Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – CUSTOM ROLES

VERSION 1.1

Fortanix Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | United States of America | ☎ +1 (650) 943-2484 |
✉ info@fortanix.com | 🌐 www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

Welcome to the Fortanix Data Security Manager (DSM) User Guide. This document describes the steps to create named Custom user roles that allow fine-grained control over what users can do in Fortanix DSM accounts and groups.

1.1 ENABLING CUSTOM ROLES

NOTE: In Fortanix DSM version 4.9:

- The Custom user roles feature must be explicitly enabled by a System Administrator using the Sys Admin Settings after the software upgrade has finished successfully.

On-Prem cluster – To enable this feature on your on-prem cluster, a System Administrator must do the following:

1. Go to the System Administration **Settings** page and click the **NEW FEATURES** tab from the left panel.
2. On the New Features page, enable the toggle for **Custom Roles**.

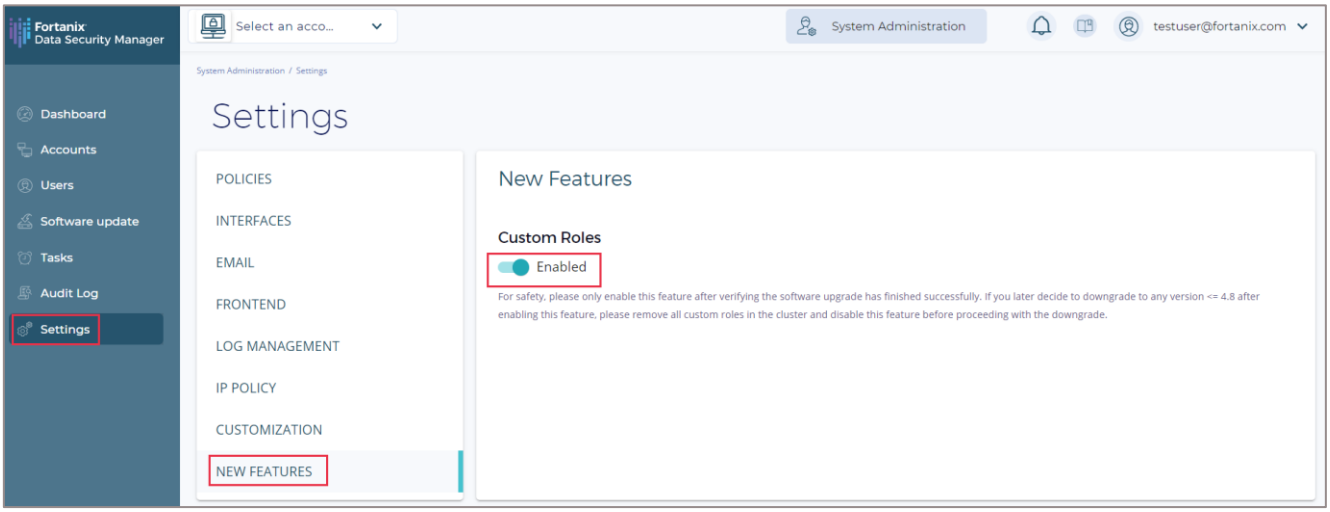

FIGURE 1: ENABLE CUSTOM ROLES

WARNING:

Enable this feature only after verifying the software upgrade has finished successfully. If you later decide to downgrade to any version <= 4.8 after enabling this feature, then remove all custom roles in the cluster and disable this feature before proceeding with the downgrade.

2.0 DEFINITIONS

- **Fortanix Data Security Manager** -

  Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

- **Accounts** -

  A Fortanix DSM account is the top-level container for security objects managed by the Fortanix DSM. An account is generally associated with an organization, rather than an individual. Security objects, groups, and applications belong to exactly one account. Different accounts are fully isolated from each other. *See support for more information.*

- **Users** -

  Users are associated with an email address. A user can be a member of one or more accounts. Depending on permissions, users can:

  - Perform management operations like adding or modifying users or groups
  - Create security objects
  - Change properties of security objects
  - Review logs of Fortanix DSM activity

  ⚠ **Users cannot perform cryptographic operations. Only applications can perform cryptographic operations.**

- **Groups** -

  A group is a collection of security objects created by and accessible by users and applications which belong to the group. The user who creates a group automatically gets assigned the role of the group administrator. You can add more users to the group in the role of administrators or auditors. You can also add applications to the group to enable the applications to create and use security objects in that group. *See support for more information.*

Access policies are set at the group level, so all security objects in a group share the same access policy. Any number of users and/or applications can be assigned to a group. *Some examples of usage of groups are given in the Authorization section*.

Quorum policies can also be set at group level. A Quorum policy mandates that all security sensitive operations in that group would require a quorum approval. Such operations include using a key for cryptographic operations or deleting or updating a group. *See Quorum Policy for more information.*

- **Applications** -

  An application can use Fortanix DSM to generate, store, and use security objects, such as cryptographic keys, certificates, or an arbitrary secret. Applications can authenticate to Fortanix DSM using an API key (a secret token) or a TLS client certificate. An application can interact with Fortanix DSM using the REST APIs or using the PKCS#11, JCE, or CNG providers. *See support for more information.*

- **Fortanix Data Security Manager Security Objects** –

  A security object is any datum stored in Fortanix DSM (for example a key, a certificate, a password, or other security objects). Each security object is assigned to exactly one group. users and applications assigned to the group have permission to see the security object and to perform operations on it. *See support for more information.*

3.0 CUSTOM ROLES

Custom user roles allow fine-grained control over what users can do in the Fortanix DSM accounts and groups. There are two types of Custom user roles: **Custom account role** and **Custom group role**.

Before the introduction of Custom user roles, Fortanix DSM only had five built-in roles for users. They are Account Administrator, Account Member, Account Auditor, Group Administrator, and Group Auditor. These are now referred to as "**legacy roles**".

An Account Administrator can create an arbitrary number of Custom account roles, with custom account permissions.

A user with a Custom group role can have a user-defined set of permissions that will apply for operations requested by that user on objects within the group.

3.1 CUSTOM ACCOUNT ROLE

A Custom account role has the following properties:

- permissions: the set of account-level permissions assigned to the user. See *Section 3.5* below for a complete list of account permissions.
- exclusive: this can be set to "true" or "false". If a Custom account role is marked as "exclusive", that is, its value is set to "true", then it cannot be co-assigned with any other role.
- all-groups role (optional): this is the unique ID of a Custom group role. If this is specified in the Custom account role, it means that the user will also have the selected group role for all the groups in Fortanix DSM.

 **NOTE**:

- Each user can have multiple Custom account roles assigned to them as long as none of the assigned roles is marked "exclusive", otherwise, only one exclusive role can be assigned to the user. The same restriction applies to "all-groups roles".
- All legacy account roles (Account Administrator, Account Member, and Account Auditor) are "exclusive". See *Section 3.4* below for the definition of legacy account roles in terms of the above properties.

3.2 CUSTOM GROUP ROLE

A Custom group role has the following properties:

- permissions: the set of group-level permissions assigned to the user. See *Section 3.8* below for a complete list of group permissions.
- exclusive: this can be set to "true" or "false". If a Custom group role is marked as "exclusive", that is, its value is set to "true", then it cannot be co-assigned with any other role.

 **NOTE**:

- Each user can have multiple Custom group roles in any given group (in addition to the "all-groups role" inherited from Custom account role(s)) as long as none of the assigned roles is marked "exclusive", otherwise, only one exclusive role can be assigned to the user.
- All legacy group roles (Group Administrator and Group Auditor) are "exclusive". See *Section 3.4* below for the definition of legacy account roles in terms of the above properties.

3.3 MANAGING CUSTOM USER ROLES

Following are some restrictions on the role objects in order to maintain referential integrity and exclusivity rules explained earlier:

- A Custom user role cannot be deleted if it is referenced anywhere, that is, assigned to a user, or in the case of Custom group roles, if it is referenced in a Custom account role as an "all-groups role".
- When updating Custom accounts or group roles, the "exclusive" flag cannot be changed once it is set.
- When updating Custom account roles, the "all-groups role" ID cannot be changed.

Additionally, to prevent privilege escalation, a user is not allowed to add permissions that they do not currently have to a role. This includes both creating and updating account and group roles. Moreover, users are not allowed to assign a role that is more powerful that their role(s) to other users, for the same reason.

3.4 LEGACY ROLES IN TERMS OF CUSTOM USER ROLES

The Fortanix DSM "legacy roles" can be expressed in terms of Custom user roles as follows:

- Account Administrator:
  - permissions: all account permissions.
  - exclusive: **true**
  - all-groups role: **Group Administrator**
- Account Member:
  - permissions: `CREATE_LOCAL_GROUPS`, `CREATE_EXTERNAL_GROUPS`, `ALLOW_KEY_CUSTODIAN`, `ALLOW_QUORUM_REVIEWER`, `GET_CHILD_ACCOUNTS`, `GET_ADMIN_APPS`, `GET_CUSTOM_ROLES`, `GET_EXTERNAL_ROLES`, `GET_ALL_USERS`, `GET_ACCOUNT_USAGE`.
  - exclusive: **true**
  - all-groups role: **none**
- Account Auditor:
  - permissions: `ALLOW_KEY_CUSTODIAN`, `ALLOW_QUORUM_REVIEWER`, `GET_ALL_APPROVAL_REQUESTS`, `GET_CHILD_ACCOUNTS`, `GET_ADMIN_APPS`, `GET_CUSTOM_ROLES`, `GET_EXTERNAL_ROLES`, `GET_ALL_USERS`, `GET_ACCOUNT_USAGE`.
  - exclusive: **true**
  - all-groups role: **Group Auditor**
- Group Administrator:
  - permissions: all group permissions.
  - exclusive: **true**
- Group Auditor:
  - permissions: `GET_GROUP`, `GET_SOBJECTS`, `GET_APPS`, `GET_PLUGINS`, `GET_GROUP_APPROVAL_REQUESTS`, `GET_AUDIT_LOGS`.
  - exclusive: **true**

3.5 CREATING A CUSTOM ACCOUNT ROLE

To create a Custom account role:

1. Click the **Users** tab in the Fortanix DSM main menu.
2. Select the **CUSTOM ACCOUNT ROLES** tab and click the Add button to add a new custom role.
3. In the "Add New Custom Account Role" form:
   a. Enter a name for the Custom account role in the **Custom Role Name** field.
   b. Select the toggle for **Exclusive Role** to keep this Custom account role exclusive, that is, it cannot be co-assigned with any other Custom account role. Disable it to allow adding more Custom account roles to a user in addition to the current role.
   c. You can configure the following permissions for the custom account role:
      - **Account**
        - **Manage Logging**: A user with this permission is allowed to update the Log management settings in the account configuration where the user can:
          - Add custom log management integrations.
          - Delete custom log management integrations.
          - Modify custom log management integrations.
          - Enable/Disable audit logging to debug an application against invalid API requests (4XX errors).

          For more information, refer to the User's Guide: Logging.

        - **Manage Authentication**: A user with this permission is allowed to update the Authentication settings in the account configuration where the user can:
          - Configure password authentication or
          - Configure Single Sign-On (SSO) authentication

          For *more information, refer to the User's Guide: Authentication.*

        - **Manage Workspace CSE**: A user with this permission is allowed to:
          - Create, update, and delete the Google Workspace CSE Client-Side Encryption API settings in the account configuration.

          For *more information, refer to the User's Guide: Workspace CSE Client-Side Encryption.*

- **Unwrap Workspace CSE Privileged**: A user with this permission is allowed to:
  - Unwrap the Data Encryption Key (DEK) and decrypt the Google Workspace application's data.
  - Call the privileged unwrap API. This permission is needed for exporting all of your organization's Workspace data.
- **Manage Account Client Configs**: A user with this permission is allowed to:
  - Create, update, and delete the Client Configuration options for the PKCS#11, KMIP, and Common client in the account configuration

  For more information, refer to the User's Guide: Client Configurations.

- **Create Account Approval Policy**: A user with this permission is allowed to
  - Create a Quorum approval policy for an account.

  NOTE: Updating/Deleting account Quorum policy is managed by the policy itself.

  For more information, refer to the User's Guide: Quorum Policy.

- **Set Approval Request Expiry**: A user with this permission is allowed to update Quorum approval request expiration time.
- **Update Account Custom Metadata Attributes**: A user with this permission is allowed to update an account's custom metadata attributes.
- **Manage Account Subscription**: A user with this permission is allowed to manage an account's subscription (only relevant for SaaS accounts).
- **Manage Account Profile**: A user with this permission is allowed to manage an account's profile settings and allowed to:
  - Update the account name
  - Upload a custom logo for the account
  - Update the country, description, organization, phone, and notification preferences

  For more information, refer to the User's Guide: Account Customization.

- **Delete Account**: A user with this permission is allowed to delete an account.

- **Administrative Apps**

- **Create Admin Apps**: A user with this permission is allowed to create an account administrative app.
- **Update Admin Apps**: A user with this permission is allowed to update an account administrative app.
- **Delete Admin Apps**: A user with this permission is allowed to delete an account administrative app.
- **Retrieve Admin App Secrets**: A user with this permission is allowed to retrieve an account administrative app credentials.
- **Manage Admin Apps**: A user with this permission is allowed to create, update, and delete account administrative apps, retrieve an account administrative app, and get all the account administrative apps.

  For more information, refer to the User's Guide: Authentication.

- **Custom Roles**
  - **Create Custom Roles**: A user with this permission is allowed to create a custom account role for a user.
  - **Update Custom Roles**: A user with this permission is allowed to update a custom account role for a user.
  - **Delete Custom Roles**: A user with this permission is allowed to delete a custom account role for a user.
  - **Manage Custom Roles**: A user with this permission is allowed to create, update, and delete a custom account role for a user.
- **Users**
  - **Invite Users to Account**: A user with this permission is allowed to invite users to an account.
  - **Delete Users From Account**: A user with this permission is allowed to delete users from an account.
  - **Update Users Account Role**: A user with this permission is allowed to update another user's account role. When the user is assigning a new role to another user the principal user must themselves have that role in order to assign the new role.

- **Update Users Account Enabled State**: A user with this permission is allowed to enable or disable a user in an account or tenant account.
- **Manage Account Users**: A user with this permission is allowed to:
  - Invite users to an account.
  - Delete users from an account.
  - Update another user's account role.
  - Enable/Disable a user in an account/tenant account.
  - Get all the users in an account.

- **External Roles**
  - **Create External Roles**: A user with this permission is allowed to create an account external role.
  - **Sync External Roles**: A user with this permission is allowed to sync account external roles.
  - **Delete External Roles**: A user with this permission is allowed to delete an account external role.
  - **Manage External Roles**: A user with this permission is allowed to:
    - Create an account external role**.**
    - Sync account external roles.
    - Delete an account external role.
    - Get all the external roles.
- **Security Object Policies**
  - **Create Account Security Object Policies** A user with this permission is allowed to create various account-level security object policies including cryptographic policy, key metadata policy, and key history policy.
  - **Update Account Security Object Policies**: A user with this permission is allowed to update various account-level security object policies including cryptographic policy, key metadata policy, and key history policy.
  - **Delete Account Security Object Policies**: A user with this permission is allowed to delete various account-level security object policies including cryptographic policy, key metadata policy, and key history policy.

- **Manage Account Security Object Policies**: A user with this permission is allowed to create, update, and delete various account-level security object policies including cryptographic policy, key metadata policy, and key history policy.

For more information, refer to the User's Guide: Cryptographic Policy, User's Guide: Key Metadata Policy, and User's Guide: Key Undo Policy.

- **Child Accounts**
  - **Create Child Accounts**: A user with this permission is allowed to create a tenant account.
  - **Update Child Accounts**: A user with this permission is allowed to update a tenant account.
  - **Delete Child Accounts**: A user with this permission is allowed to delete a tenant account.
  - **Create Child Accounts**: A user with this permission is allowed to add users to a tenant account.
  - **Get Child Accounts**: A user with this permission is allowed to get all the tenant accounts.
  - **Get Child Account Users**: A user with this permission is allowed to get all the users from a tenant account.
  - **Manage Child Accounts**: A user with this permission is allowed to do all the operations in a tenant account.

NOTE: The above permissions are only applicable to Fortanix DSM SaaS accounts with reseller subscription.

- **Miscellaneous**
  - **Create Local Groups**: A user with this permission is allowed to create a local group in the account.
  - **Create External Groups**: A user with this permission is allowed to create a new group backed by external HSM/KMS.
  - **Allow Quorum Reviewer**: A user with this permission is allowed to participate as a quorum approver in a Quorum approval policy for the account.

- **Allow Key Custodian**: A user with this permission is allowed to participate in the key custodian policy to add and view a key component.

- **Read**
  - **Get Admin Apps**: A user with this permission is allowed to get all the account administrative apps.
  - **Get All Approved Requests**: A user with this permission grants read access to all Quorum approval requests in the account.
  - **Get Custom Roles**: A user with this permission is allowed to get all the custom roles from the account.
  - **Get External Roles**: A user with this permission is allowed to get all the external roles from the account.
  - **Get All Users**: A user with this permission is allowed to get all the users from an account.
  - **Get Account Usage**: A user with this permission is allowed to get the usage metrics of a particular account.

d. **All Groups Role** (optional): Optionally, you can also select a Custom group role for the Custom account role. If selected, the user will have the specified group role in all the Fortanix DSM groups.

4. Click **SAVE** to save the new custom role.
5. The Custom account role is created successfully.
6. To view the Custom account role, click the **Users** tab from the left panel and click the **CUSTOM ACCOUNT ROLES** tab. You will see the new role added to the.

3.6 EDITING A CUSTOM ACCOUNT ROLE

To edit a custom account role:

1. Click the Users  tab in the Fortanix DSM main menu.
2. Click the **CUSTOM ACCOUNT ROLES** tab.
3. In the Custom account roles table, hover on the custom role that you want to edit and click the edit  button at the end of the row.
4. Make the necessary permission updates and click **SAVE** to save the updates.

3.7 DELETING A CUSTOM ACCOUNT ROLE

A custom account role can only be deleted if no users are mapped to the role. To delete a custom account role:

1. Click the **Users** tab in the Fortanix DSM main menu.
2. Click the **CUSTOM ACCOUNT ROLES** tab.
3. In the Custom account roles table, hover on the custom role that you want to delete and click the delete button at the end of the row.
4. If no users are mapped to the custom account role, click **DELETE** to confirm the deletion.

If users are mapped to an account custom role, then first remove the users, and then delete the custom account role using the steps described above.

3.8 ASSIGNING A USER TO A CUSTOM ACCOUNT ROLE

After a custom account role has been created, you can invite a user to the account with that custom account role. To invite a user with a custom account role:

1. Click the **Users** tab in the Fortanix DSM main menu.
2. On the Users page, click the Add User button to add a new user.
3. In the "Add new users to the account" section:
   a. Select the **INVITE BY EMAIL** option.
   b. Enter the user's email.
   c. Select the **Custom Account role** option.
   d. From the **Select a custom account role** drop down, select an existing custom account role, and click **INVITE** to invite the user to this role.

3.9 CHANGING A USER'S ROLE TO A CUSTOM ACCOUNT ROLE

3.9.1 EDIT A USER'S ROLE

1. Click the **Users** tab in the Fortanix DSM main menu.
2. In the Users table, click the user whose role you want to edit.

3. In the detailed view of the user, hover on the existing user role next to the user's name and click the edit icon .

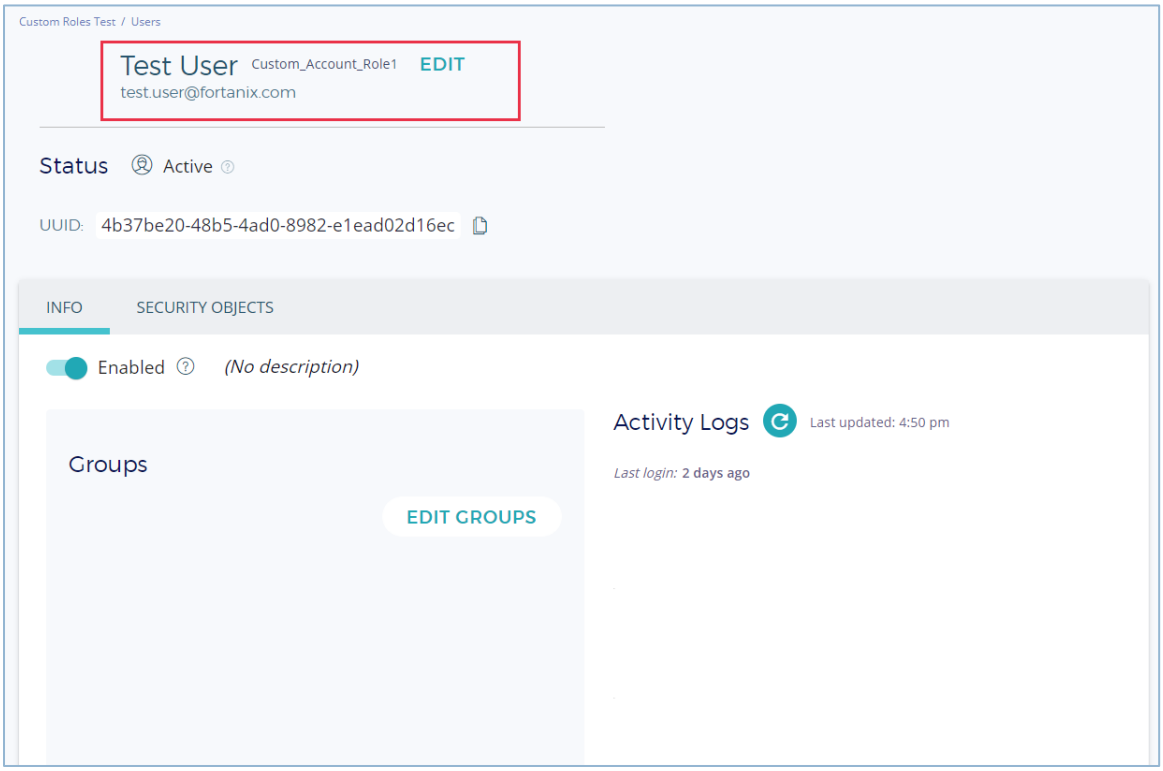

FIGURE 2: EDIT USER ROLE

4. In the EDIT ROLE dialog box, select the **Custom account role** option.
5. In the **Select a custom role** drop down, select the custom account role that you want to assign to the user. The permissions associated with the selected role are displayed.
6. Click **SAVE** to save the new role for the user.

3.9.2 EDIT AN EXTERNAL USER ROLE

1. Click the **Users** tab in the Fortanix DSM main menu.
2. On the Users page, click the Add User button to add a new LDAP user from the directory.
3. Select the **SEARCH LDAP DIRECTORY** option.

NOTE: If the LDAP integration is configured in the Account Settings page, then the provider name will be listed for selection in the **SOURCE** drop down.

4. Select the source and click **SEARCH DIRECTORY**.
5. The users are listed in the table.
6. To edit an LDAP user's permission, select the check box for the user and click the edit icon  .
7. In the "Edit role" dialog box, select the **Custom account role** option.
8. Select the custom account role from the drop down and click **SAVE** to save the role changes.
9. The external user now has the new custom account role assigned for the account.

3.10 CREATING A CUSTOM GROUP ROLE

A custom group role can be created:

- From the **CUSTOM GROUP ROLES** tab on the Groups page.
- From the **External Roles** page while mapping a user to a group.
- While inviting a user to an account as an Account Member.

3.10.1 CREATE A CUSTOM GROUP ROLE FROM THE GROUP DETAILED VIEW

To create a Custom group role from the Groups page:

1. Go to the **Groups** page, and click the **CUSTOM GROUP ROLES** tab.
2. Click the add  button to create a new custom group role.
3. Enter the name of the group custom role in the **Role Name** field.
4. Select the toggle for **Exclusive Role** to keep this Custom group role exclusive, that is, it cannot be co-assigned with any other Custom group role. Disable it to allow adding more Custom group roles to a user in addition to the current role.
5. You can configure the following permissions for the group custom role:
    - **Group**
        - **Create Group Approval Policy**: A user with this permission is allowed to:
            - Create a Quorum approval policy for a group.

             **NOTE**: Updating/Deleting group Quorum policy is managed by the policy itself.

            For more information, refer to the User's Guide: Quorum Policy.

- **Update Group External Links**: A user with this permission is allowed to update an existing HSM/External KMS group configuration. Note that this is only useful for groups backed by external HSM/KMS.
  - Add a new HSM/External KMS group.
  - Update an existing HSM/External KMS group configuration.
  - Delete an existing HSM/External KMS group.
  - Sync keys in an existing HSM/External KMS group.

  For more information, refer to the User's Guide: Quorum Policy.
- **Manage Group Client Configs**: A user with this permission is allowed to:
  - Create, update, and delete the Client Configuration options for the PKCS#11, KMIP, and Common client in the group configuration.

  For more information, refer to the User's Guide: Client Configurations.
- **Update Group Profile**: A user with this permission is allowed to:
  - Update the name of the group.
  - Update the description of the group.
  - Update the custom metadata of the group created using Fortanix DSM SaaS easy wizard integrations.
- **Delete Group**: A user with this permission is allowed to delete the group.
- **Map External Roles for Apps**: A user with this permission is allowed to:
  - Create external roles for mapping and set the permissions for applications authorized through LDAP.
  - Update the group's external role for applications authorized through LDAP.
  - Delete the group's external role for applications authorized through LDAP.
- **Map External Roles for Users**: A user with this permission is allowed to:
  - Create external roles for mapping and define the group roles for users authorized through LDAP.
  - Update the external role for users authorized through LDAP in a group.
  - Delete the external role for users authorized through LDAP in a group.
- **Map External Roles**: A user with this permission is allowed to:

        - Map external roles for apps in a group.
        - Map external roles for users in a group.
    - **Add Users to Group**: A user with this permission is allowed to add users to a group.
    - **Delete Users from Group**: A user with this permission is allowed to delete users from a group.
    - **Update Users Group Role**: A user with this permission is allowed to update the user's role in a group.
    - **Manage Group Users**: A user with this permission is allowed to update the user's role in a group.
        - Add users to a group.
        - Delete users from a group.
        - Update the user's role in a group.
    - **Manage Group Wrapping Key**: A user with this permission is allowed to update the key encryption key (KEK) in a group.
        - Add KEK to a group.
        - Delete KEK from a group.
        - Update the KEK in a group.
- **Security Object Policies**
    - **Create Group Security Object Policies**: A user with this permission is allowed to create various group-level security object policies including cryptographic policy, key metadata policy, and key history policy for a particular group.
    - **Update Group Security Object Policies**: A user with this permission is allowed to update various group-level security object policies including cryptographic policy, key metadata policy, and key history policy for a particular group.
    - **Delete Group Security Object Policies**: A user with this permission is allowed to delete various group-level security object policies including cryptographic policy, key metadata policy, and key history policy for a particular group.

- **Manage Group Security Object Policies**: A user with this permission is allowed to create, update, delete, and various group-level security object policies including cryptographic policy, key metadata policy, and key history policy for a particular group.

For more information, refer to the User's Guide: Cryptographic Policy, User's Guide: Key Metadata Policy, and User's Guide: Key Undo Policy.

- **Custodian policy**
  - **Create Group Custodian Policy**: A user with this permission is allowed to create a Key custodian policy for a particular group.
  - **Update Group Custodian Policy**: A user with this permission is allowed to update the Key custodian policy for a particular group.
  - **Delete Group Custodian Policy**: A user with this permission is allowed to delete the Key custodian policy for a particular group.
  - **Manage Group Custodian Policy**: A user with this permission is allowed to create, update, and delete the Key custodian policy for a particular group.

For more information, refer to the User's Guide: Key Components.

- **App**
  - **Create Apps**: A user with this permission is allowed to create cryptographic apps in the Fortanix DSM groups.

    NOTE:
    - This permission is not applicable for Fortanix DSM Admin apps.
    - This permission is not applicable for Fortanix DSM LDAP apps since the mapping for these apps are determined dynamically.
    - A user creating this app must have all the necessary group permissions for performing crypto operations.
    - The app permissions will be restricted based on the user's permission in that group.
  - **Update Apps**: A user with this permission is allowed to update cryptographic apps in the Fortanix DSM groups.

- **Retrieve App Secrets**: A user with this permission is allowed to retrieve cryptographic app secrets.
- **Delete Apps**: A user with this permission is allowed to delete cryptographic apps in the group.
- **Manage Apps**: A user with this permission is allowed to:
  - Create cryptographic apps in a group.
  - Update cryptographic apps in a group.
  - Retrieve cryptographic app secrets from a group.
  - Delete cryptographic apps from a group.
  - Get cryptographic apps from a group.

- **Plugin**
  - **Create Plugins**: A user with this permission is allowed to create a plugin in the group.
  - **Update Plugins**: A user with this permission is allowed to update a plugin in the group.
  - **Invoke Plugins**: A user with this permission is allowed to invoke a plugin added to the group.
  - **Delete Plugins**: A user with this permission is allowed to delete a plugin from the group.
  - **Manage Plugins**: A user with this permission is allowed to:
    - Create plugins in a group.
    - Update plugins in a group.
    - Invoke the plugins added to a group.
    - Delete plugins from a group.
- **Security Object**
  - **Create Security objects**: A user with this permission is allowed to:
    - Generate keys in a group.
    - Import keys into a group.
    - Import an unwrapped key into a group.
    - Import keys from components into a group.

- Copy keys into a group. This permission is required in the destination group.

- **Export Security Objects**: A user with this permission is allowed to:
  - Export keys from a group.
  - Export a key by wrapping it with another key from a group.
  - Export key as components from a group.
- **Copy Security Objects**: A user with this permission is allowed to copy a key from the source group to another group. This permission is required in the source group.
- **Wrap Security Objects**: A user with this permission is allowed to use a key for wrapping another key. This permission is required in the group where the wrapping key belongs.
- **Unwrap Security Objects**: A user with this permission is allowed to use a key for unwrapping another key. This permission is required in the group where the unwrapping key belongs.
- **Update Security Objects Enabled State**: A user with this permission is allowed to enable or disable a security object in a group.
- **Rotate Security Objects**: A user with this permission is allowed to update the key rotation policy to rotate a key automatically.
- **Delete Security Objects**: A user with this permission is allowed to delete keys from a group.
- **Destroy Security Objects**: A user with this permission is allowed to destroy keys from a group.
- **Revoke Security Objects**: A user with this permission is allowed to mark a security object as deactivated or compromised in a group. The user can also set the deactivate date for the keys.
- **Activate Security Objects**: A user with this permission is allowed to activate keys in a group. The user can also set the activation date for the keys.
- **Revert Security Objects**: A user with this permission is allowed to restore the state of the security objects if a Key Undo Policy is configured for the

group. If the revert operation moves the key back to some other group, then this permission is required in that group as well.

- **Delete Key Material**: A user with this permission is allowed to delete the key material from a key.
- **Move Security Objects**: A user with this permission is allowed to update the group that the key belongs to, to a different group.
- **Update Key Operations**: A user with this permission is allowed to edit the key permissions in a group.
- **Update Security Objects Policies**: A user with this permission is allowed to update individual security objects' policies such as RSA Options, and the Key access justification policy for GCP External Key Manager.
- **Update Security Objects Profile**: A user with this permission is allowed to update the key name, description, and custom metadata, and download the public key of the keys in a group.
- **Scan External Security Objects**: A user with this permission is allowed to scan keys in HSM/External KMS groups.
- **Restore External Security Objects**: A user with this permission is allowed to restore an external key from its backup in Fortanix DSM when the external key is purged from an external KMS.
- **Derive Security Objects**: A user with this permission is allowed to use a key to derive another key.
- **Transform Security Objects**: A user with this permission is allowed to use a BIP32 key that accepts an index input and creates a non-hardened child in the same network as the parent key.

- **Miscellaneous**
  - **Wrap Workspace CSE**: A user with this permission is allowed to wrap the Data Encryption Key (DEK) used to encrypt the Google Workspace application's data.
  - **Unwrap Workspace CSE**: A user with this permission is allowed to unwrap the Data Encryption Key (DEK) and decrypt the Google Workspace application's data.

- **Workspace CSE:** A user with this permission is allowed to:
  - Wrap the Data Encryption Key (DEK) used to encrypt the Google Workspace application's data.
  - Unwrap the Data Encryption Key (DEK) and decrypt the Google Workspace application's data

- **Read**
  - **Get Group**: A user with this permission is allowed to:
    - Get all the group details.
    - Get all groups that have external roles configured.
  - **Get Security Objects**: A user with this permission is allowed to get all the keys in a group.
  - **Get Apps**: A user with this permission is allowed to:
    - Get all the apps in a group.
    - Get all the LDAP groups if the app is authorized through LDAP.
    - Get the app credentials
  - **Get Plugins**: A user with this permission is allowed to get all the plugins in a group.
  - **Get Group Approval Requests**: A user with this permission is allowed to get all approval requests for a group.
  - **Get Audit Logs:** A user with this permission is allowed to get the audit logs of a particular session.

6. Click **SAVE** to save the custom group role.
7. The custom group role is now created.

3.10.2 CREATE A CUSTOM GROUP ROLE FROM THE EXTERNAL ROLES PAGE

To create a custom group role from the External Roles page:

1. Go to the **Groups** page, and click the **EXTERNAL ROLES** tab.
2. Create a new external role if you have the LDAP integration on the **Account Settings** page.
3. After the external roles are mapped and displayed in the table, in the **Groups for users** column, click **MAP TO GROUPS** for the external role for which you want to assign a group.

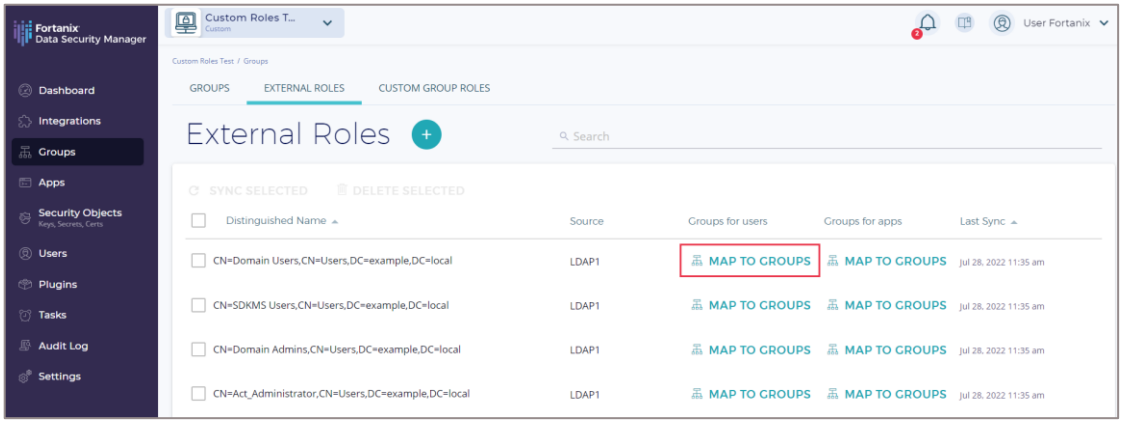

FIGURE 3: MAP EXTERNAL ROLE TO A GROUP

4. In the MAPPING TO GROUPS dialog, click the **MAP GROUPS FOR USERS** tile.
5. From the **Search for groups to add to** column, select the group which you want to map for the external role.
6. In the **Current groups** column, Click **EDIT** to change the default **Group Auditor** role to a **Custom Group Role**.
7. Select the **CUSTOM GROUP ROLE** option and click **ADD NEW CUSTOM GROUP ROLE** to create a new custom group role for the external role.

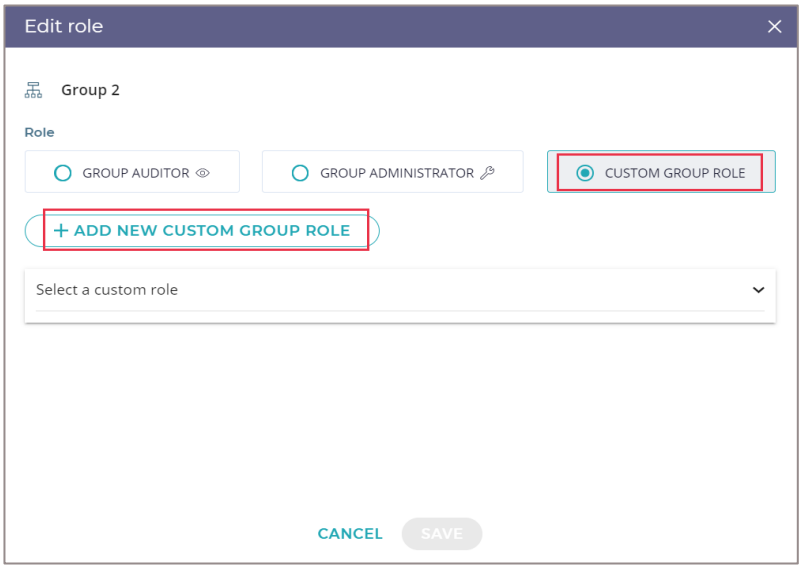

FIGURE 4: CREATE A GROUP CUSTOM ROLE

8. Follow *steps 3-4* in the previous section (*Section 3.8.1*) to create a new custom group role.

9. Click **SAVE CUSTOM ROLE** to save the new Custom group role.
10. Click **SAVE** to assign this new Custom group role to the External role user.

3.10.3 CREATE A CUSTOM GROUP ROLE FROM THE INVITE USERS PAGE

To create a custom group role:

1. Go to the **Users** page and click the **USERS** tab.
2. Click the Add  button to invite a user to a custom group role.
3. Click the **INVITE BY EMAIL** option and enter the email of the user to invite for the custom group role.
4. Select **Account member** and click **NEXT**.
5. In the **Assigning the new user to groups** section, select the group from the first column to which you want to assign the user.
6. In the second column, click **EDIT** to change the default **Group Auditor** role to a **Custom Group Role**.
7. Select the **CUSTOM GROUP ROLE** option and click **ADD NEW CUSTOM GROUP ROLE** to create a new custom group role for the user.
8. Follow *steps 3-4* in *Section 3.8.1* to create a new custom group role.
9. Click **SAVE CUSTOM ROLE** to save the new Custom group role.
10. Click **SAVE** at the bottom of the form to assign this new Custom group role to the user.

3.11 EDITING A CUSTOM GROUP ROLE

To edit the Custom group role:

1. Click the **Groups** tab in the Fortanix DSM main menu.
2. Click the **CUSTOM GROUP ROLES** tab.
3. In the Custom group roles table, click ⋮ button corresponding to the custom role that you want to edit and click the **Edit Role** option from the drop-down menu.
4. Make the necessary permission updates and click **SAVE** to save the updates.

3.12 DELETING A CUSTOM GROUP ROLE

To delete the Custom group role:

1. Click the **Groups** tab in the Fortanix DSM main menu.
2. Click the **CUSTOM GROUP ROLES** tab.
3. In the Custom group roles table, click ⋮ button corresponding to the custom role that you want to remove and click the **Delete Role** option from the drop-down menu.
4. Click the **DELETE** option to remove the role.

3.13 ASSIGNING A CUSTOM GROUP ROLE TO USER/EXTERNAL ROLE

A custom group role can be assigned to a user during the following scenarios:

- Inviting a user to an account as an **Account member** on the Users page.
- Inviting a user to an account as a **Custom account role** on the Users page.
- Mapping a user to a group as External Roles on the **External Roles** page.

3.13.1 ASSIGN A CUSTOM GROUP ROLE TO A USER

To assign a user to a custom group role:

1. Go to the **Users** page and click the **USERS** tab.
2. Click the Add  button to invite a user to a custom group role.
3. Click the **INVITE BY EMAIL** option and enter the email of the user to invite for the custom group role.
4. Select **Account member** or **Custom account role** and click **NEXT**.
5. In the **Assigning the new user to group** column, select the group to which you want to assign the user with a custom group role.

11. Click **EDIT** to change the default **Group Auditor** role to a **Custom Group Role**.
12. Repeat *Steps 7-10* from the previous section (*Section 3.8.2*) to assign a user to a Custom group role.

3.13.2 ASSIGN A CUSTOM GROUP ROLE TO AN EXTERNAL ROLE

1. Go to the **Groups** page and click the **EXTERNAL ROLES** tab.
2. In the External Roles table, for a particular external role, under the **Groups for users** column, click **MAP TO GROUPS**.
3. In the MAPPING TO GROUPS window, select the **MAP GROUPS FOR USERS** tile.
4. In the **MAPPING TO GROUPS FOR USERS** window, select the group to which you want to assign the user with a custom group role from the first column.
5. In the “Current groups” column, select the **Custom group role** option and assign the external role to a custom group role.

4.0 DOCUMENT INFORMATION

4.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/8137714707220-User-s-Guide-Custom-Role

4.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com