin.bat`**.
- During IBM Security Key Lifecycle Manager installation, if you use the defaults,

  ```
  LDAP_DBNAME = USERDB40
  SKLM_DBUSER = SKLMDB40
  SKLM_DBPORT# = 50060
  ```

  SKLM_DBUSERPASSWD is the IBM Security Key Lifecycle Manager database password that you specified during the installation.
- During IBM Security Key Lifecycle Manager installation, if you use the defaults,

  ```
  LDAP_DBNAME = USERDB40
  SKLM_DBUSER = SKLMDB40
  SKLM_DBPORT# = 50060
  ```

  SKLM_DBUSERPASSWD is the IBM Security Key Lifecycle Manager database password that you specified during the installation.
- All the `.py` python scripts are present in the *<SKLM_INSTALL_HOME>*`\bin\LDAPIntegration` directory.

<SKLM_INSTALL_HOME> path typically,

Windows
`C:\Program Files\IBM\SKLMV40`

Linux
`/opt/IBM/SKLMV40`

3. Run the following command.

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
<SKLM_INSTALL_HOME>\bin\LDAPIntegration\removeGroupsFromDefRepos.py
```

4. From the WebSphere Integrated Solutions Console, modify `Security role to user/group mapping` for removing the administrator role mapping to `klmGUICLIAccessGroup`.
   a. Log on to WebSphere Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`).
   b. In the navigation bar, click **Applications** > **Application Types** > **Application Types** > **WebSphere enterprise applications**.
   c. Click the **sklm_kms** link.
   d. In the **Enterprise Applications** > **sklm_kms** page, under the **Detail Properties** section, click the **Security role to user/group mapping** link.
   e. In the **Enterprise Applications** > **sklm_kms** > **Security role to user/group mapping** page, select the **administrator** role.
   f. Click **Map Groups**.
   g. Select **klmGUICLIAccessGroup** from the list and click the left arrow button to remove **klmGUICLIAccessGroup** from the list.
   h. Click **OK**.
   i. Click the **Save** link to save the configuration.
5. Restart WebSphere Application Server
6. Run the following command.

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython
-f <SKLM_INSTALL_HOME>\bin\LDAPIntegration\addGroupsToDBRepos.py
```

7. Run the following command.

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython
-f <SKLM_INSTALL_HOME>\bin\LDAPIntegration\updateLDAPReposConfig.py <LDAPRepos Name
- name used earlier when LDAP repos was created>
```

What to do next
Add security role to user/group mapping and map administrator role to `klmGUICLIAccessGroup`.

Adding security user roles from WebSphere Integrated Solutions Console

You must add security role to user or group mapping, and map administrator role to `klmGUICLIAccessGroup` for integrating IBM Security Key Lifecycle Manager with LDAP user repositories.

About this task

Procedure

1. Log on to WebSphere Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`) as a `wasadmin` user.

2. In the navigation bar, click **Applications** > **Application Types** > **Application Types** > **WebSphere enterprise applications**.
3. Click the **sklm_kms** link.
4. In the **Enterprise Applications** > **sklm_kms** page, under the **Detail Properties** section, click the **Security role to user/group mapping** link.
5. In the **Enterprise Applications** > **sklm_kms** > **Security role to user/group mapping** page, select the **administrator** role.
6. Click **Map Groups**.
7. In the **Enterprise Applications** > **sklm_kms** > **Security role to user/group mapping** > **Map users/ groups**page:
   a. Under the **Search and Select Groups** section, in the **Search string** text box, enter `klmGUICLIAccessGroup`.
   b. Click **Search**.
   c. Select `klmGUICLIAccessGroup` from the list and click the right arrow button.

      `klmGUICLIAccessGroup` is added to the **Selected** list.
   d. Click **OK**.
   e. Click **OK** in the **Enterprise Applications** > **sklm_kms** > **Security role to user/group mapping** page.
8. Click the **Save** link to save the configuration information.

What to do next
Restart WebSphere Application Server.

Adding LDAP users to IBM Security Key Lifecycle Manager application groups

You must add LDAP Users to IBM Security Key Lifecycle Manager Application Groups to integrate IBM Security Key Lifecycle Manager with LDAP user repositories.

Procedure

1. Go to the *<SKLM_INSTALL_HOME>*`/bin` folder.

   Note: All the `.py` python scripts are present in the *<SKLM_INSTALL_HOME>*`/bin/LDAPIntegration` directory.

   <SKLM_INSTALL_HOME> path typically,

   Windows
   `C:\Program Files\IBM\SKLMV40`

   Linux
   `/opt/IBM/SKLMV40`
2. Run the following commands:

```
wsadmin.bat -user <wasadmin user> -password <waasadmin passwd> -lang jython -f
addLDAPUserToGroup.py <user uniqueName> <group name>
```

   Notes: On Linux platforms, use **`wsadmin.sh`** instead of **`wsadmin.bat`**

   The user unique name is the Unique Name component in LDAP registry. For example:

```
uid=001,c=in,ou=bluepages,o=ibm.com
```

For an LDAP user who needs IBM Security Key Lifecycle Manager admin access, the user must be made member of `klmGUICLIAccessGroup` and `klmSecurityOfficerGroup`. To do so, run the following commands:

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
<SKLM_INSTALL_HOME>\bin\LDAPIntegration\addLDAPUserToGroup.py
<user uniqueName> klmGUICLIAccessGroup
```

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
<SKLM_INSTALL_HOME>\bin\LDAPIntegration\addLDAPUserToGroup.py
<user uniqueName> klmSecurityOfficerGroup
```

What to do next
Take IBM Security Key Lifecycle Manager application backup.

Integrating LDAP by using WebSphere Integrated Solutions Console

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.

Before you begin
For prerequisite information, see "LDAP configuration" on page 137

Procedure

1. Add LDAP repository to the federated repository. For the instructions, see "Adding LDAP repository to the federated repository" on page 138.
2. Create the database for LDAP configuration.
   a. Open the DB2 command window.
   b. Run the following command to create the database.

   ```
   db2  create database USERDB40 using codeset UTF-8 territory US
   ```
3. Update the data source from the WebSphere Integrated Solutions Console with `jndi` name `jdbc/wimXADS`. For the instructions, see "Updating a data source from WebSphere Integrated Solutions Console" on page 119.
4. Restart WebSphere Application Server.
5. Copy `db2jcc.jar and db2jcc_license_cu.jar` from the `DB2SKLMV40` directory to the *WAS_HOME*`/lib` directory.

   Note: Ensure that the non-administrator or non-root user account has access to the `db2jcc.jar and db2jcc_license_cu.jar` files.

   `DB2SKLMV40` path:

   Windows
   drive`:\Program Files\IBM\DB2SKLMV40\java`

   Linux
   path`/IBM/DB2SKLMV40/java`

   Default definition of *WAS_HOME* variable is typically:

   Windows
   `C:\Program Files\IBM\WebSphere\AppServer`

   Linux
   `/opt/IBM/WebSphere/AppServer`

6. Create database-based repository to hold all the IBM Security Key Lifecycle Manager application groups. For the instructions, see “Creating a database-based repository” on page 139.
7. From WebSphere Integrated Solutions Console, add security role to user/group mapping and map administrator role to `klmGUICLIAccessGroup` . For the instructions, see “Adding security user roles from WebSphere Integrated Solutions Console” on page 140.
8. Restart WebSphere Application Server.
9. Add LDAP users to IBM Security Key Lifecycle Manager application groups. For the instructions, see “Adding LDAP users to IBM Security Key Lifecycle Manager application groups” on page 141
10. Take the IBM Security Key Lifecycle Manager application backup. The data in the database-based repository is also backed up.

What to do next

After LDAP is configured, you must run the subsequent tasks. For more information, see “Post-LDAP configuration tasks to support LDAP integration” on page 119

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, MD-NC119
Armonk, NY 10504-1785
US

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119

Armonk, NY 10504-1785
US

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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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_.

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

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

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

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

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

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

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

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

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

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

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

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

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

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

Product Number: