


Reset-AADUserPassword playbook from GitHub

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

This playbook will reset the user password using Graph API. It will send the password (which is a random guid substring) to the user's manager. The user will have to reset the password upon login.

QUICK DEPLOYMENT OPTIONS

Deploy with incident trigger (recommended)

<https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2FAzure-Sentinel%2Fmaster%2FPlaybooks%2FReset-AADUserPassword%2Fincident-trigger%2Fazuredeploy.json> 

After deployment, attach this playbook to an automation rule so it runs when the incident is created.

Prerequisites:

You will need to grant User.ReadWrite.All permissions to the managed identity. Run the following code replacing the managed identity object id. You find the managed identity object id on the Identity blade under Settings for the Logic App.

```
$MIGuid = "<Enter your managed identity guid here>"
$MI = Get-AzureADServicePrincipal -ObjectId $MIGuid

$GraphAppId = "00000003-0000-0000-c000-000000000000"
$PermissionName = "User.ReadWrite.All"
$roleName="Password Administrator"

$GraphServicePrincipal = Get-AzureADServicePrincipal -Filter "appId eq '$GraphAppId'"
$AppRole = $GraphServicePrincipal.AppRoles | Where-Object {$_.Value -eq $PermissionName -and $_.AllowedMemberTypes -eq "User"}
New-AzureADServiceAppRoleAssignment -ObjectId $MI.ObjectId -PrincipalId $MI.ObjectId `
-ResourceId $GraphServicePrincipal.ObjectId -Id $AppRole.Id
$role = Get-AzureADDirectoryRole | Where {$_.displayName -eq $roleName}
if ($role -eq $null) {
$roleTemplate = Get-AzureADDirectoryRoleTemplate | Where {$_.displayName -eq $roleName}
Enable-AzureADDirectoryRole -RoleTemplateId $roleTemplate.ObjectId
$role = Get-AzureADDirectoryRole | Where {$_.displayName -eq $roleName}
}
Add-AzureADDirectoryRoleMember -ObjectId $role.ObjectId -RefObjectId $MI.ObjectId
```

Make sure to add **Sentinel Contributor + Logic App Contributor** roles to the Managed Identity at a resource group level, to successfully run the logic app.

SOURCE:

<https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks/Reset-AADUserPassword> 