IBM Security Guardium Key Lifecycle Manager Version 4.1.0.1

REST Service Documentation

IBM Confidential

Configure Kerberos Authentication REST Service

Use **`Configure Kerberos Authentication REST Service`** to configure IBM® Security Guardium® Key Lifecycle Manager to use Kerberos as the authentication mechanism with the Db2® database.

Operation

`POST`

URL

`https://host:port/SKLM/rest/v1/ckms/kerberos/configure`

By default, Guardium Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Guardium Key Lifecycle Manager installation, you can modify these default ports.

Note: The non-secure port 9080 is not applicable when IBM Security Guardium Key Lifecycle Manager is deployed in a containerized environment.

Request

Request Parameters

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

Request Headers

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

Request Body

JSON object with the following specification.

JSON property name	Description
`dbServiceName`	Specify the name of the Db2 service principal that you registered in the Kerberos database. For example, `db2instance/FQDN_gklmserver@REALMNAME`.
`userId`	Specify the user ID or client principal that you registered in the Kerberos database to access the Db2 service. For example, `sklmdb41`.
`password`	Specify the password of the client principal.
`wasUserName`	Specify the WebSphere® Application Server login user ID for the IBM Security Guardium Key Lifecycle Manager server administrator profile.
`wasUserPassword`	Specify the password for the WebSphere Application Server login user ID.

Response

Response Headers

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

Success Response Body

JSON object with the following specification.

JSON property name	Description
`code`	Returns the code that is specified by the `status` property.
`status`	Returns the status to indicate if the operation was successful.

Error Response Body

JSON object with the following specification.

JSON property name	Description
`code`	Returns the application error code.
`message`	Returns a message that describes the error.

Example

To configure Kerberos authentication

```
https://localhost:9443/SKLM/rest/v1/ckms/kerberos/configure
{"dbServiceName":"sklmdb41/gklmServer@EXAMPLE.COM","userId":"sklmdb41",
"password":"dbpassword","wasUserName":"wasadmin","wasUserPassword":"waspassword"}
```

Success response

```
{
  "code": "CTGKM3561I",
  "status": "CTGKM3561I The Guardium Key Lifecycle Manager server is configured to
use Kerberos authentication with the database. The Guardium Key Lifecycle Manager
server is restarted and will be unavailable for a few minutes."
}
```

Error response

```
{
  "code": "CTGKM3573E",
  "message": "CTGKM3573E Failed to configure Kerberos because the server cannot
connect to the Db2 database. Ensure that the client and service principals are
registered with correct credentials in the Kerberos database."
}
```

Get Kerberos Configuration REST Service

Use **`Get Kerberos Configuration REST Service`** to retrieve details of the Kerberos configuration on the server.

Operation

`GET`

URL

`https://`*`host`*`:`*`port`*`/SKLM/rest/v1/ckms/kerberos/getConfiguration`

By default, Guardium® Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM® Security Guardium Key Lifecycle Manager installation, you can modify these default ports.

Note: The non-secure port 9080 is not applicable when IBM Security Guardium Key Lifecycle Manager is deployed in a containerized environment.

Request

Request Parameters

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

Request Headers

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

Response

Response Headers

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

Content-Type	`application/json`
Content-Language	Locale for the response message.

Success Response Body

JSON object with the following specification.

Json property name	Description
kdcServerHostame	Fully-qualified host name of the computer that hosts the Kerberos server.
realmName	Name of the Kerberos realm name.
dbServiceName	Name of the database service that you registered in the Kerberos server. For example: `sklmdb41/gklmserver.example.com@EXAMPLE.COM`
userId	Client principal that you registered in the Kerberos server.

Error Response Body

JSON object with the following specification.

JSON property name	Description
code	Returns the application error code.
message	Returns a message that describes the error.

Example

To retrieve Kerberos configuration details

```
https://localhost:9443/SKLM/rest/v1/ckms/kerberos/getConfiguration
```

Success response

```
{
  "kdcServerHostame": "kserver.example.com",
  "realmName": "EXAMPLE.COM",
  "dbServiceName": "sklmdb41/gklmserver.example.com@EXAMPLE.COM",
  "userId": "sklmdb41"
}
```

Error response

```
{
  "CTGKM3565I": "CTGKM3565I Cannot retrieve Kerberos configuration details. The
Guardium Security Key Lifecycle Manager server is not configured to use Kerberos
authentication with the database."
}
```

Configure Kerberos on Multi-Master REST Service

Use **`Configure Kerberos on Multi-Master REST Service`** to configure IBM® Security Guardium® Key Lifecycle Manager that is deployed in a Multi-Master setup to use Kerberos as the authentication mechanism with the Db2® database.

Operation

`POST`

URL

`https://host:port/SKLM/rest/v1/ckms/kerberos/configureOnMM`

By default, Guardium Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM Security Guardium Key Lifecycle Manager installation, you can modify these default ports.

Note: The non-secure port 9080 is not applicable when IBM Security Guardium Key Lifecycle Manager is deployed in a containerized environment.

Request

Request Parameters

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

Request Headers

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

Request Body

JSON object with the following specification.

JSON property name	Description
userId	Specify the user ID or client principal that is registered in the Kerberos database to access the Db2 service. For example, `sklmdb41`.
password	Specify the password of the client principal.
wasUserName	Specify the WebSphere® Application Server login user ID for the IBM Security Guardium Key Lifecycle Manager server administrator profile.
wasUserPassword	Specify the password for the WebSphere Application Server login user ID.
{**ipHostName**, **dbServiceName**}	Specify the fully-qualified host name of the master server and the name of service principal that you register on that master server. Specify the parameter values for every master server in the cluster. For example:

	`{"ipHostName":"misstate1","dbServiceName":"sklmdb41/misstate1.example.com"},`
	`{"ipHostName":"haena1","dbServiceName":"klmdb41/haena1.ex.com"}`

Response

Response Headers

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

Success Response Body

JSON object with the following specification.

JSON property name	Description
`code`	Returns the code that is specified by the **`status`** property.
`status`	Returns the status to indicate if the operation was successful.

Error Response Body

JSON object with the following specification.

JSON property name	Description
`code`	Returns the application error code.
`message`	Returns a message that describes the error.

Example

To configure Kerberos

```
https://localhost:9443/SKLM/rest/v1/ckms/kerberos/configureOnMM
[
{"userId":"sklmdb41","password":"klmpassword","wasUserName":"wasadmin",
"wasUserPassword":"waspassword"},
{"ipHostName":"host1","dbServiceName":"sklmdb41/host1.example.com"},
{"ipHostName":"misstate1","dbServiceName":"klmdb41/misstate1.ex.com"},
{"ipHostName":"haena1","dbServiceName":"klmdb410/haena1.exm.com"}]
```

Success response

```
{
  "code": "CTGKM3574I",
  "status": "CTGKM3574I Kerberos is configured on all master servers of the Multi-
Master cluster. The cluster is restarted and will be unavailable for a few
minutes."
}
```

Error response

```
{
  "code": "CTGKM3573E",
  "message": "CTGKM3573E Failed to configure Kerberos because the server cannot
connect to the Db2 database. Ensure that the client and service principals are
registered with correct credentials in the Kerberos database."
}
```

Remove Kerberos Configuration REST Service

Use **`Remove Kerberos Configuration REST Service`** to delete the existing Kerberos configuration from the server.

Operation

`POST`

URL

`https://host:port/SKLM/rest/v1/ckms/kerberos/remove`

By default, Guardium® Key Lifecycle Manager server listens to non-secure port 9080 (HTTP) and secure port 9443 (HTTPS) for communication. During IBM® Security Guardium Key Lifecycle Manager installation, you can modify these default ports.

Note: The non-secure port 9080 is not applicable when IBM Security Guardium Key Lifecycle Manager is deployed in a containerized environment.

Request

Request Parameters

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

Request Headers

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

Request Body

JSON object with the following specification.

JSON property name	Description
`wasUserName`	Specify the WebSphere Application Server login user ID for the IBM Security Key Lifecycle Manager server administrator profile.
`wasUserPassword`	Specify the password for the WebSphere Application Server login user ID.

Response

Response Headers

Header name	Value and description
`Status Code`	**200 OK** The request was successful. The response body contains the requested representation. **400 Bad Request**

	The authentication information was not provided in the correct format. **401 Unauthorized** The authentication credentials were missing or incorrect. **404 Not Found Error** The processing of the request fails. **500 Internal Server Error** The processing of the request fails because of an unexpected condition on the server.
`Content-Type`	`application/json`
`Content-Language`	Locale for the response message.

Success Response Body

JSON object with the following specification.

JSON property name	Description
`code`	Returns the code that is specified by the **`status`** property.
`status`	Returns the status to indicate if the operation was successful.

Error Response Body

JSON object with the following specification.

JSON property name	Description
`code`	Returns the application error code.
`message`	Returns a message that describes the error.

Example

To remove Kerberos configuration

```
https://localhost:9443/SKLM/rest/v1/ckms/kerberos/remove
{"wasUserName":"wasadmin","wasUserPassword":"waspassword"}
```

Success response

```
{
  "code":"CTGKM3564I",
  "status":"CTGKM3564I The existing Kerberos configuration is removed. The
Guardium Key Lifecycle Manager server will use the database user credentials to
authenticate with the database. The Guardium Key Lifecycle Manager server is
restarted and will be unavailable for a few minutes."
}
```

Error response

```
{
  "code":"CTGKM3576E",
  "message":"CTGKM3576E The Remove Kerberos Configuration Rest Service failed.
First remove the Kerberos configuration from the database and retry the
operation."
}
```