

# Dell Security Center Quickstart Guide

## Azure Account: Paid Azure Subscription vs. Free Azure Account

Both paid Azure subscriptions and free Azure accounts are supported for Dell Security Center tenant setup, as follows:


- **Paid Azure subscription:** Dell provides an automated tenant setup script. This script requires Azure's Cloud Shell, which is included in a paid subscription to Azure.
- **Free Azure account:** A free Azure account requires a tenant to be set up manually, as Azure's Cloud Shell is not provided with a free account.

Microsoft offers pay-as-you-go subscriptions that are budget-friendly. Free Azure accounts can easily be upgraded to paid subscriptions. See <https://azure.microsoft.com>.


## Set up tenant when using a paid Azure subscription

The basic implementation process includes these steps:

1. Retrieve the two emails sent to you from **tenantservices@dellsecuritycenter.com**. You will need these during setup.

Dell Data Security 

### Thank you for your purchase



This solution is a cutting edge security protection product.  
It protects data, prevents data leakage, and secures endpoints from the centrally managed Dell Security Center.

**Start protecting your environment today!**

[Register your account](#)

Verification Email: `{{VerificationEmail}}`

Sign-on URL: `{{URL}}`


---

#### Learn more about the console

The Dell Security Center is responsible for the management of Dell's award winning data security products.

[Administrator guide and documentation](#)

[Quickstart Guide](#)




---

#### Support and references


[Support website and videos](#)

[Common questions](#)

[Support phone numbers](#)



**Dell**  
Tech Support



### Dell Security Center

#### Verification Code

Enter the following verification code into the corresponding field in the Dell Security Center Setup Wizard

**`{{.VerificationCode}}`**

2. Click **Register your account** from your welcome email to get started.



3. The setup wizard opens. Click **Next** and enter the verification email and code from these emails into the setup wizard.

Verification

From your 'Welcome' and 'Verification Code' emails, please enter your assigned credentials to continue setup.

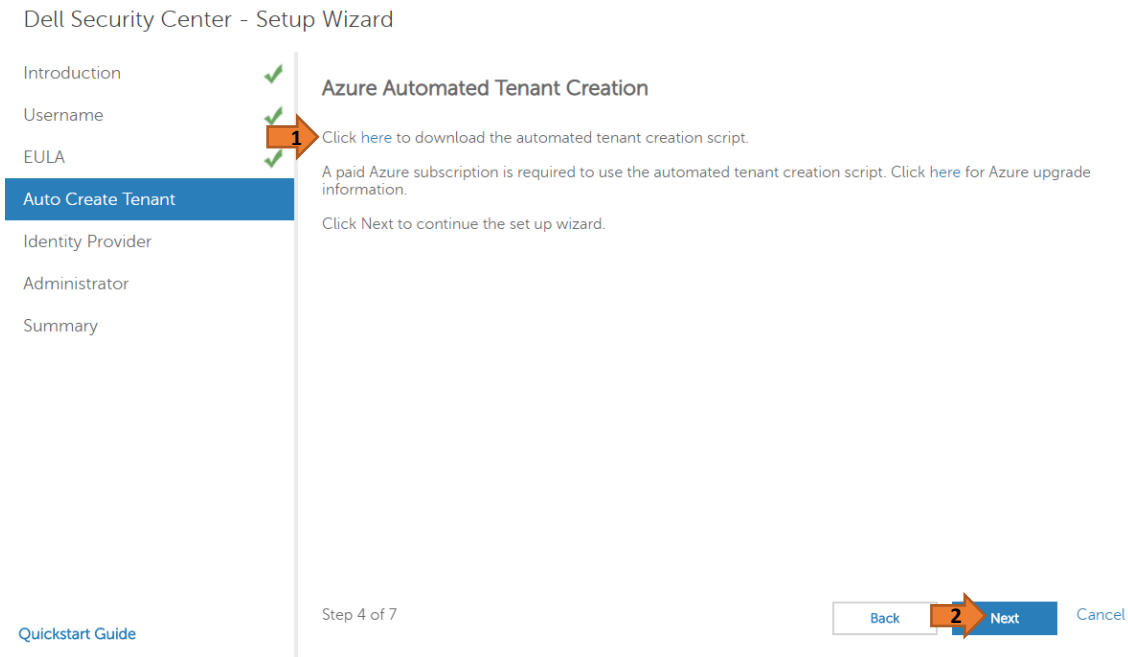
Email:

Code:

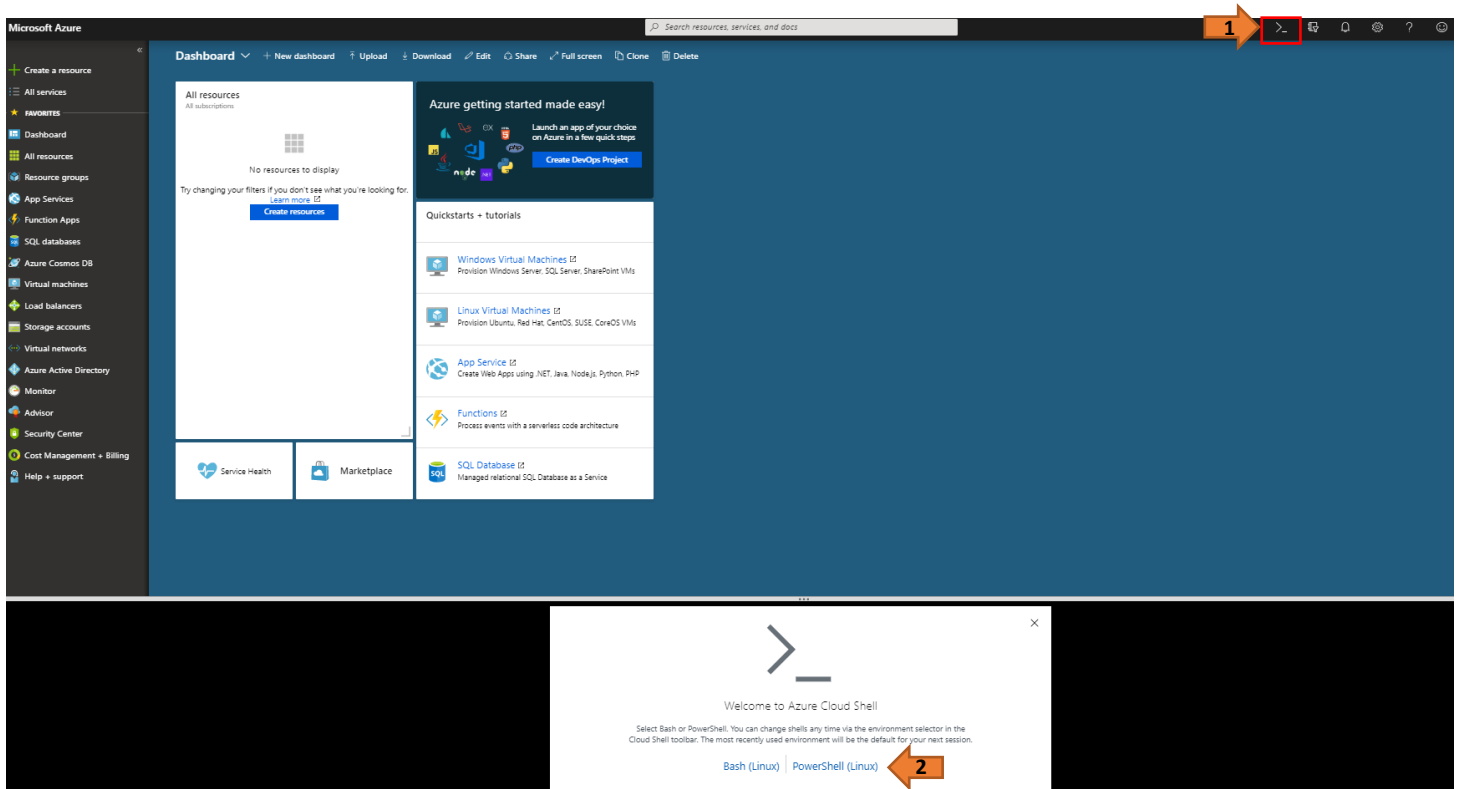
4. Read and accept the Terms and Conditions of the license agreement.

I accept the terms and conditions of the license agreement.

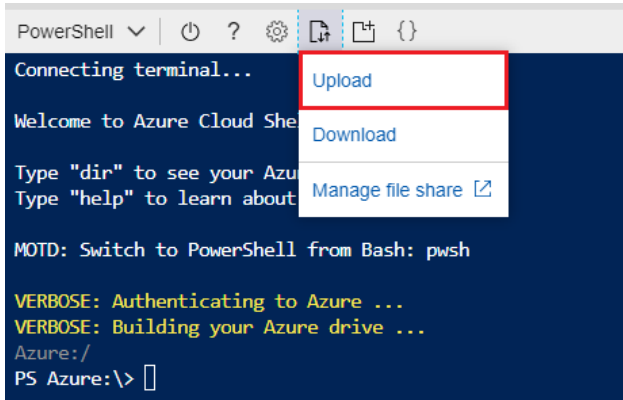
5. Download the automated tenant creation script and click **Next**.



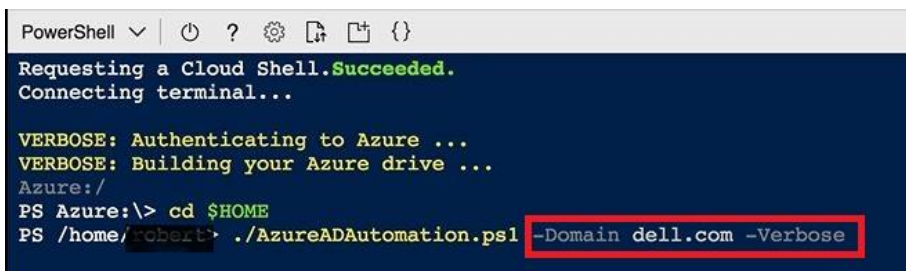
- 6. Login to the Microsoft Azure Portal at <https://azure.microsoft.com/en-us/account>.
- 7. Launch the Cloud Shell console and click **Powershell (Linux)**.



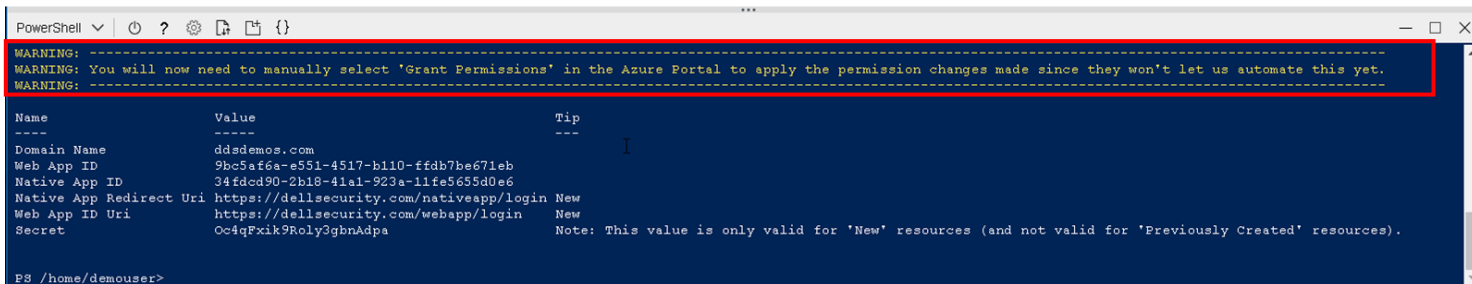
8. Upload the *AzureADAutomation.ps1* script.



9. Run the *AzureADAutomation.ps1* script and enter your Domain Name. (Ex: -Domain dell.com -Verbose).



10. Once the script returns with a warning message, grant permissions for the Dell Security Web App in the Azure portal.



11. To grant permissions for the Dell Security Web App and Dell Security Native App, the *Required Permissions* must be updated.

- a. Navigate to **Azure Active Directory > App registrations > Dell Security Web App > Settings > Required permissions**. Click **Grant Permissions**.

**Dell Security Web App** Registered app

1 Settings Manifest Delete

Display name: Dell Security Web App

Application ID: bdf89650-fd38-4223-ba00-09130070f7d8

Application type: Web app / API

Object ID: 22277627-9d04-4b5c-9fc7-f8dac9c85ff1

Managed application in local directory: Dell Security Web App

Home page: http://dellsecurity.com/webapp/login

2 Required permissions

3 Grant permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	2	1
Microsoft Graph	3	0
Windows Azure Service Management API	0	1

**Important:** The Dell Security Web App must have permissions granted first. If the native app is attempted to have permissions granted first, the following error will appear:

**Grant permissions**

Failed to grant permissions for application Dell Security Native App

by me 12 minutes ago

- b. Navigate to **Azure Active Directory > App registrations > Dell Security Native App > Settings > Required permissions**. Click **Grant Permissions**.

**Dell Security Native App** Registered app

1 Settings Manifest Delete

Display name: Dell Security Native App

Application ID: 47c28507-78e9-4827-81a9-4f53883ace59

Application type: Native

Object ID: 95f2d015-a744-4e13-b572-288993ea5e42

Managed application in local directory: Dell Security Native App

Home page: https://dds demos.com/DellSecurityWebApp

2 Required permissions

3 Grant permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	1
Dell Security Web App	0	1

12. Copy the Domain Name, Application IDs, Application Uri, and the Secret from the script output and enter them in the Identity Provider setup wizard.

```
PowerShell
WARNING: -----
WARNING: You will now need to manually select 'Grant Permissions' in the Azure Portal to apply the permission changes made since they won't let us automate this yet.
WARNING: -----
Name                Value                Tip
----                -
Domain Name         ddsdemos.com
Web App ID          9bc5af6a-e551-4517-b110-ffdb7be671eb
Native App ID       34fdcd90-2b18-41a1-923a-11fe5655d0e6
Native App Redirect Uri https://dellsecurity.com/nativeapp/login New
Web App ID Uri      https://dellsecurity.com/webapp/login New
Secret              Oc4qFxiK9Roly3gbnAdpa Note: This value is only valid for 'New' resources (and not valid for 'Previously Created' resources).

PS /home/demouser>
```

## Identity Provider

Enter your domain name and the application ID of the Dell Cloud Security application you registered in Azure AD. If you have not previously registered them, do that now at [Azure AD Login](#). See the [Quick Start Guide](#) for more information.

Domain Name:	<input type="text" value="Example: companydomain.onmicrosoft.com"/>
Web App ID:	<input type="text" value="11111111-1111-1111-1111-111111111111"/>
Native App ID:	<input type="text" value="11111111-1111-1111-1111-111111111111"/>
Native App Redirect Uri:	<input type="text" value="https://RedirectUri"/>
Web App ID Uri:	<input type="text" value="Example: http://companydomain/companyserver"/>
Secret:	<input type="text" value="11111111111111111111"/>

13. After validating your Azure AD credentials, enter the email address of the administrator for Dell Security Center.

Administrator Email:	<input type="text" value="exampleadmin@email.com"/>
Confirm Administrator Email:	<input type="text" value="exampleadmin@email.com"/>

14. Carefully review the summary to ensure all information is accurate. Dell recommends that you save this information for future reference.

Dell Security Center - Setup Wizard

- Introduction ✓
- Username ✓
- EULA ✓
- Auto Create Tenant ✓
- Identity Provider ✓
- Administrator ✓
- Summary**

**Summary**

Confirm the below information and then click Finish. It is recommended to save this information for future references.

Domain: [ddsp.com](#)

Administrator: [ddanagama@credaz.com](#)

Web App ID: [ddsp243h-2489-4c62-99cd-8267dbf4d816](#)

Native App ID: [518fa827-c03f-4a01-9c85-0e7e449217a0](#)

Native App Redirect Uri: [http://localhost](#)

Web App ID Uri: [https://ddsp.com/DdspServiceTest](#)

**i** Sign-On URL: <https://freshhastepantl.console.ddsp.com/webui/login>  
This URL will be activated after setup.

Quickstart Guide

Step 7 of 7


15. Click **Finish** to complete the setup wizard.


## Set up tenant when using a free Azure account

The basic implementation process includes these steps:

1. Retrieve the two emails sent to you from **tenantservices@dellsecuritycenter.com**. You will need these during setup.

Dell Data Security

Thank you for your purchase 



This solution is a cutting edge security protection product. It protects data, prevents data leakage, and secures endpoints from the centrally managed Dell Security Center.

**Start protecting your environment today!**

[Register your account](#)

**Verification Email:** `{{.VerificationEmail}}`


**Sign-on URL:** `{{.URL}}`

Learn more about the console

The Dell Security Center is responsible for the management of Dell's award winning data security products.

[Administrator guide and documentation](#)

[Quickstart Guide](#)


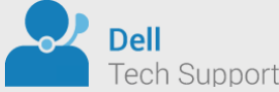


Support and references

[Support website and videos](#)

[Common questions](#)

[Support phone numbers](#)



**Dell Security Center**

Verification Code

Enter the following verification code into the corresponding field in the Dell Security Center Setup Wizard

`{{.VerificationCode}}`

2. Click **Register your account** from your welcome email to get started.



This solution is a cutting edge security protection product. It protects data, prevents data leakage, and secures endpoints from the centrally managed Dell Security Center.

**Start protecting your environment today!**

[Register your account](#)

**Verification Email:** `{{.VerificationEmail}}`

**Sign-on URL:** `{{.URL}}`



3. The setup wizard opens. Click **Next** and enter the verification email and code from these emails into the setup wizard.

Verification

From your 'Welcome' and 'Verification Code' emails, please enter your assigned credentials to continue setup.

Email:

Code:

4. Read and accept the Terms and Conditions of the license agreement.

I accept the terms and conditions of the license agreement.

5. Click **Next**.

Dell Security Center - Setup Wizard

- Introduction
- Username
- EULA
- Auto Create Tenant**
- Identity Provider
- Administrator
- Summary

### Azure Automated Tenant Creation

Click [here](#) to download the automated tenant creation script.

A paid Azure subscription is required to use the automated tenant creation script. Click [here](#) for Azure upgrade information.

Click Next to continue the set up wizard.

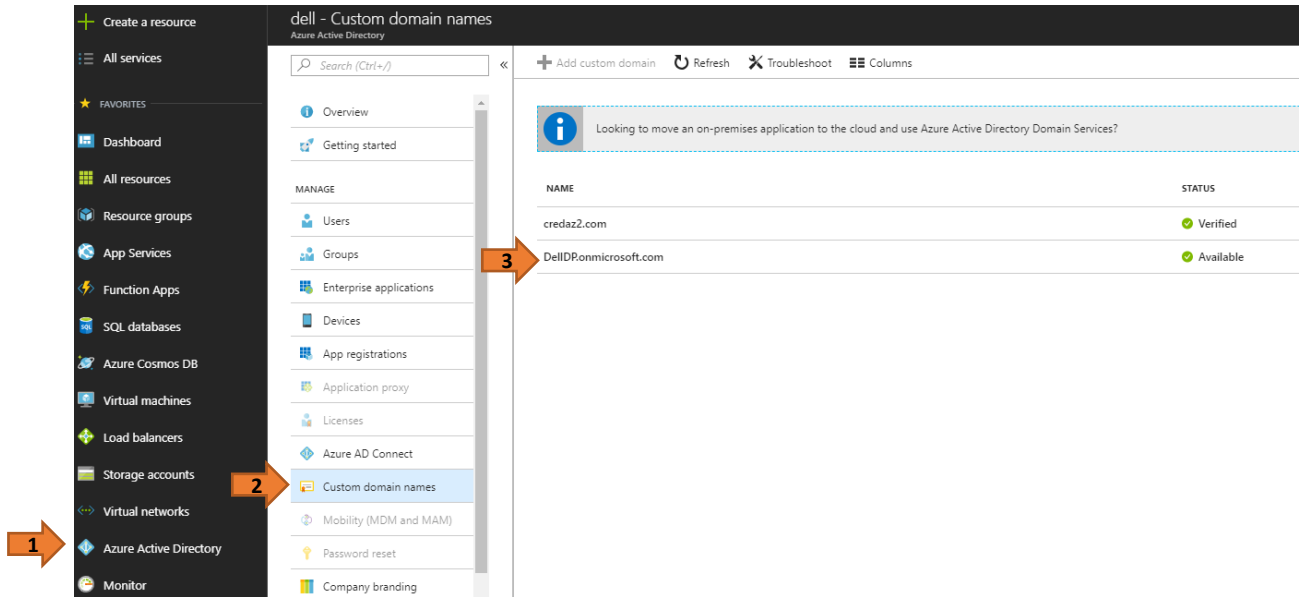
Quickstart Guide

Step 4 of 7

[Back](#) **1** [Next](#) [Cancel](#)

6. Information from Azure Active Directory must be entered into the setup wizard.
  - a. Login to the Microsoft Azure Portal at <https://azure.microsoft.com/en-us/account>
  - b. From Azure Active Directory, retrieve your Domain Name (for example, domain.onmicrosoft.com), and enter it in the setup wizard.

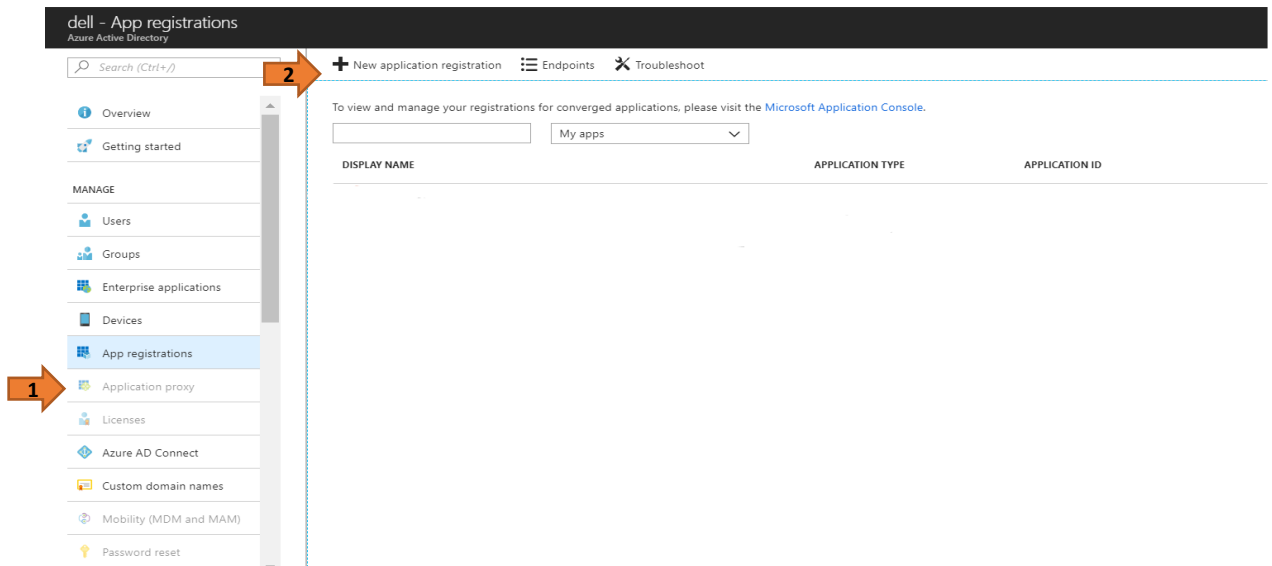
**Note:** The *Name* will be used for step 10 as the *Domain Name*.



- c. From Azure, navigate to **App registration > New application registration** to your two Application IDs.

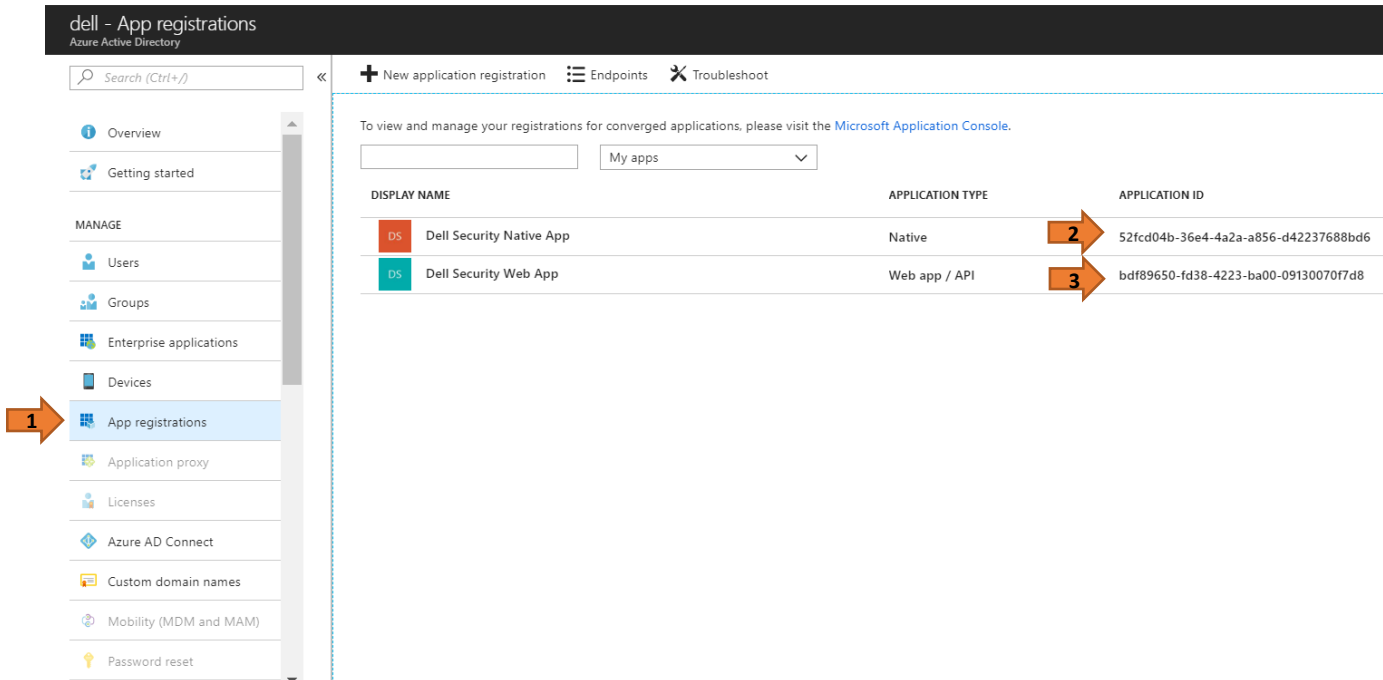
	<b>Application 1</b>	<b>Application 2</b>
Name	Dell Security Web App	Dell Security Native App
Application Type	Web app / API	Native
Sign-on URL	<a href="https://dellsecurity.com/webapp/login">https://dellsecurity.com/webapp/login</a>	<a href="https://dellsecurity.com/nativeapp/login">https://dellsecurity.com/nativeapp/login</a>

**Note:** These sites are not expected to resolve, and do not require being able to resolve.



**Note:** The *Sign-on URL* for the Native App is used for step 10 as the *Native App Redirect URI*.

6. Once registered, Azure provides Application IDs for both Apps.

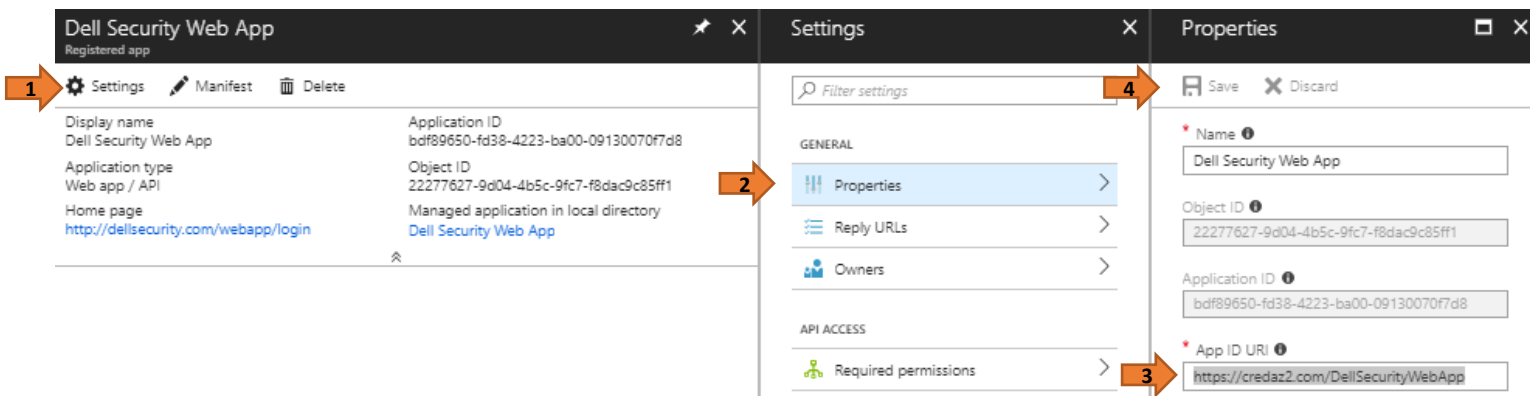


**Important:** Copy the *Application ID* for both Native App and Web App for step 10.

7. To register the Apps, the *App ID URI*, *Graph Keys*, *Required permissions*, and *groupMembershipClaims* must be updated.

- App ID URI:** Navigate to **Settings > Properties** to change the *App ID URI* to change current GUID to the home page for the Web App. Click **Save**.

(Ex: Change "<https://domain.com/6f6d082a-5b93...>" to "<https://domain.com/DellSecurityWebApp>")



**Important:** Copy the updated *App ID URI* to use for step 10 as the *Web App ID URI*.

- GraphKey (only for Web App):** Navigate to **Settings > Keys** to add a password.
  - In the *Description* field, enter **GraphKey**.
  - In the *Expires* field, select **Never Expires** from the menu.
  - The *Value* field is automatically generated. Click **Save** when finished.

**Important:** Upon save, ensure that the generated *Value* is copied for use in the setup wizard. Once this page is navigated away from, the auto-generated *Value* key is hidden.

**Note:** The *Value* is used for step 10 as the *Secret* code.

**Dell Security Web App** Registered app

Display name	Dell Security Web App	Application ID	bdf89650-fd38-4223-ba00-09130070f7d8
Application type	Web app / API	Object ID	22277627-9d04-4b5c-9fc7-f8dac9c85ff1
Home page	<a href="http://dellsecurity.com/webapp/login">http://dellsecurity.com/webapp/login</a>	Managed application in local directory	Dell Security Web App

**Settings**

- GENERAL
  - Properties
  - Reply URLs
  - Owners
- API ACCESS
  - Required permissions
  - Keys**
- TROUBLESHOOTING + SUPPORT
  - Troubleshoot
  - New support request

**Keys**

Save Discard Upload Public Key

DESCRIPTION	EXPIRES	VALUE
GraphyKey	12/31/2299	Hidden

Key description Duration Value will be disp

**Public Keys**

THUMBPRINT	START DATE
No results.	

**Keys**

Save Discard Upload Public Key

Copy the key value. You won't be able to retrieve after you leave this blade.

**Passwords**

DESCRIPTION	EXPIRES	VALUES
GraphyKey	12/31/2299	48K7w62PPmB7WFS6Oob6CviAH+7gPYknL92tABbnvCY=

Key description Duration Value will be displayed on save

**c. Required Permissions:** Navigate to **Settings > Required permissions > Add to Add API access.**

**Dell Security Web App** Registered app

Display name	Dell Security Web App	Application ID	bdf89650-fd38-4223-ba00-09130070f7d8
Application type	Web app / API	Object ID	22277627-9d04-4b5c-9fc7-f8dac9c85ff1
Home page	<a href="http://dellsecurity.com/webapp/login">http://dellsecurity.com/webapp/login</a>	Managed application in local directory	Dell Security Web App

**Settings**

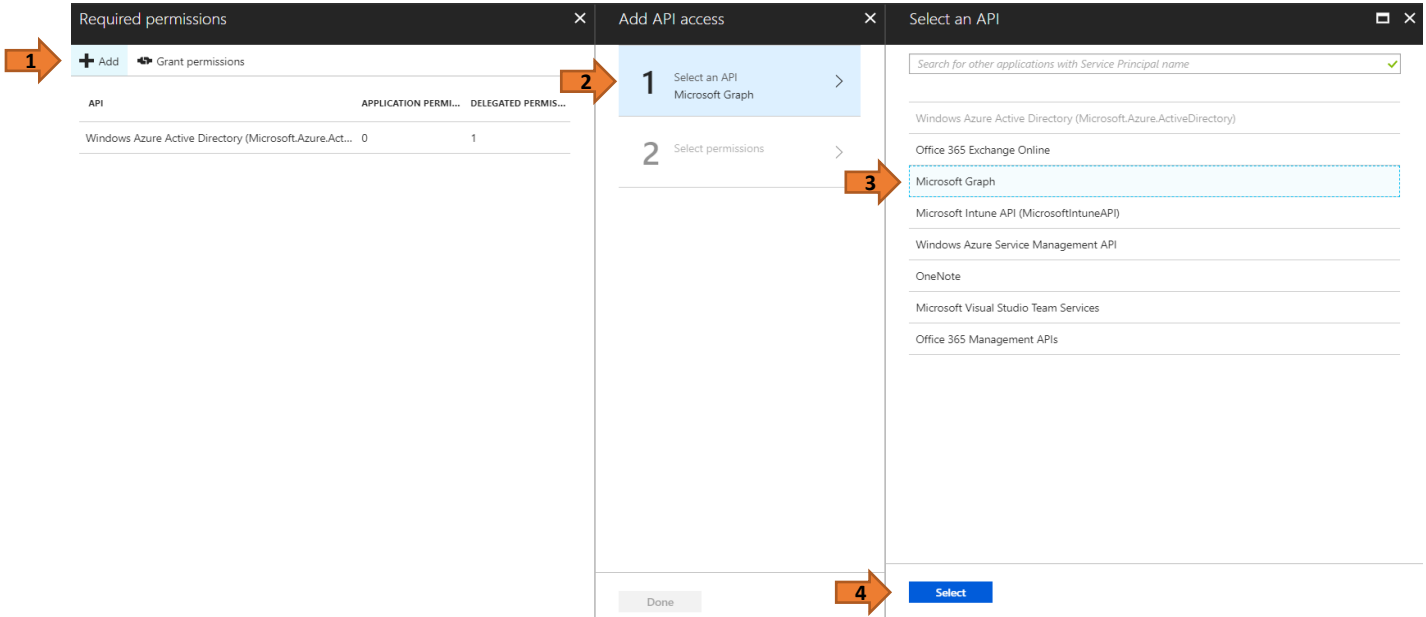
- GENERAL
  - Properties
  - Reply URLs
  - Owners
- API ACCESS
  - Required permissions
  - Keys
- TROUBLESHOOTING + SUPPORT
  - Troubleshoot
  - New support request

**Required permissions**

+ Add Grant permissions

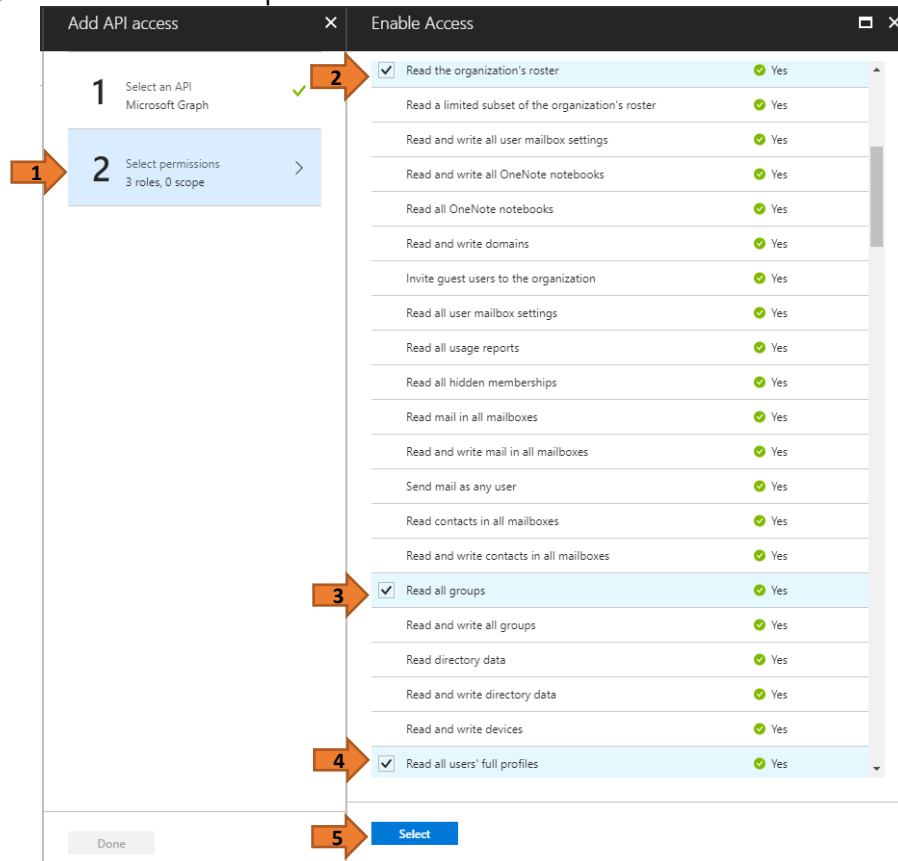
API	APPLICATION PERM...	DELEGATED PERMIS...
Windows Azure Active Directory (Microsoft.Azure.Act...	0	1

a. Click **Select an API > Microsoft Graph**. Click **Select**.



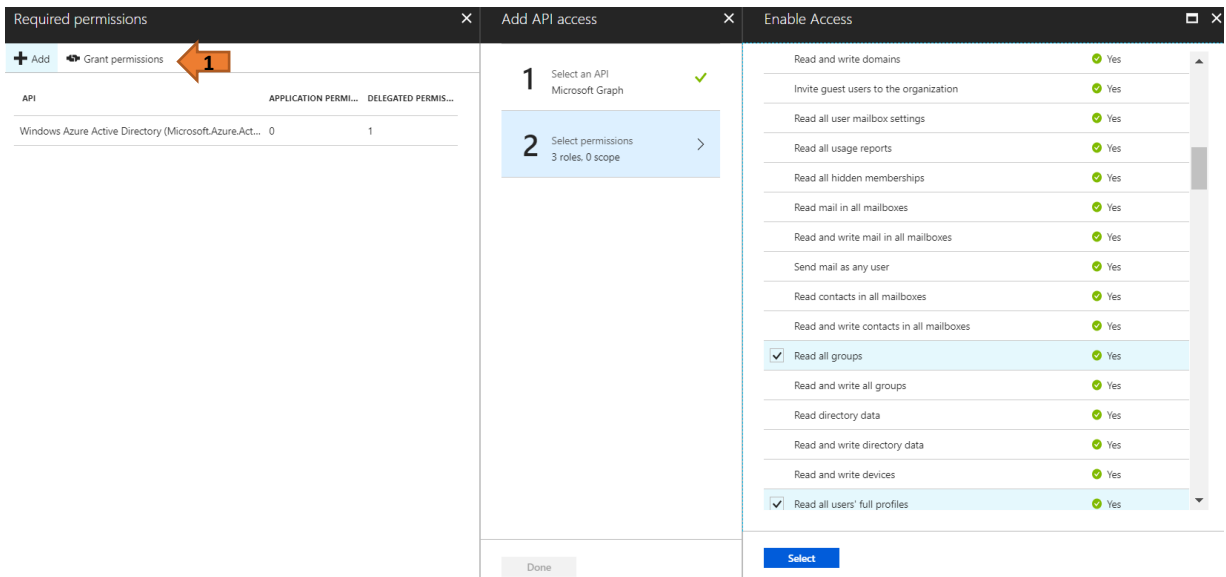
b. From **Select Permissions**, choose the following permissions:

1. Read the organization's roster
2. Read all groups
3. Read all users' full profiles



c. Click **Select**.

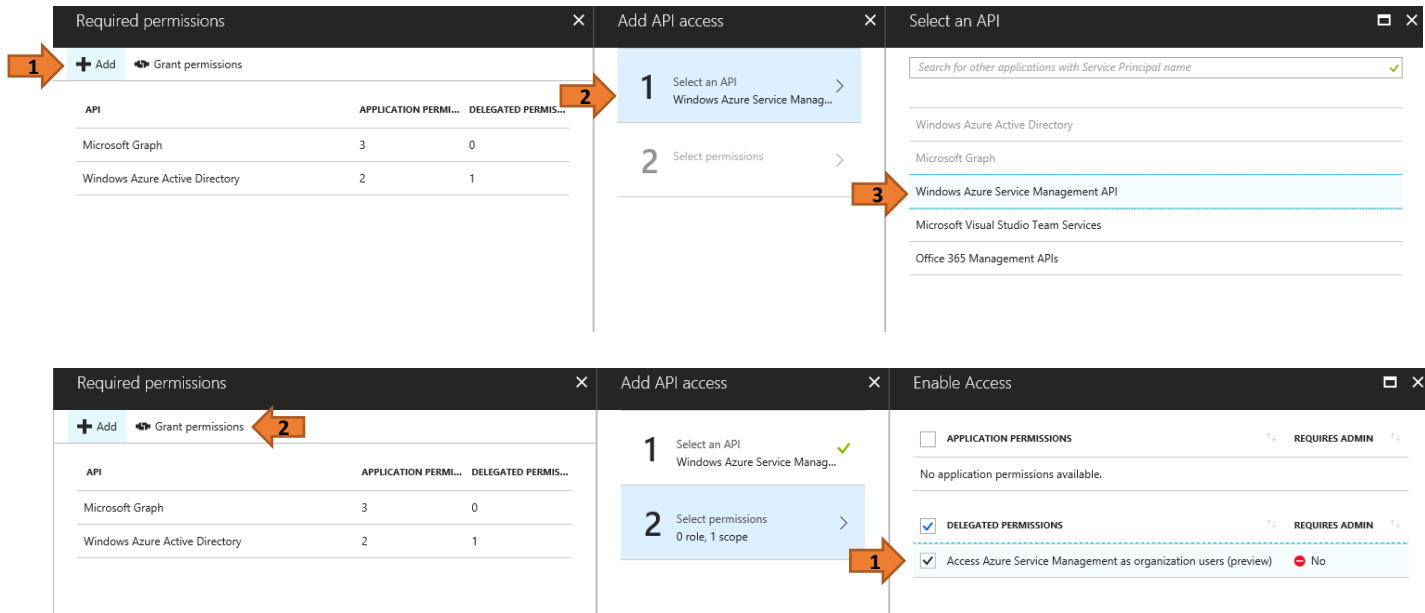
d. Click **Grant Permissions** to save.



Repeat steps for *Required permissions* for the following API with the same Web App:

e. **Windows Azure Service Management API**

1. Access Azure Service Management as organizations users (preview)



- f. **Windows Azure Active Directory**
1. Manage apps that this app creates or owns
  2. Read and write all applications

The screenshot shows the 'Required permissions' and 'Enable Access' windows in the Azure AD portal. In the 'Required permissions' window, the 'Windows Azure Active Directory' API is selected, and the 'Grant permissions' button is highlighted with a red arrow labeled '4'. In the 'Enable Access' window, the 'Manage apps that this app creates or owns' and 'Read and write all applications' permissions are checked, with red arrows labeled '2' and '3' pointing to them respectively. A warning message at the top of the 'Enable Access' window states: 'You are adding permission(s) that require an admin to consent, users will not be able to use the application until an admin grants permissions to the application.'

API	APPLICATION PERM...	DELEGATED PERMIS...
Microsoft Graph	3	0
Windows Azure Active Directory	0	1

APPLICATION PERMISSIONS	REQUIRES ADMIN
Read directory data	Yes
Read and write domains	Yes
Read and write directory data	Yes
Read and write devices	Yes
Read all hidden memberships	Yes
<input checked="" type="checkbox"/> Manage apps that this app creates or owns	Yes
<input checked="" type="checkbox"/> Read and write all applications	Yes
Read and write domains	Yes
DELEGATED PERMISSIONS	REQUIRES ADMIN
Access the directory as the signed-in user	No
Read directory data	Yes
Read and write directory data	Yes

- d. **groupMembershipClaims**: Navigate to Manifest.
- a. Change "groupMembershipClaims": null, to "groupMembershipClaims": "SecurityGroup",
  - b. Click **Save**.

**Important:** Make these changes for both Native App and Web App.

The screenshot shows the 'Edit manifest' window for the 'Dell Security Web App'. The 'Manifest' button is highlighted with a red arrow labeled '1'. The 'Save' button is highlighted with a red arrow labeled '3'. In the JSON manifest code, the 'groupMembershipClaims' property is updated from null to 'SecurityGroup', with a red arrow labeled '2' pointing to the new value.

```

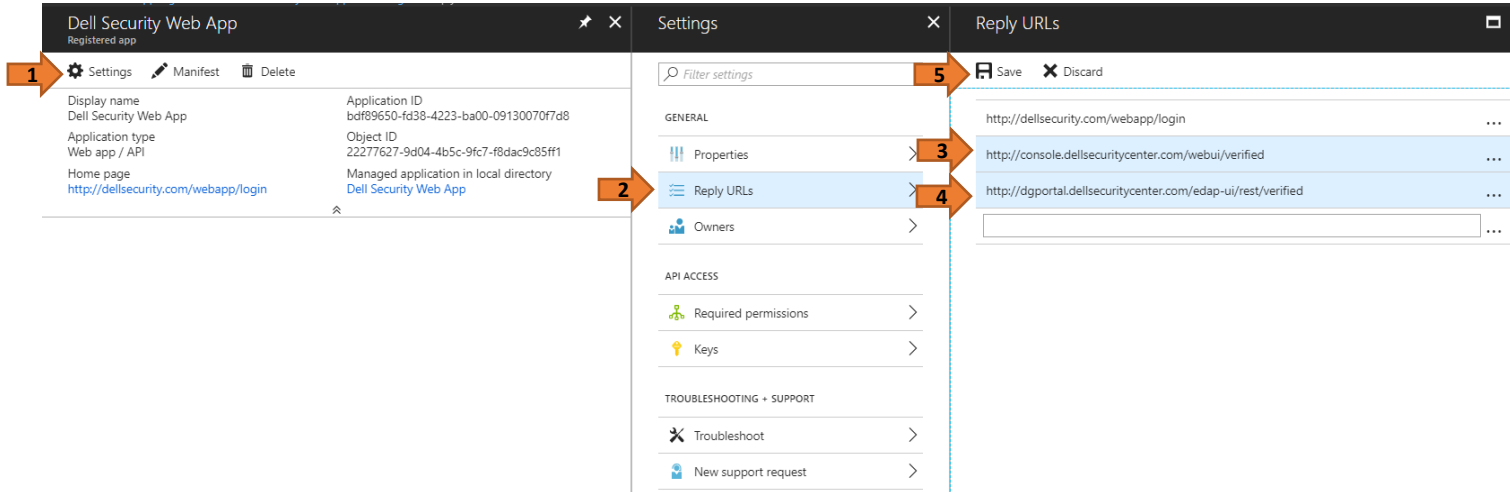
1 {
2   "appId": "8357266b-5534-4043-9d93-59f6f0b43c10",
3   "appRoles": [],
4   "availableToOtherTenants": false,
5   "displayName": "Dell Security Web App",
6   "errorUrl": null,
7   "groupMembershipClaims": "SecurityGroup",
8   "optionalClaims": null,
9   "acceptMappedClaims": null,
10  "homepage": "http://dellcloudsecurity.com/t56745/login",
11  "informationalUrls": {
12    "privacy": null,
13    "termsOfService": null
14  },
15  "identifierUris": [
16    "https://credaz2.com/c3573aa7-6254-4665-9792-f8089b53c5c8"
17  ],
18  "keyCredentials": [],
19  "knownClientApplications": [],
20  "logoutUrl": null,
21  "oauth2AllowImplicitFlow": false,
22  "oauth2AllowUrlPathMatching": false,
23  "oauth2Permissions": [

```

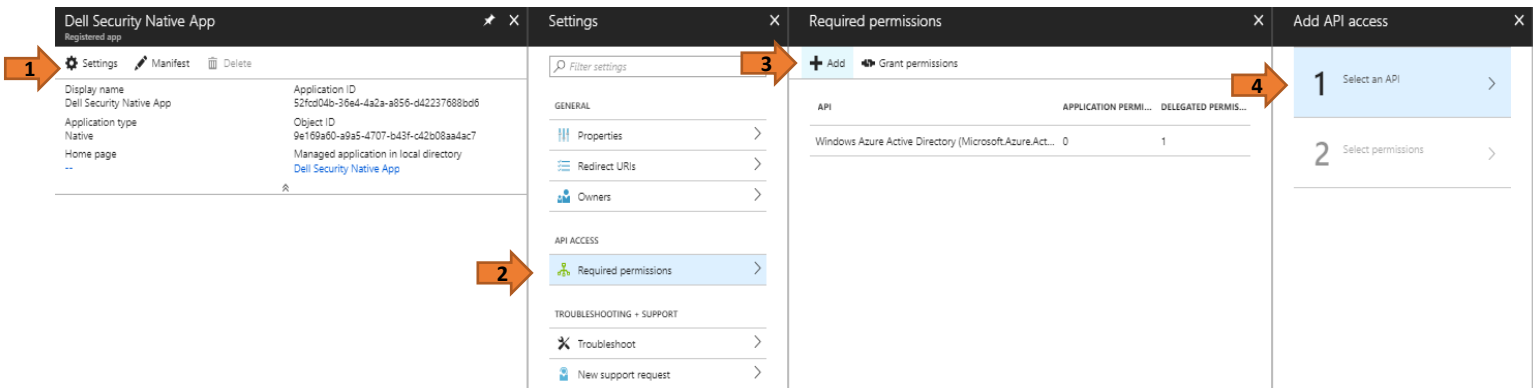
8. Navigate to **Settings > Reply URIs**. Add the Consoles and Data Guardian portals to the Reply URIs in the App Registration for the Web App. Click **Save**.

Console: <https://console.dellsecuritycenter.com/webui/verified>

DG Portal: <https://dgportal.dellsecuritycenter.com/edap-ui/rest/verified>

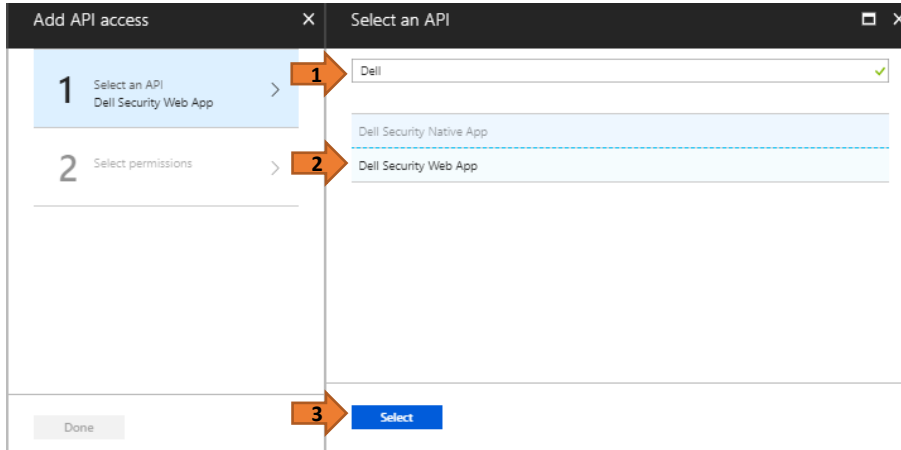


9. To link the Native App with the Web App, access to API for the Web App must be added under settings for the Native App.  
a. Navigate to **Settings > Required permissions > Add > Select an API**.

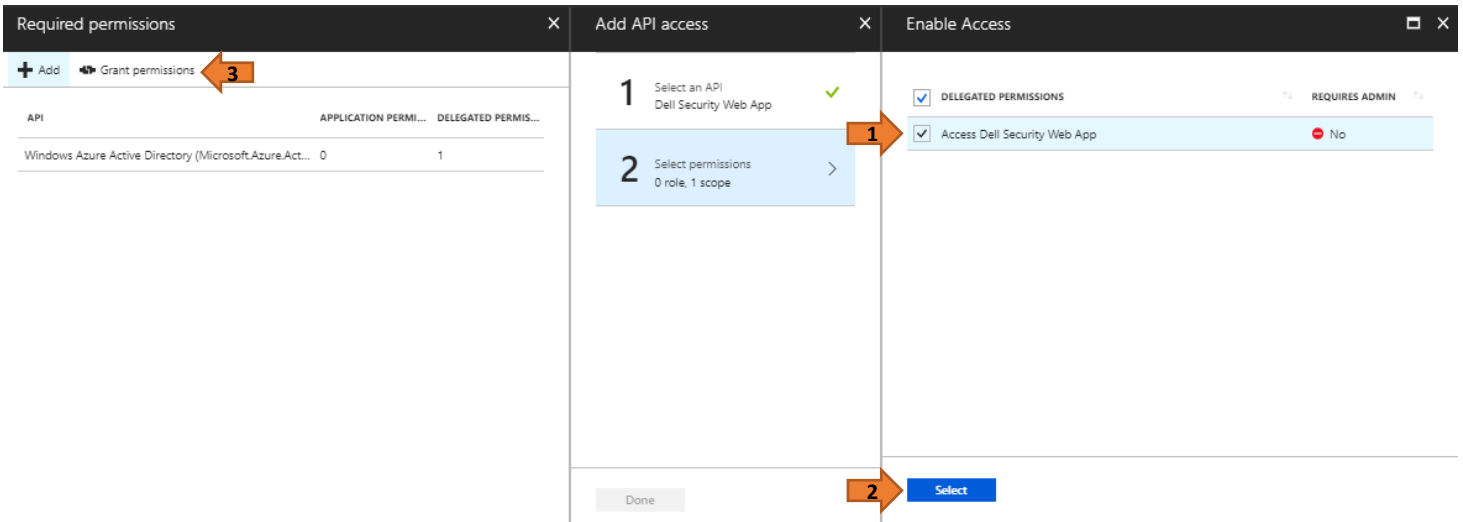




- b. When selecting an API, type in **Dell Security Web App**, press **Enter**, and click **Select**.









- c. Select the check box for *Access Dell Security Web App*. Click **Select**, and then click **Grant permissions**.



10. Enter the *Domain Name*, *Web App ID*, *Native App ID*, *Native App Redirect Uri*, *Web App Uri*, and the *Secret (GraphKey)* in the Identity Provider setup wizard.

## Identity Provider

Enter your domain name and the application ID of the Dell Cloud Security application you registered in Azure AD. If you have not previously registered them, do that now at [Azure AD Login](#). See the [Quick Start Guide](#) for more information.

Domain Name:	<input type="text" value="Example: companydomain.onmicrosoft.com"/>	
Web App ID:	<input type="text" value="11111111-1111-1111-1111-111111111111"/>	
Native App ID:	<input type="text" value="11111111-1111-1111-1111-111111111111"/>	
Native App Redirect Uri:	<input type="text" value="https://RedirectUri"/>	
Web App ID Uri:	<input type="text" value="Example: http://companydomain/companyserver"/>	
Secret:	<input type="text" value="11111111111111111111"/>	

11. After validating your Azure AD credentials, enter the email addresses of the administrators for Dell Security Center.

Administrator Email:	<input type="text" value="exampleadmin@email.com"/>
Confirm Administrator Email:	<input type="text" value="exampleadmin@email.com"/>

12. Carefully review the summary to ensure all information is accurate. Dell recommends that you save this information for future reference.

### Dell Security Center - Setup Wizard

- Introduction
- Username
- EULA
- Auto Create Tenant
- Identity Provider
- Administrator
- Summary**

#### Summary

Confirm the below information and then click Finish.  
It is recommended to save this information for future references.

Domain:

Administrator:

Web App ID:

Native App ID:

Native App Redirect Uri:

Web App ID Uri:

Sign-On URL: <https://credaz.com/credaztenant1.console.ddspcenter.com/webui/login>  
This URL will be activated after setup.

Step 7 of 7

[Quickstart Guide](#)

13. Click **Finish** to complete the setup wizard.