EntraID setup for guest users

THis articke explains what needs to be done on EntraID to get Guest users working in Loftware Cloud. Same information applies for NiceLabel Subscription model.

- **Mar 13, 2025**
- **Knowledge**

Title

EntraID setup for guest users

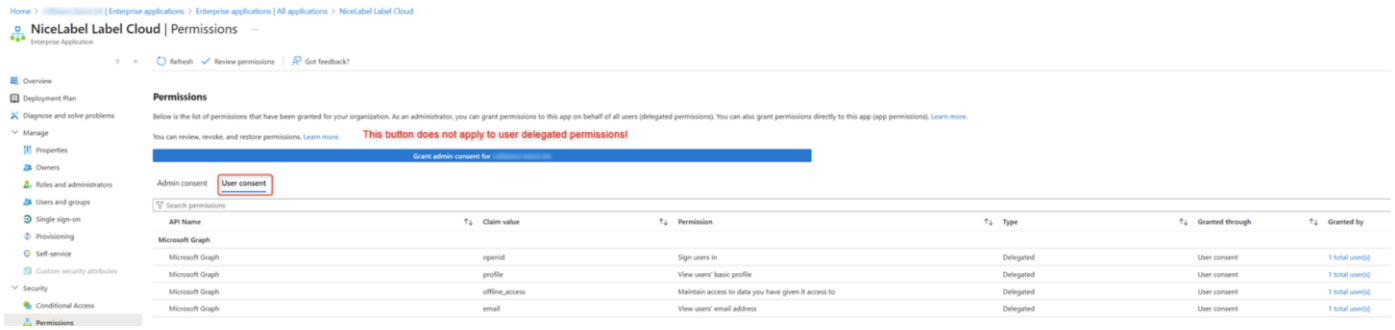
Question

Guest users are blocked from signing into Loftware Cloud.

User needs admin consent to log into Loftware Cloud.

Answer

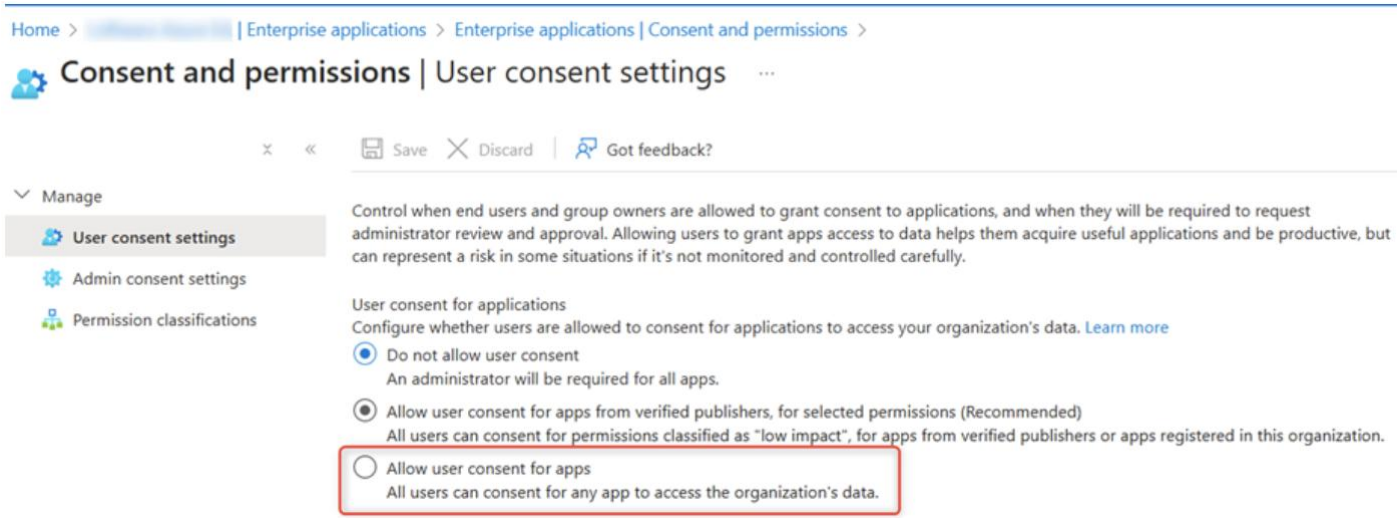
For guest users in Loftware Cloud or users on NiceLabel subscription only "delegated user consent" permissions are required: *openid*, *profile*, *email*, *offline_access*.



The user trying to log into Loftware Cloud has 3 options for consenting to these permissions (can be restricted further via User Assignment):

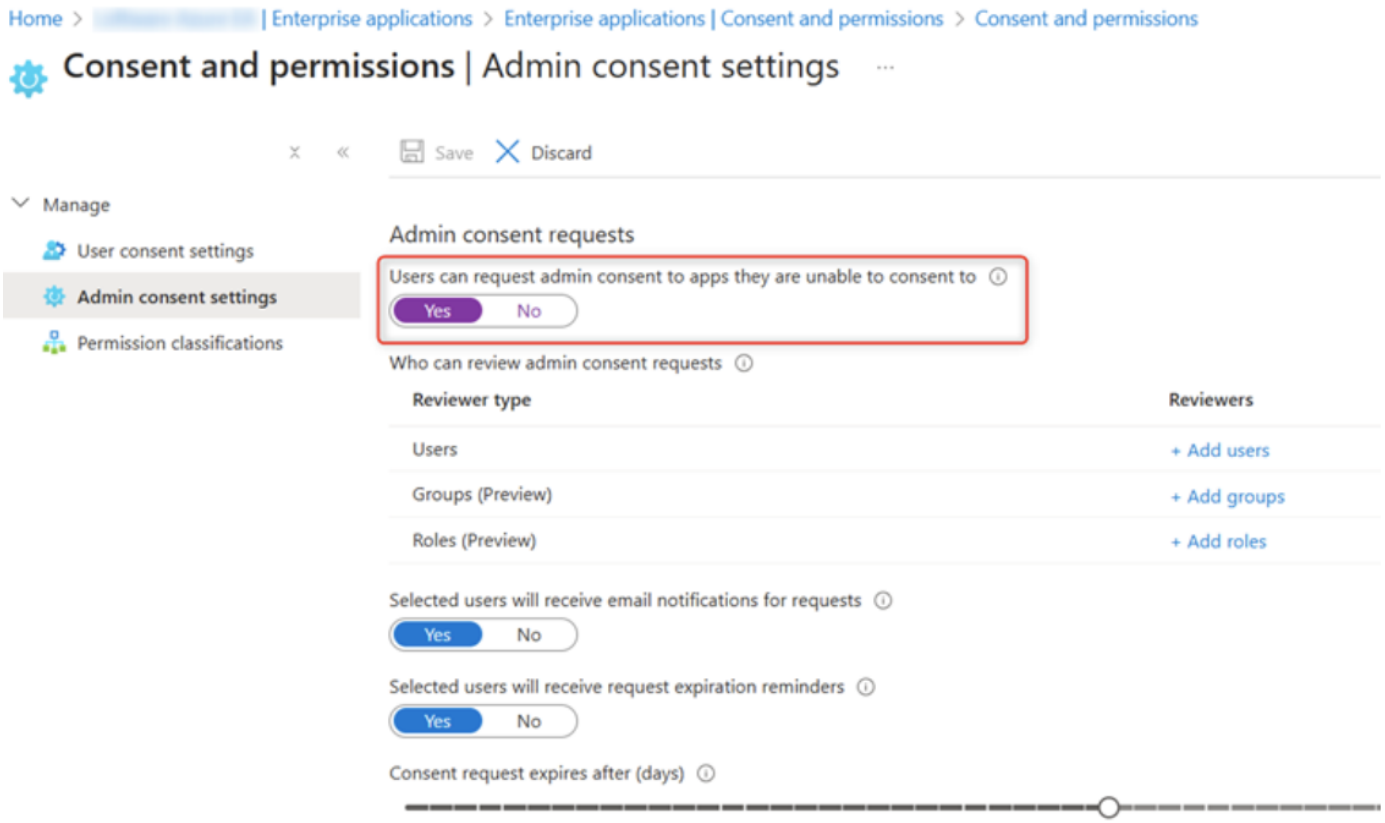
1. Allow users to consent to their own permission requests, instead of requiring an administrator
2. Enable the Admin Consent flow, which will allow users to request consent approval from an administrator
3. Preauthorize individual user principals or all principals

1. Allow users to consent to their own permission requests, instead of requiring an administrator
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/user-admin-consent-overview
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=portal

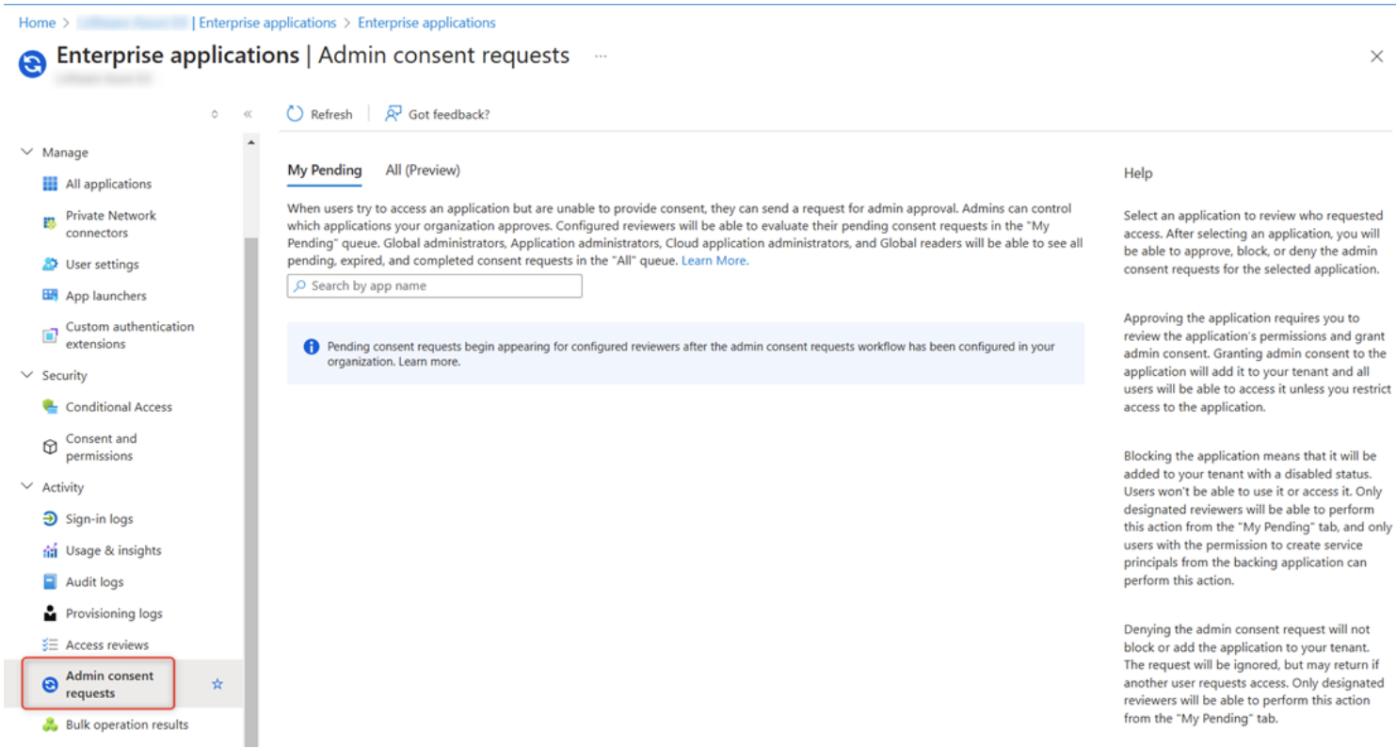


Each user who logs in to Loftware Cloud/License Center/Cloud Designer will be prompted to approve requested permissions without requiring admin approval. Enterprise Application User Assignment and Loftware Cloud RBAC (Role based access control) can still be used to restrict which users can access the application.

2. Enable the Admin Consent flow, which will allow users to request consent approval from an administrator
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-admin-consent-workflow



Each user who logs in to Loftware Cloud/License Center/Cloud Designer will be denied permission to consent to permissions, but will be given the option to ask for admin approval. You must have your AAD admins approve pending consent requests:



3. Preauthorize individual user principals or all principals
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-consent-single-user
https://learn.microsoft.com/en-us/entra/identity-platform/permissions-consent-overview#preauthorization
3.1 Preauthorize individual user principals

Connect to MgGraph with:
Connect-MgGraph

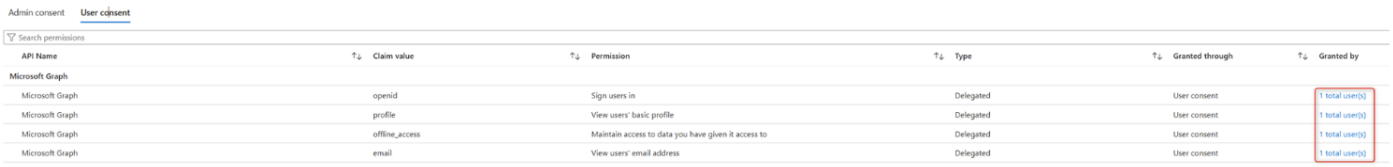
extra params if needed for your environment
Connect-MgGraph -TenantId [ID] -Scopes "Application.ReadWrite.All",
"DelegatedPermissionGrant.ReadWrite.All"

Use this to get Graph API "ResourceId" from an existing permission grant:
Get-MgOauth2PermissionGrant -Filter "clientId eq '[Object Id]' and consentType eq 'Principal'"

ObjectId = NiceLabel Label Cloud Enterprise App ObjectId

Use the command below to preauthorize a single user:
$params = @{
ClientId = "[Object Id]"
ConsentType = "Principal"
PrincipalId = "[PrincipalId]"
ResourceId = "[ResourceId]"
Scope = "openid email profile offline_access"
}
New-MgOauth2PermissionGrant -BodyParameter $params

Client Id = NiceLabel Label Cloud Enterprise App ObjectId
PrincipalId = User principal ObjectId
ResourceId = Microsoft Graph App Id (from previous Get-MgOauth2PermissionGrant step)



3.2 Preauthorize all principals

Connect to MgGraph with:
Connect-MgGraph

extra params if needed for your environment
Connect-MgGraph -TenantId [ID] -Scopes "Application.ReadWrite.All",
"DelegatedPermissionGrant.ReadWrite.All"

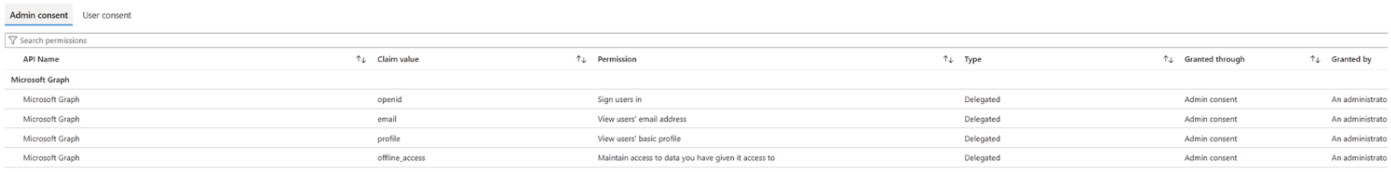
Use this to get Graph API "ResourceId" from an existing permission grant:
Get-MgOauth2PermissionGrant -Filter "clientId eq '[Object Id]' and consentType eq 'Principal'"

ObjectId = NiceLabel Label Cloud Enterprise App ObjectId

To authorize all principals:
$params = @{
ClientId = "[Object Id]"
ConsentType = "AllPrincipals"
ResourceId = "[ResourceId]"
Scope = "openid email profile offline_access"

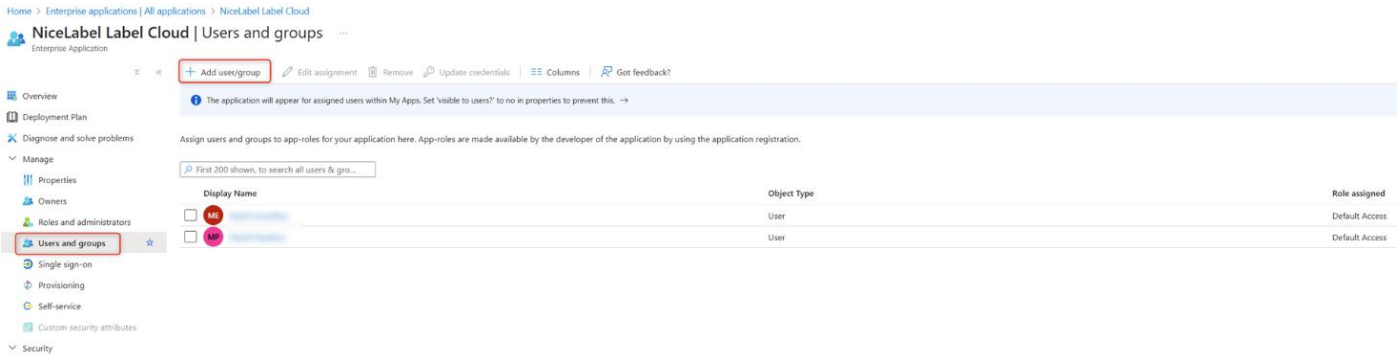
}
New-MgOauth2PermissionGrant -BodyParameter $params

Client Id = NiceLabel Label Cloud Enterprise App ObjectId
ResourceId = Microsoft Graph App Id (from previous Get-MgOauth2PermissionGrant step)



General info about User Assignment:
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/assign-user-or-group-access-portal?pivots=portal

If User Assignment is required/preferred, simply assign users who should be able to login to the Loftware Label Cloud Enterprise Application (and Loftware Cloud RBAC):



Additional Notes

Last Published Date

3/13/2025, 11:47 AM