



Indhold

6.0 Updating the internal Integration App credentials	1
6.1 Make sure we are actually dealing with an expired Secret.....	1
6.2 Create a new Secret.....	4
6.3 Replacing the expired secret	5

6.0 Updating the internal Integration App credentials

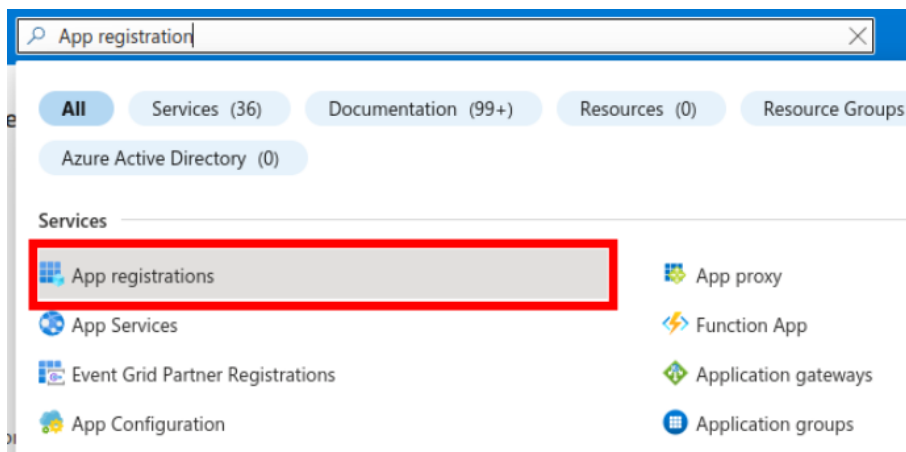
Back in section 3.3: [Azure app Integration - ENG](#), we created the App-registration that holds the permissions needed by the Integration App. The Integration App has access to these permissions via a Secret that we created for the App-registration. This Secret has an Expire Date. Once the Secret is expired the Integration App cannot longer perform the required operations when it is called by the TDC Erhverv Selfservice system.

At this point you could choose to follow section 3 again from the beginning - this would guide you through creating a *new* App-registration and install a *new* copy of the Integration App in a *new* resource group. This is a lot of work and could require a new internal security review. Alternately you can follow this guide to create a new Secret and activating it with the Integration App you already have installed.

To start, log in-to the target Azure Tenant on <https://portal.azure.com/> using an account that is Global Administrator. If you are not a Global Administrator some of the steps below will not work for you.

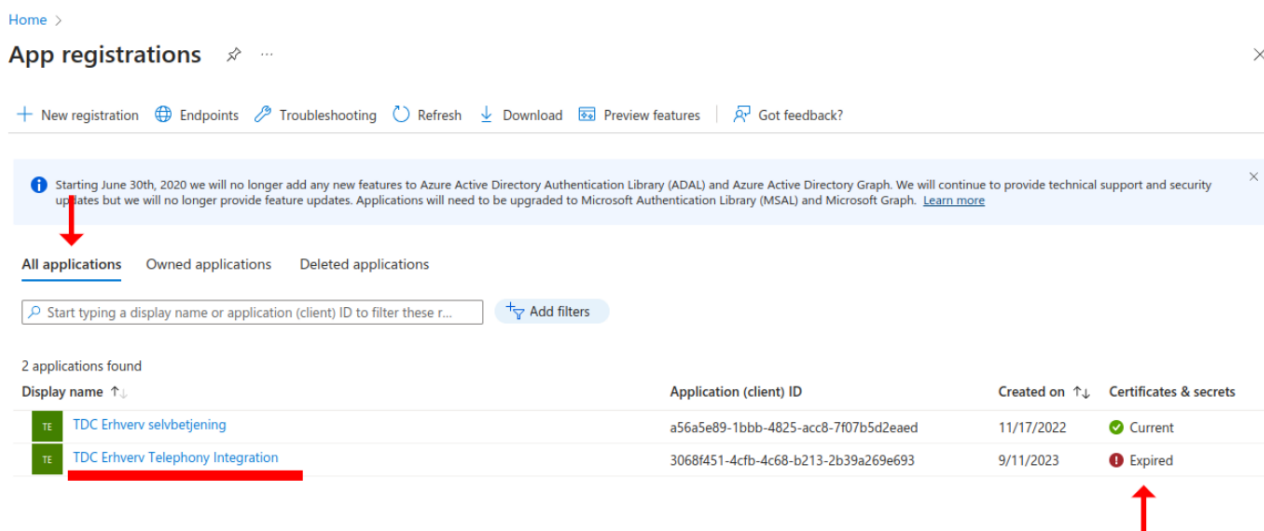
6.1 Make sure we are actually dealing with an expired Secret

Before we start changing things, let's make sure the core issue is indeed an expired Secret. First search for "App registrations" and go to that section.



From here click “All applications” and look for the App-registration you created when originally installing the Integration App. In this example it was called “TDC Erhverv Telephony Integration” but if you have no idea then review [Azure app FAQ - ENG](#) to see how to read the exact App-registration id from your Function App configuration.

As you can see in the screenshot below, in this case there is an alert showing that the App-registration has an expired Secret. But remember that an App-registration can have multiple secrets, so we do not know yet if it is the secret used by our Integration App that is expired. To investigate further click the correct App-registration to see the details.





Go to the section “[Certificates & secrets](#)”. Find the Secret you used during the original installation of the Integration App. If you have multiple secrets here and are unsure which one you used then review section 7.2: [Azure app FAQ - ENG](#) to see how to read the exact secret from your Function App.

In this case the correct secret is “[TDC Erhverv Telephony Integration](#)” - and we can see that the Expires-time is in the past. This Secret needs to be replaced, so see how, proceed to the next section.

Home > App registrations > TDC Erhverv Telephony Integration

TDC Erhverv Telephony Integration | Certificates & secrets

Search Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
TDC Erhverv Telephony Integration	9/25/2023	xDn*****	6a92456c-49e7-4776-9437-13b98f77ef...

If you are a power-user, you can also fire off the following request to the App self-test function (adjust host name and key to match you own App). If the response message contains the line “*Error connecting to Teams using credentials. Cause: Response status code does not indicate success: 401 (Unauthorized)*” then this is also an indication that the Secret is expired.

```
curl https://nuudaytob-5sutozr67fiik.azurewebsites.net/api/psweb?code=3Br2w2pK1I6qflrILnMvZl-sMQk2Fj58amQx1Ng-nogoAzFuTsZg4g== \
-d '{"function":"Test"}' \
-H "Content-Type: application/json" -X GET
```

Response



```
{
  "appVersion": "1.0.0",
  "command": "Test",
  "success": false,
  "message": "Exception calling \"Invoke\" with \"1\" argument(s): \"Error connecting to Teams using credentials. Cause: Response status code does not indicate success: 401 (Unauthorized).\"",
  "resultCode": "19"
}
```

6.2 Create a new Secret

Stay on the “Certificate & secrets” section of App-registration and click “New client secret”. Let’s call this new Secret “TDC Erhverv Telephony Integration 2” and choose the maximum 24-month lifetime. Then click “Add” to generate this new secret.

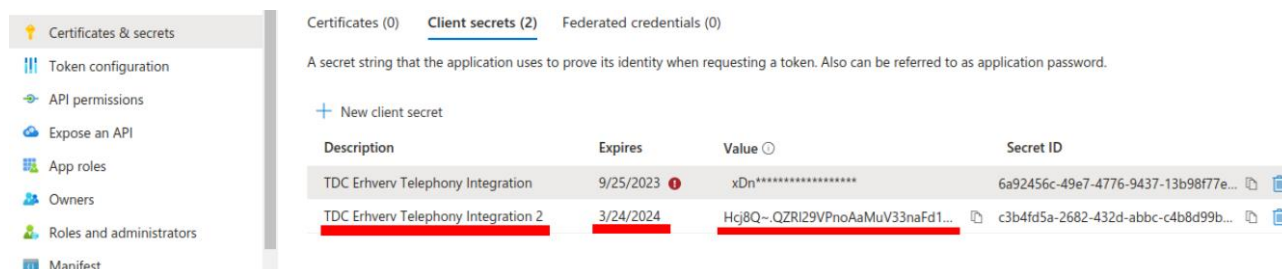
The screenshot shows the Azure portal interface. On the left, the navigation pane is open to 'Certificates & secrets' for the application 'TDC Erhverv Telephony Integration'. The main area shows a table with one client secret: 'TDC Erhverv Telephony Integration' with an expiration date of 9/25/2023. A red box highlights the '+ New client secret' button. On the right, the 'Add a client secret' dialog is open. The 'Description' field contains 'TDC Erhverv Telephony Integration 2' and the 'Expires' dropdown is set to '730 days (24 months)'. Red arrows point to these fields. The 'Add' button at the bottom of the dialog is also highlighted with a red box.

We now have a new secret. It expires 2025-09-24, make a note of this in your calendar. Also note down the secret value we will need it below, but don't share it with anyone outside your organization, not even



TDC Erhverv. In this example the secret value is: **Hcj8Q~.QZRI29VPnoAaMuV33naFd1W4yueZLPa4k**.

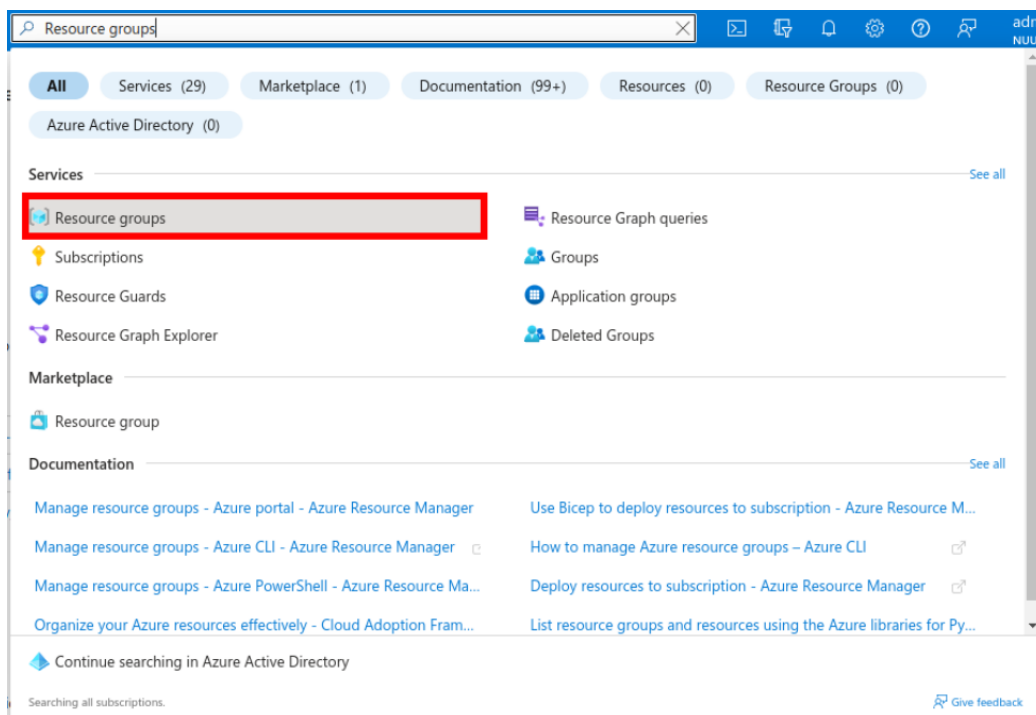
Note this down, we will need it later, and once you leave this page the secret can never be seen again.



In this case the Secret is expired, and we should delete it right now to avoid warnings about expired Secrets on the App-registration, but if your Secret is not expired *yet*, if it is only close to expiring and you are here to renew it proactively, then leave it be until we have replaced it in the Integration App. Come back here and delete the unused Secret once we are done.

6.3 Replacing the expired secret

We now have a new valid Secret for the App-registration, lets replace it in the Integration App. First go to the Ressource groups section.





Here select the Resource group that holds the installed Integration App. In our case it is the group “TDC_Erhverv_Telephony_Integration”.

Home >

Resource groups

Nuuday Blue Teams test 4 - Teams for Broadworks (blue4.testontdc.net)

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Location equals all Add filter

Showing 1 to 2 of 2 records. No grouping List view

Name	Subscription	Location
cloud-shell-storage-west europe	Bluetest4 Azure Plan	West Europe
TDC_Erhverv_Telephony_Integration	Bluetest4 Azure Plan	North Europe

The App consists of several Azure Cloud Resources. First head to the “Function App”.

Home > Resource groups >

TDC_Erhverv_Telephony_Integration

Resource group

Search Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move

- Overview
- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Events
- Settings
 - Deployments
 - Security
 - Deployment stacks
 - Policies
 - Properties
 - Locks

Essentials

Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

Showing 1 to 7 of 7 records. Show hidden types No grouping List view

Name	Type	Location
Application Insights Smart Detection	Action group	Global
Failure Anomalies - NuudayToB-5sutozr67fiik	Smart detector alert rule	Global
fnstor5sutozr67fiik	Storage account	North Europe
kv5sutozr67fiik	Key vault	North Europe
NuudayToB-5sutozr67fiik	Application Insights	North Europe
NuudayToB-5sutozr67fiik	Function App	North Europe
ServicePlanFunctionApp	App Service plan	North Europe

From here scroll down the left-hand side until you find the section **Settings > Configuration** and click it. These are the Environment Variables that Azure makes available to the Function App. Three of them are special, they are marked as “Key vault Reference”.



Home > Resource groups > TDC_Erhverv_Telephony_Integration > NuudayToB-5sutozr67fiik

NuudayToB-5sutozr67fiik | Configuration

Function App

Search [] Refresh Save Discard Leave Feedback

Microsoft Defender for Cloud
Events (preview)

Functions

- App keys
- App files
- Proxies

Deployment

- Deployment slots
- Deployment Center

Settings

- Configuration
- Authentication
- Application Insights
- Identity

Application settings

Application settings are encrypted at rest and transmitted over an encrypted channel. You can choose to display them in plain text in your browser by using the controls below. Application Settings are exposed as environment variables for access by your application at runtime. [Learn more](#)

+ New application setting Show values Advanced edit

Filter application settings []

Name	Value	Source	Deployment slot setting
APPINSIGHTS_INSTRUMENTATIONKEY	Hidden value. Click to show value	App Service	
AzureWebJobsStorage	Hidden value. Click to show value	App Service	
FUNCTIONS_EXTENSION_VERSION	Hidden value. Click to show value	App Service	
FUNCTIONS_WORKER_RUNTIME	Hidden value. Click to show value	App Service	
FUNCTIONS_WORKER_RUNTIME_VERSION	Hidden value. Click to show value	App Service	
TeamsApplicationID	Hidden value. Click to show value	Key vault Reference	
TeamsClientSecret	Hidden value. Click to show value	Key vault Reference	
TeamsTenantID	Hidden value. Click to show value	Key vault Reference	

We are looking to update the one called “TeamsClientSecret”. This is the variable that reads the expired Secret value out of the Key vault. Click it to show the settings.

NuudayToB-5sutozr67fiik | Configuration

Function App

Search []

Microsoft Defender for Cloud
Events (preview)

Functions

- App keys
- App files
- Proxies

Deployment

- Deployment slots
- Deployment Center

Settings

- Configuration
- Authentication
- Application Insights
- Identity
- Backups

Add/Edit application setting

Name: TeamsTenantID

Value: @Microsoft.KeyVault(VaultName=kv5sutozr67fiik;SecretName=TeamsTenantID)

Deployment slot setting

Key Vault Reference Details

Vault Name: kv5sutozr67fiik

Secret Name: TeamsTenantID

Ok Cancel

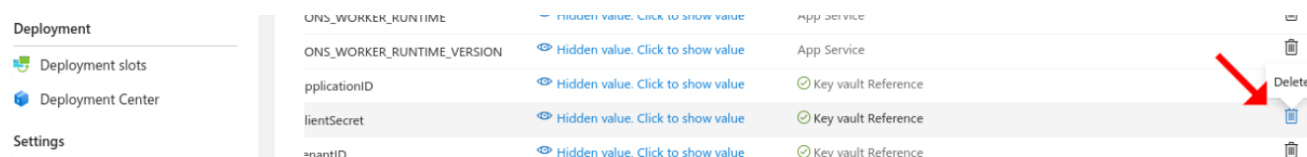


The reference has a Name and a Value. Copy these, we will need them later. In this case they are:

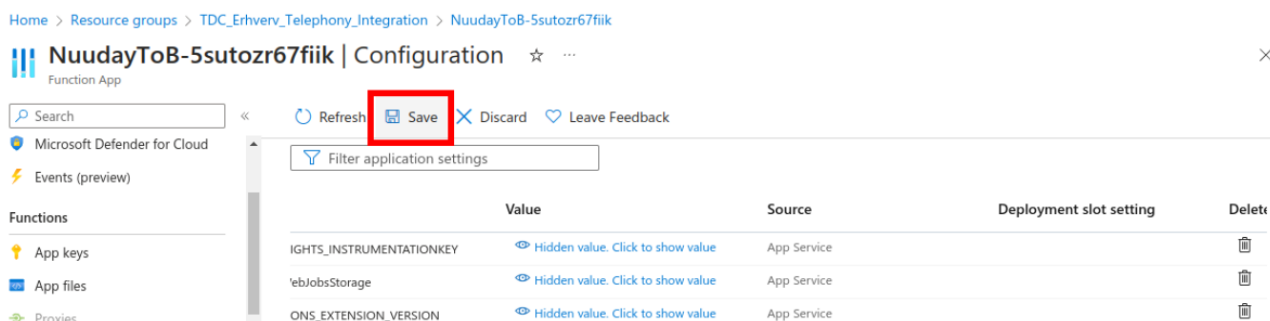
- Name: **TeamsTenantID**
- Value: **@Microsoft.KeyVault(VaultName=kv5sutozr67fiik;SecretName=TeamsTenantID)**

Note that while the name is always the same, the value will be different for every installation because the name of every Key vault instance must be unique.

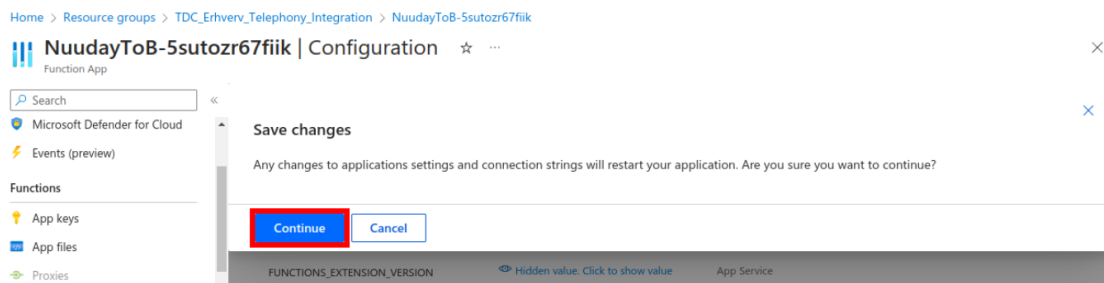
You can now click Cancel. Back on the previous page, scroll a bit to the right and **delete** the reference **TeamsClientSecret**.



To make the deletion permanent click “Save” at the top.



And then click on “Continue”.





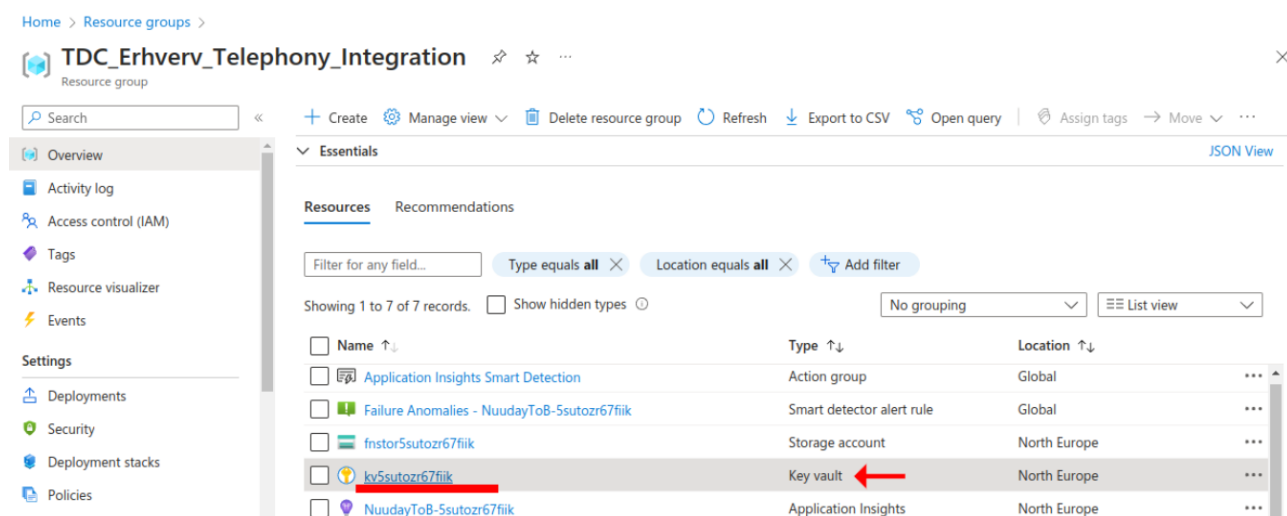
If you are a power user following along by calling the App self-test endpoint via the Function App API when the response message should now include the message: *"ClientSecret not found on env"*.

Request/response:

```
curl https://nuudaytob-<function app name>.azurewebsites.net/api/psweb?code=<api key> \
-d '{"function":"Test"}' \
-H "Content-Type: application/json" -X GET
```

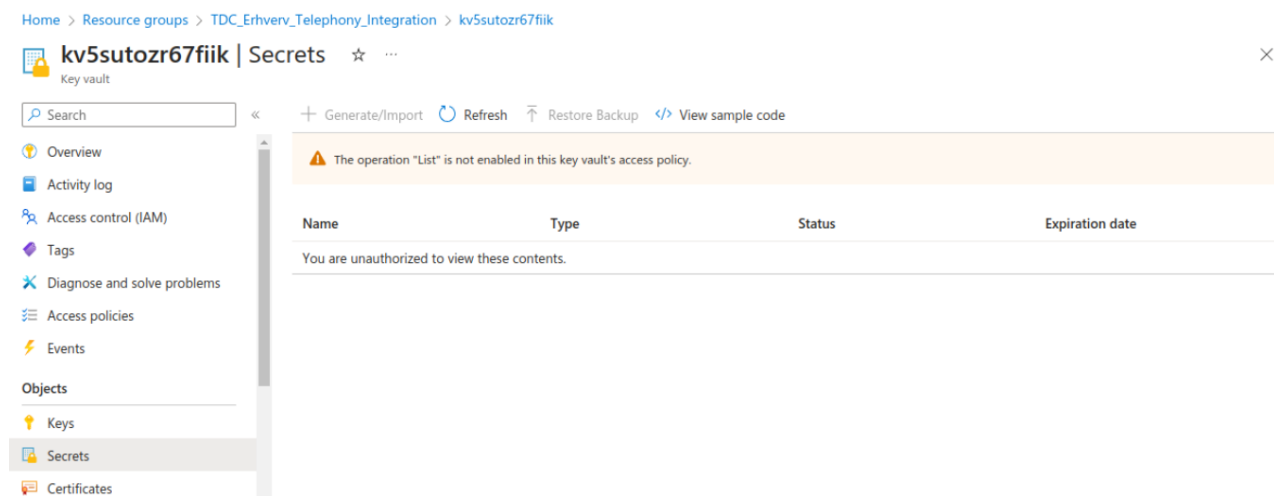
```
{
  "appVersion": "1.0.0",
  "command": "Test",
  "success": false,
  "message": "Exception calling \"Invoke\" with \"1\" argument(s): \"ClientSecret not found on env.\",
  "resultCode": "24"
}
```

Now let's update the expired secret value stored in the Key vault. To do this navigate back to the overview for the Resource group that holds your Integration App. From here click on the [Key vault](#).





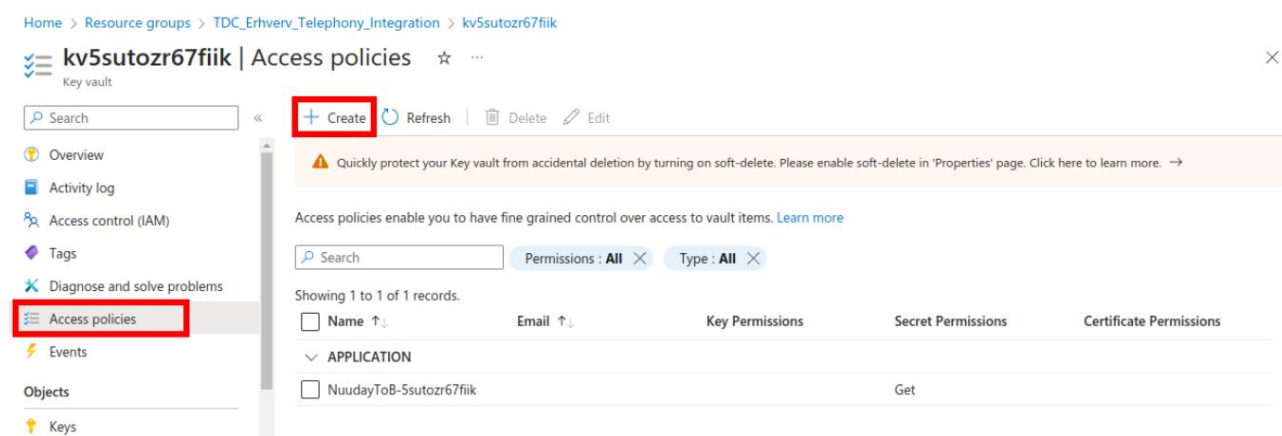
On the left-hand side of the Key vault page, navigate to the section “Secrets”.



At this point you will most likely see the message “*You are unauthorized to view these contents*” as in the screenshot above. If you do have access, you can [skip ahead](#) a bit in this guide.

Since you are a Global Administrator, you can give yourself access, to do this go to the section "Access policies". Here we can see that only one entity currently has access to read the Secrets from this Key vault. In this screenshot it is "NuudayToB-5sutozr67fiik" and you should note that this is the name of the Function App from back in the overview of installed Cloud Resources for this Resource group.

To give yourself access press "Create" to make a new policy (once we are done, we will delete this policy again).





Note that this policy will only affect this specific instance of Azure Key vault, any other Secrets in your organization will not be affected. In the column for “Secret permissions”, click “Select all” to manage all aspects of Secrets life cycle. Then click Next.

Key permissions	Secret permissions	Certificate permissions
Key Management Operations	Secret Management Operations	Certificate Management Operations
<input type="checkbox"/> Select all	<input checked="" type="checkbox"/> Select all	<input type="checkbox"/> Select all
<input type="checkbox"/> Get	<input checked="" type="checkbox"/> Get	<input type="checkbox"/> Get
<input type="checkbox"/> List	<input checked="" type="checkbox"/> List	<input type="checkbox"/> List
<input type="checkbox"/> Update	<input checked="" type="checkbox"/> Set	<input type="checkbox"/> Update
<input type="checkbox"/> Create	<input checked="" type="checkbox"/> Delete	<input type="checkbox"/> Create
<input type="checkbox"/> Import	<input checked="" type="checkbox"/> Recover	<input type="checkbox"/> Import
<input type="checkbox"/> Delete	<input checked="" type="checkbox"/> Backup	<input type="checkbox"/> Delete
<input type="checkbox"/> Recover	<input checked="" type="checkbox"/> Restore	<input type="checkbox"/> Recover

Previous **Next**

Now search for the name of your user. Once you find it click on it, to add it to the list of “Selected items”. Now click Next.

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

Home > Resource groups > TDC_Erhverv_Telephony_Integration > kv5sutozr67fiik | Access policies >

Create an access policy

kv5sutozr67fiik

Permissions **2 Principal** Application (optional) Review + create

Only 1 principal can be assigned per access policy. Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

admkasfre

admkasfre@blue4.testontdc.net - Admin

Selected item

admkasfre@blue4.testontdc.net - Admin

Previous **Next**



We are not assigning permissions to any Applications. Click “Next” here without selecting anything.

[Previous](#) [Next](#)

Verify that you have selected all Secret related Management Operations, and that your account is listed under Principal. No other options should be selected. Now click “Create”.


[Home](#) > [Resource groups](#) > [TDC_Erhverv_Telephony_Integration](#) > [kv5sutozr67fiik](#) | [Access policies](#) >

Create an access policy ...

kv5sutozr67fiik

Key Management Operations	None selected
Cryptographic Operations	None selected
Privileged Key Operations	None selected
Rotation Policy Operations	None selected

Secret Permissions

Secret Management Operations	All selected	
Privileged Secret Operations	None selected	

Certificate Permissions

Certificate Management Operations	None selected
Privileged Certificate Operations	None selected

Principal

Principal name	 - Admin	
Object ID	940b2a8f-74b9-4a18-8ac1-4b9235c28f2b	

Application

[Previous](#) [Create](#)



There is now a Policy that gives your account access to Manage all secrets in this Key vault. Click on the menu item “Secrets” on the left to navigate back to the Secrets section of this Key vault.

Home > Resource groups > TDC_Erhverv_Telephony_Integration > kv5sutozr67fiik

kv5sutozr67fiik | Access policies

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Events
Objects
Keys
Secrets
Certificates

Quickly protect your Key vault from accidental deletion by turning on soft-delete. Please enable soft-delete in 'Properties' page. Click here to learn more. →

Access policies enable you to have fine grained control over access to vault items. Learn more

Search Permissions: All Type: All

Showing 1 to 2 of 2 records.

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
APPLICATION				
NuudayToB-5sutozr67fiik			Get	
USER				
[Redacted] - Admin	admkafr@blue4.testontdc...		Get, List, Set, Delete, Recover...	

Now we can see all Secrets in this Key vault. The original installation process for the Integration App created three Secrets. The one we are interested in is called “TeamsClientSecret”. Click it.

Home > Resource groups > TDC_Erhverv_Telephony_Integration > kv5sutozr67fiik

kv5sutozr67fiik | Secrets

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Events

Quickly protect your certificates from accidental deletion by turning on soft-delete. Please enable soft-delete in 'Properties' page. Click here to learn more. →

Name	Type	Status	Expiration date
TeamsApplicationID		✓ Enabled	
TeamsClientSecret		✓ Enabled	
TeamsTenantID		✓ Enabled	

Delete the Secret called “TeamsClientSecret”.

Home > Resource groups > TDC_Erhverv_Telephony_Integration > kv5sutozr67fiik | Secrets >

TeamsClientSecret

New Version Refresh **Delete** Download Backup

Version	Status	Activation date	Expiration date
CURRENT VERSION			
7028171e6c464283957648d8bf095140	✓ Enabled		



Home > Resource groups > TDC_Erhverv_Telephony_Integration > kv5sutozr67fiik | Secrets >

TeamsClientSecret

Versions

+ New Version Refresh Delete Download Backup

Delete secret

This will permanently delete the resource and all of its versions from your vault.

Delete

Cancel

Expiration date

Now that the Secret is gone, click “Generate/Import” to make a new one.

Home > Resource groups > TDC_Erhverv_Telephony_Integration > kv5sutozr67fiik

kv5sutozr67fiik | Secrets

Key vault

Search

+ Generate/Import

Refresh

Restore Backup

View sample code

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Quickly protect your certificates from accidental deletion by turning on soft-deletion.

Name	Type
TeamsApplicationID	
TeamsTenantID	

Notifications

More events in the activity log →

Dismiss all

Deleting the secret 'TeamsClientSecret'.
The secret 'TeamsClientSecret' has been successfully deleted.
a few seconds ago

Enter the exact same Secret Name as before: **TeamsClientSecret**

Enter the secret value from the App-registration we prepared earlier. In this example it is: **Hcj8Q~.QZRI29VPnoAaMuV33naFd1W4yueZLpa4k**

Then click “Create.”

Home > Resource groups > TDC_Erhverv_Telephony_Integration > kv5sutozr67fiik | Secrets >

Create a secret

Upload options

Manual

Name *

TeamsClientSecret

Secret value *

.....

Content type (optional)

Set activation date

Set expiration date

Enabled

Yes No

Tags

0 tags

Create

Cancel



We now have a new Secret, still called “TeamsClientSecret”, but this time with the correct updated value.

The screenshot shows the Azure portal interface for a Key Vault named 'kv5sutozr67fiik'. A notification at the top right states 'Creating the secret 'TeamsClientSecret'. The secret 'TeamsClientSecret' has been successfully created.' Below this, a table lists secrets:

Name	Type	Status	Expiration date
TeamsClientSecret		✓ Enabled	
TeamsApplicationID		✓ Enabled	
TeamsTenantID		✓ Enabled	

A red arrow points to the 'TeamsClientSecret' entry in the table.

Now navigate back to the “Resource group”, click the “Function app”, and navigate to the section **Settings > Configuration**. This is back where we deleted the **Key vault reference** a while back. We are going to add it back now. Click “New application setting”.

The screenshot shows the Azure portal interface for a Function App named 'NuudayToB-5sutozr67fiik'. The 'Configuration' page is open, showing 'Application settings'. A red box highlights the '+ New application setting' button.

Enter the same Name and Value that we saved above. The name will always be “TeamsClientSecret” and the value will be of the form “@Microsoft.KeyVault(VaultName=<vault name>;SecretName=TeamsClientSecret)” ... where <vault name> is the unique name of your Key vault (ass seen in on the Key vault overview page or in the resource list in the Resource group), in this example it is **kv5sutozr67fiik**.

Click “Ok” to create this Application setting.



Home > Resource groups > TDC_Erhverv_Telephony_Integration > NuudayToB-5sutozr67fiik

NuudayToB-5sutozr67fiik | Configuration ☆ ...

Search

Functions

App keys

App files

Proxies

Deployment

Deployment slots

Deployment Center

Settings

Configuration

Authentication

Application Insights

Identity

Backups

Custom domains

Certificates

Add/Edit application setting

Name **TeamsClientSecret**

Value **@Microsoft.KeyVault(VaultName=kv5sutozr67fiik;SecretName=TeamsClientSecret)**

Deployment slot setting

Ok

Cancel

Now click “Save” and “Continue” to store this new Application setting.

1)

Home > Resource groups > TDC_Erhverv_Telephony_Integration > NuudayToB-5sutozr67fiik

NuudayToB-5sutozr67fiik | Configuration ☆ ...

Search

Functions

App keys

App files

Refresh **Save** Discard Leave Feedback

Application settings * Function runtime settings General settings

Application settings

2)

Home > Resource groups > TDC_Erhverv_Telephony_Integration > NuudayToB-5sutozr67fiik

NuudayToB-5sutozr67fiik | Configuration ☆ ...

Search

Functions

App keys

App files

Proxies

Deployment

Save changes

Any changes to applications settings and connection strings will restart your application. Are you sure you want to continue?

Continue

Cancel



There is now a new **Application setting**. Note that it still does not have the green check mark to show that it is ready for use.

Home > Resource groups > TDC_Erhverv_Telephony_Integration > NuudayToB-5sutozr67fiik

NuudayToB-5sutozr67fiik | Configuration

Search

Refresh Save Discard Leave Feedback

Functions

- App keys
- App files
- Proxies

Deployment

- Deployment slots
- Deployment Center

Settings

- Configuration
- Authentication
- Application Insights
- Identity
- Backups

+ New application setting Show values Advanced edit

Filter application settings

Name	Value	Source	Deployment slot setting
APPINSIGHTS_INSTRUMENTATIONKEY	Hidden value. Click to show value	App Service	
AzureWebJobsStorage	Hidden value. Click to show value	App Service	
FUNCTIONS_EXTENSION_VERSION	Hidden value. Click to show value	App Service	
FUNCTIONS_WORKER_RUNTIME	Hidden value. Click to show value	App Service	
FUNCTIONS_WORKER_RUNTIME_VERSION	Hidden value. Click to show value	App Service	
TeamsApplicationID	Hidden value. Click to show value	Key vault Reference	
TeamsClientSecret	Hidden value. Click to show value	Key vault Reference	
TeamsTenantID	Hidden value. Click to show value	Key vault Reference	

Updating web app settings
Successfully updated web app settings

Wait about a minute, then click **“Refresh”** and **“Continue”**. Once App reloads the new Application setting **TeamsClientSecret** should have a **green** check mark.

We are now done. You can navigate back to the Key vault, into the Access policies section, and delete the custom access you made for your user. This is good practice since only the Function app needs to be able to read the value.

If you are a power user following along by calling the App self-test endpoint via the Function App API when the response message should now say **“success: true”**.

Request/response:



```
curl https://nuudaytob-<function app name>.azurewebsites.net/api/psweb?code=<api key> \  
-d '{"function":"Test"}' \  
-H "Content-Type: application/json" -X GET
```

```
{  
  "appVersion": "1.0.0",  
  "command": "Test",  
  "success": true,  
  "message": null,  
  "resultCode": "0"  
}
```

There is no need to change anything in the in the TDC Erhverv Selfservice web portal. We have only updated the internal permissions, the public-facing API key that was previously shared with TDC Erhverv is unchanged.