

# INTEGRATING WITH ENTRUST CONNECT FOR MICROSOFT AZURE

Release: 1.0.0

Document issue: 1.2

Date of issue: March 2024

Help us to improve our documentation. Please click this link. and take our survey.

Member of Microsoft Intelligent Security Association

📕 Microsoft Security

Entrust and the Hexagon Logo are trademarks, registered trademarks and/or services marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.

© 2024 Entrust. All rights reserved.

### **Table of contents**

Revision, audience, and guide information	4
Revisions	4
Audience	4
Viewing this guide	4
Prerequisites	4
About Entrust Connect for Microsoft Azure	5
Integrating with Microsoft Azure Key Vault	6
Step 1: Create a new Azure Key Vault	6
Step 2: Generate ECS REST API Credentials	7
Step 3: Store the Entrust Certificate Services API user name and password	8
Step 4: Store the Entrust API certificate	10
Step 5: Create the App Service	12
Step 6: Update Server URL	18
Step 6: Add a system-assigned identity	19
Step 7: Assign an access policy for the App Service	20
Step 8: Enable Azure App Service Authentication	24
Troubleshooting	29
"There is no API user role configured with the Entrust Certificate Services account."	29
"The API user role within the Entrust Certificate Services account is not configured correctly."	29

## Revision, audience, and guide information

### **Revisions**

Revision	Section	Description
1.0		First release of guide
1.1	Integrating with Microsoft Azure Key Vault	Added Step 4 & 6
1.2	Minor changes	Fixed broken URL and replaced "Azure Active Directory" with "Microsoft Entra ID"

### Audience

This guide is intended for Entrust Certificate Services (ECS) users who need to integrate Azure Connect with Microsoft Key Vault.

### Viewing this guide

Although this guide can be printed, it relies on hyperlinks to other sections. It is best viewed and used electronically.

### **Prerequisites**

This guide assumes that your company already has:

- an ECS account and access to the Certificate Services REST API
- a Microsoft Azure account
- downloaded the Entrust Connect for Microsoft Azure binaries from the Entrust Website

**Note**: The Entrust Connect for Microsoft Azure App supports Microsoft Windows. Linux is not supported.

## **About Entrust Connect for Microsoft Azure**

Azure Connect allows you to request and manage Entrust SSL Certificates in your Azure Key Vault.

When you connect the Entrust Certificate Services account to your Azure Key Vault using Azure Connect, you can store and manage your certificates directly within the Key Vault.

The Key Vault is also where the Public/Private keypair is generated, and where newly issued certificates will be installed.

What you can do from the Azure Connect user interface:

- View certificates
- Create a new SSL/TLS certificate
- Install an SSL/TLS certificate
- Reissue an SSL/TLS certificate
- Renew an SSL/TLS certificate
- Revoke an SSL/TLS certificate

The Entrust Connect for Microsoft Azure binaries are available at the following link:

https://www.entrust.com/resources/tools/entrust-connect-microsoft-azure

## **Integrating with Microsoft Azure Key Vault**

Follow these steps to set up an Azure Key Vault and integrate it with Entrust Connect for Azure.

### Step 1: Create a new Azure Key Vault

- 1. Log in to the Azure portal at <u>https://portal.azure.com</u>.
- 2. In the top search panel, search for Microsoft Entra ID.
- 3. In Microsoft Entra ID, on the Overview tab, locate the Tenant ID.

= Microsoft Azure		$\mathcal P$ Search resources, services, and d	locs (G+/)		
Home >  i TenantMonkey   C Azure Active Directory	)verview … « + add > @ Man	ana tananta 🕅 What's naw 🗔 Traviaw fashuras	Got feedback? 🗸		
Overview  Preview features  Diagnose and solve problems  Manage  Users	Verview Monitorin Search your tenant Basic information	ng Tutorials			
Groups  Keternal Identities  Roles and administrators  Administrative units  Enterprise applications  Constructions  Construction	Name Tenant ID Primary domain License	TenantMonkey deaf5884-33ca-4357-b117- <mark>adc604e9a14a</mark> patrickdemo1.onmicrosoft.com Azure AD Premium P2	Users Groups Applications Devices	35 34 20 66	
Devices     App registrations	My feed				

- 4. Copy and save the last 12 digits of the **Tenant ID**. You will need it in an upcoming step.
- 5. In the top search panel, search for Key vaults.
- 6. On the Key vaults page, click Create.

Home 2	
Key vaults & - Cetait Directory	ieted yaufts 🌀 Man
Filter for any field	subscription all
Showing 1 to 1 of 1 records.	

Key vaults	~	Create key vault		
+ Create ···		Drojaet dataile		
ilter for any field Jame ↑↓		Select the subscription to manag your resources.	e deployed resources and costs. Use resource groups like fo	lders to organize and manage all
🕐 kvad61341e3aac		Subscription *	Azure subscription 1	$\sim$
		Resource group *	PsplTest Create new	~
		Instance details		
		Key vault name * 🛈	kvadx604e914a	
		Region *	East US	~
		Pricing tier * ③	Standard	$\sim$
		Recovery options		
		Soft delete protection will autom a key vault and secrets for the du within the key vault.	atically be enabled on this key vault. This feature allows you ration of the retention period. This protection applies to the	to recover or permanently delete key vault and the secrets stored

- 7. On the Create key vault screen, enter the following information:
  - a. Subscription: Select a subscription.
  - b. Resource group: Click Create new and enter a new Resource group name.
  - c. Key Vault name: Create the name using kv plus the Tenant ID you copied earlier; for example, kvadx604e914a. Do no include hyphen or space.
  - d. **Region**: Select your region.
  - e. Pricing Tier: Select the appropriate pricing tier.
- 8. Click Review and create and complete creation of the key vault.

### **Step 2: Generate ECS REST API Credentials**

Follow the steps below to generate REST API credentials from the Entrust Certificate Services (ECS) account.

- 1. Login to ECS account
- 2. Click Administration
- 3. Click Advanced Settings.
- 4. On the Advanced Settings page, click API
- 5. Click **Generate Credentials.** Note: You will need to have at least 1 active SSL certificate in your account. You will need to export this certificate into **.PFX** format for next steps.

6. Store the newly generated credentials in a safe spot. Note: The API Key role must be set to Super

# Step 3: Store the Entrust Certificate Services API user name and password

In this step, you will add the Secrets to the Key vault you just created.

For more information about the attributes of secrets, see <u>https://docs.microsoft.com/en-us/azure/key-vault/secrets/quick-create-portal</u>.

- 1. Navigate to your new Key vault.
- 2. In Settings, click Secrets.

≡ Microsoft Azure		,P Search resources, services, and docs (G+/)	
Home > kvadc604e9a14a kvadc604e9a14a   5 Key vault P Search (Ctrl+/) «	Secrets + Generate/Import 🖒 Refresh	Restore Backup	
<ul> <li>Overview</li> <li>Activity log</li> <li>Activity log</li> <li>Access control (IAM)</li> <li>Tags</li> <li>Diagnose and solve problems</li> <li>Events</li> <li>Settings</li> <li>Keys</li> <li>Secrets</li> <li>Certificates</li> <li>Access policies</li> </ul>	Name There are no secrets available.	Туре	St

3. On the Secrets page, click Generate/Import.

Microsoft Azure	ې Search reso	urces, services, and docs (G+/)
e > kvadc604e9a14a >		
eate a secret		
Jpload options	Manual	$\sim$
Name * 🕕	EntrustAPIUserName	~
Value * 🕕		
Content type (optional)		
Set activation date ①		
Set expiration date ①		
Enabled	Ves No	
Tags	0 tags	

- 4. On the **Create a secret** page, enter the following information.
  - a. Upload options: Select Manual.
  - b. Name: Enter EntrustAPIUserName. Type this value exactly as it appears here.
  - c. **Value:** Enter the Certificate Services REST API user name that was generated when creating the API key in the Certificate Services Enterprise portal.
- 5. Click Create.

You will see a confirmation message when the secret has been created successfully.

- 6. To store the Entrust REST API password, return to the Secrets page.
- 7. On the Secrets page, click Generate/Import.

treate a secret     Upload options     Manual     Name * O     EntrustAPIPassword     Value * O     Content type (optional)     Set expiration date O     Enabled     Yes     Tags     O tags	Microsoft Azure	Ø Search resources, services, and docs (G+/)
Upload options Manual   Name * O IntrustAPIPassword   Value * O	ome > Key vaults > kvad61341 reate a secret …	e3aac >
Name * O EntrustAPIPassword   Value * O   Content type (optional)   Set activation date O   Set expiration date O   Enabled Yes No   Tags 0 tags	Upload options	Manual 🗸
Value * O   Content type (optional)   Set activation date O   Set expiration date O   Enabled   Yes No   Tags   O tags	Name * 🛈	EntrustAPIPassword
Content type (optional)	Value * 🕕	······· ~
Set activation date O   Set expiration date O   Enabled   Tags   0 tags	Content type (optional)	
Set expiration date	Set activation date ①	
Enabled Yes No Tags O tags	Set expiration date 🛈	
Tags O tags	Enabled	Yes No
	Tags	0 tags

- 8. On the Create a secret page, enter the following information.
  - a. Upload options: Select Manual.
  - b. Name: Enter EntrustAPIPassword.
  - c. **Value:** Enter the Certificate Services REST API password that was generated when creating the API key in the Certificate Services Enterprise portal.
- 9. Click Create.

You will see a confirmation message when the secret has been created successfully.

### Step 4: Store the Entrust API certificate

Before performing this procedure, you must have the Certificate Services REST API certificate (PFX file) stored in an accessible location. See step 2.

For more information about importing certificates, see <u>https://docs.microsoft.com/en-us/azure/key-vault/certificates/tutorial-import-certificate.</u>

1. Navigate to your key vault and select Certificates.

■ Microsoft Azure	, P Search resources, services, and docs (G+/)	
Home > kvadc604e9a14a	rtificates	
Search (Ctrl+/)	+ Generate/Import     ○ Refresh     ↑ Restore Backup     ⊘ Manage deleted certificates     □ Certificate Co       Name     Thumbprint	ntacts 📚 Certificate Authorities
<sup>A</sup> Q Access control (IAM)	There are no certificates available.	
<ul> <li>Diagnose and solve problems</li> <li>Events</li> <li>Settings</li> </ul>		
📍 Keys		
Certificates  Certificates  Access policies  Networking		
Security     Properties		
🔒 Locks		

2. Click Generate/Import.

≡ Microsoft Azure		P Search resources, services, and docs (G+/)
Home > kvadc604e9a14a > Create a certificate	34 <b>4</b> -	
Method of Certificate Creation	Import	~
Certificate Name * ①	EntrustAPICertificate	×
Upload Certificate File *	"taha-se.testcertificates.com.pfx"	
Password		
Create		

- 3. On the Create a certificate page, enter the following information.
  - a. Method of Certificate Creation: Select Import.
  - b. Certificate Name: Enter EntrustAPICertificate.
  - c. Upload Certificate File: Select the PFX API certificate file.
  - d. **Password**: If the certificate file is password-protected, enter the certificate password.
- 4. Click Create.

### **Step 5: Create the App Service**

**Note**: Remember to follow these steps in the order they are given. The solution may not work properly if the steps are not done in the proper order.

- 1. In the Azure search panel, search for App Services.
- 2. On the App Services screen, click Create.



3. On the Create Web App screen, fill in the Instance Details and App Service Plan.

### Create Web App

-	
Instance	Details
motoriee	Dettains

Need a database? Try the new Web + Database experience. ☑

Name *	Web App name.	
		.azurewebsites.net
Publish *	● Code ○ Docker Container ○ Static Web Ap	р
Runtime stack *	ASP.NET V4.8	$\sim$
Operating System *	C Linux 💽 Windows	
Region *	East US	$\sim$
	Not finding your App Service Plan? Try a different re App Service Environment.	egion or select your
Pricing plans		

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. Learn more 🗹

Windows Plan (East US) * 🕕	ASP-azurekeyvaulttesting-8c18 (S1)				
	Create new				
Pricing plan	Standard S1 (100 total ACU, 1.75 GB memory, 1 vCPU)				

- a. In Runtime stack, select SP.NET V4.8.
- b. In Operating System, select Windows.
- c. Select an appropriate App Service Plan.

Note: The Entrust Connect for Microsoft Azure App supports Microsoft Windows. Linux is not supported.

- 4. Click Review and create and complete creation of the App Service.
- Download the Entrust Connect for Microsoft Azure App binaries from the following link:

https://www.entrust.com/resources/tools/entrust-connect-microsoft-azure

6. Unzip the file containing the Entrust Connect for Microsoft Azure App binaries.

Option 1: Upload the Connect for Microsoft Azure App Binaries to the App Services via the Microsoft Azure portal

- a. Click the App Service you just created.
- b. On the left panel, select Advanced Tools.

- c. Click **Go**. You will be directed to log in using your Entrust credentials. A new page will open.
- d. Click **Debug Console** > **CMD**.

Kudu Environment	Debug console + Process explorer Tools + Site extensions
Environment	CMD PowerShell
Build	94.30524.5227.0 (0d97b2377b)
Azure App Service	95.0.7.554
Site up time	00.02:48:12
Site folder	D:home
Temp folder	D:\local/Temp\
App Settings     Deployments     Source control info     Files     Log streaming (use cu     Processes and mini-di     Runtime versions     Site Extensions: instal	rl, not browset!) umps lied [feed
Web hooks     WebJobs: all   triggere     Functions: list   host or	rd   continuous anfig
More information	about Kudu can be found on the wiki.

- e. In the screen that appears, click the site folder.
- f. Click the wwwroot folder.

	Name	Modified	Siz
Ŧ0	deployments	10/8/2021, 4:26:57 PM	
±0	Tocks	10/8/2021, 4:26:57 PM	
TO	WWWFOOT	10/8/2021, 4:24:59 PM	
Kudu Romot	VA		
Kudu Remoto Type 'exit	♥★ ce Execution Console c' then hit 'enter' to get a new CMD process.		
Kudu Remoto Type 'exit Type 'cls'	♥★ The Execution Console ' then hit 'enter' to get a new CMD process. to clear the console		
Kudu Remoto Type 'exit Type 'cls' Microsoft N	★★ the Execution Console then hit 'enter' to get a new CMD process. to clear the console Windows [Version 10.0.14393]		
Kudu Remoto Type 'exit Type 'cls' Microsoft N (c) 2016 M	★★ te Execution Console ' then hit 'enter' to get a new CMD process. to clear the console Windows [Version 10.0.14393] ticrosoft Corporation. All rights reserved.		
Kudu Remoto Type 'exit	♥★ e Execution Console ' then hit 'enter' to get a new CMD process.		

g. Drag and drop the Connect for Microsoft Azure App binary files located into the wwwroot folder.

Drive > ··· entrust-azure-connect	> wwwroo	ot >	Search www.roo	t
▲) 🖻 🗊 ↑↓ Sort ~ ■	View ~			📑 Detai
Name	Status	Date modified	Туре	Size
🔁 runtimes	Ø	2/7/2024 10:01 AM	File folder	
🔁 www.root	0	2/7/2024 10:02 AM	File folder	
appsettings.Development	0	4/15/2022 10:23 AM	JSON File	1 KB
appsettings	0	4/15/2022 10:23 AM	JSON File	1 KB
Azure.Core.dll	0	4/15/2022 10:23 AM	Application exten	193 KB
Azure.Extensions.AspNetCore.Configurat	0	4/15/2022 10:23 AM	Application exten	28 KB
Azure.ldentity.dll	0	4/15/2022 10:23 AM	Application exten	238 KB
Azure.Security.KeyVault.Certificates.dll	0	4/15/2022 10:23 AM	Application exten	189 KB
Azure.Security.KeyVault.Secrets.dll	Ø	4/15/2022 10:23 AM	Application exten	107 KB
EntrustDataCardtAPI.deps	0	4/15/2022 10:23 AM	JSON File	198 KB
S EntrustDataCardtAPI.dll	0	4/15/2022 10:23 AM	Application exten	39 KB
EntrustDataCardtAPI	0	4/15/2022 10:23 AM	Application	171 KB

Kudu Environment Debug console - Process explorer Tools - Site extensions



- h. Go back to the Azure Portal.
- i. Click App Services.

- j. Click the name of the application you created.
- k. Click the **Application URL** to verify that the application is up and running.

## Option 2: Upload the Entrust Connect for Microsoft Azure App binaries to the App Services via Get publish profile

This option allows you to upload using any FTP client.

a. On the App Services screen, select the name of your new App Service.

= Microsoft Azure		,P Search resources, services, and docs (G+/)	
Home > App Services > App Services « TerantMankey (patrickeren 1.ormicrosoft.com) + Create ③ Manage view ~ ····	Azure-ECS-App-Wi	ר אייי מי Browse □ Stop 2 Swap ◯ Restart । Delete   ◯ Refresh 🔮 Get publish profile 🤊 Reset p	iblish profile 🔋 Share to mobile ♡
Filter for any field Name 10 Azure-ECS-App-Win	Overview     Activity log     Activity log     Access control (IAM)     Tags     Diagnose and solve problems     Security     Events (preview)	Essentials     Get publish p Get publis	URL Health Check App Service Plan FTP/deployment username FTP hostname FTPS hostname
Deployment Quickstart Deployment slots Deployment Center	Deployment     Quickstart     Deployment slots     Deployment Center     Settings	Diagnose and solve problems. Or sint-aniod diagnesis and textbehoosing experience helps you identify and resolve issues with your web app.         Application insight helps you detect and diagnese quality: issues in your upps, and helps you understand what your use actually do with it.	App Service Advisor App Fervice Advisor poolde experience on the App Servic are sorted by freshness, prior
		Http 5xx         Data In           100         339           20         309           20         309           20         309           20         309           20         309           20         309           20         309           20         309           20         309           20         309           20         309           20         309           309	

b. Click Get publish profile to download the profile.

You will see the FTP credentials in the PublishSettings file. The Get publish profile will make it easier to FTP the Connect for Microsoft Azure App binaries to the App Services using any FTP Client.

					and the second	-	-		A		
and they			-								
		Constant of the					-			and market	
		-								-	
	1.00		1					100			-
				1.00							

### Step 6: Update Server URL

Note: This step will be eliminated in a future version of the app.

- 1. Update Server URL: Open your new app from App Services
- 2. Copy the Default Domain URL

📀 azuretestrohin 🔗 🕏	۲				
✓ Search «	$\square$ Browse $\square$ Stop $\rightleftharpoons$ Swap $\bigcirc$ Restan	t 🗐 Delete   💍 Refresh 🛓	Download publish p	orofile 🏾 🏷 Reset publish profile 🛛 🔲 Share to mobile	
S Overview					
Activity log	Resource group (move) : azure-kewault-testing		Default domain	azuretestrohin azurewebsites net	
Access control (IAM)	Status : Running		App Service Plan	: ASP-azurekeyvaulttesting-8c18 (S1: 1)	
🗳 Tags	Location ( <u>move</u> ) : East US		Operating System : Windows		
Diagnose and solve problems	Subscription (move) : Entrust Enterprise Dev/	Test Subscription	Health Check	: Not Configured	
Ø Microsoft Defender for Cloud	Subscription ID : 2446ca95-166a-49ed-9	830-2faf4a40dd08			
🗲 Events (preview)	Tags ( <u>edit</u> ) : Click here to add tags				
Deployment	Properties Monitoring Logs Capab	ilities Notifications Recommer	ndations		
😎 Deployment slots	💿 Web app				
😝 Deployment Center	Name	azuretestrohin			
Settings	Publishing model	Code			
Configuration	Runtime Stack	Dotnet - v4.0			

3. Open App Service Editor

azuretestrohin   Ap Web App	op Service Editor (Preview) 🛛 🛧 …
ho editor $ imes$ «	
Development Tools	App Service Editor (Preview)
App Service Editor (Preview)	App Service Editor provides an in-browser editing experience for your App code. Learn more
	Open Editor 🗗

4. Open Main.js file and update lines 11234, 11235 with the *Default Domain* URL you copied in previous step.

	iervice Editor   azuretestrohin 👻		
n ·	EXPLORE	main.j	js www.root
	WORKING FILES	11210	styleUrls: ['./success.component.css']
$\circ$	main.js www.root/www.root	11211	31
~ ~	WWWROOT	11212	<pre>}], function () { return [{ type: src_app_entrust_service_WEBPACK_IMPORTED_MODULE_1_["EntrustService"] }]; }, null); })();</pre>
	4 www.root	11213	
<b>V</b>	▶ runtimes	11215 /	/***/ }),
	4 www.root	11216	
	▷ assets	11217 /	/***/ "./src/environments/environment.ts":
	favicon ico	11218 /	*/
$\odot$	index later I	11219	<pre>!*** ./src/environments/environment.ts ***!</pre>
	index.ntm	11220	(
▣	main.js	11222	<pre>. exposes provaded. environment exports . webpack require ) {</pre>
~	main.js.map	11223	
	polyfills.js	11224 "	'use strict";
$\sim$	polyfills.js.map	11225	_webpack_requirer(_webpack_exports);
$\bigcirc$	runtime.js	11226 /	<pre>(* harmony export (binding) */webpack_required(webpack_exports, "environment", function() { return environment; });</pre>
$\odot$	runtime.js.map	11227 /	// This file can be replaced during build by using the fileReplacements array.
	styles.is	11228 /	/ ng bullaproa replaces environment.ts with environment.proats.
	styles is man	11230	/ The fist of the replacements can be found in angular.json .
	vendezia	11231	production: true,
	venuorijs	11232	//azureserver :'https://pdevtestapimanagement.azure-api.net/',
	vendor.js.map	11233	//apiserver :'https://pdevtestapimanagement.azure-api.net/',
	appsettings.json	11234	<pre>//apiserver : https://azuretestrohin.azurewebsites.net',</pre>
	appsettings.Development.json	11235	apiserver: 'https://azuretestrohin.azurewebsites.net/',
	Azure.Core.dll	11230	// baseuriiocalstorage.getitem( baseuri ),
	Azure.Extensions.AspNetCore.Configuration.Secrets.dll	11238	k:
	Azure.Identity.dll	11239	/#
	Azure.Security.KeyVault.Certificates.dll	11240	* For easier debugging in development mode, you can import the following file
	Azure.Security.KeyVault.Secrets.dll	11241	<pre>* to ignore zone related error stack frames such as `zone.run`, `zoneDelegate.invokeTask`. *</pre>

### Step 6: Add a system-assigned identity

Set up an Azure Service to create a managed identity.

1. In the Azure portal, in the top search panel, search for App Services and configure the new App Service that you created in **Step 4**.



- 2. In the existing App Service, click Identity.
- 3. On the Identity page, select the System assigned tab.
- 4. Click the **Status** switch to **On**.
- 5. In Object ID, copy and save the alphanumeric code. You will need this in the next step.
- 6. Click Save.

### Step 7: Assign an access policy for the App Service

Assign an access policy for the App Service in your key vault.

For more information on managed identities for App Services, see <a href="https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy-portal">https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy-portal</a>

1. Navigate to your new key vault.

₽ Search	K + Create Create C Refresh   🗎 Delete 🖉 Edit
⑦     Overview       ■     Activity log       冷     Access control (IAM)       ⑦     Tags       ★     Diagnose and solve problems       第     Access policies	Access policies enable you to have fine grained control over access to vault items. Learn more           Permissions : All ×         Type : All ×
Events Objects	
Y Keys	No access policies fou
Certificates	No access policies were found. Try clearing your filters or Add policy
Settings	
≆ Access configuration	Learn more
<li>Networking</li>	
Ø Microsoft Defender for Cloud	
Properties	
Locks	

- 2. In Settings, select Access policies.
- 3. Click Add Access Policy.

Create an access policy kv3acba8ec8fe4		
Permissions 8 Principal	) Application (optional) (4) R	leview + create
Configure from a template Key, Secret, & Certificate Management	~	
Key permissions	Secret permissions	Certificate permissions
Key Management Operations	Secret Management Operations	Certificate Management Operations
Select all	Select all	Select all
🗹 Get	🖌 Get	🖌 Get
🗸 List	🗸 List	🗹 List
✓ Update	🗹 Set	Update
✓ Create	🔽 Delete	Create
✓ Import	Recover	Import
✓ Delete	🔽 Backup	✓ Delete
Recover	Restore	Recover
✓ Backup	Drivillana d Caranto Carantiana	Backup
Restore	Privileged Secret Operations	Restore
Camtographic Operations		Manage Contacts
	Purge	Manage Certificate Authorities
		Get Certificate Authorities
Decrypt		<ul> <li>List Certificate Authorities</li> </ul>
Encrypt		Set Certificate Authorities
Unwrap Key		Delete Certificate Authorities
Wrap Key		Privileged Certificate Operations
Venty		Select all
Sign		
Privileged Key Operations		L Purge
Salact all		
Previous Next		

- 4. On the Add access policy screen, select the following:
  - a. Configure from template (optional): Select Key, Secret, & Certificate Management.
  - b. Select Principal: Select None selected. The Principal pane appears.
  - c. Paste in the **Object ID** you copied in the last step.
  - d. Click Select.

Home > Key vaults	s > kv3acba8ec8f	e4   Access policies >		
Create an a kv3acba8ec8fe4	ccess poli	су		
Permissions	8 Principal	③ Application (optional)	(d) Review + create	
Principal is requ	ired.			×
Only 1 principal can Use the new embedo	be assigned per acc ded experience to s	ess policy. elect a principal. The previous po	pup experience can be accessed	I here. Select a principal
	c-4b44-8e4e-1bc5	7ecca184		×
azurete 38052e	estrohin 1c-30d2-4a22-a56f-a	30552323a3b		

ected item	
tem selected	
Previous Next	

5. Under Add access policy on the left, click Add.



6. On the Access policies page for your key vault, confirm that the new access policy

appears in the Current Access Policies list.

Note: The new access policy is not applied until you confirm and **Save** on the **Access** polices page.

7. Click Save.

After deploying the Connect for Microsoft Azure App Service, Microsoft, by default, will publish a public facing URL; e.g., https://azure-ecs-app-win.azurewebsites.net

To avoid unauthorized users from accessing the application, set up an identity provider by following the steps in the next section.

### **Step 8: Enable Azure App Service Authentication**

The goal of this step is to provide your users with an authentication process to access the Entrust Connect for Microsoft Azure App.

- 1. In Azure App Services, click your application.
- 2. In the left panel click Authentication.

, <sup>O</sup> Search (Ctrl+/)	Send us your feedback
P Tags	
Diagnose and solve problems	
Security	
Events (preview)	
eployment	
Quickstart	
Deployment slots	
Deployment Center	
ttings	Add an identity provider
L Confinentian	Choose an identity providers include Microsoft, Facebook, Google, and Twitter.
Comparation	Learn more about identity providers d'
Authentication	Artid identifies provides
Identity	Here restricts because
Backups	
Custom domains	
TIS/SSI settings	

- 3. Click Add identity provider.
- 4. In the screen that appears, select Microsoft.

se an identity provider from th	e dropdown below to start.
ty provider *	Select identity provider
	Microsoft
	Sign in Microsoft and Azure AD identities and call Microsoft APIs
	O Facebook
	Sign in Facebook users and call Facebook APIs
	G Google
	Sign in Google users and call Google APIs
	y Twitter
	Sign in Twitter users and call Twitter APIs
	OpenID Connect (preview)
	Sign in users with OpenID Connect

A new screen appears.

ome > App Services > Azure-EC	vider	
Rud an identity pro	vider	
prigos - T.Z. Hardenia		
Basics Permissions		
Identity provider *	Microsoft	Y
App registration		
An app registration associates your your provider to create a new one. I	identity provider with your app. Enter the app registration information	n here, or go to
	Create new ann registration	
App registration type "	Pick an existing and registration in this directory	
	<ul> <li>Provide the details of an existing app registration</li> </ul>	
Name * 🔘	Azure-ECS-App-Win	
Supported account types *	Current tenant - Single tenant	
	Any Azure AD directory - Multi-tenant	
	Any Azure AD directory & personal Microsoft accounts	
	O Personal Microsoft accounts only	
	Help me choose	
App Service authentication settle	ngs	6
Requiring authentication ensures all you'll need your own code for speci	users of your app will need to authenticate. If you allow unauthentica fic authentication requirements. Learn more B	ited requests,
Restrict access *	Require authentication	
-	Allow unauthenticated access	
Unauthenticated requests *	HTTP 302 Found redirect: recommended for websites	1
	HTTP 401 Unauthorized: recommended for APIs	-
	O HTTP 403 Forbidden	
Redirect to	Microsoft	$\sim$
Token store 🕤		

- a. In App registration type, select Create new app registration.
- b. In Supported account types, select Current tenant.
- c. In Restrict access, select Require Authentication.
- d. In Unauthenticated requests, select HTTP 302.
- e. Select the **Token store** checkbox.
- 5. Click Add.

= Microsoft Azure		e s	earch resources, services, and docs (G+/)	
Home > Azure-ECS-App-Win Azure-ECS-App-V App Service Search (Ctrl+/)	Vin   Authentication «                                   Send us your feedback			
<ul> <li>Overview</li> <li>Activity log</li> <li>Access control (IAM)</li> <li>Tags</li> <li>Diagnose and solve problems</li> <li>Security</li> <li>Events (preview)</li> </ul> Deployment <ul> <li>Quickstart</li> <li>Deployment slots</li> <li>Deployment Center</li> </ul>	<ul> <li>With App Service you can choo which provider is handling auth</li> <li>Authentication settings</li> <li>App Service authentication</li> <li>Restrict access</li> <li>Unauthenticated requests</li> <li>Redirect to</li> <li>Token store</li> <li>Identity provider</li> <li>+ Add provider</li> </ul>	yse an identity provider to manage user ide hentication for your app. Learn more O' Edit Enabled Require authentication Return HTTP 302 Found (Redirect to id Microsoft Enabled	entities and authentication flows. Add providers here, edit so lentity provider)	ettings, and decide
Settings			rpp (clent) ib	
Configuration	Microsoft (Azure-ECS-App-W	/in)	b27a3c8b-5ebb-4498-a4d6-e58b5a22c5e3	
Authentication				
Application Insights				
% Identity				
🕜 Backups				
🔤 Custom domains				
TLS/SSL settings				

- 6. In the screen that appears, copy the App (client) ID of the new Identity.
- 7. Search for Microsoft Entra ID.
- 8. In the left panel, select App registrations.

≡	Microsoft Azure	P Search resources, services, and docs (G+/)	Þ.	C,	Q	۲	0	ጽ	DEFAULT DIRECTORY
Но	me > Default Directory								
	Azure Active Directory	App registrations 🖈 …							×
0	Overview	+ New registration 🔀 Endpoints 🖉 Troubleshooting 🖒 Refresh 🞍 Download 🐻 Preview features   🛇 Go	feedback?						
	Preview features	() Try out the new App registrations search preview/ Click to enable the preview. $ ightarrow$							×
Ma	nage	A Startion June 20th 2020 valuel no lonner will any new features to Annee Active Directory Authentication Elevery (ADA1) and Annee Active Directory Active Directory Authentication Elevery (ADA1) and Annee Active Directory Acti	D Granh We wi	il contin	ue to pr	ovide te	ebnical s	innort :	and security undates but we X
*	Users	will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more							Rectangle
24 10	Groups External Identities	All applications Owned applications Deleted applications (Preview) Applications from personal account							
2.	Roles and administrators								×
28 11	Administrative units Enterprise applications	Display name Application (clier	) ID				Created	on	Certificates & secrets
q	Devices	EN EntrustDataCardtAPIAng b55e91f0-f7df-4b	8-9ce7-db67i	o27fafa1	1		9/22/20	21	🛇 Current
- 89,	App registrations								
۵	Identity Governance								
15	Application proxy								

9. In the search box, paste the App (client) ID you copied in the previous step.

### 10. Redirect URIs are generated.



## Troubleshooting

This section lists problems or error messages you might encounter during or after the Azure integration, along with advice for their resolution.

### "There is no API user role configured with the Entrust Certificate Services account."

### **Cause of the problem:**

You will see this error message if the user credential for the ECS REST API has been deleted but is still configured in the Entrust Connect for Microsoft Azure Application.

### How to fix the problem:

Update the user credential for the ECS REST API in the Connect for Microsoft Azure Application to match the credentials in the Entrust Certificate Services account.

### "The API user role within the Entrust Certificate Services account is not configured correctly."

### **Cause of the problem:**

You will see this error message if the API user role in the Entrust Certificate Services account is not correctly configured.

### How to fix the problem:

Ensure that the API user role is correctly configured as follows:

- 1. An active and issued TLS/SSL client certificate is bound to the API.
- 2. Access Permission is set to Super.
- 3. Auto Approve is enabled.