



ENTRUST

Microsoft Double Key Encryption and Entrust KeyControl

Integration Guide

2024-06-21

Member of
Microsoft Intelligent
Security Association



Table of Contents

1. Introduction	1
1.1. Product configuration	1
1.2. Features tested	1
1.3. Requirements	1
2. Deploy Entrust KeyControl	3
2.1. Deploy an Entrust KeyControl cluster	3
2.2. Install certificate authority (CA) certificate	4
2.3. Create a Cloud Key Management Vault in Entrust KeyControl	4
3. Deploy a Microsoft 365 client computer	6
3.1. Create a Microsoft 365 client computer	6
3.2. Install the root CA certificate	8
4. Create a key for Microsoft 365 DKE	9
4.1. Create a key set for DKE	9
4.2. Create a cloud key for Microsoft 365 DKE	9
5. Configure Microsoft Azure	12
5.1. Create an app registration in Azure	12
5.2. Add compliance label	16
5.3. Add label policies	20
6. Test integration	25
6.1. Test access to the cloud key for DKE	25
6.2. Install the Microsoft 365 apps in the Microsoft 365 client computer	25
6.3. Create a test document protected by DKE	26
7. Integrating with an HSM	29
8. Additional resources and related products	30
8.1. nShield Connect	30
8.2. nShield as a Service	30
8.3. KeyControl	30
8.4. Entrust digital security solutions	30
8.5. nShield product documentation	30

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.

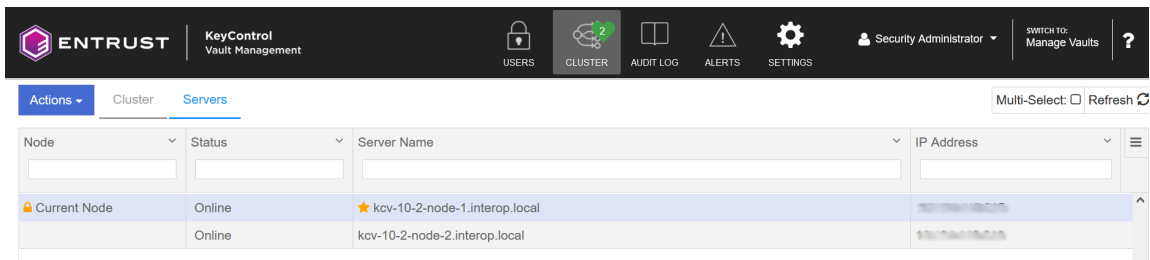
1. [Deploy an Entrust KeyControl cluster](#)
2. [Install certificate authority \(CA\) certificate](#)
3. [Create a Cloud Key Management Vault in Entrust KeyControl](#)

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.



Node	Status	Server Name	IP Address
Current Node	Online	★ kcv-10-2-node-1.interop.local	
	Online	kcv-10-2-node-2.interop.local	

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.

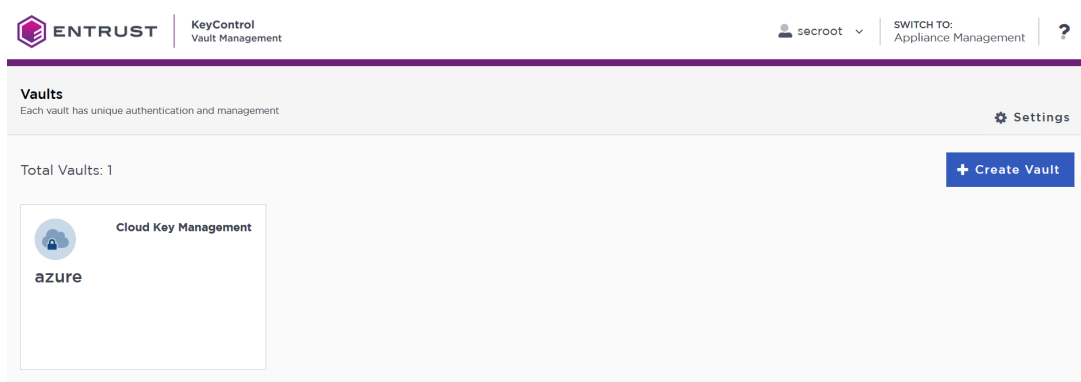
1. Create a vault per [Creating a Vault](#). The vault **Type** is **Cloud Key Management**.



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.

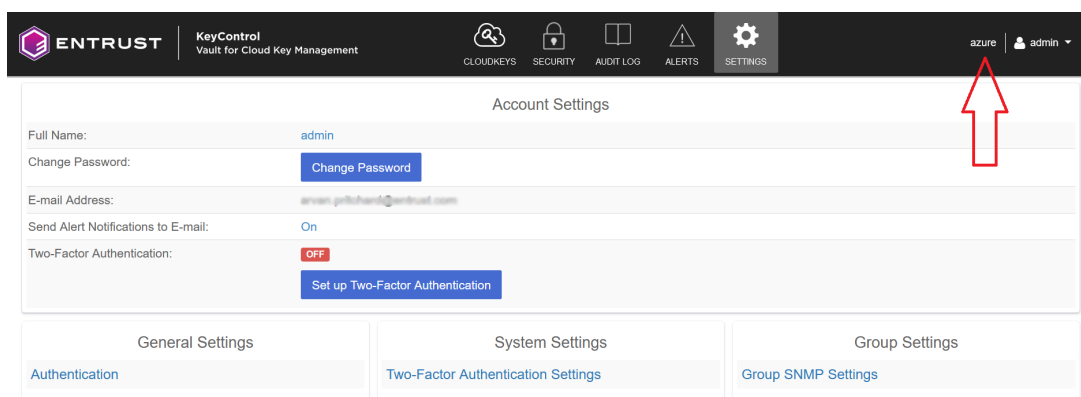
2. Bookmark the **Vault URL**. Copy the **User Name** and **Temporary Password**.
3. The newly created Vault is added to the **Vault Management** dashboard.

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:



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 * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Virtual machine name * ⓘ ✓

Region * ⓘ

Availability options ⓘ

Availability zone * ⓘ

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘ

Image * ⓘ ✓

[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 * ⓘ ✓

[See all sizes](#)

Enable Hibernation (preview) ⓘ

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernation to enable this feature. [Learn more](#)

Administrator account

Username * ⓘ ✓

Password * ✓

Confirm password * ✓

VM architecture ⓘ Arm64 x64
i Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

Size * ⓘ
[See all sizes](#)

Enable Hibernation (preview) ⓘ
i 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 * ⓘ ✓

Password * ✓

Confirm password * ✓

3. Notice the VM created.

Microsoft Azure Search resources, services, and docs (G+)

Home > CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20240513134439 | Overview

Deployment

Search << Delete Cancel Redeploy Download Refresh

Overview Inputs Outputs Template

✓ Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsDesktop.Window... Start time: 5/13/2024, 2:05:30 PM
Subscription: Entrust Corp - DPS Correlation ID: d690ddd4-11c5-4205-8994-ea002cd3e55

Resource group: ms-dke-keycontrol

Deployment details

Resource	Type	Status	Operation details
ms-365-client	Microsoft.Compute/virtualMachines	OK	Operation details
ms-365-client530_z1	Microsoft.Network/networkInterfaces	Created	Operation details
ms-365-client-vnet	Microsoft.Network/virtualNetworks	OK	Operation details
ms-365-client-ip	Microsoft.Network/publicIPAddresses	OK	Operation details
ms-365-client-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details

Next steps

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

Go to resource Create another VM

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.

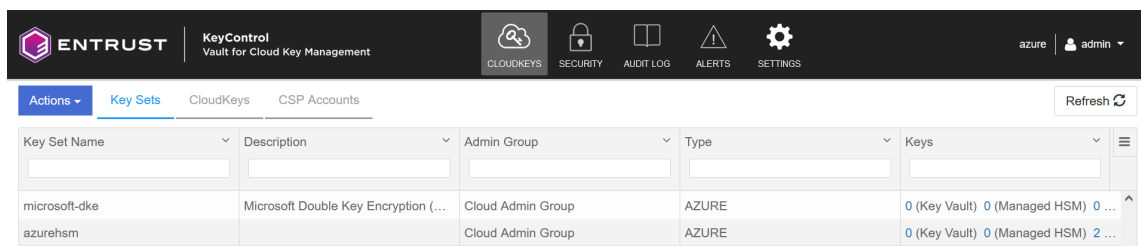
Chapter 4. Create a key for Microsoft 365 DKE

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.



Key Set Name	Description	Admin Group	Type	Keys
microsoft-dke	Microsoft Double Key Encryption (...)	Cloud Admin Group	AZURE	0 (Key Vault) 0 (Managed HSM) 0 ...
azurehsm		Cloud Admin Group	AZURE	0 (Key Vault) 0 (Managed HSM) 2 ...

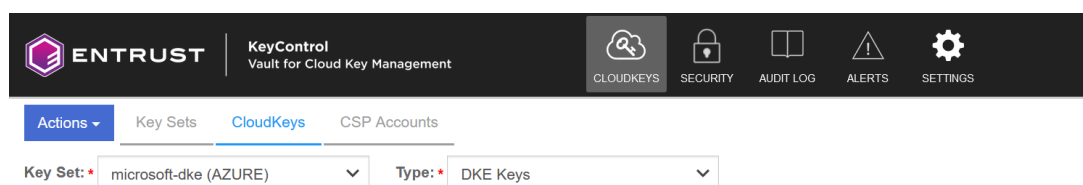
The number of DKE keys in each Key Set is shown on the **Key Sets** tab, last column in the right.

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.



There are no Cloudkeys to show. Please create one from Actions.

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

Description.

Create CloudKey ✕

Details | Access | Schedule

Type	AZURE
Key Set	microsoft-dke

Name *

dke-key-1

Description

Microsoft Double Key Encryption (DKE) integration with Entrust KeyControl.

Cancel

Continue

- 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.

Create CloudKey ✕

Details | Access | Schedule

Permissions

Cipher *

RSA-2048 ▼

Azure Accounts *

Allow all Specific Tenants

Cancel

Continue

- 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.

The screenshot displays the Entrust KeyControl interface. At the top, the logo 'ENTRUST' is on the left, and navigation icons for 'CLOUDKEYS', 'SECURITY', 'AUDIT LOG', 'ALERTS', and 'SETTINGS' are on the right. The user 'admin' is logged in. Below the navigation bar, there is an 'Actions' dropdown menu and four tabs: 'Details' (selected), 'DKE Permissions', 'Tags', and 'Versions'. The main content area shows the details for a key named 'dke-key-1'. The details are as follows:

Name:	dke-key-1
Key Id:	a89827aa7224aa1924996a782711527
DKE uri:	https://vaulter12.entrust.com/vaulter/keys/13e-a873a-44a4-8a30-a89827aa7224aa1924996a782711527/dke_keys.dke-key-1
Description:	Microsoft Double Key Encryption (DKE) integration with Entrust KeyControl.
Key Type:	Asymmetric
Cipher Type:	RSA-2048
Cloud Status ⓘ :	AVAILABLE
Key Source:	KEYCONTROL
Key Set:	microsoft-dke
Key Vault:	dke_keys
Rotation Schedule:	Every 1 year Rotate Now
Last Rotation Date:	05/10/2024

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.

- [Create an app registration in Azure](#)
- [Add compliance label](#)
- [Add label policies](#)

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:

Microsoft Azure

Home > MSFT | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

MS-365-DKE-Entrust-KeyControl ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (MSFT only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

5. Select **Register**.

The newly created registration appears.

Microsoft Azure

Home > MSFT | App registrations >

MS-365-DKE-Entrust-KeyControl

Search

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

^ Essentials

Display name	Client credentials
MS-365-DKE-Entrust-KeyControl	Add a certificate or secret
Application (client) ID	Redirect URIs
19873959-4213-4860-a234-6293ab142976	1_web, 0_spa, 0_public_client
Object ID	Application ID URI
5c7f16ad-29ab-4386-b485-7e83051c6214	Add an Application ID URI
Directory (tenant) ID	Managed application in local directory
683c6a87-524e-4247-a677-8033a009a761	MS-365-DKE-Entrust-KeyControl
Supported account types	
My organization only	

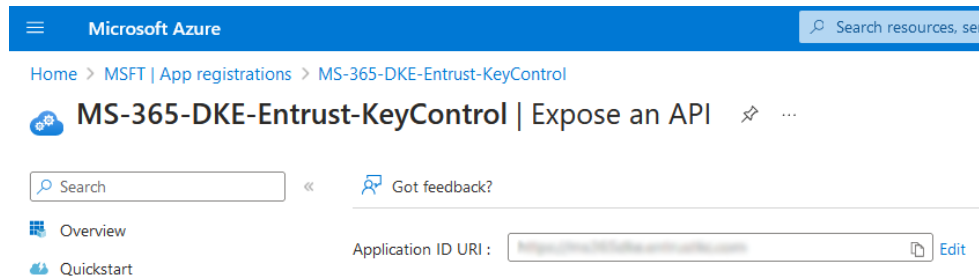
Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API

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:

Add a scope



Scope name * ⓘ

user_impersonation ✓

https://www.kmsi.com/identity/user_impersonation

Who can consent? ⓘ

Admins and users Admins only

Admin consent display name * ⓘ

user_impersonation ✓

Admin consent description * ⓘ

Allow the app to act as the logged-in user.

User consent display name ⓘ

e.g. Read your files ✓

User consent description ⓘ

e.g. Allows the app to read your files.

State ⓘ

Enabled Disabled

Add scope

Cancel

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:

The screenshot shows the Azure portal interface for configuring an API. The breadcrumb trail is: Home > MSFT | App registrations > MS-365-DKE-Entrust-KeyControl. The page title is 'MS-365-DKE-Entrust-KeyControl | Expose an API'. A search bar and a 'Got feedback?' link are at the top. A left-hand navigation pane lists various management options, with 'Expose an API' selected. The main content area includes a feedback prompt, the 'Application ID URI' field, and a section for 'Scopes defined by this API'. Below this is a table of scopes, and a section for 'Authorized client applications' with a table of client applications.

Scopes	Who can consent	Admin consent display...	User consent display n...	State
https://msft.azure.com/ /user_impersonation	Admins and users	user_impersonation		Enabled

Client Id	Scopes
00000000-0000-0000-0000-000000000000	1
00000000-0000-0000-0000-000000000000	1

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:

Provide basic details for this label

The protection settings you choose for this label will be immediately enforced on the items or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name * ⓘ

dke-key-1

Display name * ⓘ

dke-key-1

Label priority ⓘ

ⓘ By default, this label will be assigned the highest priority, but you can change this after it's created. X

Highest

Description for users * ⓘ

Protect Microsoft 365 content with DKE using dke-key-1.

Description for admins ⓘ

Protect Microsoft 365 content with DKE using dke-key-1.

Label color ⓘ



Next

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

For example:

Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Fabric and Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

Items
Be aware that restricting the scope to only files or emails might impact access control settings and where the label can be applied. [Learn more](#)

Files
Protect files created in Word, Excel, PowerPoint, and more.

Emails
Protect messages sent from all versions of Outlook.

Meetings
Protect calendar events and meetings scheduled in Outlook and Teams.

Parent label will automatically inherit meeting scope from sub labels

Groups & sites
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first [complete these steps](#) to enable the feature.

Schematized data assets (preview)
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

When scoped to schematized data assets, we recommend also scoping to Files so this label can be used in protection policies to control access to items in multicloud data sources. [Learn about protection policies](#)

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

For example:

Choose protection settings for the types of items you selected

The protection settings you configure will be enforced when the label is applied to items in Microsoft 365.

- Control access**
Control who can access and view labeled items.
- Apply content marking**
Add custom headers, footers, and watermarks to labeled items.
- Protect Teams meetings and chats**
Configure protection settings for Teams meetings and chats.

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:

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

[Assign permissions](#)

2 items

Users and groups	Permissions	Edit	Delete
frank@mgmt.com	Co-Author		
frank@mgmt.com	Co-Author		

Use Double Key Encryption ⓘ

https://cloudkeys12.entrust.com/v1/cloudkeys/20001234-483a-44c4-8c90-4a8f19a0e110/dke_keys.dke--key--1

[Back](#) [Next](#)



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:

The screenshot shows the Entrust KeyControl interface. The top navigation bar includes 'ENTRUST', 'KeyControl Vault for Cloud Key Management', and icons for 'CLOUDKEYS', 'SECURITY', 'AUDIT LOG', 'ALERTS', and 'SETTINGS'. The user is logged in as 'admin'. The main content area shows the 'Details' tab for a cloud key named 'dke-key-1'. The key ID is 'ed9857ea7334ab192209c700711157' and the DKE URI is 'https://cloudkeys12.entrust.com/v1/cloudkeys/20001234-483a-44c4-8c90-4a8f19a0e110/dke_keys.dke--key--1'.

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

For example:

✔ Your sensitivity label was created

Creating the label is just the first step in labeling and protecting content. To make this label available to users in your org, you can auto-apply it to specific content and publish it to users' apps.

Next steps

- Publish label to users' apps
Create a publishing policy to show the label in Office apps, SharePoint, Teams, and Microsoft 365 Groups so users can apply it to content themselves. [Learn more about publishing labels](#)
- Don't create a policy yet
You can publish or auto-apply this label later.

Recommended resources based on your settings

[Review prerequisites](#) to get the most out of your access control settings
[Review prerequisites](#) for applying sensitivity labels to Fabric and Power BI content.
[Review a Microsoft Purview Data Map tutorial](#) on how to start scanning assets and automatically apply this label
[Configure co-authoring for Office desktop apps](#) so multiple users can simultaneously edit labeled docs that have access control settings applied.

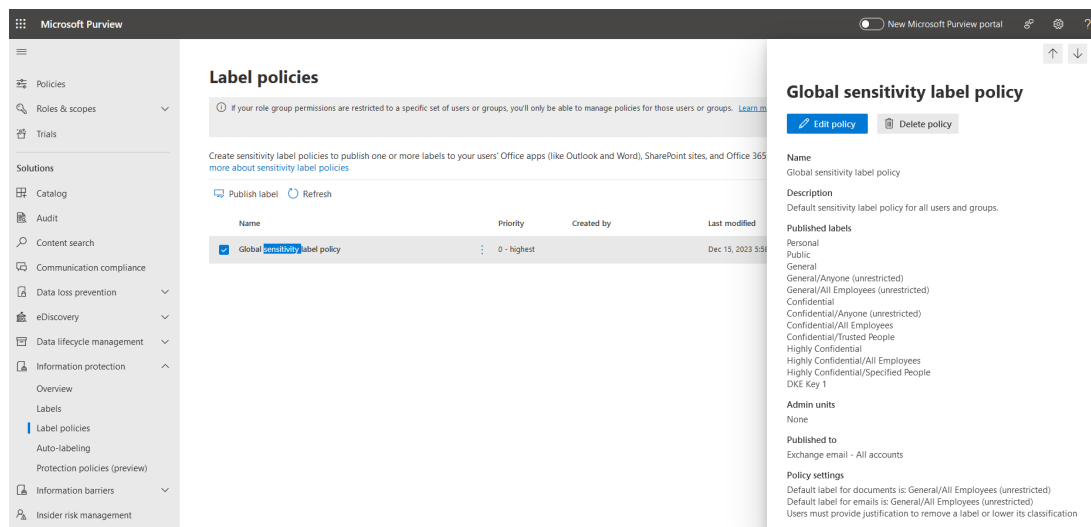
16. Create any other labels you need following the steps above.

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:

Sensitivity labels to publish

If you select a sublabel, the corresponding parent will also be published automatically.

14 selected

<input checked="" type="checkbox"/>	Label	Scope
<input checked="" type="checkbox"/>	Confidential/All Employees (unrestricted)	File, Email
<input checked="" type="checkbox"/>	Confidential	File, Email
<input checked="" type="checkbox"/>	Confidential/Anyone (unrestricted)	File, Email
<input checked="" type="checkbox"/>	Confidential/All Employees	File, Email
<input checked="" type="checkbox"/>	Confidential/Trusted People	File, Email
<input checked="" type="checkbox"/>	Highly Confidential	File, Email
<input checked="" type="checkbox"/>	Highly Confidential/All Employees	File, Email
<input checked="" type="checkbox"/>	Highly Confidential/Specified People	File, Email
<input checked="" type="checkbox"/>	DKE Key 1	File, Email
<input checked="" type="checkbox"/>	dke-key-1	File, Email, SchematizedData

6. Select **Next**.

For example:

Choose sensitivity labels to publish

When published, the labels you choose here will be available in specified users' Office apps (Word, Excel, PowerPoint, and Outlook), SharePoint and Teams sites, and Microsoft 365 Groups.

Sensitivity labels to publish

Personal
Public
General
General/Anyone (unrestricted)
General/All Employees (unrestricted)
Confidential
Confidential/Anyone (unrestricted)
Confidential/All Employees
Confidential/Trusted People
Highly Confidential
Highly Confidential/All Employees
Highly Confidential/Specified People
DKF Key 1

dkf-key-1

Edit

Next

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:

Review and finish

Name

Global sensitivity label policy

Description

Default sensitivity label policy for all users and groups.

[Edit](#)

Publish these labels

Personal

Public

General

General/Anyone (unrestricted)

General/All Employees (unrestricted)

Confidential

Confidential/Anyone (unrestricted)

Confidential/All Employees

Confidential/Trusted People

Highly Confidential

Highly Confidential/All Employees

Highly Confidential/Specified People

DKE Key 1

dke-key-1

[Edit](#)

Publish to users and groups

Exchange email - All accounts

[Edit](#)

Policy settings

Default label for documents is: General/All Employees (unrestricted)

Default label for emails is: General/All Employees (unrestricted)

Users must provide justification to remove a label or lower its classification

[Edit](#)

[Back](#)

[Submit](#)

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:

 **Policy updated**

Your sensitivity label policy has been updated.

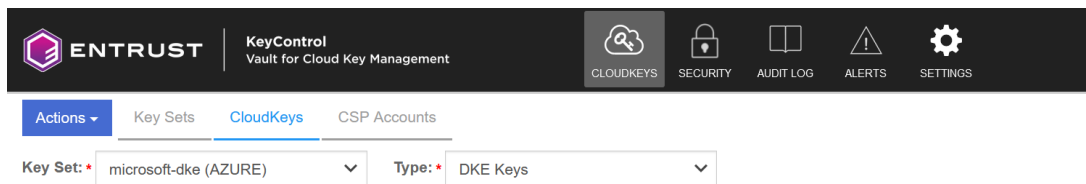
Chapter 6. Test integration

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.



There are no Cloudkeys to show. Please create one from Actions.

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.

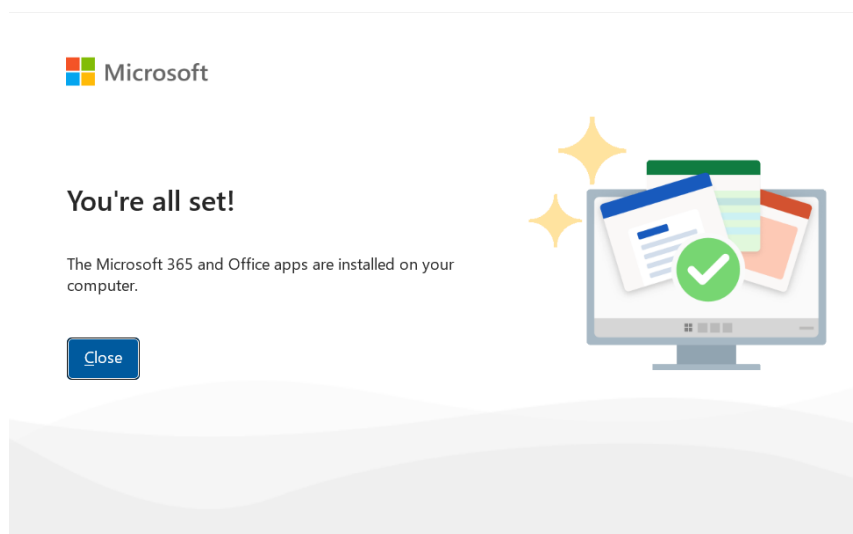
For example:



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**.

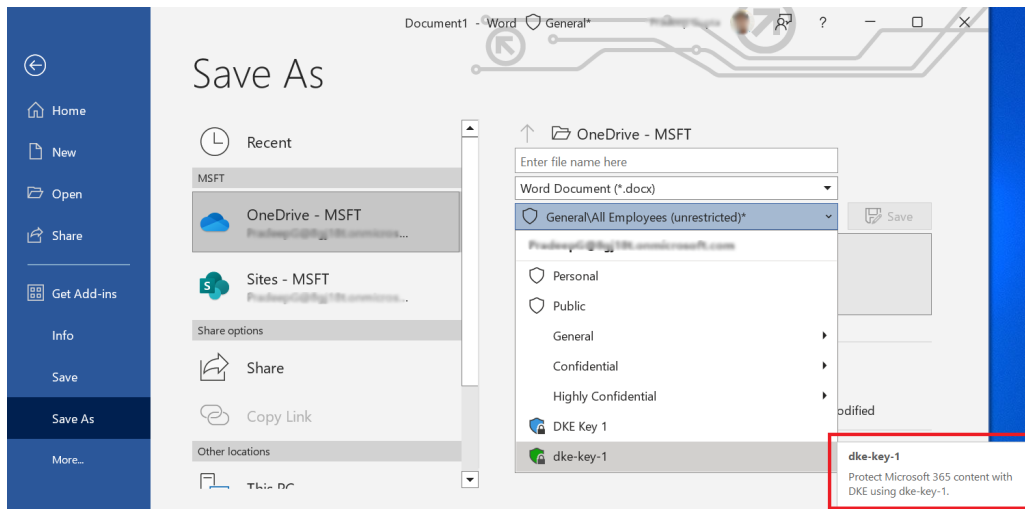


6.3. Create a test document protected by DKE

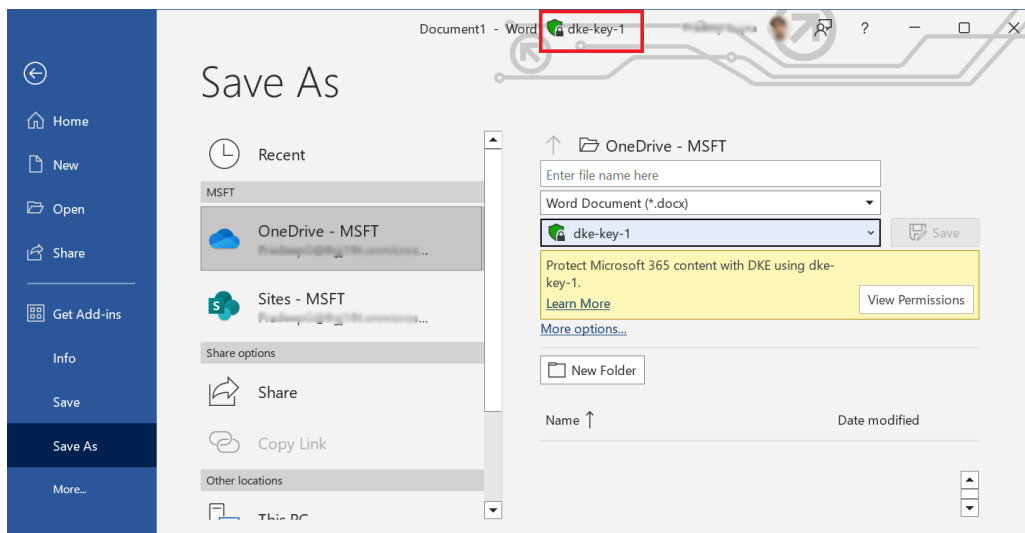
A **Word** document is created in this section for testing purposes. You can choose another Microsoft 365 app instead.

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.

Microsoft Word

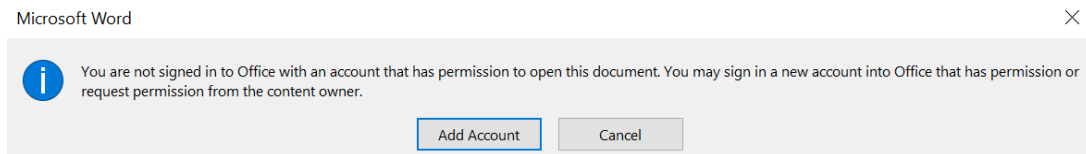
Sorry, Word can't open this document for editing in a browser because it is protected by Information Rights Management (IRM). To edit this document, please open it in the desktop version of Microsoft Word.

Your feedback helps Microsoft improve Word. [Give feedback to Microsoft](#)

Open in Desktop App

Open in Reading View

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