

# Microsoft Azure AD Configuration Guide

Use this guide along with the [Data Tab Configuration](#) guide to configure a Microsoft Azure AD-integrated SecureAuth® Identity Platform (formerly SecureAuth IdP) realm.

## Prerequisites

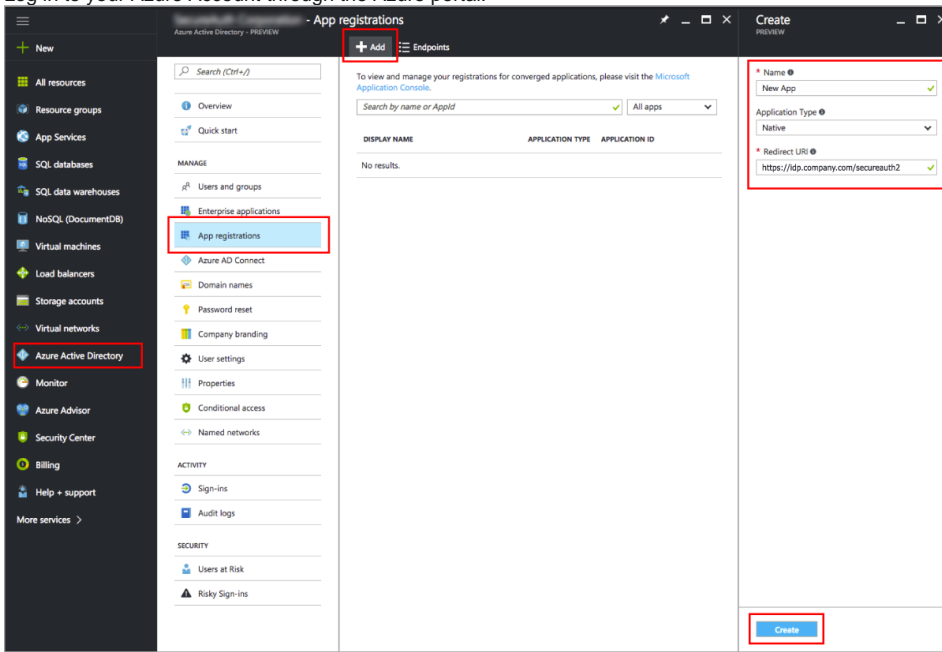
- Identity Platform version 19.07 and earlier
- Have Azure AD and access to the admin console
- Create or designate an existing administrator service account with read and optional write access for the Identity Platform
- Create a Native Client Application on Azure AD (see Azure AD configuration below)
- OPTIONAL: Have [Azure Powershell](#) installed to use Powershell commands to get user properties

## Contents

- [Azure AD configuration](#)
- [Identity Platform configuration](#)
- [OPTIONAL: PowerShell commands to get user properties](#)

## Azure AD configuration

1. Log in to your Azure Account through the Azure portal.

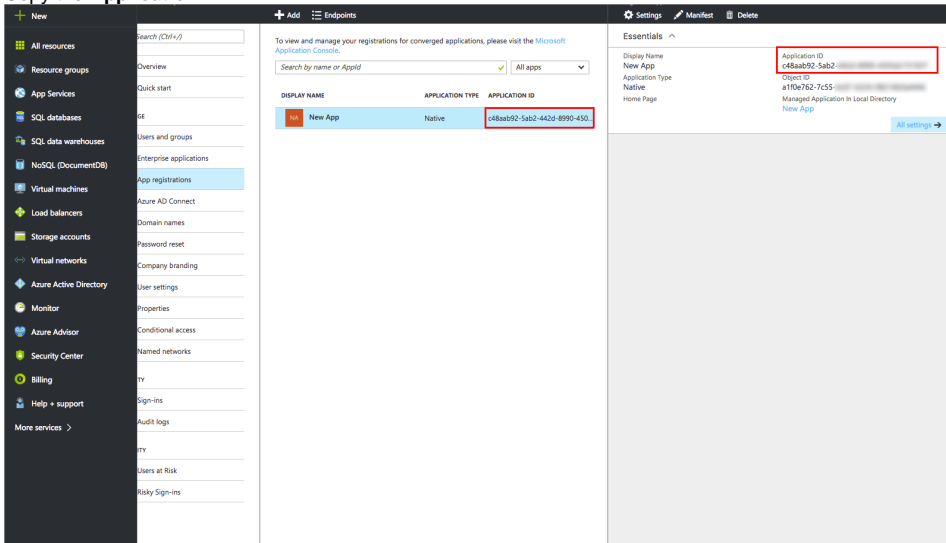


2. Select **Azure Active Directory**.
3. Select **App registrations**.
4. Click **Add**.
5. In the **Create** section, set the following:

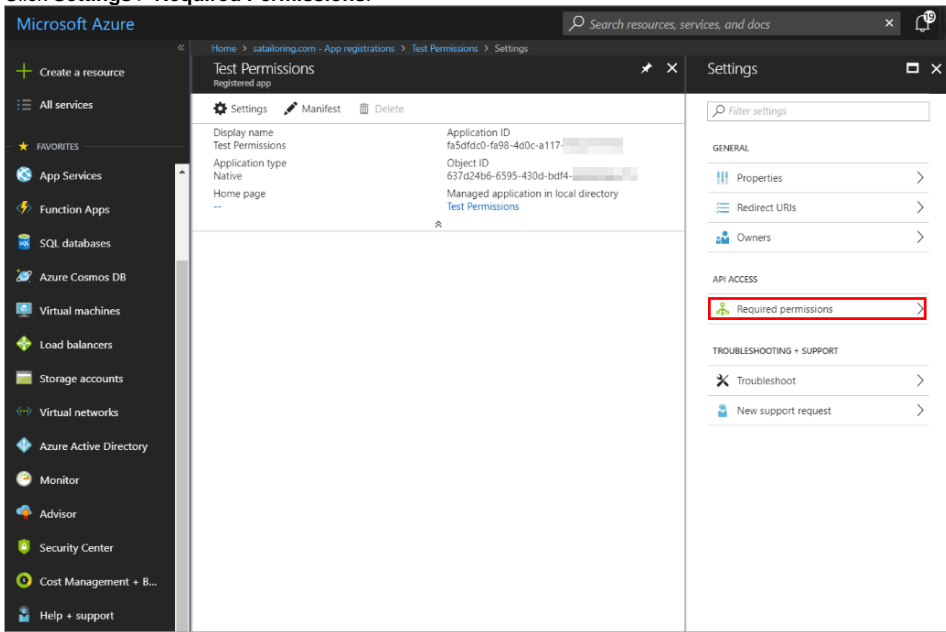
<b>Name</b>	Set a name for the new application.
<b>Application Type</b>	Set to <b>Native</b> .
<b>Redirect URI</b>	Set to the Fully Qualified Domain Name (FQDN) of the Identity Platform appliance, followed by the realm to which Azure AD is integrated.  For example, <code>https://idp.company.com/secureauth2</code>

6. Click **Create**.
7. From the **App registrations** panel, select the new application you just created.

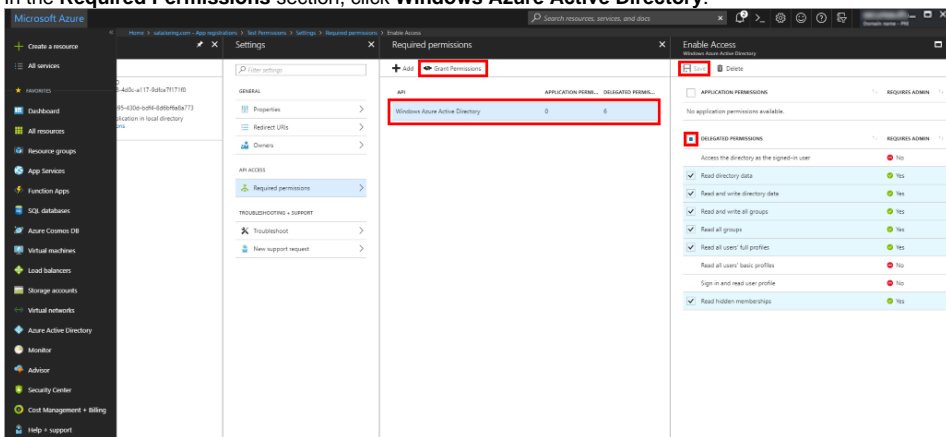
8. Copy the Application ID.



9. Click Settings > Required Permissions.



10. In the Required Permissions section, click Windows Azure Active Directory.



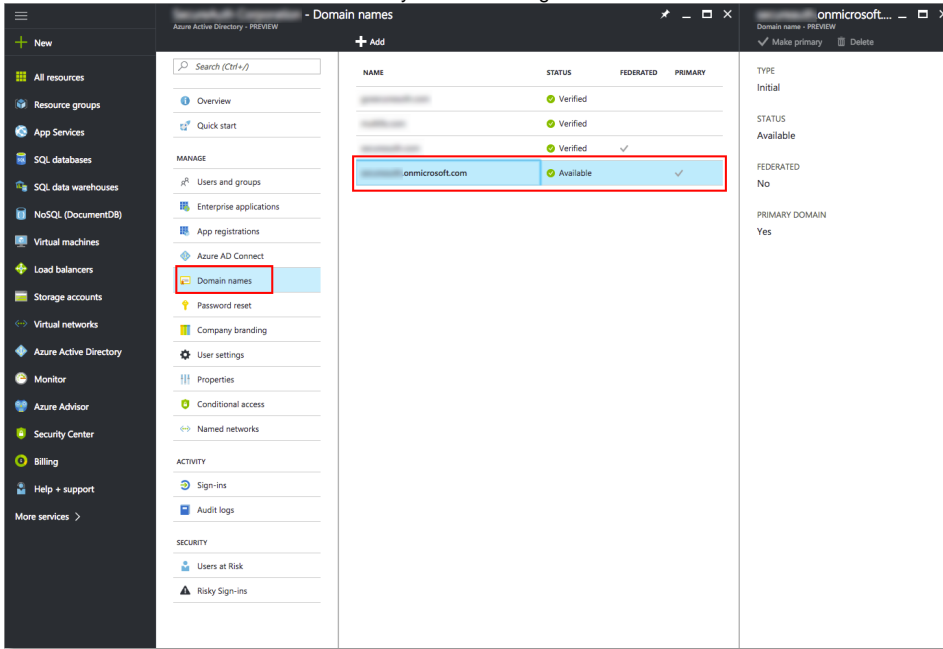
11. In the **Enable Access** section, delegate the permissions to be granted.

12. Click **Save**.

13. In the **Required permissions** section, click **Grant Permissions**.

14. From the Azure Active Directory menu, click **Domain names**.

- Copy the **.onmicrosoft.com** domain name. You will need this domain name in the Identity Platform configuration.



## Identity Platform configuration

- Select the **Data** tab.
- In the **Membership Connection Settings** section, set the following:

<b>Datatore Type</b>	Set to <b>Microsoft Azure AD</b> .
<b>Data Credentials</b>	Provide the username and password of the administrator service account.
<b>Azure Settings</b>	<p><b>Tenant Domain:</b> Set to the <b>.onmicrosoft</b> tenant domain that was copied from the Azure portal.</p> <p><b>Client ID:</b> Set to the Application ID that was copied from the Azure portal.</p>
<b>Group Permissions</b>	To restrict access to the realm (if you have such restrictions), provide a list of <b>Allowed Groups</b> and <b>Denied Groups</b> in a comma delimited format.

▼ Membership Connection Settings

---

**Datastore Type**

Type:

---

**Data Credentials**

Username:

Password:   Hidden

---

**Azure Settings**

Tenant Domain:

Client ID:

---

**Group Permissions**

Allowed Groups:

Denied Groups:

3. Click **Test Connection**.
4. **Save** your changes.
5. To complete the remaining configurations, see the [Data Tab Configuration](#) guide.

## OPTIONAL: PowerShell commands to get user properties

You can use PowerShell commands to get user properties.

1. Install Azure PowerShell: <https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-3.6.1>
2. To ensure that the PowerShell commands function properly, be sure the SetExecutionPolicy is Unrestricted.
3. Run the following commands.



### Command List

1. `$Cred = Get-Credential` [The value for this credential must be the onmicrosoft account associated with the Azure tenant].
2. `Connect-AzureAD -Credential $Cred`
3. `Get-AzureADUser`
4. `Get-AzureADUser -ObjectID "<Value of the Object ID"> | fl`

After the fourth command is executed, the AzureAD profile should resemble what is shown in the following screenshot.

```
PS C:\WINDOWS\system32> Get-AzureADUser -ObjectId "4ffa6d76-f5b9-4b94-829f-7818ad111111" | fl
ExtensionProperty      : ([odata.metadata, https://graph.windows.net/c1878e39-da5d-40c0-b593-67de.../odata/$metadata#directoryObjects/Micro
soft.DirectoryServices.User/@element), [odata.type, Microsoft.DirectoryServices.User], [createdDateTime,
9/29/2017 7:17:05 PM], [employeeId, ...]
DeletionTimestamp     :
ObjectId              : 4ffa6d76-f5b9-4b94-829f-7818ad111111
ObjectType            : User
AccountEnabled        : True
AgeGroup              :
AssignedLicenses      : {}
AssignedPlans         : {}
City                  :
CompanyName           :
ConsentProvidedForMinor :
Country               :
CreationType          :
Department            :
DirSyncEnabled        : True
DisplayName           : Admin Taylor
FacsimileTelephoneNumber :
GivenName             : Admin
IsCompromised         :
ImmutableId           : XR7QFH6PHEKS7Za...
JobTitle              :
LastDirSyncTime       : 7/24/2018 10:28:56 PM
LegalAgeGroupClassification :
Mail                  : admin@secureauth.com
MailNickName          : admin-adm
Mobile                :
OnPremisesSecurityIdentifier : S-1-5-21-2317069134-3415035726-...
OtherMails            : {}
PasswordPolicies      : DisablePasswordExpiration
PasswordProfile       :
PhysicalDeliveryOfficeName :
PostalCode            :
PreferredLanguage     :
ProvisionedPlans      : {}
ProvisioningErrors    : {}
ProxyAddresses        : (smtp:admin-adm@secureauth.com,microsoft.com)
RefreshTokensValidFromDateTime : 10/19/2017 8:00:06 PM
ShowInAddressList     :
SignInNames           : {}
SipProxyAddress       :
State                 :
StreetAddress         :
Surname               : Taylor
TelephoneNumber       : 8589001111
UsageLocation         :
UserPrincipalName     : admin-adm@secureauth.com,microsoft.com
UserType              : Member
```

4. Verify that User Properties on the AzureAD Profile match with the Profile Fields configured on the **Data** tab in the Identity Platform.

▼ Profile Fields				
Property	Source	Field	Data Format	Writable
Groups	<a href="#">Default Provider</a>	<input type="text"/>		<input type="checkbox"/>
First Name	<a href="#">Default Provider</a>	<input type="text" value="givenName"/>		<input type="checkbox"/>
Last Name	<a href="#">Default Provider</a>	<input type="text" value="surname"/>		<input type="checkbox"/>
Phone 1	<a href="#">Default Provider</a>	<input type="text" value="telephoneNumber"/>		<input type="checkbox"/>
Phone 2	<a href="#">Default Provider</a>	<input type="text" value="mobile"/>		<input type="checkbox"/>
Phone 3	<a href="#">Default Provider</a>	<input type="text" value="otherMobile"/>		<input type="checkbox"/>
Phone 4	<a href="#">Default Provider</a>	<input type="text"/>		<input type="checkbox"/>
Email 1	<a href="#">Default Provider</a>	<input type="text" value="mail"/>		<input type="checkbox"/>
Email 2	<a href="#">Default Provider</a>	<input type="text"/>		<input type="checkbox"/>