

RSA SECURID[®] ACCESS

Implementation Guide

Microsoft Azure Active Directory

Gina Salvazo, RSA Partner Engineering
Last Modified: October 23, 2017

Solution Summary

RSA Cloud Authentication Service provides additional security to Microsoft Azure Active Directory. Microsoft Azure Active Directory performs the primary authentication while RSA's provides the security of multi-factor authentication.

RSA SecurID Access Features	
Microsoft Azure Active Directory	
On Premise Methods	
RSA SecurID	<input checked="" type="checkbox"/>
On Demand Authentication	<input checked="" type="checkbox"/>
Risk-Based Authentication (AM)	<input type="checkbox"/>
Cloud Authentication Service Methods	
Authenticate App	<input checked="" type="checkbox"/>
FIDO Token	<input checked="" type="checkbox"/>
SSO	
SAML SSO	<input type="checkbox"/>
HFED SSO	<input type="checkbox"/>
OIDC SSO	<input checked="" type="checkbox"/>

Identity Assurance	
Collect Device Assurance and User Behavior	<input checked="" type="checkbox"/>

Configuration Summary

All of the supported use cases of RSA SecurID Access with Microsoft Azure Active Directory require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Microsoft Azure Active Directory can be integrated with RSA Cloud Authentication Service in the following way:

OIDC via RSA Cloud Service

[Cloud Authentication Service – Cloud Configuration Microsoft Azure Active Directory Configuration](#)

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

OIDC via RSA Cloud Service

To configure RSA Cloud Service, you must add Azure AD as a Relying Party in the RSA SecurID Access Console. During configuration of the RSA Cloud Service you will need some information from the Azure AD.

Before You Begin

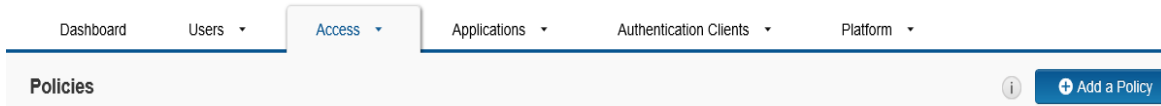
RSA SecurID Access requirements:

- Register a user with an authenticator.
- Create an Access Policy.

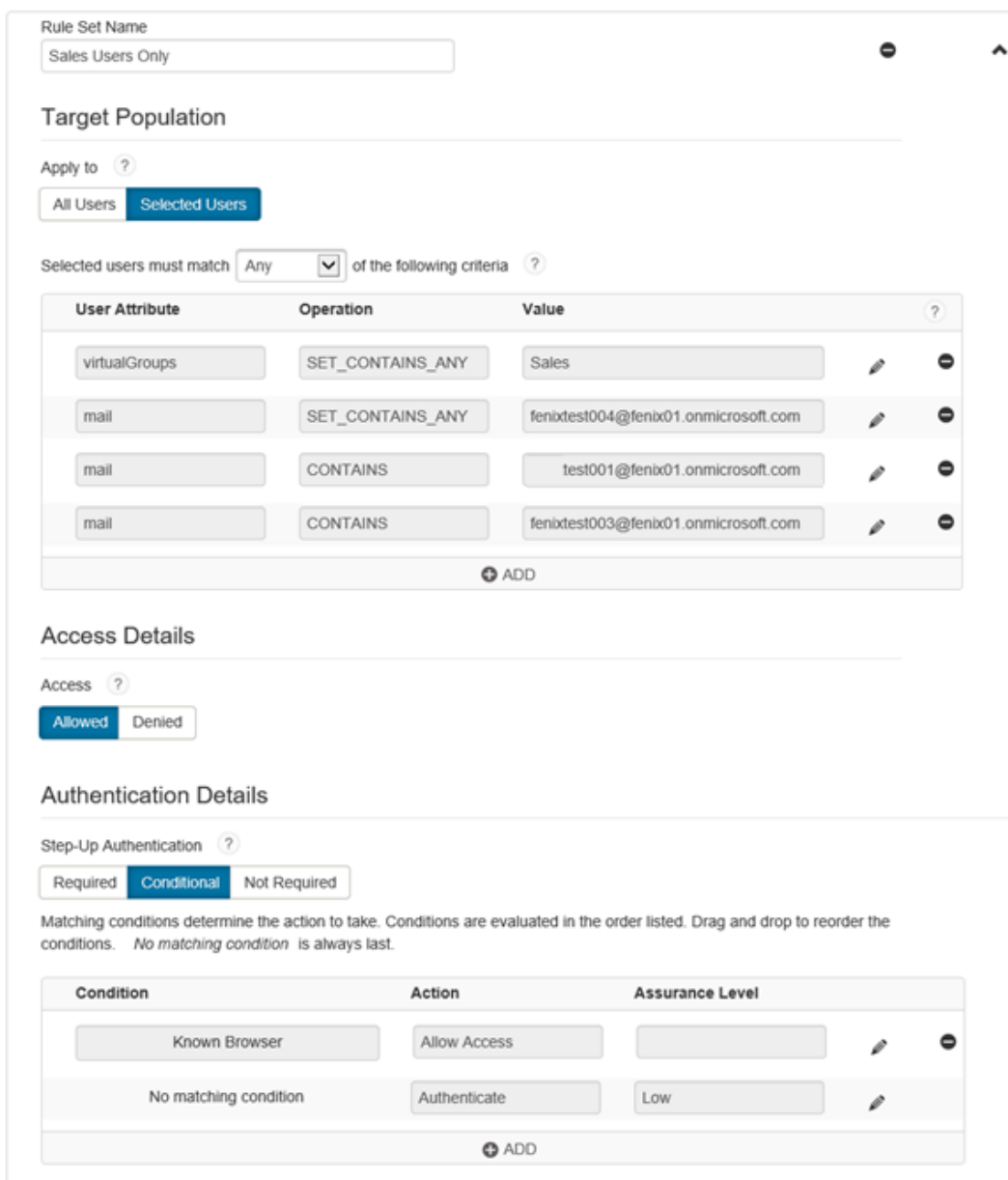
Microsoft Azure Active Directory

Create RSA Access Policies

1. Log in to the RSA SecurID Access Administration Console.
2. Navigate to **Access > Policies**.



3. Click **+Add a Policy**.
4. Below is an example of a policy which allows specific users access to the application and denies all others.



Rule Set Name: Sales Users Only

Target Population: Apply to **Selected Users**

Selected users must match **Any** of the following criteria

User Attribute	Operation	Value	
virtualGroups	SET_CONTAINS_ANY	Sales	
mail	SET_CONTAINS_ANY	fenixtest004@fenix01.onmicrosoft.com	
mail	CONTAINS	test001@fenix01.onmicrosoft.com	
mail	CONTAINS	fenixtest003@fenix01.onmicrosoft.com	

Access Details: **Allowed**

Authentication Details: **Conditional**

Matching conditions determine the action to take. Conditions are evaluated in the order listed. Drag and drop to reorder the conditions. *No matching condition* is always last.

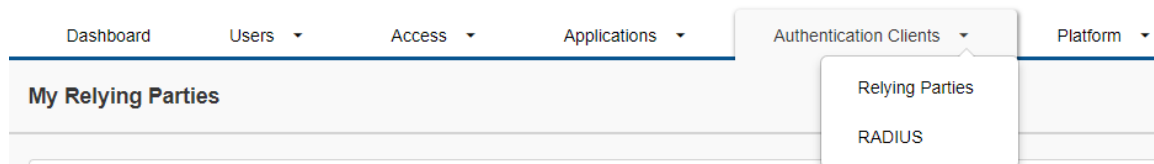
Condition	Action	Assurance Level	
Known Browser	Allow Access		
No matching condition	Authenticate	Low	

Microsoft Azure Active Directory

Add Azure Active Directory as a Relying Party in RSA SecurID Access

Procedure

1. Log in to the RSA SecurID Access Administration Console.
2. Navigate to **Authentication Clients > Relying Parties** menu item at the top of the page.

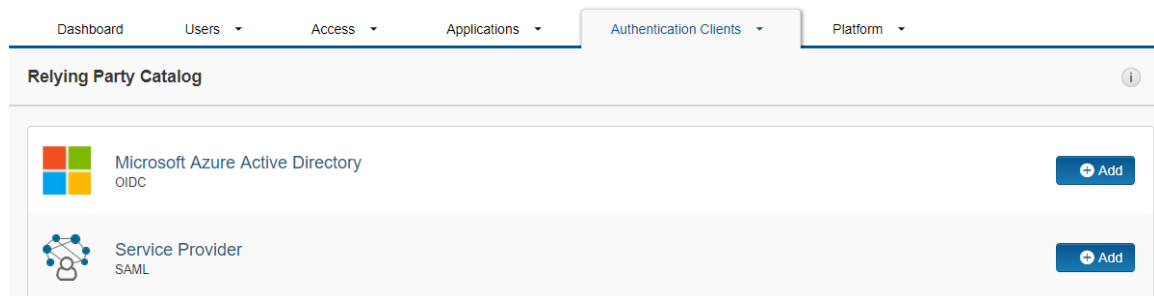


3. Click the **Add a Relying** button on the **My Relying Parties** page.



4. From the Relying Party Catalog select the **+Add** button for Azure Active Directory.

Note: If you do not see the Azure Active Directory option please contact RSA Support.



5. Enter a name for the Azure Active Directory in the **Name** field on the **Basic Information** page.
6. Click the **Next Step** button.

Microsoft Azure Active Directory

- On the Authentication page, use the pulldown list and select the Access Policy you previously configured.

The screenshot shows the 'Authentication' configuration page in the Azure Active Directory portal. On the left, a navigation pane lists three steps: '1. Basic Information', '2. Authentication', and '3. Connection Profile'. The 'Authentication' step is currently selected. The main content area is titled 'Authentication' and contains the following text: 'Azure Active Directory manages primary authentication, and the Cloud Authentication Service manages additional authentication.' Below this text is a dropdown menu labeled 'Access Policy for Additional Authentication' with a question mark icon, currently showing 'New Policy'. At the bottom right of the page, there are two buttons: 'Cancel' and 'Next Step' with a right-pointing arrow.

- Select **Next Step**.
- The **Authorization Server Issuer URL** is a generated value which will be needed later to configure the Azure AD.
- In the Relying Party Issuer URL, replace the **company_id** with your Azure AD Directory ID. To locate your Directory ID, login to the Azure portal and navigate to **Azure Active Directory > Manage > Properties** and copy the **Directory ID**. In this example the Relying Party Issuer URL would be <https://sts.windows.net/00ac1892-a9e5-4bd1-949a-9eb02db2449c>.
- Enter the **Client ID**. This can be any value but must match the **ClientID** configured in the Azure AD.
- Verify the **Azure Active Directory Application ID** is **bfda057e-d676-4c42-9742-6eea99bbdc1**.

The screenshot shows the 'Connection Profile' configuration page in the Azure Active Directory portal. On the left, the navigation pane shows '3. Connection Profile' as the selected step. The main content area is titled 'Connection Profile' and contains the following text: 'Configure the relationship between the Cloud Authentication Service as the provider and Azure Active Directory as the relying party.' Below this text are four input fields, each with a question mark icon: 'Authorization Server Issuer URL' (value: https://voyager-fenix-02.auth-dev2.securid.com/oidc-fe), 'Relying Party Issuer URL' (value: https://sts.windows.net/00ac1892-a9e5-4bd1-949a-9eb02db2449c), 'Client ID' (value: custom-control-id), and 'Azure Active Directory Application ID' (value: bfda057e-d676-4c42-9742-6eea99bbdc1). At the bottom right, there are two buttons: 'Cancel' and 'Save and Finish'.

- Click **Save and Finish**.
- Click **Publish Changes**.

Publish Changes Status: Changes Pending

Partner Product Configuration

This section provides instructions for configuring the Microsoft Azure Active Directory with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Microsoft Azure Active Directory components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Before You Begin

- Install Microsoft Azure AD Connect and synchronize your on-premise AD. This is the same on-premise AD configured in RSA SecurID Access as an Identity source.
- Configure at least one Azure AD cloud application.

For additional information on Microsoft Azure Active Directory and AAD Connect refer to

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect>.

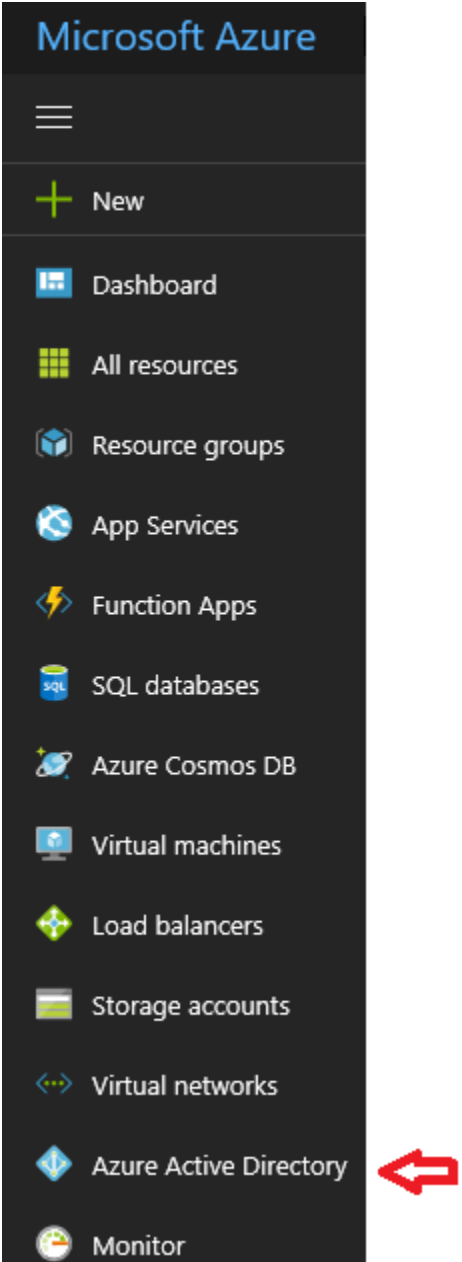
For an example on how to configure Azure AD application refer to the Microsoft Salesforce tutorial.

<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-salesforce-tutorial>

Microsoft Azure Active Directory

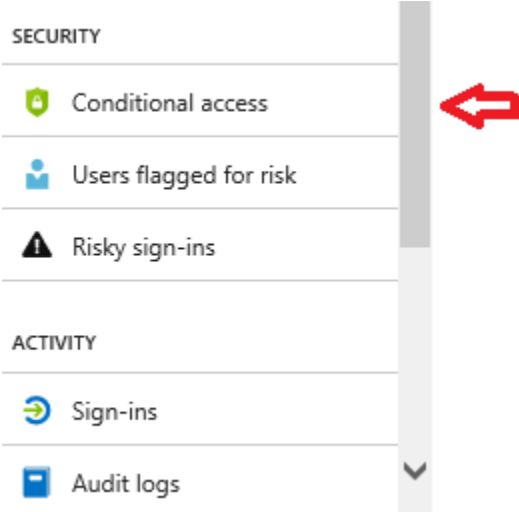
Microsoft Azure Active Directory Configuration

1. Login to Azure Portal <https://portal.azure.com>.
2. Navigate to **Azure Active Directory**.

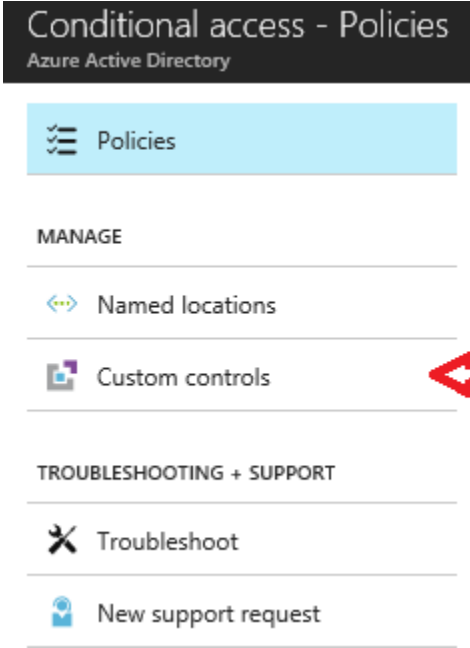


Microsoft Azure Active Directory

3. The Azure Active Directory menu list will open. Scroll down to **SECURITY > Conditional access**.

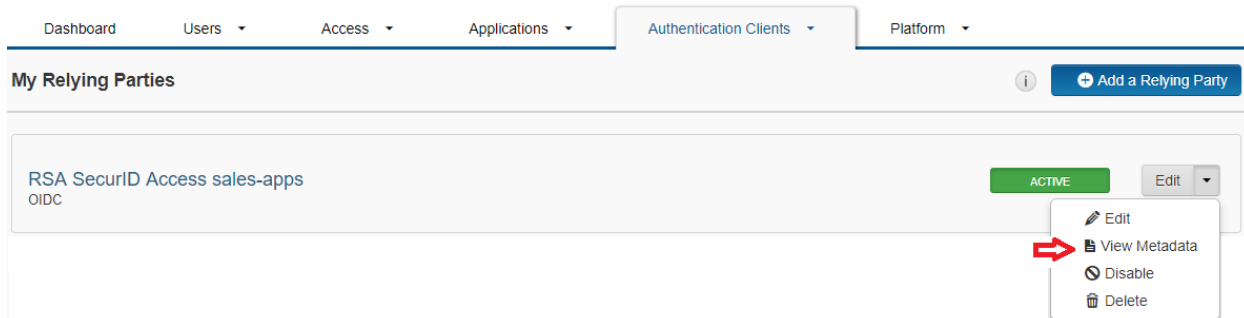


4. On the Conditional access page, click on **Custom controls**.



Microsoft Azure Active Directory

5. Click **+ New custom control**.
6. A window with a JSON script will open. Replace the default script with the metadata file copied from your RSA SecurID Access Console. Navigate to **Authentication Clients > Relying Parties**. Select the **Edit** pulldown and click **View Metadata**. Copy and paste script into JSON window.



- a. **Name:** must be unique between all Custom controls.
- b. **AppID:** enter `bfda057e-d676-4c42-9742-6eea99bbdec1`.
- c. **ClientID:** enter the **Client ID** value from step 11 on page 7.
- d. **DiscoveryUrl:** enter the **Authorization Server Issuer URL** appended by `/.well-known/openid-configuration`.
- e. **Id:** need to be unique between all Custom controls.
- f. **Name:** same as step 6a.
- g. **Type:** enter `mfa-policy`.
- h. **Value:** needs to have a single space between quotes.

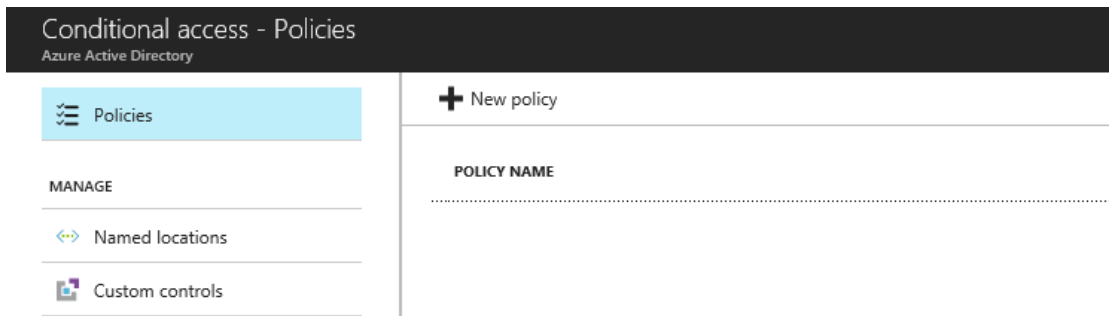
Enter the JSON for customized controls given by your claim providers.

```
{
  "Name": "RSA SecurID Access sales-apps",
  "AppId": "bfda057e-d676-4c42-9742-6eea99bbdec1",
  "ClientId": "custom-control-id",
  "DiscoveryUrl": "https://voyager-fenix-02.auth-dev2.sercurid.com/oidc-fe/.well-known/openid-configuration",
  "Controls": [{
    "Id": "RSA SecurID Access sales-apps",
    "Name": "RSA SecurID Access sales-apps",
    "ClaimsRequested": [{
      "Type": "mfa-policy",
      "Value": "",
      "Values": null
    }
  ]
}]
}
```

7. Click **Create**.

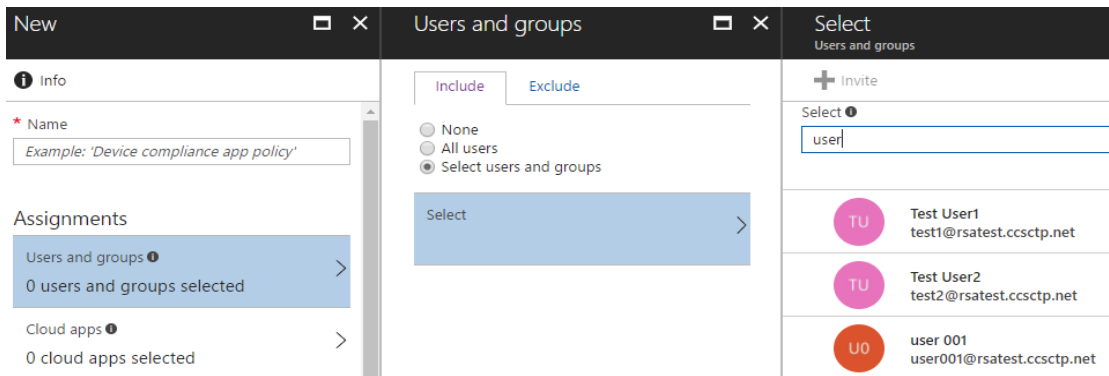
Microsoft Azure Active Directory

8. From the Conditional access menu, select **Policies**. Click **+ New policy**.

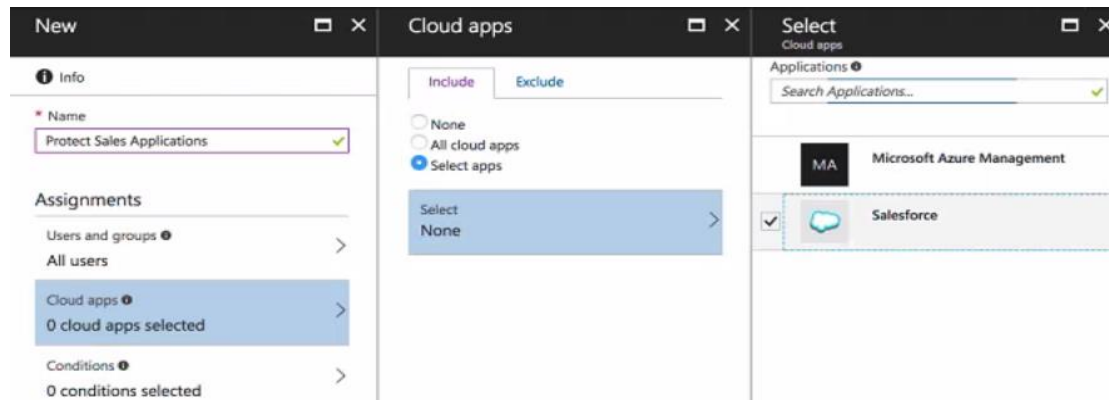


9. Enter a name for the new policy for example *Protect Sales Applications*.
10. Under Assignments, select **Users and groups**.
11. Select the users which require additional authentication.
12. In the Users and groups window, click **Done**.

Note: To avoid locking out the administrator account select the Exclude tab and exclude the administrator from this policy.



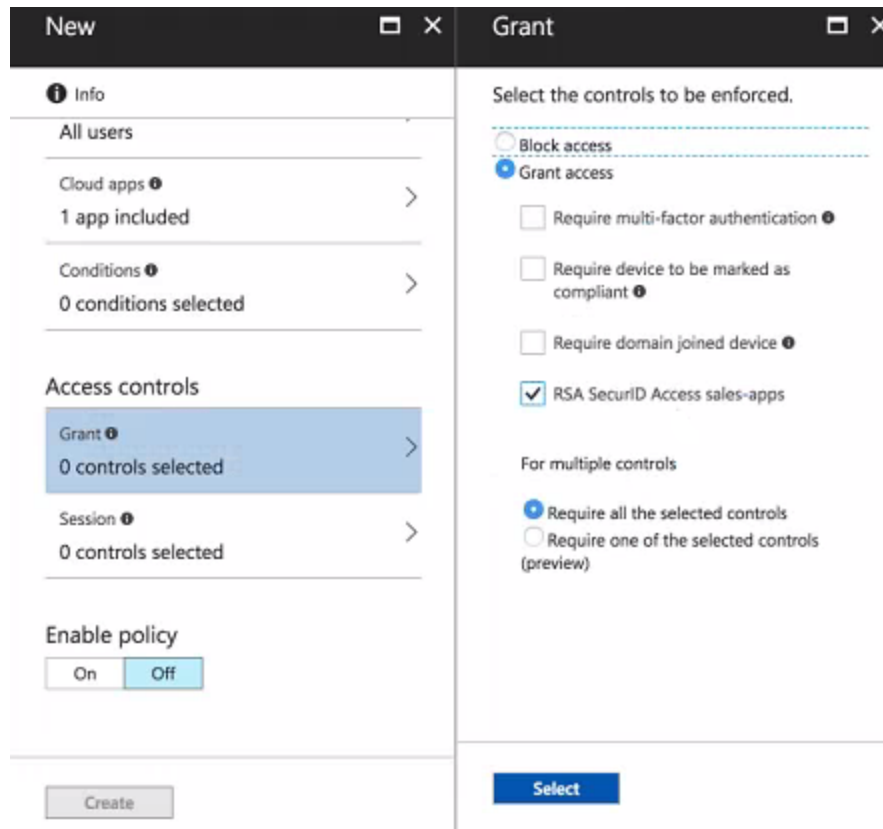
13. Under Assignments, select **Cloud apps**.
14. In the Cloud apps > Include window, select which apps this policy will apply to.



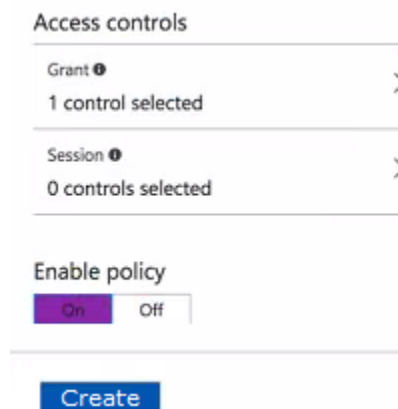
15. In the Cloud apps window, click **Done**.

Microsoft Azure Active Directory

16. Select **Access controls**.
17. Click **Grant**.
18. In the Grant window, select **Grant access** and select the Custom control you created in step 6 page 11.



19. Click **Select**.
20. Select **On** to enable the policy.

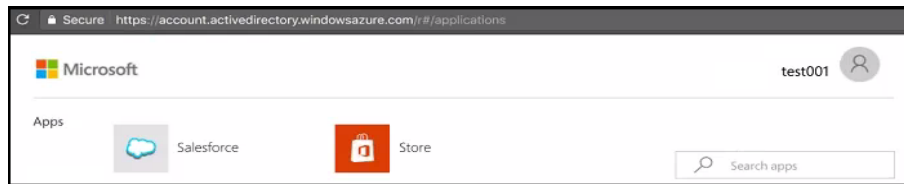


21. Click **Create**.

Microsoft Azure Active Directory

User Experience

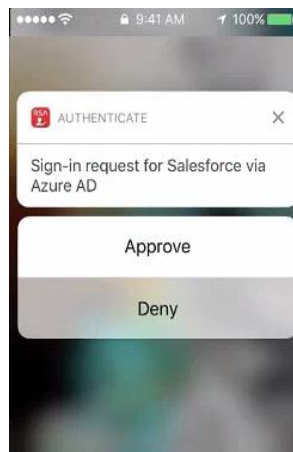
1. Login to the Azure portal.



2. Select a protect application.
3. This will redirect you to RSA for additional authentication.



4. Receive your Approve request on your RSA Authenticator.



5. Click **Approve**.
6. Your successfully logged in to your protect application home page.

