

## EntraID setup for guest users

This article 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 screenshot shows the 'Permissions' page for the 'NiceLabel Label Cloud' application in the Microsoft Entra admin center. A red box highlights the 'User consent' button. Below the button is a table of permissions granted to the application.

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph	openid	Sign users in	Delegated	User consent	1 total users
Microsoft Graph	profile	View users' basic profile	Delegated	User consent	1 total users
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	User consent	1 total users
Microsoft Graph	email	View users' email address	Delegated	User consent	1 total users

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?pivot=portal>

The screenshot shows the 'Consent and permissions | User consent settings' page in the Microsoft Entra admin center. The 'Allow user consent for apps' option is highlighted with a red box.

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications  
Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- Do not allow user consent  
An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)  
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- Allow user consent for apps  
All users can consent for any app to access the organization's data.

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>

Home > [Tenant Name] | Enterprise applications > Enterprise applications | Consent and permissions > Consent and permissions

### Consent and permissions | Admin consent settings

Save Discard

Manage

- User consent settings
- Admin consent settings**
- Permission classifications

#### Admin consent requests

Users can request admin consent to apps they are unable to consent to  Yes  No

Who can review admin consent requests

Reviewer type	Reviewers
Users	+ Add users
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests  Yes  No

Selected users will receive request expiration reminders  Yes  No

Consent request expires after (days)

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:

Home > [Tenant Name] | Enterprise applications > Enterprise applications

### Enterprise applications | Admin consent requests

Refresh Got feedback?

Manage

- All applications
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions
- Security
  - Conditional Access
  - Consent and permissions
- Activity
  - Sign-in logs
  - Usage & insights
  - Audit logs
  - Provisioning logs
  - Access reviews
  - Admin consent requests**
  - Bulk operation results

#### My Pending All (Preview)

When users try to access an application but are unable to provide consent, they can send a request for admin approval. Admins can control which applications your organization approves. Configured reviewers will be able to evaluate their pending consent requests in the "My Pending" queue. Global administrators, Application administrators, Cloud application administrators, and Global readers will be able to see all pending, expired, and completed consent requests in the "All" queue. [Learn More.](#)

Search by app name

**i** Pending consent requests begin appearing for configured reviewers after the admin consent requests workflow has been configured in your organization. [Learn more.](#)

Help

Select an application to review who requested access. After selecting an application, you will be able to approve, block, or deny the admin consent requests for the selected application.

Approving the application requires you to review the application's permissions and grant admin consent. Granting admin consent to the application will add it to your tenant and all users will be able to access it unless you restrict access to the application.

Blocking the application means that it will be added to your tenant with a disabled status. Users won't be able to use it or access it. Only designated reviewers will be able to perform this action from the "My Pending" tab, and only users with the permission to create service principals from the backing application can perform this action.

Denying the admin consent request will not block or add the application to your tenant. The request will be ignored, but may return if another user requests access. Only designated reviewers will be able to perform this action from the "My Pending" tab.

### 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)
```

Admin consent    User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph	openid	Sign users in	Delegated	User consent	1 total user(s)
Microsoft Graph	profile	View users' basic profile	Delegated	User consent	1 total user(s)
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	User consent	1 total user(s)
Microsoft Graph	email	View users' email address	Delegated	User consent	1 total user(s)

#### 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)

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Microsoft Graph	email	View users' email address	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator

### General info about User Assignment:

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/assign-user-or-group-access-portal?pivot=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):

Home > Enterprise applications | All applications > NiceLabel Label Cloud

NiceLabel Label Cloud | Users and groups

+ Add user/group | Edit assignment | Remove | Update credentials | Columns | Get feedback?

The application will appear for assigned users within My Apps. Set 'visible to users' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. App-roles are made available by the developer of the application by using the application registration.

First 200 shown, to search all users & groups...

Display Name	Object Type	Role assigned
MS [redacted]	User	Default Access
MP [redacted]	User	Default Access

### Additional Notes

#### Last Published Date

3/13/2025, 11:47 AM