AWS CLOUD KEY MANAGEMENT

Integration Guide

Applicable Devices:

KMES Series 3

Applicable Versions:

6.3.1.x

TABLE OF CONTENTS

[1] OVERVIEW OF THE AWS KMS / KMES SERIES 3 INTEGRATION 3
[1.1] About AWS Key Management Service (KMS) 3
[1.2] Customer managed keys 3
[1.3] Key Benefits of the Integration 3
[2] CREATE CREDENTIALS FOR COMMUNICATION BETWEEN THE KMES SERIES 3 AND AWS KMS 5
[2.1] Create an Access Key in AWS IAM 5
[2.2] Create a Cloud Credential on the KMES 5
[3] CREATE A CUSTOMER MANAGED KEY IN AWS KMS 6
[4] CREATING AND PUSHING KEYS FROM THE KMES SERIES 3 TO AWS KMS 8
[4.1] Create a new HSM Protected Key Group 8
[4.2] Pushing keys to AWS KMS 9
[5] LOGGING 12
[5.1] Tracking the progress/status of jobs 12
[5.2] Viewing AWS-related events in the Audit log 12
APPENDIX A: XCEPTIONAL SUPPORT 13

[1] OVERVIEW OF THE AWS KMS / KMES SERIES 3 INTEGRATION

[1.1] ABOUT AWS KEY MANAGEMENT SERVICE (KMS)

From AWS's website: "AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs."

Please refer to the following URL on the AWS documentation website for more information about AWS Key Management Service (KMS): https://docs.aws.amazon.com/kms/index.html

[1.2] CUSTOMER MANAGED KEYS

Customer managed keys are KMS keys in your AWS account that you create, own, and manage. You have full control over these KMS keys, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the KMS keys, and scheduling the KMS keys for deletion.

Customer managed keys appear on the **Customer managed keys** page of the AWS Management Console for AWS KMS.

The customer managed keys feature also allows you to import existing symmetric keys into AWS KMS. For this integration, this means being able to create symmetric HSM Protected keys on a KMES Series 3 device, and then pushing those keys to AWS KMS from the KMES application interface.

Keys that are pushed to AWS KMS can be used with other services inside AWS, such as the following:

- Amazon S3
- The Transparent Data Encryption functionality in Amazon RDS and Amazon DynamoDB
- Amazon Route 53
- AWS Lambda

AWS KMS also has its own API that customers can use with their own applications to access and use keys stored in AWS KMS.

For this integration, keys will be created and stored on the KMES Series 3, synchronized to AWS KMS, and then subsequently managed via the KMES application interface.

[1.3] KEY BENEFITS OF THE INTEGRATION

The AWS KMS / KMES Series 3 integration provides several benefits:

- **Key provenance:** You are the sole owner of your keys, so you have the ability to control the location and distribution of them.

- **Added assurance:** Keys that are created on the KMES and imported into AWS KMS never leave the HSM boundary. Because, even once in AWS KMS, the keys are stored on hardware security modules on the backend.
- **Centralized key management:** You can manage your keys and access policies from a single location and user interface, whether the data they protect resides in the cloud or on your premises.
- **Audit compliance:** Many audits require you to escrow keys outside of the cloud provider. This is accomplished with this integration.

[2] CREATE CREDENTIALS FOR COMMUNICATION BETWEEN THE KMES SERIES 3 AND AWS KMS

Before the KMES Series 3 can push key material to AWS KMS, credentials must be created in the AWS IAM service and then configured on the KMES. In AWS IAM, these credentials will take the form of an **Access Key**. On the KMES, the credentials will take the form of a **Cloud Credential**.

[2.1] CREATE AN ACCESS KEY IN AWS IAM

1. Log in to the AWS Management Console.
2. Navigate to the Identity & Access Management (IAM) service: https://console.aws.amazon.com/iam/home
3. On the right side of the page, under "Quick Links", click on **My security credentials**.
4. There are 3 tabs on this page: "AWS IAM credentials", "AWS CodeCommit credentials", and "Amazon MCS credentials". Select the first tab (AWS IAM credentials).
5. Under "Access keys for CLI, SDK, & API access", click the **Create access key** button.
6. Create a symmetric access key. Upon completion you will be given 2 values: "Access Key ID" and "Secret Access Key". You may write these down and populate a CSV file with these values, or you can use the on-page option to download and save the CSV. It should be in the following format:

   ```
   Access key ID,Secret access key
   AccessID,AccessKey
   ```

   NOTE: This is the only time you will be able to view your secret key. Be sure to write it down/save it now.
7. Copy or move the CSV file containing the Access Key to the storage medium that is configured on your KMES Series 3 device.

[2.2] CREATE A CLOUD CREDENTIAL ON THE KMES

1. Log in to the KMES Series 3 application interface using the default admin identities.
2. Select *Identity Management* -> *Cloud Credentials* from the sidebar.
3. Right-click and select **Add** -> **Cloud Credential** (or click the **Add Cloud Credential** button at the lower-right).
   a. Name = Any name of your choosing
   b. Service = Amazon Web Services
   c. Access Name = Leave this blank; it will auto-populate after import.
   d. Click **Import** and select the CSV file with your Key IDs.
   e. Click **OK** to save.

[3] CREATE A CUSTOMER MANAGED KEY IN AWS KMS

This section will explain how to create a customer managed key in AWS KMS. The KMS key will be created devoid of key material so that the KMES can be the source of the key material. The process for pushing keys from the KMES to AWS KMS will be explained in a later section.

1. Log in to the AWS Management Console.
2. Navigate to the Key Management Service.
3. Select *Customer managed keys* in the left menu, then click the orange **Create key** button in the upper-right portion of the page.
4. Step 1: Configure key
    a. Key type = Symmetric
    b. Key material origin = External

       NOTE: The "KMS" option also works, but it generates a key, so the KMES will not have the key material for this initial key. The "External" option will create a placeholder key without key material, allowing the KMES to provide key material in later steps.
    c. Regionality = Single-Region key
    d. Click the **Next** button.
5. Step 2: Add labels
    a. Alias = Any nickname of your choosing
    b. Description = Optional
    c. Tags = Optional
    d. Click the **Next** button.
6. Step 3: Define key administrative permissions
    a. Key administrators = Select your user account
    b. Key deletion = Check the box, "Allow key administrators to delete this key."
    c. Click the **Next** button.
7. Step 4: Define key usage permissions
    a. This account = Select your user account
    b. Other AWS accounts = Optional
    c. Click the **Next** button.
8. Step 5: Review

   a. Ensure the top 3 fields (Key configuration, Alias and description, and Tags) are correct.
   b. The final (4th) field is "Key policy". Copy and paste the contents of the key policy into a file and save with the JSON extension. This file needs to be copied or moved to the storage medium that is configured on your KMES Series 3 device.
   c. Click the **Finish** button.

9. It will prompt you to download a wrapping key and import token. Click **Cancel** to skip it.
10. Back on the main Key Management Service (KMS) page, make a copy of the generated key ID (should be formatted like "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"). This ID (and the policy) will be needed for the "AWS Properties" tab when creating an HSM Protected Key Group on the KMES in the next section.

[4] CREATING AND PUSHING KEYS FROM THE KMES SERIES 3 TO AWS KMS

This section will explain how to create a new HSM Protected Key Group on the KMES and how the different key operations work for pushing keys to AWS KMS.

NOTE: If a firewall is configured in your environment, ensure that the ***.amazonaws.com:443** endpoint is allowed from the KMES out to the internet. If a more specific endpoint is preferred or required, please refer to the following documentation: https://docs.aws.amazon.com/general/latest/gr/kms.html

[4.1] CREATE A NEW HSM PROTECTED KEY GROUP

Key groups act as both a container for keys and a template by which keys are created within the key group, allowing you to define various key attributes, such as the type of key and the key rotation schedule, and the service to use (e.g., Amazon Web Services).

1. Log in to the KMES Series 3 application interface using the default admin identities.
2. Select *Key Management* -> *Keys* from the sidebar.
3. Right-click and select **Add** -> **Key Group** (or click the **Create** button at the upper-right).
    a. Key Type = Symmetric
    b. Storage Location = HSM Protected
    c. Click **OK**.

   NOTE: Asymmetric keys are not supported for the AWS KMS integration.
4. Group tab setup
    a. Name = Any name of your choosing
    b. Service = Amazon Web Services
    c. Credential = Click **Select** and choose the credential that was created from the CSV in section 2.2.
    d. Key Type = AES
    e. Key Length = AES-256
    f. Key Usage = Encrypt + Decrypt
    g. Rotate Key = Leave box checked if you want the key group to rotate keys on a schedule.
    h. Rotate every = Set the desired rotation interval.
    i. Keep key valid for = Set the length of time that keys created in the key group should remain valid.
5. Info tab setup
    a. Leave blank/default
6. AWS Properties tab setup

a. Alias = Any nickname of your choosing
b. Description = Optional
c. Region = Select the AWS region where the KMS key was created in section 3.1.
d. Active Key ID = Enter the key ID formatted like "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" (from step 10 of the instructions in section 3.1).
e. Policy = Click **Import Policy** and select the policy that was saved as a JSON file in step 8b of section 3.1. The policy specifies the permissions used to access the customer master key in AWS.
f. Disable key after rotating = Check/uncheck as desired
g. Click **OK** to finish creating the HSM Protected Key Group.

[4.2] PUSHING KEYS TO AWS KMS

There are two main operations that can be performed on keys that are part of an AWS HSM Protected Key Group:

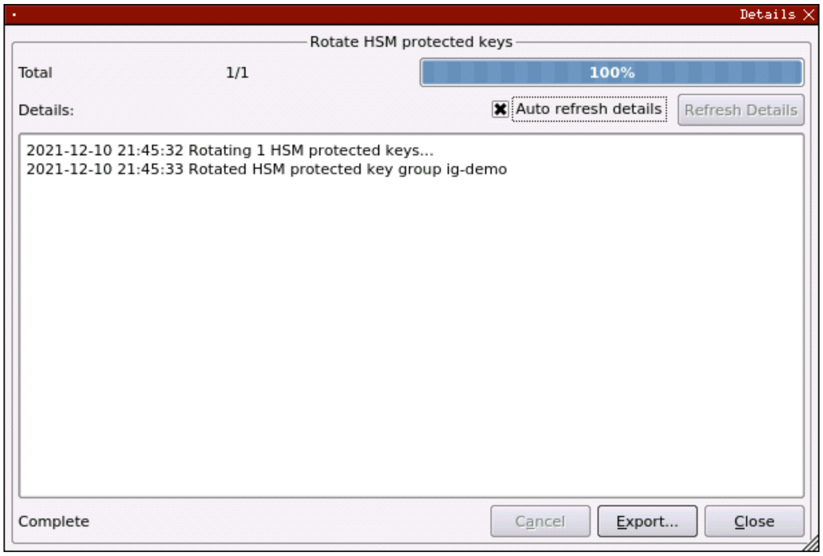
- Rotate on an HSM Protected Key Group - This forces a new key to be generated on the KMES and then uploaded to AWS with the alias configured under the AWS Properties tab assigned to the key. On the "Customer managed keys" page in AWS KMS, you will see that if you keep rotating, the old key ID loses the alias, and the most recently created key has the alias assigned.
- Synchronize on an HSM Protected Key - This updates the given key ID in AWS with the selected key. As an example, the key material can be deleted from AWS for a key, then you can right-click that same key in the KMES and synchronize it and re-add the key material. Key material can also be deleted from AWS by checking the appropriate check box when synchronizing in the KMES.

NOTE: For this integration, the only way that keys should be generated inside an AWS HSM Protected Key Group is by force rotating the key group or simply waiting for a key rotation to occur based on the configured rotation schedule.

For demonstration purposes, we will force rotate the HSM Protected Key Group to generate and push the first key to AWS KMS. To do so, please follow the steps outlined below:

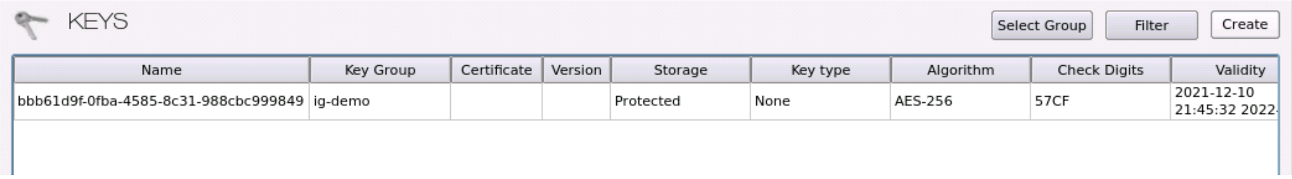
1. Make sure that the KMES is set to be the designated device for rotating key material (under **Administration** -> **Configuration** -> **HSM Protected Key Options**).
2. Select *Key Management* -> *Keys* from the sidebar.
3. Right-click on the HSM Protected Key Group that was created in the previous section, then select **Cloud** -> **Force Rotate**.
4. A job will be started to rotate and synchronize this key to the AWS KMS account that was specified for the key group. Navigate to **Logging and Reporting** -> **Jobs** and double-click on the **Rotate HSM protected keys** job that was just started. If the synchronization is successful, a message similar to the following will be

shown:



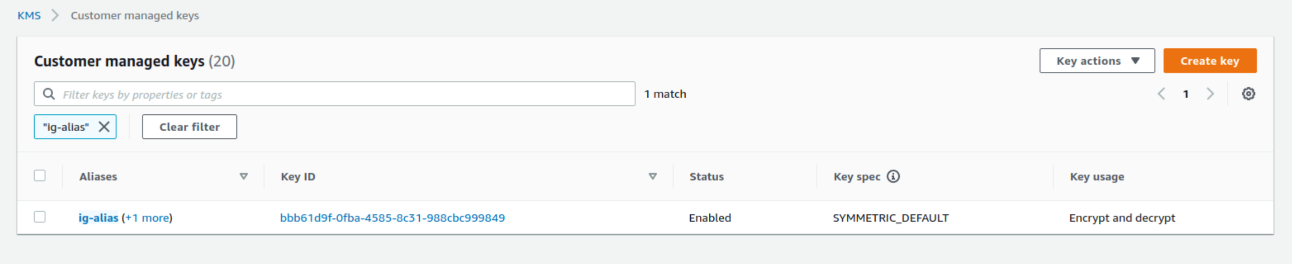
```
2021-12-10 21:45:32 Rotating 1 HSM protected keys...
2021-12-10 21:45:33 Rotated HSM protected key group ig-demo
```

5. Once the job is finished, navigate back to the *Keys* view and select the key group of the key that was just synchronized. We can see that the key is listed now under the key group:



Name	Key Group	Certificate	Version	Storage	Key type	Algorithm	Check Digits	Validity
bbb61d9f-0fba-4585-8c31-988cbc999849	ig-demo			Protected	None	AES-256	57CF	2021-12-10 21:45:32 2022

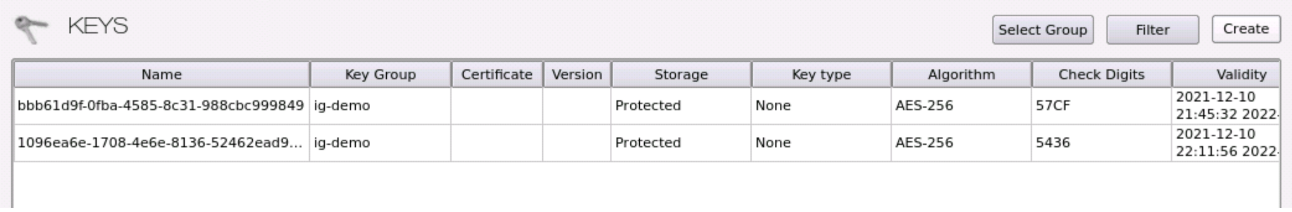
We can see the key in AWS KMS as well, with the alias assigned that was configured on the AWS Properties tab for the HSM Protected Key Group:



KMS > Customer managed keys
Customer managed keys (20)
Key actions ▼
Create key
Filter keys by properties or tags
1 match
"ig-alias" ✕
Clear filter

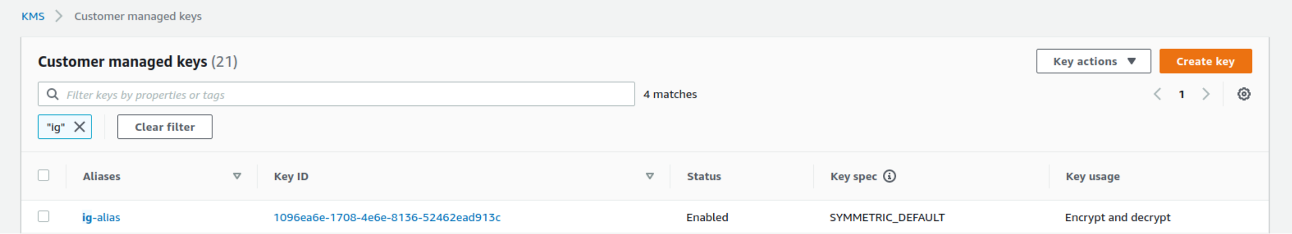
□	Aliases	Key ID	Status	Key spec	Key usage
□	ig-alias (+1 more)	bbb61d9f-0fba-4585-8c31-988cbc999849	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

6. Right-click the AWS HSM Protected Key Group again and select **Cloud** -> **Force Rotate**. The new key that is generated (e.g., 1096ea6e...) will be listed with the first key that was generated in the key group:



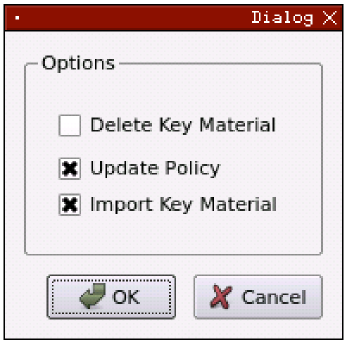
Name	Key Group	Certificate	Version	Storage	Key type	Algorithm	Check Digits	Validity
bbb61d9f-0fba-4585-8c31-988cbc999849	ig-demo			Protected	None	AES-256	57CF	2021-12-10 21:45:32 2022
1096ea6e-1708-4e6e-8136-52462ead9...	ig-demo			Protected	None	AES-256	5436	2021-12-10 22:11:56 2022

In AWS, this new key will now be assigned the alias configured for the HSM Protected Key Group (e.g., ig-alias) and the previously active Key ID will lose the alias.


KMS > Customer managed keys
Customer managed keys (21)
Key actions ▼
Create key
Filter keys by properties or tags
4 matches
"ig" ✕
Clear filter
< 1 >

☐	Aliases	Key ID	Status	Key spec	Key usage
☐	ig-alias	1096ea6e-1708-4e6e-8136-52462ead913c	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

7. The other key operation mentioned at the beginning of this section was synchronizing on an HSM Protected Key. This would mean synchronizing, or optionally deleting, key material for any of the previously active Key IDs. To do so, select the AWS HSM Protected Key Group, then right-click one of the previously active key IDs and select **Cloud** -> **Synchronize**. This will open the following dialog:



☐ Delete Key Material

☒ Update Policy

☒ Import Key Material

8. The "Update Policy" and "Import Key Material" options will be selected by default. It would only make sense to import key material if the key material had been deleted for the associated Key ID previously, either in AWS KMS or via the "Delete Key Material" option shown here. Regardless of the synchronization option that is performed, a new job will be created on the *Logging and Reporting* -> *Jobs* page where the progress of the operation can be tracked.

[5] LOGGING

This section will explain how to track the progress/status of jobs related to AWS HSM Protected Key Groups, as well as how to view AWS-related events in the Audit Log.

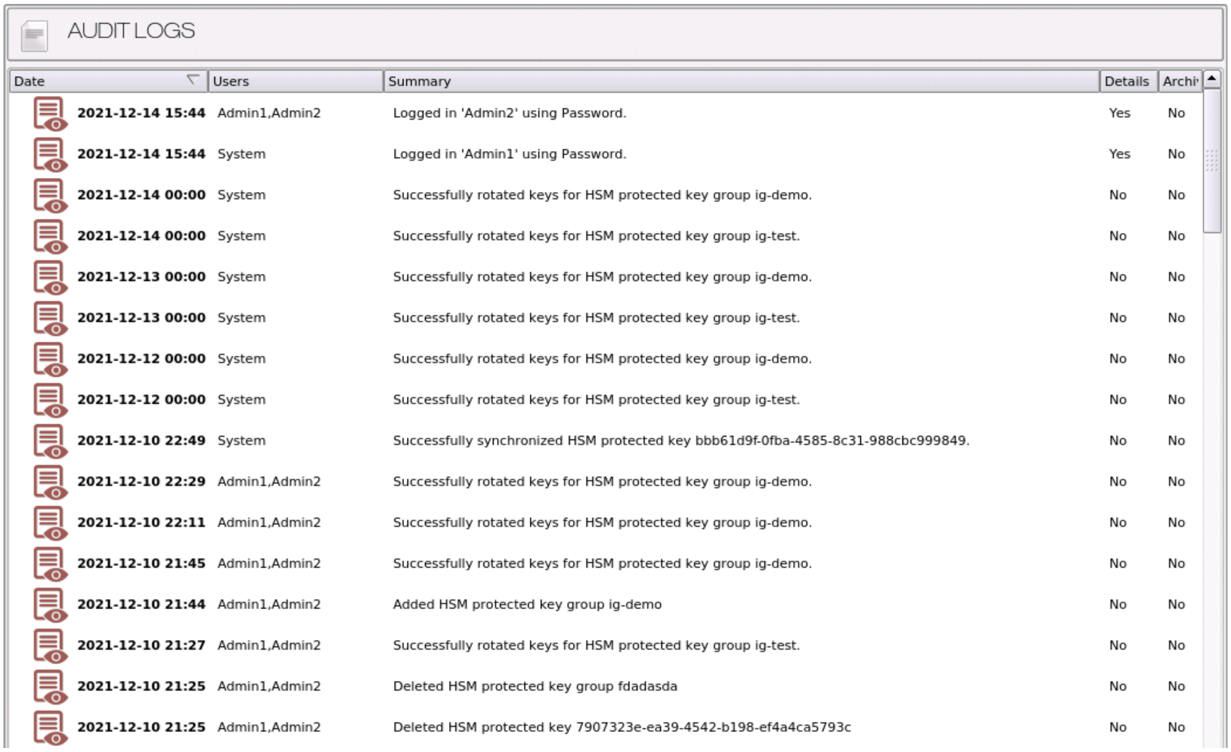
[5.1] TRACKING THE PROGRESS/STATUS OF JOBS

It has already been mentioned in previous sections that the progress/status of jobs related to AWS can be viewed under **Logging and Reporting** -> **Jobs**. Events specific to this integration that would initiate a new job include the following:

- Rotate HSM protected key(s)
- Synchronize HSM protected key(s)

[5.2] VIEWING AWS-RELATED EVENTS IN THE AUDIT LOG

AWS-related events can also be viewed under **Logging and Reporting** -> **Audit Logs**. The following is an example of how these log entries would appear.



Date	Users	Summary	Details	Archi
2021-12-14 15:44	Admin1,Admin2	Logged in 'Admin2' using Password.	Yes	No
2021-12-14 15:44	System	Logged in 'Admin1' using Password.	Yes	No
2021-12-14 00:00	System	Successfully rotated keys for HSM protected key group ig-demo.	No	No
2021-12-14 00:00	System	Successfully rotated keys for HSM protected key group ig-test.	No	No
2021-12-13 00:00	System	Successfully rotated keys for HSM protected key group ig-demo.	No	No
2021-12-13 00:00	System	Successfully rotated keys for HSM protected key group ig-test.	No	No
2021-12-12 00:00	System	Successfully rotated keys for HSM protected key group ig-demo.	No	No
2021-12-12 00:00	System	Successfully rotated keys for HSM protected key group ig-test.	No	No
2021-12-10 22:49	System	Successfully synchronized HSM protected key bbb61d9f-0fba-4585-8c31-988cbc999849.	No	No
2021-12-10 22:29	Admin1,Admin2	Successfully rotated keys for HSM protected key group ig-demo.	No	No
2021-12-10 22:11	Admin1,Admin2	Successfully rotated keys for HSM protected key group ig-demo.	No	No
2021-12-10 21:45	Admin1,Admin2	Successfully rotated keys for HSM protected key group ig-demo.	No	No
2021-12-10 21:44	Admin1,Admin2	Added HSM protected key group ig-demo	No	No
2021-12-10 21:27	Admin1,Admin2	Successfully rotated keys for HSM protected key group ig-test.	No	No
2021-12-10 21:25	Admin1,Admin2	Deleted HSM protected key group fdadasda	No	No
2021-12-10 21:25	Admin1,Admin2	Deleted HSM protected key 7907323e-ea39-4542-b198-ef4a4ca5793c	No	No

APPENDIX A: XCEPTIONAL SUPPORT

In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

ENGINEERING CAMPUS

864 Old Boerne Road
Bulverde, Texas, USA 78163
Phone: +1 830-980-9782
+1 830-438-8782
E-mail: info@futurex.com

XCEPTIONAL SUPPORT

24x7x365
Toll-Free: 1-800-251-5112
E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com