

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	
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		P Search resources, services, and d	locs (G+/)	
me > TenantMonkey Azure Active Directory		ie tenants 👩 What's new 🗔 Preview features	🕞 Got faadback? 🖂	
Overview Preview features Diagnose and solve problems	Overview Monitoring			
nage Users	Basic information			
Groups	Name	TenantMonkey	Users	35
External Identities	Tenant ID	deaf5884-33ca-4357-b117- <mark>adc604e9a14a</mark> 🗈	Groups	34
Roles and administrators Administrative units	Primary domain	patrickdemo1.onmicrosoft.com	Applications	20
Enterprise applications	License	Azure AD Premium P2	Devices	66
Devices	My feed			
App registrations				

- 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 3	
Key vaults &	trd youths 🌀 Man
	subscription all
Showing 1 to 1 of 1 records.	

Key vaults « Default Directory	Create key vault		
+ Create ···			
	Project details		
Filter for any field Name ↑↓	Select the subscription to manage your resources.	deployed resources and costs. Use resource groups like fol	ders 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	~
	Recovery options		
		tically be enabled on this key vault. This feature allows you t ation of the retention period. This protection applies to the	

- 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.

		P Search resources, services, and docs (G+/)	
Home > kvadc604e9a14a kvadc604e9a14a Key vauit P Search (Ctrl+/) «			
 Overview Activity log Access control (IAM) Tags Diagnose and solve problems Events Events Settings Keys Secrets Certificates Access policies 	Name There are no secrets available.	Туре	St

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

Microsoft Azure	P Search re	sources, services, and docs (G+/)
e > kvadc604e9a14a >		
ate a secret		
pload options	Manual	\checkmark
ame * 💿	EntrustAPIUserName	×
alue * 🕕		
ontent type (optional)		
et activation date ①		
et expiration date ①		
nabled	Yes No	
gs	0 tags	
24		

- 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.

upload options Manual Name * O EntrustAPIPassword Value * O	Microsoft Azure	Ø Search resources, services, and docs (G+/)
Name * ① EntrustAPIPassword Value * ① Content type (optional) Set activation date ① Set expiration date ① Enabled Yes No		e3aac >
Value * O · · · · · · · · · · · · · · · · · ·	Upload options	Manual 🗸
Content type (optional) Set activation date Set expiration date Set ex	Name * 🛈	EntrustAPIPassword
Set activation date Set expiration date Enabled Yes No	Value * 🕕	······· ~
Set expiration date C Enabled Ves No	Content type (optional)	
Enabled Yes No	Set activation date ①	
	Set expiration date 🛈	
Tags 0 tags	Enabled	Yes No
	Tags	0 tags
Create		

- 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+/)	
ome > kvadc604e9a14a		
kvadc604e9a14a Ce	tificates …	
© Search (Ctrl+/) «	+ Generate/Import	tificate Contacts 🎏 Certificate Authorities
Overview	Name Generate/Import Thumbprint	Status
Activity log	There are no certificates available.	
Access control (IAM)		
Tags		
Diagnose and solve problems		
🗲 Events		
Settings		
📍 Keys		
Secrets		
Certificates		
Access policies		
Is Networking		
Security		
Properties		
🔒 Locks		

2. Click Generate/Import.

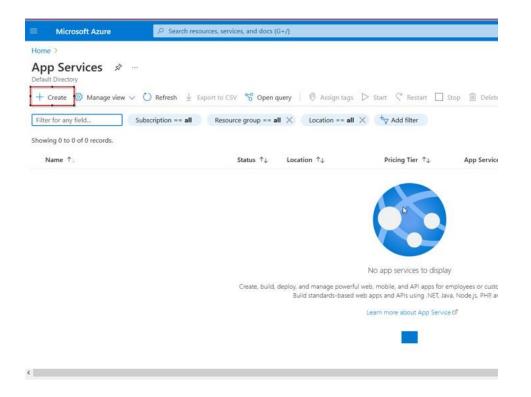
≡ Microsoft Azure		P Search resources, services, and docs (G+/)
Home > kvadc604e9a14a > Create a certificate)	
Method of Certificate Creation	import	~
Certificate Name * ①	EntrustAPICertificate	×
Upload Certificate File *	"taha-se.testcertificates.com.pfx"	
Password		
Create		

- 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 Detai	5

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

Name * Web App name.		
		.azurewebsites.net
Publish *	● Code ○ Docker Container ○ Static We	ь Арр
Runtime stack *	ASP.NET V4.8	\sim
Operating System *	C Linux 💿 Windows	
Region *	East US	~
	O Not finding your App Service Plan? Try a different App Service Environment.	ent region 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 Control + Other Control + Con
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:\localTemp\
App Settings Deployments Source control info Files Log streaming (use cc Processes and mini-d Runtime versions Site Extensions: instat	umps
Web hooks WebJobs: all triggere Functions: list host c	
More information	about Kudu can be found on the wiki.

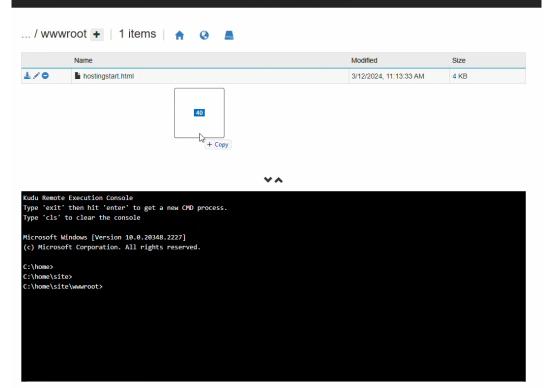
- e. In the screen that appears, click the site folder.
- f. Click the wwwroot folder.

Name		Modified	S
LO Deployments		10/8/2021, 4:26:57 PM	
LO Tocks		10/8/2021, 4:26:57 PM	
		10/8/2021, 4:24:59 PM	
Kudu Remote Execution Console	**		
Kudu Remote Execution Console Type 'exit' then hit 'enter' to ş			
Kudu Remote Execution Console Type 'exit' then hit 'enter' to β Type 'cls' to clear the console			
Type 'exit' then hit 'enter' to g Type 'cls' to clear the console	yet a new CMD process.		
Type 'exit' then hit 'enter' to a	get a new CMD process. 4393]		
Type 'exit' then hit 'enter' to g Type 'cls' to clear the console Microsoft Windows [Version 10.0.1	get a new CMD process. 4393]		

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

Drive > ··· entrust-azure-connect > wwwroot > Search wwwroot				
▲) 🖄 🕅 ↑↓ Sort ~ ■	View ~			🕕 Details
Name	Status	Date modified	Туре	Size
📒 runtimes	0	2/7/2024 10:01 AM	File folder	
n 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.Identity.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	0	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 « TerantMarkey (patrickermo1.orm/crosoft.com) + Create @ Manage view ~ ···	Azure-ECS-App-Wi App Service) Reset publish profile 🚦 Share to mobile 👳 Sa
Filter for any field Name 1: Azure-ECS-App-Win	Overview Activity log Activity log Access control (IAM) Tags Diagnose and solve problems Socurity Events (preview)	Essentials Resource group (change) : Azure-ECS-App-Service-Recource Status : Running Location : Central US Subscription (change) : Azure subscription 1 Subscription ID : c! Tags (Edit) : Click here to add tags	t publish profile URL i h Health Check i N App Service Plan i A FTP/deployment username i fi FTP hostname i fi FTPS hostname i fi
Deployment Quickstart Deployment slots Deployment Center	 Quickstart Deployment slots 	Diagnose and solve problems Cur self-service dispersite and too dischooling experience Netropy to dispersite and too dischooling experience Netropy to dispersive stude stude sets and your web spip	
	Settings III Configuration Authentication Application Insights Identity Backups Custom domains TLS/SSL settings Networking Scale up (App Service plan) Scale out (App Service plan) Scale out (App Service plan) Web/obs	Http Sox Data In 100 358 50 368 50 208 50 208 50 208 50 208 50 208 50 208 50 208 50 208 50 208 50 208 50 208 50 318	Data Out 408 338 338 338 338 338 338 338 3

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.

COLUMN TWO IS NOT	and the local data in		and the second		Contraction of the local division of the loc
and the second second	Chief and the second second	in in faith of proper	CONTRACTOR OF	the second second second	10.00
			EL DE		And a second second
	1.111	10000		1.000	121.10

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 🔗	★ …	
	🖬 Browse 🔲 Stop 💳 Swap 📿 Restart 🛅 Delete 🛛 🏷 Refrest	n 🞍 Download publish profile 🏷 Reset publish profile 🛛 🗍 Share to mobile
Overview		
Activity log	Resource group (move) : azure-keyvault-testing	Default domain : azuretestrohin.azurewebsites.net
Access control (IAM)	Status : Running	App Service Plan : ASP-azurekeyvaulttesting-8c18 (S1: 1)
🔷 Tags	Location (move) : 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-9830-2faf4a40dd08	
🗲 Events (preview)	Tags (<u>edit</u>) : Click here to add tags	
Deployment	Properties Monitoring Logs Capabilities Notifications Reco	ommendations
🖶 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 🗗

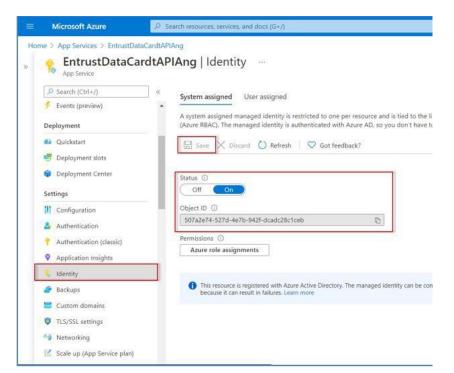
4. Open Main.js file and update lines 11234, 11235 with the *Default Domain* URL you copied in previous step.

EXPLORE	main.js www.root
✓ WORKING FILES	11210 styleUrls: ['./success.component.css']
main.js www.root/www.root	11211 }]
▲ WWWROOT	<pre>11212 }], function () { return [{ type: src_app_entrust_service_WEBPACK_IMPORTED_MODULE_1_["EntrustService"] }]; }, null); })(</pre>
⊿ www.root	11213 11214
▷ runtimes	11215 /***/ }),
	11216
⊿ www.root	11217 /***/ "./src/environments/environment.ts":
▷ assets	11218 /*!***********************************
favicon.ico	11219 !*** ./src/environments/environment.ts ***!
index.html	11220 ***********************************
main.js	11221 /*! exports provided: environment */
main.js.map	11222 /***/ (function(module,webpack_exports_,webpack_require) {
polyfills.js	11223
	11224 "use strict"; 11225 webpack require .r(webpack exports);
polyfills.js.map	<pre>11225 _webpack_requirerc_webpack_exports, 11226 /* harmony export (binding) */ webpack require .d(webpack exports , "environment", function() { return environment; });</pre>
runtime.js	11227 / This file can be replaced during build by using the 'fileReplacements' array.
runtime.js.map	11228 // `ng buildprod` replaces `environment.ts` with `environment.prod.ts`.
styles.js	11229 // The list of file replacements can be found in `angular.json`.
styles.js.map	11230 const environment = {
vendor.is	11231 production: true,
vendor.js.map	11232 //azureserver :'https://pdevtestapimanagement.azure-api.net/',
	11233 //apiserver :'https://pdevtestapimanagement.azure-api.net/',
appsettings.json	11234 //apiserver : https://azuretestrohin.azurevebsites.net',
appsettings.Development.json	<pre>11235 apiserver: 'https://azuretestrohin.azurewebsites.net/', 11236 // baseUrl:localStorage.getItem('baseUrl'),</pre>
Azure.Core.dll	11250 // Daseor1:10talstorage.gertem, Daseor1), 11237 KENDO UI LICENSE: "/kendo-ui-license.txt"
Azure.Extensions.AspNetCore.Configuration.Secrets.dll	1123) k:
Azure.Identity.dll	11239 /*
Azure.Security.KeyVault.Certificates.dll	11240 * For easier debugging in development mode, you can import the following file
	11241 * to ignore zone related error stack frames such as `zone.run`, `zoneDelegate.invokeTask`.
Azure.Security.KeyVault.Secrets.dll	11347 *

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 https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy-portal

1. Navigate to your new key vault.

₽ Search	K + Create 🖒 Refresh 🗊 Delete 🖉 Edit
 ⑦ Overview ☑ Activity log ⁰ Access control (IAM) ◊ Tags ✗ Diagnose and solve problems 	Access policies enable you to have fine grained control over access to vault items. Learn more Search Permissions : All × Type : All ×
€ Access policies	
Events Objects Keys	
Secrets	No access policies fou
Certificates	No access policies were found. Try clearing your filters or Add policy
Settings	Learn more
Æ Access configuration	Learn note
Networking	
Ø Microsoft Defender for Cloud	
Properties	
Locks	

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

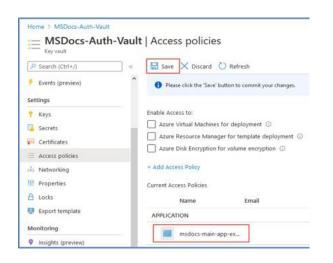
Create an access policy kv3acba8ec8fe4		
Permissions S Principal	Application (optional)	leview + create
Configure from a template		
Key, Secret, & Certificate Management	\vee	
Key permissions	Secret permissions	Certificate permissions
Key Management Operations	Secret Management Operations	Certificate Management Operations
Select all	Select all	Select all
🗹 Get	🖌 Get	🗹 Get
🗹 List	🖌 List	✓ List
✓ Update	🖌 Set	Update
✓ Create	🗸 Delete	Create
✓ Import	Recover	Import
✓ Delete		✓ Delete
Recover	Restore	Recover
✓ Backup		Backup
Restore	Privileged Secret Operations Select all	Restore
Cryptographic Operations		Manage Contacts
Select all	Purge	Manage Certificate Authorities
		Get Certificate Authorities
Decrypt		 List Certificate Authorities
Encrypt		Set Certificate Authorities
Unwrap Key		Delete Certificate Authorities
Wrap Key		Privileged Certificate Operations
Verify		Select all
Sign		
Privileged Key Operations		Purge
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		ess policy. elect a principal. The previous po	pup experience can be accessed	I here. Select a principal
	c-4b44-8e4e-1bc5	7ecca184		×
	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.

,₽ Search (Ctrl+/) ≪ Send us your fe	edback
♦ Tags	
Diagnose and solve problems	
Security	
Events (preview)	
Deployment	
Guidstart	
Deployment slots	
Deployment Center	
Deployment Center	Add an identity provider
Settings	Choose an identity provider to manage the user identities and authentication flow for your application. Providers include Microsoft, Facebook, Google, and Twitter.
Configuration	Learn more about identity providers d'
& Authentication	
Application Insights	Add identity provider
🕻 identity	
🖀 Backups	
Custom domains	
TLS/SSL settings	

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

ose an identity provider from th	e dropdown below to start.
Identity provider *	Select identity provider 🗸 🗸
	Microsoft
	Sign in Microsoft and Azure AD identities and call Microsoft APIs
	() 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.

	vider …	
Basics Permissions		
Identity provider *	Microsoft	Y
App registration		
	identity provider with your app. Enter the app registration information Learn more D [*]	here, or go to
App registration type *	Create new app registration	
	Pick an existing app registration in this directory	
	O Provide the details of an existing app registration	
Name * 🕕	Azure-ECS-App-Win	
Supported account types *	Current tenant - Single tenant	
	O Any Azure AD directory - Multi-tenant	
	O Any Azure AD directory & personal Microsoft accounts	
	O Personal Microsoft accounts only	
	Help me choose	
App Service authentication setti	ings	2
	I users of your app will need to authenticate. If you allow unauthentica ific authentication requirements. Learn more \mathbb{D}^{\prime}	ted requests,
Restrict access *	Require authentication	
	Allow unauthenticated access	
Unauthenticated requests *	HTTP 302 Found redirect: recommended for websites	1
	O 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.

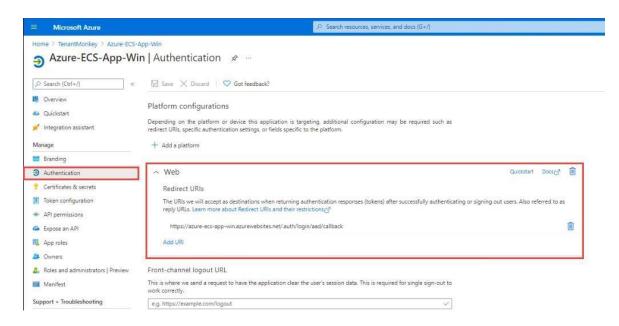
= Microsoft Azure		2 9	search resources, services, and docs (G+/)	
App Service	Vin Authentication			
 Overview Activity log Access control (IAM) Tags Diagnose and solve problems Security Events (preview) Deployment Quickstart Deployment slots Deployment Center 		hentication for your app. Learn more 6	entities and authentication flows. Add providers here, edit se dentity provider) App (client) ID	attings, and decide
Settings				
III Configuration	Microsoft (Azure-ECS-App-W	(in)	b27a3c8b-5ebb-4498-a4d6-e58b5a22c5e3	
Authentication				
Application Insights				
% Identity				6
🥔 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	℅ Search resources, services, and docs (G+/)	D 🔂 🗘		DEFAULT DIRECTORY
ome > Default Directory				
Azure Active Directory	y App registrations 🛷 …			
Overview	≪ + New registration ⊕ Endpoints 🤌 Troubleshooting 🖒	Refresh 🛓 Download 🖽 Preview features 🛛 💝 Got feedback?		
Preview features Diagnose and solve problems	Try out the new App registrations search preview! Click to enable the search preview?	he preview. →		
inage	Starting June 30th, 2020 we will no longer add any new features to	o Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to p	rovide technical support a	and security updates but we
Users	will no longer provide feature updates. Applications will need to be	e upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more		
Groups External Identities	All applications Owned applications Deleted application	ons (Preview) Applications from personal account		
Roles and administrators	P b55e91f0-f7df-4b28-9ce7-db67b27fafa1			
Administrative units				
Administrative units		Application (client) ID	Created on	Certificates & secrets
	Display name	Application (client) to		certificates à secrets
Enterprise applications	EntrustDataCardtAPIAng	b55e91f0-f7df-4b28-9ce7-db67b27fafa1	9/22/2021	Current
Enterprise applications Devices			9/22/2021	
Administrative units Enterprise applications Devices App registrations Identity Governance			9/22/2021	

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.