Fortanix®

Integration Guide

FORTANIX DATA SECURITY MANAGER WITH DOUBLE KEY ENCRYPTION FOR MICROSOFT 365

Fortanix, Inc. | 800 West El Camino Real | Suite 180 | Mountain View, CA 94040 | United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

This article describes how to integrate **Fortanix Data Security Manager (DSM)** with **Microsoft 365 Double Key Encryption (DKE)**. It also contains the information that a user needs to:

- Create Encryption Key in Fortanix DSM.
- Configure and deploy the DKE Service in Microsoft Azure/IIS.
- Create Sensitivity label with DKE encryption enabled in Microsoft 365 account.
- Use Double Key Encryption labels to protect data.

2.0 TERMINOLOGY REFERENCES

- **DSM – Fortanix Data Security Manager**

  Fortanix Data Security Manager (DSM) is the cloud solution secured with Intel® SGX. With 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.

- **DKE – Double Key Encryption**

  Double Key Encryption is a compliance feature in Microsoft 365 suite of services, which uses two keys together to cryptographically protect content. The advantage is that organizations can bring in external key as one of the key, to control the encryption mechanism. See more details here https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption

3.0 PREREQUISITES

- A Fortanix DSM Account.
- Access to the following services in the Microsoft Azure Portal:
  - App Services (if deploying DKE service on Azure)
  - Active Directory
  - App Registration
- Microsoft Compliance Center https://compliance.microsoft.com/.

- For Microsoft (MS) Office end-user: Microsoft 365 Apps for enterprise version 2009 or later installed on your Windows Desktop.
    - Make sure Microsoft Active Directory Rights Management Services Client file `msipc.dll` is installed at one of these locations.
        - `C:\Program Files (x86)\Microsoft Office\root\Office16\MSIPC`
        - `C:\Program Files\Microsoft Office\root\Office16\MSIPC`
    - If not present, try reinstalling MS Office.

4.0 CONFIGURE FORTANIX DATA SECURITY MANAGER

An asymmetric encryption key is required to be created in Fortanix DSM in your organization's account. This key would later be exposed through REST API to DKE Service for consumption by Microsoft 365. Following are the steps to configure the key:

1. Log in to your organization's Fortanix DSM account. For testing purposes, a trial account can be created here https://sdkms.fortanix.com.
2. Go to the **Security Objects** page and click the **+** button to create a new key.
3. Enter the **Security Object name**. In this document, the key name used is **`MicrosoftDKEServiceKey`**.
4. Assign the key to an existing group or create a new group.
5. Select **GENERATE** to generate a new key.
6. Select the key type as **RSA**.

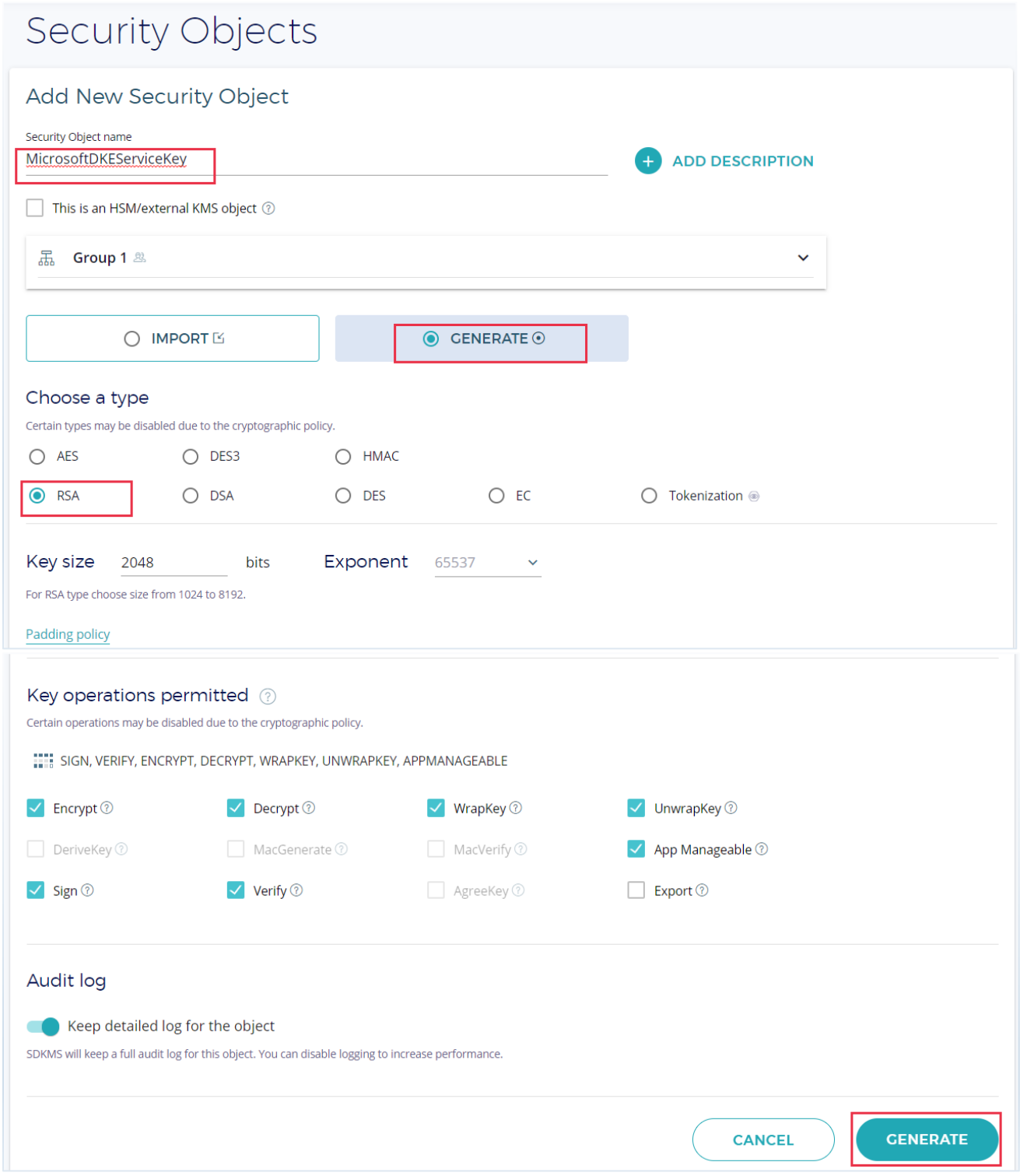

FIGURE 1: CREATE AN RSA KEY

7. In the same group as the new security object, create a new App. Copy the API Key on this app. Refer to the Fortanix DSM Getting Started Guide for steps to create an App. This would be required while deploying the DKE Service.

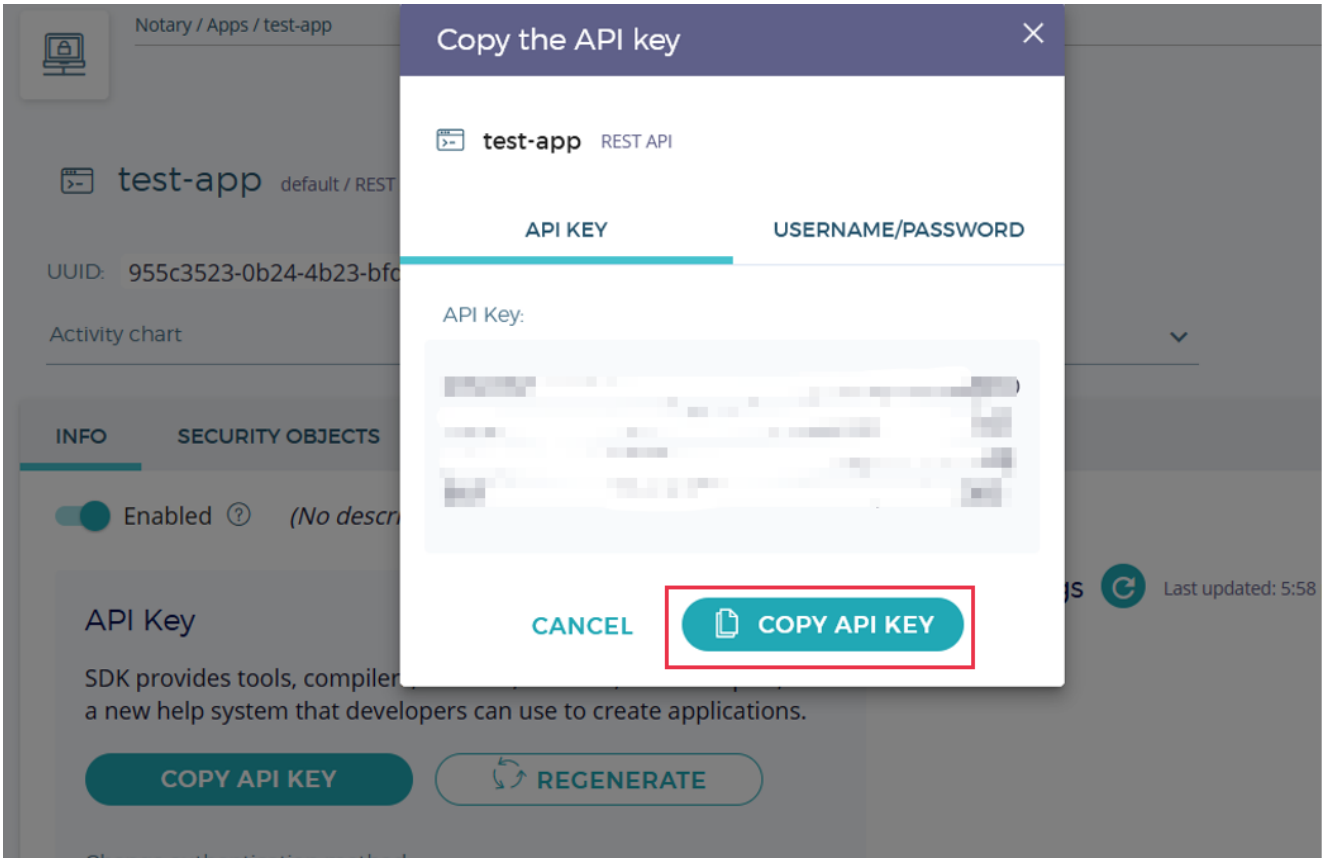

FIGURE 2: COPY THE API KEY OF THE APP

5.0 DEPLOY DKE SERVICE

A Double Key Encryption Service is required to be deployed, which exposes the external key for use by Microsoft 365 services. Microsoft provides a sample DKE Service code which works with local encryption key file https://github.com/Azure-Samples/DoubleKeyEncryptionService

Fortanix provided DKE Service is enhanced to add support for Fortanix DSM Keys. This now serves keys and offloads decryption operations to Fortanix DSM, instead of operating on local key files.

The DKE service can be easily installed as Azure App Service or on your on-premises IIS Server.

5.1 DEPLOY ON IIS

- Download the DKE Service deployment bundle from here https://s3-us-west-1.amazonaws.com/downloads.fortanix.com/dke-service/Fortanix-DSM-DKE-Service-1.0.zip
- Unzip this zip file into the IIS `wwwroot` folder. For example: `C:\inetpub\wwwroot\AspNetCore46`
    - Edit the `appsettings.json` file and add configurations as per Section 5.3.
    - Load your application.

NOTE: Make sure that the IIS deployment is accessible over the internet to your Microsoft Office end-user. This is because Microsoft Apps directly access DKE Service for Key access and decryption.

5.2 DEPLOY ON AZURE APP SERVICE

1. Download the DKE Service deployment bundle from here https://s3-us-west-1.amazonaws.com/downloads.fortanix.com/dke-service/Fortanix-DSM-DKE-Service-1.0.zip
2. Unzip this zip file locally into some temporary folder. Edit the `appsettings.json` file and add configurations as per *Section 5.3*. Zip the folder again and keep it ready for *Section 5.2.1*.
3. In your browser, sign into the Microsoft Azure portal and go to **App Services** > **Create**.
4. Select your subscription and resource group and define your instance details.
5. Enter the **Name** which will form the DKE Service endpoint.
6. For the **Publish** field, select **code**.
7. For the **Runtime stack** field, select **.NET Core 3.1 (LTS)**.
8. At the bottom of the page, click **Review + create**, and then select **Add**.

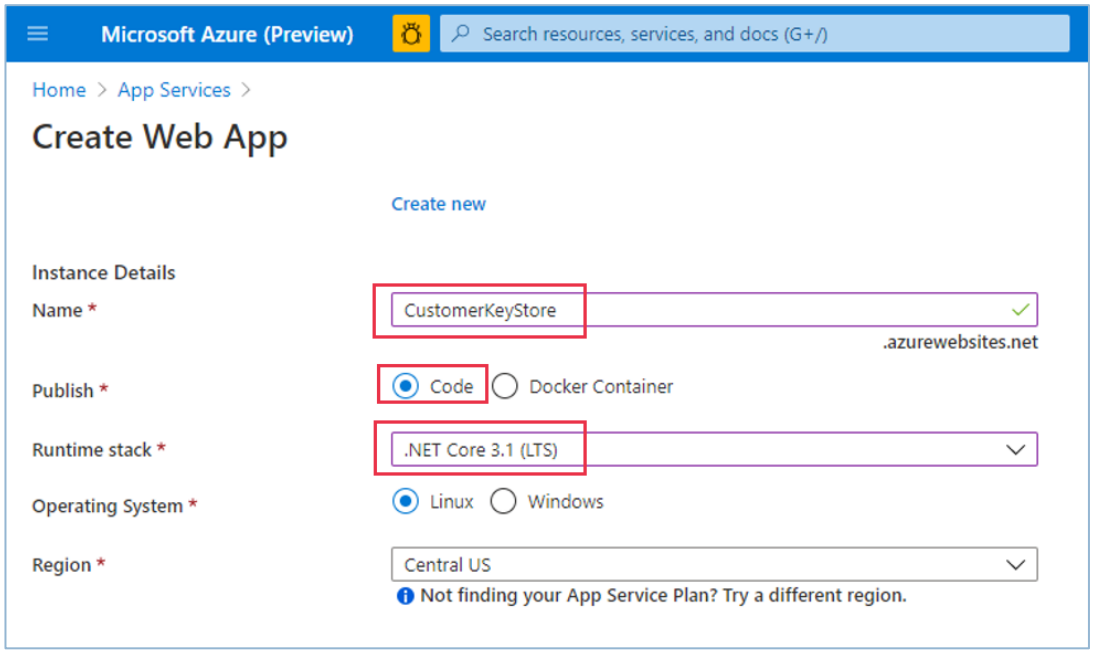

FIGURE 3: CREATE WEB APP

5.2.1 PUBLISH CODE

After the Web App is created, the actual DKE Service can be installed by uploading the DKE service artifact zip file as following:

1. Go to "https://<WebAppName>.scm.azurewebsites.net/ZipDeployUI".

   For example: https://dkeservice.scm.azurewebsites.net/ZipDeployUI

2. Drag and drop the DKE service zip file as per Step 2 of *Section 5.2*.

5.3 CONFIGURE DKE SERVICE

The DKE service requires a few configurations to be set up as explained in the sections below. Set the deployment configuration in the file `appsettings.json` as following:

5.3.1 TENANT ID

Edit the section `ValidIssuers` and update the value:

`https://sts.windows.net/<tenantid>/`

where `<tenantid>` is the Azure Active Directory tenant ID. For example:

```
"AzureAd": {
      "Instance": "https://login.microsoftonline.com/",
      "ClientId": "[Client_id-of-web-api-eg-2ec40e65-ba09-4853-bcde-bcb60029e596]",
      "TenantId": "common",
      "Authority": "https://login.microsoftonline.com/common/v2.0",
      "TokenValidationParameters": {
              "ValidIssuers": [
                      "https://sts.windows.net/9c99431e-b513-44be-a7d9-e7b500002d4b/"
              ]
       }
}
```

5.3.2 JWT AUDIENCE

Edit the section `JwtAudience` with the endpoint of the IIS server or Azure App Service endpoint. For example:

```
"JwtAudience" : "https://dkeservice.mycompanydomain.com"
```

5.3.3 DSM API ENDPOINT

Edit the section `FortanixDSMConfig:ApiEndpoint` with the endpoint of the Fortanix DSM cluster. For example:

```
"FortanixDSMConfig": {
    "ApiEndpoint": "https://sdkms.fortanix.com"
}
```

5.3.4 DSM API KEY

Edit the section `FortanixDSMConfig:ApiKey` with the authentication DSM API Key copied from *Section 4*. For example:

```
"FortanixDSMConfig": {
    "ApiKey": "BJ0oijJYHYU78h6g...05KGkh84GJLK"
}
```

5.3.5 AUTHORIZED EMAIL ADDRESSES

NOTE: This is an optional configuration.

Add section `AuthorizedEmailAddress` with the list of specific users allowed to use Fortanix DSM Keys for decryption. If this is empty or not present, then all the users from your Azure AD tenant are allowed access. For example:

```
"AuthorizedEmailAddress": ["userA@xyz.com", "userB@xyz.com"]
```

5.3.6 FINAL CONFIGURATION

Following is an example of the final `appsettings.json` file:

```
{
   "AzureAd": {
            "Instance": "https://login.microsoftonline.com/",
            "ClientId": "[Client_id-of-web-api-eg-2ec40e65-ba09-4853-
 bcde-bcb60029e596]",
            "TenantId": "common",
            "Authority":
 "https://login.microsoftonline.com/common/v2.0",
            "TokenValidationParameters": {
                    "ValidIssuers": ["https://sts.windows.net/9c99431e-
 b513-44be-a7d9-e7b500002d4b/"]
            }
    },
    "Logging": {
            "LogLevel": {
                    "Default": "Information"
```

```
            },
            "EventLog": {
                    "LogLevel": {
                            "Default": "Information"
                     }
            }
   },
   "AllowedHosts": "*",
   "JwtAuthorization":
 "https://login.windows.net/common/oauth2/authorize",
   "JwtAudience": "https://dkeservice.mycompanydomain.com",
   "AuthorizedEmailAddress": ["userA@xyz.com", "userB@xyz.com"],
   "FortanixDSMConfig": {
            "ApiEndpoint": "https://sdkms.fortanix.com",
            "ApiKey": "BJ0oijJY...0kh84GJLK"
   }
}
```

5.4 REGISTER DKE APP IN AZURE AD

The deployed DKE Service must be registered for Microsoft 365 access. This registration allows Microsoft apps to generate authentication tokens for the DKE service.

1. In your browser, open the Microsoft Azure portal, and go to **All Services** > **Other** > **App registrations**.
2. Select **New registration** and enter a meaningful name.
3. Select an account type from the options displayed (usually the value to be selected is “Single tenant”).

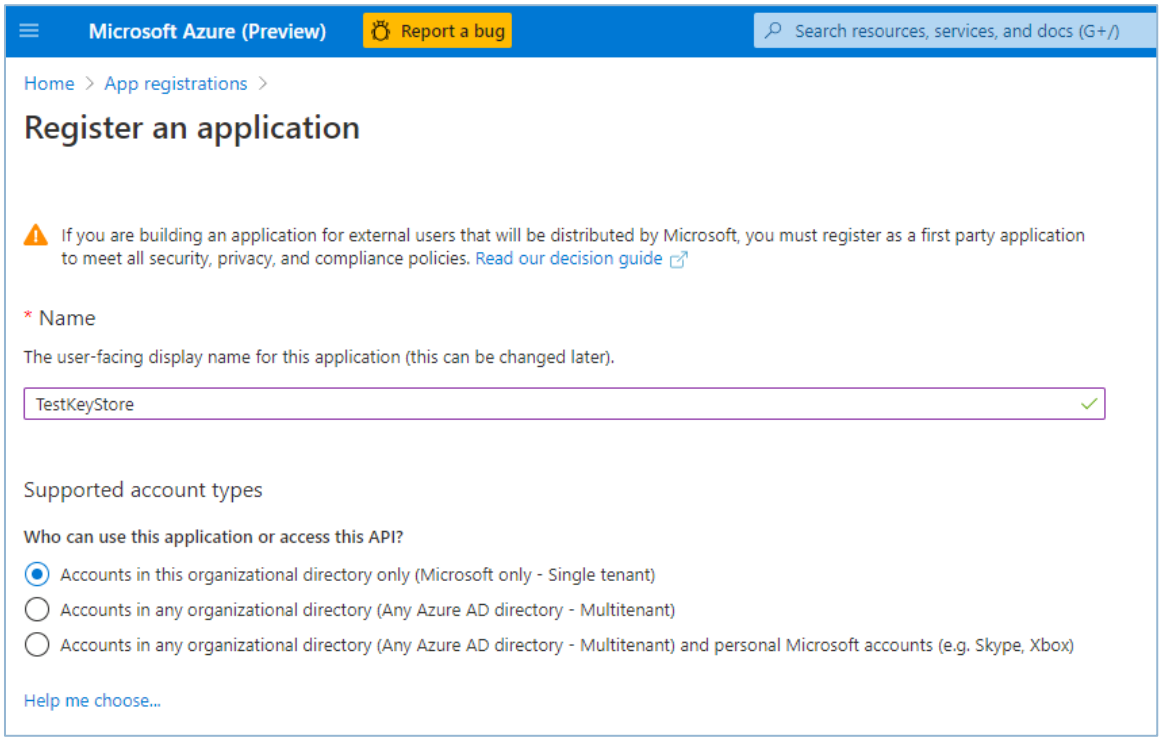

FIGURE 4: REGISTER APPLICATION

4. At the bottom of the page, select **Register** to create the new App Registration.
5. In your new App Registration, in the left pane, under **Manage**, select **Authentication**.
6. In the Platform configurations, click **Add a platform**.
7. On the **Configure platforms** popup, select **Web**.
8. Under **Redirect URIs**, enter the URI of your double key encryption service. Enter the DKE Service Endpoint URL, For example: https://dkeservice.azurewebsites.net
9. Under **Implicit grant and hybrid flows**, select the **ID tokens** check box.
10. Click **Configure** to save your changes.
11. On the left pane, select **Expose an API**, then next to Application ID URI, click **Set**. Enter the DKE Service endpoint URL, For example: https://dkeservice.azurewebsites.net. Click **Save**.
12. On the **Expose an API** page, in the **Scopes defined by this API** section, select **Add a scope**. In the new scope form:
    a. Define the **Scope name** as `user_impersonation`.
    b. Select the administrators and users who can consent.
    c. Define any remaining values required.
    d. Click **Add scope** to save your changes.

13. On the **Expose an API** page, in the **Authorized client applications** section, select **Add a client application**. In the new client application:
    a. Define the **Client ID** as **`d3590ed6-52b3-4102-aeff-aad2292ab01c`** (Please use this exact value). This value is the Microsoft Office client ID which enables Office to obtain an access token against the DKE Service.
    b. Under **Authorized scopes**, select the **user_impersonation** scope.
    c. Click **Add application** to save your changes.

14. Repeat the above steps for another Client ID as **`c00e9d32-3c8d-4a7d-832b-029040e7db99`** (Please use this exact value). This value is the client ID for Microsoft Azure Information Protection Client.

5.5 CREATE SENSITIVITY LABELS USING DKE

In the Microsoft 365 compliance center:

1. Create a new sensitivity label and apply encryption as you would otherwise.
2. Select **Use Double Key Encryption** and enter the endpoint URL for your key. For example: https://***dkeservice.mycompanydomain.com/*MicrosoftDKEServiceKey**.
   Where **MicrosoftDKEServiceKey** is the name of the Fortanix DSM Key created in *Section 4.0*.

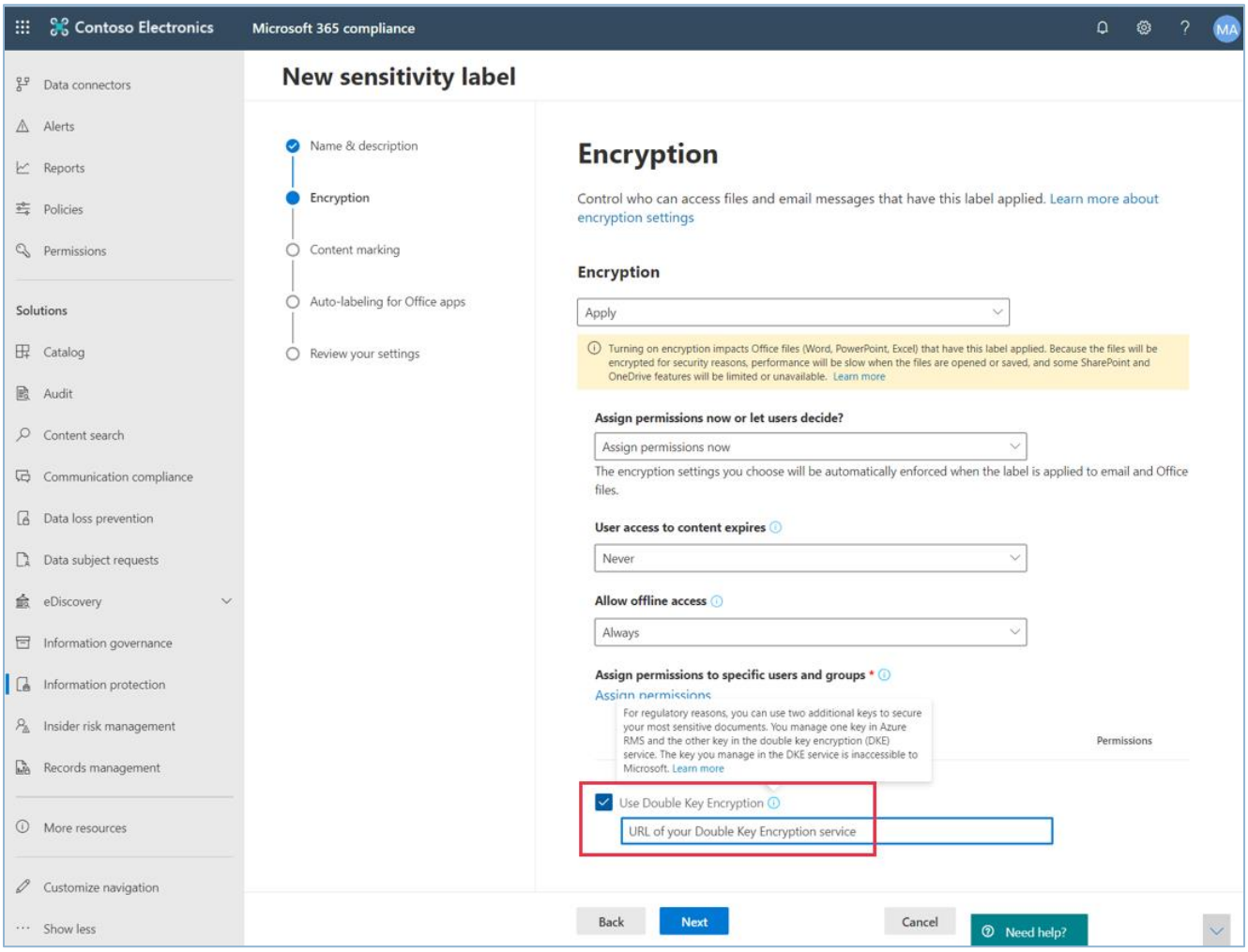

FIGURE 5: NEW SENSITIVITY LABEL

Any DKE labels that you add will start appearing for users in the latest versions of Microsoft 365 Apps for the enterprise.

Now you can apply these labels to the Microsoft Documents. Once these labels are applied, the document is kept encrypted using Fortanix DSM Keys.

6.0 REFERENCES

1. Double Key Encryption for Microsoft 365: https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption
2. Double Key Encryption Troubleshooting guide by Microsoft: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/dke-troubleshooting/ba-p/2234252

3. Fortanix DSM Getting started:

   https://support.fortanix.com/hc/en-us/articles/360015809372-Getting-Started-with-SDKMS

7.0 DOCUMENT INFORMATION

7.1 DOCUMENT LOCATION

The latest published version of this document is located at: https://support.fortanix.com/hc/en-us/articles/4403253339412-Fortanix-Data-Security-Manager-with-Double-Key-Encryption-for-Microsoft-365

7.2 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