Microsoft Double Key Encryption and Entrust KeyControl

Integration Guide

2024-06-21

Member of
Microsoft Intelligent
Security Association

Microsoft Security

Table of Contents

Chapter 1. Introduction

This document describes the integration of Microsoft 365 Double Key Encryption (DKE) with the Entrust KeyControl key management solution. KeyControl serves as a key manager for encryption keys by using various protocols, including KMIP.

1.1. Product configuration

Entrust has successfully tested the integration of Entrust KeyControl with Microsoft 365 DKE in the following configurations:

Product	Version
Entrust KeyControl	10.2

1.2. Features tested

Entrust has successfully tested the following features:

- Create DKE key
- Rotate DKE key
- Remove DKE key
- Delete DKE key
- Cancel DKE key deletion

1.3. Requirements

1.3.1. Licensing

DKE is supported with Microsoft 365 Enterprise E5 or above licenses. See System and licensing requirements for DKE.

1.3.2. Microsoft 365 applications

DKE is supported on Microsoft 365 applications on Windows desktop versions. It is not supported for access via the web or Mac versions of Microsoft 365.

1.3.3. Documentation

Before starting the integration process, familiarize yourself with:

- Microsoft Online Documentation.
- Entrust KeyControl Online Documentation Set.
- Entrust KeyControl Cloud Key Management for DKE.

Chapter 2. Deploy Entrust KeyControl

In order to provide uninterrupted access to the keys, in production deploy a cluster of at least 2 KeyControl Vault instances behind a load balancer. Use the load balancer FQDN when specifying the URL of the DKE key in the compliance label, and when registering the Azure application that provides authentication for the service.

If you use a single KeyControl instance you can access it directly, and use its FQDN directly. We will use the term 'Service FQDN' for the address used to access the service whether it is a load balancer or KeyControl instance.

You will need to include the Service FQDN in the SSL certificate on the cluster. In order to register the Azure App, the Service FQDN needs to be in a domain verified with the Azure account, see Add your custom domain name to your tenant.

The following steps summarize the deployment of the Entrust KeyControl.

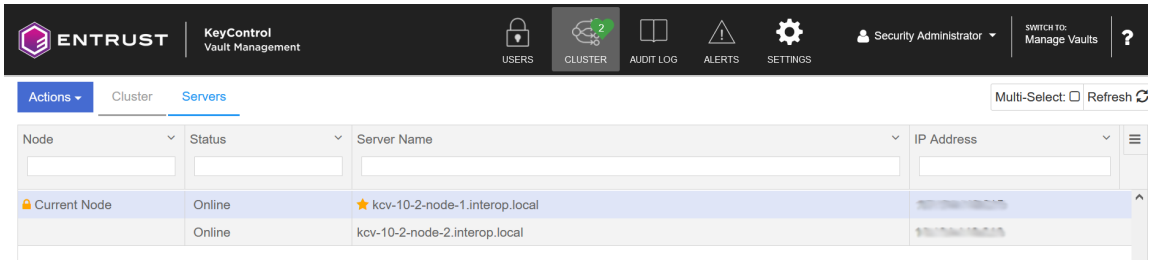
1. Deploy an Entrust KeyControl cluster
2. Install certificate authority (CA) certificate
3. Create a Cloud Key Management Vault in Entrust KeyControl

2.1. Deploy an Entrust KeyControl cluster

For the purpose of this integration, a single-node Entrust KeyControl cluster was deployed in Azure. This cluster can be reached at the load balancer hostname.

1. Deploy the Entrust KeyControl node per Deploying a KeyControl Vault Node in Azure.
2. Bookmark the public IP.
3. Configure the node per Configuring the First KeyControl Vault Node.
4. If deploying two-nodes, configure the second node per Configuring Additional KeyControl Vault Nodes.

Following is an example of the WEB GUI of a two-node Entrust KeyControl cluster deployed on-premises.



2.2. Install certificate authority (CA) certificate

The Entrust KeyControl cluster needs a certificate from your private root CA, or a trusted public CA, per your organization policies.

1. Create a certificate signing request (CSR) per Creating a Certificate Signing Request.
2. Have your private root CA, or a trusted public CA, sign the CSR.
3. Install the signed certificate per Installing External Certificates for Internal and External Webservers.

2.3. Create a Cloud Key Management Vault in Entrust KeyControl

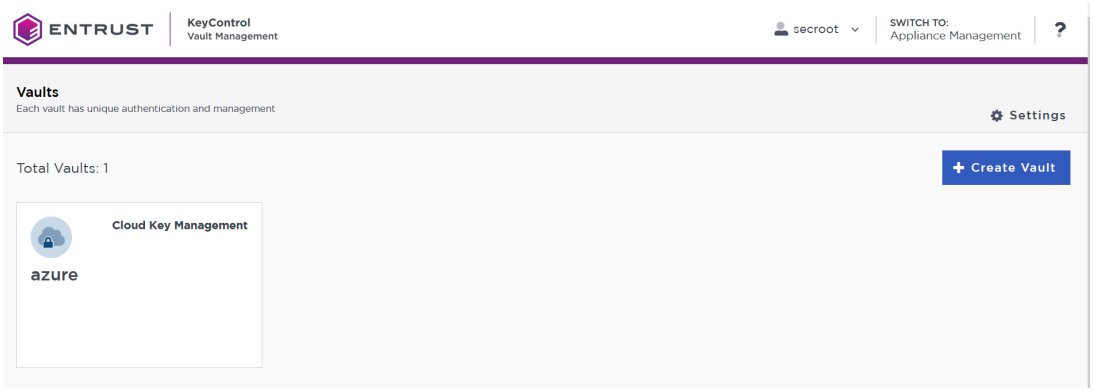
The Entrust KeyControl Vault appliance supports different type of vaults that can be used by all type of applications. This section describes how to create a **Cloud Key Management** vault in the Entrust KeyControl vault server.

1. Create a vault per Creating a Vault. The vault **Type** is **Cloud Key Management**.

> Once the vault is created successfully, the new vault's URL and sign-in credentials will be emailed to the administrator's email address entered above. In closed gap environments where email is not available, the URL and sign-in credentials are displayed at this time.

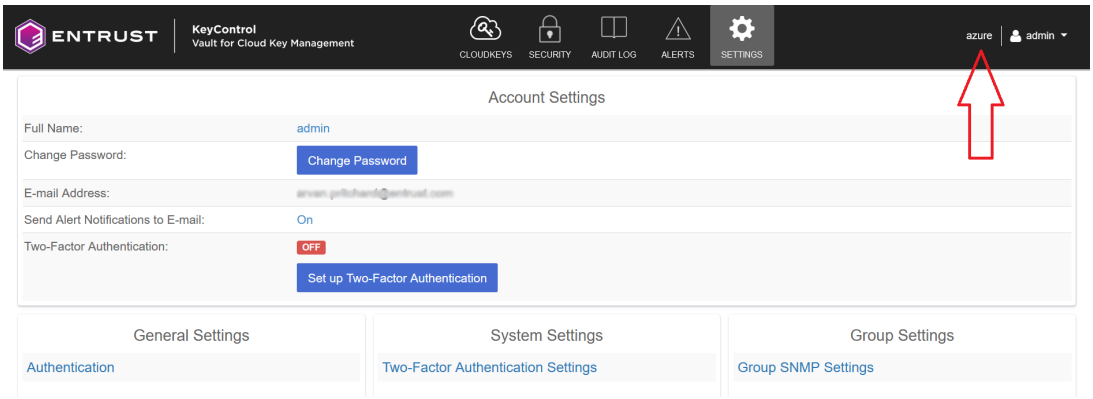
2. Bookmark the **Vault URL**. Copy the **User Name** and **Temporary Password**.
3. The newly created Vault is added to the **Vault Management** dashboard.

   For example:



4. Sign in to the URL provided above with the temporary password. Change the initial password when prompted. Sign in again to verify.
5. Notice the new vault.

   For example:



Chapter 3. Deploy a Microsoft 365 client computer

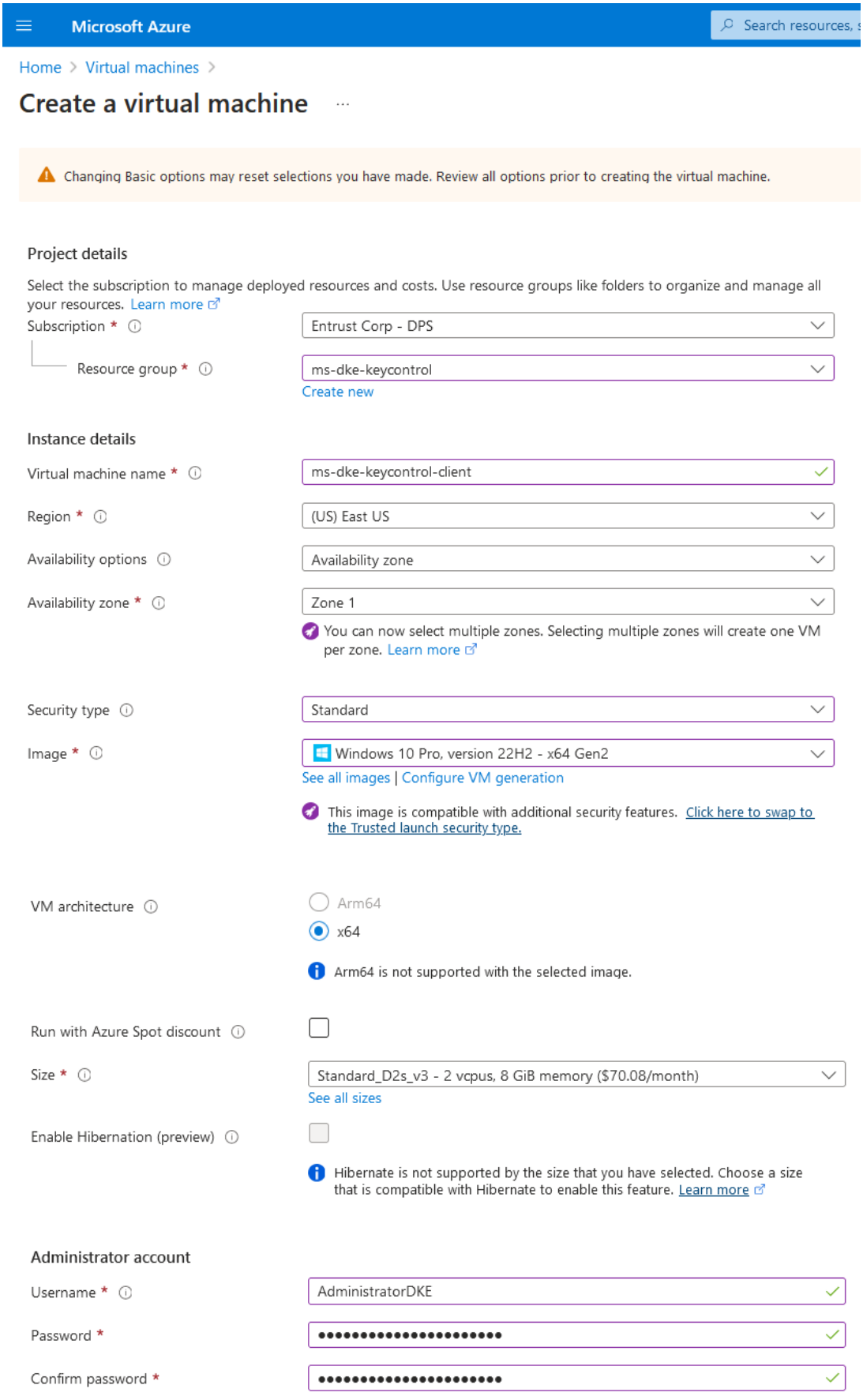
For the purpose of this integration, the Microsoft 365 client computer was deployed as a VM in Azure. You can also use an existing Microsoft 365 client computer.

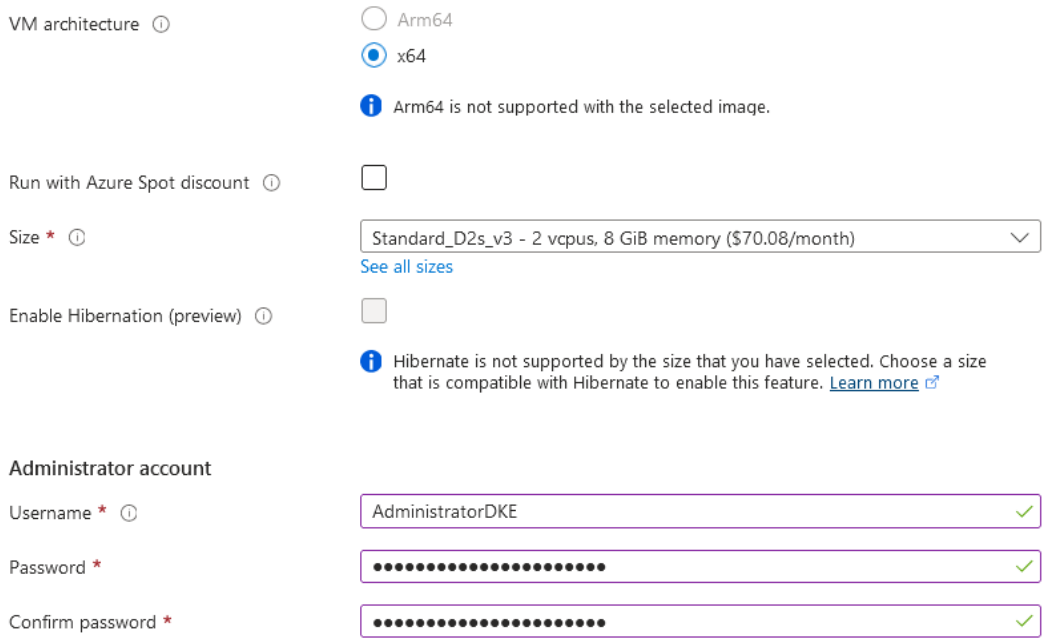
- Create a Microsoft 365 client computer
- Install the root CA certificate

3.1. Create a Microsoft 365 client computer

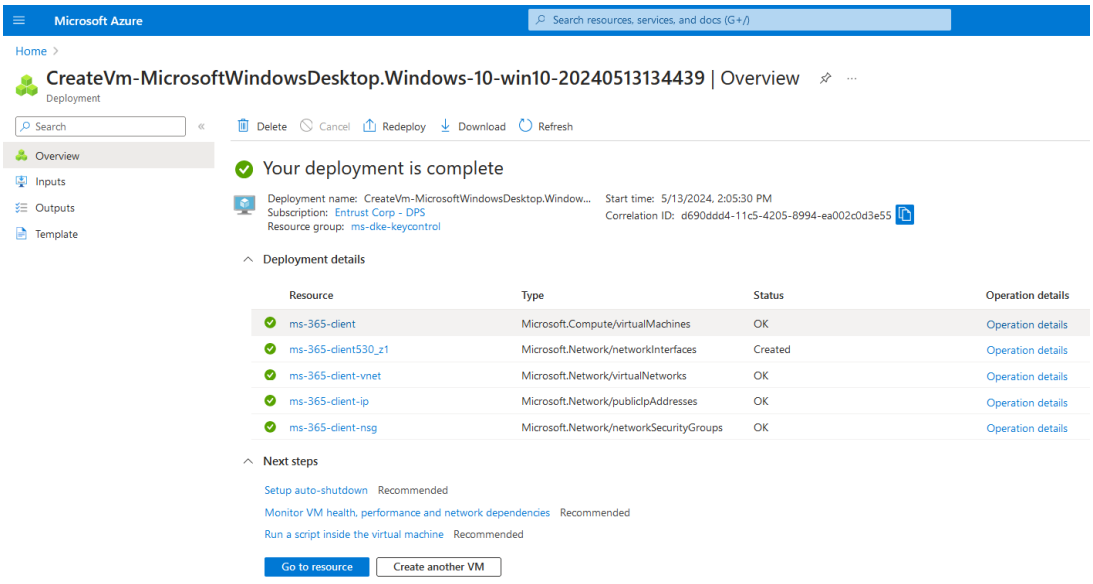
1. Sign in to the Azure portal https://portal.azure.com/#home with any valid account.
2. Navigate to **Virtual Machines** and create the Microsoft 365 client computer.

   For example:


Microsoft Azure
Search resources,
Home > Virtual machines >
Create a virtual machine
Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources. Learn more
Subscription *
Entrust Corp - DPS
Resource group *
ms-dke-keycontrol
Create new
Instance details
Virtual machine name *
ms-dke-keycontrol-client
Region *
(US) East US
Availability options
Availability zone
Availability zone *
Zone 1
You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more
Security type
Standard
Image *
Windows 10 Pro, version 22H2 - x64 Gen2
See all images | Configure VM generation
This image is compatible with additional security features. Click here to swap to the Trusted launch security type.
VM architecture
Arm64
x64
Arm64 is not supported with the selected image.
Run with Azure Spot discount
Size *
Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($70.08/month)
See all sizes
Enable Hibernation (preview)
Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. Learn more
Administrator account
Username *
AdministratorDKE
Password *
Confirm password *



3. Notice the VM created.



3.2. Install the root CA certificate

Install a certificate from your private root CA, or a trusted public CA. If using a private root CA, use the same used to sign the Entrust KeyControl cluster CSR. Install the certificate in the **Trusted Root Certificate Authorities** folder.

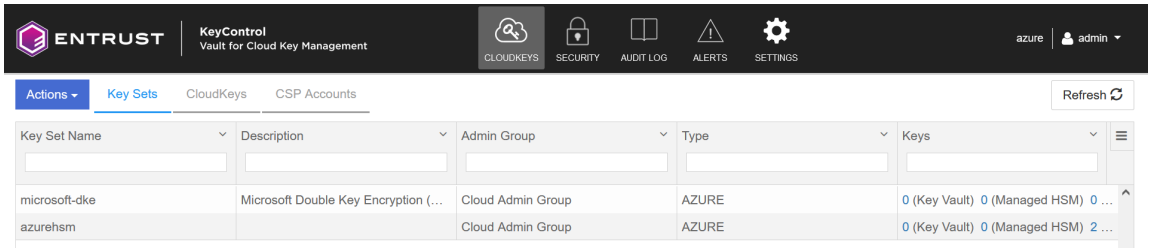
Chapter 4. Create a key for Microsoft 365 DKE

1. Create a key set for DKE
2. Create a cloud key for Microsoft 365 DKE

4.1. Create a key set for DKE

Create the key set per Creating a Key Set for DKE.

For example, the key set named **microsoft-dke** was created for the purpose of this integration.



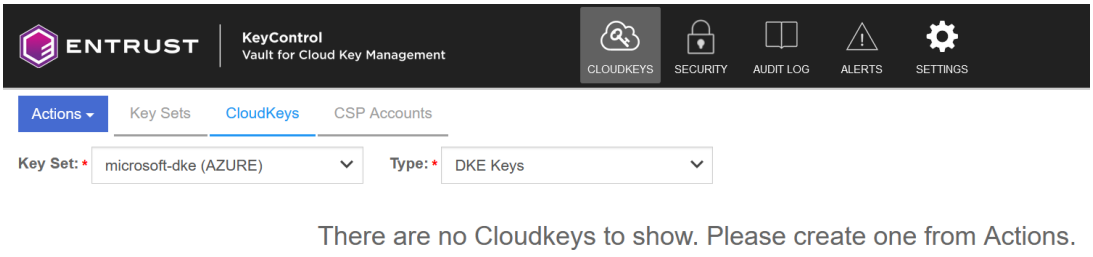
The number of DKE keys in each Key Set is shown on the **Key Sets** tab, last column in the right.

4.2. Create a cloud key for Microsoft 365 DKE

The Microsoft 365 DKE keys are not replicated to Azure. These are stored in the Entrust KeyControl in a separate area alongside the Azure KeyVaults and managed HSMs.

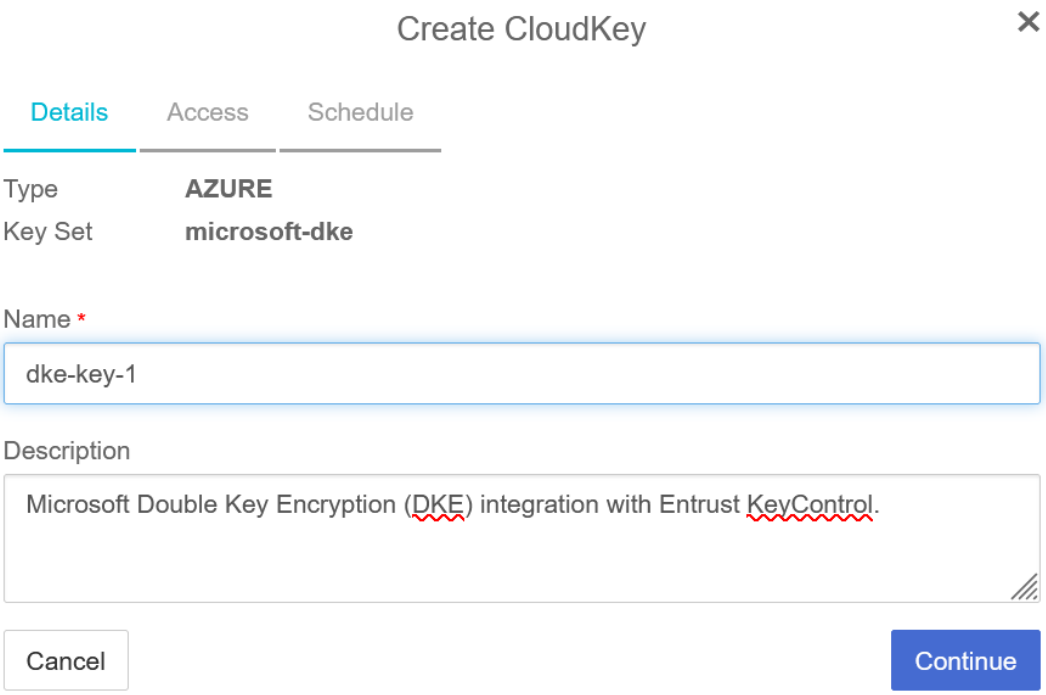
Create a cloud key per Creating a CloudKey for DKE. For example:

1. In the **Actions** menu select **Key Set** and **Type** as shown.



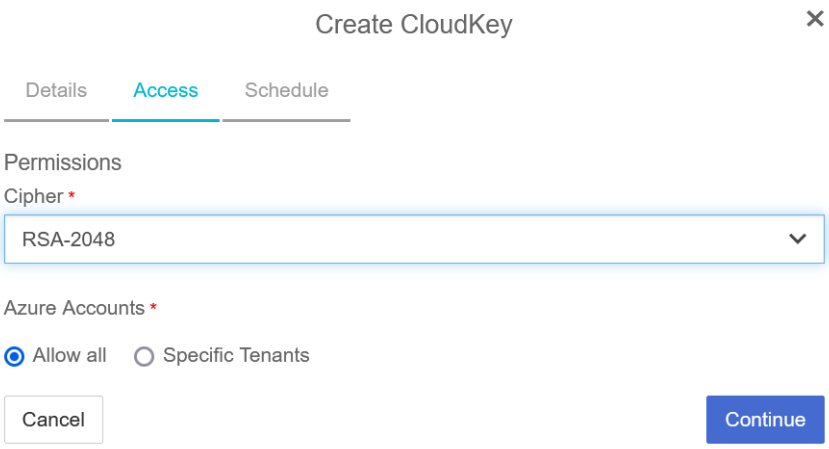
2. In the **Details** tab of the **Create CloudKey** window, enter the **Name** and

Description.



3. In the **Access** tab select which Azure accounts can access the key. Select either **Allow all** or **Specific Tenants**. This selection can be changed later, after the key is created.

> If specific tenants are specified, only users who authenticate with those tenants can access the key for DKE encryption and decryption.

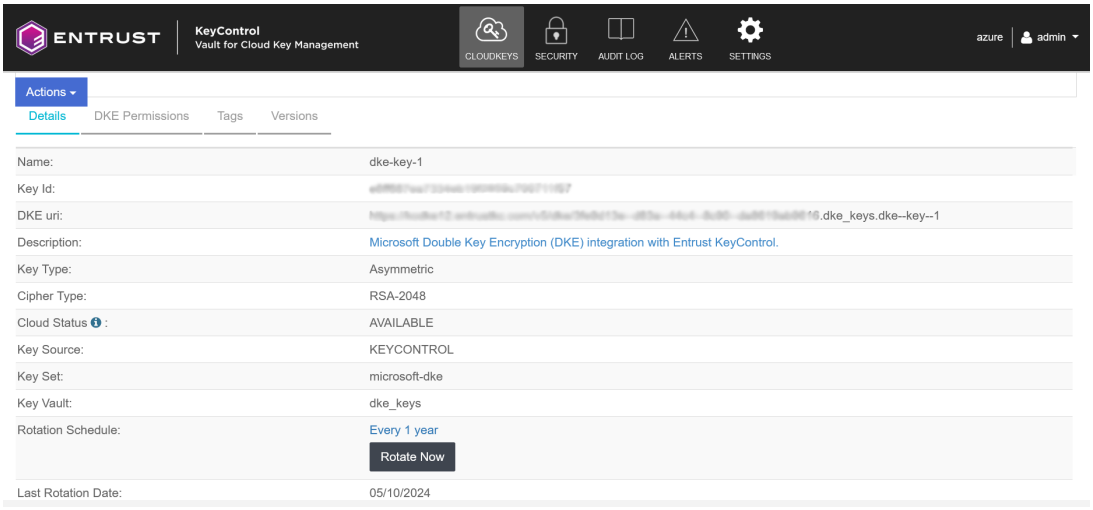


4. In the **Schedule** tab select the rotation schedule.

> Key rotation and tag setting behave the same as any other cloud keys. Key deletion moves the key into a Pending

> Delete state for a chosen period. The key is fully deleted at the end of that period or can be recovered or manually purged earlier. DKE keys can be disabled, and while disabled cannot be used for DKE encryption or decryption.

5. Select the key just created and scroll down to see the details. Notice the various tabs.



Chapter 5. Configure Microsoft Azure

For the purpose on this integration, the Azure Microsoft Entra accounts were provided by Microsoft as a Microsoft 365 development environment. The actual users are part of the quick-start environment Microsoft offers. These have Microsoft 365 Enterprise E5 or above licenses. Alternatively, use your own account with provided it has the license listed above.

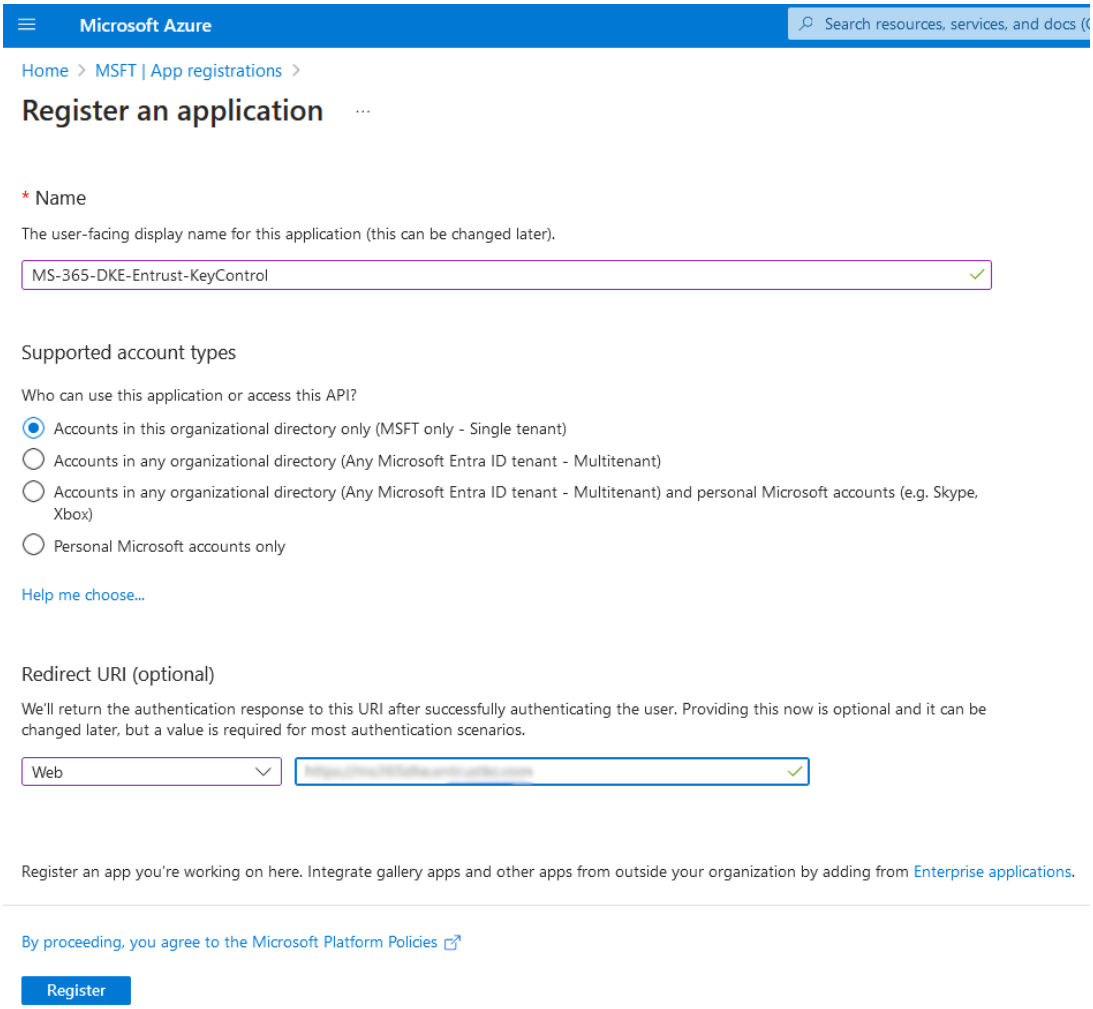
The Microsoft 365 account is linked to an Azure Active Directory. Users will be authenticated with it in order to be able to decrypt using the DKE keys. The tenant GUID can be specified in the DKE Cloud Key's DKE Permissions list to restrict access to a particular tenant, or list of tenants.

5.1. Create an app registration in Azure

Authentication to access the DKE decryption is performed by an Azure App registration for the FQDN in the URL specified in the compliance label. This requires the FQDN to be in a verified domain for that Azure tenant.

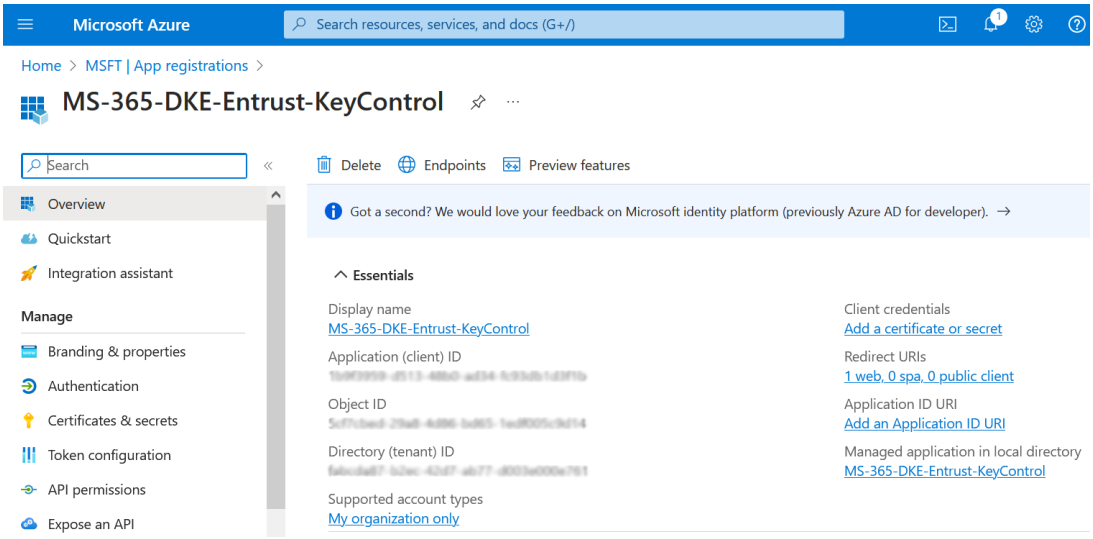
1. Sign in to the Azure portal https://portal.azure.com/#home with the Microsoft 365 account.
2. Navigate to **Microsoft Entra ID** (old **Azure Active Directory**). Type **Microsoft Entra ID** in the search box and select it from the pull-down menu.
3. Select **App registrations** in the left pane, then select the **+ New registration** icon in the right pane.
4. Enter the **Name**, a user-facing or friendly name. Select the radio button for **Who can use this application or access this API?**. Select the applicable **Supported account types** and enter the public URL of the Entrust KeyControl in **Redirect URI**.

   For example:



5. Select **Register**.

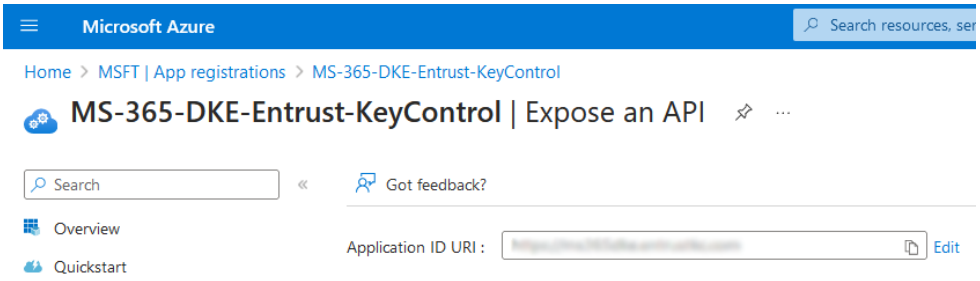
   The newly created registration appears.



6. Select **Expose an API** in the left pane.

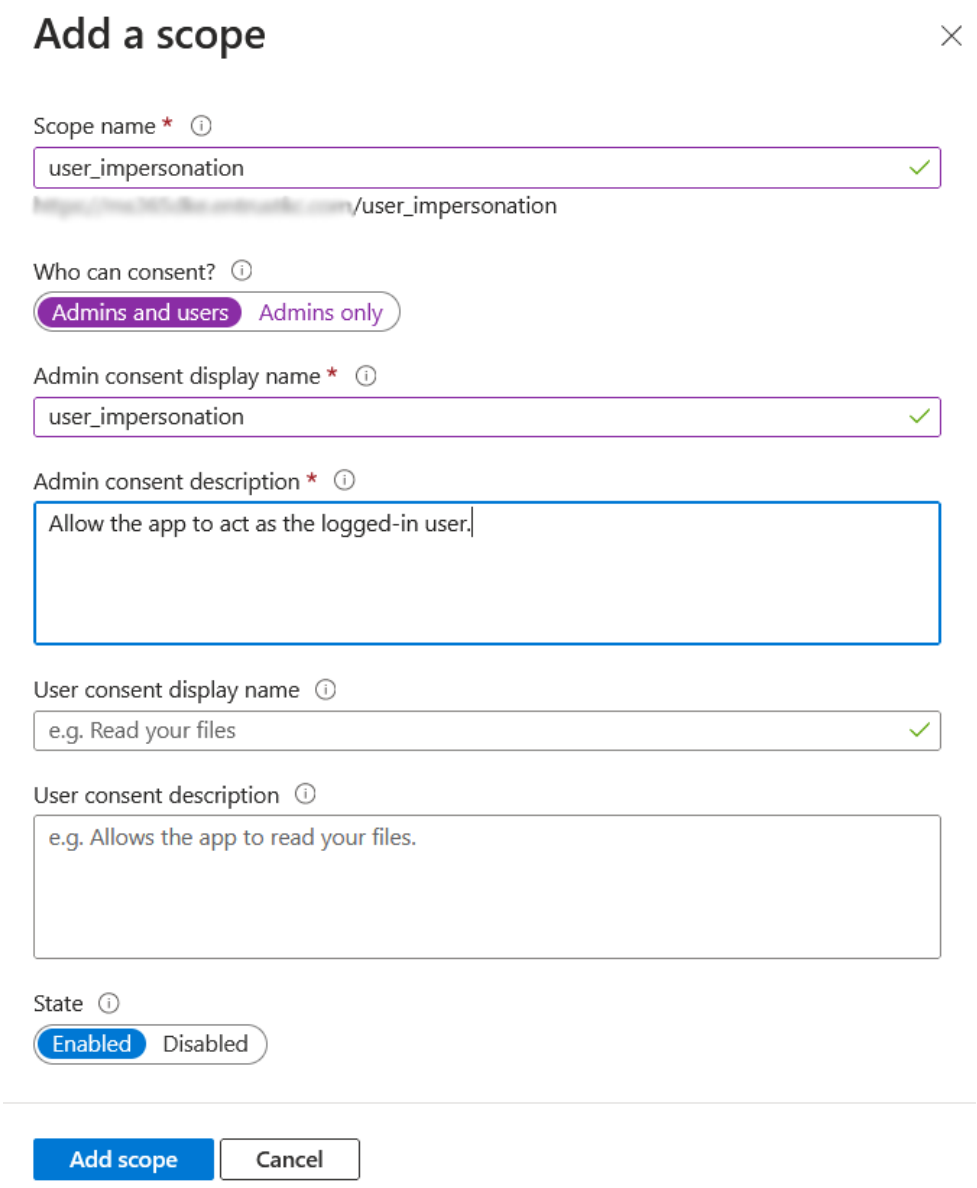
7. Select the **+** icon next to **Application ID URI**. Enter your information, then select **Save and continue**.

   For example:



8. Select the **+** icon next to **Add a scope** to add a scope defined by this API. Enter your information, then select **Add scope**.

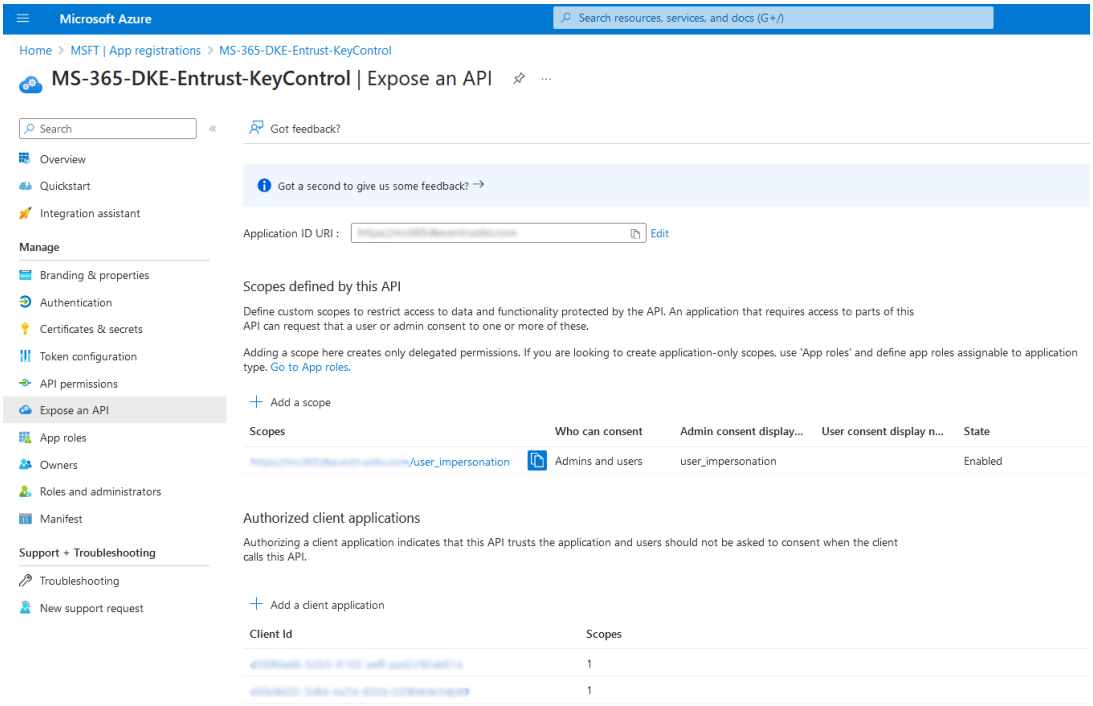
   For example:



9. Select the **+** icon next to **Add a client application** to add an authorized client application. Add the following Microsoft predefined IDs. These are same for everybody, and can be found at Set up Double Key Encryption. Check **Authorized scopes**, then select **Add application**.

ID	Value
Microsoft Office client ID	d3590ed6-52b3-4102-aeff-aad2292ab01c
Information protection client ID	c00e9d32-3c8d-4a7d-832b-029040e7db99

For example:

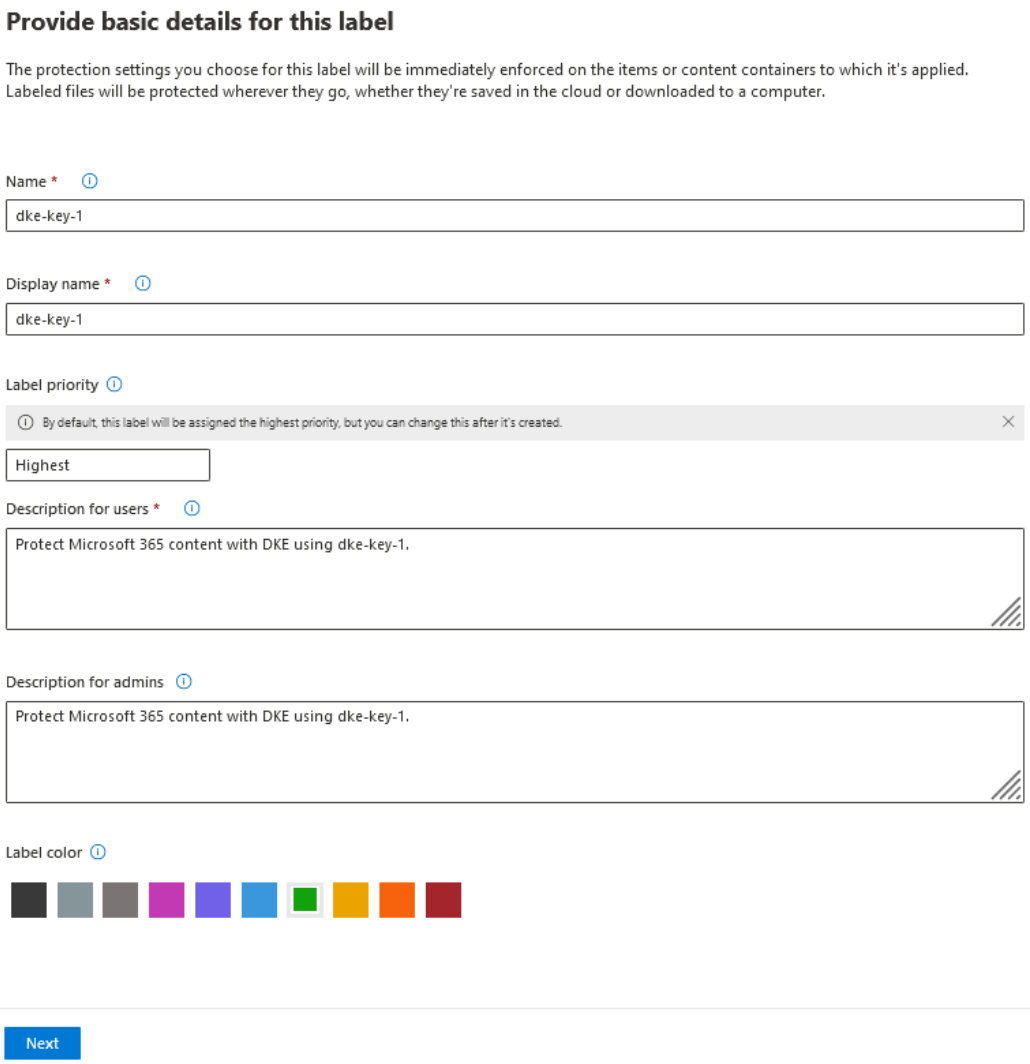


5.2. Add compliance label

Compliance labels are configured in the Microsoft Compliance portal and distributed to specified users and groups in Active Directory. A DKE label contains a URL which can be used to obtain the public key of the DKE key and a corresponding decryption URL.

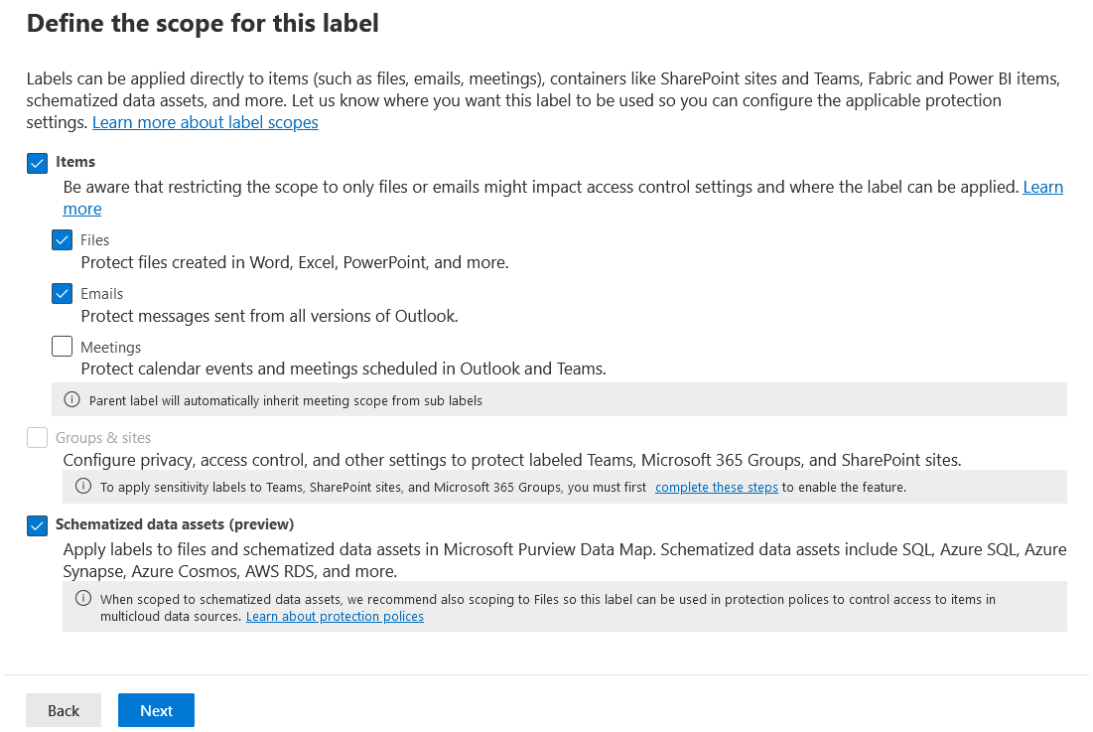
1. Sign in to the Microsoft Purview Compliance Portal at https://compliance.microsoft.com/homepage with the Microsoft 365 account.
2. Select **Labels** under Information protection.
3. Select **Information protection** in the left pane, then select **Labels**.
4. Select the **+** icon next to **Create a label**.
5. In the **Provide basic details for this label** window, enter your information, then select **Next**.

   For example:



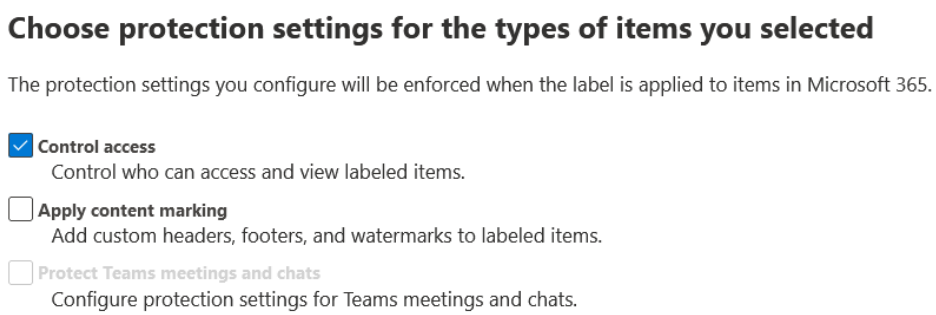
6. In the **Define the scope of this label** window, under **Items**, check **Files** and **Emails**. Un-check **Meetings**, then select **Next**.

   For example:



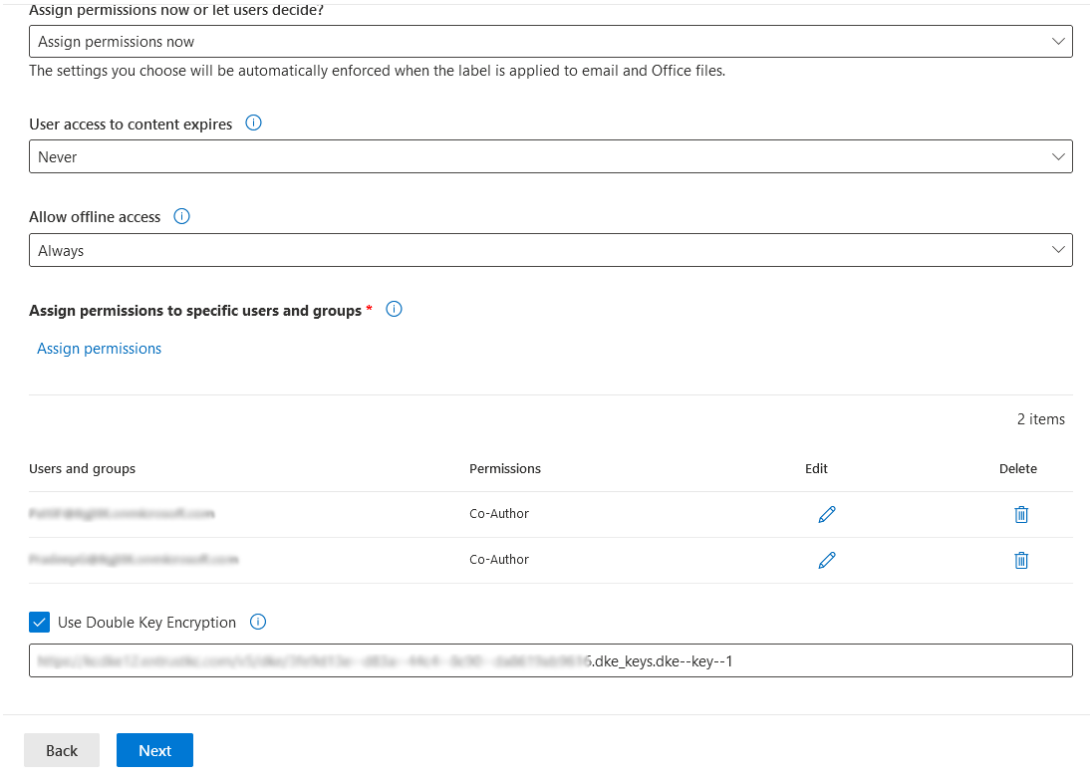
7. In the **Choose protections settings for the types of items you selected** window, check **Control access**, then select **Next**.

   For example:



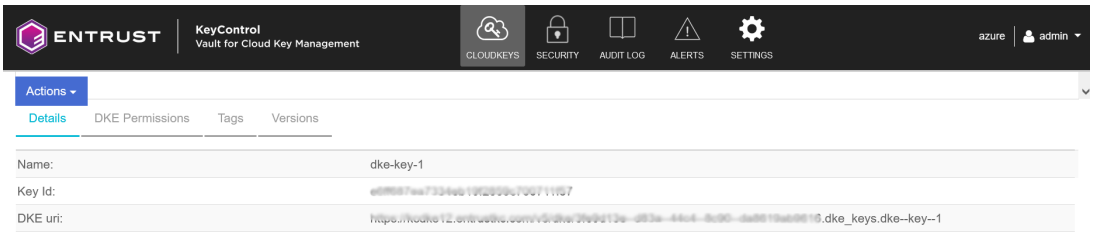
8. In the **Access Control** window, select the **Configure access control settings** radio button.
9. Select **Assign permissions** and add your users or groups.
10. Check **Use Double Key Encryption** and enter the URL for the cloud key, then select **Next**.

    For example - **Access Control** window:



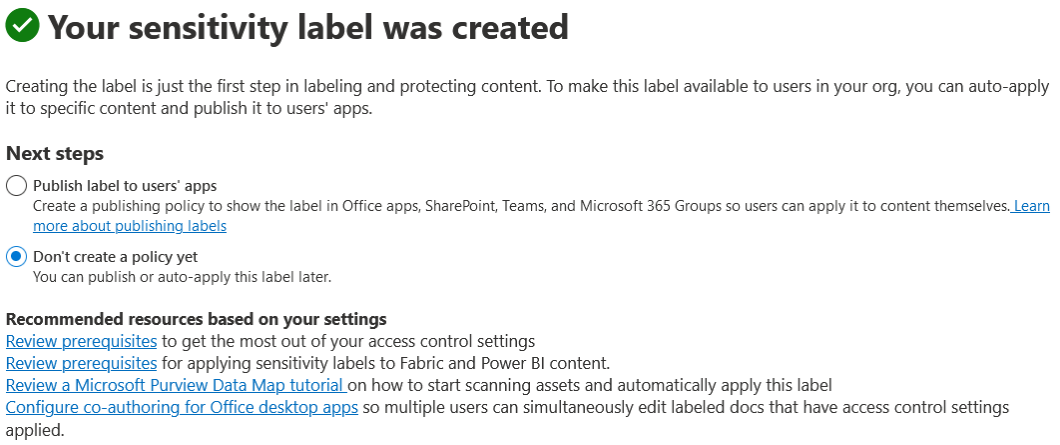
The URL for the cloud key is the **DKE uri** of the cloud key created in Create a cloud key for Microsoft 365 DKE.

For example:



11. In the **Auto-labeling for files and emails**, select per your organizations policies, then select **Next**.
12. In the **Define protection settings for groups and sites** windows, check the settings that apply per your organizations policies, then select **Next**.
13. In the **Auto-labeling for schematized data assets (preview)**, select per your organizations policies, then select **Next**.
14. In the **Review your settings and finish** windows, select and review as needed, then select **Create label**.
15. In the **Your sensitivity label was created**, select the **Don't create a policy yet** radio button, then select **Done**.

    For example:



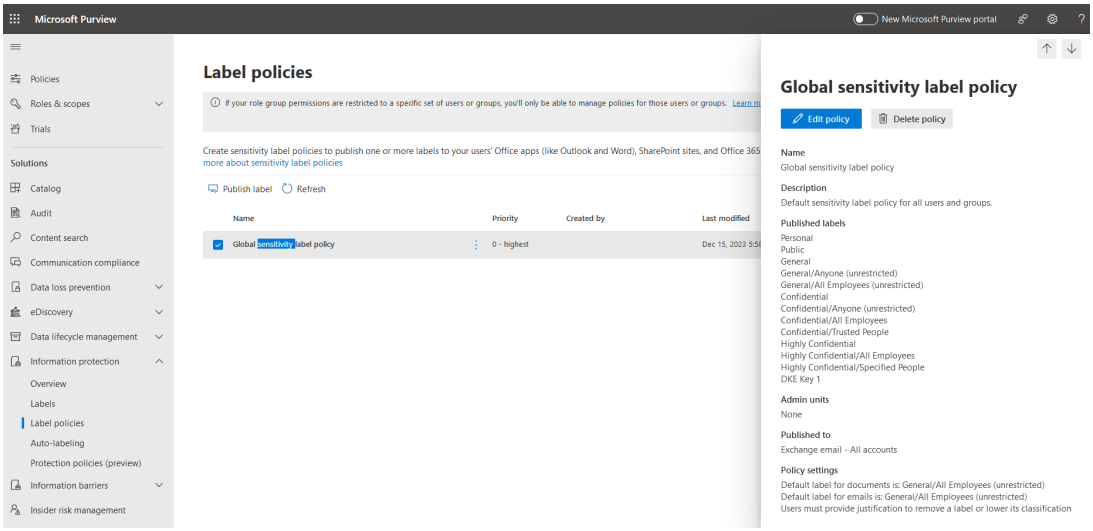
16. Create any other labels you need following the steps above.

5.3. Add label policies

The following steps describe the process of adding the new labels to an existing policy.

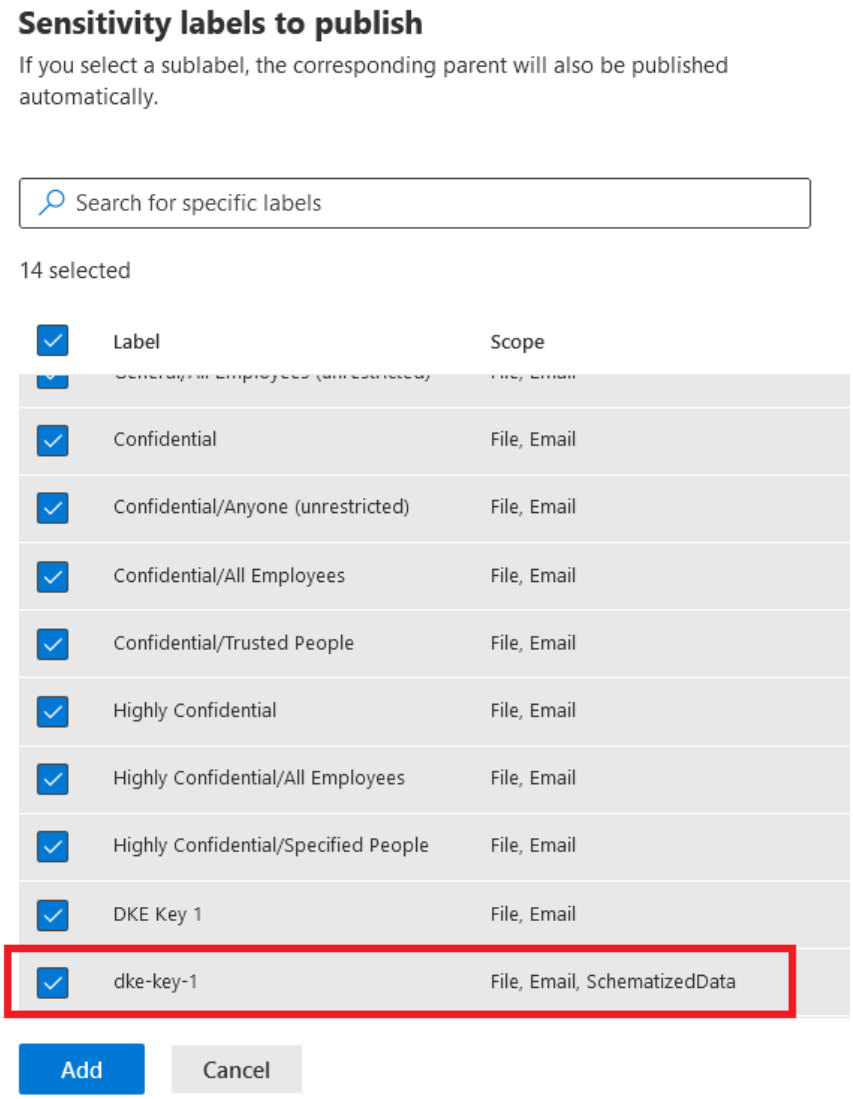
1. Sign in to the Azure portal https://portal.azure.com/#home with the Microsoft 365 account.
2. Open the Microsoft Purview Compliance Portal at https://compliance.microsoft.com/homepage.
3. Select **Labels** under Label policies.
4. Double-click on the selected label to open the **Global selectivity label policy**, then select **Edit policy**.

   For example:



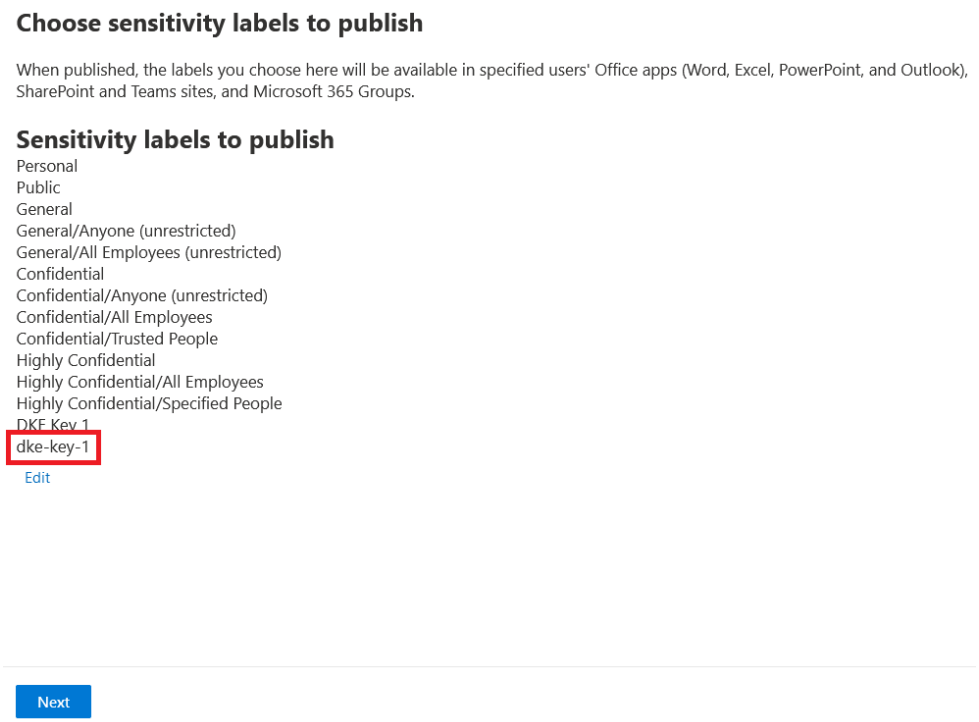
5. In the **Choose sensitivity labels to publish** window, select **Edit**. Check the new labels created in Add compliance label, then select **Add**.

   For example:



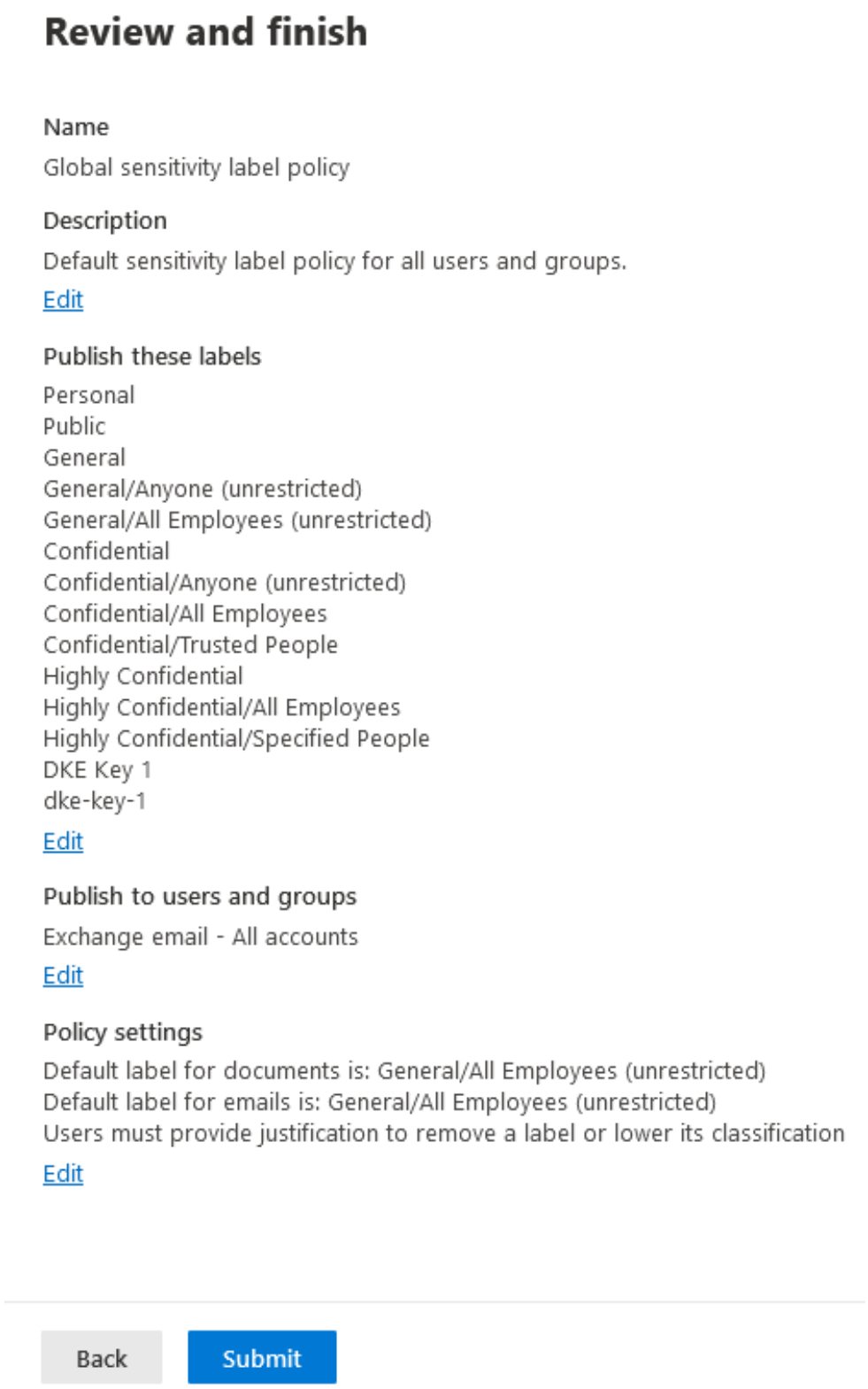
6. Select **Next**.

   For example:



7. In the **Assign admin units** window, add or remove administrative units per your organizations policies, then select **Next**.
8. In the **Publish to users and groups** window, add users and groups per your organizations policies, then select **Next**.
9. In the **Policy settings** windows, check applicable policies. Then select **Next**.
10. In the **Default settings for documents** window, select the **Default label** per your organizations policies, then select **Next**.
11. In the **Default settings for emails** window, select the **Default label** per your organizations policies. Check **Email inherits highest priority label from attachments** if applicable, then select **Next**.
12. In the **Default settings for meetings and calendar events** window, select the **Default label** per your organizations policies, then select **Next**.
13. In the **Default settings for Fabric and Power BI content** window, select the **Default label** per your organizations policies, then select **Next**.
14. In the **Name your policy** window, select **Next**.
15. In the **Review and finish**, make any edits necessary, then select **Submit**.

    For example:



The labels will be propagated according to the policy. It may take some time to appear to the end users.

16. Select **Done**.

For example:

Your sensitivity label policy has been updated.

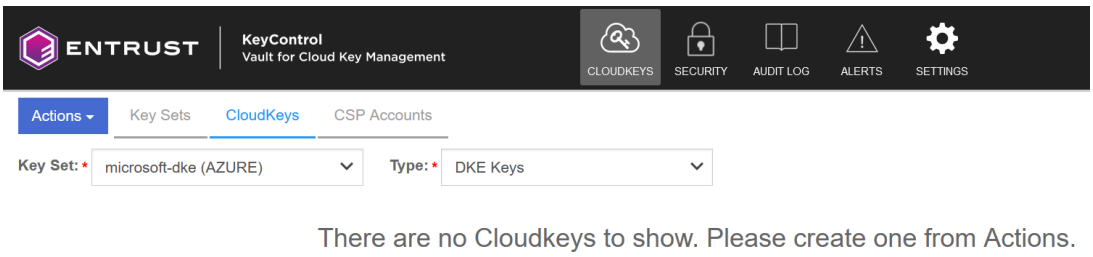
Chapter 6. Test integration

1. Test access to the cloud key for DKE
2. Install the Microsoft 365 apps in the Microsoft 365 client computer
3. Create a test document protected by DKE

6.1. Test access to the cloud key for DKE

These steps test access to the cloud key for DKE created in Create a cloud key for Microsoft 365 DKE.

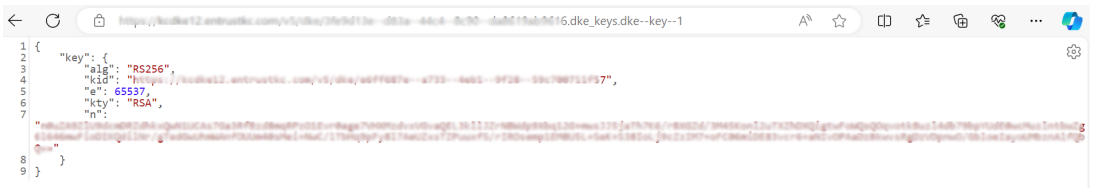
1. Sign in to the Entrust KeyControl Vault URL created in Create a Cloud Key Management Vault in Entrust KeyControl .
2. In the **Actions** menu, select the **Key Set** and **Type** as follows.



3. Select the key and scroll down to see the **Details** tab.
4. Copy the **DKE uri**.
5. Sign in to the Microsoft 365 client computer.
6. Open a browser and paste the **DKE uri** copied above.

   The cloud key for DKE should be accessible.

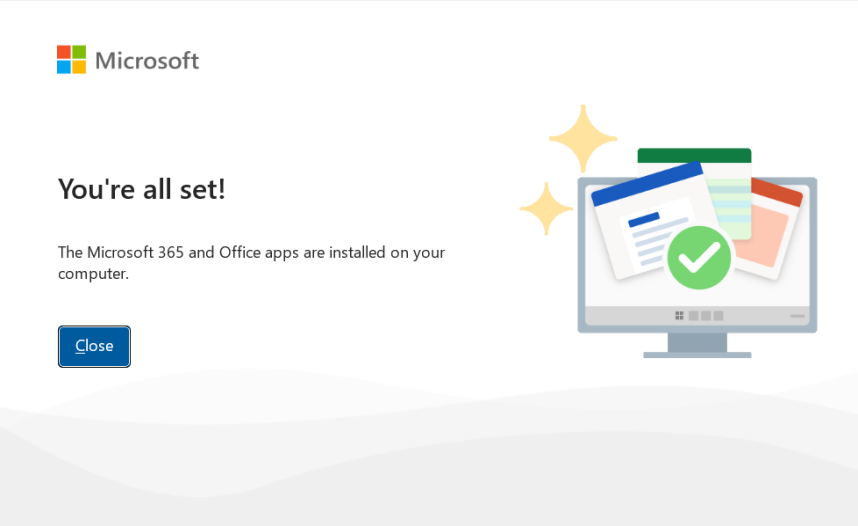
   For example:



6.2. Install the Microsoft 365 apps in the Microsoft 365 client computer

1. Sign in to the Microsoft 365 client computer.

2. Open a browser and sign in to https://office.com with the Microsoft 365 account.
3. In the **Welcome to Microsoft 365** windows, select **Install and more**. In the pull-down menu select **Install Microsoft 365 apps**.
4. In the **Office apps and devices** box, select **Install Office**. The **OfficeSetup** installer will be downloaded to your download folder.
5. Execute the **OfficeSetup** installer.
6. After the installations completes, select **Close**.

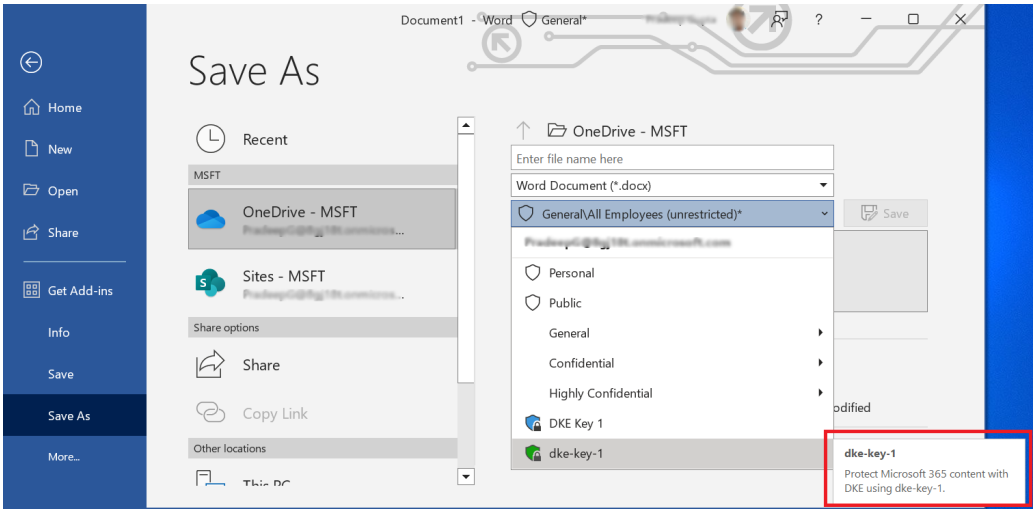


6.3. Create a test document protected by DKE

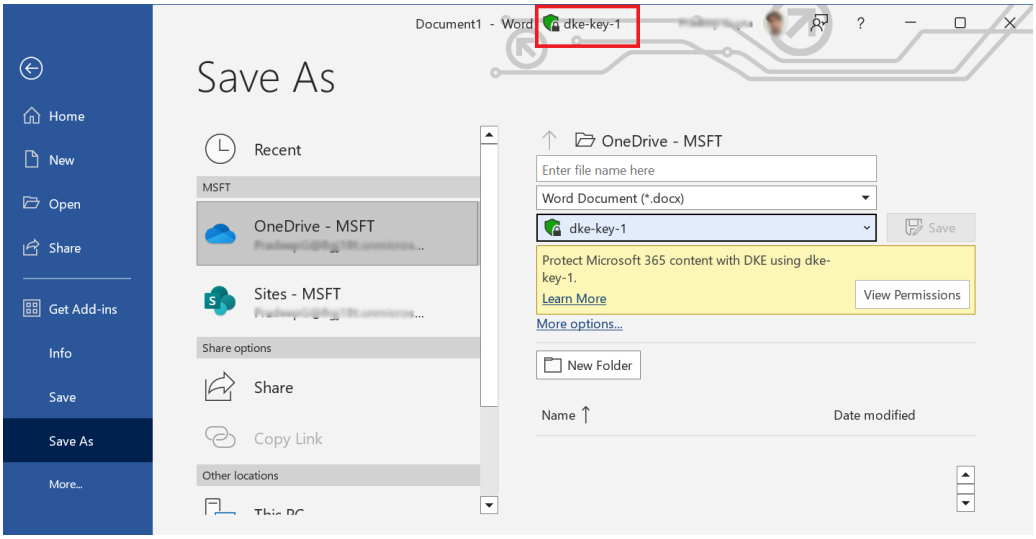
A **Word** document is created in this section for testing purposes. You can choose another Microsoft 365 app instead.

1. Sign in to the Microsoft 365 client computer.
2. Type **Word** in the search box to open Microsoft Word. Notice the Microsoft 365 account shows up on the top of the **Good afternoon** window.
3. Choose a **Blank document**. Enter some text. When saving the document, use the security classification pull-down menu to select the cloud key for DKE created in Create a cloud key for Microsoft 365 DKE .

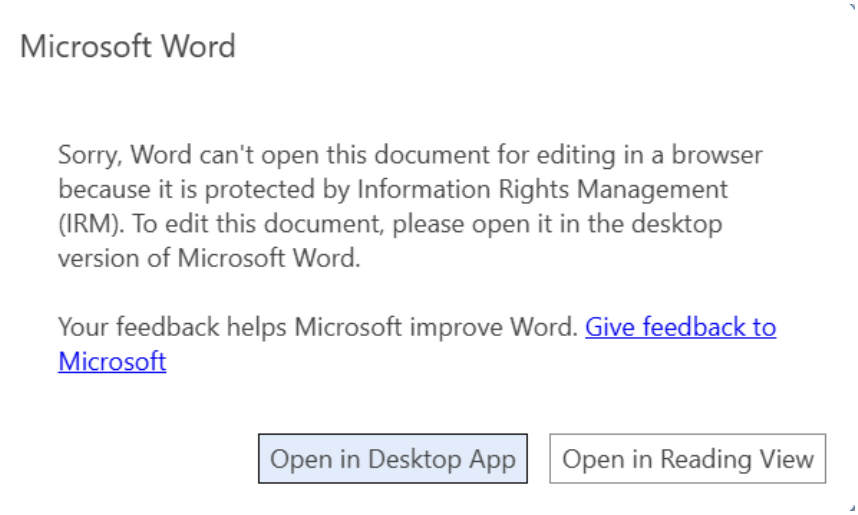
   For example:



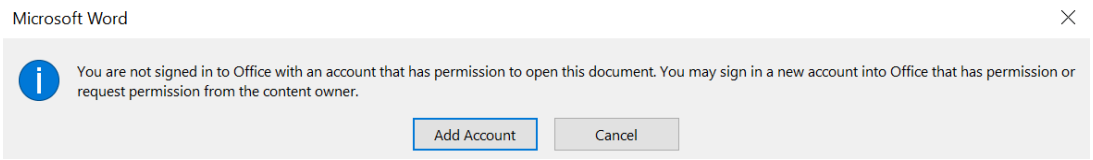
4. After saving the document, notice the protection icon in the top middle of the **Save As** window showing the cloud key for DKE.



5. The document can be opened and edited as desired in the desktop app. An attempt to open the document in the browser will fail with the following message.



6. An attempt to open the document in another PC will fail with the following message.



Chapter 7. Integrating with an HSM

For guidance on integrating the Entrust KeyControl with a Hardware Security Module (HSM), consult with your HSM vendor. If you are using an Entrust nShield HSM, refer to the Entrust KeyControl nShield HSM Integration Guide available at Entrust documentation library.

Chapter 8. Additional resources and related products

8.1. nShield Connect

8.2. nShield as a Service

8.3. KeyControl

8.4. Entrust digital security solutions

8.5. nShield product documentation