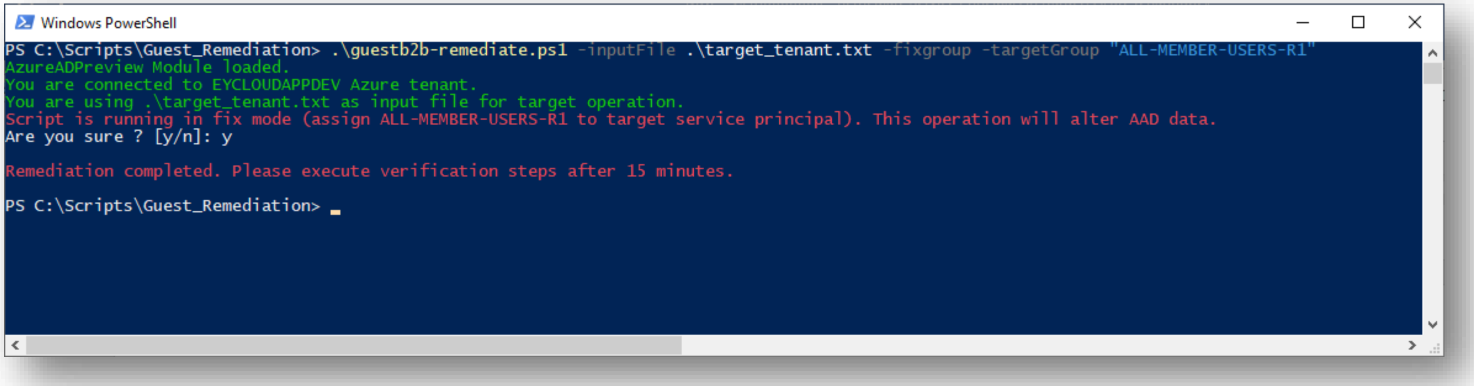
Implementation Steps

For each Target Azure tenant, and related input file(s), follow below steps:

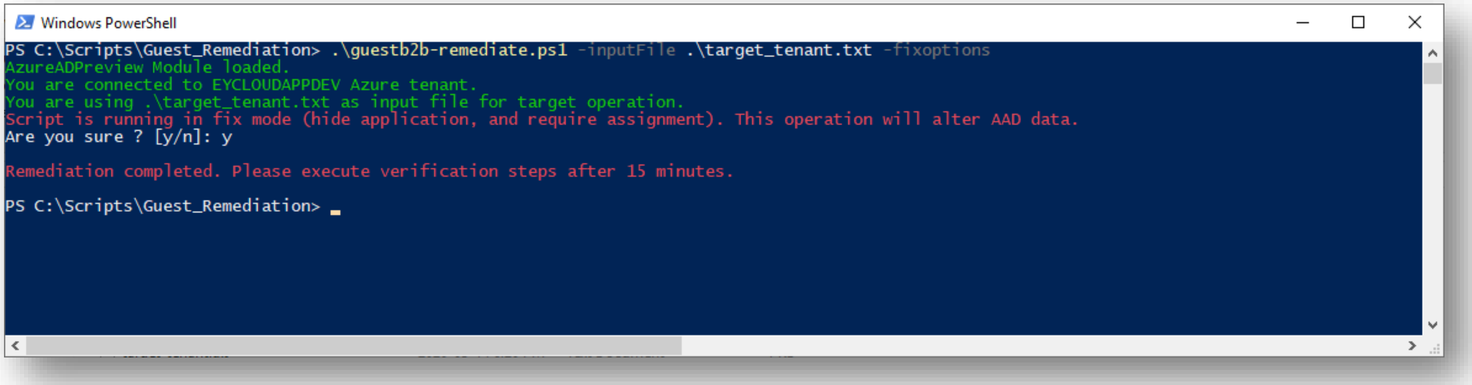
1. Execute script against each target input file, and target dynamic group (following Table 2), using corresponding - *fixgroup*, and -*targetGroup* switches, confirm with '**y**' that you would like to start remediation part:



```
PS C:\Scripts\Guest_Remediation> .\guestb2b-remediate.ps1 -inputFile .\target_tenant.txt -fixgroup -targetGroup "ALL-MEMBER-USERS-R1"
AzureADPreview Module loaded.
You are connected to EYCLOUDAPPDEV Azure tenant.
You are using .\target_tenant.txt as input file for target operation.
Script is running in fix mode (assign ALL-MEMBER-USERS-R1 to target service principal). This operation will alter AAD data.
Are you sure ? [y/n]: y

Remediation completed. Please execute verification steps after 15 minutes.

PS C:\Scripts\Guest_Remediation> _
```

2. When script finishes execution, wait additional 15 minutes to let Azure backend to process changes. Next execute Validation, steps 1-3. Do not continue with next step, if verification steps 1-3 are not successful.

3. Execute script against each target input file, using corresponding - *fixoptions*, confirm with '**y**' that you would like to start remediation part



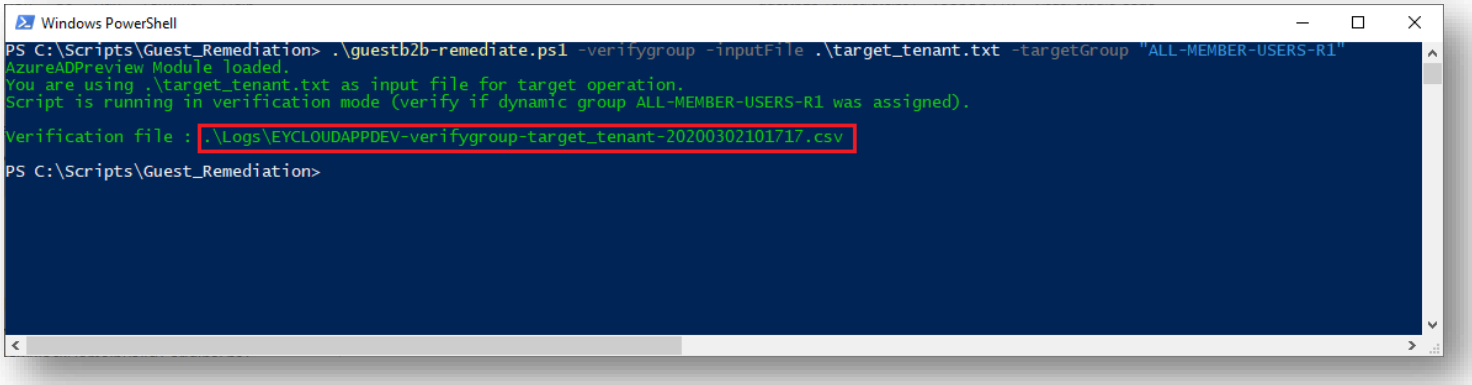
```
PS C:\Scripts\Guest_Remediation> .\guestb2b-remediate.ps1 -inputFile .\target_tenant.txt -fixoptions
AzureADPreview Module loaded.
You are connected to EYCLOUDAPPDEV Azure tenant.
You are using .\target_tenant.txt as input file for target operation.
Script is running in fix mode (hide application, and require assignment). This operation will alter AAD data.
Are you sure ? [y/n]: y

Remediation completed. Please execute verification steps after 15 minutes.

PS C:\Scripts\Guest_Remediation> _
```

4. Wait 15 minutes, and execute Validation, steps 4-6.

Validation Steps

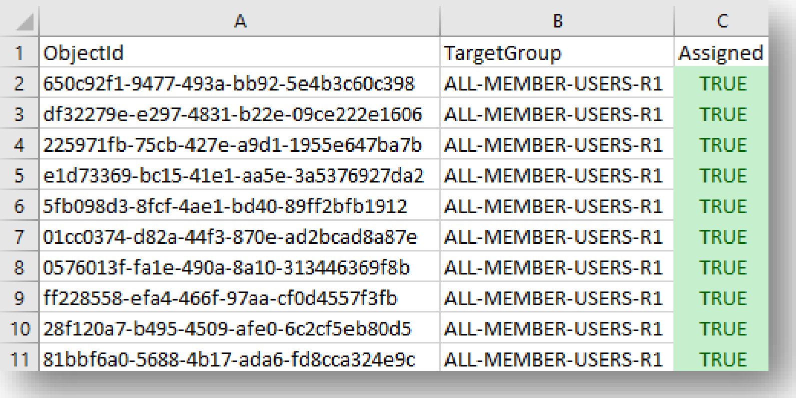
For each Target Azure tenant, and related input file(s) from Table 2, follow below steps:

1. Execute script against each input file from Table 2, using *-verifygroup* switch, and providing target group name with *-targetGroup* switch:



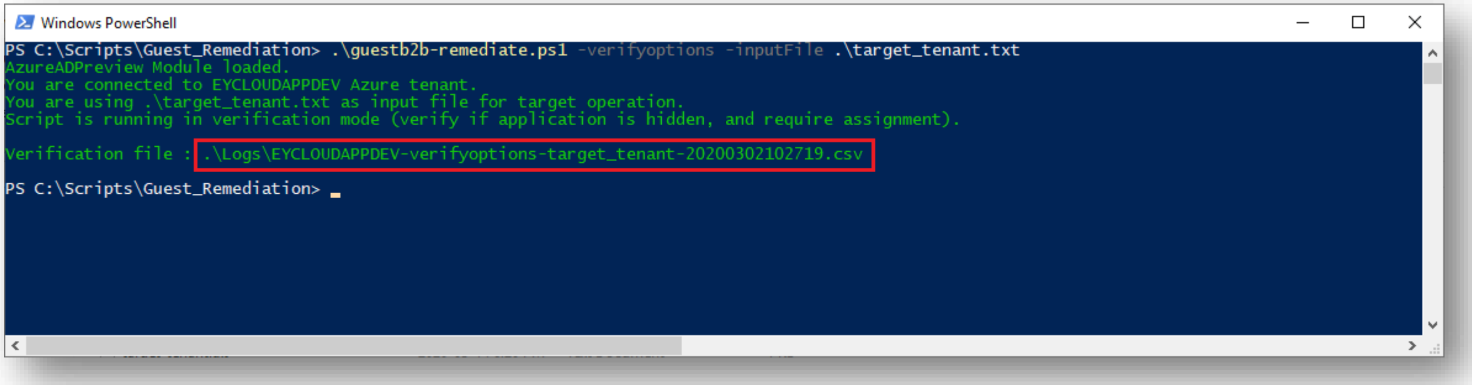
```
PS C:\Scripts\Guest_Remediation> .\guestb2b-remediate.ps1 -verifygroup -inputFile .\target_tenant.txt -targetGroup "ALL-MEMBER-USERS-R1"
AzureADPreview Module loaded.
You are using .\target_tenant.txt as input file for target operation.
Script is running in verification mode (verify if dynamic group ALL-MEMBER-USERS-R1 was assigned).

Verification file : .\Logs\EYCLOUDAPPDEV-verifygroup-target_tenant-20200302101717.csv

PS C:\Scripts\Guest_Remediation>
```

2. Wait for script execution, take a note of output file name.
3. Open output file in Excel, and verify if ***Assigned*** column holds TRUE value only:



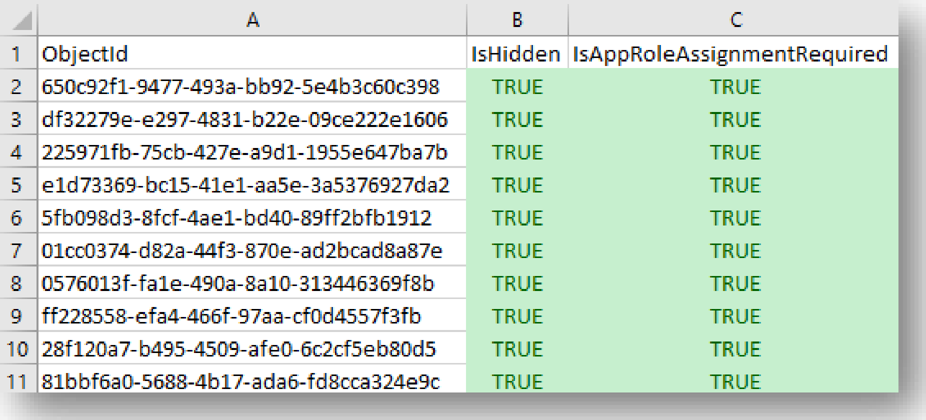
	A	B	C
1	ObjectId	TargetGroup	Assigned
2	650c92f1-9477-493a-bb92-5e4b3c60c398	ALL-MEMBER-USERS-R1	TRUE
3	df32279e-e297-4831-b22e-09ce222e1606	ALL-MEMBER-USERS-R1	TRUE
4	225971fb-75cb-427e-a9d1-1955e647ba7b	ALL-MEMBER-USERS-R1	TRUE
5	e1d73369-bc15-41e1-aa5e-3a5376927da2	ALL-MEMBER-USERS-R1	TRUE
6	5fb098d3-8fcf-4ae1-bd40-89ff2bfb1912	ALL-MEMBER-USERS-R1	TRUE
7	01cc0374-d82a-44f3-870e-ad2bcad8a87e	ALL-MEMBER-USERS-R1	TRUE
8	0576013f-fa1e-490a-8a10-313446369f8b	ALL-MEMBER-USERS-R1	TRUE
9	ff228558-efa4-466f-97aa-cf0d4557f3fb	ALL-MEMBER-USERS-R1	TRUE
10	28f120a7-b495-4509-afe0-6c2cf5eb80d5	ALL-MEMBER-USERS-R1	TRUE
11	81bbf6a0-5688-4b17-ada6-fd8cca324e9c	ALL-MEMBER-USERS-R1	TRUE

4. Execute script against each input file from Table 2, using *-verifyoptions* switch:



```
PS C:\Scripts\Guest_Remediation> .\guestb2b-remediate.ps1 -verifyoptions -inputFile .\target_tenant.txt
AzureADPreview Module loaded.
You are connected to EYCLOUDAPPDEV Azure tenant.
You are using .\target_tenant.txt as input file for target operation.
Script is running in verification mode (verify if application is hidden, and require assignment).

Verification file : .\Logs\EYCLOUDAPPDEV-verifyoptions-target_tenant-20200302102719.csv

PS C:\Scripts\Guest_Remediation> _
```

5. Wait for script execution, take a note of output file name.
6. Open output file in Excel, and verify if ***IsHiddem**, and **IsAppRoleAssignmentRequired*** columns holds TRUE values only:



	A	B	C
1	ObjectId	IsHidden	IsAppRoleAssignmentRequired
2	650c92f1-9477-493a-bb92-5e4b3c60c398	TRUE	TRUE
3	df32279e-e297-4831-b22e-09ce222e1606	TRUE	TRUE
4	225971fb-75cb-427e-a9d1-1955e647ba7b	TRUE	TRUE
5	e1d73369-bc15-41e1-aa5e-3a5376927da2	TRUE	TRUE
6	5fb098d3-8fcf-4ae1-bd40-89ff2bfb1912	TRUE	TRUE
7	01cc0374-d82a-44f3-870e-ad2bcad8a87e	TRUE	TRUE
8	0576013f-fa1e-490a-8a10-313446369f8b	TRUE	TRUE
9	ff228558-efa4-466f-97aa-cf0d4557f3fb	TRUE	TRUE
10	28f120a7-b495-4509-afe0-6c2cf5eb80d5	TRUE	TRUE
11	81bbf6a0-5688-4b17-ada6-fd8cca324e9c	TRUE	TRUE

Recovery Steps

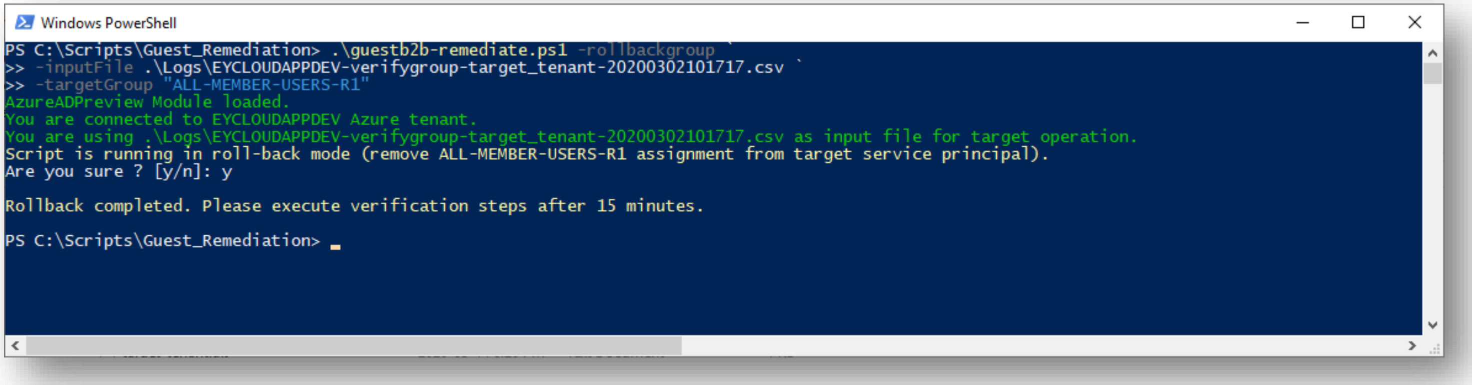
To successfully recover all Service Principals to previous state, we have to use verification .csv files created during prerequisite script execution. Those files are located under **Logs** folder, and holds following names:

- *<tenant name>-verifygroup-<input file base name>-<time stamp>.csv*
- *<tenant name>-verifyoptions-<input file base name>-<time stamp>.csv*

We have to use both files as input files for rollback script run. If we will use the files without any changes – we will rollback all Service Principals to previous state. To rollback just selected ones – either create new files which holds just selected rows from above files, or remove unwanted rows, leaving just Service Principals data which require rollback. Alternatively follow manual roll-back steps from Appendix.

For full roll-back, follow below steps:

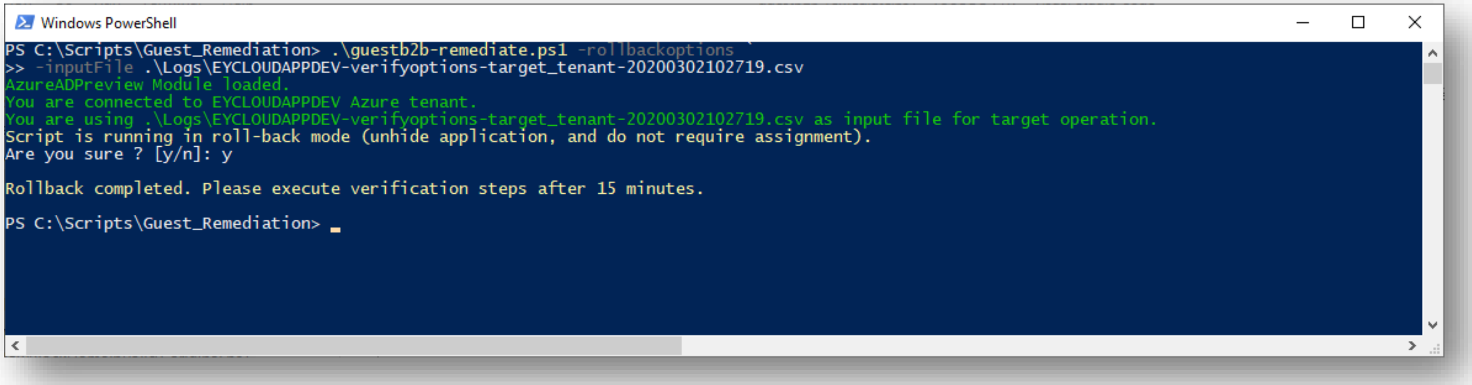
1. Execute script against *<tenant name>-verifygroup-<input file base name>-<time stamp>.csv* file, and target dynamic group (following Table 2), using corresponding *-rollbackgroup*, and *-targetGroup* switches, confirm with '**y**' that you would like to start rollback:



```
PS C:\Scripts\Guest_Remediation> .\guestb2b-remediate.ps1 -rollbackgroup `
>> -inputFile .\Logs\EYCLOUDAPPDEV-verifygroup-target_tenant-20200302101717.csv `
>> -targetGroup "ALL-MEMBER-USERS-R1"
AzureADPreview Module loaded.
You are connected to EYCLOUDAPPDEV Azure tenant.
You are using .\Logs\EYCLOUDAPPDEV-verifygroup-target_tenant-20200302101717.csv as input file for target operation.
Script is running in roll-back mode (remove ALL-MEMBER-USERS-R1 assignment from target service principal).
Are you sure ? [y/n]: y

Rollback completed. Please execute verification steps after 15 minutes.

PS C:\Scripts\Guest_Remediation> _
```

2. When script finishes execution, wait additional 15 minutes to let Azure backend to process changes. Next - execute Validation, steps 1-3, and confirm if new verify .csv file is identical to the one used for remediation.

3. Execute script against *<tenant name>-verifyoptions-<input file base name>-<time stamp>.csv* file, using *-rollbackoptions switch*, confirm with '**y**' that you would like to start rollback:



```
PS C:\Scripts\Guest_Remediation> .\guestb2b-remediate.ps1 -rollbackoptions `
>> -inputFile .\Logs\EYCLOUDAPPDEV-verifyoptions-target_tenant-20200302102719.csv
AzureADPreview Module loaded.
You are connected to EYCLOUDAPPDEV Azure tenant.
You are using .\Logs\EYCLOUDAPPDEV-verifyoptions-target_tenant-20200302102719.csv as input file for target operation.
Script is running in roll-back mode (unhide application, and do not require assignment).
Are you sure ? [y/n]: y

Rollback completed. Please execute verification steps after 15 minutes.

PS C:\Scripts\Guest_Remediation> _
```

4. When script finishes execution, wait additional 15 minutes to let Azure backend to process changes. Next - execute Validation, steps 4-6, and confirm if new verify .csv file is identical to the one used for remediation.

Appendix

I. Errors expected in Audit Log due to remediation

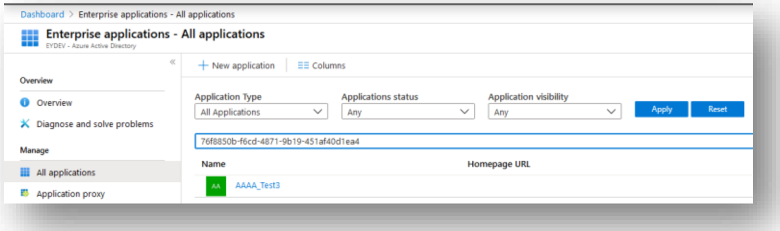
If there is a legitimate need for a guest user to log into an app, that has been remediated, you can identify the change as the cause of an issue via the sign in logs. There will be a login failure event logged for the user/app with a sign-in error code of **50105**.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes

II. Manual remediation

If manual remediation is required, follow below steps for single Service Principal, if target application is known:

1. Login to the target Azure AD Tenant using your MSP01 account thru https://portal.azure.com
2. Navigate to Enterprise applications blade, and search for target application using **Application ID** (not service Principal ID):

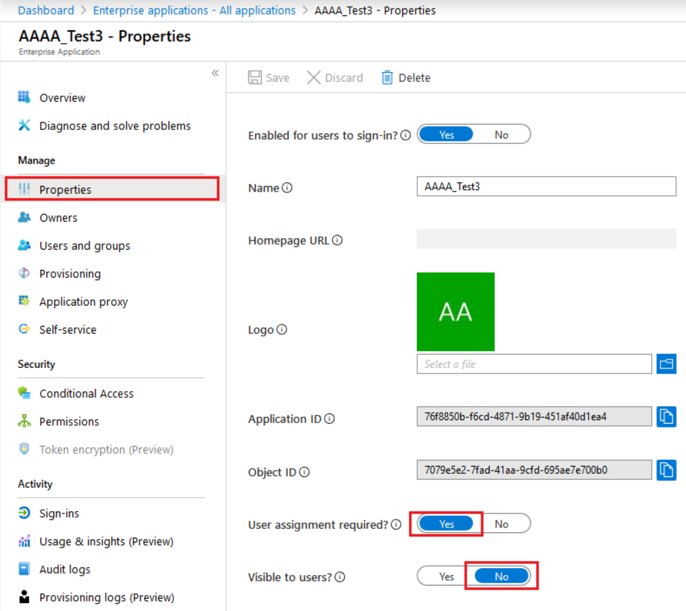

Dashboard > Enterprise applications - All applications
Enterprise applications - All applications
EYDEV - Azure Active Directory
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
New application
Columns
Apply
Reset

Application Type: All Applications
Applications status: Any
Application visibility: Any

76f8850b-f6cd-4871-9b19-451af40d1ea4

Name	Homepage URL
AA AAAA_Test3	

3. Click on selected application, and click **Properties** on left pane. Select **Yes** for '*User assignment required?*' option, and **No** for '*Visible to users?*':


Dashboard > Enterprise applications - All applications > AAAA_Test3 - Properties
Overview
Diagnose and solve problems
Manage
Properties
Owners
Users and groups
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption (Preview)
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Save
Discard
Delete
Select a file

AAAA_Test3 - Properties
Enterprise Application

Enabled for users to sign-in? [✓ Yes] No

Name: AAAA_Test3

Homepage URL:

Logo: AA

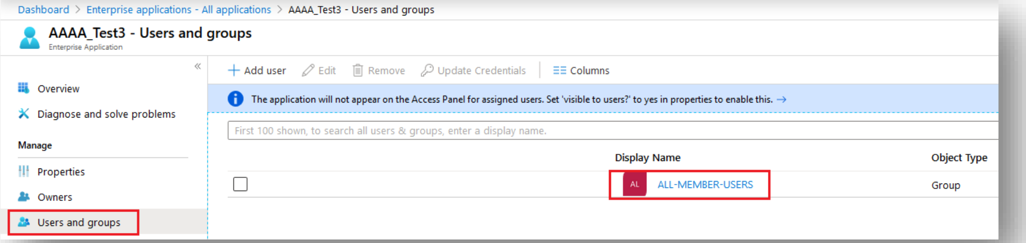
Application ID: 76f8850b-f6cd-4871-9b19-451af40d1ea4

Object ID: 7079e5e2-7fad-41aa-9cfd-695ae7e700b0

User assignment required? [✓ Yes] No

Visible to users? Yes [✓ No]

4. Click on *Users and groups*, and assign selected **ALL-MEMBER-USERS-Rx** group


Dashboard > Enterprise applications - All applications > AAAA_Test3 - Users and groups
Overview
Diagnose and solve problems
Manage
Properties
Owners
Users and groups
Add user
Edit
Remove
Update Credentials
Columns
First 100 shown, to search all users & groups, enter a display name.

AAAA_Test3 - Users and groups
Enterprise Application

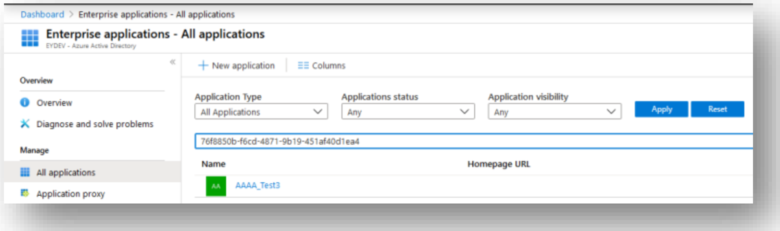
The application will not appear on the Access Panel for assigned users. Set 'visible to users?' to yes in properties to enable this. →

	Display Name	Object Type
□	AL ALL-MEMBER-USERS	Group

III. Manual roll-back

If manual roll-back is required, follow below steps for single Service Principal, if target application is known:

1. Login to the target Azure AD Tenant using your MSP01 account thru https://portal.azure.com
2. Navigate to Enterprise applications blade, and search for target application using **Application ID** or **Application DisplayName** (not service Principal ID):



Dashboard > Enterprise applications - All applications

Enterprise applications - All applications
EYDEV - Azure Active Directory

Application Type: All Applications
Applications status: Any
Application visibility: Any

76f8850b-f6cd-4871-9b19-451af40d1ea4

Name	Homepage URL
AA AAAA_Test3	

3. Click on selected application, and click **Properties** on left pane. Select **No** for '*User assignment required?*' option, and **Yes** for '*Visible to users?*':
4. Click on *Users and groups*, and remove any group which follow **ALL-MEMBER-USERS-*** name (e.g. ALL-MEMBER-USERS-R1 .. R10)