Microsoft Azure AD (Entra ID): Revoke Active Azure Sessions and Disable Users in Azure

Overview

The new response action, available in InsightIDR and InsightConnect, allows SOC analysts to revoke active sessions and disable users in Azure Active Directory (Entra ID). This action utilizes the Azure AD Admin plugin in InsightConnect and integrates with Microsoft Graph API to perform the necessary operations.

How It Works

The response action comprises three main steps:

1. Lookup User: Checks if the user exists in Azure AD.
2. Revoke Active Azure Sessions: Revokes any active sessions for the user.
3. Disable Azure User: Disables the user's account in Azure AD.

Permissions Required

To perform these actions, the following application-only permissions are required in Azure AD:

- User.EnableDisableAccount.All: Enable and disable user accounts.
- User.Read.All: Read all users' full profiles.
- User.RevokeSessions.All: Revoke all sign-in sessions for a user.

Configuring App Registration in Azure

To enable these permissions and configure the app registration in Azure, follow these steps:

Register an Application in Azure AD

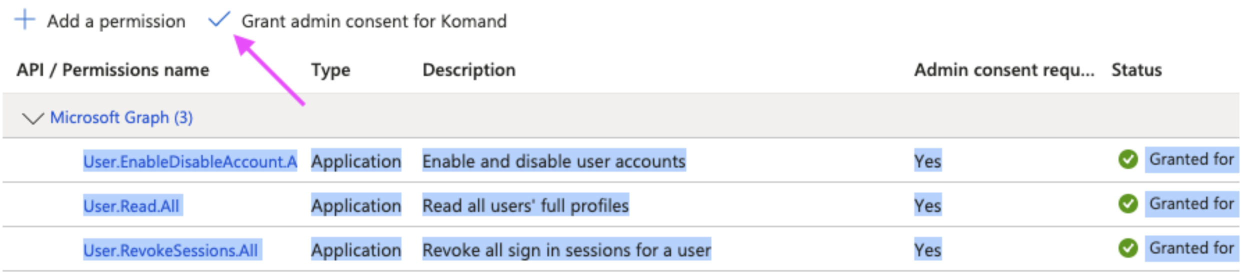
1. Sign in to the Azure portal.
2. In the side navigation of the Azure portal, click Entra ID, then select App Registrations in the secondary navigation menu.
3. Click New Registration.
4. Complete the form with the following details:

- Name: InsightConnect
- Application type: Web app/API
- Sign-in URL: https://login.microsoftonline.com

5. Click Create.
6. Save the application registration to Azure, copy and save the Application ID.

Configure API Permissions

1. After registration, go to the application's API permissions page.
2. Click Add a permission and select Microsoft Graph.
3. Choose Application permissions and add the required permissions: User.EnableDisableAccount.All, User.Read.All, and User.RevokeSessions.All.
4. Click Add permissions.
5. Click Grant admin consent for [your organization] to grant the necessary permissions.



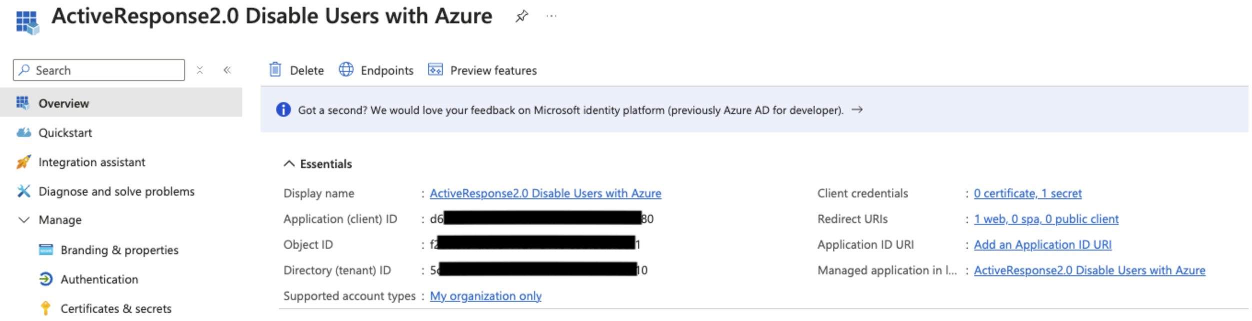
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
User.EnableDisableAccount.A	Application	Enable and disable user accounts	Yes	✓ Granted for
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for
User.RevokeSessions.All	Application	Revoke all sign in sessions for a user	Yes	✓ Granted for

Create Client Secret

1. Go to the Certificates & secrets page.
2. Click New client secret, provide a description, and set an expiration period.
3. Click Add and save the client secret value (you will need this later).

Obtain Tenant ID

1. The tenant ID can be found in the side navigation of Azure Active Directory > Overview.
2. Copy and save the tenant ID for later use.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

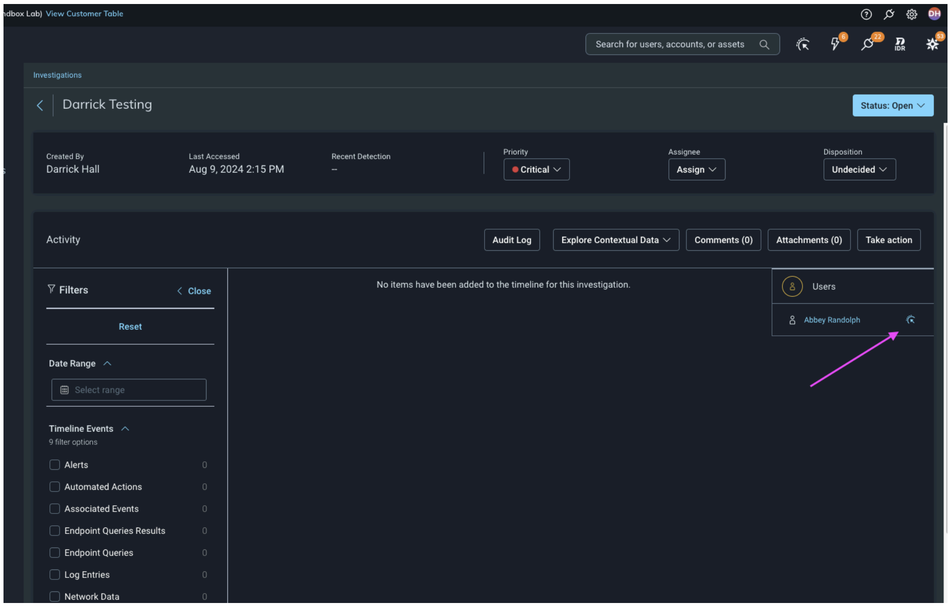
Display name : ActiveResponse2.0 Disable Users with Azure
Application (client) ID : d6[redacted]80
Object ID : f[redacted]1
Directory (tenant) ID : 5[redacted]10
Supported account types : My organization only

Client credentials : 0 certificate, 1 secret
Redirect URIs : 1 web, 0 spa, 0 public client
Application ID URI : Add an Application ID URI
Managed application in l... : ActiveResponse2.0 Disable Users with Azure

Initial Setup within InsightIDR and InsightConnect

InsightIDR Configuration

1. Navigate to InsightIDR:
   - Log in to your InsightIDR account.
   - Go to the Investigations tab.
   - Create a new investigation.
   - Add a test user to the investigation by selecting Explore Contextual Data.
   - Select Inspect Actor Activity.
   - Search for your test user, select the test user, and hit Apply.
   - Refresh the page.
   - On the right-hand navigation, you should now see a user as shown in the screenshot below.
   - Select the symbol next to the user's name.
   - Hit Disable User.



Darrick Testing

Created By: Darrick Hall

Last Accessed: Aug 9, 2024 2:15 PM

Recent Detection: --

Priority: Critical

Assignee: Assign

Disposition: Undecided

No items have been added to the timeline for this investigation.

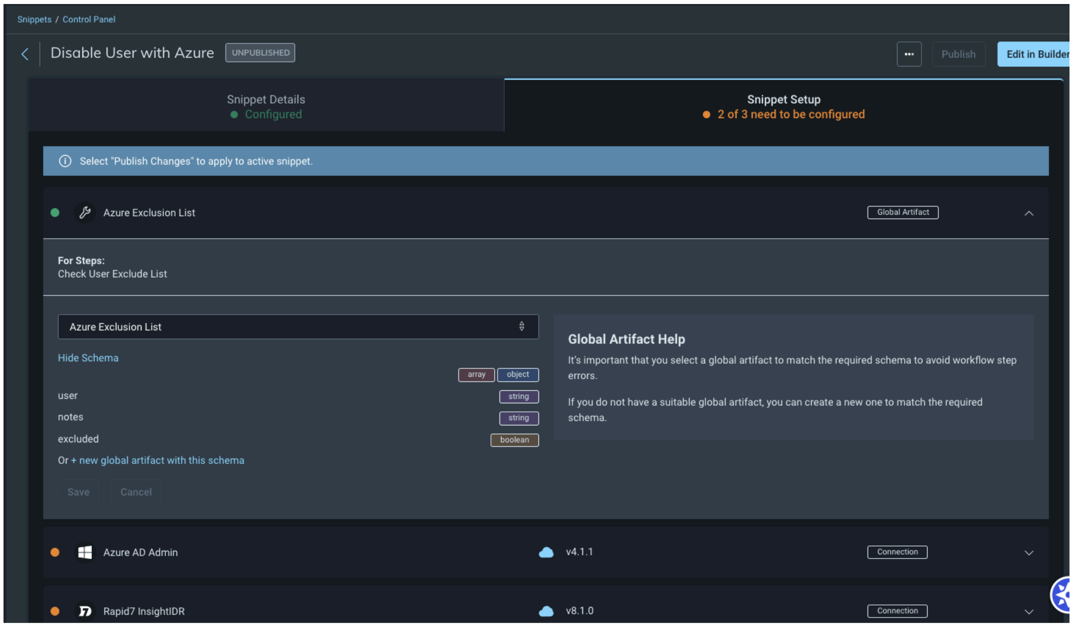
Users: Abbey Randolph

   - Choose Disable User with Azure.
   - Select Configure in InsightConnect.
2. Snippet Setup in InsightConnect:
   - This takes you to the page for the Disable User with Azure snippet.
   - Select the Snippet Setup tab.
   - For the step Azure Exclusion List, select + new global artifact with this schema (see screenshot below).
   - Name the global artifact (e.g., "Azure Active Response User Exclusion List").
   - Select Create Global Artifact.

    - Select Azure AD Admin, choose a connection if you have already created one, if not select either cloud or your orchestrator, and then choose add a new connection.
    - Save.
    - Choose Rapid7 InsightIDR and perform the same steps as with the Azure AD Admin step.
    - Publish.

InsightConnect Configuration

1. Install the Azure AD Admin Plugin:
    - Log in to InsightConnect.
    - Go to the Plugins & Tools section and install the Azure AD Admin plugin.
2. Configure the Plugin:
    - Add a new connection using the client ID, tenant ID, and client secret from Azure.
    - Test the connection to ensure it is set up correctly.
3. Create and Configure Snippets:
    - Go to the Workflows section and create a new workflow or snippet.
    - Add the following steps using the Azure AD Admin plugin:
        1. Get Azure User Info: Configure to lookup the user in Azure.
        2. Revoke Active Azure Sessions: Configure to revoke the user's active sessions.
        3. Disable Azure User: Configure to disable the user's account.



Select "Publish Changes" to apply to active snippet.

For Steps:
Check User Exclude List

Azure Exclusion List

user string
notes string
excluded boolean

Global Artifact Help

It's important that you select a global artifact to match the required schema to avoid workflow step errors.

If you do not have a suitable global artifact, you can create a new one to match the required schema.

Azure AD Admin v4.1.1 Connection

Rapid7 InsightIDR v8.1.0 Connection

4. Publish the Workflow:

    - Once the workflow is configured, publish it to make it available for use in response actions.

Testing the Response Action

1. Add a Test User to an Investigation:
    - In InsightIDR, create an investigation and add a test user.
    - Apply the new response action to verify it performs as expected.
2. Verify Results:
    - Check the logs and results in InsightConnect to ensure the user lookup, session revocation, and account disabling actions were successful.

Troubleshooting the Azure AD Admin Plugin

If your Azure AD Admin plugin fails to authorize, check the plugin's error logs. Common issues include invalid connection settings, incorrect Application ID, Tenant ID, or Secret Key.

Common Connection Error Messages

- Authentication request status: 401: Indicates the Secret Key is invalid.
- Authentication request status: 400: Indicates the Tenant ID or Application ID is invalid.

Summary

This new response action enhances your security operations by allowing rapid response to threats involving Azure AD users. By following the configuration steps outlined above, you can set up and test the new action to ensure it meets your needs.