

IBM Security Guardium Key Lifecycle Manager

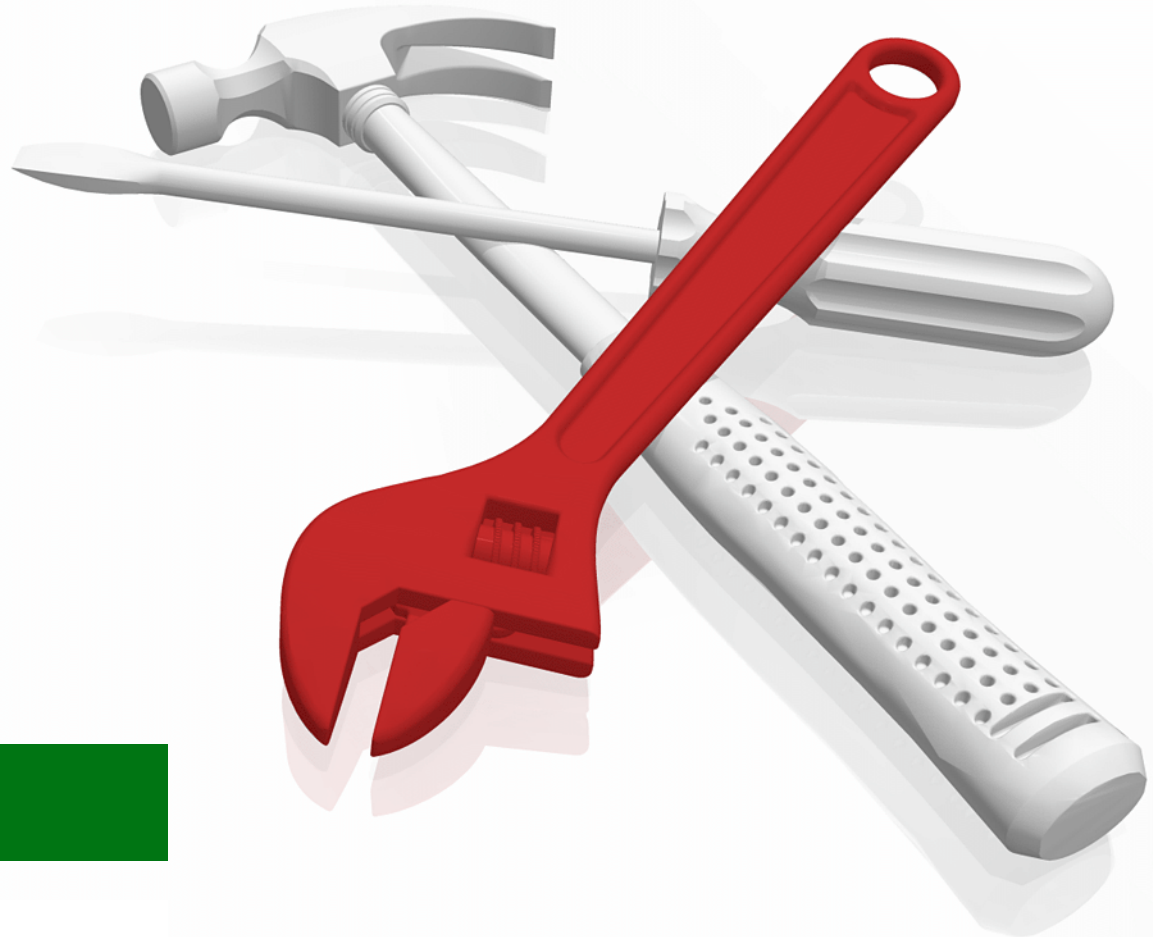
Rinkesh Bansal

Aditi Prasad

Shiv Jha

Saandiip Koturwwar

Alka Acharya





IBM Redbooks

IBM Security Guardium Key Lifecycle Manager

July 2021

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

Second Edition (July 2021)

This edition applies to version 4.1.0.1 of IBM Security Guardium Key Lifecycle Manager (product number 5724-T60).

© Copyright International Business Machines Corporation 2021. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	v
Trademarks	vi
Preface	vii
Authors	vii
Now you can become a published author, too!	viii
Comments welcome	viii
Stay connected to IBM Redbooks	viii
Chapter 1. Introduction	1
1.1 Overview	2
1.2 What's new in IBM Security Guardium Key Lifecycle Manager v4.1.0.1	3
1.3 Comparing IBM Security Guardium Key Lifecycle Manager Traditional Edition and Container Edition	4
Chapter 2. IBM Security Guardium Key Lifecycle Manager Traditional Edition installation	5
2.1 Pre-installation tasks	6
2.2 Installing IBM Security Guardium Key Lifecycle Manager Traditional Edition in a GUI mode 7	
2.3 Verifying successful installation	13
2.4 Installing IBM Security Guardium Key Lifecycle Manager Traditional Edition in silent mode 15	
2.5 Installing fix pack for IBM Security Guardium Key Lifecycle Manager Traditional Edition 21	
Chapter 3. Installing Container Edition	27
3.1 Deployment prerequisites	28
3.2 Installing IBM Security Guardium Key Lifecycle Manager on Red Hat OpenShift	29
3.2.1 Installing IBM Security Guardium Key Lifecycle Manager Container Edition on Red Hat OpenShift with PostgreSQL	29
3.2.2 Activating the license and logging in to IBM Security Guardium Key Lifecycle Manager	33
3.2.3 Installing IBM Security Guardium Key Lifecycle Manager Container Edition on Red Hat OpenShift with Db2U	36
3.2.4 Exposing non-HTTP port in Red Hat OpenShift installation	37
3.2.5 Installing IBM Security Guardium Key Lifecycle Manager Container Edition as Fix Pack on Red Hat OpenShift	39
3.2.6 Troubleshooting in Red Hat OpenShift	39
3.3 Installing IBM Security Guardium Key Lifecycle Manager Container Edition on Kubernetes 41	
3.3.1 Installing IBM Security Guardium Key Lifecycle Manager on Kubernetes	41
3.3.2 Installing IBM Security Guardium Key Lifecycle Manager Container Edition as Fix Pack on Kubernetes	42
3.3.3 Troubleshooting in Kubernetes environment	43
3.4 Installing IBM Security Guardium Key Lifecycle Manager Container Edition on IBM z/OS Container Extensions	44
3.4.1 Installing IBM Security Guardium Key Lifecycle Manager on IBM zCX with PostgreSQL	44

3.4.2	Installing IBM Security Guardium Key Lifecycle Manager with Db2 for z/OS	45
3.4.3	Installing IBM Security Guardium Key Lifecycle Manager Container Edition as Fix Pack in z/CX Environment	47
Chapter 4.	Migrating data	49
4.1	Migrating from an earlier version of IBM Security Key Lifecycle Manager	50
4.2	Inline migration	51
4.3	Cross migration	54
4.3.1	Cross migration by using backup and restore utility	54
4.3.2	Cross migration by using backup and restore from GUI	57
Chapter 5.	Configuring IBM Security Guardium Key Lifecycle Manager	59
5.1	Configuring an TLS/KMIP certificate for IBM Security Guardium Key Lifecycle Manager	60
5.1.1	Logging in to IBM Security Guardium Key Lifecycle Manager GUI	60
5.1.2	Creating a self-signed server certificate	61
5.1.3	Creating a third-party CA signed server certificate	63
5.1.4	Exporting and downloading Server certificate	66
5.2	Backing up and restoring IBM Security Guardium Key Lifecycle Manager	67
5.2.1	Backing up IBM Security Guardium Key Lifecycle Manager	67
5.2.2	Restoring IBM Security Guardium Key Lifecycle Manager	69
5.3	Configuring replication for IBM Security Guardium Key Lifecycle Manager	71
5.3.1	Configuring the master server for replication	72
5.3.2	Configuring the master server for Incremental Replication	75
5.3.3	Configuring the clone server for replication	77
5.4	Configuring a Multi-Master cluster	80
5.4.1	Types of servers in a Multi-Master cluster	81
5.4.2	Setting up minimal deployment of a Multi-Master cluster	81
5.4.3	Agent Status	87
5.4.4	HADR takeover scenarios	88
5.5	Integrating LDAP with IBM Security Guardium Key Lifecycle Manager Traditional Edition by using configuration scripts	91
5.5.1	Preparing for the configuration	91
5.5.2	LDAP configuration database and updating the data source for WIM	92
5.5.3	Creating a database-based repository	96
5.6	Integrating LDAP with IBM Security Guardium Key Lifecycle Manager Container Edition	101
5.7	Configuring signed CA certificates for IBM Security Guardium Key Lifecycle Manager portal and IBM WebSphere console access	105
Related publications		115
IBM Redbooks		115
Online resources		115
Help from IBM		115

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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 grant 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

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

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

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 actual people or business enterprises 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.

Trademarks

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

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX®	IBM®	System z®
Db2®	IBM Security™	Tivoli®
DS8000®	Redbooks®	WebSphere®
Guardium®	Redbooks (logo)  ®	z/OS®

The following terms are trademarks of other companies:

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

OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redbooks® publication describes the installation, integration, and configuration of IBM Security Guardium® Key Lifecycle Manager.

Authors

This book was produced by a team of IBM® specialists from around the world.

Rinkesh Bansal is a Senior Development and Release Manager for Encryption and Key Management products at IBM. He is expert in Key Management domain and has more than 18 years of experience. He joined IBM in 2009, working with IBM Security™ Guardium Key Lifecycle (GKLM) team since 2012. His experience includes roles as an Install package developer, test engineer, test lead, automation lead, Project Manager, and Release Manager. He currently manages the GKLM development team. He is a passionate innovator with 10 patents and an enthusiastic speaker at various conferences, colleges, and schools.

Aditi Prasad is an Advisory Software Engineer at IBM. She joined IBM in 2008 and is working with the IBM Security GKLM team since 2012. She is the Level 3 support lead for GKLM. She has 13 years of experience with more than 7 years in Security Domain. She holds a Masters degree in Computer Science from Pune University, India.

Shiv Jha is a Test Lead and Project Manager for IBM Security GKLM product in IBM. He joined IBM in 2013 and has 17 years of experience. He is working with the GKLM team for last 7 years. Shiv holds a Masters degree in Computer Science from BITS Pilani, India.

Saandiip Koturwwar is a Senior QA specialist in IBM, India. He has 15 years of experience in the QA domain. He joined IBM in 2007 and has been working with IBM Security GKLM team since 2015. His experience includes roles as a test engineer and automation engineer. He holds a Masters degree in Computer Science and Engineering from Aurangabad University, India.

Alka Acharya has been working in the IBM Software Labs as an Information Developer since November 2018. She is responsible for authoring and delivering the customer-facing documentation for IBM Security GKLM. She has 15 years of experience in delivering product and training documentation. She holds a Bachelor's degree in Engineering (Computer Science) from the University of Pune, India.

Thanks to the author of the previous edition:

An Chen

Client Technical Specialist, IBM Australia

Thanks to the following people for their contributions to this project:

Bert Dufrasne

Project Leader, IBM Redbooks®, San Jose Center

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- ▶ Send your comments in an email to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, IBM Redbooks
Dept. Security Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- ▶ Find us on LinkedIn:

<http://www.linkedin.com/groups?home=&gid=2130806>

- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>

- ▶ Stay current on recent Redbooks publications with RSS Feeds:

<http://www.redbooks.ibm.com/rss.html>



Introduction

This chapter provides a general overview of IBM Security Guardium Key Lifecycle Manager, new features of IBM Security Guardium Key Lifecycle Manager v4.1.0.1, and a comparison between IBM Security Guardium Key Lifecycle Manager Container Edition and IBM Security Guardium Key Lifecycle Manager Traditional Edition.

This chapter includes the following topics:

- ▶ 1.1, “Overview” on page 2
- ▶ 1.2, “What’s new in IBM Security Guardium Key Lifecycle Manager v4.1.0.1” on page 3
- ▶ 1.3, “Comparing IBM Security Guardium Key Lifecycle Manager Traditional Edition and Container Edition” on page 4

1.1 Overview

IBM Security Guardium Key Lifecycle Manager provides key storage, key serving, and key lifecycle management for storage devices, tape drives, databases, and applications from IBM and other vendors. For more information, see [IBM Documentation](#).

IBM Security Guardium Key Lifecycle Manager supports the following methods for communicating with client devices and applications to manage and serve cryptographic keys:

- ▶ Key Management Interoperability Protocol (KMIP)

You can use KMIP operations for secure communication between the IBM Security Guardium Key Lifecycle Manager server and the self-encrypting devices that are KMIP compatible, such as Spectrum Scale and VMware.

- ▶ IPP

Some self-encrypting devices use IBM proprietary Protocol (IPP) to communicate with IBM Security Guardium Key Lifecycle Manager server for Cryptographic keys, such as LTO tape drives, and IBM DS8000® data at rest.

- ▶ REST APIs

You can use IBM Security Guardium Key Lifecycle Manager REST key serving interface to manage and serve Cryptographic keys for applications that support REST APIs, such as Cloud applications.

For more information, see the following resources:

- ▶ [Support Dashboard \(bookmark this link\)](#)
- ▶ [Hardware, Operating System and other requirements](#)
- ▶ [Supported Storage and Non-storage devices](#)

1.2 What's new in IBM Security Guardium Key Lifecycle Manager v4.1.0.1

IBM Security Guardium Key Lifecycle Manager v4.1.0.1 includes the following key features:

- ▶ IBM Security Key Lifecycle Manager was rebranded as IBM Security Guardium Key Lifecycle Manager.
- ▶ IBM Security Guardium Key Lifecycle Manager is now available in Container edition that supports the following container platforms:
 - Red Hat OpenShift
 - Kubernetes
 - IBM Z/OS Container Extensions (zCX)
- ▶ Groups of clients can be created and the new workflow used to manage clients to enable seamless sharing and serving of cryptographic objects among them
- ▶ Support for Log Event Extended Format (LEEF) format for audit logs
- ▶ Support for IBM Java JCEPlus and JCEPlusFIPS provider for cryptographic operations
- ▶ Important features in IBM Security Guardium Key Lifecycle Manager Container Edition:
 - User Management through IBM Security Guardium Key Lifecycle Manager graphical user interface (GUI)
 - LDAP configuration through IBM Security Guardium Key Lifecycle Manager GUI
 - Support for PostgreSQL database for storing cryptographic keys and metadata
- ▶ Important features in IBM Security Guardium Key Lifecycle Manager Traditional Edition:
 - New prerequisite utility for accurate prerequisite checking before installation
 - Installation of IBM Security Guardium Key Lifecycle Manager as a domain (Microsoft Active Directory) user on a domain-managed Windows system.
 - Multi-Master Agent status on IBM Security Guardium Key Lifecycle Manager GUI for easy monitoring
 - New utility to convert master in Multi-Master cluster to Standalone
 - Password-less authentication with the database (Db2) by using Kerberos

1.3 Comparing IBM Security Guardium Key Lifecycle Manager Traditional Edition and Container Edition

IBM Security Guardium Key Lifecycle Manager 4.1 supports Traditional Edition and Container Edition. The editions are compared in Table 1-1.

Table 1-1 Comparison between GKLM Traditional and Container Editions

Features	Traditional Edition	Container Edition
Deployment Platform	Windows IBM AIX® Linux (x86-64, PPC, Linux on z)	Red Hat OpenShift Kubernetes IBM zCX
Deployment time	~1 hour	~2 minutes
Backup and Restore support	Yes	Yes
Replication Support	Yes	Yes
Multi-Master Support	Yes	No
Administration through GUI	Yes	Yes
Administration through REST	Yes	Yes
Administration through CLI	Yes	No
Key serving through KMIP	Yes	Yes
Key serving through IPP	Yes	Yes
Key serving through REST	Yes	Yes
User Management	Through IBM WebSphere® Application Server	through GKLM GUI
LDAP configuration	Through IBM WebSphere Application Server UI or scripts	through GKLM GUI
Kerberos support	Yes	No
Bundled products	WebSphere Application Server traditional IBM Db2® Standard Edition IBM Java	WebSphere Application Server Liberty IBM Java
Supported database	Db2 Standard Edition	PostgreSQL Db2U (only on Red Hat OpenShift) Db2 on Z/OS (only on IBM zCX)



IBM Security Guardium Key Lifecycle Manager Traditional Edition installation

This chapter describes the tasks that are associated with the installation of IBM Security Guardium Key Lifecycle Manager v4.1.0.1 for Traditional Edition and fix packs.

This chapter includes the following topics:

- ▶ 2.1, “Pre-installation tasks” on page 6
- ▶ 2.2, “Installing IBM Security Guardium Key Lifecycle Manager Traditional Edition in a GUI mode” on page 7
- ▶ 2.3, “Verifying successful installation” on page 13
- ▶ 2.4, “Installing IBM Security Guardium Key Lifecycle Manager Traditional Edition in silent mode” on page 15
- ▶ 2.5, “Installing fix pack for IBM Security Guardium Key Lifecycle Manager Traditional Edition” on page 21

2.1 Pre-installation tasks

You can install IBM Security Guardium Key Lifecycle Manager Traditional Edition on distributed platforms.

Before installing the IBM Security Guardium Key Lifecycle Manager Traditional Edition, complete the following prerequisite tasks:

- ▶ Ensure that the hardware and operating system meet the prerequisites that are provided in the [IBM Security Guardium Key Lifecycle Manager Support Matrix](#) document.
- ▶ Ensure that you follow the guidelines that are listed in the [Installation guidelines](#) topic in the IBM Documentation (formerly IBM Knowledge Center).
- ▶ Run the prerequisite check script to ensure that the system requirements are met. For more information, see [Checking prerequisites](#).

Download the following installation files from [this web page](#):

- SGKLM_4.1_FOR_WINDOWS_SERVER_1OF2.zip
- SGKLM_4.1_FOR_WINDOWS_SERVER_2OF2.zip

- ▶ Extract the files to a temporary directory on your system such that disk1 and disk2 are in same folder, as shown in Figure 2-1.

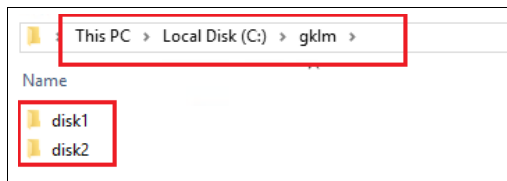


Figure 2-1 Extracted folders from installation files

- ▶ After files are extracted, go to the disk1 folder and ensure that the launchpad.bat script is extracted to the disk1 directory, as shown in Figure 2-2.

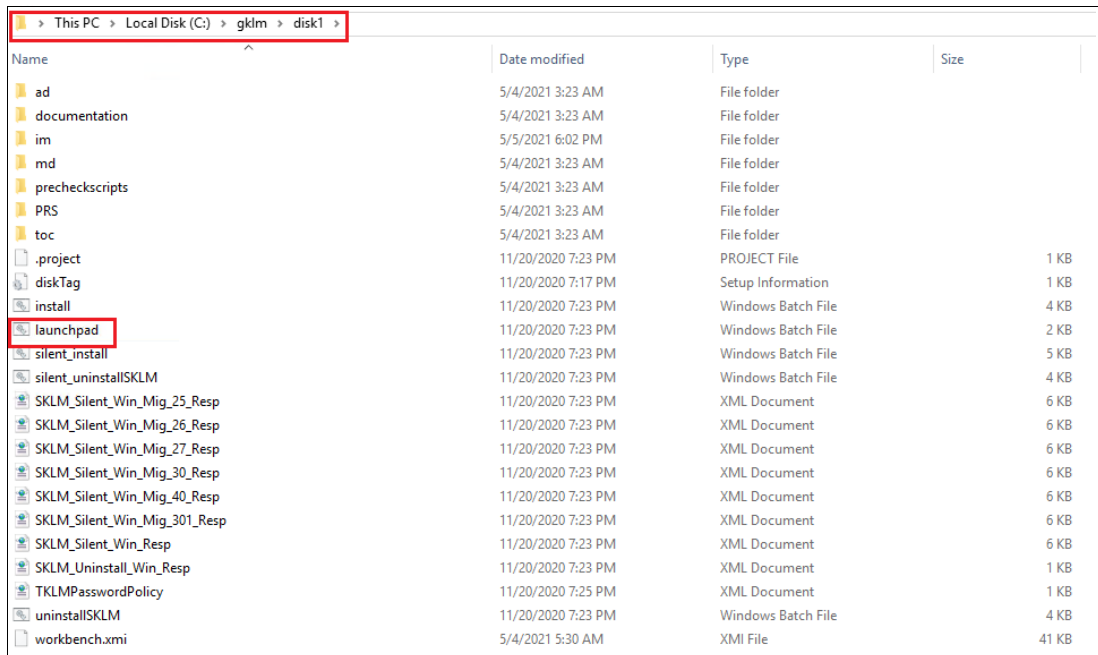


Figure 2-2 Extracted installation files in disk1 directory

2.2 Installing IBM Security Guardium Key Lifecycle Manager Traditional Edition in a GUI mode

Complete the following steps to install IBM Security Guardium Key Lifecycle Manager v4.1.0.0 Traditional Edition:

1. Double-click the **1aunhpad.bat** script available in the `disk1` folder to start the installation wizard. Enter 1 to select English as the locale, and press **Enter** to proceed with installation process, as shown in Figure 2-3.

```
Choose the locale for Installation Manager.  
1. English  
2. French  
3. German  
4. Spanish  
5. Italian  
6. Japanese  
7. Korean  
8. Simplified Chinese  
9. Traditional Chinese  
Enter the number that is corresponding to the locale you want to use for the installation (English is selected by default)  
t) : 1
```

Figure 2-3 Select Locale

Prerequisite checker checks required availability for CPU and RAM, as shown in Figure 2-4.

```
Choose the locale for Installation Manager.  
1. English  
2. French  
3. German  
4. Spanish  
5. Italian  
6. Japanese  
7. Korean  
8. Simplified Chinese  
9. Traditional Chinese  
Enter the number that is corresponding to the locale you want to use for the installation (English is selected by default)  
t) : 1  
Selected locale is English.  
Starting IBM Security Guardium Key Lifecycle Manager.  
No preinstalled IBM Installation Manager found on the system.  
"SKLM Pre-requisite check" started  
checking CPU speed - PASSED  
checking required memory - PASSED  
"SKLM Pre-requisite check" - PASSED  
Installing IBM Security Guardium Key Lifecycle Manager v4.1.0  
880 File(s) copied
```

Figure 2-4 Prerequisite checker

The installation GUI is displayed if no issues are found by the prerequisite checker.

2. All components are required for an installation, as shown in Figure 2-5. Click **Next**.

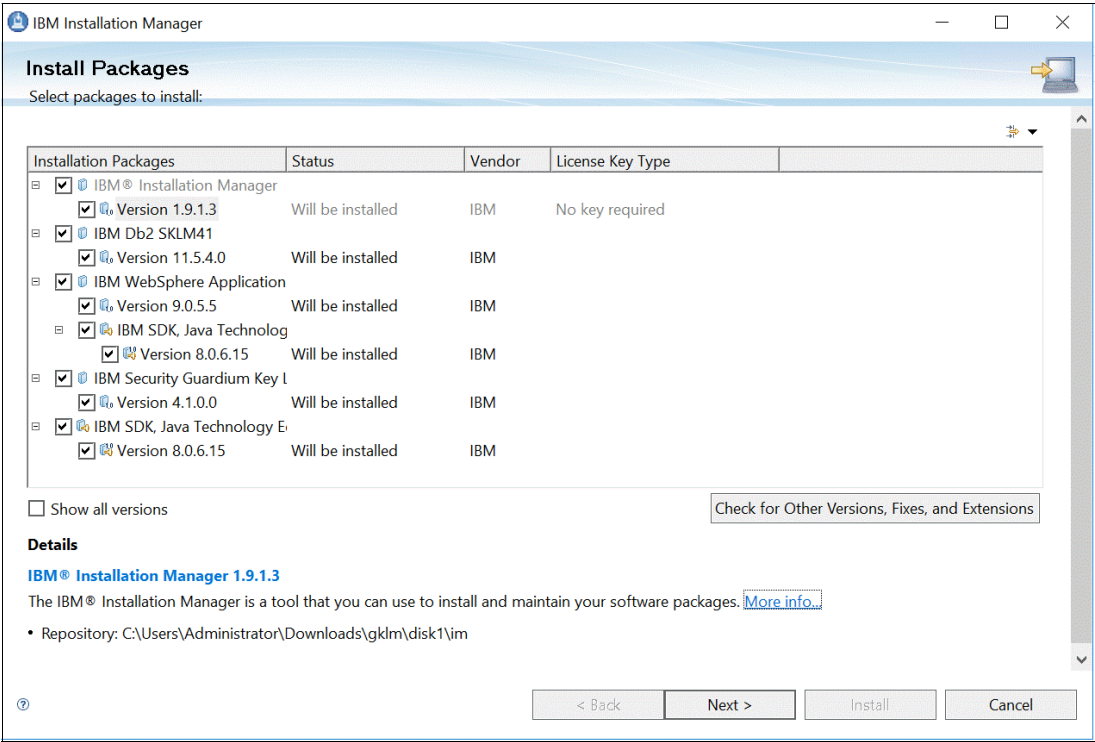


Figure 2-5 Components to be installed

3. Review and accept the terms in the license agreement, as shown in Figure 2-6. Click **Next**.

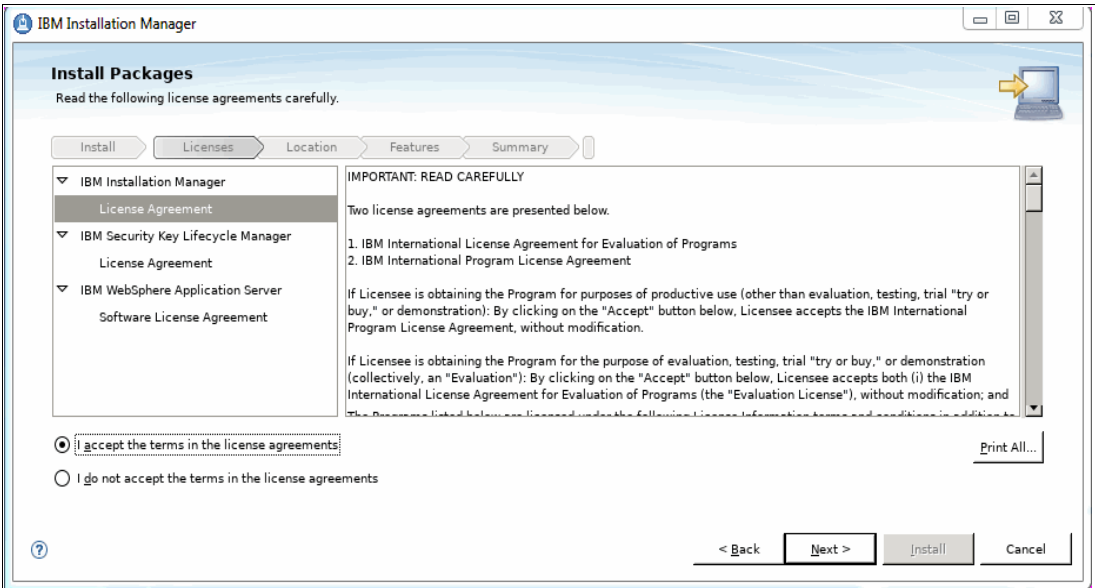


Figure 2-6 Accepting the terms in the license agreement

- Specify the installation path for the Shared Resources Directory and IBM Installation Manager, as shown in Figure 2-7 on page 9. Click **Next**.

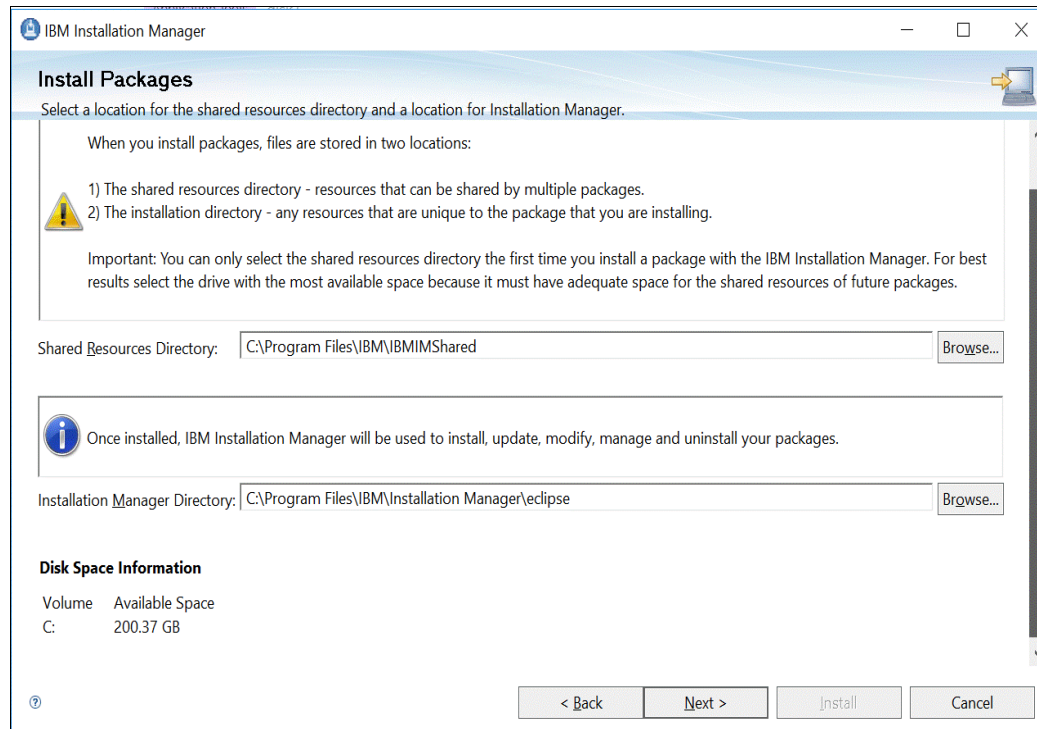


Figure 2-7 Shared Resources Directory and Installation Manager installation path

- Specify the installation path or keep default path for the IBM Db2, IBM WebSphere Application Server, and IBM Security Guardium Key Lifecycle Manager, as shown in Figure 2-8. Click **Next**.

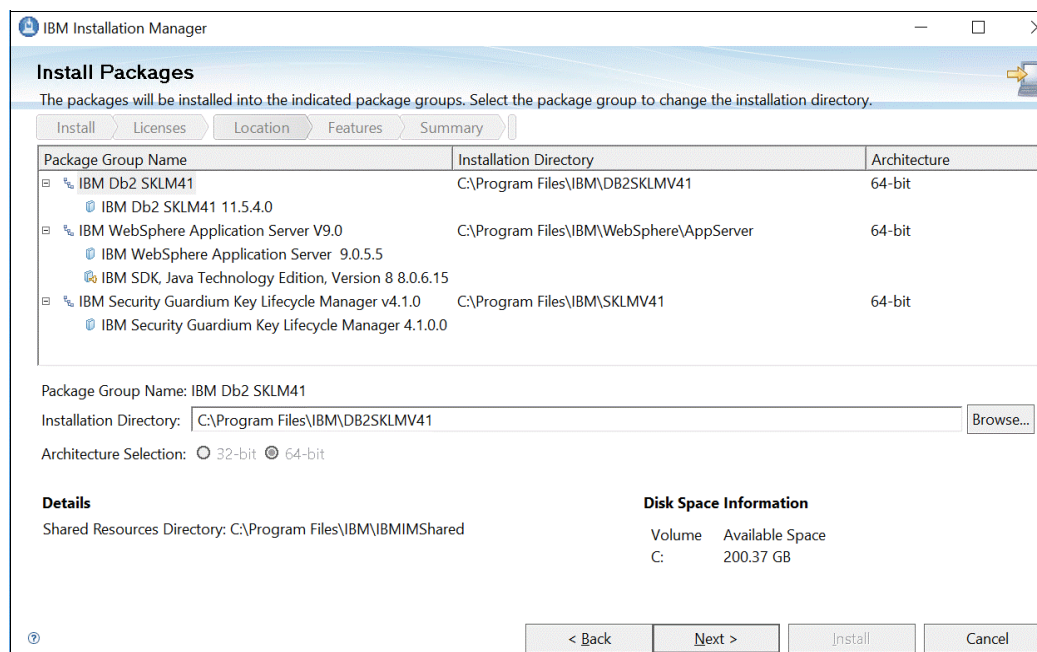


Figure 2-8 Db2 and WebSphere applications installation path

6. Click **Next** on the Translation selection page, as shown in Figure 2-9.

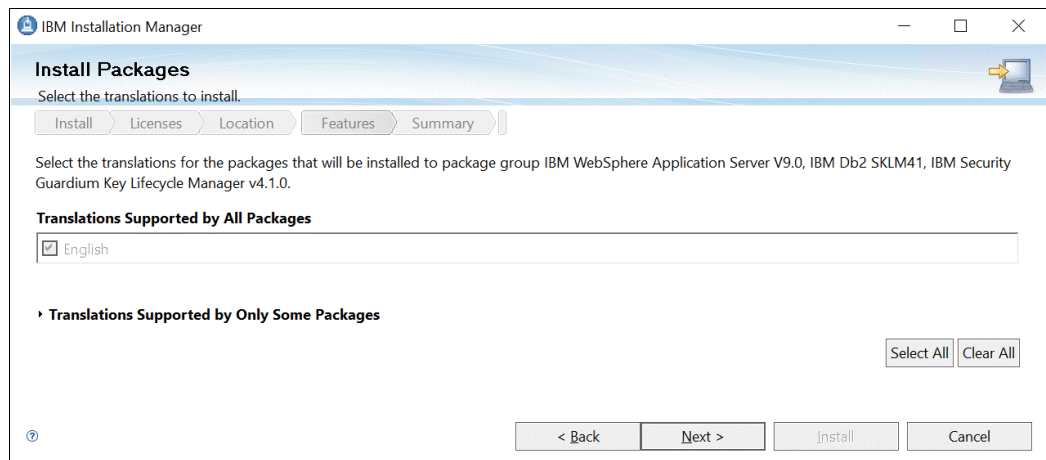


Figure 2-9 Translation packages

7. Confirm the packages to be installed, as shown in Figure 2-10. Click **Next**.

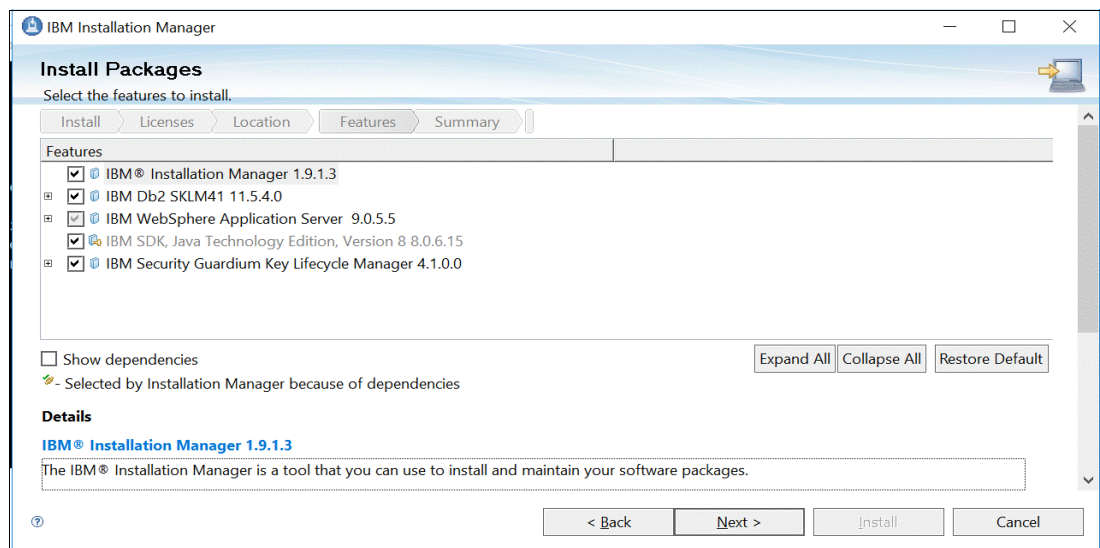


Figure 2-10 Confirm packages to be installed

8. Specify the credentials and home directory for the Db2 instance owner account and the Db2 port, as shown in Figure 2-11. If the specified Db2 Administrator ID does not exist, a user is created. Ensure to record credentials, Db2 port, and other information for future use. Click **Next**.

The screenshot shows the 'Install Packages' window in IBM Installation Manager. The 'Features' tab is selected, showing the configuration for 'IBM Db2 SKLM41 11.5.4.0'. The configuration includes a section for 'Database Configuration Details' with the following fields:

Db2 Administrator ID *	sklmdb41
Db2 Administrator Password *	*****
Confirm Password *	*****
Administrator/Database Home *	C:
Database Name *	SKLMD41
Db2 Port *	50070

Below the fields, a note states: 'Note: The Db2 Administrator user will run all the IBM Security Guardium Key Lifecycle Manager processes. For a domain user, specify the ID as DomainName\UserName or UserName@DomainName.'

Figure 2-11 Db2 instance owner account details

9. Specify the credentials for the IBM WebSphere Application Server administrator wasadmin account, WebSphere Application Server Port, IBM Security Guardium Key Lifecycle Manager administrator SKLMAdmin account, and the IBM Security Guardium Key Lifecycle Manager Ports, as shown in Figure 2-12. Ensure to record credentials and port information for future use. Click **Next**.

The screenshot shows the 'Install Packages' window in IBM Installation Manager. The 'Features' tab is selected, showing the configuration for 'IBM Security Guardium Key Lifecycle Manager 4.1.0.0'. The configuration includes two sections: 'Application Server Administration' and 'IBM Security Guardium Key Lifecycle Manager Application Administration'. The fields are as follows:

Application Server Administration		IBM Security Guardium Key Lifecycle Manager Application Administration	
User Name *	wasadmin	User Name *	SKLMAdmin
Password *	*****	Password *	*****
Confirm Password *	*****	Confirm Password *	*****
HTTPS Admin Port *	9083	HTTPS Port Number *	9443
		HTTP Port Number *	9080

Figure 2-12 WebSphere Application Server and GKLM users and ports

10. Do not select the Migrate Encryption Key Manager (EKM) option unless the installation is intended for a migration from EKM, as shown in Figure 2-13. Click **Next**.

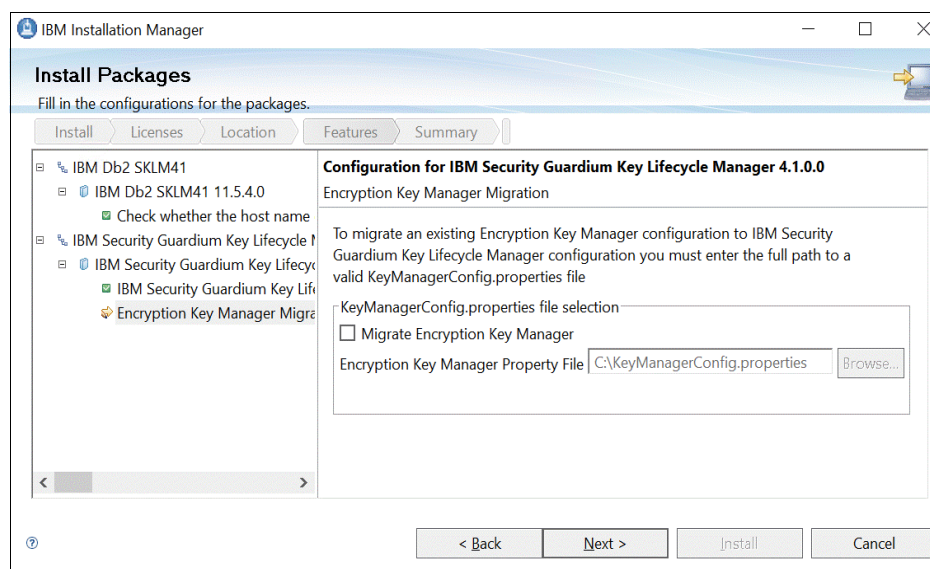


Figure 2-13 Clear the Migration Encryption Key Manager option

11. Review the installation summary and click **Install** to start the installation of IBM Security Guardium Key Lifecycle Manager, as shown in Figure 2-14.

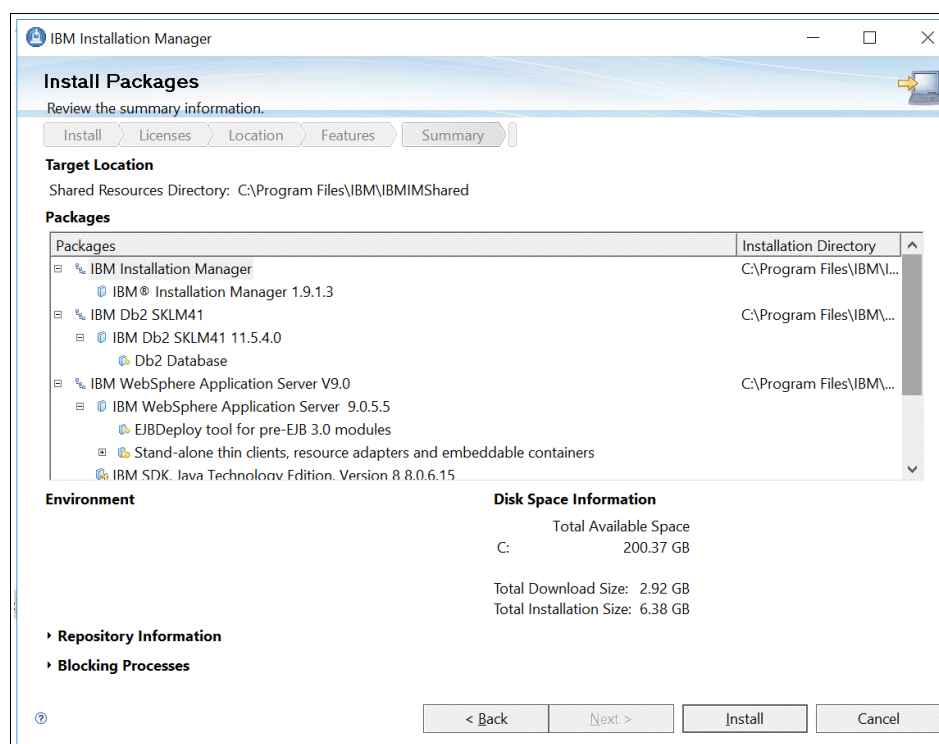


Figure 2-14 Installation summary information

12. After a successful installation, select **None** and then, click **Finish** to exit the installation wizard, as shown in Figure 2-15.

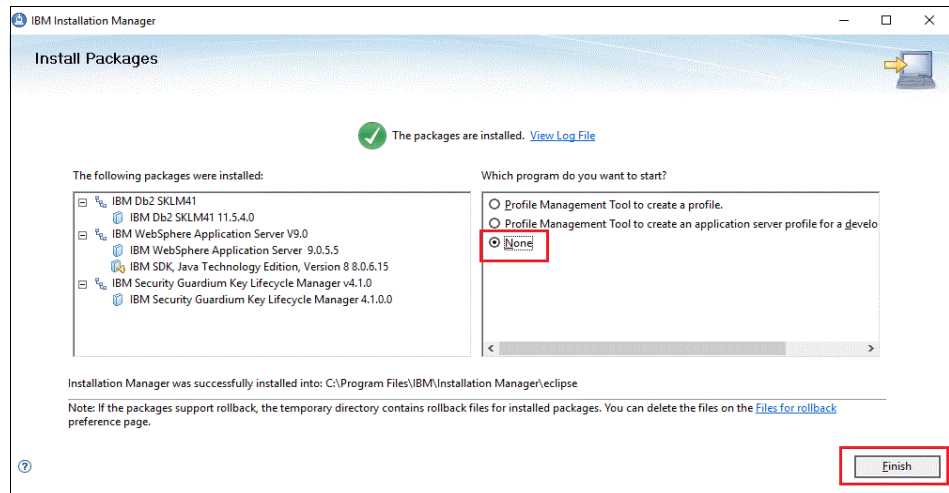


Figure 2-15 Installation Successful

2.3 Verifying successful installation

Complete the following steps to check for a successful installation:

1. Start a web browser.
2. Log in to IBM Security Guardium Key Lifecycle Manager (see Figure 2-16) by going to the following URL and using SKLMAdmin user and password set during the installation:
`https://<ip address/hostname>:<port>/ibm/SKLM/login.jsp`

Important: IBM Security Guardium Key Lifecycle Manager v4.1.0.1 uses port 9443 for GUI and REST APIs by default.



Figure 2-16 Login page

3. After logging in to IBM Security Guardium Key Lifecycle Manager GUI, the Welcome window is displayed, as shown in Figure 2-17

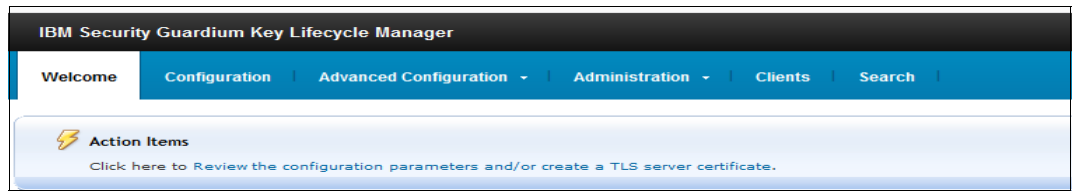


Figure 2-17 IBM Security Guardium Key Lifecycle Manager Welcome page

4. Click the question mark in the upper right corner and select the **About** option from the menu, as shown in Figure 2-18.

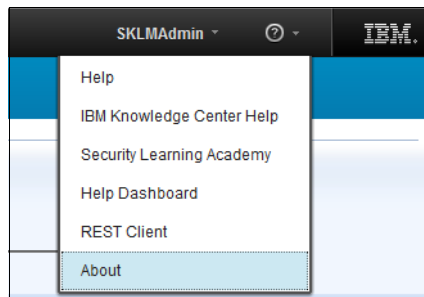


Figure 2-18 About menu

5. Verify the installed version of IBM Security Guardium Key Lifecycle Manager and its components, as shown in Figure 2-19.

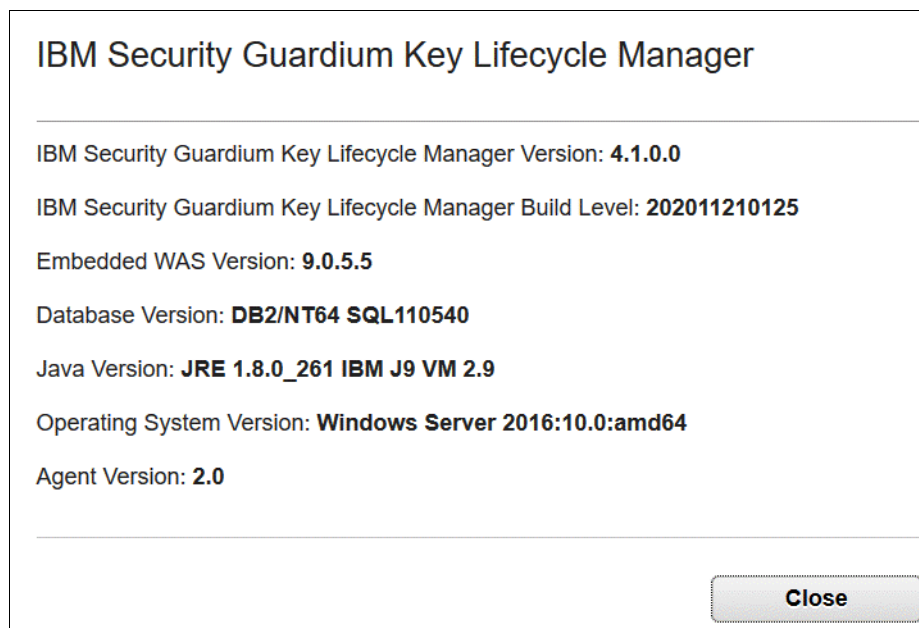


Figure 2-19 IBM Security Guardium Key Lifecycle Manager Version Information

2.4 Installing IBM Security Guardium Key Lifecycle Manager Traditional Edition in silent mode

You can install IBM Security Guardium Key Lifecycle Manager Traditional Edition on distributed platforms in silent mode by using the process that is outlined in this section. These steps are documented for Linux. However, similar steps can be used for AIX, Linux on Linux on IBM System z®, and Windows operating system after changing installation directories.

Complete the following steps:

1. Keep all the files of the installation package in a temporary directory on your system. Extract the files to same location so that post extraction disk1 and disk2 are in same folder, as shown in Example 2-1.

Example 2-1 Extracted folders from installation package

```
[root@testGKLM411 GKLM41GA]# tar -xvzf SGKLM_4.1_FOR_LINUX_SERVER_10F2.tar.gz
[root@testGKLM411 GKLM41GA]# tar -xvzf SGKLM_4.1_FOR_LINUX_SERVER_20F2.tar.gz
[root@testGKLM411 GKLM41GA]# ls -l
total 6739236
drwxr-xr-x 9 root root      4096 Nov 20 12:26 disk1
drwxr-xr-x 3 root root       35 Nov 20 12:23 disk2
-rw-r--r-- 1 root root 4245576797 May  8 08:21
SGKLM_4.1_FOR_LINUX_SERVER_10F2.tar.gz
-rw-r--r-- 1 root root 2655395262 May  8 08:23
SGKLM_4.1_FOR_LINUX_SERVER_20F2.tar.gz
```

2. After you extract the files, the installation script `silent_install.sh` is extracted to the disk1 directory, as shown in Example 2-2.

Example 2-2 Extracted installation files in disk1 directory

```
[root@testGKLM411 GKLM41GA]# ls -l disk1
total 104
drwxr-xr-x 6 root root   85 Nov 20 12:23 ad
-rwxr-xr-x 1 root root  170 Nov 20 12:17 diskTag.inf
drwxr-xr-x 2 root root   68 Nov 20 12:26 documentation
drwxr-xr-x 10 root root 4096 Nov 20 12:26 im
-rwxr-xr-x 1 root root 3026 Nov 20 12:25 install.sh
-rwxr-xr-x 1 root root 1995 Nov 20 12:25 launchpad.sh
drwxr-xr-x 4 root root   82 Nov 20 12:25 md
drwxr-xr-x 3 root root  180 Nov 20 12:26 prechecksripts
drwxr-xr-x 12 root root 4096 Nov 20 12:26 PRS
-rwxr-xr-x 1 root root 4286 Nov 20 12:25 silent_install.sh
-rwxr-xr-x 1 root root 1167 Nov 20 12:25 silent_install_withoutIM.sh
-rwxr-xr-x 1 root root 3604 Nov 20 12:25 silent_uninstallSKLM_linux.sh
-rwxr-xr-x 1 root root 6175 Nov 20 12:25 SKLM_Silent_Linux_Mig_25_Resp.xml
-rwxr-xr-x 1 root root 6175 Nov 20 12:25 SKLM_Silent_Linux_Mig_26_Resp.xml
-rwxr-xr-x 1 root root 6181 Nov 20 12:25 SKLM_Silent_Linux_Mig_27_Resp.xml
-rwxr-xr-x one root root 6257 Nov 20 12:25 SKLM_Silent_Linux_Mig_301_Resp.xml
-rwxr-xr-x 1 root root 6253 Nov 20 12:25 SKLM_Silent_Linux_Mig_30_Resp.xml
-rwxr-xr-x 1 root root 6254 Nov 20 12:25 SKLM_Silent_Linux_Mig_40_Resp.xml
-rwxr-xr-x 1 root root 5978 Nov 20 12:25 SKLM_Silent_Linux_Resp.xml
-rwxr-xr-x 1 root root  847 Nov 20 12:25 SKLM_Uninstall_Linux_Resp.xml
-rwxr-xr-x 1 root root  624 Nov 20 12:26 TKLMPasswdPolicy.xml
drwxr-xr-x 2 root root   23 Nov 20 12:25 toc
-rwxr-xr-x 1 root root 3514 Nov 20 12:25 uninstallSKLM_linux.sh
```

3. To perform a fresh installation, edit and update all the user inputs, such as repository location where installation binaries are present, installation directory, and user credentials, in the input response file SKLM_Silent_Linux_Resp.xml.

Note: Installation binaries bundle sample response files for performing a fresh installation and data migration from the installed version of IBM Security Guardium Key Lifecycle Manager. For a fresh installation, the sample response filename is SKLM_Silent_Linux_Resp.xml.

Complete the following steps:

- a. Create a backup copy of the sample response file SKLM_Silent_Linux_Resp.xml, as shown in Example 2-3.

Example 2-3 Backup Sample Response File

```
[root@testGKLM411 disk1]# cp SKLM_Silent_Linux_Resp.xml
SKLM_Silent_Linux_Resp.xml_backup
```

- b. Using any editor (for example, vi), open the response file SKLM_Silent_Linux_Resp.xml for editing, as shown in Example 2-4.

Example 2-4 Edit Sample Response File

```
[root@testGKLM411 disk1]# vi SKLM_Silent_Linux_Resp.xml
```

- c. Update the repository location to point to the local directory where the installation package was extracted in Step 1, as shown in Example 2-5.

Example 2-5 Update Repository Location

```
<server>
  <repository location='/Setups/GKLM41GA/disk1/im' />
  <repository location='/Setups/GKLM41GA/disk1' />
</server>
```

- d. Update the IBM Installation Manager installLocation to install IBM Installation Manager at specified location, as shown in Example 2-6.

Example 2-6 Update IM Installation Location

```
<profile id='IBM Installation Manager'
installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
  <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse' />
```

- e. Update the IBM Db2 location to install IBM Db2 database at specified location, as shown in Example 2-7.

Example 2-7 Update Db2 Installation Location

```
<profile id='IBM Db2 SKLM41' installLocation='/opt/IBM/DB2SKLMV41'>
  <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV41' />
```

- f. Update user.DB2_ADMIN_ID to specify username of the Db2 user that administers the Db2 database, as shown in Example 2-8. This user is an operating system-level user.

Example 2-8 Update Db2 Administrator ID

```
<data key='user.DB2_ADMIN_ID,com.ibm.sk1m41.db2.lin.ofng' value='sk1mdb41' />
```

- g. Update user.DB2_ADMIN_PWD and user.CONFIRM_PASSWORD to specify the password for the operating system level Db2 user that is specified in user.DB2_ADMIN_ID. The values are specified in encrypted format and values for user.DB2_ADMIN_PWD and user.CONFIRM_PASSWORD must match, as shown in Example 2-9.

Example 2-9 Update password for Db2 user in encrypted format

```
<data key='user.DB2_ADMIN_PWD,com.ibm.sk1m41.db2.lin.ofng'
value='QTh/0AiFvr1jhs9gn0YkGA==' />
  <data key='user.CONFIRM_PASSWORD,com.ibm.sk1m41.db2.lin.ofng'
value='QTh/0AiFvr1jhs9gn0YkGA==' />
```

Important: The plain-text password for Db2 Administrator user must meet the operating system password complexity requirements. If this requirement is not met, the installation for IBM Security Guardium Key Lifecycle Manager fails.

- h. To convert password from plain-text to encrypted format that is acceptable for IBM Installation manager, use the imcl utility that is provided under the im/tools folder, as shown in Example 2-10.

Example 2-10 Using imcl utility to get encrypted password

```
[root@testGKLM411 tools]# ./imcl encryptString SKLM@db2
QTh/0AiFvr1jhs9gn0YkGA==
[root@testGKLM411 tools]#
```

- i. Update the home directory of the IBM Db2 user that is specified in Step f, as shown in Example 2-11.

Example 2-11 Update home directory of Db2 user

```
<data key='user.DB2_DB_HOME,com.ibm.sk1m41.db2.lin.ofng'
value='/home/sk1mdb41' />
```

- j. Update the value of the database name, as shown in Example 2-12.

Example 2-12 Update Db2 database name

```
<data key='user.DB2_DB_NAME,com.ibm.sk1m41.db2.lin.ofng' value='SKLMDB41' />
```

- k. Update the value of the database port, as shown in Example 2-13.

Example 2-13 Update Db2 database port

```
<data key='user.DB2_DB_PORT,com.ibm.sk1m41.db2.lin.ofng' value='50070' />
```

- l. Update the value for DB2_LOCATION to the installation location for Db2 database, as shown in Example 2-14. Ensure that this value is same as value for parameter IBM Db2 location that was specified in Step e.

Example 2-14 Update Db2 Install Location

```
<data key='user.DB2_LOCATION,com.ibm.sk1m41.db2.lin.ofng'
value='/opt/IBM/DB2SKLMV41' />
```

- m. Update the value for DB2_DB_LHOME to the home location for Db2 database user, as shown in Example 2-15. Ensure that this value is same as value for parameter DB2_DB_HOME location that was specified in Step i.

Example 2-15 Update DB2_DB_LHOME

```
<data key='user.DB2_DB_LHOME,com.ibm.sk1m41.db2.lin.ofng' value='/home/sk1mdb41' />
```

- n. Update the value of the user group under which the Db2 user is to be created. The group name cannot be longer than 8 characters, as shown in Example 2-16.

Example 2-16 Update Db2 admin user group

```
<data key='user.DB2_ADMIN_GRP,com.ibm.sk1m41.db2.lin.ofng' value='sk1mdb41' />
```

Tip: Parameter user.DB2_ADMIN_GRP is not applicable for Windows operating system.

- o. Update the installation location for IBM WebSphere Application Server to install IBM WebSphere Application Server at the specified location, as shown in Example 2-17.

Example 2-17 Update IM Installation Location

```
<profile id='IBM WebSphere Application Server V9.0'
installLocation='/opt/IBM/WebSphere/AppServer'>
  <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer' />
```

- p. Update the installation location for IBM Security Guardium Key Lifecycle Manager to install GKLM at a specified location, as shown in Example 2-18.

Example 2-18 Update GKLM Installation Location

```
<profile id='IBM Security Guardium Key Lifecycle Manager v4.1.0'
installLocation='/opt/IBM/SKLMV41'>
  <data key='eclipseLocation' value='/opt/IBM/SKLMV41' />
```

- q. Update user.WAS_ADMIN_ID to specify username of the WebSphere Application Server Administrator user, which administers the WebSphere Application Server, as shown in Example 2-19.

Example 2-19 Update WebSphere Application Server Administrator ID

```
<data key='user.WAS_ADMIN_ID,com.ibm.sk1m41.linux' value='wasadmin' />
```

- r. Update user.WAS_ADMIN_PASSWORD and user.WAS_ADMIN_CONF_PWD to specify the password of the WebSphere Application Server user that was specified in user.WAS_ADMIN_ID. The values are specified in encrypted format and values for user.WAS_ADMIN_PASSWORD and user.WAS_ADMIN_CONF_PWD must match, as shown in Example 2-20.

Example 2-20 Update password for WebSphere Application Server Administrator user in encrypted format

```
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sk1m41.linux'
value='e9PjN93MeQxwnSs9VXJFMw==' />
  <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sk1m41.linux'
value='e9PjN93MeQxwnSs9VXJFMw==' />
```

- s. Update user.SKLM_ADMIN_USER to specify username of the IBM Security Guardium Key Lifecycle Manager Administrator user that administers the GKLM, as shown in Example 2-21.

Example 2-21 Update GKLM Administrator User

```
<data key='user.SKLM_ADMIN_USER,com.ibm.sk1m41.linux' value='SKLMAdmin' />
```

- t. Update user.SKLM_ADMIN_PASSWORD and user.SKLM_ADMIN_CONF_PWD to specify password of the GKLM user that was specified in user.SKLM_ADMIN_USER. The values are specified in encrypted format and values for user.SKLM_ADMIN_PASSWORD and user.SKLM_ADMIN_CONF_PWD must match, as shown in Example 2-22.

Example 2-22 Update password for user in encrypted format

```
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sk1m41.linux'
value='9YTRJMRIydDSdfhaHPs1ag==' />
  <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sk1m41.linux'
value='9YTRJMRIydDSdfhaHPs1ag==' />
```

- u. Update the value of the GKLM Application port on which GKLM listens for requests on a secure channel, as shown in Example 2-23.

Example 2-23 Update GKLM Application secure listening port

```
<data key='user.SKLM_APP_PORT,com.ibm.sk1m41.linux' value='9443' />
```

- v. Update the value of the WebSphere Application Server Administrator port on which WebSphere Application Server listens for requests on a secure channel. Users can access the WebSphere Application Server GUI console by connecting to this port, as shown in Example 2-24.

Example 2-24 Update WebSphere Application Server Administrator secure listening port

```
<data key='user.WAS_ADMIN_PORT,com.ibm.sk1m41.linux' value='9083' />
```

- w. Update the value of the GKLM Application port on which GKLM listens for requests on a non-secure channel, as shown in Example 2-25.

Example 2-25 Update GKLM Application unsecured listening port

```
<data key='user.SKLM_APP_NS_PORT,com.ibm.sk1m41.linux' value='9080' />
```

- x. Save all the changes and close the file.
4. At the command prompt, run the command that is shown in Example 2-26 to perform silent installation.

Example 2-26 Perform Silent installation

```
[root@testGKLM411 disk1]# ./silent_install.sh SKLM_Silent_Linux_Resp.xml
-acceptLicense
```

5. GKLM installer starts the installation, beginning with running prerequisite checker. If all of the prerequisites are met, it continues with the installation of GKLM (see Example 2-27).

The Installation process might display a warning message before showing a final success message. This warning message is related to the 64-bit version of Installation Manager not being supported. This known issue can be safely ignored.

Example 2-27 Installation Console Output - All prerequisites are met

```
[root@sklm41gal disk1]# ./silent_install.sh SKLM_Silent_Linux_Resp.xml
-acceptLicense
No preinstalled IBM Installation Manager found on the system.
Installing IBM Security Guardium Key Lifecycle Manager v4.1.0
Sun May 16 09:06:15 PDT 2021 - SKLM Prerequisite check started.
Db2 prerequisite check - PASSED.
Checking required shell - PASSED
Checking required memory - PASSED
Checking executable permissions - PASSED
Checking kernel parameters - PASSED
Checking SELinux - PASSED
Checking CPU speed - PASSED
Sun May 16 09:06:15 PDT 2021 - SKLM Prerequisite check - PASSED .
check /tmp/SKLMPreqCheck.log for more details.
Installed com.ibm.cic.agent_1.9.1003.20200730_2125 to the
/opt/IBM/InstallationManager/eclipse directory.
Installed com.ibm.sklm41.db2.lin.ofng_11.5.4.0 to the /opt/IBM/DB2SKLMV41
directory.
Installed com.ibm.websphere.BASE.v90_9.0.5005.20200807_2041 to the
/opt/IBM/WebSphere/AppServer directory.
Installed com.ibm.java.jdk.v8_8.0.6015.20200725_0800 to the
/opt/IBM/WebSphere/AppServer directory.
Installed com.ibm.sklm41.linux_4.1.0.00 to the /opt/IBM/SKLMV41 directory.
CRIMA1137W WARNING: The following packages do not support the 64-bit version of
Installation Manager that you are using: IBM Db2 SKLM41 version 11.5.4.0, IBM
Security Guardium Key Lifecycle Manager version 4.1.0.0. If you continue, you
might have issues with installation and deployment. For information about 64-bit
mode support for a package, see the package documentation.
```

Explanation: The 64-bit version of Installation Manager checks each package for 64-bit support. If a package does not support the 64-bit version, you receive a warning.

User Action: Use a 32-bit version of Installation Manager to install the package. **Installation process is complete. Please look into Installation Manager logs for details.**

```
[root@sklm41gal disk1]#
```

If any prerequisite is not met but is not a mandatory prerequisite (for example, Db2 kernel settings), it displays a warning and prompts the user for input before continuing with the installation, as shown in Example 2-28.

Example 2-28 Installation Console Output: Prerequisite not met

```
[root@testGKLM411 disk1]# ./silent_install.sh SKLM_Silent_Linux_Resp.xml
-acceptLicense
No preinstalled IBM Installation Manager found on the system.
Installing IBM Security Guardium Key Lifecycle Manager v4.1.0
```

```
Fri May 14 02:44:36 PDT 2021 - SKLM Prerequisite check started.
Db2 prerequisite check - PASSED.
Checking required shell - PASSED
Checking required memory - PASSED
Checking executable permissions - PASSED
Checking kernel parameters - WARNING
Checking SELinux - PASSED
Checking CPU speed - PASSED
Fri May 14 02:44:37 PDT 2021 - SKLM Prerequisite check - PASSED with WARNING.
The Prerequisite check passed with one or more warnings. Review the warning
details in /tmp/SKLMPreqCheck.log. Press any key to continue.
```

For more information about verifying a successful installation, see 2.3, “Verifying successful installation” on page 13.

2.5 Installing fix pack for IBM Security Guardium Key Lifecycle Manager Traditional Edition

The [IBM Fix Central website](#) provides fixes and updates for the software, hardware, and operating system, including IBM Security Guardium Key Lifecycle Manager fix packs.

The following section describes how to install fix pack FP0001 over IBM Security Guardium Key Lifecycle Manager V4.1.0.0.

Note: Make sure to back up the current WebSphere Application Server and IBM Security Guardium Key Lifecycle Manager configuration before installing the fix pack. For more information about the backup and restore process for the IBM Security Guardium Key Lifecycle Manager configuration, see Chapter 5.2, “Backing up and restoring IBM Security Guardium Key Lifecycle Manager” on page 67.

To install the fix pack for IBM Security Guardium Key Lifecycle Manager, complete the following steps:

1. Back up the WebSphere Application Server files, as shown in Example 2-29.

Example 2-29 Backing up the WebSphere Application Server files

```
C:\>cd "%Program Files\IBM\WebSphere%"
C:\Program Files\IBM\WebSphere>AppServer\bin\stopServer.bat server1
ADMU0116I: Tool information is being logged in file C:\Program

Files\IBM\WebSphere\AppServer\profiles\KLMPProfile\logs\server1\stopServer.log
ADMU7702I: Because server1 is registered to run as a Windows Service, the
          request to stop this server will be completed by stopping the
          associated Windows Service.
ADMU0116I: Tool information is being logged in file C:\Program

Files\IBM\WebSphere\AppServer\profiles\KLMPProfile\logs\server1\stopServer.log
ADMU0128I: Starting tool with the KLMPProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.
```

```
C:\Program Files\IBM\WebSphere>AppServer\java\8.0\bin\jar -cvfM AppServer.zip
AppServer
```

NOTE: It will take sometime to create compressed file by using above command.

```
C:\Program Files\IBM\WebSphere>AppServer\bin\startServer.bat server1
```

```
ADMU0116I: Tool information is being logged in file C:\Program
```

```
Files\IBM\WebSphere\AppServer\profiles\KLMPProfile\logs\server1\startServer.log
```

```
ADMU7701I: Because server1 is registered to run as a Windows Service, the
           request to start this server will be completed by starting the
           associated Windows Service.
```

```
ADMU0116I: Tool information is being logged in file C:\Program
```

```
Files\IBM\WebSphere\AppServer\profiles\KLMPProfile\logs\server1\startServer.log
```

```
ADMU0128I: Starting tool with the KLMPProfile profile
```

```
ADMU3100I: Reading configuration for server: server1
```

```
ADMU3200I: Server launched. Waiting for initialization status.
```

```
ADMU3000I: Server server1 open for e-business; process id is 4572
```

-
2. Create the C:\sklminstall_fp directory, transfer the fix pack package that was downloaded from [IBM Fix Central](#) to the folder. Extract the fix pack package and run the **updateSKLM.bat** script to start the update wizard (the script requires executable permission), as shown in Example 2-30.

Example 2-30 Preparing for the fix pack installation

```
C:\sklminstall_fp>dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 62B7-12D0
```

```
Directory of C:\sklminstall_fp
```

```
05/10/2021  07:20 AM    <DIR>          .
05/10/2021  07:20 AM    <DIR>          ..
03/26/2021  08:52 AM                4,760 silent_updateSKLM.bat
03/26/2021  08:52 AM    <DIR>          skl
03/26/2021  08:52 AM                842 SKLM_Uninstall_Win_Resp.xml
03/26/2021  08:52 AM                4,719 updateSKLM.bat
03/26/2021  08:52 AM                382 updateSKLM.xml
               4 File(s)              10,703 bytes
               3 Dir(s)  210,361,110,528 bytes free
```

```
C:\sklminstall_fp>updateSKLM.bat "C:\Program Files\IBM\Installation Manager"
```

```
"C:\Program Files\IBM\WebSphere\AppServer" wasadmin wasadmin_password
```

```
Adding service
```

```
About to install FixPack...
```

```
Stopping SKLM Server...
```

```
"C:\Program Files\IBM\WebSphere\AppServer"\bin\stopServer.bat server1 -profileName
```

```
KLMPProfile -username wasadmin -password *****
```

```
ADMU0116I: Tool information is being logged in file C:\Program
```

```
Files\IBM\WebSphere\AppServer\profiles\KLMPProfile\logs\server1\stopServer.log
```

```
ADMU0128I: Starting tool with the KLMPProfile profile
```

```
ADMU3100I: Reading configuration for server: server1
```

```
ADMU3201I: Server stop request issued. Waiting for stop status.
```


ADMU4000I: Server server1 stop completed.

Launching InstallManager...

```
"C:\Program Files\IBM\Installation Manager"\eclipse\IBMIM.exe -input  
C:\sklinstall_fp\updateSKLM.xml
```

3. The wizard identifies the current installed version and fix pack level. Select **IBM Security Guardium Key Lifecycle Manager V4.1.0** and then, click **Next**, as shown in Figure 2-20.

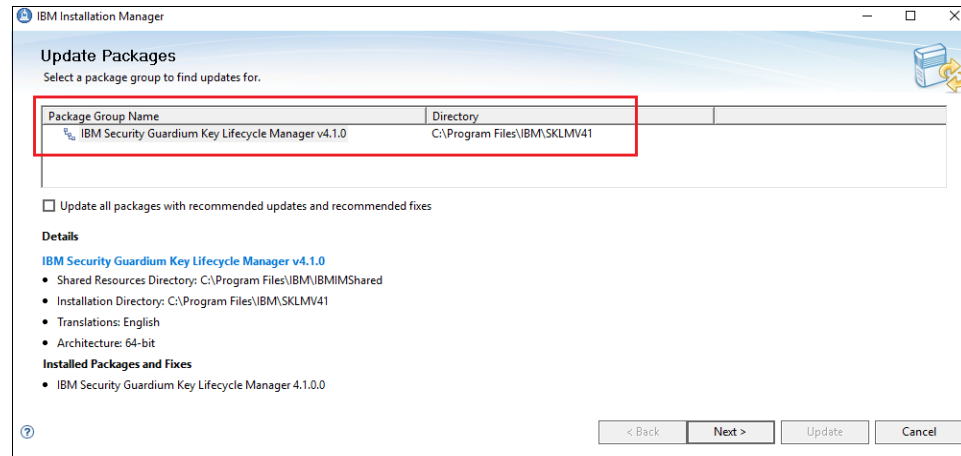


Figure 2-20 Package group to be updated

4. Select the fix pack to be installed and click **Next**, as shown in Figure 2-21.

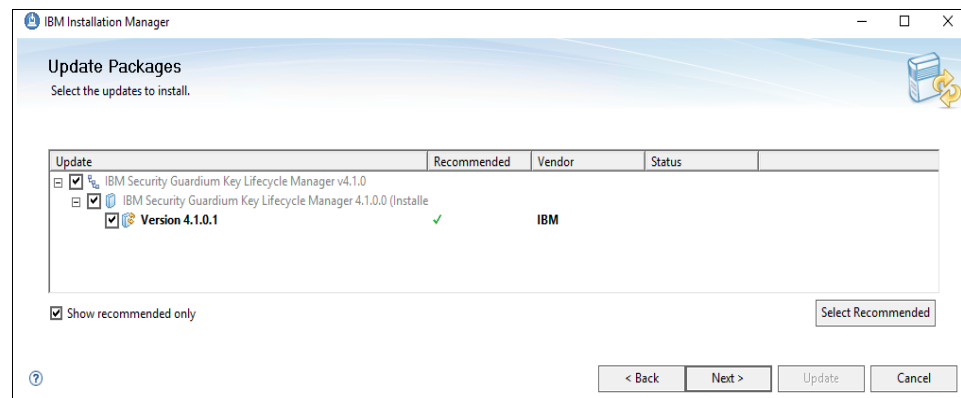


Figure 2-21 Fix pack to be installed

5. Review and accept the terms in the license agreement and click **Next**, as shown in Figure 2-22.

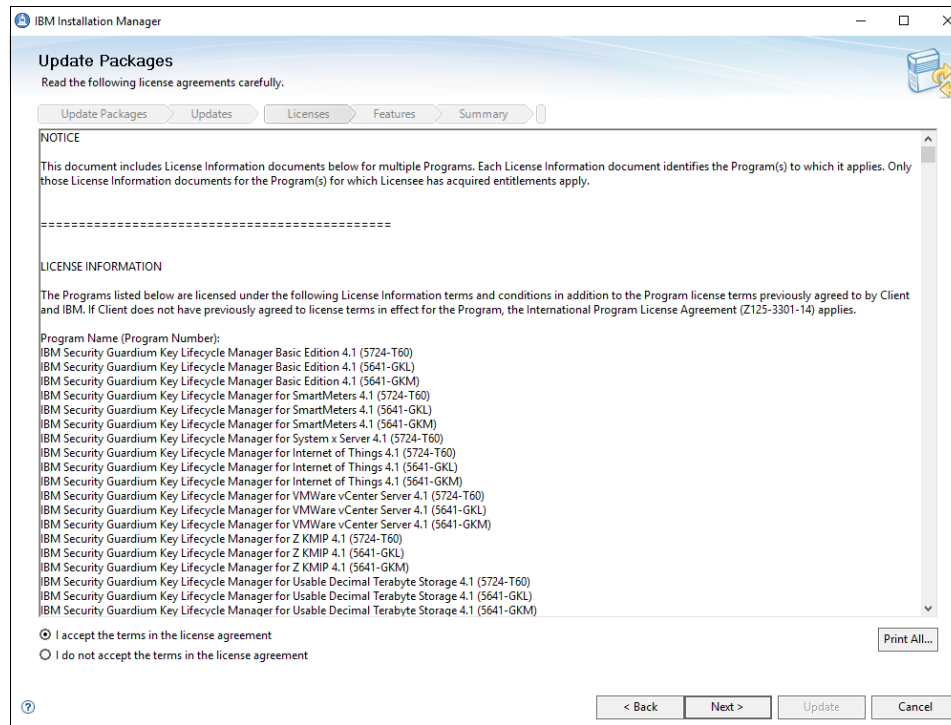


Figure 2-22 License agreements

6. Select the features to be installed and click **Next**, as shown in Figure 2-23.

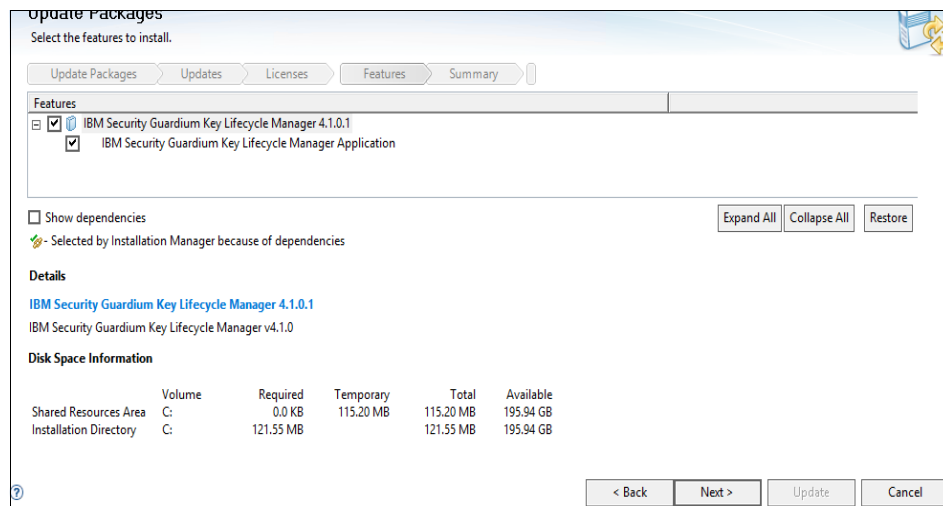


Figure 2-23 Features to be installed

7. Enter the passwords for the wasadmin, SKLAdmin, and sklmb41 accounts. Then, click **Validate Credentials**, as shown in Figure 2-24.

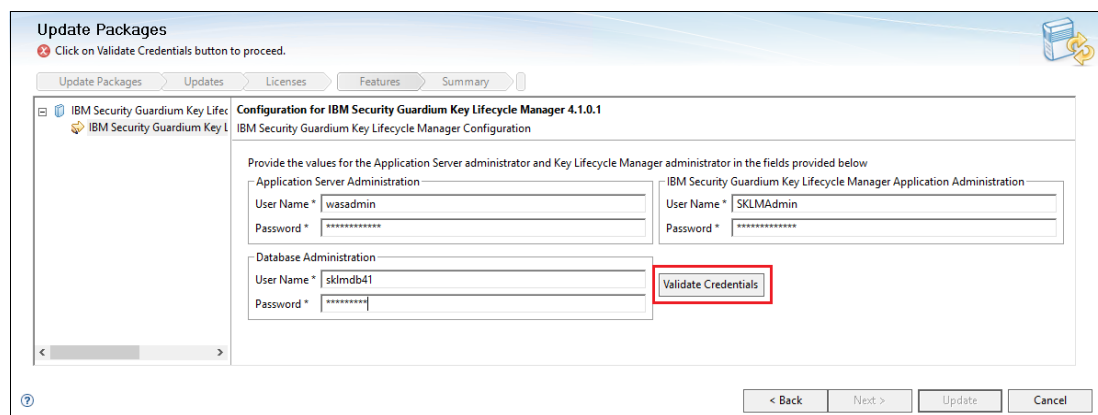


Figure 2-24 Validate Credentials window

8. When the passwords are validated successfully, the Next button becomes active. Click **Next**, as shown in Figure 2-25.

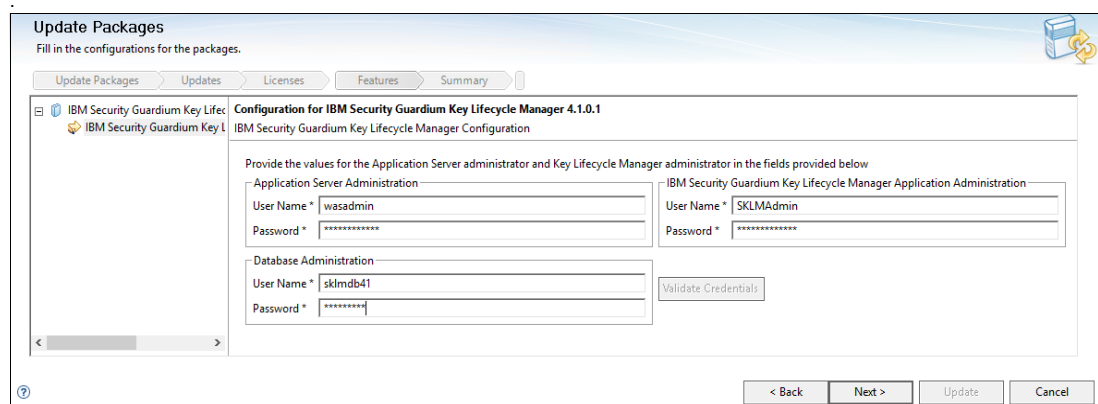


Figure 2-25 Validate Credentials window

9. Confirm the installation details and click **Update** to install the fix pack, as shown in Figure 2-26.

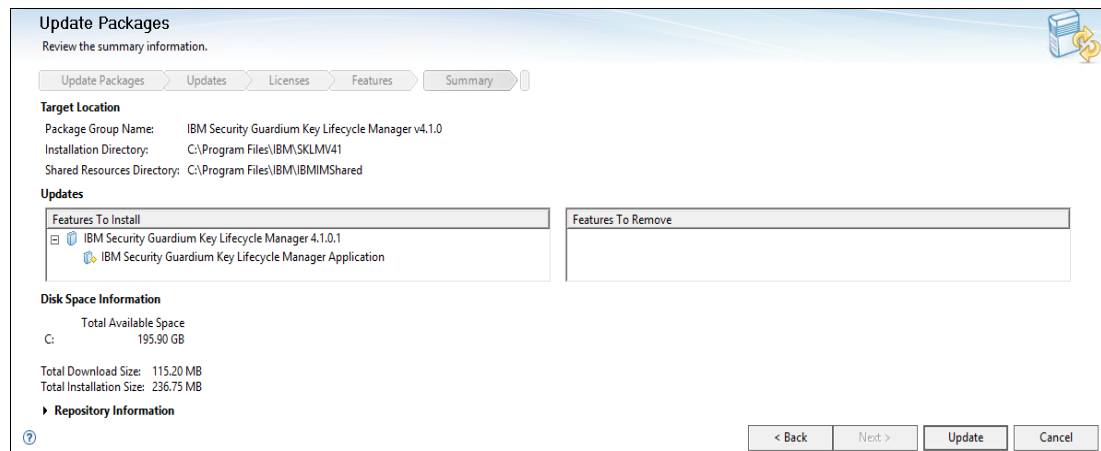


Figure 2-26 Pre-Installation details

10. After a successful installation, review the installation summary and click **Finish** to exit the wizard, as shown in Figure 2-27.

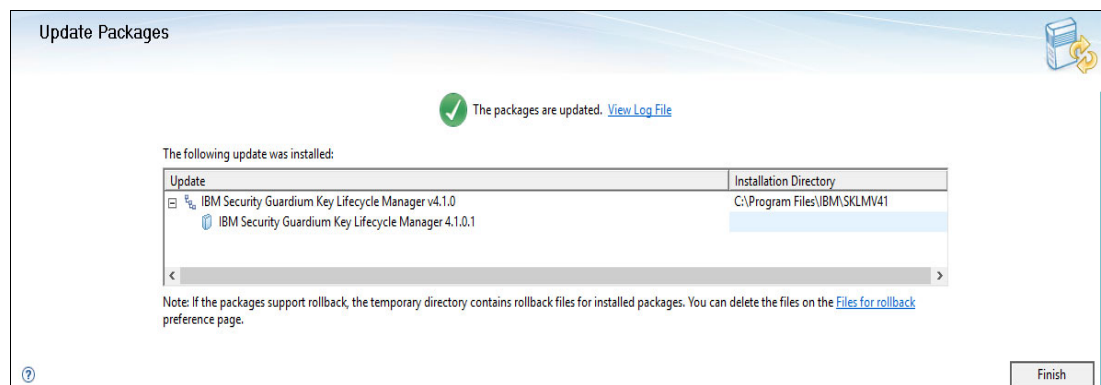


Figure 2-27 Fixpack installation successful

11. Log in to the IBM Security Guardium Key Lifecycle Manager GUI and click the question mark in the upper right corner. Then, select **About** to verify the installed software details, as shown in Figure 2-28.

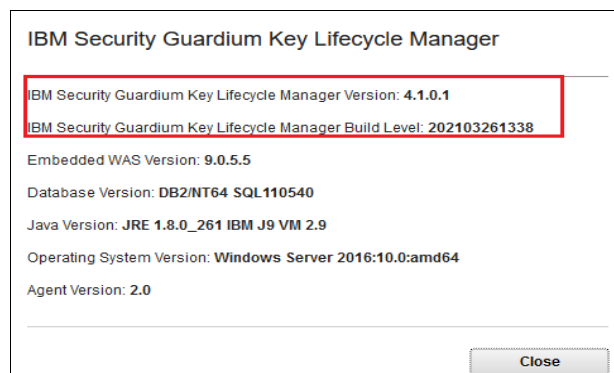


Figure 2-28 IBM Security Guardium Key Lifecycle Manager version information



Installing Container Edition

This chapter describes the tasks that are associated with the initial installation of IBM Security Guardium Key Lifecycle Manager v4.1.0.1 for Container Edition and fix packs.

This chapter includes the following topics:

- ▶ 3.1, “Deployment prerequisites” on page 28
- ▶ 3.2, “Installing IBM Security Guardium Key Lifecycle Manager on Red Hat OpenShift” on page 29
- ▶ 3.3, “Installing IBM Security Guardium Key Lifecycle Manager Container Edition on Kubernetes” on page 41
- ▶ 3.4, “Installing IBM Security Guardium Key Lifecycle Manager Container Edition on IBM z/OS Container Extensions” on page 44

3.1 Deployment prerequisites

Complete the following steps before you deploy IBM Security Guardium Key Lifecycle Manager in a Red Hat OpenShift Container platform:

1. Obtain the container installation files (elmages) and license activation file:
 - a. Obtain the container installation files (elmages) and license activation file for IBM Security Guardium Key Lifecycle Manager container from [IBM Passport Advantage](#). The user should download following files:
 - License File: SGKLM_4.1_CONTAINER_LICENSE_MP.zip
 - Container image for x86-64 platform: SGKLM_4.1_CONTAINER_LIC_LN64_BIT.tar
- Tip:** You can avoid downloading the container installation files if you plan to pull the container image directly from the [Docker Hub](#) repository.
- b. Extract the container installation files and openshift-helm.zip/k8s-helm.zip file to a local repository directory. You must provide the location of this directory in the values.yaml file in the chart.
2. Install IBM License Service:
 - a. Install the IBM License Service. For more information, see the relevant section in https://ibm.biz/license_service4containers.
 - b. Verify the installation by running the commands that are shown in Example 3-1. Note down the host, port, and service token values from the command output to be updated in the Helm charts file.

Example 3-1 Commands to verify license server

Red Hat OpenShift commands

```
# oc get pods --namespace ibm-common-services
# oc get service --namespace ibm-common-services
# oc get secret ibm-licensing-token -o jsonpath={.data.token} -n
ibm-common-services | base64 -d
```

Kubernetes commands

```
# kubectl get pods --namespace ibm-common-services
# kubectl get service --namespace ibm-common-services
# kubectl get secret ibm-licensing-token -o jsonpath={.data.token} -n
ibm-common-services | base64 -d
```

- c. Update the following parameters in the values.yaml that is bundled with sample Helm charts (openshift-helm.zip / k8s-helm.zip), as shown in Example 3-2.

Example 3-2 Parameter to be updated in values.yaml

```
config:
sklmapp_license:
license_service_host
license_service_port
secret:
license_service_token
```

3.2 Installing IBM Security Guardium Key Lifecycle Manager on Red Hat OpenShift

To install IBM Security Guardium Key Lifecycle Manager on Red Hat OpenShift, complete the following steps:

1. Install a Red Hat OpenShift Container Platform cluster.
 - a. Obtain Red Hat OpenShift Container Platform Version 4.2 or later.
 - b. Review the minimum system requirements. For more information, see the [Support Matrix](#).
 - c. Install an OpenShift Container Platform cluster, and ensure that it is up and running. For more information, see [Red Hat OpenShift Documentation](#).
 - d. Configure the persistent volume storage.

2. Obtain the Red Hat OpenShift Command line (CLI) tool.

Obtain the `oc` command line tool per the version of Red Hat OpenShift container platform and your operating system. For more information, see [Getting started CLI](#).

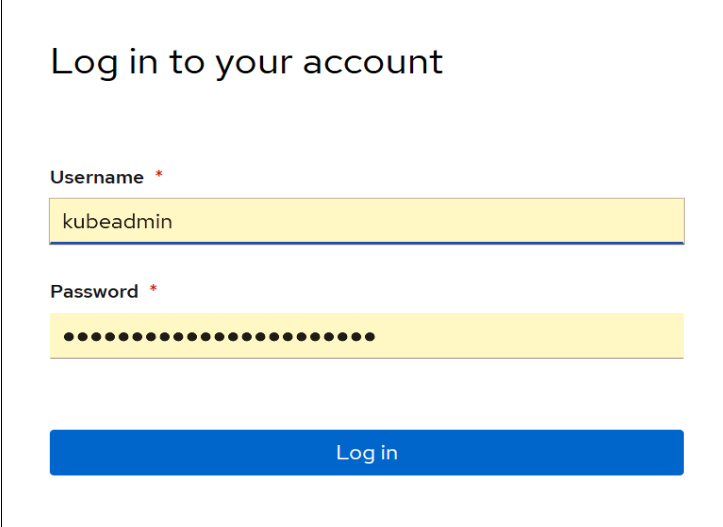
3. Obtain the Helm charts.

Install Helm Version 2.17.0 on the system from which you access the cluster. For more information, see [Helm Install](#).

3.2.1 Installing IBM Security Guardium Key Lifecycle Manager Container Edition on Red Hat OpenShift with PostgreSQL

Complete the following steps to install IBM Security Guardium Key Lifecycle Manager container on Red Hat OpenShift with PostgreSQL. Make sure that the PostgreSQL database is deployed and postgresQL pods are running:

1. Obtain the log-in token:
 - a. Log in to the Red Hat OpenShift Container Platform by using the `kubeadmin` credentials, as shown in Figure 3-1.



Log in to your account

Username *

kubeadmin

Password *

.....

Log in

Figure 3-1 Login to OCP cluster

- b. Click the **Copy Login Command** option, as shown in Figure 3-2.

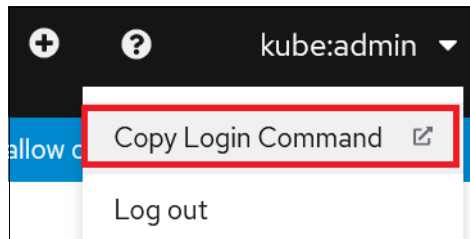


Figure 3-2 Copy Login Command

- c. Click **Display Token** (see Figure 3-3).

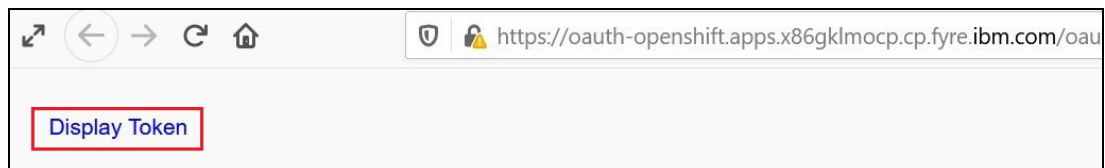


Figure 3-3 Display Token link

- d. Copy the log in command that is displayed in the Log in with this token section, as shown in Figure 3-4.



Figure 3-4 Login command

- e. Use the copied command to log in to the OCP server by using the command line tool (**oc**), as shown in Example 3-3.

Example 3-3 Login to OpenShift Container Platform cluster with OC command line tool

```
oc login --token=sha256~za6Se4Lpj5YI7-1Ikt2n_APVHqH7sE_i2NoQV4nQXhY
--server=https://api.xgklmcp.cp.fyre.ibm.com:6443
```

Logged into "https://api.xgklmcp.cp.fyre.ibm.com:6443" as "kube:admin" using the token provided.

You have access to 60 projects, the list has been suppressed. You can list all projects with 'oc projects'

Using project "sklm".

2. Browse to the openshift-helm directory and apply the Security Context Constraint (SCC) by using the command that is shown in Example 3-4.

Example 3-4 Apply WebSphere Liberty security context

```
c:\>oc apply -f liberty_scc.yaml
securitycontextconstraints.security.openshift.io/ibm-websphere-scc configured
```

3. Create the WebSphere service account and bind the ibm-websphere-scc to the namespace (project) sklm, as shown in Example 3-5.

Example 3-5 Create WebSphere service account

```
c:\>oc create serviceaccount websphere -namespace sklm
serviceaccount/websphere created

c:\>oc adm policy add-scc-to-user ibm-websphere-scc -z websphere -namespace sklm
securitycontextconstraints.security.openshift.io/ibm-websphere-scc added to:
["system:serviceaccount:sklm:websphere"]
```

4. Update the values.yaml file and modify the parameter values in the file according to your requirements.
5. Run the **helm install** command, as shown in Example 3-6.

Example 3-6 Helm install command

```
c:\>helm install sklmapp sklmapp
NAME: sklmapp
LAST DEPLOYED: Sat May 8 12:48:00 2021
NAMESPACE: sklm
STATUS: deployed
REVISION: 1
TEST SUITE: None
```

6. Verify the installation:
 - a. Log in to the Red Hat OpenShift Container Platform.
 - b. In the left window, click **Workloads** → **Pods**. A new pod for the application is created with the status as Running, as shown in Figure 3-5.

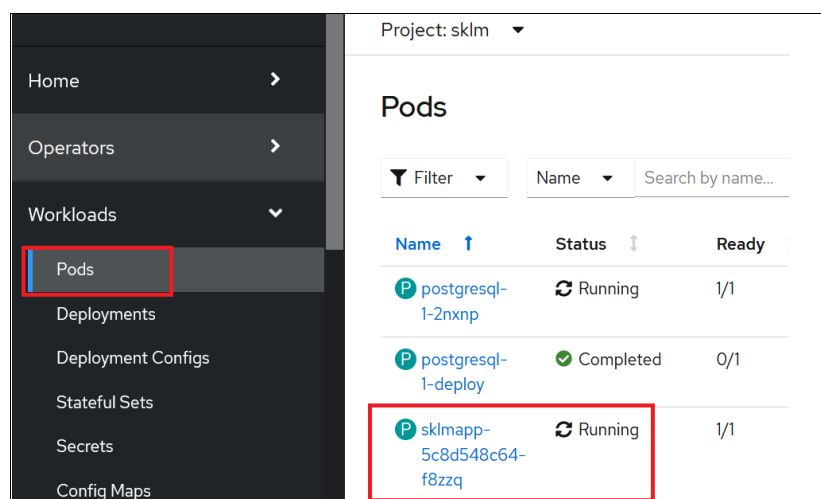


Figure 3-5 Verifying GKLM installation

7. To access the application, create a route:
 - a. In the left window, click **Networking** → **Routes**. Then, click **Create Route**, as shown in Figure 3-6.



Figure 3-6 Create Route

- b. Enter the suitable values for the route Name (for example, sklm-route), as shown in Figure 3-7.

The screenshot shows the 'Create Route' form. At the top, it says 'Project: sklm' with a dropdown arrow. Below this is the title 'Create Route' and a description: 'Routing is a way to make your application publicly visible.' The form has three main sections: 'Name *' with a text input field containing 'sklm-route' (highlighted with a red box), 'Hostname' with a text input field containing 'www.example.com', and 'Path' with a text input field containing '/'. Below the 'Path' field is a description: 'Path that the router watches to route traffic to the service.'

Figure 3-7 Specifying route name

- c. Select the Service, Target Port, Security as enabled and TLS_Termination as Passthrough, as shown in Figure 3-8.

Service *

sklmapp

Service to route to.

+ Add Alternate Service

Target Port *

9443 → 9443 (TCP)

Target port for traffic.

Security

☒ Secure route

Routes can be secured using several TLS termination types for serving certificates.

TLS Termination *

Passthrough

Figure 3-8 Specify Route details

- d. Specify the Insecure Traffic as Redirect and click **Create**, as shown in Figure 3-9.

Insecure Traffic

Redirect

Policy for traffic on insecure schemes like HTTP.

Create Cancel

Figure 3-9 Specify Insecure Traffic mode for Route

3.2.2 Activating the license and logging in to IBM Security Guardium Key Lifecycle Manager

Complete the following steps:

1. Open a web browser.
2. Log in to IBM Security Guardium Key Lifecycle Manager at the following URL and by using the SKLMAdmin user and password that was set during the installation process:
`https://<ip address/hostname>:<port>/ibm/SKLM/login.jsp`

Note: Use the port number in the URL, which is mapped in the Route details, as shown in Figure 3-8 on page 33.

3. In the Configuration page that appears, select **I accept the terms in the License Agreements** option, as shown in Figure 3-10.

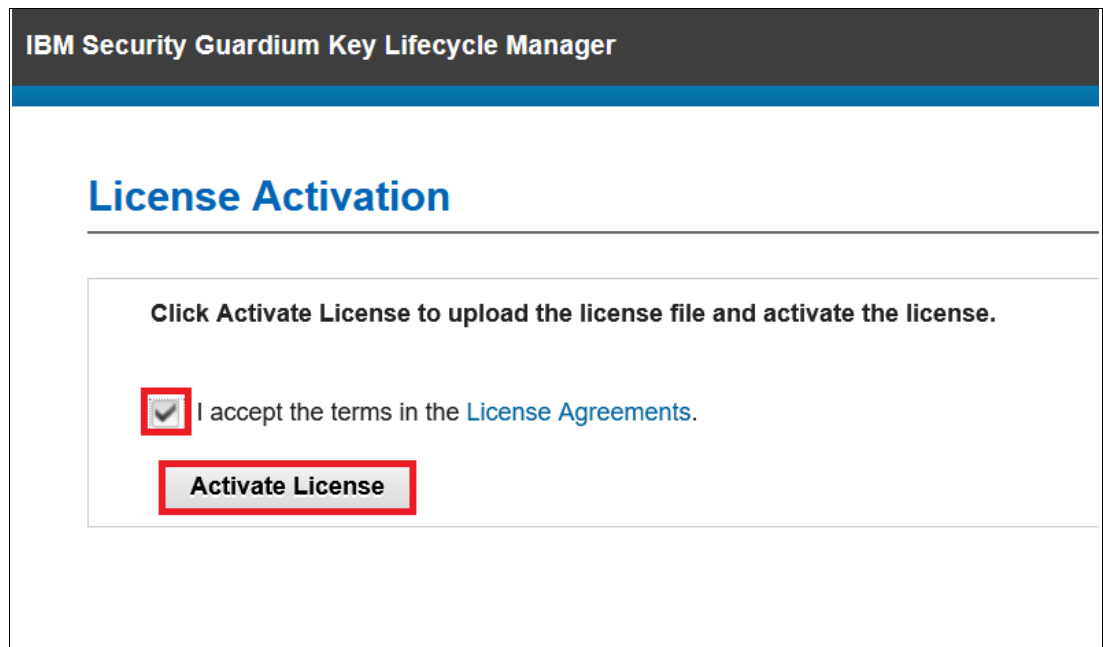


Figure 3-10 License Activation Page

4. Click **Activate License** and upload the IBM Security Guardium Key Lifecycle Manager license activation file from the local file-system, as shown in Figure 3-11.

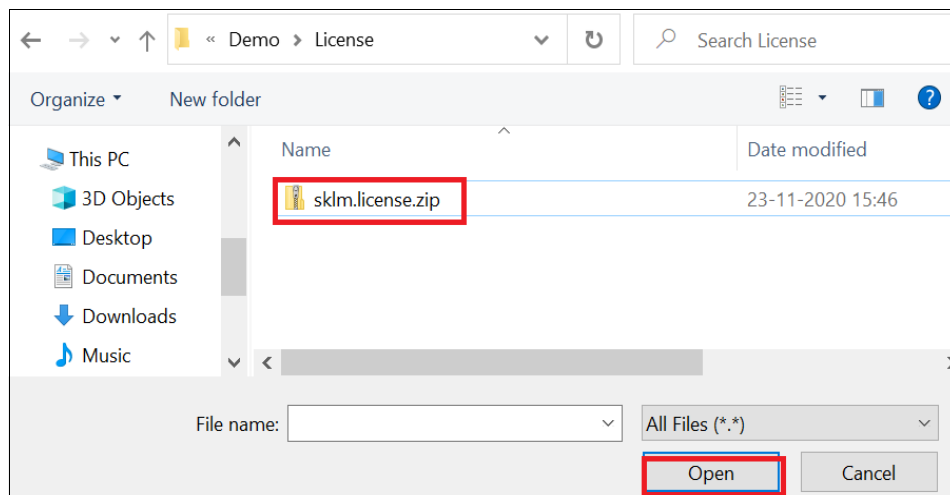


Figure 3-11 Upload license file

Note: You must download the license activation file from [IBM Passport Advantage Site](#) as described in Step 4a in 3.2, “Installing IBM Security Guardium Key Lifecycle Manager on Red Hat OpenShift” on page 29.

5. After you upload the license file, it shows the success message, as shown in Figure 3-12.

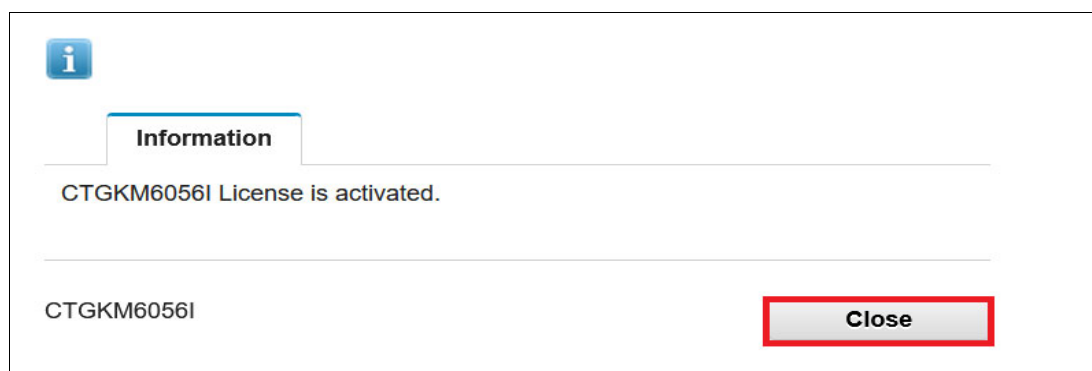


Figure 3-12 License upload success message

6. Click **Close**. You are redirected to the Login page, as shown in Figure 3-13.



Figure 3-13 Log in to IBM Security Guardium Key Lifecycle Manager

7. Log in to the IBM Security Guardium Key Lifecycle Manager GUI by using the SKLMAdmin user and verify that the license is activated. After the license is activated, you see the GKLM welcome page, as shown in Figure 3-14.

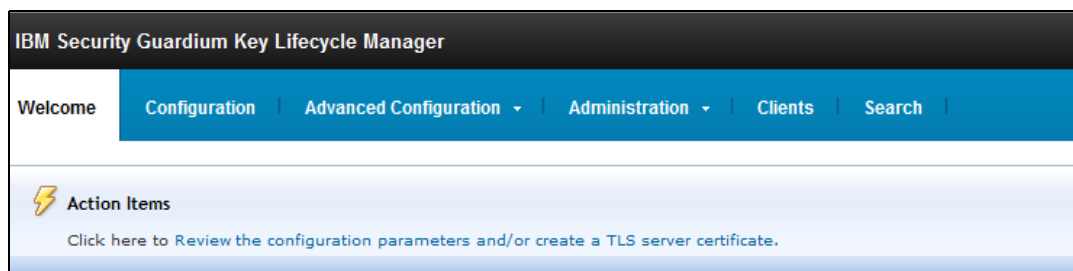


Figure 3-14 Welcome page after license activation

3.2.3 Installing IBM Security Guardium Key Lifecycle Manager Container Edition on Red Hat OpenShift with Db2U

The IBM Security Guardium Key Lifecycle Manager also can be installed with IBM Db2 container version, Db2U. The installation steps with Db2U are similar to installing with PostgreSQL. For more information about installing Db2U, see [Deploying Db2U on OpenShift Cluster Platform](#).

After the Db2U installation is complete, run the command that is shown in Example 3-7 to get port details.

Example 3-7 Get the Db2U Services Details

```
oc get svc
NAME                                TYPE      CLUSTER-IP    EXTERNAL-IP  PORT(S)
AGE
db2u-release-1-db2u                ClusterIP  172.30.70.176  <none>
50000/TCP,50001/TCP,25000/TCP,25001/TCP,25002/TCP,25003/TCP,25004/TCP,25005/TCP
29m
db2u-release-1-db2u-engn-svc      NodePort   172.30.43.152  <none>
50000:30654/TCP,50001:30363/TCP
29m
db2u-release-1-db2u-internal      ClusterIP  None           <none>
50000/TCP,9443/TCP
29m
db2u-release-1-db2u-ldap          ClusterIP  172.30.179.248 <none>
50389/TCP
29m
db2u-release-1-db2u-rest-svc      NodePort   172.30.13.126  <none>
50050:30430/TCP
29m
db2u-release-1-etcd              ClusterIP  None           <none>
2380/TCP,2379/TCP
29m
```

Update the details of Db2 database in values.yaml (Openshift-helm.zip):

- ▶ sklmdb_host (172.30.43.152) and sklmdb_port (30654) from service db2u-release-1-db2u-engn-svc.
- ▶ sklmdb_type must be db2.
- ▶ If you did not use db_username and db_name during the Db2U installation, the default values must be used for sklmdb_username (db2inst1) and sklmdb_name (bludb).

3.2.4 Exposing non-HTTP port in Red Hat OpenShift installation

When you deploy the IBM Security Guardium Key Lifecycle Manager on Red Hat OpenShift, with route definition, you can access the application with HTTP ports only. To access the application with non-HTTP port (IPP, KMIP), you must make some configuration settings. Complete the following steps to configure route for IPP and KMIP ports:

1. Define the routes for other ports (IPP and KMIP) as described in 3.2.1, “Installing IBM Security Guardium Key Lifecycle Manager Container Edition on Red Hat OpenShift with PostgreSQL” on page 29 with details (see Example 3-8).

Example 3-8 Route details

```
Route Name - IPP-route
Service - sklm
Target Port - 3801
Security - Secure route checked
    TLS Termination - Passthrough
    Insecure Traffic - Redirect

Route Name - IPP-secure-route
Service - sklm
Target Port - 1441
Security - Secure route checked
    TLS Termination - Passthrough
    Insecure Traffic - Redirect

Route Name - KMIP-route
Service - sklm
Target Port - 5696
Security - Secure route checked
    TLS Termination - Passthrough
    Insecure Traffic - Redirect
```

2. Log in to the infrastructure system by using root credentials.

Note: The infrastructure node includes a public IP and the information about which is provided with the OpenShift cluster creation.

3. Open the `haproxy.cfg` file with `vi` or a similar editor, as shown in Example 3-9.

Example 3-9 Open haproxy.cfg

```
#cd /etc/haproxy
#vi haproxy.cfg
```

4. Update the file with entries for each route that is defined for IPP and KMIP ports, as shown in Example 3-10. Save the changes.

Note: Depending on the OpenShift cluster configuration, the number of Master and Worker nodes varies. You must replace the private IP for all Master and Worker nodes for backend entry in the example.

Example 3-10 Update with route entries

```
frontend IPP-route
    bind *:33801
    default_backend IPP-route
    mode tcp
    option tcplog

backend IPP-route
    balance source
    mode tcp
    server worker0 10.17.91.228:33801 check
    server worker1 10.17.94.243:33801 check
    server worker2 10.17.95.61:33801 check

frontend IPP-secure-route
    bind *:31441
    default_backend IPP-secure-route
    mode tcp
    option tcplog

backend IPP-secure-route
    balance source
    mode tcp
    server worker0 10.17.91.228:31441 check
    server worker1 10.17.94.243:31441 check
    server worker2 10.17.95.61:31441 check

frontend KMIP-route
    bind *:35696
    default_backend IKMIP-route
    mode tcp
    option tcplog

backend KMIP-route
    balance source
    mode tcp
    server worker0 10.17.91.228:35696 check
    server worker1 10.17.94.243:35696 check
    server worker2 10.17.95.61:35696 check
```

5. Restart the haproxy service, as shown in Example 3-11.

Example 3-11 Restart haproxy

```
#systemctl restart haproxy
```

3.2.5 Installing IBM Security Guardium Key Lifecycle Manager Container Edition as Fix Pack on Red Hat OpenShift

If you installed IBM Security Guardium Key Lifecycle Manager v4.1 and plan to install v4.1.0.1, complete the following steps:

1. Update the `values.yaml` in the Helm chart (`Openshift-helm.zip`) with a build tag for the newer version (specifically 4.1.0.1).
2. Run the **helm upgrade** command to update the build with two parameters: `release name` and `chart name` (for example: `sklmapp`), as shown in Example 3-12.

Example 3-12 Helm upgrade command

```
helm upgrade sklmapp sklmapp
Release "sklmapp" has been upgraded. Happy Helming!
NAME: sklmapp
LAST DEPLOYED: Sun May  9 15:48:58 2021
NAMESPACE: sklmbd2
STATUS: deployed
REVISION: 2
TEST SUITE: None
```

3. Verify the upgrade of deployment by using the **helm list** command, as shown in Example 3-13. The `REVISION` shows an updated value (2, in our example).

Example 3-13 Helm list command

```
c:\>helm list -a
NAME      NAMESPACE      REVISION      UPDATED
STATUS    CHART           APP VERSION
sklmapp   sklmbd2         2             2021-05-09 15:48:58.5430135 +0530 IST
deployed  sklmapp-1.1.0   4.1
```

3.2.6 Troubleshooting in Red Hat OpenShift

The following commands can help you identify any issue that you might encounter while you are deploying IBM Security Guardium Key Lifecycle Manager in Red Hat OpenShift:

► List Pods

This command helps to list the pods that were created by GKLM deployment, which provides information, such as Type, Cluster-IP, and Port, as shown in Example 3-14.

Example 3-14 List pod command for OpenShift

```
#oc get pod | grep sklm
NAME      TYPE    CLUSTER-IP    EXTERNAL-IP  PORT(S)
AGE
sklmapp   NodePort 172.30.116.64  <none>
9443:31443/TCP,1441:31441/TCP,5696:31696/TCP,3801:31801/TCP,1111:32331/TCP,2222:30
123/TCP   19h
```

► **Describe Pod**

This command helps to get the information about a specific pod. This command also provides the complete information about the pod from the pod creation, as shown in Example 3-15.

Example 3-15 Describe pod command for OpenShift

```
#oc describe pod sklmapp
```

► **Get Service Details**

This command helps to get the service information that is defined by GKLM deployment. It also shows other information, such as Nodeport, ClusterIP, and mapped host ports, as shown in Example 3-16.

Example 3-16 Get service details command for OpenShift

```
#oc get svc
NAME          TYPE      CLUSTER-IP   EXTERNAL-IP  PORT(S)
AGE
db2-db2u          ClusterIP  172.30.174.140  <none>
50000/TCP,50001/TCP,25000/TCP,25001/TCP,25002/TCP,25003/TCP,25004/TCP,25005/TCP
19h
db2-db2u-engn-svc NodePort   172.30.113.104  <none>
50000:31653/TCP,50001:32706/TCP
19h
db2-db2u-internal ClusterIP   None            <none>
50000/TCP,9443/TCP
19h
db2-db2u-ldap    ClusterIP  172.30.4.204   <none>  50389/TCP
19h
db2-db2u-rest-svc NodePort   172.30.245.77  <none>  50050:31974/TCP
19h
db2-etcd          ClusterIP   None            <none>
2380/TCP,2379/TCP
19h
sklmapp           NodePort   172.30.116.64   <none>
9443:31443/TCP,1441:31441/TCP,5696:31696/TCP,3801:31801/TCP,1111:32331/TCP,2222
:30123/TCP  19h
```

► **Pod Logs**

This command helps displays the pod logs during the deployment of GKLM so that you can identify the root cause of deployment errors, as shown in Example 3-17.

Example 3-17 Pod logs command for OpenShift

```
#oc logs -f sklmapp-5c8d548c64-kh7rw
```

3.3 Installing IBM Security Guardium Key Lifecycle Manager Container Edition on Kubernetes

Before installing the IBM Security Guardium Key Lifecycle Manager on Kubernetes cluster, make sure that you completed the steps that are provided 3.1, “Deployment prerequisites” on page 28. Then, complete the following steps:

1. Prepare the Kubernetes cluster.

Set up a Kubernetes cluster. You can use Version 1.17 or later. For more information, see [this web page](#).

2. Obtain the Helm charts.

Install Helm Version 3.4.0 on the system from which you access the Kubernetes cluster. For more information, see [this web page](#).

3. Create a storage class for persistent storage.

Create a storage class for persistent storage of the database and the IBM Security Guardium Key Lifecycle Manager application data. For more information, see [this web page](#).

3.3.1 Installing IBM Security Guardium Key Lifecycle Manager on Kubernetes

Complete the following steps on the system on which you installed Helm:

1. Extract the k8s-helm.zip file.
2. In the directory where you extracted the files, browse to the k8s-helm -> sklm directory.
3. Open the values.yaml file and modify the parameter values in the file according to your requirements. The file includes information about the mandatory parameters to be updated and a description of all the parameters.
4. Browse to the k8s-helm directory and run the command as shown in Example 3-18 with name and chartname both as sklm.

Example 3-18 Helm install command

```
# helm install sklm sklm
NAME: sklm
LAST DEPLOYED: Sun May  9 16:45:14 2021
NAMESPACE: default
STATUS: deployed
REVISION: 1
TEST SUITE: None
```

5. Run the command that is shown in Example 3-19 to determine the available node port that is assigned to the service.

Example 3-19 Get service details

```
# kubectl get svc
NAME      TYPE      CLUSTER-IP  EXTERNAL-IP  PORT(S)
AGE
kubernetes ClusterIP 10.233.0.1   <none>       443/TCP
142d
postgresqlb NodePort 10.233.24.187 <none>      5432:32432/TCP
4m49s
```

```
sklmapp      NodePort    10.233.39.88    <none>
9443:30443/TCP,1441:31441/TCP,5696:32696/TCP,3801:31801/TCP,1111:31111/TCP,2222:32
222/TCP      4m49s
```

6. Start the IBM Security Guardium Key Lifecycle Manager GUI by using following URL:

`https://master_server_IP_address:port/ibm/SKLM/login.jsp`

Where,

`master_server_IP_address` is the IP address of the master server on the Kubernetes cluster.

And port is the node port of `sklmapp` service (30443 in this example).

7. Activate the license and verify the log in. For more information, see “Activating the license and logging in to IBM Security Guardium Key Lifecycle Manager” on page 33.

3.3.2 Installing IBM Security Guardium Key Lifecycle Manager Container Edition as Fix Pack on Kubernetes

If you installed IBM Security Guardium Key Lifecycle Manager v4.1 and are planning to update with IBM Security Guardium Key Lifecycle Manager v4.1.0.1 on top of it, complete the following steps:

1. Update the `values.yaml` file with a build tag (4.1.0.1, in our example).
2. Run the `helm` command to update the build with two parameters release name and chart name (`sklm` in our example), as shown in Example 3-20.

Example 3-20 Helm upgrade command

```
# helm upgrade sklm sklm
Release "sklm" has been upgraded. Happy Helming!
NAME: sklm
LAST DEPLOYED: Sun May  9 17:14:36 2021
NAMESPACE: default
STATUS: deployed
REVISION: 2
TEST SUITE: None
```

3. Verify the upgrade by using the `helm list` command. The revision column shows the updated value, as shown in Example 3-21.

Example 3-21 Verify helm update

```
# helm list -a
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
sklm	default	2	2021-05-09 17:14:36.432063241
+0530 IST deployed		sklm-0.1.0	4.1
sklmnfsrelease	default	1	2020-12-22 15:06:09.246916985
+0530 IST deployed		nfs-client-provisioner-1.2.93.1.0	

3.3.3 Troubleshooting in Kubernetes environment

The following commands can help you identify any issue that you might encounter while you are deploying the IBM Security Guardium Key Lifecycle Manager in the Kubernetes cluster:

► List Pods

This command helps to get more pod information, such as status (Running or Exited), and Readiness (1/1), as shown in Example 3-22.

Example 3-22 List pod command for Kubernetes

```
#kubect1 get pods
NAME                                READY   STATUS
RESTARTS   AGE
postgresqldb-78fbf89b68-t4bn2      1/1     Running   0
51m
sklmapp-fdfc6cd6c-pgjdk             1/1     Running   3
51m
sklmnfsrelease-nfs-client-provisioner-797fc84478-thxfx 1/1     Running   81
138d
```

► Describe Pod

This command helps to get more information about the pod from the time the pod is created, as shown in Example 3-23.

Example 3-23 Describe pod command for Kubernetes

```
#kubect1 describe pod sklmapp-fdfc6cd6c-pgjdk
```

► Pod Logs

This command helps to get the logs for GKLM pod during deployment. The pod ID is obtained by using the **kubect1 get pods** command, as shown in Example 3-24.

Example 3-24 Pod logs command for Kubernetes

```
# kubect1 logs -f sklmapp-fdfc6cd6c-pgjdk
```

► Get Service Details

This command helps to get the service information that is defined by the GKLM deployment. It also shows other information, such as Nodeport, ClusterIP, and mapped host ports, as shown in Example 3-25.

Example 3-25 Get service details command for Kubernetes

```
# kubect1 get svc
NAME      TYPE      CLUSTER-IP  EXTERNAL-IP  PORT(S)
AGE
kubernetes ClusterIP 10.233.0.1   <none>       443/TCP
142d
postgresqldb NodePort 10.233.24.187 <none> 5432:32432/TCP
4m49s
sklmapp    NodePort 10.233.39.88 <none>
9443:30443/TCP,1441:31441/TCP,5696:32696/TCP,3801:31801/TCP,1111:31111/TCP,2222
:32222/TCP 4m49s
```

3.4 Installing IBM Security Guardium Key Lifecycle Manager Container Edition on IBM z/OS Container Extensions

You can install IBM Security Guardium Key Lifecycle Manager on IBM Z/OS Container Extensions (zCX) environment with Db2 for z/OS or PostgreSQL database.

3.4.1 Installing IBM Security Guardium Key Lifecycle Manager on IBM zCX with PostgreSQL

To install the IBM Security Guardium Key Lifecycle Manager on an IBM zCX environment with PostgreSQL, complete the following steps:

1. Install the PostgreSQL database by using a Docker command, as shown in Example 3-26.

Example 3-26 Docker command for PostgreSQL

```
docker run -itd -v gklmpostgresvolume:/var/lib/postgresql/data -e
POSTGRES_PASSWORD=GKLM@postgres -e POSTGRES_USER=gklmdb41 -e POSTGRES_DB=gklmdb41
-p 5432:5432 --restart always postgres
```

2. Create an environment variable list file (gklmevz.txt) with the parameters that are shown in Example 3-27 for the IBM Security Guardium Key Lifecycle Manager container.

Example 3-27 Sample gklmevz.txt

```
DB_TYPE=postgres
DB_NAME=gklmdb41
DB_USER=gklmdb41
DB_PASSWORD=GKLM@postgres
DB_HOST=9.x.x.x
DB_PORT=5432
LICENSE=accept
SKLM_SEED=68d95f0081f1dbfc0b06de9b0916df1c
SKLMADMIN_USERNAME=skladmin
SKLMADMIN_PASSWORD=change@Me123
```

3. Install the IBM Security Guardium Key Lifecycle Manager container, as shown in Example 3-28.

Example 3-28 Docker run command for GKLM Container

```
docker run --name gklmapp -itd -p 9443:9443 -p 3801:3801 -p 5696:5696 -p 1441:1441
--env-file=gklmevz.txt -v gklmAppVolume:/opt/ibm/wlp/usr/products --restart
always ibmcom/sklm:4.1.0.1
```

4. Start the IBM Security Guardium Key Lifecycle Manager GUI by using following URL:

https://IP_address/Hostname:port/ibm/SKLM/login.jsp

Where,

IP_address/Hostname is the IP address or FQDN of the IBM Security Guardium Key Lifecycle Manager server.

And port is the port number that IBM Security Guardium Key Lifecycle Manager server listens on for requests.

5. For more information about activating the license and verifying the log in, see 3.2.2, “Activating the license and logging in to IBM Security Guardium Key Lifecycle Manager” on page 33.

3.4.2 Installing IBM Security Guardium Key Lifecycle Manager with Db2 for z/OS

To install the IBM Security Guardium Key Lifecycle Manager on zCX environment with Db2 for z/OS®, complete the following steps:

1. Install Db2 for z/OS. For more information, see [Installing or migrating to Db2](#).
2. Create a database that uses the parameter values that are shown in Example 3-29.

Example 3-29 Database variable

```
DB_USER=gk1mdb41
DB_NAME=gk1mdb41
```

Note: Make sure the Db2 user has suitable permission to create table space and tables.

3. Obtain the container installation files (eImages) and license activation file for IBM Security Guardium Key Lifecycle Manager and for Db2 for z/OS (db2jcc_license_cisuz.jar).

Note: The db2jcc_license_cisuz.jar file is used by the Guardium Key Lifecycle Manager container to connect to the Db2 for z/OS database.

4. Create a file (Dockerfile) with the content that is shown in Example 3-30 and save the file in the same directory where you saved the license file for Db2 for z/OS (db2jcc_license_cisuz.jar) on the host system.

Example 3-30 Sample Dockerfile

```
# Extend from SKLM Application Repository
ARG LATEST_IMAGE
FROM ${LATEST_IMAGE}
ARG DB2_LICENSE_FILE=${DB2_LICENSE_FILE}

#Copy license file to SKLM
COPY $DB2_LICENSE_FILE /opt/ibm/wlp/usr/sklm/custom

# Set Environment variable
ENV DB2_LICENSE_FILE=$DB2_LICENSE_FILE
```

5. Log in to the host system and browse to the directory where you saved the eImage, license, and Docker files, as shown in Example 3-31.

Example 3-31 Connect to z/CX system

```
# ssh -p 8022 <user-name>@<zCX-IP-Address>
# cd /GKLM/
```

6. Extract the Docker image of the Guardium Key Lifecycle Manager application from the image file, as shown in Example 3-32.

Example 3-32 Docker image load command

```
#docker load -i GKLM_4.1.0.1_CONTAINER_FOR_ZCX.tar
```

7. Verify that the Docker image is listed in the local repository, as shown in Example 3-33.

Example 3-33 Docker image list command

# docker images	REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
	sklm	Rel_4101.S390X	d101350128d8	1 hour ago	1.02GB

8. Build the Docker image of the Guardium Key Lifecycle Manager application by using the Docker file to include the Db2 license file, as shown in Example 3-34.

Example 3-34 Build docker image with z/OS Db2 license

```
#docker build -t gklmzos --build-arg LATEST_IMAGE=sklm:Rel_4101.s390x --build-arg DB2_LICENSE_FILE=db2jcc_license_cisuz.jar --no-cache .
```

9. Create an environment variable list file (gklmenvz.txt) with the parameters that are shown in Example 3-35 for the IBM Security Guardium Key Lifecycle Manager container.

Example 3-35 Sample gklmenvz.txt

```
DB_TYPE=zos_db2
DB_NAME=gklmdb41
DB_USER=gklmdb41
DB_PASSWORD=xxxxx
DB_HOST=9.x.x.x
DB_PORT=446
LICENSE=accept
SKLM_SEED=68d95f0081f1dbfc0b06de9b0916df1c
SKLMADMIN_USERNAME=skladmin
SKLMADMIN_PASSWORD=adminpassword
```

10. Run the IBM Security Guardium Key Lifecycle Manager Docker container, as shown in Example 3-36.

Example 3-36 Docker run command for GKLM Container

```
docker run --name gklmapp -itd -p 9443:9443 -p 3801:3801 -p 5696:5696 -p 1441:1441 --env-file=sklmenvz.txt -v gklmAppVolume:/opt/ibm/wlp/usr/products gklmzos
```

11. Start the IBM Security Guardium Key Lifecycle Manager graphical GUI by using the following URL:

https://IP_address/hostname:port/ibm/SKLM/login.jsp

Where,

IP_address/hostname is the IP address or FQDN of the IBM Security Guardium Key Lifecycle Manager server.

Port is the port number that IBM Security Guardium Key Lifecycle Manager server listens on for requests.

12. For more information about activating the license and verifying the login, see “Activating the license and logging in to IBM Security Guardium Key Lifecycle Manager” on page 33.

3.4.3 Installing IBM Security Guardium Key Lifecycle Manager Container Edition as Fix Pack in z/CX Environment

If you installed IBM Security Guardium Key Lifecycle Manager v4.1 and plan to update IBM Security Guardium Key Lifecycle Manager v4.1.0.1 on top of it, complete the following steps:

1. List all containers that are running by using a Docker command, as shown in Example 3-37.

Example 3-37 Docker list container command

```
#docker ps -a
```

2. Kill the GKLM Container without deleting the volume, as shown in Example 3-38.

Example 3-38 Docker kill command for GKLM container

```
#docker kill a36e51a24e0e  
a36e51a24e0e
```

3. Start the IBM Security Guardium Key Lifecycle Manager container and point to the same volume by using a Docker command, as shown in Example 3-39.

Example 3-39 Docker run command for GKLM container

```
docker run --name sklmapp -itd -p 9443:9443 -p 3801:3801 -p 5696:5696 -p 1441:1441  
--env-file=sklmenvz.txt -v sklmAppVolume:/opt/ibm/wlp/usr/products --restart  
always ibmcom/sklm:4.1.0.1
```

4. After the IBM Security Guardium Key Lifecycle Manager container deployment is successful, log in to the GUI and verify the version.



Migrating data

This chapter describes the different options that are available and corresponding steps that are involved in migrating the data from an older version of IBM Security Guardium Key Lifecycle Manager to version 4.1.0.1.

This process is applicable for IBM Security Guardium Key Lifecycle Manager Traditional Edition only.

This chapter includes the following topics:

- ▶ 4.1, “Migrating from an earlier version of IBM Security Key Lifecycle Manager” on page 50
- ▶ 4.2, “Inline migration” on page 51
- ▶ 4.3, “Cross migration” on page 54

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

IBM Security Guardium Key Lifecycle Manager does not support a direct upgrade of an installed version to a newer version. However, it supports data migration by using the following methods:

► **Inline migration**

When the host system of the target version is the same as the existing version, use inline migration of data. In this case, a new copy of GKLM is installed on the same host machine and data is copied from the GKLM instance of existing version to the GKLM instance of the target version.

Inline migration option is not available for fix pack releases and is available for major and Mod releases only. (Every Mod Release or a Fix Pack has a specific naming convention. The format is Version. Release. Mod. FixPack [V.R.M.F.]).

► **Cross migration**

When the host system of the target version is different than the host system of the existing version, use the cross migration approach for data migration. The existing version and target version can be installed on host machines with different versions of operating system. For example, the existing version can be installed on a Windows operating system while the target version can be installed on host machine with the Linux operating system and vice-versa.

IBM Security Guardium Key Lifecycle Manager provides sample properties files that you can use to cross migrate data. This method is preferable for migration.

Supported migration paths and migration methods are shown in Figure 4-1.

Existing version	Minimum required level	Supported?		Notes*
		Inline migration	Cross migration	
4.0	General availability (GA)	✓	✓	Upgrading IBM Security Guardium Key Lifecycle Manager to Version 4.1
3.0.1	General availability (GA)	✓	✓	
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 → V4.1)*
IBM Tivoli Key Lifecycle Manager V 2.0**	Fix pack 6			Upgrading IBM Tivoli Key Lifecycle Manager to IBM Security Guardium Key Lifecycle Manager 4.1
IBM Tivoli Key Lifecycle Manager V 1.0**	Fix pack 7			
Encryption Key Manager V 2.1**	-	✓	✓	Upgrading Encryption Key Manager to IBM Security Guardium Key Lifecycle Manager 4.1

Figure 4-1 Supported migration paths and methods

Note: Migration from IBM Tivoli® Key Lifecycle Manager and Encryption Key Manager (EKM) is not covered in this section. For more information, see the following resources:

- ▶ [Migrating from Encryption Key Manager](#)
- ▶ [Migrating from IBM Tivoli Key Lifecycle Manager](#)

4.2 Inline migration

Complete the following steps to inline migrate IBM Security Key Lifecycle Manager V2.7.0.6 to Version 4.1.0.0:

1. Run the `launchpad.sh` script to start the installation wizard, and follow the installation process that is described in Chapter 2, “IBM Security Guardium Key Lifecycle Manager Traditional Edition installation” on page 5.

Up until Version 4.1.0.0, the installer detects the version that is installed on the machine. Change the HTTPS WebSphere Application Server port 9083 - 9087. Provide the credentials of the WebSphere Application Server user and GKLM user of the previously installed and detected version. Click **Validate Credentials**, and then, click **Next** (see Figure 4-2).

IBM Installation Manager

Install Packages

Fill in the configurations for the packages.

Install Licenses Location Features Summary

IBM Db2 SKLM41

IBM Db2 SKLM41 11.5

Check whether the

IBM Security Guardium Key Lifecycle Manager

IBM Security Guardium Key Lifecycle Manager

Configuration for IBM Security Guardium Key Lifecycle Manager 4.1.0.0

IBM Security Guardium Key Lifecycle Manager Configuration

Installer has detected that a previous version (2.7.0.6) of the IBM Security Guardium Key Lifecycle Manager is already installed on this machine. Provide the values for the Application Server administrator and Key Lifecycle Manager administrator of the previous version of the application in the fields provided below.

Application Server Administration

User Name * wasadmin

Password * *****

Password for skmdb27 * *****

HTTPS WAS Port for v4.1 * 9087

Validate Credentials

IBM Security Guardium Key Lifecycle Manager Application Administration

User Name * SKLMAdmin

Password * *****

HTTPS Port for v4.1 * 9443

HTTP Port for v4.1 * 9080

< Back Next > Install Cancel

Figure 4-2 Configuration details

2. Review the installation summary and click **Install** to install the product, as shown in Figure 4-3.

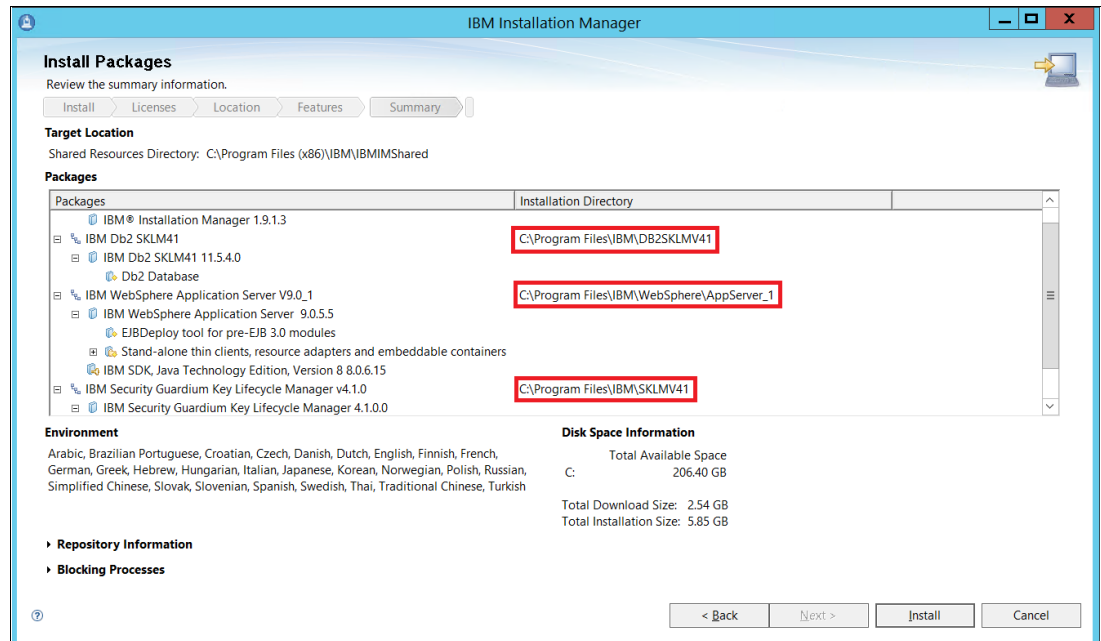


Figure 4-3 Installation summary

3. After a successful installation, select the **None** option and click **Finish** to exit the installation wizard, as shown in Figure 4-4.

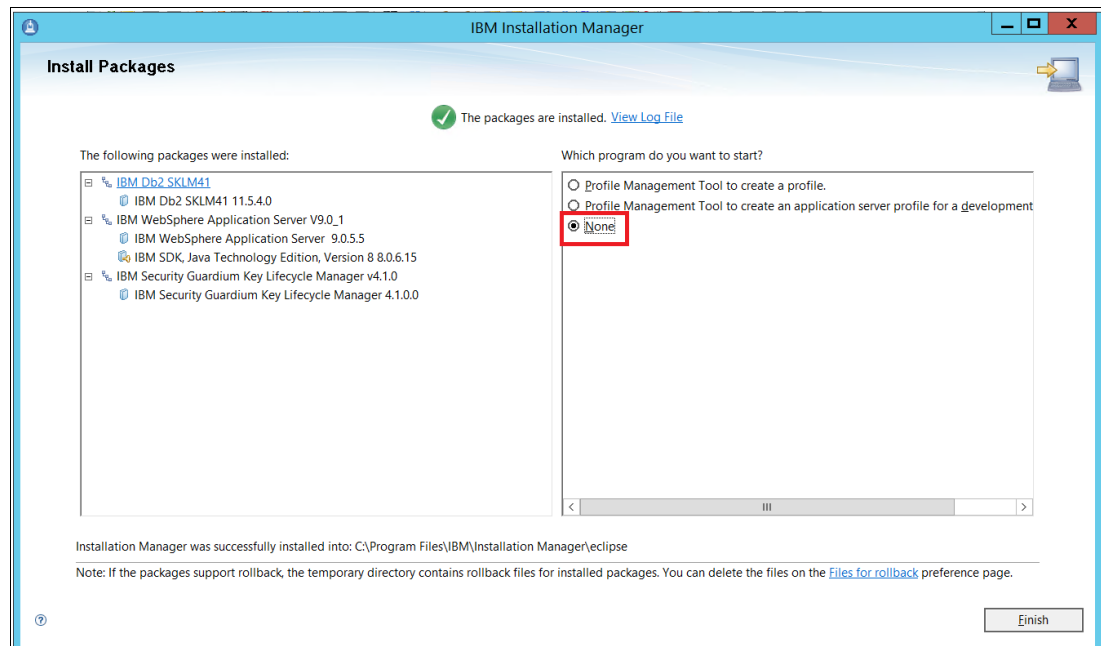


Figure 4-4 Installation Successful

4. Log on to the IBM Security Guardium Key Lifecycle Manager portal to confirm the version and that the previous data is migrated, as shown in Figure 4-5.



Figure 4-5 Configuration and version details

5. You can now install the fix pack, as described in 2.5, “Installing fix pack for IBM Security Guardium Key Lifecycle Manager Traditional Edition” on page 21.

4.3 Cross migration

Cross migration of data from source GKLM system to target system can be performed by using one of the following approaches.

- ▶ Back up and restore utility.
- ▶ Regular backup that is taken from GKLM GUI. This feature is available for backup of version 2.7 onwards.

4.3.1 Cross migration by using backup and restore utility

Complete the following steps to cross migrate data from IBM Security Guardium Key Lifecycle Manager V3.0.0.0 to Version 4.1.0.1 by using utility scripts:

1. Find the migration utility on the server where IBM Security Guardium Key Lifecycle Manager V4.1.0.1 is installed, as shown in Figure 4-6.

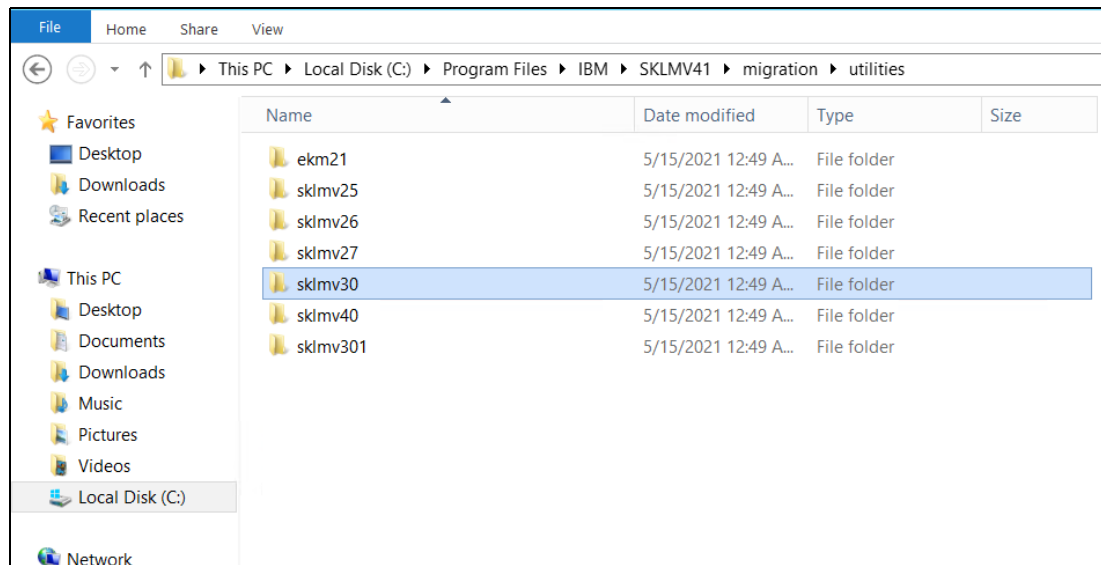


Figure 4-6 Migration Utility

2. Transfer the corresponding version of the utility directory to the server where IBM Security Key Lifecycle Manager V3.0.0.0 is installed (in this case, it is the sklmv30 directory), as shown in Figure 4-7 on page 55.

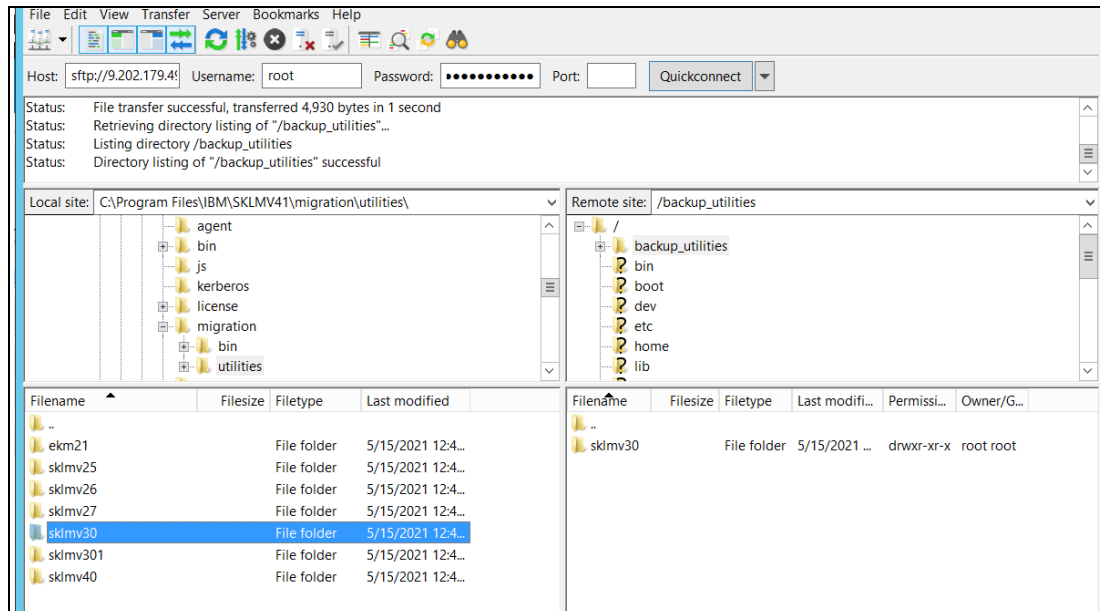


Figure 4-7 Transfer migration utility to source system

3. Modify the backup.properties file to include the WAS_HOME, JAVA_HOME paths and correct credentials for the sklmb30 (Db2 user for source system) and wasadmin accounts, as shown in Example 4-1.

Example 4-1 Modifying the backup.properties file

```
[root@sklm sklmv30]# ls
additional_backup.properties  backup.properties  backupV30.bat
com.ibm.sklm.server.migrate.sklmv30.jar  restore.properties  restoreV30.bat
additional_restore.properties  backupUsersRolesGroups.py  backupV30.sh
readme.html  restoreUserRolesGroups.py  restoreV30.sh
[root@sklm sklmv30]#
[root@sklm sklmv30]# cat backup.properties
WAS_HOME=/opt/IBM/WebSphere/AppServer
JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0
BACKUP_PASSWORD=Change@Password123
DB_PASSWORD=Change@Password123
WAS_USER_PWD=Change@Password123
[root@sklm sklmv30]#
```

4. Run the backupV30.sh script to generate the cross-platform migration file. The migration file is in the backup directory within the utility directory, as shown in Example 4-2.

Example 4-2 Generating the migration file

```
[root@sklm sklmv30]# chmod +x *.sh
[root@sklm sklmv30]# ./backupV30.sh
CURR_DIR=/backup_utilities/sklmv30/
Backup completed, please refer to backup.log for more details.
[root@sklm sklmv30]# ls backup/
backupStatus.properties  sklm_v3.0.0.0_20210515035746-0700_migration_backup.jar
[root@sklm sklmv30]#
```

- Transfer the migration file to the destination server where IBM Security Key Lifecycle Manager V4.1.0.1 is installed, as shown in Figure 4-8.

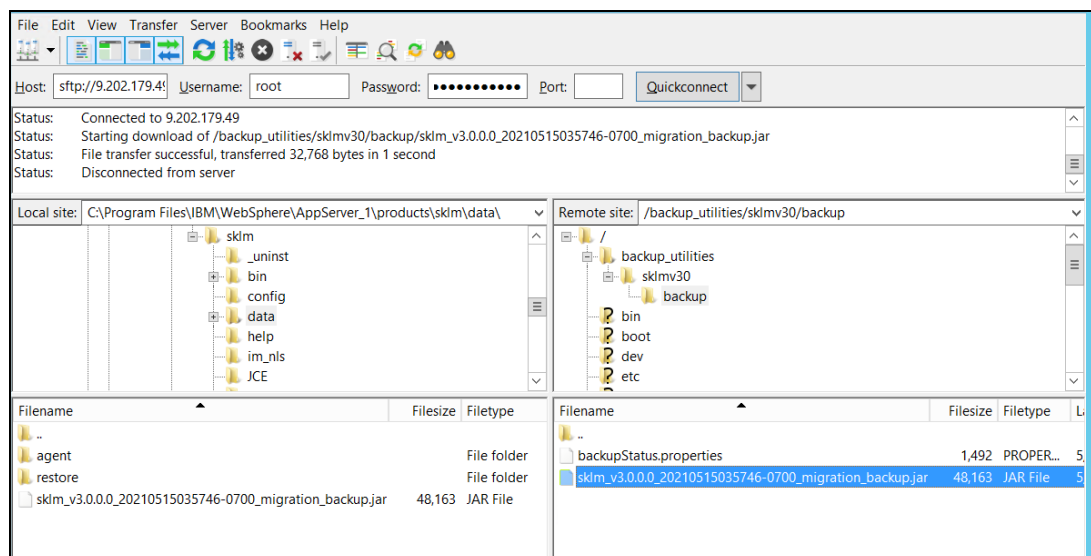


Figure 4-8 Transfer backup file to destination

- In the IBM Security Guardium Key Lifecycle Manager V4.1.0.1, modify the restore.properties file to include the WAS_HOME, JAVA_HOME and RESTORE_FILE paths and correct password for the Backup, Db2 user, and wasadmin accounts, as shown in Figure 4-9.

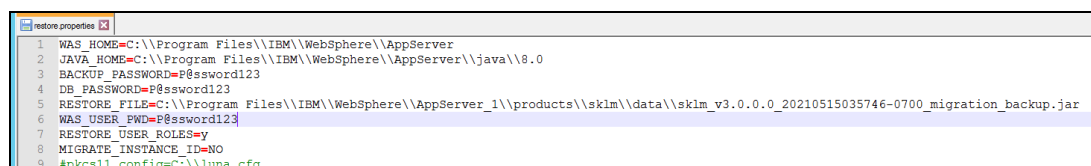


Figure 4-9 Update restore.properties

To restore the user accounts along with their passwords from source GKLM version to GKLM V4.1.0.1, set RESTORE_USER_ROLES=y. If the destination GKLM system is configured with HSM, uncomment the line for parameter pkcs11.cfg and set its value to point to the path of the HSM configuration file.

- Run restoreV30.bat to perform restore operation, as shown in Example 4-3

Example 4-3 Perform restore operation

```

c:\Program Files\IBM\SKLMV41\migration\utilities\sklmv30>restoreV30.bat
CURR_DIR c:\Program Files\IBM\SKLMV41\migration\utilities\sklmv30\

```

Credentials for same user accounts that exist on both source and target servers are not migrated.

Restore completed, Please refer to restore.log for more details.

For the changes to take effect, restart the IBM Security Guardium Key Lifecycle Manager server.

```

c:\Program Files\IBM\SKLMV41\migration\utilities\sklmv30>

```

Note: In IBM Security Guardium Key Lifecycle Manager V4.1.0.1, user credentials for the user accounts that are on source and target servers are not migrated. In that case, if user SKLMAdmin exists on IBM Security Key Lifecycle Manager V3.0.0.0, its user credentials are not migrated to IBM Security Guardium Key Lifecycle Manager V4.1.0.1. User SKLMAdmin can log in by using the same password that was set before the data migration operation was started.

8. Check `restore.log` for the presence of any error or exception during the restore operation.
9. Restart the WebSphere Application Server from the Windows services console, as shown in Figure 4-10.

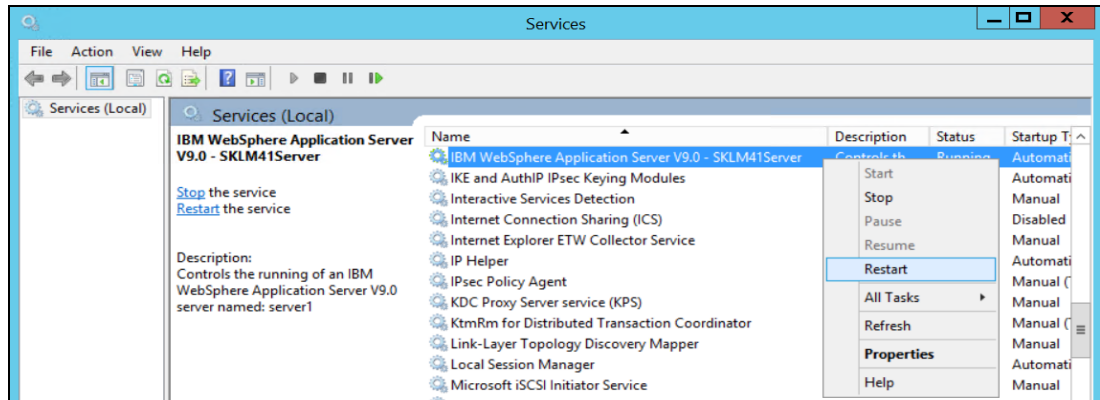


Figure 4-10 Restart WebSphere Application Server

10. Log in to the IBM Security Guardium Key Lifecycle Manager GUI and verify that the data was migrated successfully.

4.3.2 Cross migration by using backup and restore from GUI

Complete the following steps to cross migrate IBM Security Key Lifecycle Manager V3.0.0.0 to Version 4.1.0.1 by using GKLM GUI:

1. Log in to GUI interface for IBM Security Guardium Key Lifecycle Manager V3.0.0.0 and back up the GKLM server by using the steps that are described in 5.2.1 “Backing up IBM Security Guardium Key Lifecycle Manager” on page 67.
2. Transfer the backup file from the file system that is hosting IBM Security Guardium Key Lifecycle Manager V3.0.0.0 to the server where IBM Security Guardium Key Lifecycle Manager V4.1.0.1 is installed, as shown in Figure 4-8 on page 56.
3. Log in to GUI interface for IBM Security Guardium Key Lifecycle Manager V4.1.0.1 and perform a restore operation by using the steps that are described in 5.2.2 “Restoring IBM Security Guardium Key Lifecycle Manager” on page 69. The restore operation restarts the WebSphere Application Server server automatically and GKLM server is unavailable for some time.
4. Log in back to the IBM Security Guardium Key Lifecycle Manager V4.1.0.1 GUI and verify that the data was migrated successfully.



Configuring IBM Security Guardium Key Lifecycle Manager

This chapter describes the tasks that are associated with configuring IBM Security Guardium Key Lifecycle Manager and includes the following topics:

- ▶ 5.1, “Configuring an TLS/KMIP certificate for IBM Security Guardium Key Lifecycle Manager” on page 60
- ▶ 5.2, “Backing up and restoring IBM Security Guardium Key Lifecycle Manager” on page 67
- ▶ 5.3, “Configuring replication for IBM Security Guardium Key Lifecycle Manager” on page 71
- ▶ 5.4, “Configuring a Multi-Master cluster” on page 80
- ▶ 5.5, “Integrating LDAP with IBM Security Guardium Key Lifecycle Manager Traditional Edition by using configuration scripts” on page 91
- ▶ 5.6, “Integrating LDAP with IBM Security Guardium Key Lifecycle Manager Container Edition” on page 101
- ▶ 5.7, “Configuring signed CA certificates for IBM Security Guardium Key Lifecycle Manager portal and IBM WebSphere console access” on page 105

5.1 Configuring an TLS/KMIP certificate for IBM Security Guardium Key Lifecycle Manager

After you install IBM Security Guardium Key Lifecycle Manager, you must configure secure communication by using the TLS protocol.

5.1.1 Logging in to IBM Security Guardium Key Lifecycle Manager GUI

Complete the following steps to log in to IBM Security Guardium Key Lifecycle Manager graphical user interface (GUI):

1. Start a web browser.
2. Log in to IBM Security Guardium Key Lifecycle Manager (see Figure 5-1) by going to the following URL and using SKLMAdmin user and password that was set during the installation:
`https://<ip address/hostname>:<port>/ibm/SKLM/login.jsp`

Important: IBM Security Guardium Key Lifecycle Manager v4.1.0.1 uses port 9443 for GUI and REST APIs by default.



Figure 5-1 Log in page

After logging in to IBM Security Guardium Key Lifecycle Manager GUI, you can create Server certificate for TLS communication. Server certificate can be one of the following types:

- ▶ Self-Signed Certificate. For more information, see “Creating a self-signed server certificate” on page 61.
- ▶ Third-party CA Signed Certificate. For more information, see “Creating a third-party CA signed server certificate” on page 63 for more details.

5.1.2 Creating a self-signed server certificate

To create a self-signed server certificate, complete the following steps:

1. Click **Advanced Configuration** → **Server certificates** and then, click **Add**, as shown in Figure 5-2.

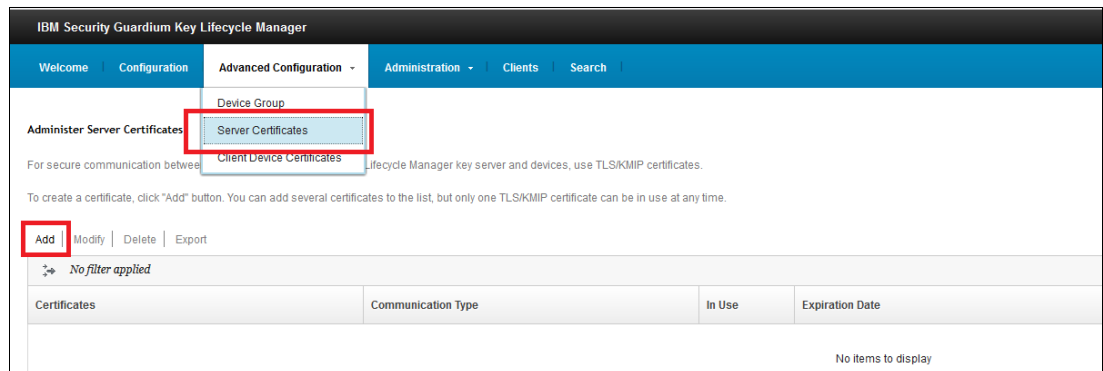


Figure 5-2 Server certificate

2. Select the **Create a self-signed certificate** option and complete the details, as shown in Figure 5-3. The validity period determines how long the certificate is valid. By default, IBM Security Guardium Key Lifecycle Manager creates 2048-bit RSA public-private key pair for Server certificates.

The screenshot shows the 'Add TLS/KMIP Certificate' form. It has two radio buttons: 'Create a self-signed certificate' (selected) and 'Request certificate from a third-party provider'. Below the first option, there are four fields: '*Certificate label in keystore:' with the value 'sklm server', '*Certificate description (common name):' with the value 'sklm server', '*Validity period of new certificate (in days; for example, 3 years is 365 x 3 = 1095 days):' with the value '1095', and '*Algorithm:' with the value 'RSA'. There is also an expandable section for 'Optional Certificate Parameters'. At the bottom, there are 'Add Certificate' and 'Cancel' buttons.

Figure 5-3 Self-signed Server Certificate - Add page

3. After all details are completed, click **Add Certificate**.
4. A message is displayed that confirms that the certificate was successfully created, as shown in Figure 5-4 on page 62. Click **Close**.

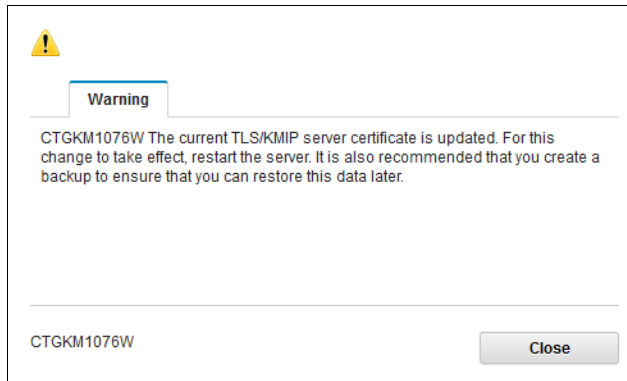


Figure 5-4 Server certificate created successfully

5. Verify the details of new server certificate, as shown in Figure 5-5.

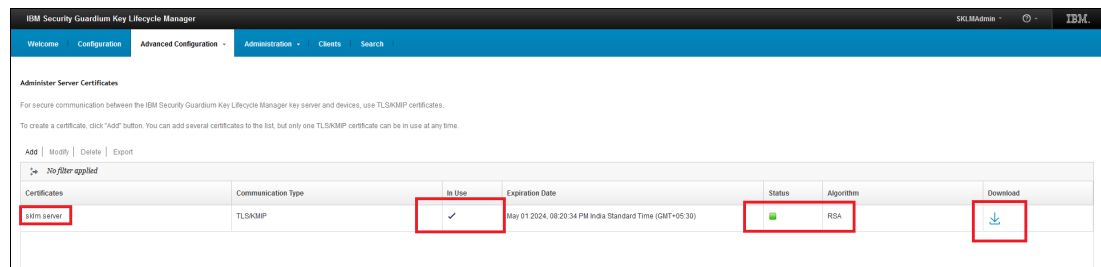


Figure 5-5 Self-signed server certificate Status

6. Validate the status from the Welcome page as well, as shown in Figure 5-6.

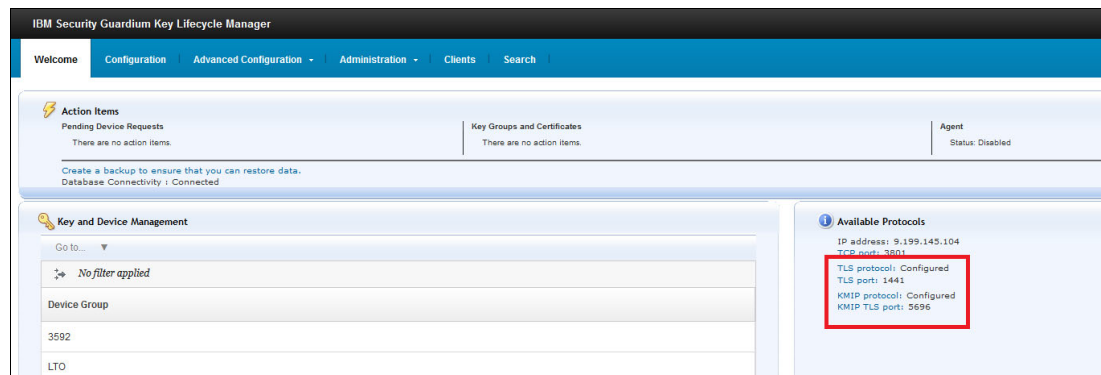


Figure 5-6 Welcome page with Server certificate configured

7. Restart the IBM Security Guardium Key Lifecycle Manager by selecting the **skladmin** user in the upper right corner. Click **Restart Server**, as shown in Figure 5-7.

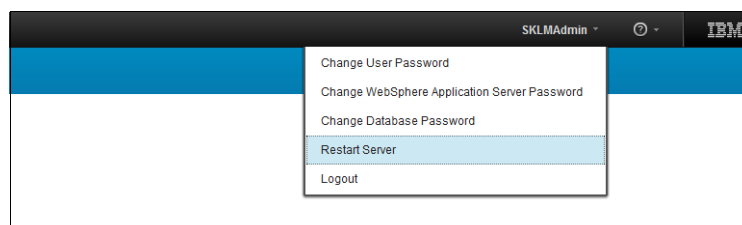


Figure 5-7 Restarting Server

5.1.3 Creating a third-party CA signed server certificate

To create a certificate request for a signed CA server certificate, complete the following steps:

1. Click **Advanced Configuration** → **Server certificates** and then, click **Add**, as shown in Figure 5-2 on page 61.
2. Select **Request certificate from a third-party provider**, specify the certificate details and validity period, and then, click **Add certificate**, as shown in Figure 5-8.

Add TLS/KMIP Certificate

☐ Create a self-signed certificate
Use a self-signed certificate in a known environment. A client cannot verify a self-signed certificate before accepting a connection.

☒ Request certificate from a third-party provider
Use a certificate generated by a third-party provider as a more secure means of communication. A client can verify a certificate from a third-party provider before accepting a connection.

Generate Certificate Request for Third-party Provider

*Certificate label in keystore:
server cert ca

*Certificate description (common name):
server cert ca

*Validity period of new certificate (in days; for example, 3 years is 365 x 3 = 1095 days):
1095 The interval in days ranges from 1 to 9000

*Algorithm:
RSA

Optional Certificate Parameters

Add Certificate Cancel

Figure 5-8 Third-Party CA signed Server certificate - Add Page

3. A message that confirms the successful certificate signing request is displayed, as shown in Figure 5-4 on page 62. Click **Close**.
4. Validate the status of the created certificate, which is in **Pending** state, as shown in Figure 5-9.

IBM Security Guardium Key Lifecycle Manager

Welcome Configuration Advanced Configuration Administration Clients Search

Administer Server Certificates

For secure communication between the IBM Security Guardium Key Lifecycle Manager key server and devices, use TLS/KMIP certificates.

To create a certificate, click "Add" button. You can add several certificates to the list, but only one TLS/KMIP certificate can be in use at any time.

Add Modify Delete Export

Certificates	Communication Type	In Use	Expiration Date	Status	Algorithm	Download
server_cert_ca	TLS/KMIP	✓	May 01 2024, 08:52:40 PM India Standard Time (GMT+05:30)	Pending		Download

Figure 5-9 Third-party CA Signed Server certificate Status: Pending

Note: The most recently created server certificate from the IBM Security Guardium Key Lifecycle Manager GUI becomes the active certificate for the server, which might break the communication between the configured devices and the server. Plan carefully when you need a new server certificate.

The server certificate with Pending status is shown with a question mark. The certificate signing request file is automatically created in the GKLM data directory, as shown in Figure 5-10, as shown in the following example:

Linux: /opt/IBM/WebSphere/AppServer/products/sklm/data

Windows: C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data

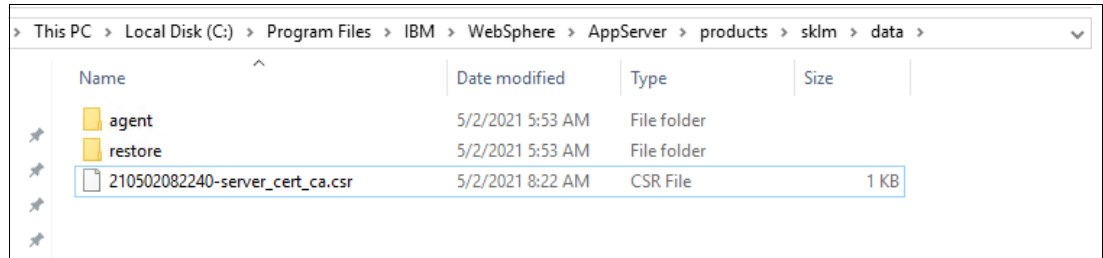


Figure 5-10 CSR file in operating system directory

5. The CSR file can be download from IBM Security Guardium Key Lifecycle Manager GUI by clicking the download link (see Figure 5-9 on page 63) or directly from the data directory by using file copy tools like scp, sftp.
6. Get the certificate signing request file signed from the trusted CA.
7. Upload the signed certificate in GKLM data directory again, as shown in Figure 5-11.

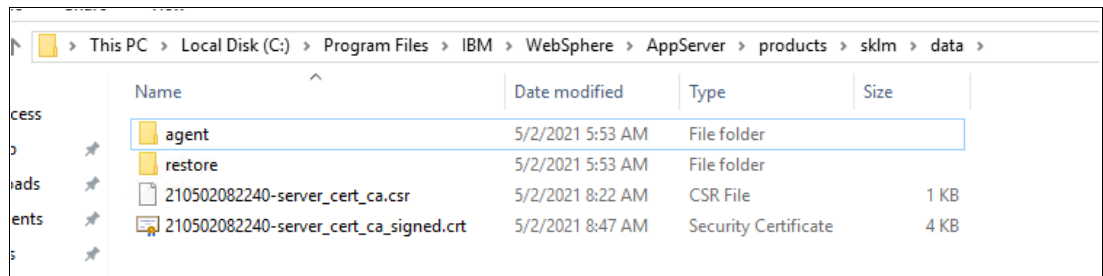


Figure 5-11 Signed CA certificate uploaded in data directory

8. Go to Welcome page in the IBM Security Guardium Key Lifecycle Manager GUI and check the Action Items.
9. Click **Third-party certificates pending import**, as shown in Figure 5-12.

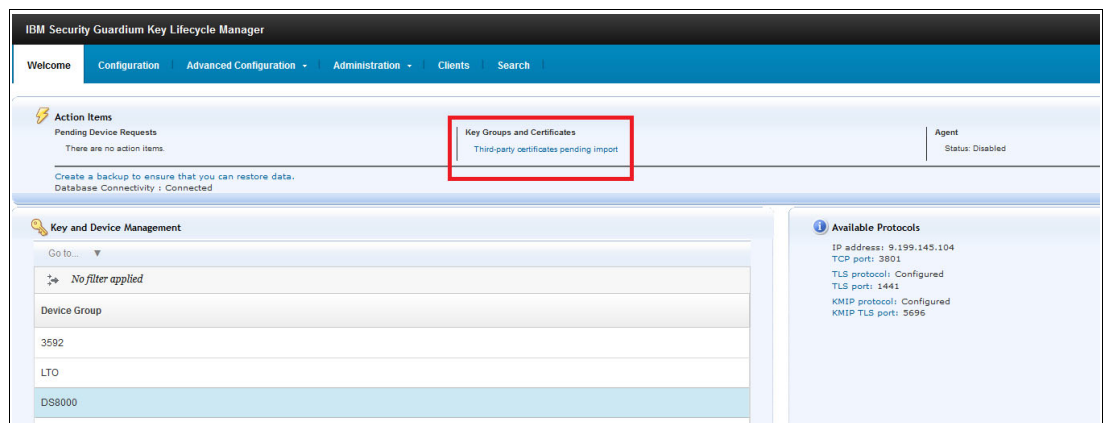


Figure 5-12 Third-party Certificate pending import

10. On the **Import** page, select the Pending certificate, and click **Import**, as shown in Figure 5-13.

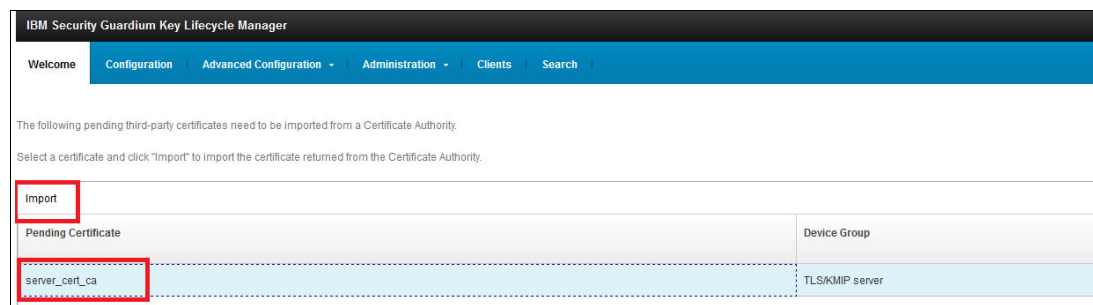


Figure 5-13 Select Certificate for upload

11. Click **Browse**, as shown in Figure 5-14.

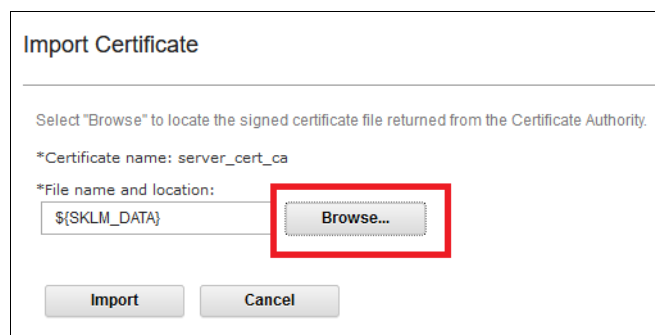


Figure 5-14 Browse for signed certificate

12. Select signed certificate and click **Select**, as shown in Figure 5-15.

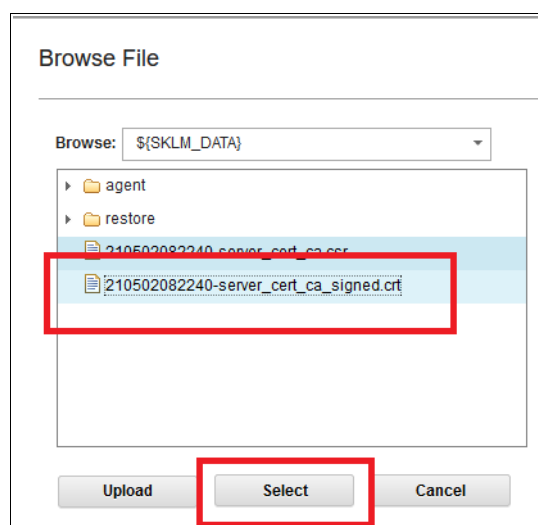


Figure 5-15 Import Signed Certificate

13. Click **Import**, as shown in Figure 5-16.

Figure 5-16 Import Signed certificate

14. After importing the signed certificate, the status of the server certificate changes to **Valid**, as shown in Figure 5-17.

Certificates	Communication Type	In Use	Expiration Date	Status	Algorithm
server_cert_ca	TLS/KMIP	✓	May 01 2031, 04:17:37 AM India Standard Time (GMT+05:30)	Valid	RSA

Figure 5-17 Valid Server Certificate

15. Restart the IBM Security Guardium Key Lifecycle Manager Server, as shown in Figure 5-7 on page 62.

5.1.4 Exporting and downloading Server certificate

To establish TLS communication, you might need to download IBM Security Guardium Key Lifecycle Manager Server certificate to get it trusted on the client side.

Complete the following steps to export and download the TLS/KMIP Server certificate:

1. Log in to IBM Security Guardium Key Lifecycle Manager GUI and browse to **Advanced Configuration** → **Server certificates** page.
2. Select the server certificate, which is marked in Use.
3. Click the download icon, as shown in Figure 5-18.

Certificates	Communication Type	In Use	Expiration Date	Status	Algorithm	Download
server_cert_ca	TLS/KMIP	✓	May 01 2031, 04:17:37 AM India Standard Time (GMT+05:30)	Valid	RSA	Download

Figure 5-18 Export & download certificate

4. Click **Download** to download the exported certificate on your local machine, as shown in Figure 5-19.

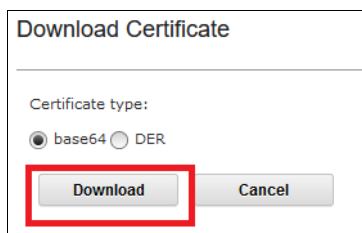


Figure 5-19 Download certificate

The TLS/KMIP Certificate is now exported and downloaded.

5.2 Backing up and restoring IBM Security Guardium Key Lifecycle Manager

IBM Security Guardium Key Lifecycle Manager creates cross-platform backup files in a manner that is independent of operating systems and the directory structure of the server. You can restore the backup files to an operating system that is different from the one from which it was backed up. For example, you can restore a backup file that is taken on a Linux system and restore it on a Windows system. Your role must have permissions to back up or to restore files.

5.2.1 Backing up IBM Security Guardium Key Lifecycle Manager

To back up IBM Security Guardium Key Lifecycle Manager, complete the following steps:

1. Log on to the IBM Security Guardium Key Lifecycle Manager GUI.
2. Click **Administration** → **Backup and Restore**, as shown in Figure 5-20.

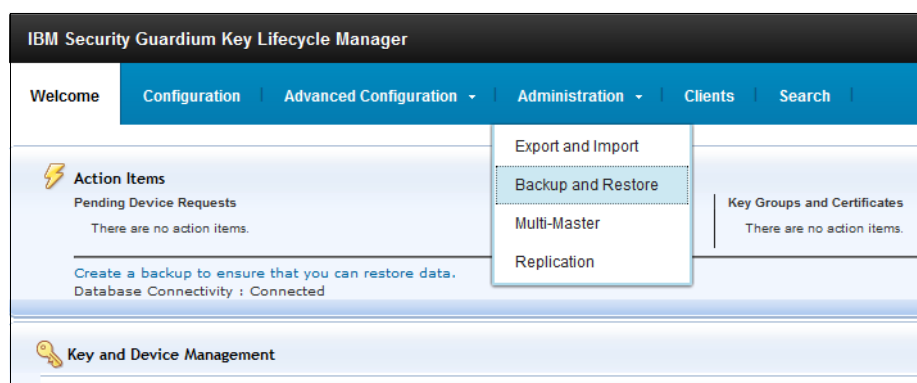


Figure 5-20 Backup and Restore menu

- Click **Browse** to specify the backup repository location. the default location is the GKLM data directory. Click **Create**, as shown in Figure 5-21.

*Backup repository location:

Backup File	Backup File
-------------	-------------

Figure 5-21 Backup and Restore Browse directory

- In the Create Backup window (as shown in Figure 5-22), enter the password and a description for the backup and then, click **Create Backup**. This password is required to restore this backup.

Create Backup

*Backup location:

*Create password:

*Retype password:

Backup description:

Figure 5-22 Create Backup

- A confirmation window is displayed. Click **OK**.
- When the backup is complete, the information window is displayed, as shown in Figure 5-23. Click **Close**.

Information

CTGKM0241I \${SKLM_DATA}\sklm_v4.1.0.1_20210502105656-0700_backup.jar was successfully created.

CTGKM0241I

Figure 5-23 Backup successful

- The backup file is shown in the table. Click the **download** icon to download this backup, as shown in Figure 5-24. This backup file must be protected and can be used for recovery during disaster situations.

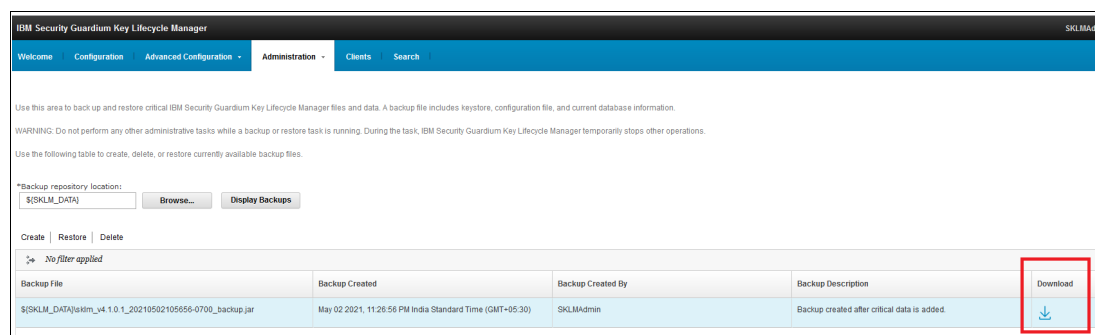


Figure 5-24 Download backup file

5.2.2 Restoring IBM Security Guardium Key Lifecycle Manager

To restore IBM Security Guardium Key Lifecycle Manager, complete the following steps:

- Ensure that the backup archive file is uploaded to the GKLM data directory of the IBM Security Guardium Key Lifecycle Manager server.
- Log in to the IBM Security Guardium Key Lifecycle Manager GUI.
- Click **Administration** → **Backup and Restore**. You should see all the backup files in the GKLM data, as shown in Figure 5-25.

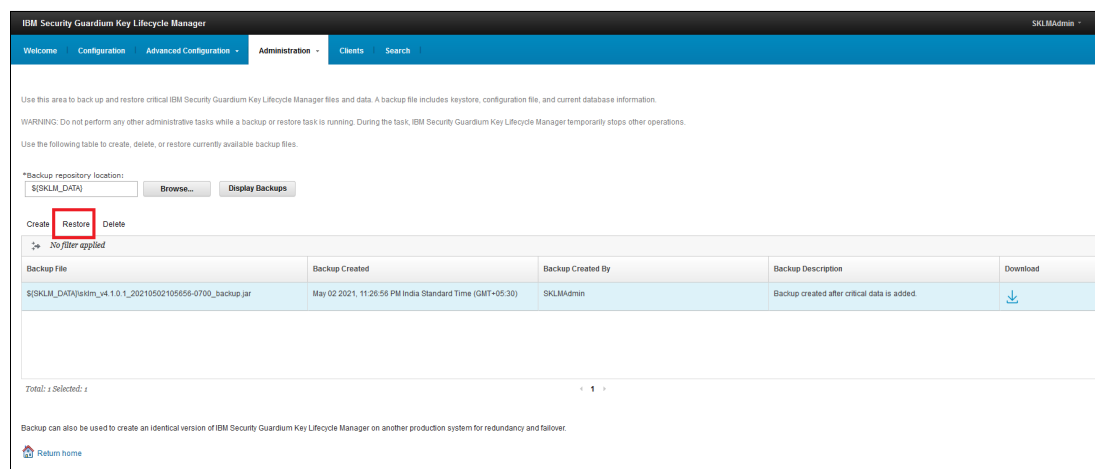


Figure 5-25 Display Backups

- Select the backup file, click **Restore**, as shown in Figure 5-25.

5. Enter the password that was specified during the backup process and click **Restore Backup**, as shown in Figure 5-26.

Restore From Backup

Restoring the system will stop the IBM Security Guardium Key Lifecycle Manager server.

The key and configuration data will be restored to the level of the backup that you select. Any changes made after the selected backup will be lost, including the meta data.

*Backup location and file name:
\${SKLM_DATA}\sklm_v4.1.0.1_20210502105656-0700_backup.jar

*Enter password:
.....

After restoring from this backup, the IBM Security Guardium Key Lifecycle Manager server will be restarted automatically.

Restore Backup Cancel

Figure 5-26 Restore Backup

6. Read the instructions carefully, which are shown in confirmation window and then, click **OK** (see Figure 5-27). The restore process might take some time to complete, depending on the size of the data.

Confirm

The system will be restored from
\${SKLM_DATA}\sklm_v4.1.0.1_20210502105656-0700_backup.jar.

the key and configuration data will be restored to the level of the backup that you select. Any changes made after the selected backup will be lost, including the metadata.

After restoring from this backup, the server will be restarted automatically.

OK Cancel

Figure 5-27 Restore confirmation box with important instructions

Note: All of the data that was present in the IBM Security Guardium Key Lifecycle Manager server is erased when the backup is restored. IBM Security Guardium Key Lifecycle Manager Server is restarted after the restore is successful and the server remains unavailable for key serving during the restart process.

A confirmation message is displayed when the backup is restored successfully, as shown in Figure 5-28.

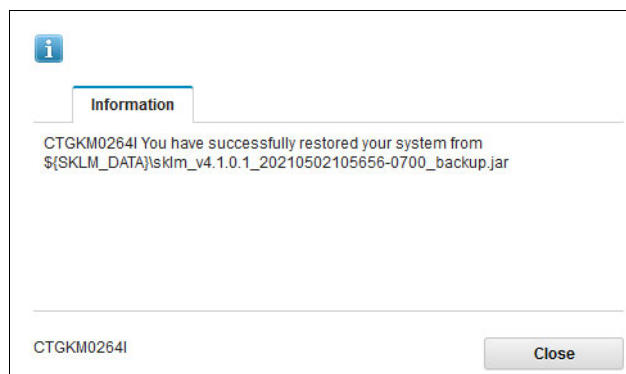


Figure 5-28 Restore Successful

5.3 Configuring replication for IBM Security Guardium Key Lifecycle Manager

IBM Security Guardium Key Lifecycle Manager can be configured to automatically replicate cryptographic keys, configuration files, and other critical data from a master server to up to 20 clone servers. The automatic replication ensures continuous keys and certificates availability to encrypting devices.

The data replication enables cloning of IBM Security Guardium Key Lifecycle Manager environments to multiple servers in a manner that is independent of operating systems and directory structures of the servers.

The master server is the primary system that is replicated. The replication process is triggered only when new keys or devices are added or modified on the master server.

Each clone server is identified by an IP address or host name, and a port number. The server uses the properties in the `ReplicationSKLMConfig.properties` file to control the replication process.

IBM Security Guardium Key Lifecycle Manager Replication can be configured in three modes:

- ▶ **Master-Clone Full Replication:** In this mode, full data backup of master server is replicated on the clone server. The default replication schedule is 1 day and the minimum schedule can be 1 hour.
- ▶ **Master-Clone Incremental Replication:** In this mode, data that is created on the master server is replicated on the clone server since the last backup instead of full data replication. The default replication schedule is 1 minute, which also is the minimum. Incremental replication is near real-time synchronization.
Incremental Replication can be configured only with Full Replication.
- ▶ **Master only for scheduled backup:** This mode also is called *scheduled backup*. In this mode, only a master server is configured with no clone. This mode takes a full automated backup at the scheduled time only if new keys or certificates are created.

The following actions are performed by IBM Security Guardium Key Lifecycle Manager replication server during Full Replication:

1. Check whether a backup is required at the scheduled time.
2. If no backup is required (no keys are created), replication is skipped.
3. If the backup is required (new keys are created), IBM Security Guardium Key Lifecycle Manager replication master server triggers the replication process.
4. The replication master server starts a secure TLS 1.2 communication with clone servers.
5. The replication master server transmits the backup file that was created.
6. The replication clone server restores the backup.
7. The replication clone server sends the status to Replication master.
8. The replication clone server is restarted at the end of the process.

5.3.1 Configuring the master server for replication

To configure the master server for replication, complete the following steps:

1. Log on to the IBM Security Guardium Key Lifecycle Manager GUI and browse to **Administration** → **Replication**, as shown in Figure 5-29.

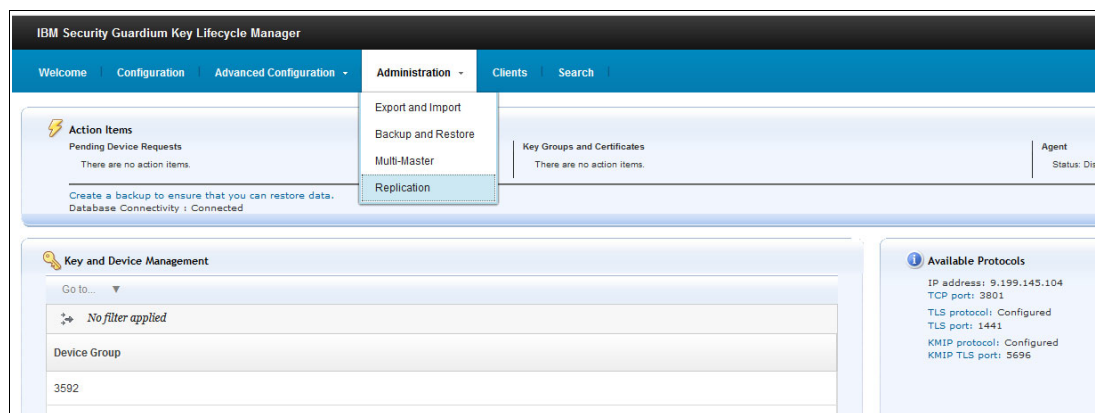


Figure 5-29 Replication Menu

2. Select the **Master** role, and click **OK**, as shown in Figure 5-30 on page 73.

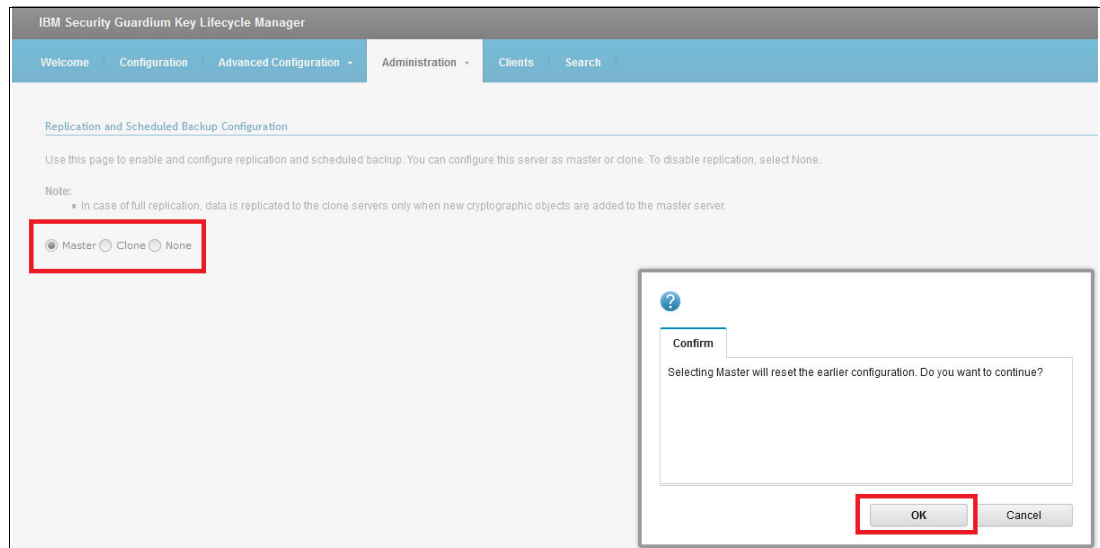


Figure 5-30 Replication master selection

- From the list, select any certificate to be used for the replication, enter the passphrase for protecting backup files and then, click **Add Clone** to add the clone servers. Save the replication configuration, and then, click **Start Replication Server**, as shown in Figure 5-31.

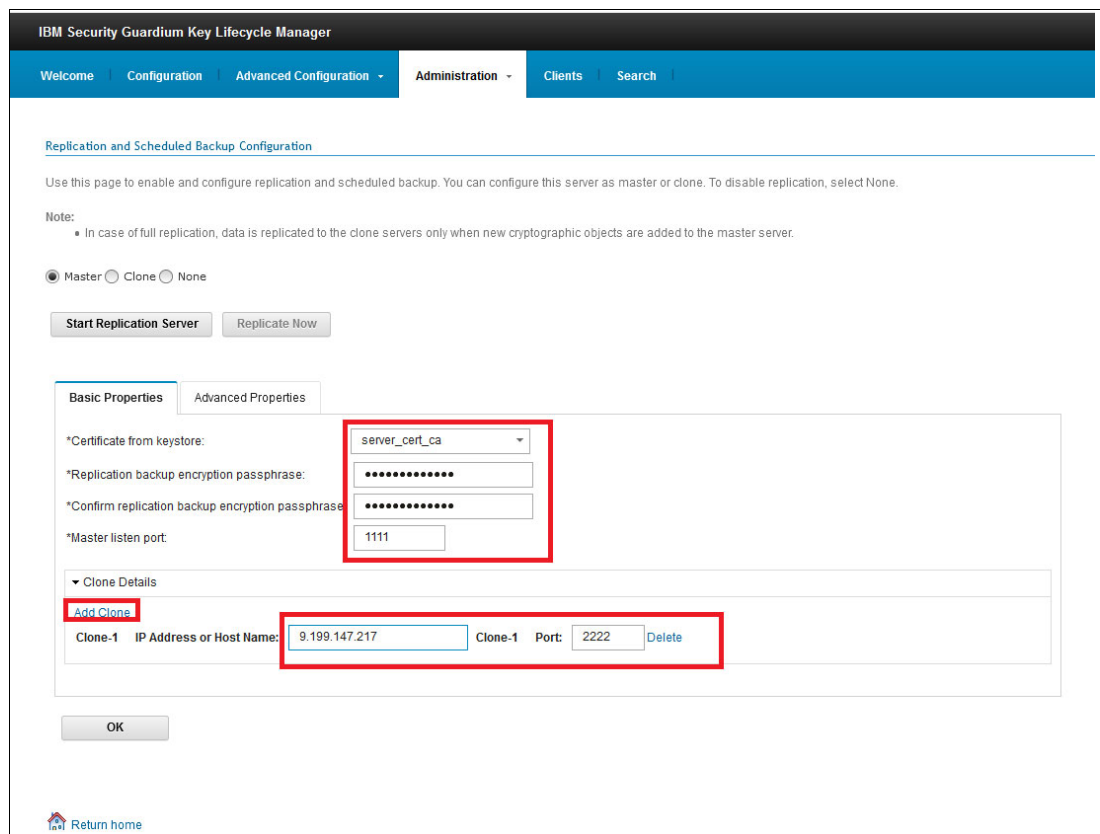


Figure 5-31 Replication Master configuration

Notes: Consider the following points:

- ▶ Any available certificates, regardless of whether they are being used, can be used for replication. However, the chosen certificate must exist on the clone servers.
- ▶ The host name of the clone server must be resolvable by using the `/etc/hosts` file or DNS.
- ▶ Make sure that the firewall is configured to enable communication between Master and Clones on configured ports.
- ▶ Make sure to use mapped ports of the clone if IBM Security Guardium Key Lifecycle Manager Container edition is used.

4. Click **OK** to save the master server configuration. Then, click **OK** in the confirmation dialog box.
5. Click **Start Replication Server**, as shown in Figure 5-32.

Replication and Scheduled Backup Configuration

Use this page to enable and configure replication and scheduled backup. You can configure this server as master or clone. To disable replication, select None.

Note:

- In case of full replication, data is replicated to the clone servers only when new cryptographic objects are added to the master server.

☒ Master ☐ Clone ☐ None

Start Replication Server Replicate Now

Basic Properties Advanced Properties

*Certificate from keystore: server_cert_ca

*Replication backup encryption passphrase:

*Confirm replication backup encryption passphrase:

*Master listen port: 1111

▼ Clone Details

[Add Clone](#)

Clone-1	IP Address or Host Name:	9.199.147.217	Clone-1	Port:	2222	Delete
---------	--------------------------	---------------	---------	-------	------	------------------------

OK

Figure 5-32 Replication Master: Start Replication Server

6. A confirmation window is shown when the Replication server is started, as shown in Figure 5-33.

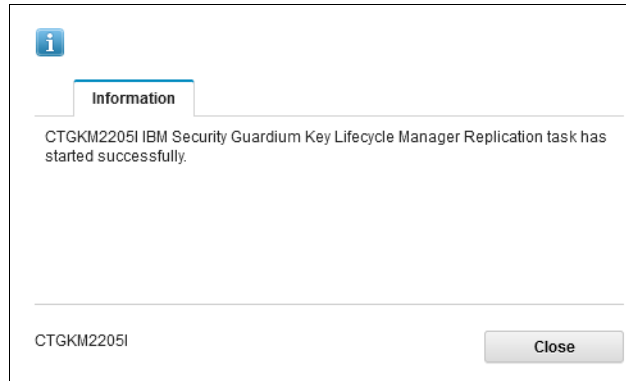


Figure 5-33 Replication Task started successfully

7. Browse to the Welcome page and check the status of replication server, as shown in Figure 5-34.

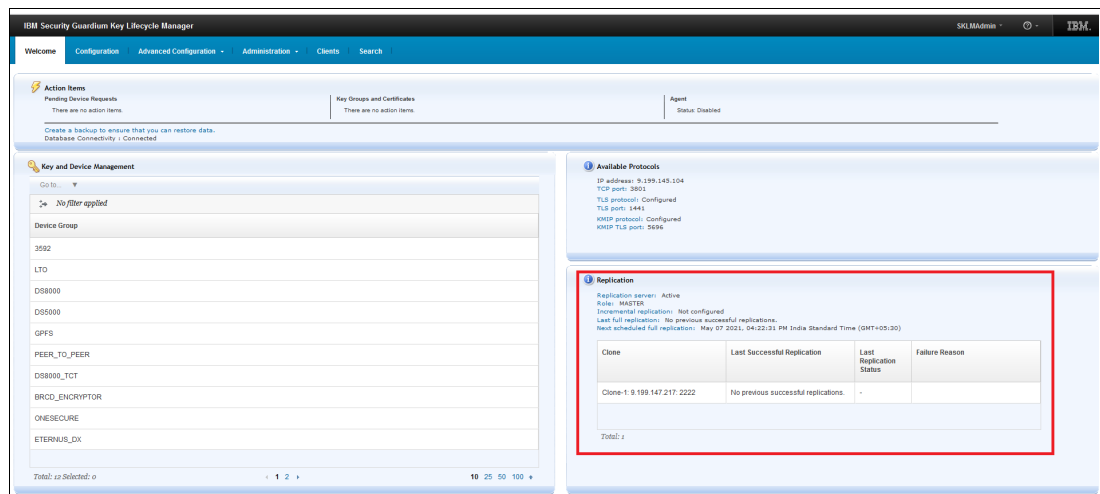


Figure 5-34 Replication Master status on Welcome page

This step completes the configuration of master server for full replication.

5.3.2 Configuring the master server for Incremental Replication

To configure the master server for incremental replication, complete the following steps:

1. Follow the steps for configuring master in full replication mode, as described in “Configuring the master server for replication” on page 72.
2. Click **Administration** → **Replication**.
3. Click the **Advanced Properties** tab, as shown in Figure 5-35 on page 76.

Figure 5-35 Replication Master - Advanced Configuration Menu

4. Select the **Incremental replication frequency (in seconds):** option and click **OK**, as shown in Figure 5-36.

Figure 5-36 Replication Master with Incremental option enabled

5. Click **OK** in the confirmation window.
6. Click **Stop Replication Server**.
7. Click **Start Replication Server**.
8. Browse to the **Welcome** page to check the Replication status, as shown in Figure 5-37.

Clone	Last Successful Replication	Last Replication Status	Failure Reason
Clone-1: 9.199.147.217: 2222	No previous successful replications.	-	

Total: 1

Figure 5-37 Replication Master in Incremental mode: Welcome page status

This step completes the configuration of Replication Master in Incremental mode.

5.3.3 Configuring the clone server for replication

The replication process enables the cloning of IBM Security Guardium Key Lifecycle Manager environment from master server to multiple clone servers. IBM Security Guardium Key Lifecycle Manager supports up to 20 clones with one master.

To configure the clone server for replication, complete the following steps:

1. Log in to the master server and take a backup. For more information, see “Backing up IBM Security Guardium Key Lifecycle Manager” on page 67.
2. Copy the backup file that was created in Step 1 to clone server.
3. Log in to the clone server and restore the backup file. For more information, see “Restoring IBM Security Guardium Key Lifecycle Manager” on page 69.

The clone server restarts automatically after the restore is successful.

Note: It is important that same server certificate is available on all masters and clones in a replication cluster. If a certificate that is configured on Replication master configuration page is not available on clones, replication does not work.

If a server certificate on the master is replaced because expiration or any other reason, make sure that the same server certificate is copied to clone servers with the private key. This task can be done by using one of the following methods:

- Backup from the master and restore on the clone (preferred option).
- Use [Key Export REST API](#) to export public-private key pair on the master server and [Key Import REST API](#) to import public-private key pair on the clone servers.

4. Log in to the clone server and browse to the **Administration** → **Replication** page.

5. Select the **Clone** option, configure the ports as wanted and then, click **OK**, as shown in Figure 5-38.

IBM Security Guardium Key Lifecycle Manager

Welcome | Configuration | Advanced Configuration | Administration | Clients | Search

Replication and Scheduled Backup Configuration

Use this page to enable and configure replication and scheduled backup. You can configure this server as master or clone. To disable replication, select None.

Note:

- In case of full replication, data is replicated to the clone servers only when new cryptographic objects are added to the master server.

☐ Master ☒ Clone ☐ None

Start Replication Server

Basic Properties | Advanced Properties

*Master listen port: 1111

*Clone listen port: 2222

OK

Figure 5-38 Replication Clone: Configuration window

6. Click **Start Replication Server**, as shown in Figure 5-39.

☐ Master ☒ Clone ☐ None

Start Replication Server

Basic Properties | Advanced Properties

Figure 5-39 Replication Clone: Start Replication Server

7. A success message is displayed when the Replication clone server is started successfully, as shown in Figure 5-40.

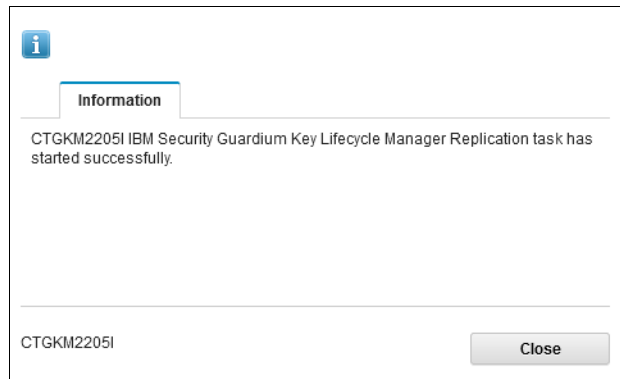


Figure 5-40 Replication Clone started successfully

8. Navigate to the Welcome page to see the Replication clone status, as shown in Figure 5-41.

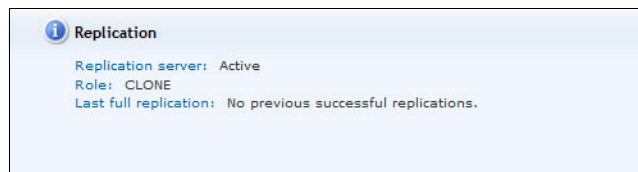


Figure 5-41 Replication Clone status: Welcome page

5.4 Configuring a Multi-Master cluster

Implementation of a high availability (HA) solution requires configuring IBM Security Guardium Key Lifecycle Manager master servers in a Multi-Master cluster. All IBM Security Guardium Key Lifecycle Manager instances in the cluster point to a single data source that is configured for Db2 HA disaster recovery (HADR) to ensure real-time availability of the latest data to all the master servers in the cluster.

You can use the IBM Security Guardium Key Lifecycle Manager Multi-Master configuration for data transmission to achieve the following objectives:

- Ensure consistent and continuous data availability of IBM Security Guardium Key Lifecycle Manager across the organization.
- Avoid a single point of failure by using the HA solution.
- Place master servers at several physical sites; that is, distributed across the network.

To set up HADR, you must configure the necessary Db2 parameters in the IBM Security Guardium Key Lifecycle Manager master servers with a primary database and a standby database. Figure 5-42 shows a simple deployment of IBM Security Guardium Key Lifecycle Manager and Db2 HADR for a Multi-Master environment where four instances (master servers) of Db2 HADR and N instances of IBM Security Guardium Key Lifecycle Manager are configured.

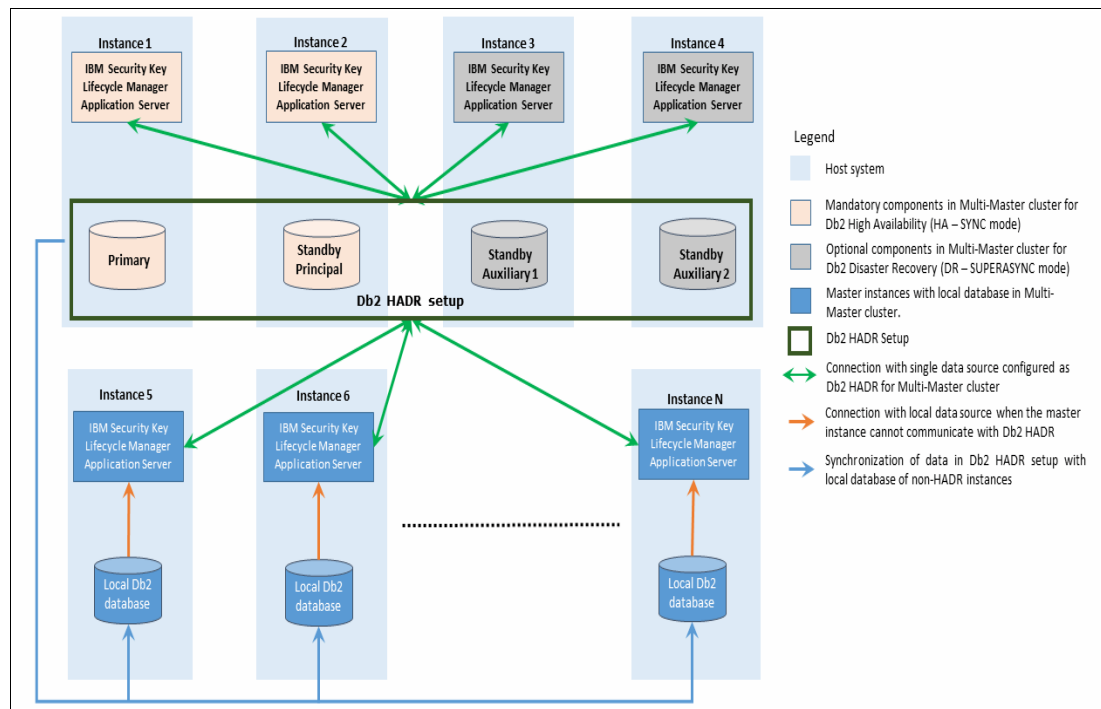


Figure 5-42 Deployment example

Note: The Multi-Cluster setup is more suitable in a dynamic environment, which requires frequent key or certificate creation or modification. For a relatively static environment, the backup/restore and replication approach is recommended.

5.4.1 Types of servers in a Multi-Master cluster

In a Multi-Master cluster, servers can be of different types that are described in this section.

Primary

This server is where the database is up and applications can connect and update data. All servers in the HADR cluster point to this database. Only one primary server can be used in the cluster at a time.

Principal standby

This standby server of the HADR cluster is the target for the defined SYNCMODE from the primary server. Only one standby can be the principal standby at a time.

Auxiliary standby

Any standby server of the HADR, which is not the principal standby, can be the Auxiliary standby server. The only syncmode that is supported for the Auxiliary standby is SUPERASYNC. Any server in the HADR cluster beyond the first two is an Auxiliary standby. This server is for disaster recovery (DR) purposes, and as such often is placed in a geographically dispersed data center.

Master Server or Non-Standby Server

Any server that is not Primary or Standby, is set up as master server. Master servers are the servers that connect to the database that is being used by Db2 HADR.

If data synchronization service is configured, the primary server sends regular backups to this server (every 24 hours by default). This backup server can be used for DR because it includes the backup from primary. For more information about data synchronization service, see [Data Synchronization Service](#).

5.4.2 Setting up minimal deployment of a Multi-Master cluster

This section covers the configuration of the minimal deployment of a Multi-Master cluster, as shown in Figure 5-43.

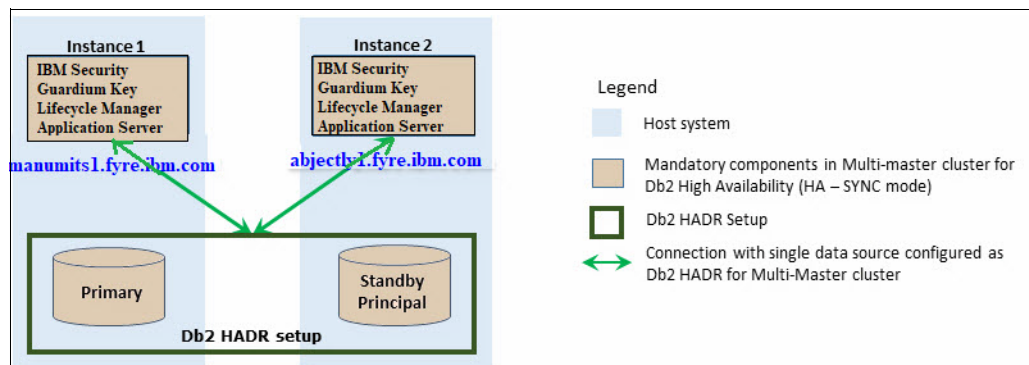


Figure 5-43 Minimal deployment of a Multi-Master cluster

The deployment includes the following prerequisites:

- ▶ Both primary and standby Db2 database servers are installed on the same version of the operating system.
- ▶ The Db2 version that is installed on the IBM Security Guardium Key Lifecycle Manager primary and standby master servers match.
- ▶ A dedicated network is used for the Db2 HADR primary and standby connections.
- ▶ Db2 user names and passwords are the same on all masters servers of IBM Security Guardium Key Lifecycle Manager Multi-Master cluster.

For more information about requirements for Multi-Master configuration, see [IBM Documentation \(formerly IBM Knowledge Center\)](#).

You also must ensure that your computer host name is configured correctly before you set up IBM Security Guardium Key Lifecycle Manager master servers for a Multi-Master configuration. You can resolve an IP address to a host name by editing the `/etc/hosts` file.

For Db2 HADR configuration, you must update the `/etc/hosts` file in the primary and standby master servers of the cluster to enable host name to IP address mapping, as shown in Example 5-1.

Example 5-1 The `/etc/hosts` file on the primary master and standby master servers

Primary Master

```
[root@manumits1 ~]$ cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
10.41.4.87  manumits1.fyre.ibm.com manumits1
10.41.5.152 abjectly1.fyre.ibm.com abjectly1
```

Standby Master

```
[root@abjectly1 ~]# cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
10.41.5.152 abjectly1.fyre.ibm.com abjectly1
10.41.4.87  manumits1.fyre.ibm.com manumits1
```

Complete the following steps:

1. Update the Db2 kernel parameters on the primary master and standby master servers if IBM Security Guardium Key Lifecycle Manager is installed on a Linux operating system by editing the `/etc/sysctl.conf` file, as shown in Example 5-2.

Example 5-2 Db2 kernel parameters

```
#Example for a computer with 16GB of RAM:
kernel.shmmni=4096
kernel.shmmax=17179869184
kernel.shmall=8388608
#kernel.sem=<SEMMSL> <SEMMNS> <SEMOPM> <SEMMNI>
kernel.sem=250 1024000 32 4096
kernel.msgmni=16384
kernel.msgmax=65536
kernel.msgmnb=65536
```

For more information about setting up kernel parameters, see [IBM Documentation \(formerly IBM Knowledge Center\)](#).

2. Log on to the IBM Security Guardium Key Lifecycle Manager portal on the primary master server, and add a server certificate on the primary master server. For more information, see 5.1, “Configuring an TLS/KMIP certificate for IBM Security Guardium Key Lifecycle Manager” on page 60.
3. After the server certificate is added and marked as in use, click **Administration** → **Multi-Master**. Click **Multi-Master** and then, click **OK** to start the Multi-Master configuration, as shown in Figure 5-44.

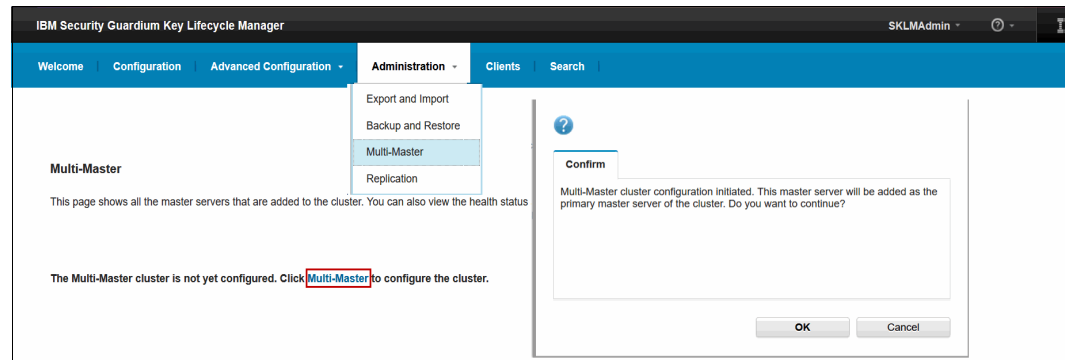


Figure 5-44 Multi-Master configuration

4. Click **Add Master** to add the standby master server. Then, specify the details in the **Basic Properties** tab, as shown in Figure 5-45.

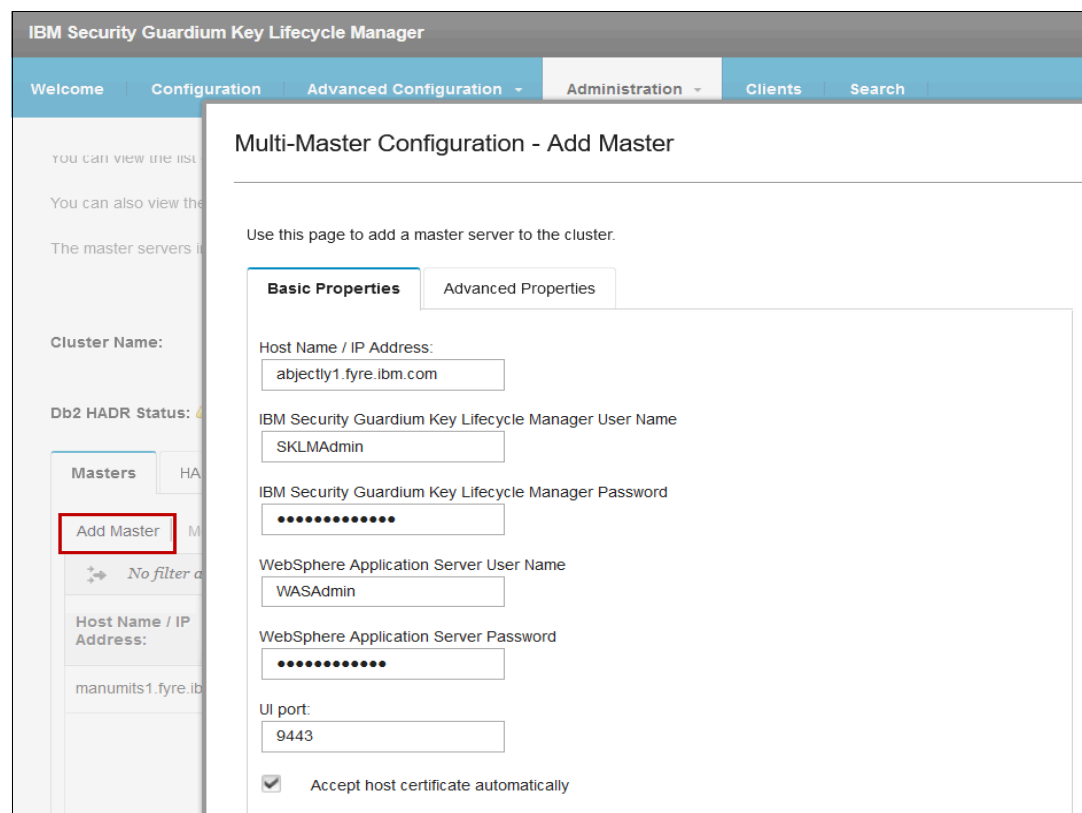


Figure 5-45 Multi-Master Configuration: Basic Properties

5. Select **Advanced Properties** and then, select **Yes** to make the server that is added a standby master. Keep the defaults for HADR port and Standby priority index, as shown in Figure 5-46.

The screenshot shows the 'Multi-Master Configuration - Add Master' dialog box with the 'Advanced Properties' tab selected. The 'Do you want to set this master server as standby?' question has the 'Yes' radio button selected and highlighted with a red box. Below it, the 'HADR port' is set to '60028' and the 'Standby priority index' is set to '1', both of which are also highlighted with red boxes. The left sidebar shows the 'Masters' tab and an 'Add Master' button.

Figure 5-46 Multi-Master Configuration - Advanced Properties

Note: The standby server to be added must be a clean installation with no configurations on it. Even a server certificate should not be created on the server that is added as the standby.

6. Click **Check Prerequisites** to verify whether the standby master server meets the requirement, as shown in Figure 5-47.

The screenshot shows the same 'Multi-Master Configuration - Add Master' dialog box as in Figure 5-46, but with an 'Information' dialog box overlaid on the right. The 'Information' dialog box contains the message: 'CTGKM3228I abjectly1.fyre.ibm.com met all the pre requisites and can be added into the cluster.' and a 'Close' button. The background dialog box is dimmed, but the 'Yes' radio button and the 'HADR port' and 'Standby priority index' fields remain visible.

Figure 5-47 Checking prerequisites

- Click **Add** to add the standby master server (the process might take some time to complete). A confirmation message is shown when the standby server is successfully added, as shown in Figure 5-48.

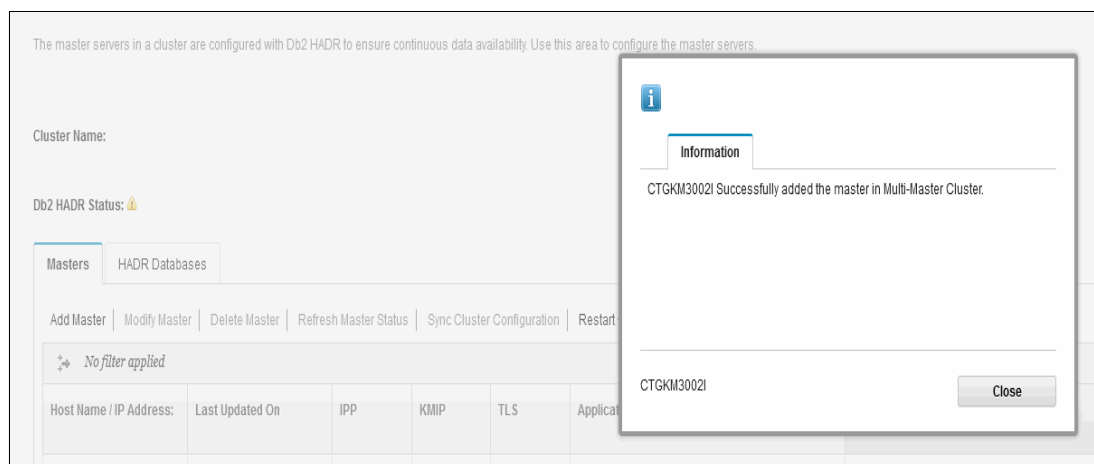


Figure 5-48 Confirmation of the standby master successfully added

- Verify the HADR status on the master and standby servers, as shown in Example 5-3.

Example 5-3 HADR status

```
[sklmb41@manumits1 ~]$ db2pd -d sklmb41 -hadr
```

```
Database Member 0 -- Database SKLMB41 -- Active -- Up 2 days 10:01:04 -- Date
2021-05-07-01.53.30.743979
```

```

HADR_ROLE = PRIMARY
REPLAY_TYPE = PHYSICAL
HADR_SYNCMODE = SYNC
STANDBY_ID = 1
LOG_STREAM_ID = 0
HADR_STATE = PEER
HADR_FLAGS = TCP_PROTOCOL
PRIMARY_MEMBER_HOST = manumits1.fyre.ibm.com
PRIMARY_INSTANCE = sklmb41
PRIMARY_MEMBER = 0
STANDBY_MEMBER_HOST = abjectly1.fyre.ibm.com
STANDBY_INSTANCE = sklmb41
STANDBY_MEMBER = 0
HADR_CONNECT_STATUS = CONNECTED

```

output omitted.....

```
[[sklmb41@abjectly1 ~]$ db2pd -d sklmb41 -hadr
```

```
Database Member 0 -- Database SKLMB41 -- Active Standby -- Up 0 days 00:21:50 --
Date 2021-05-07-01.54.37.267242
```

```

HADR_ROLE = STANDBY
REPLAY_TYPE = PHYSICAL
HADR_SYNCMODE = SYNC
STANDBY_ID = 0

```

```

LOG_STREAM_ID = 0
HADR_STATE = PEER
HADR_FLAGS = TCP_PROTOCOL
PRIMARY_MEMBER_HOST = manumits1.fyre.ibm.com
PRIMARY_INSTANCE = sk1mdb41
PRIMARY_MEMBER = 0
STANDBY_MEMBER_HOST = abjectly1.fyre.ibm.com
STANDBY_INSTANCE = sk1mdb41
STANDBY_MEMBER = 0
HADR_CONNECT_STATUS = CONNECTED

```

output omitted.....

9. The IBM Security Guardium Key Lifecycle Manager portal for both primary and standby server also reflect the Multi-Master status on the welcome page, as shown in Figure 5-49 and Figure 5-50.

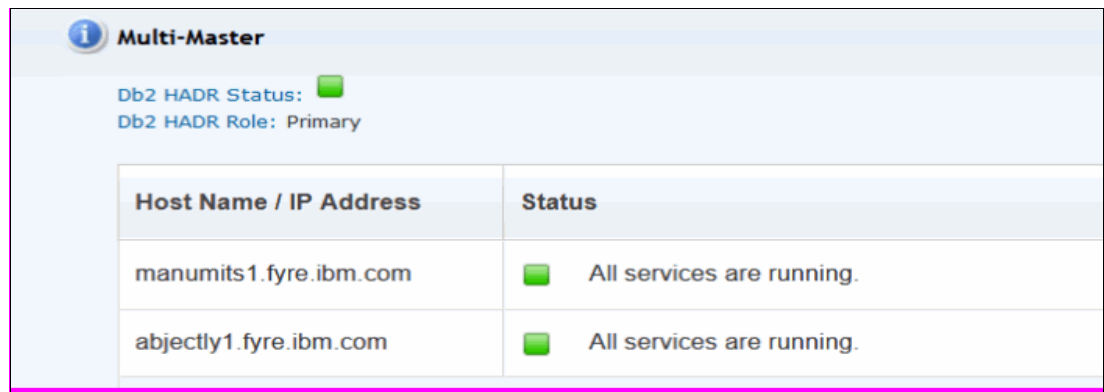


Figure 5-49 Multi-Master status on primary server

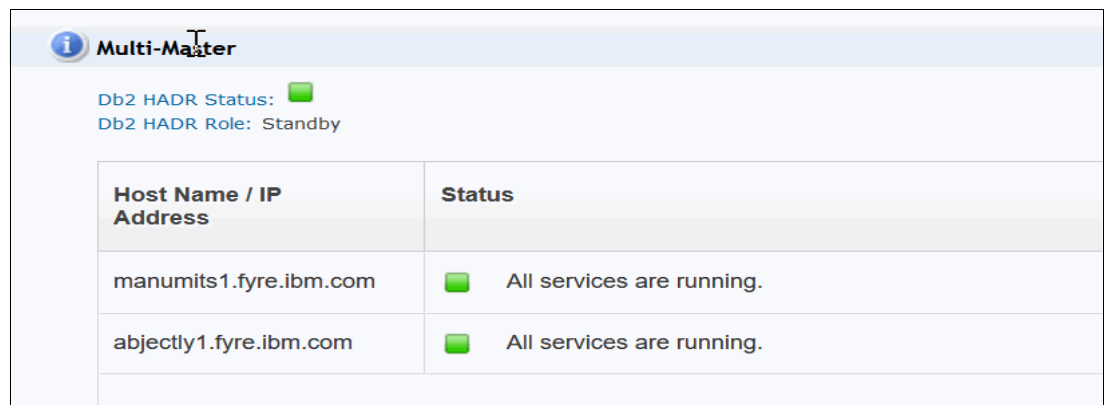


Figure 5-50 Multi-Master status on standby server

5.4.3 Agent Status

You can view the status of Agent service and Agent certificate expiry status on IBM Security Guardium Key Lifecycle Manager GUI, notification area.

Complete the following steps:

1. Log in to the IBM Security Guardium Key Lifecycle Manager GUI.

On the Welcome page notification area, a panel for Agent is available. This window shows the status (Started/ Stopped /Disabled) of the Agent service, as shown in Figure 5-51.

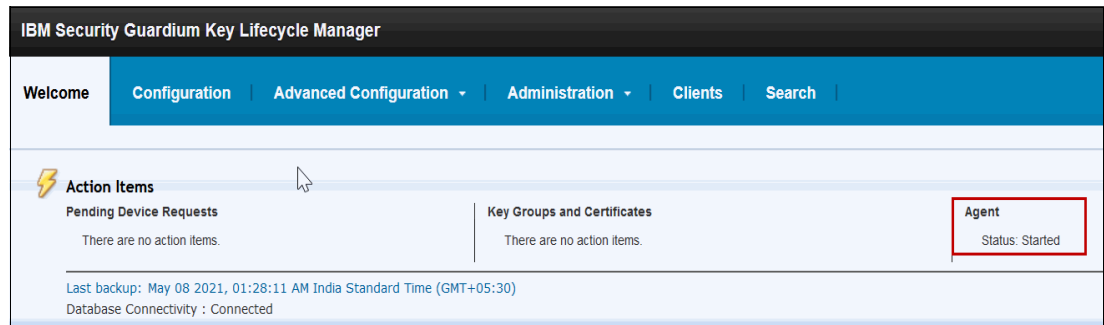


Figure 5-51 Agent Status

Agent service status is disabled by default when you install IBM Security Guardium Key Lifecycle Manager.

The notification area on the Welcome page also indicates whether the Agent certificate expired or expires soon, as shown in Figure 5-52.

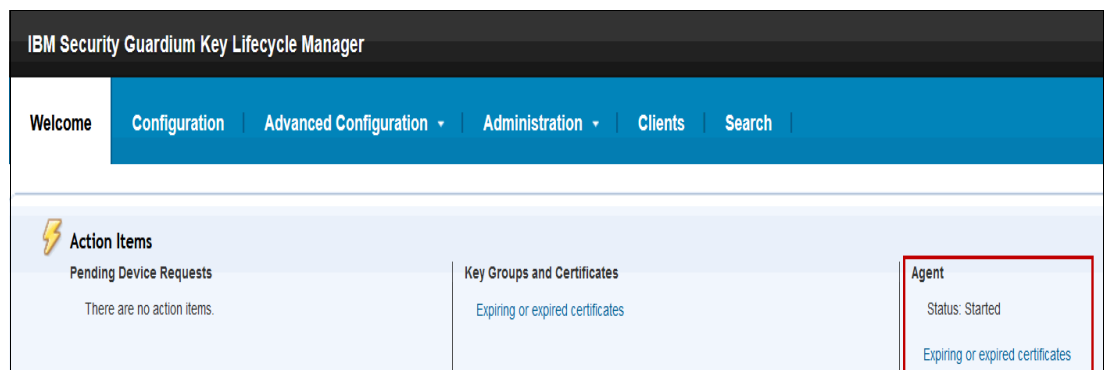


Figure 5-52 Agent Certificate Expiry Status

2. Click **Expiring or expired certificates** to see which certificate expired or is to expire soon.

5.4.4 HADR takeover scenarios

This section describes the takeover scenarios that are listed in Table 5-1. It also explains the Multi-Master behavior starting with version 4.1.0.1, where Auto takeover is no longer supported.

Table 5-1 HADR takeover scenarios

Primary agent	Primary database	Principal standby agent	Principal standby database	Manual takeover
Up	Down	Up	Up	Yes, if required for write operations. Promote the principal Standby server to Primary.
Down or unreachable	Down or unreachable	Up	Up	
Down	Down or unreachable	Up or Down	Down or unreachable	Promote an auxiliary Standby server (if it exists) to Primary.

For more information about how to recover a cluster from a read-only state see, [Recovering Multi-Master cluster from read-only state](#).

Primary database down

This section describes the primary database down scenario, as shown in Figure 5-53.

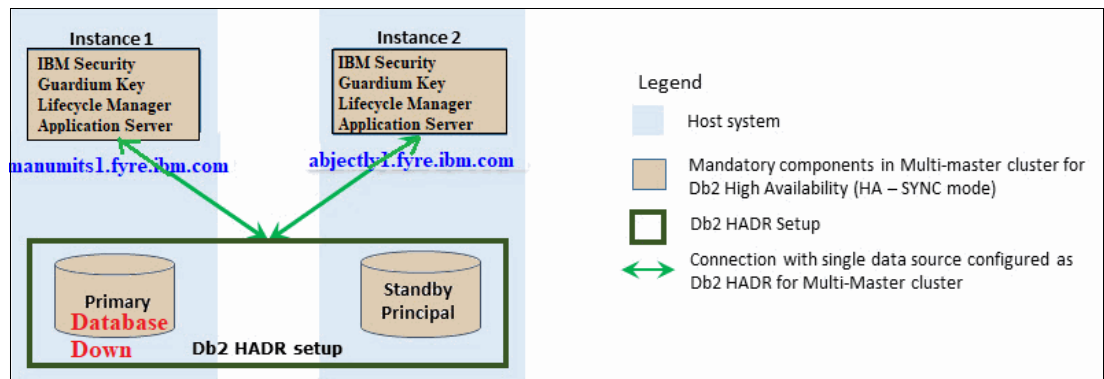


Figure 5-53 Primary database down

When the primary database is unreachable, the cluster goes in read-only state. This state ensures that key serving is not affected.

You can confirm that the standby database is connected in read-only state from the **Welcome** → **Multi-Master** section on the IBM Security Guardium Key Lifecycle Manager graphical user interface, as shown in Figure 5-54.

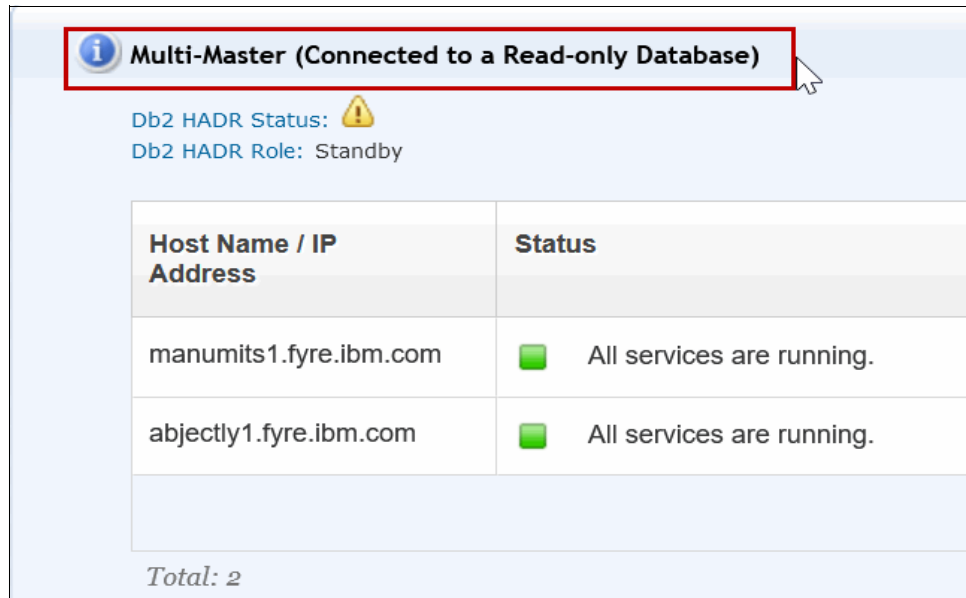


Figure 5-54 Multi-Master cluster read-only state

In this state, the entire cluster remains in read-only mode and no new crypto objects can be created. Created crypto objects can continue to be served.

Note: Do not perform any takeover operations until it is known that you cannot recover the original primary server.

If any takeover operations are not performed, the cluster remains operating in read-only mode and your key serving is not affected. You can wait for the database of the primary master server to be reachable again so that the cluster restores its healthy state.

Primary server down or connection is lost between primary and standby servers

This section describes the primary server down scenario, as shown in Figure 5-55.

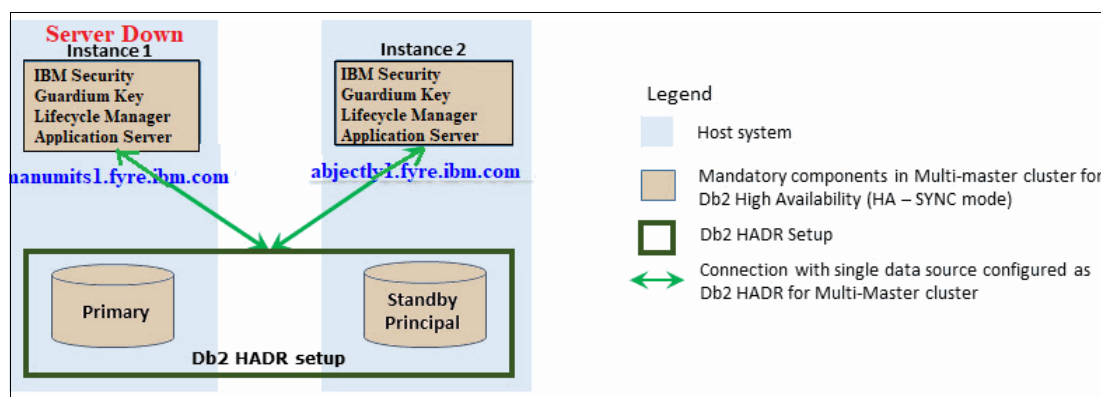


Figure 5-55 Multi-Master primary server down

Consider the following points:

- ▶ When the primary server is unreachable or down, the cluster operates in read-only state. Auto Takeover is not applicable starting with GKLM V4.1.0.1.
- ▶ After the network between the primary server and principal standby is restored or the primary server is brought up, the cluster becomes healthy and recovers from read-only state.
- ▶ If the primary server is unavailable or unreachable for a longer duration, and write operations must be performed on the cluster, the principal standby server must be promoted as primary.

Run the following command to promote the current principle standby server to become new primary by using the `sklmTakeoverHADR.sh/.bat` script, as shown in Example 5-4.

Example 5-4 Promote principal standby to primary

Run the `sklmTakeover.sh` script on the principal standby server.

```
[root@abjectly1 agent]# ./sklmTakeoverHADR.sh /opt/IBM/WebSphere/AppServer/HADR Takeover successful.
```

Verify the standby server is promoted to primary, using the following command:

```
[sklmbd41@abjectly1 ~]$ db2pd -d sklmbd41 -hadr
Database Member 0 -- Database SKLMBD41 -- Active -- Up 3 days 21:53:03 -- Date
2021-05-10-23.25.50.671871
```

```

HADR_ROLE = PRIMARY
REPLAY_TYPE = PHYSICAL
HADR_SYNCMODE = SYNC
STANDBY_ID = 1
LOG_STREAM_ID = 0
HADR_STATE = DISCONNECTED
HADR_FLAGS =
PRIMARY_MEMBER_HOST = abjectly1.fyre.ibm.com
PRIMARY_INSTANCE = sklmbd41
PRIMARY_MEMBER = 0
STANDBY_MEMBER_HOST = manumits1.fyre.ibm.com
STANDBY_INSTANCE = sklmbd41
STANDBY_MEMBER = 0

```

```
HADR_CONNECT_STATUS = DISCONNECTED
output omitted.....
```

Note: The HADR state shows disconnected because the primary master server in the cluster is still unreachable.

- ▶ After the connectivity is restored, the original primary server is reachable again, and the principal standby server is promoted as primary, the Multi-Master cluster must be recovered from a possible split-cluster scenario. For more information, see [this IBM Support web page](#).

5.5 Integrating LDAP with IBM Security Guardium Key Lifecycle Manager Traditional Edition by using configuration scripts

You can integrate LDAP with IBM Security Guardium Key Lifecycle Manager by using LDAP configuration scripts. The configuration scripts also take the backup of IBM WebSphere configuration and IBM Security Guardium Key Lifecycle Manager data.

The following data might need to be restored to the state it was before the LDAP configuration steps were run:

- ▶ IBM WebSphere Application Server configuration data for IBM Security Guardium Key Lifecycle Manager
- ▶ IBM Security Guardium Key Lifecycle Manager application data

5.5.1 Preparing for the configuration

Complete the following steps to prepare for running the LDAP configuration scripts:

1. Log on to the server where IBM Security Guardium Key Lifecycle Manager is installed, and open the `config.py` file under `SKLM_INSTALL_HOME\bin\LDAPIntegration`. `SKLM_INSTALL_HOME` points to following directories:
 - Windows: `C:\Program Files\IBM\SKLMV41`
 - Linux: `/opt/IBM/SKLMV41/`
2. Edit the `config.py` file to add values to properties, such as `ip` (the IP address of the LDAP server), `port` (the port to connect to LDAP server), `LDAP_server_type` (the type of LDAP server, such as IDS), and `base_entry` (distinguished name of the base entry), as shown in Example 5-5.

Example 5-5 Editing the config.py file

```
[root@manumits1 bin]# cat /opt/IBM/SKLMV41/bin/LDAPIntegration/config.py
import string, sys
LDAP_server_type="IDS"
login_id="uid"
ip="ldapservers.company.com"
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=company.com"
scope="direct"
backupPassword="Change@Password123"
```

Note: Make sure to change the value for property in backupPassword. This password is used while creating the IBM Security Guardium Key Lifecycle Manager application backup.

5.5.2 LDAP configuration database and updating the data source for WIM

To create the database for the LDAP configuration and update the data source for WebSphere Identity Manager (WIM), complete the following steps:

1. Create the database for the LDAP configuration (example: USERDB41) and connect to USERDB41 to verify successful creation, as shown in Example 5-6.

Example 5-6 Creating the database

```
[root@manumits1 LDAPIntegration]# su - sklmb41
[sklmb41@manumits1 ~]$ db2 create database USERDB41 using codeset UTF-8
territory US
DB20000I The CREATE DATABASE command completed successfully.
[sklmb41@manumits1 ~]$ db2 connect to USERDB41
Database Connection Information
Database server      = DB2/LINUX8664 11.5.4.0
SQL authorization ID = SKLMB41
Local database alias = USERDB41

[sklmb41@manumits1 ~]$ db2 connect reset
DB20000I The SQL command completed
successfully.
```

- Log on to the WebSphere Integrated Solutions Console as wasadmin and select **Resource** → **JDBC** → **Data Sources** → **WIM Data Source** to update the data source, as shown in Figure 5-56.

WebSphere software Welcome wasadmin

View: All tasks

Resources

- Schedulers
- Object pool managers
- Java EE default resources
- JMS
- JDBC
 - JDBC providers
 - Data sources**
 - Data sources (V4 - deprecated)
- Resource Adapters
- Concurrency
- Cache instances
- Mail
- URL
- Resource Environment

with connections for accessing the database. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

Scope: =All scopes

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

All scopes

Preferences

New... Delete Test connection Manage state...

Select	Name	JNDI name	Scope	Provider	Description	Category
<input type="checkbox"/>	DefaultApp Datasource	DefaultDatasource	Node=SKLMNode,Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application	
<input type="checkbox"/>	SKLM Alternate XA Datasource	jdbc/sklmAltXADS	Node=SKLMNode,Server=server1	SKLM XA DB2 JDBC Provider	SKLM Alternate XA Datasource	
<input type="checkbox"/>	SKLM DataSource	jdbc/sklmDS	Node=SKLMNode,Server=server1	SKLM non-XA DB2 JDBC Provider	SKLM DataSource	
<input type="checkbox"/>	SKLM scheduler XA Datasource	jdbc/sklmXADS	Node=SKLMNode,Server=server1	SKLM XA DB2 JDBC Provider	SKLM scheduler XA Datasource	
<input type="checkbox"/>	WIM Data Source	jdbc/wimXADS	Node=SKLMNode,Server=server1	SKLM XA DB2 JDBC Provider	WIM Data Source	

Figure 5-56 Updating WIM Datasource

3. Update the database name from SKLMDB41 to USERDB41, as shown in Figure 5-57.

The screenshot shows the WebSphere software configuration console. The left sidebar contains a tree view with the following structure:

- View: All tasks
- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
 - Schedulers
 - Object pool managers
 - Java EE default resources
 - JMS
 - JDBC
 - JDBC providers
 - Data sources
 - Data sources (V4 - deprecated)
 - Resource Adapters
 - Concurrency
 - Cache instances
 - Mail
 - URL
 - Resource Environment
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

The main panel is titled 'Data store helper class name' and 'Security settings'. The 'Data store helper class name' section has two radio buttons: 'Select a data store helper class' (selected) and 'Specify a user-defined data store helper'. The 'Select a data store helper class' section shows a list of data store helper classes provided by WebSphere Application Server:

- DB2 Universal data store helper (com.ibm.websphere.rsadapter.DB2UniversalDataStoreHelper)
- DB2 for iSeries data store helper (com.ibm.websphere.rsadapter.DB2AS400DataStoreHelper)

The 'Security settings' section has four dropdown menus for authentication aliases:

- Authentication alias for XA recovery: (none)
- Component-managed authentication alias: sklm_db
- Mapping-configuration alias: (none)
- Container-managed authentication alias: sklm_db

The 'Common and required data source properties' section contains a table with the following data:

Name	Value
Driver type	4
Database name	USERDB41
Server name	127.0.0.1
Port number	50070

Figure 5-57 Updating database name in WIM Datasource

4. Click **Apply** and then, **Save** to save the configuration changes.

5. Select the **WIM Data Source** and click **Test Connection** to ensure the connection is working, as shown in Figure 5-58.

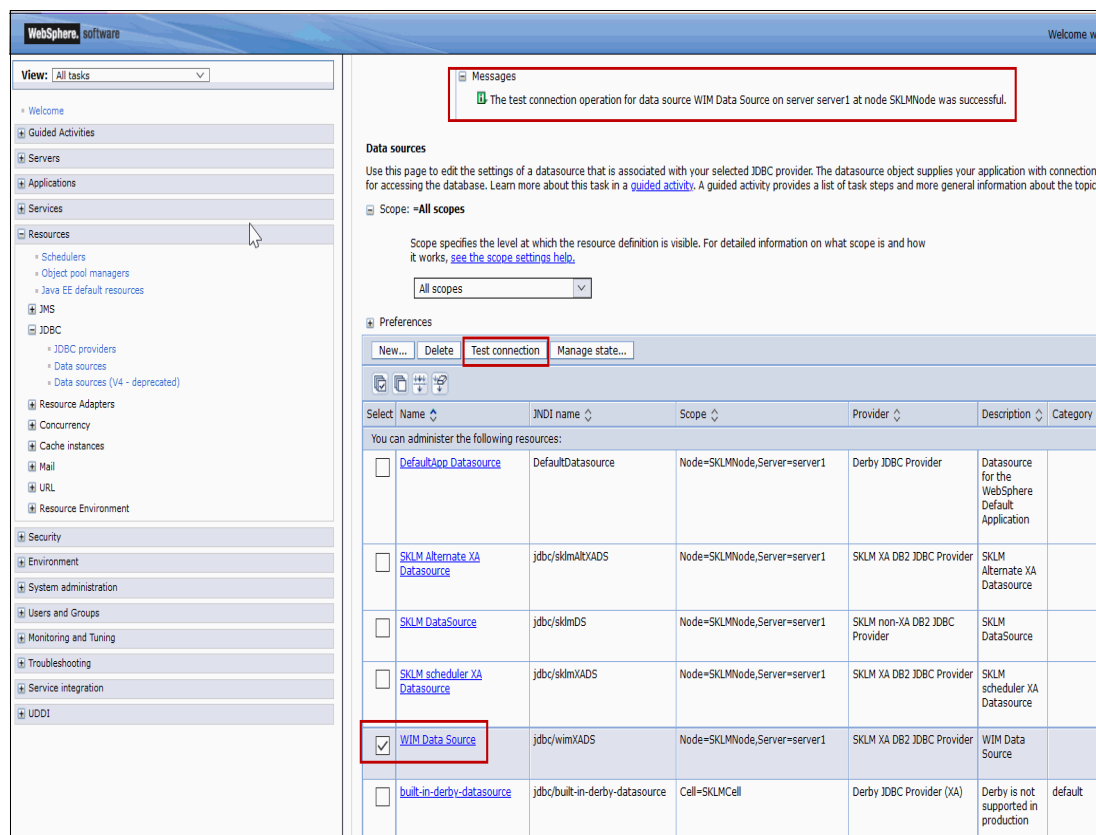


Figure 5-58 Test Connection with WIM Data Source

6. Copy the Db2 driver and license to the WAS_HOME/lib folder, as shown in Example 5-7.

Example 5-7 Copying the essential Db2 drivers

```
[root@manumits1 bin]# cp /opt/IBM/DB2SKLMV41/java/db2jcc*
/opt/IBM/WebSphere/AppServer/lib
[root@manumits1 bin]# ls -al /opt/IBM/WebSphere/AppServer/lib/db2jcc*
-rwxr-x--- 1 root root 6568346 May 13 16:02
/opt/IBM/WebSphere/AppServer/lib/db2jcc4.jar
-rwx----- 1 root root 3618758 May 13 16:02
/opt/IBM/WebSphere/AppServer/lib/db2jcc.jar
-rwxr-x--- 1 root root 1534 May 13 16:02
/opt/IBM/WebSphere/AppServer/lib/db2jcc_license_cu.jar
```

Note: Make sure the db2jcc* jars under the WAS_HOME/lib directory have the Db2 admin (sklmb41) as the owner of the files.

5.5.3 Creating a database-based repository

To create a database-based repository, complete the following steps:

1. Open the file `soap.client.props`, and edit the `com.ibm.SOAP.requestTimeout` property (the default value of `com.ibm.SOAP.requestTimeout` is 360). Then, change the value to 0, as shown in Example 5-8.

Example 5-8

```
[root@manumits1 LDAPIntegration]# cat
/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/properties/soap.client.props |
grep com.ibm.SOAP.requestTimeout
com.ibm.SOAP.requestTimeout=0
```

2. Restart the WebSphere server, as shown in Example 5-9

Example 5-9 Restart the WebSphere Application Server

```
[root@manumits1 bin]# /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
-username wasadmin -password Change@Password123
ADMU0116I: Tool information is being logged in file

/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the KLMProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.

[root@manumits1 bin]# /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
ADMU0116I: Tool information is being logged in file

/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/startServer.log
ADMU0128I: Starting tool with the KLMProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server server1 open for e-business; process id is 52786
```

3. Run the command to create a database-based repository that is shown in Example 5-10.

Example 5-10 Creating a database-based repository

```
[root@manumits1 LDAPIntegration]# pwd
/opt/IBM/SKLMV41/bin/LDAPIntegration
[root@manumits1 bin]# ./wsadmin.sh -username wasadmin -password Change@Password123
-lang jython -f /opt/IBM/SKLMV41/bin/LDAPIntegration/createdBRepos.py
/opt/IBM/WebSphere/AppServer/ USERDB41 sklmdb41 Change@Password123 50070
WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector;
The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment and are
available as arguments that are stored in the argv variable:
"/opt/IBM/WebSphere/AppServer/, USERDB41, sklmdb41, G@KdLbM2, 50070]"
washome=/opt/IBM/WebSphere/AppServer/
Creating DB Repository Tables in SKLM DB..

Created DB Repository Tables in SKLM DB..
Creating DB Repository..
```

CWWIM5046W Each configured repository must contain at least one base entry. Add a base entry before saving the configuration. For LDAP repository, add the LDAP server before adding the base entry.

Created DB Repository - SKLMDBRepos...CWWIM5046W Each configured repository must contain at least one base entry. Add a base entry before saving the configuration. For LDAP repository, add the LDAP server before adding the base entry.

Adding DB Repository base entry...

CWWIM5028I The configuration is saved in a temporary workspace. You must use the "\$AdminConfig save" command to save it in the master repository.

Added DB Repository base entry - o=sklmrepdb.ibm...CWWIM5028I The configuration is saved in a temporary workspace. You must use the "\$AdminConfig save" command to save it in the master repository.

Adding base entry to realm...

CWWIM5028I The configuration is saved in a temporary workspace. You must use the "\$AdminConfig save" command to save it in the master repository.

Added base entry to realm - o=sklmrepdb.ibm...CWWIM5028I The configuration is saved in a temporary workspace. You must use the "\$AdminConfig save" command to save it in the master repository.

Saving Config...

4. Verify that the database-based repository was created and listed in the realm, as shown in Figure 5-59.

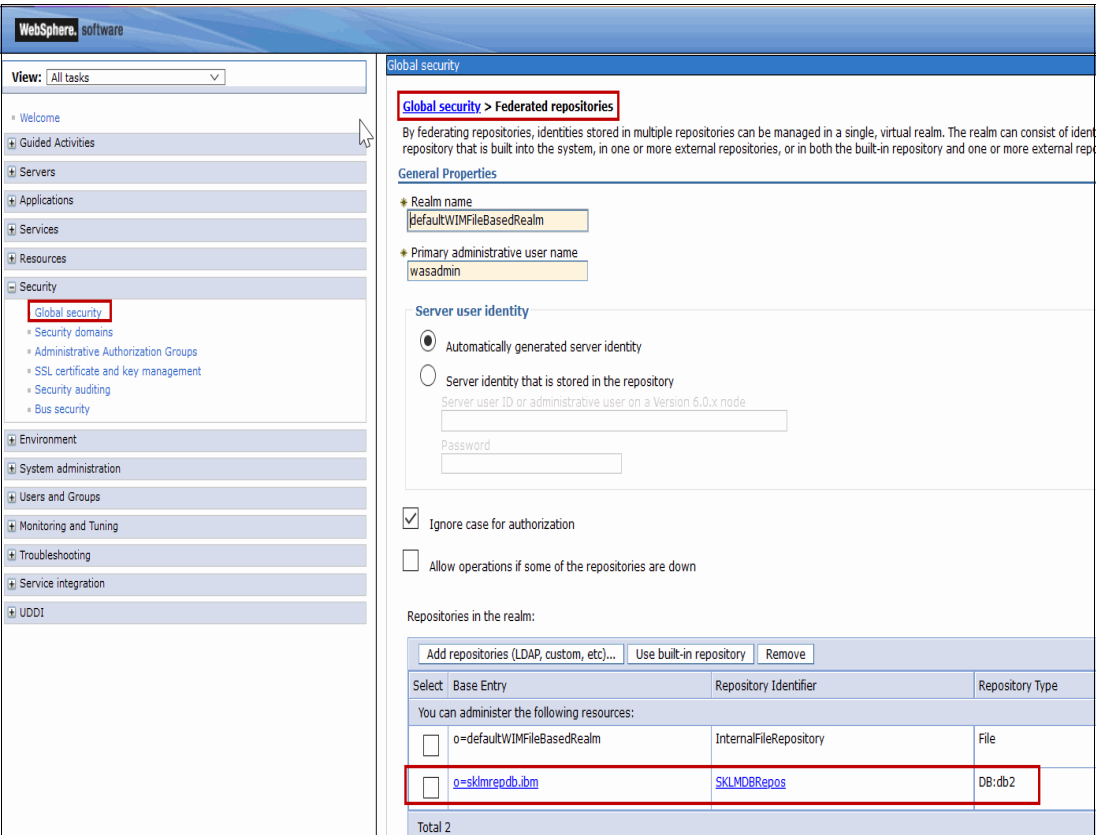


Figure 5-59 Repositories in the realm

5. Run the `sklmLDAPConfigure.sh` script to configure the IBM Security Guardium Key Lifecycle Manager (GKLM) with the LDAP server, as shown in Example 5-11. This script also removes the GKLM application groups from the file-based repository and adds them to database-based repository. It also updates the IBM WebSphere federated repository with the LDAP-based repository. Finally, the script maps the administrator role to `klmGUICLIAccessGroup` for integrating IBM GKLM with LDAP user repositories.

Example 5-11 Configuring with LDAP server

```
[root@manumits1 bin]# cd /opt/IBM/SKLMV41/bin/LDAPIntegration/
[root@manumits1 LDAPIntegration]# ./sklmLDAPConfigure.sh
"/opt/IBM/WebSphere/AppServer" "/opt/IBM/SKLMV41" wasadmin
Change@Password123Change@Password123 sklmadmin
Change@Password123Change@Password123 "/opt/IBM/DB2SKLMV41"
Stopping WAS
Backup KLMPProfile..
Starting WAS
SKLM Backup started
SKLM Backup Finished
LDAP Configuration Started..
LDAP Configuration Ends..
Restarting WAS...
Removing Groups from File Based Repository..
Groups removed from file based repository..
Modify Security Role to User/group mapping to remove the administrator role
mapping to klmGUICLIAccessGroup..
Restarting WAS...
Add the SKLM Application groups to database based repository..
update the WAS federated repository with LDAP repository..
Add Security Role to User/group mapping and map administrator role to
klmGUICLIAccessGroup ..
Restarting WAS...
```

6. The `sklmLDAPConfigure.sh` script also creates a backup of IBM WebSphere Application Server configuration data and IBM Security Guardium Key Lifecycle Manager application data at `SKLM_DATA`, as shown in Example 5-12.

Example 5-12 WebSphere and IBM Security Guardium Key Lifecycle Manager backups

WebSphere profile backup:

```
[root@manumits1 /]# ls -al
/opt/IBM/WebSphere/AppServer/products/sklm/data/WASProfile*
-rw-r--r-- 1 root root 133068355 May 13 16:46
/opt/IBM/WebSphere/AppServer/products/sklm/data/WASProfile_Backup
```

IBM Security Guardium Key Lifecycle Manager backup:

```
[[root@manumits1 /]# ls -al /opt/IBM/WebSphere/AppServer/products/sklm/data/sklm_*
-rw-r--r-- 1 sklmb41 sklmb41 49706 May 13 16:51
/opt/IBM/WebSphere/AppServer/products/sklm/data/sklm_v4.1.0.1_20210513165151+0530_
backup.jar
```

7. Verify that the IBM Security Guardium Key Lifecycle Manager is configured with the LDAP server from the IBM WebSphere Integrated Console, as shown in Figure 5-60.

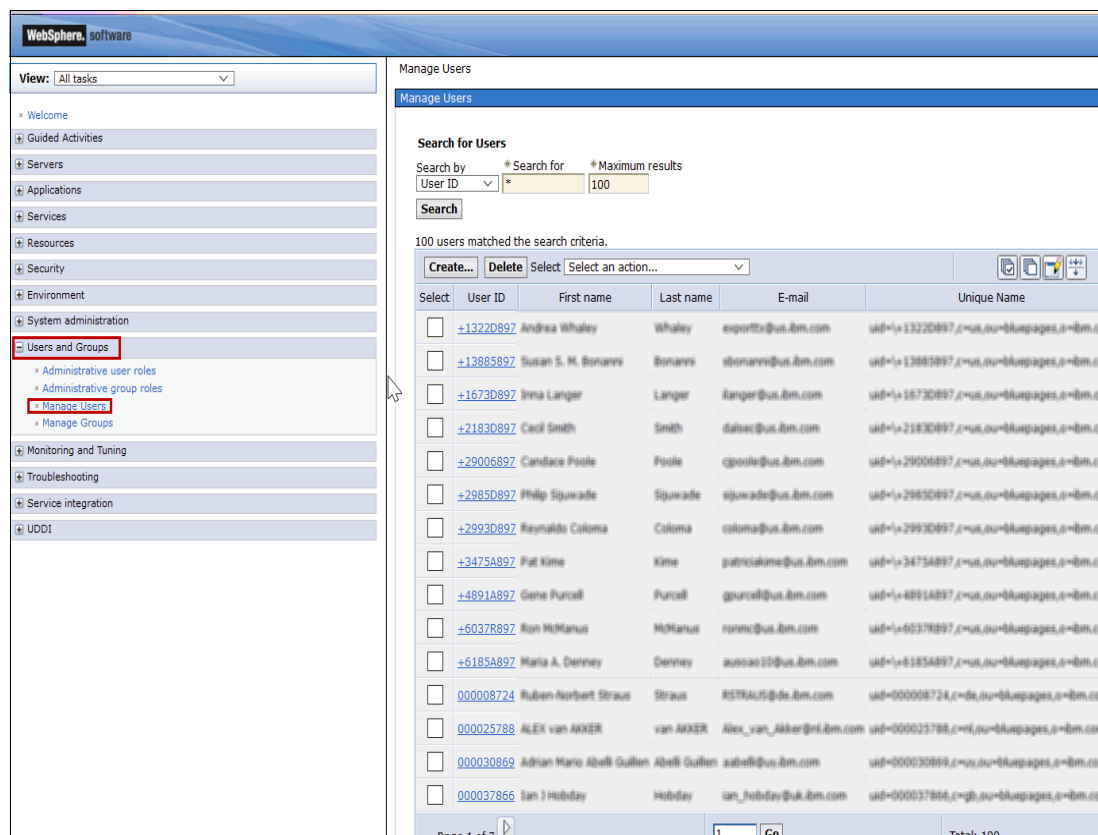


Figure 5-60 Verify LDAP configuration

8. For any LDAP users and groups that need IBM Security Key Lifecycle Manager admin access, the user also must be made a member of `klmSecurityOfficerGroup`, as shown in Example 5-13.

Example 5-13 Adding LDAP users and groups to `klmSecurityOfficerGroup`

```
[root@manumits1 LDAPIntegration]# ./addLDAPUserToGroup.sh
"/opt/IBM/WebSphere/AppServer" "/opt/IBM/SKLMV41" wasadmin Change@Password123
"uid=067195744,c=in,ou=ldapservers,o=company.com" skladmin Change@Password123
```

9. Log on to the IBM Security Guardium Key Lifecycle Manager portal with the configured LDAP account to verify the configuration, as shown in Figure 5-61.

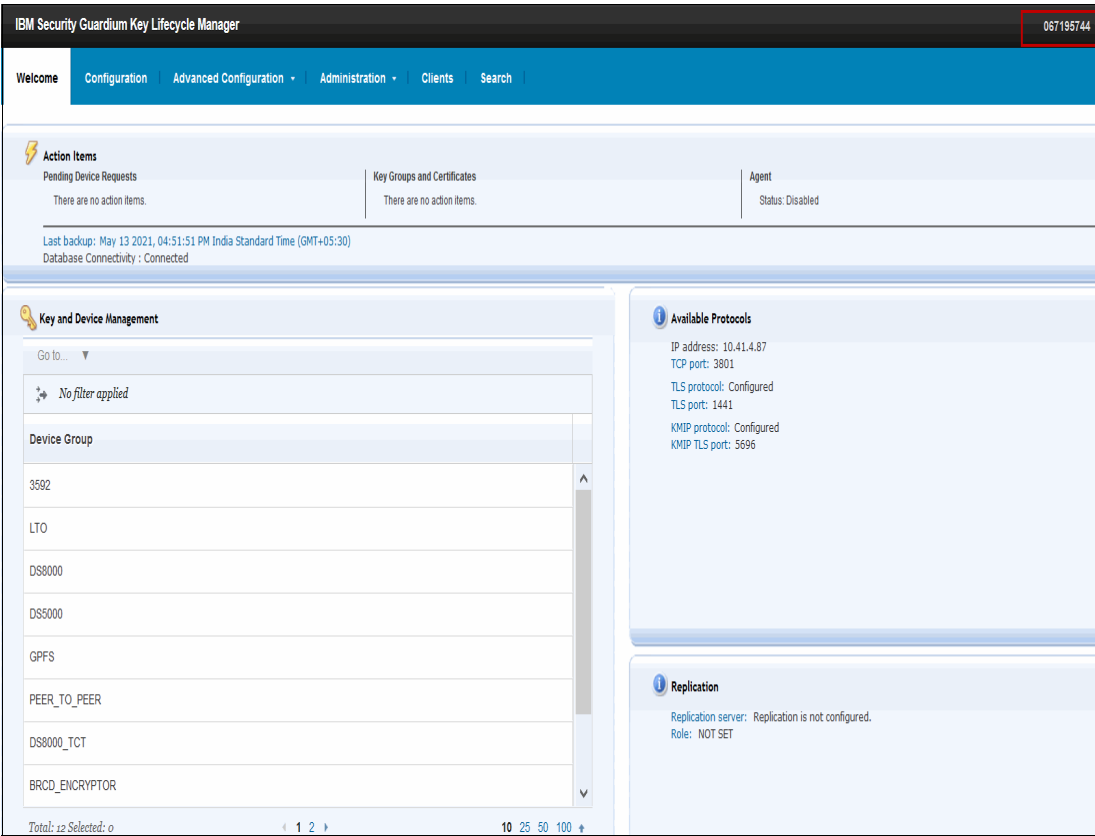


Figure 5-61 Logging on to the IBM Security GKLM portal by using an LDAP account

5.6 Integrating LDAP with IBM Security Guardium Key Lifecycle Manager Container Edition

Complete the following steps to configure IBM Security Guardium Key Lifecycle Manager containerized edition to use the Lightweight Directory Access Protocol (LDAP) for user authentication:

1. Log in to the IBM Security Guardium Key Lifecycle Manager portal, click **User Management** tab, as shown in Figure 5-62.

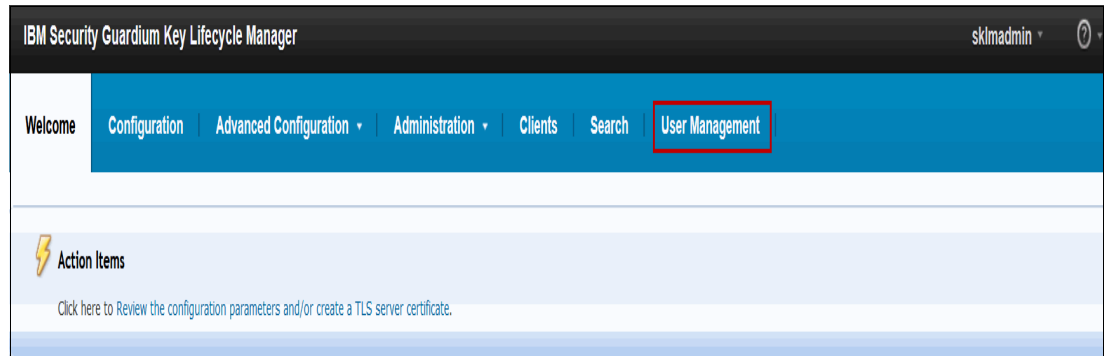


Figure 5-62 IBM Security Guardium Key Lifecycle Manager Containerized Edition portal

2. In the User Management window, click **Configuration** and then, click **Update**, as shown in Figure 5-63.

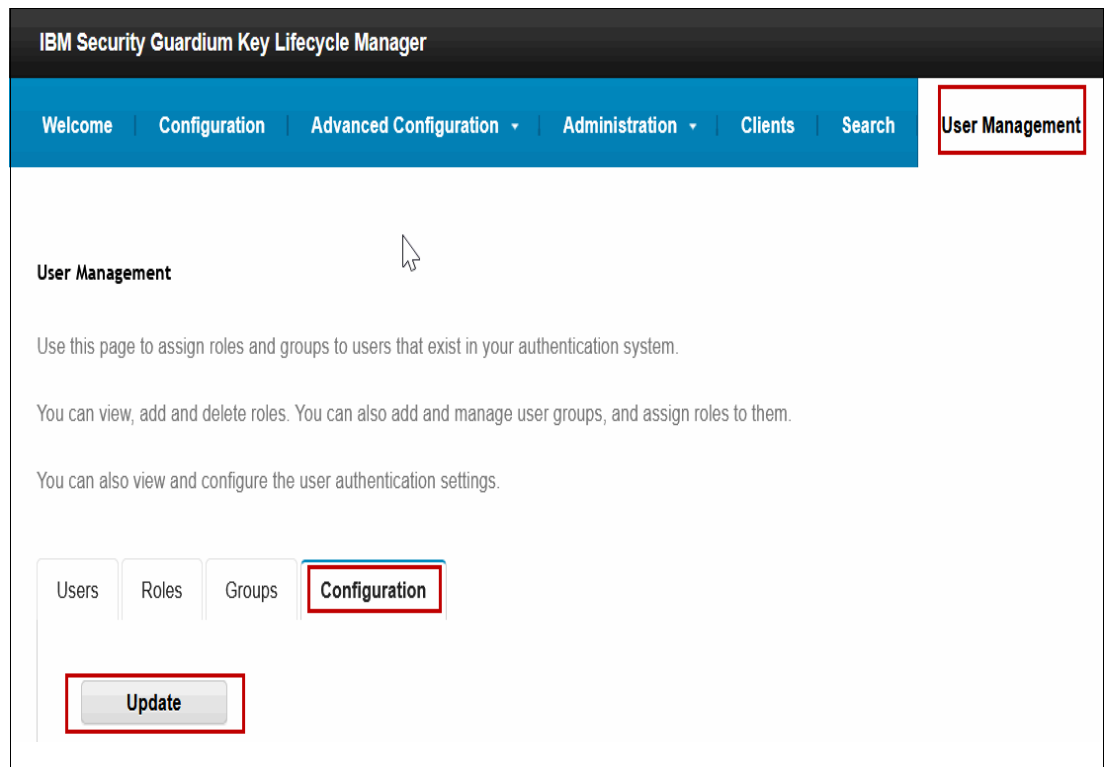


Figure 5-63 Configuring LDAP

3. Configure LDAPUser Authentication by clicking the **LDAP Authentication** tab. Select the **Enable LDAP-based Authentication** option. Enter all of the information about the LDAP server, such as the LDAP Server type, LDAP Host, port, Base Entry, as shown in Figure 5-64. Then, click **Update**.

Figure 5-64 Configure User Authentication - Basic configurations

After all if the details are updated, you are logged out of the graphical user interface.

4. Log in to the portal as SKLMAdmin. Then, go to the **User Management** → **Users** tab and click **Add**. Search for the user that must be added as the administrator. Then, select that user and click **Select**, as shown in Figure 5-65.

Figure 5-65 Add User Assignment

5. Assign the correct roles and groups to the LDAP user by selecting the **Assign Roles** and **Assign Groups** tabs.

6. Click **Assign Roles** and assign the klmSecurityOfficer role to the LDAP user, as shown in Figure 5-66.

The screenshot shows the 'Add User Assignment' dialog box with the 'Assign Roles' tab selected. The 'User Name' field is populated with a masked email address. The 'Assigned Roles' section shows 'klmSecurityOfficer' has been assigned. A list of roles is displayed on the left, with 'klmClientUser' selected. A search bar on the right contains 'klmSecurityOfficer'. The 'Save' button is at the bottom.

Add User Assignment

User Name: [masked]@067195744.[masked].com)

Assign Roles

Assigned Roles: klmSecurityOfficer

Search for roles..

klmBackup
klmClientUser
klmConfigure
klmCreate
klmDelete
klmFileTransfer
klmGet
klmModify
klmRestore
klmView

>>
<<

Save

Figure 5-66 Assign Roles

7. Assign the LDAP user to groups, such as klmGUICLIAccessGroup and klmSecurityOfficerGroup, as shown in Figure 5-67. Then, click **Save**. Assigning these groups ensures that the user can access the IBM Security Guardium Key Lifecycle Manager portal. You can assign them to specific groups based on your needs.

The screenshot shows the 'Add User Assignment' dialog box with the 'Assign Groups' tab selected. The 'User Name' field is populated with a masked email address. The 'Assigned Groups' section is empty. A list of groups is displayed on the left, with 'LTOAdmin', 'LTOAuditor', and 'LTOOperator' visible. A search bar on the right contains 'klmBackupRestoreGroup', 'klmGUICLIAccessGroup', and 'klmSecurityOfficerGroup'. The 'Save' button is at the bottom and is highlighted with a red box.

User Name: [masked]@067195744,c-[masked].com)

Assign Groups

Assigned Groups:

Search for groups..

LTOAdmin
LTOAuditor
LTOOperator

>>
<<

Search for groups..

klmBackupRestoreGroup
klmGUICLIAccessGroup
klmSecurityOfficerGroup

Save

Figure 5-67 Assign Group

8. Verify your configuration by logging in to the IBM Security Guardium Key Lifecycle Manager portal by using the LDAP account that is configured as the administrator, as shown in Figure 5-68.

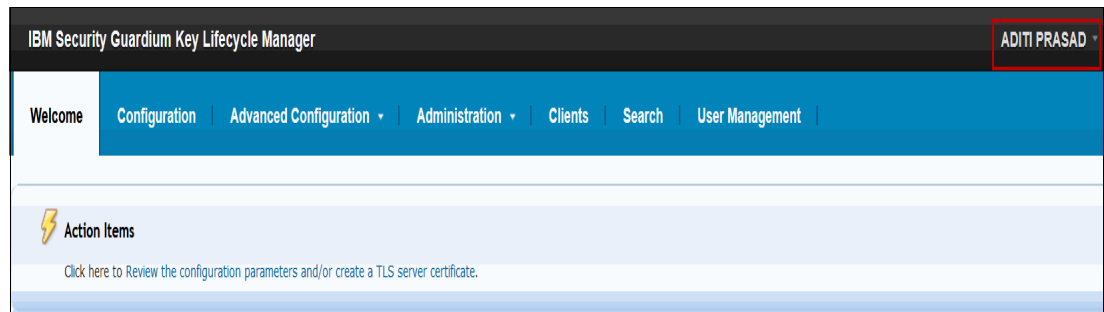


Figure 5-68 Logging on to the Container Edition IBM Security GKLM portal by using LDAP account

9. In the Containerized edition of IBM Security Guardium Key Lifecycle Manager, you can continue to log in by using the SKLMAdmin account (file-based repository). In the Configure User Authentication window, click **File Authentication** and then, select the **Enable File-based Authentication** option, as shown in Figure 5-69.

The screenshot shows the 'Configure User Authentication' window. On the left, there are two tabs: 'File Authentication' (which is selected) and 'LDAP Authentication'. In the 'File Authentication' section, there is a checkbox labeled 'Enable File-based Authentication' which is checked. Below this, there are three text input fields: '*Administrator User Name:' with the value 'skladmin', '*Administrator Password:' with masked characters, and '*Confirm Administrator Password:' with masked characters. At the bottom of the form is an 'Update' button.

Figure 5-69 File-based Authentication

If you do not select the File-based Authentication option, only LDAP accounts are active to log in to the IBM Security Guardium Key Lifecycle Manager.

Note: Unlike in Traditional edition, you can continue to use your SKLMAdmin account to log in to the IBM Security Guardium Key Lifecycle Manager along with the LDAP user account.

5.7 Configuring signed CA certificates for IBM Security Guardium Key Lifecycle Manager portal and IBM WebSphere console access

Before you begin, ensure that you completed the following tasks:

- ▶ Submitted a Certificate Signing Request (CSR) for CA approval in an IBM WebSphere Application Server environment.
- ▶ Received the certificates from the CA.

Complete the following steps:

1. Log on to the IBM WebSphere Integrated Solutions Console (<https://<IP address>:9083/ibm/console/login.do?cell=SKLMCell,Profile=KLMProfile>). Select **Security** and then, **SSL certificate and key management**. Then, select **Key stores and certificates**, as shown in Figure 5-70.

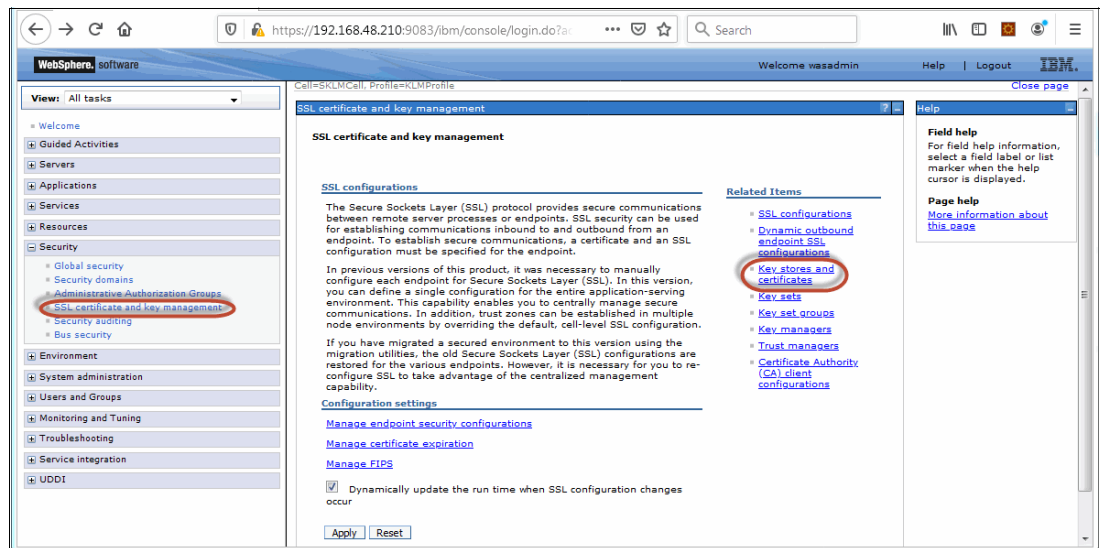


Figure 5-70 Key stores and certificates

2. Select the **NodeDefaultKeyStore** resource, as shown in Figure 5-71.

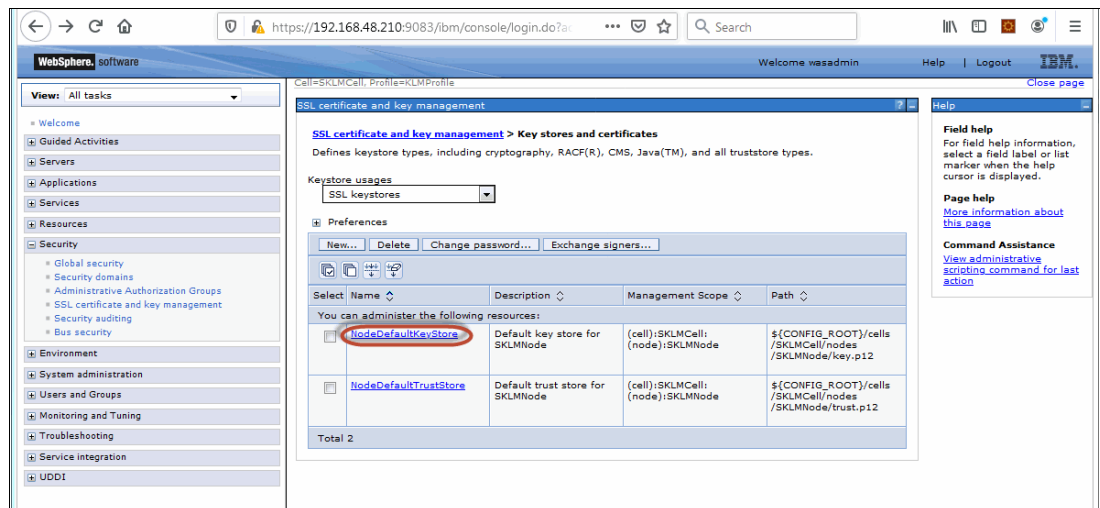


Figure 5-71 Key stores and certificates

3. Select **Personal certificate request** to generate the signing request, as shown in Figure 5-72.

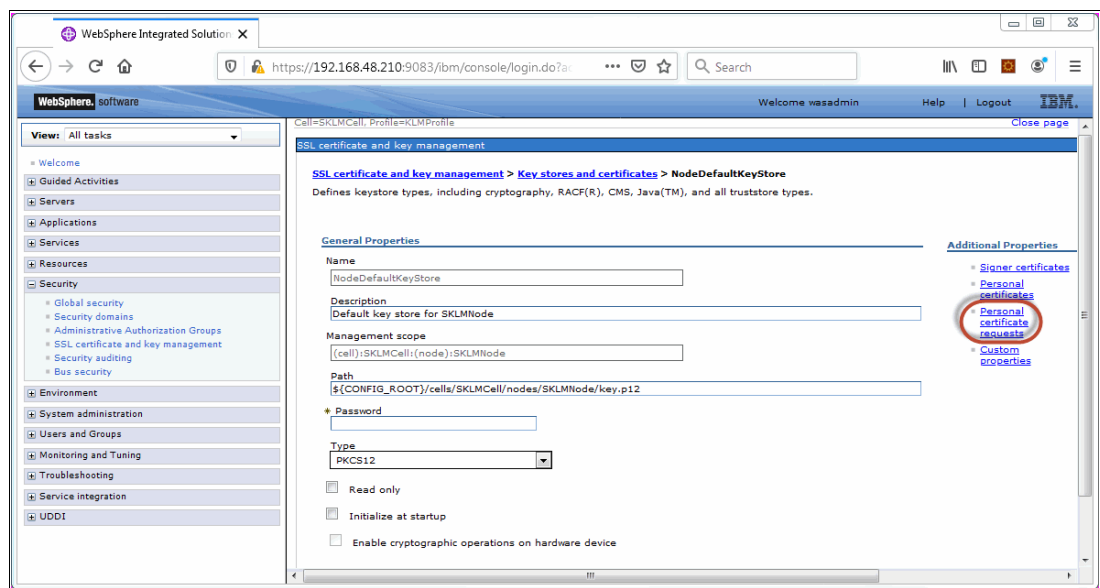


Figure 5-72 Personal certificate requests

4. Click **New** to specify the certificate details, as shown in Figure 5-73.

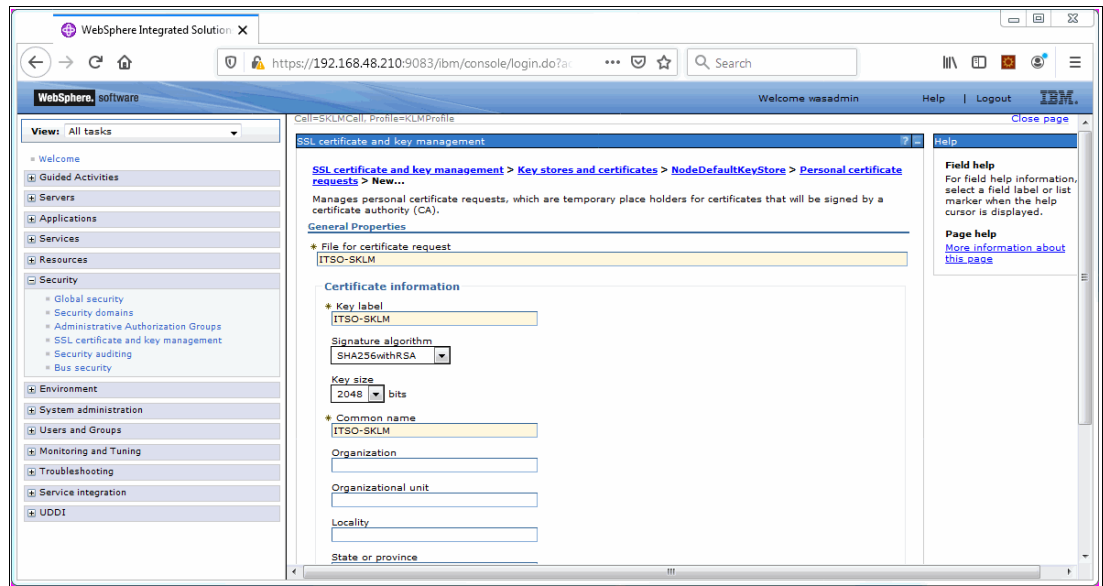


Figure 5-73 Certificate details

The default location for the signing request is <WAS_HOME>/profiles/KLMProfile/etc, as shown in Figure 5-74.

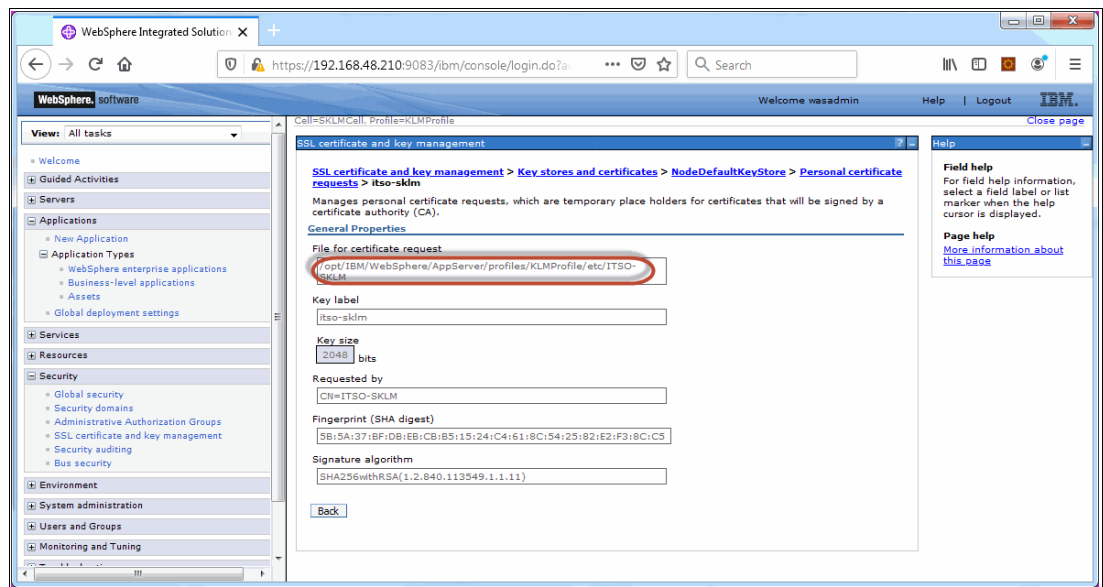


Figure 5-74 Signing Request default location

- Send the request to a signing authority, and upload the signed certificate and the root certificate of the signing authority to the <WAS HOME>/profiles/KLMProfile/etc directory. Then, click **NodeDefaultKeyStore** → **Personal certificates** → **Receive from a certificate authority** to import the signed certificate, as shown in Figure 5-75.

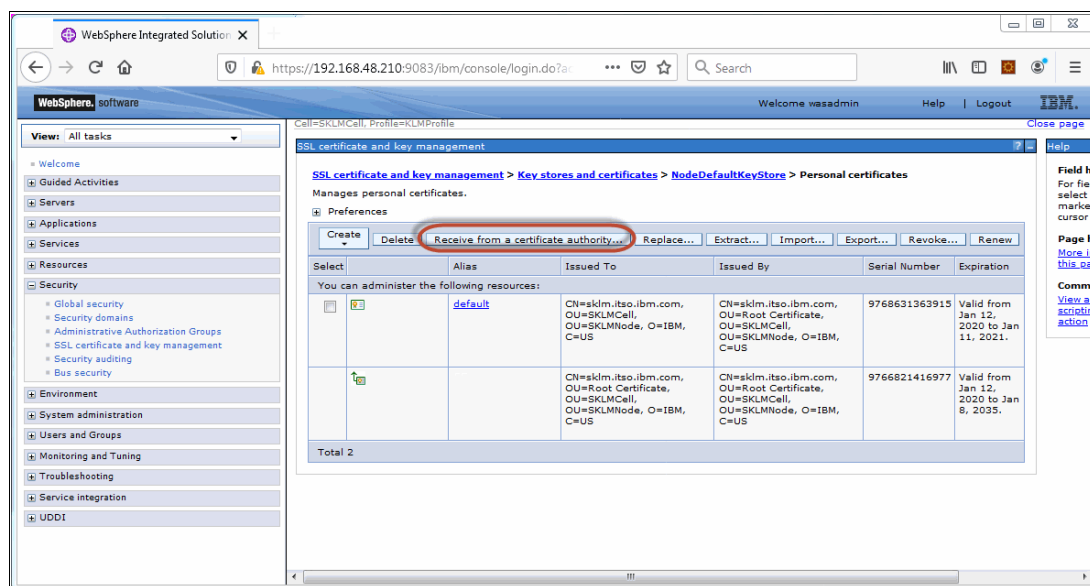


Figure 5-75 Selecting Receive certificate from CA

- Specify the file name of the signed certificate to import. Click **OK** and save the configuration, as shown in Figure 5-76.

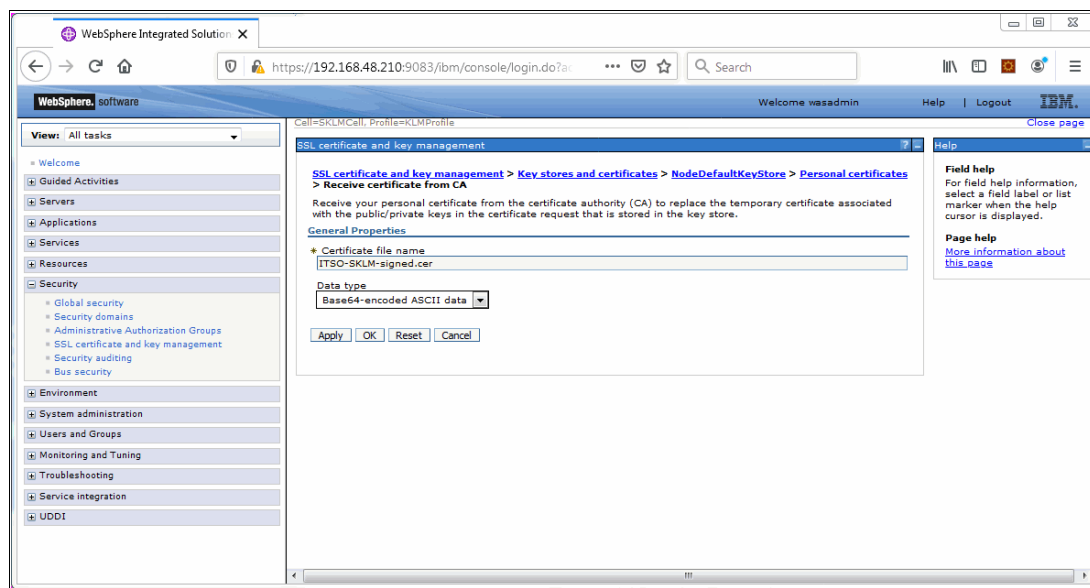


Figure 5-76 Importing the signed certificate

7. Select **NodeDefaultKeyStore** → **Signer certificates** to import the root certificate and intermediate certificates, as shown in Figure 5-77.

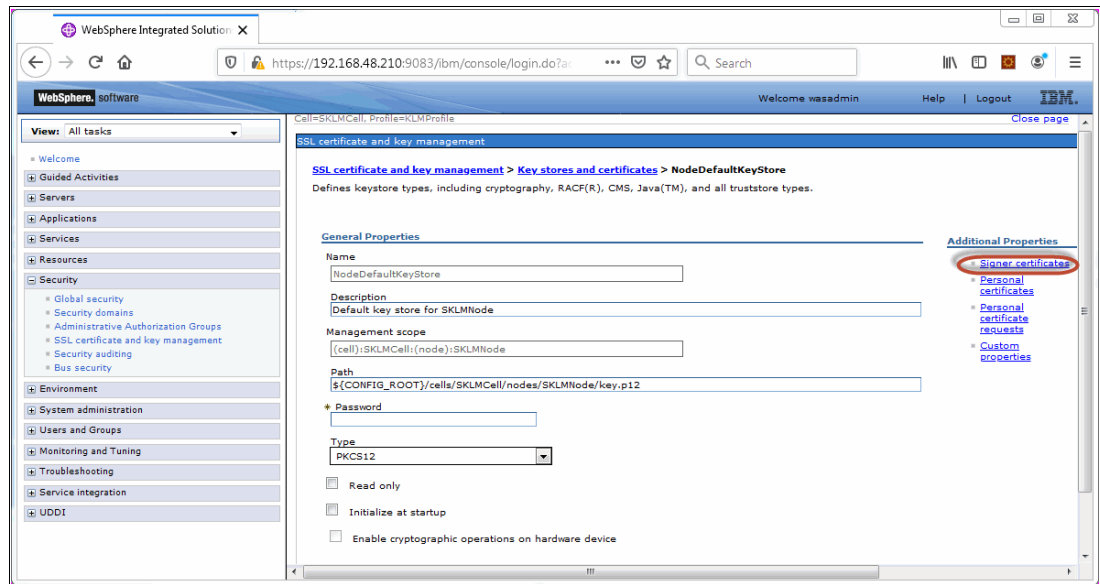


Figure 5-77 Signer certificates

8. Select **Add** and specify the details of the root certificate. Click **OK** and save the configuration, as shown in Figure 5-78.

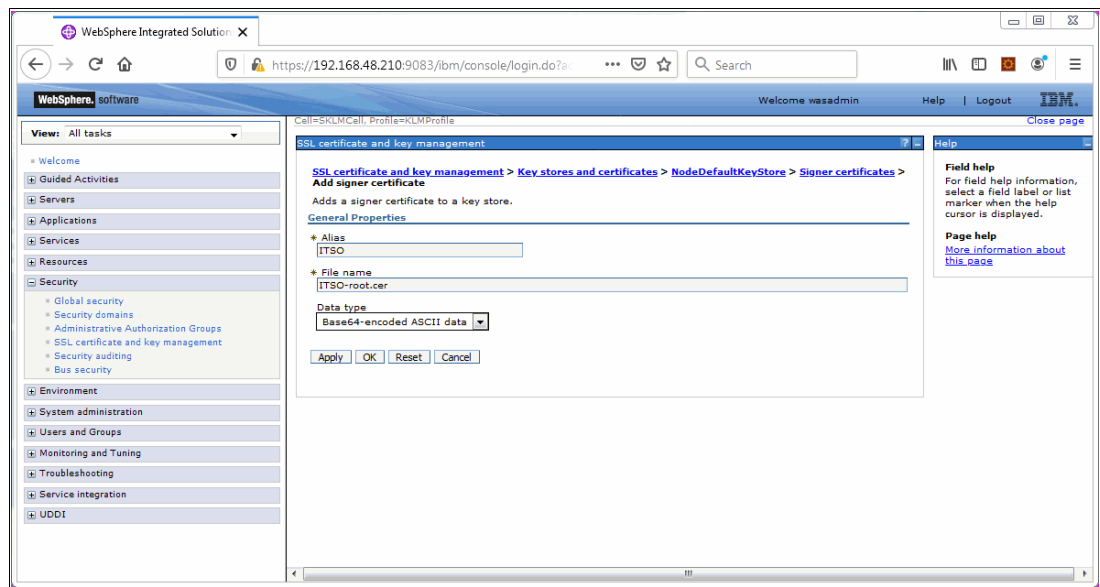


Figure 5-78 Certificate details

9. Select **NodeDefaultKeyStore** → **Personal certificates** to verify that the certificates are imported correctly, as shown in Figure 5-79.

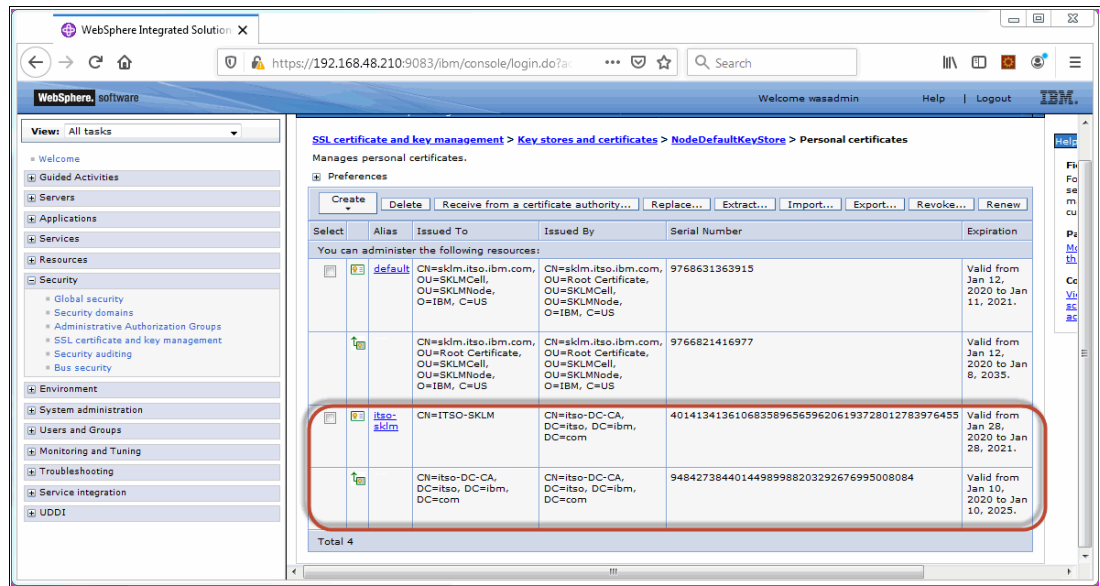


Figure 5-79 Imported certificates

10. Select the default certificate and click **Replace** to replace the default with the signed certificate, as shown in Figure 5-80.

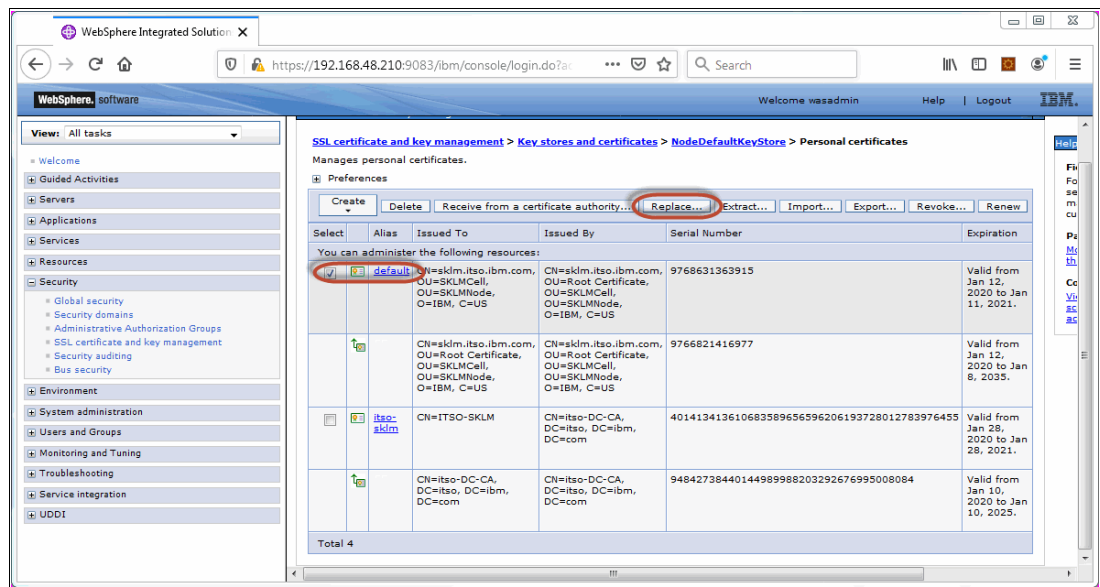


Figure 5-80 Replacing the default certificate

11. Select the certificate from the drop-down menu, click **OK**, and save the configuration, as shown in Figure 5-81.

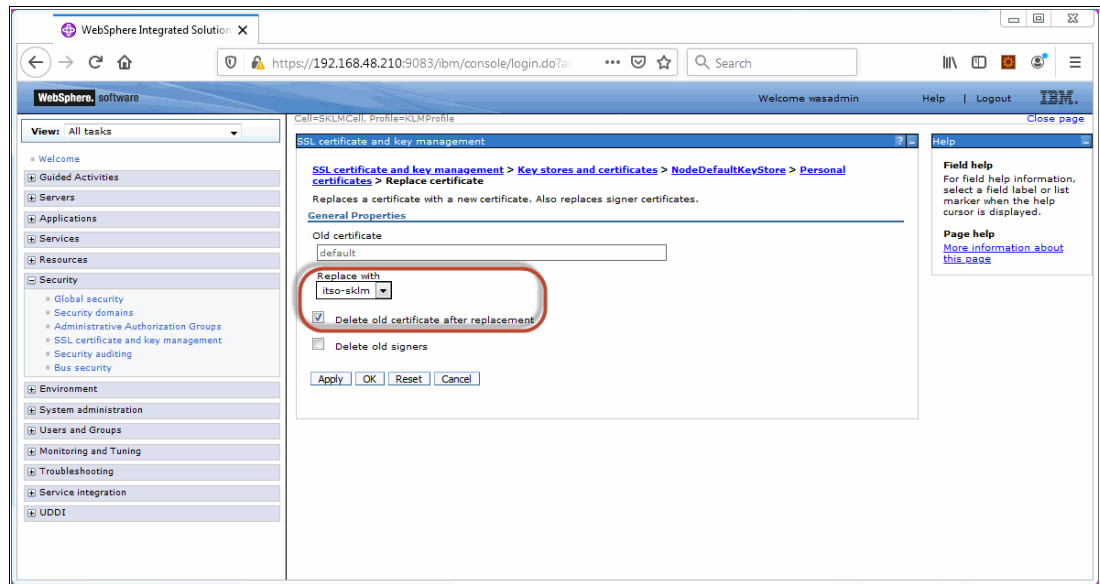


Figure 5-81 Replacement certificate and deleting the old certificate

12. Restart the IBM WebSphere Application Server and add the signer to the trust stores, as shown in Example 5-14.

Example 5-14 Adding the new signer certificate to the trust store

```
[root@sk1m ~]# /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1 -username
wasadmin -password Change@Password123
ADMU0116I: Tool information is being logged in file
```

```
/opt/IBM/WebSphere/AppServer/profiles/KLMPProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the KLMPProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.
```

```
[root@sk1m ~]# /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
ADMU0116I: Tool information is being logged in file
```

```
/opt/IBM/WebSphere/AppServer/profiles/KLMPProfile/logs/server1/startServer.log
ADMU0128I: Starting tool with the KLMPProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server server1 open for e-business; process id is 19702
[root@sk1m ~]# /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1 -username
wasadmin -password Change@Password123
ADMU0116I: Tool information is being logged in file
```

```
/opt/IBM/WebSphere/AppServer/profiles/KLMPProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the KLMPProfile profile
ADMU3100I: Reading configuration for server: server1
```

*** SSL SIGNER EXCHANGE PROMPT ***

SSL signer from target host 192.168.48.210 is not found in truststore
/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/etc/trust.p12.

Here is the signer information (verify the digest value matches what is displayed
at the server):

Subject DN: CN=sklm.itso.ibm.com, OU=ITSO, O=IBM, L=SYD, ST=NSW, C=AU
Issuer DN: CN=itso-DC-CA, DC=itso, DC=ibm, DC=com
Serial number: 401413413669045698007453891124786212800299026
Expires: Fri Jan 29 18:15:49 EST 2021
SHA-1 Digest: 3D:28:D3:BC:33:53:03:79:04:1D:1F:F2:DE:05:4B:9A:5C:80:28:13
MD5 Digest: 47:51:49:3C:9F:82:C4:43:80:82:0D:19:34:AA:A7:2F

Subject DN: CN=itso-DC-CA, DC=itso, DC=ibm, DC=com
Issuer DN: CN=itso-DC-CA, DC=itso, DC=ibm, DC=com
Serial number: 94842738440144989988203292676995008084
Expires: Fri Jan 10 00:21:35 EST 2025
SHA-1 Digest: 3D:28:D3:BC:33:53:03:79:04:1D:1F:F2:DE:05:4B:9A:5C:80:28:13
MD5 Digest: 47:51:49:3C:9F:82:C4:43:80:82:0D:19:34:AA:A7:2F

Add signer to the truststore now? (y/n) y

A retry of the request may need to occur if the socket times out while waiting for
a prompt response. If the retry is required, note that the prompt will not be
redisplayed if (y) is entered, which indicates the signer has already been added
to the truststore.

ADMU3201I: Server stop request issued. Waiting for stop status.

ADMU4000I: Server server1 stop completed.

[root@sklm~]# /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1

ADMU0116I: Tool information is being logged in file

/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/startServer.log

ADMU0128I: Starting tool with the KLMProfile profile

ADMU3100I: Reading configuration for server: server1

ADMU3200I: Server launched. Waiting for initialization status.

ADMU3000I: Server server1 open for e-business; process id is 20182

13. Open the browser to verify that the connection is secured, as shown in Figure 5-82.

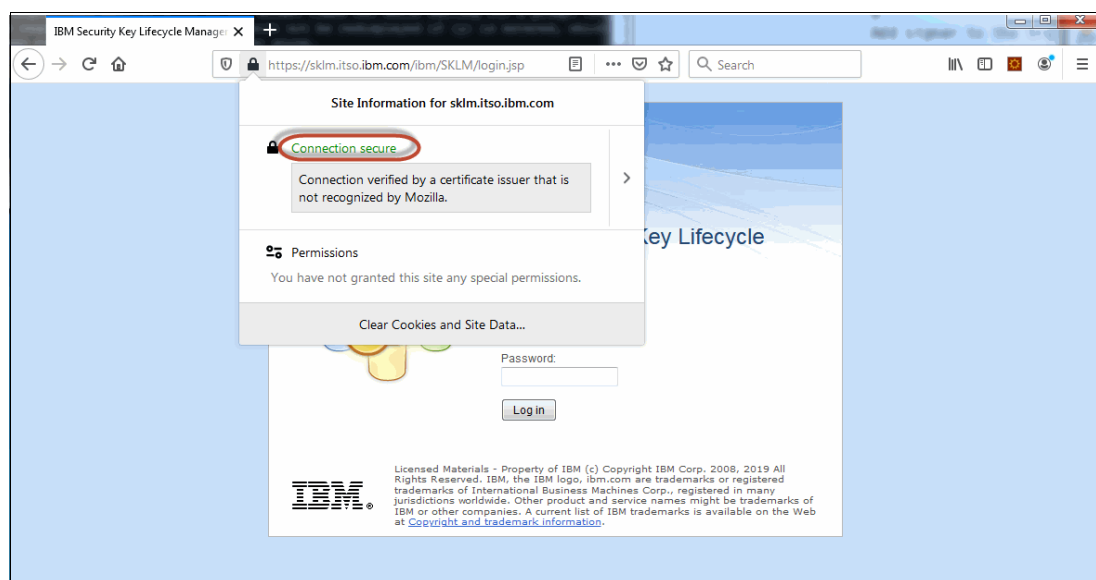


Figure 5-82 Verifying the connection

Related publications

The publications that are listed in this section are considered suitable for a more detailed description of the topics that are covered in this book.

IBM Redbooks

The following IBM Redbooks publication provides more information about the topics in this book:

IBM DS8000 Encryption for data at rest, Transparent Cloud Tiering, and Endpoint Security (DS8000 Release 9.0), REDP-4500

You can search for, view, download, or order this document and other Redbooks, Redpapers, web docs, drafts, and additional materials, at the following website:

ibm.com/redbooks

Online resources

The following websites are also relevant as further information sources:

- ▶ IBM Security Key Lifecycle Manager:
<https://www.ibm.com/docs/en/sgklm/4.1?topic=quick-start-guide>
- ▶ IBM Security Key Lifecycle Manager Dashboard:
<https://www.ibm.com/support/pages/node/876126>
- ▶ IBM Security Key Lifecycle Manager Support Matrix:
<https://www.ibm.com/support/pages/node/296957>

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services



SG24-8472-01

ISBN 0738459909

Printed in U.S.A.

Get connected

