



Onsight NOW Administrator Guide

Copyright

Onsight NOW: IT Admin Guide

Doc #: 400401-06 Rev: A

August 2025

Information in this document is subject to change without notice. Reproduction in any manner whatsoever without the written permission of Librestream is strictly forbidden.

Copyright Notice:

Copyright 2004-2025 Librestream Technologies Incorporated. All Rights Reserved.

Patents Notice:

United States Patent # 7,221,386, together with additional patents pending in Canada, the United States, and other countries, all of which are in the name of Librestream Technologies Inc.

Trademark Notice

Librestream, the Librestream logo, Onsight, the Onsight logo, Onsight NOW, the Onsight NOW logo, Onsight Connect, Onsight Flow, Onsight Workspace, Onsight Cube, Onsight Collaboration Hub, Onsight Smartcam, Onsight Platform Manager, and Onsight Teamlink are either registered trademarks or trademarks of Librestream Technologies Incorporated in Canada, the United States, European Union and/or other countries. All other trademarks are the property of their respective owners.

Contents

1	Checklist.....	5
2	Enterprise Application: Registration.....	6
	2.1 Manage Onsite NOW Microsoft Entra ID Application	6
	2.1.1 Microsoft Permissions	6
	2.1.1.1 Application Permissions	7
	2.1.1.2 Delegated Permissions.....	7
	2.1.2 Granting Consent to Onsite NOW Permissions.....	8
	2.1.3 Assigning Users to Onsite NOW	10
	2.2 Add Users and Groups	11
	2.2.1 User Types and Roles	11
	2.2.2 Adding a User Group	12
	2.3 External Users	15
	2.3.1 Inviting External Users Using Microsoft Entra ID.....	15
	2.3.2 Signing Into a Different Organization as an External User.....	15
3	Organization Settings.....	17
	3.1 Microsoft Permissions.....	17
	3.1.1 Consent to Permissions.....	17
	3.1.2 Revoking Permissions	18
	3.1.3 Disabling Permissions in Onsite NOW	19
	3.1.4 Revoking Permissions in Entra ID.....	20
	3.2 Licenses.....	23
	3.3 Divisions	23
4	Settings.....	24
	4.1 Homepage Layout	24
	4.2 Permissions.....	25
	4.2.1 Meetings	25
	4.2.2 Contacts	25
	4.2.3 Guest Contacts	25
	4.3 Ida Knowledge Sources	26
	4.3.1 Add SharePoint Source	26
	4.3.2 Add Azure Storage BLOB Source.....	27
	4.3.3 Supported Document Types for Indexing.....	27
	4.4 Collections.....	27
	4.5 Reports	29
	4.6 Calls	29
	4.6.1 Tenant Setup for Teams Ad Hoc Calling via PowerShell & ACS Immutable ID	30
	4.6.2 Teams Ad Hoc Calling – Microsoft Teams Phone License Assignment	31
	4.7 Custom Messages	31
	4.8 Users 32	
	4.9 Group Settings	32
	4.9.1 Entra Group Synchronization	32
	4.9.1.1 Assigning Setting to Groups	33
	4.9.1.2 Ida Document Sources	34
	4.9.1.3 Assigning Group Priority	34
	4.10 SharePoint Configuration.....	34
	4.10.1 Collections - SharePoint Configuration	34
	4.10.2 Creating a new Onsite NOW SharePoint site	34

4.10.3	Create SharePoint Document Libraries.....	38
4.10.3.1	Create the Collections Document Library	38
4.10.3.2	Create the Ida Documents Library.....	38
4.10.4	Collections Folder Structure.....	38
4.10.5	Configure SharePoint Drive in Onsite NOW.....	39
4.10.6	Configure SharePoint for Onsite NOW Tagging.....	40
4.10.6.1	Categories.....	40
4.10.6.2	Tags	40
4.10.6.3	SharePoint Term Store.....	40
4.10.6.4	Required API Permissions.....	40
4.10.6.5	Configuring The Document Library	41
4.10.6.6	Managing Categories and Tags in Onsite NOW	43
4.11	Ida Knowledge Source Configuration	44
4.11.1	Ida Document Indexing from SharePoint [Optional]	44
4.11.1.1	Customer Prerequisites.....	44
4.11.1.2	SharePoint Site.....	45
4.12	Granting Onsite NOW Sites.Selected permissions to the SharePoint	45
4.12.1	Grant read/write permissions to the Onsite NOW SharePoint site using Graph Explorer.....	46
4.12.2	Grant read/write permissions to the Onsite NOW SharePoint site using Postman.....	47
4.12.3	Ida Document Indexing from Azure Blob Storage [Optional]	49
4.13	External Applications	50
4.13.1	Application Registration	50
4.13.2	Application Configuration	51
4.13.3	Obtaining and Using Tokens	52
4.13.4	Using External Applications Resources.....	52
5	Analytics	54
6	Ida Dashboard	54
7	Web Browser Notifications.....	55
7.1	How to Receive Web browser notifications	55
7.1.1	For PC's and Android devices.....	55
7.1.2	Mac/iOS (Safari and Chrome)	55
8	Support.....	56

1 Checklist

This checklist provides guidance on the steps needed to complete the Onsight NOW installation and configuration.

- ☐ [Custom Branding Guide](#) if required.
- ☐ Consult the [Firewall, Proxy & Security Settings Configuration Guide](#).
- ☐ Access *app.onsightnow.com (or app.onsightgov.us for Government Cloud customers) and sign in.
- ☐ Grant Consent and tenant-wide access (Default).
- ☐ Assign Onsight NOW admin access to an Entra admin so they can access admin settings within the enterprise application.
- ☐ Within Entra, [Add users or groups](#) to the Onsight NOW application.
- ☐ Configure [Application Settings](#), and [Collections & SharePoint Integration](#).
- ☐ Consult and modify [Onsight NOW Permissions](#) as necessary.
- ☐ Validate the [Organization Settings](#).
- ☐ Validate Onsight NOW connectivity by making a test call.




Note: This also validates the Firewall.

- ☐ Validate SharePoint by accessing the camera and taking a picture.
- ☐ Validate the [Outlook Add-in](#) feature.
- ☐ Verify that the Calendar displays upcoming events.
- ☐ Enable Teams Ad-hoc calling settings as required. Refer to the [Calls](#) section and perform a test call.

2 Enterprise Application: Registration

To enable users within an organization to log in to Onsight NOW using their Microsoft accounts, an IT administrator must set up and configure their [Microsoft Entra ID](#)¹ environment. Librestream will use your organization's [Microsoft Entra ID Tenant Identifier \(ID\)](#) to register the organization and provide access to Onsight NOW as an enterprise application. The customer will provide their Microsoft domain to Librestream as part of the onboarding process. Librestream will use the domain to look up the tenant ID.

The organization will need to manage the Onsight NOW application within Entra. This includes granting consent for users, the application permissions required by Onsight NOW, and enabling access to the external application for users.

 **Important:** Please add *.onsightnow.com (or *.onsightgov.us for Government Cloud customers) to your firewall whitelist during onboarding.

2.1 Manage Onsight NOW Microsoft Entra ID Application

Before users from an organization can log in to Onsight NOW, Librestream will use the organization's [Tenant ID](#) as the unique ID for configuring Onsight NOW access for their [Microsoft Entra ID](#) instance. This will enable an IT administrator to:

- Authenticate their organization's users.
- Manage permissions and user assignments for the Onsight NOW application.

After Librestream has confirmed your Onsight NOW registration, the IT administrator can set up the Onsight NOW [Microsoft Entra ID](#) application.


A [Microsoft Entra ID](#) administrator will need to perform the following tasks:

- Grant consent to required permissions for the Onsight NOW [Microsoft Entra ID](#) enterprise application.
- Manage the assignment of the Onsight NOW app to users and groups within their [Microsoft Entra ID](#) tenant.

2.1.1 Microsoft Permissions

Onsight NOW requests a set of Microsoft API permissions required for various platform features and services. The following sections describe how Onsight NOW uses these permissions. An Entra Admin is required to complete the Microsoft permissions configuration. Permissions are divided into two categories Application and Delegated.

Application permissions allow the application to act independently of any user context. Delegated permissions allow the application to act on behalf of the signed-in user.

 **Tip:** When an application registers within an organization's tenant, a Microsoft Entra administrator must provide consent for applications that require this permission. The Entra ID administrator roles that should be sufficient are **Privileged Role Administrator** and **Global Administrator**.

1. Microsoft Entra ID is the new product name for Azure Active Directory (AAD).

2.1.1.1 Application Permissions

The following permissions are application scoped to access resources:

Graph

- **Sites.Selected (Application):** This permission enables Onsite NOW:
 - To read and save call recordings to SharePoint and retrieve responses from Ida on behalf of the application. (Application)
 - To read and index documents from SharePoint for use by Ida.
 - To allow guests or Entra external users to capture images and add them to call Collections.
 - **IMPORTANT:** See section [2.1.2](#) for instructions on granting this permission to Onsite NOW.
 - **IMPORTANT:** See section [4.12.1](#) to complete the Sites.Selected permission setup by a SharePoint administrator.
- **Users.ReadBasic.All:** This permission allows users to find contacts and send guest invites within their [Microsoft Entra ID](#) directory. It can also search the directory for additional connections to call, chat, and share content.
- **GroupMember.Read.All:** Allows the application to get the contacts for groups assigned to the enterprise application and send guest invites. (Scope: Application)

SharePoint

- **Sites.Selected (Application):** Read term sets and terms (categories and tags) that are applied to a document and apply new metadata to a document.
- **TermStore.ReadWrite.All:** Read existing term sets and terms from the term store and create new terms.

2.1.1.2 Delegated Permissions

The following permissions are delegated permissions to access resources:

File Permissions

- **Files** – Required for minimal application functionality.
- **Files.ReadWrite.All:** (**Deprecated: Not recommended**, use Files.Read.All / Sites.Selected (Delegated) instead.) This permission enables Onsite NOW to read and save files to SharePoint that the user has access to. It is required to search, view, and save SharePoint files such as [Industrial Digital Assistant \(Ida\)](#), indexed documents and knowledge collections and their contents, such as captured images and reports and search them for presenting content related to a call, chat, or other activity.
- **Files.Read.All:** This permission enables Onsite NOW to perform Ask Ida searches and read files from any SharePoint site to which the user has access. It is required to be able to search and view SharePoint files such as Ida indexed documents, knowledge collections and their contents, such as captured images and reports and search them for presenting content related to a call, chat, or other activity.
- **Sites.Selected (Delegated):** This permission enables Onsite NOW:
 - To read and save files to SharePoint on behalf of the authenticated user (Delegated).
 - This allows users to read/write collections to SharePoint for selected sites.
It's required to save knowledge collections and their contents, such as captured images and reports and search them for presenting content related to a call, chat, or other activity.
 - It's also required for Onsite NOW to be able to read and index documents from SharePoint for use by Ida.
 - **IMPORTANT:** This permission is granted within Onsite NOW under Settings – Microsoft Permissions – Sites.Selected.

See section [3.1 Microsoft Permissions](#) for further details.

Contacts Permissions

- **Users.Read.All:** This permission allows the loading of user profile pictures.
- **GroupMember.Read.All:** (*Deprecated: Replaced by the GroupMember.Read.All Application permission*) Allows the application to get the contacts for groups assigned to the enterprise application and send guest invites. (Scope: Delegated)
 - **Note:** If your organization uses Entra ID 'Guest users' and directory access is restricted, choose Application scope and ensure that GroupMember.Read.All (Application) and one of either User.Read.All (Application) or User.ReadBasic.All (Application) are enabled for your Enterprise application.

Calendar Permissions

- **Calendars.Read:** This permission enables the app to get Outlook calendar events for upcoming meetings.

Email Permissions

- **Mail.Read:** This permission is required to access users' emails to surface relevant documents during searches. This event will be activated through direct user action (e.g., typing in the Ask and Search bar) or implicit triggers, such as presenting content related to a call, chat, or other activity.

Group Settings Permissions

- **Application.Read.All:** This permission is required to read groups assigned to Onsign NOW as an enterprise application within MS Entra. It allows group settings management within Onsign NOW.

External Connector Permissions

- **ExternalConnector.Read.All:** This permission is required to allow Onsign NOW to query third-party connectors.
- **ExternalItem.Read.All:** This permission is required to allow Onsign NOW to read from third-party connectors.



Tip: When an application registers within an organization's tenant, an Azure administrator must provide consent for applications that require these permissions.

OpenID Connect (OIDC) scopes

- **email:** This permission provides access to the user's email address. Onsign NOW uses it for display purposes and identity federation.
- **offline_access:** This permission allows Onsign NOW to request and use refresh tokens. Refresh tokens enable the app to continue using Microsoft [Application Programming Interface \(API\)](#)s without needing to re-authenticate.
- **openid:** This permission is required for authenticating to Onsign NOW using a [Microsoft Entra ID](#) account. It indicates that Onsign NOW will use [Microsoft Entra ID](#) to sign in.
- **profile:** This permission provides basic user information, such as a user's name.

For a more detailed description of these permissions, please refer to the [Microsoft Graph permissions reference](#) documentation.

2.1.2 Granting Consent to Onsign NOW Permissions

Onsign NOW requires access to Microsoft APIs and services. A [Microsoft Entra ID](#) Tenant administrator must grant several permissions. The recommended permission method is for the admin to grant [Tenant-wide admin consent](#) to Onsign NOW.

A customer [Microsoft Entra ID](#) administrator with permission to grant admin consent to applications on behalf of the organization should perform these actions.

1. Launch Onsignt NOW. Select from:

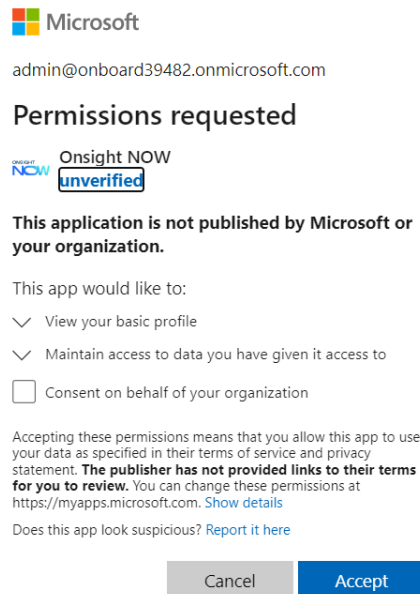
- a. **Public:** <https://app.onsightnow.com>
- b. **US Government:** <https://app.onsightgov.us/>

2. Click the **Sign in with Microsoft** button.

3. Sign in with a Microsoft Admin account for the target

4. *Microsoft Entra ID* tenant.

5. The Onsignt NOW permissions consent screen should display. This lists the permissions required by Onsignt NOW. For example,



a. *Figure 2-1 Onsignt NOW Permission*

6. Select **Consent on behalf of your organization** and click **Accept**.

7. After accepting, login will complete, and you'll be redirected to Onsignt NOW.

8. The Onsignt NOW Entra ID Enterprise Application is now added to your Azure Tenant.

9. Login to your MS Entra ID tenant and assign yourself the Onsignt NOW Super Administrator role. This will allow you to enable permissions from within the Onsignt NOW application.

10. Log out of Onsignt NOW and log back in to apply your role as Onsignt NOW Super Administrator.

11. See **Section 2.3** for applying **Microsoft permissions** within Onsignt NOW.

2.1.3 Assigning Users to Onsignt NOW

You can control access to Onsignt NOW within your organization using [Microsoft Entra enterprise application user assignment](#).

1. Within the **Azure Portal**, navigate to **Microsoft Entra ID > Enterprise Applications**.

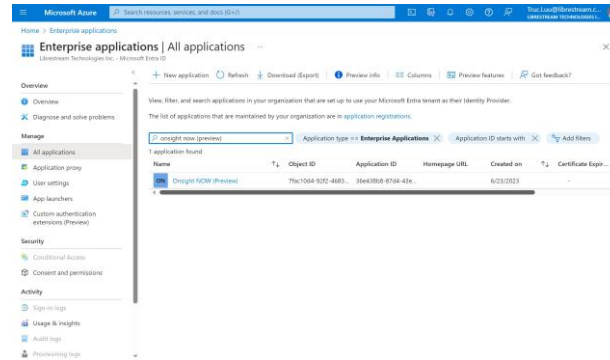


Figure 2-3 Azure Portal

2. Click the Onsignt NOW application and select **Properties**.

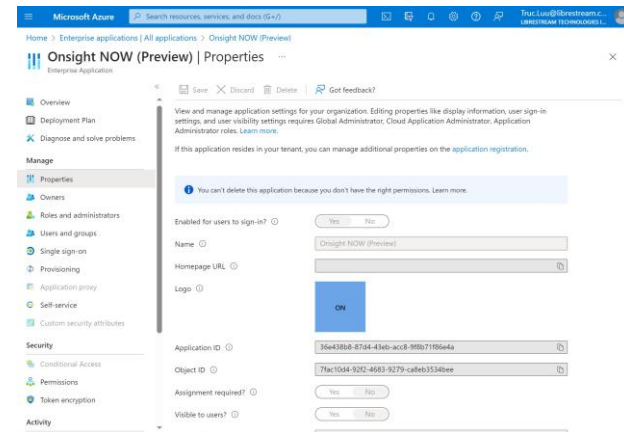


Figure 2-4 Onsignt NOW Properties

3. Locate the **Assignment required** option. Select:
 - **Yes**, to force an administrator to assign users to this application before they can access it.
 - **No**, to allow all users to sign in and access all apps and services by obtaining an access token for this service.



Note: For an application to display within your **My Apps** portal, the user must be assigned as a user or as a member of a group.

4. If **Assignment required** is set to **Yes**, then navigate to the **Add Users & Groups** section to complete the procedure.

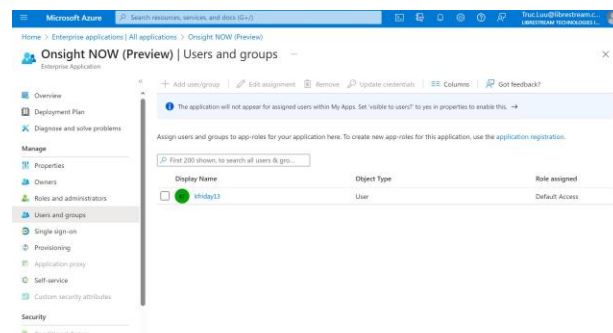


Figure 2-5 Users & Groups

2.2 Add Users and Groups

Assigning Users and Groups is necessary only if the external application properties for **Assignment required** is set to **Yes**. If **Assignment required** is set to **No**, all users will have access to Onsight NOW with the default **User** application role. To change a user's role(s), they must be assigned individually or as part of a group.

Microsoft Entra groups manage users that need the same level of security and access to shared Microsoft resources such as SharePoint. For example, consider using a software security group for developers and a production group for users.

The application owner or a group administrator creates groups. When a tenant is added, Onsight NOW grants all members access, and membership can be assigned within one or more groups to any user from the tenant. Each group has an owner, and the owner can independently assign membership to users.

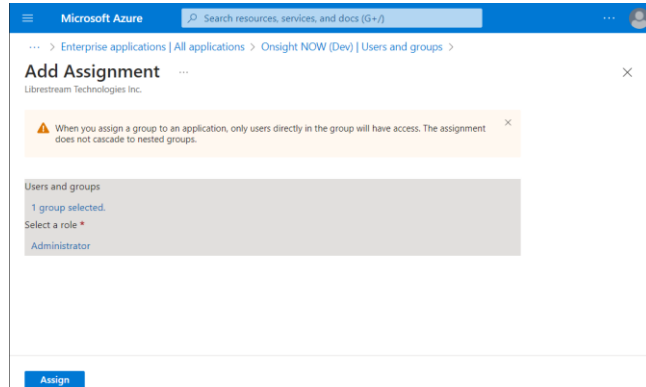


Figure 2-6 Adding a Group



Note: While it's possible to nest groups within groups, permissions do not cascade down, nor do child groups inherit permissions from the parent.



Note: When assigning multiple roles to a user or group e.g. Administrator and Curator, for each role you want to assign you must repeat the process by and add the user or group. E.g. A user would have two entries in the Users and Groups list, one for Administrator and one for Curator.

2.2.1 User Types and Roles

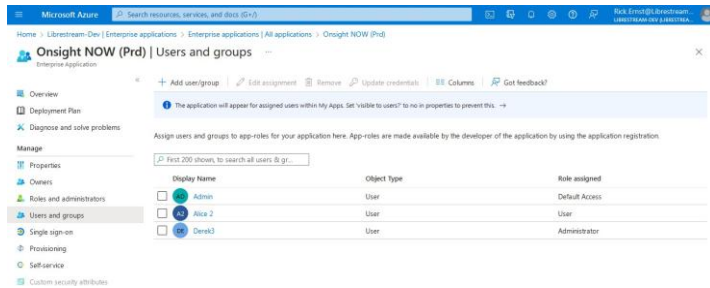


Figure 2-7 User Types & Roles

Azure can assign users with the following Onsight NOW application roles:

- **Super Administrator**¹ – The *Microsoft Entra ID administrator* must be assigned this role in order to change Microsoft Permissions within the app and when using the Divisions feature. This role can configure the tenant and create divisions. See the **Divisions App Note** for more information.
- **Administrator** – The administrator should be assigned this role to give access to privileged operations, such as managing Onsight NOW settings for your tenant. This is the recommended role for administrators who do not have access to the Microsoft Entra ID tenant.
- **User** – Assign the **User** role to limit access and permissions. It assigns standard user permissions.
- **Curator** – The Ida content curator has access to all documents and collections in the tenant for the purposes of evaluating Ida responses. The curator helps Ida refine its response accuracy.

Users not assigned explicitly to the Onsight NOW application will be granted the **User** role. If all users in your Entra ID Tenant are granted use of Onsight NOW, they will only need to be assigned explicitly if you wish to grant the **Super Administrator or Administrator** role.

¹NOTE: As an Entra ID administrator assign yourself the **Super Administrator** role within Onsight NOW so you can access the Settings page within the application and complete the permissions configuration. **Also, assign the Super Administrator role to**

administrators who wish to use the Divisions feature.

2.2.2 Adding a User Group

Onsight NOW must be added as an enterprise application. To add a new user group, you will need to:

- 1. Login to your Azure portal and navigate to your **Microsoft Entra ID** page.

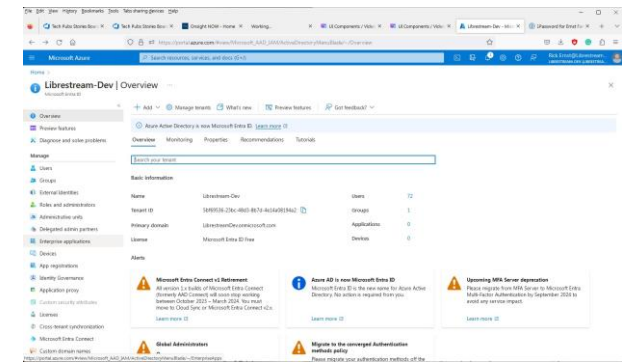


Figure 2-8 Microsoft Entra ID Page

- 2. Locate and select **Enterprise Applications** on the left.

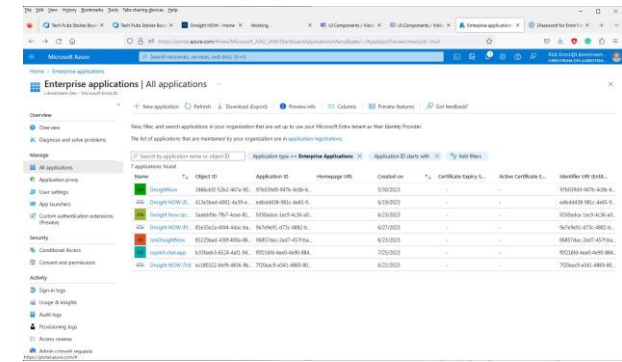


Figure 2-9 Enterprise Applications

- 3. Locate and select your Onsight NOW application from the **All Applications** list. The application Overview page appears.

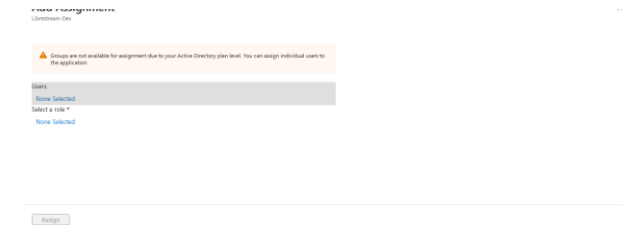


Figure 2-10 Application Overview

- 4. Within the application **Overview** page, locate **Getting Started** and select **1. Assign users and groups**. The **Users and groups** page appears.

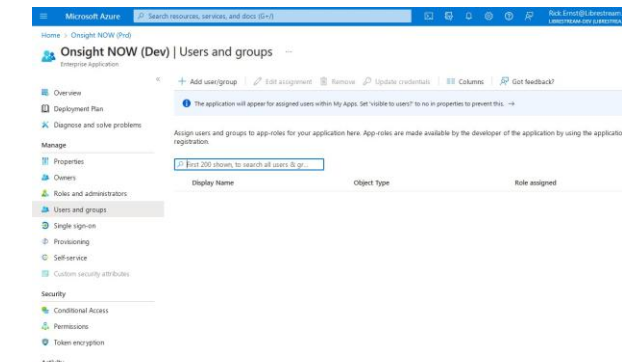


Figure 2-11 Onsight NOW Users and Groups

- Click the **+ Add user/group** tab. The **Add Assignment** page appears.

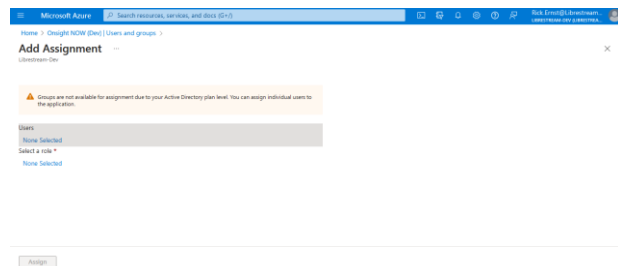


Figure 2-12 Add Assignment Page

- Locate **Users and groups** and click the **None Selected** link. The **Users and groups** pop-up appears.

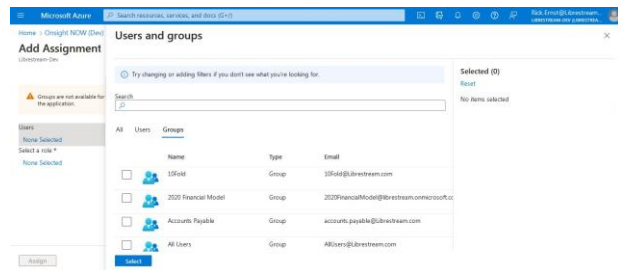


Figure 2-13 Adding a User

- Click to enable the check box next to a username or group within the list.

Tip: Consider entering text within the **Search** field to locate a specific user or group. Click the **Users** or **Groups** tab to refine your selection options.

- Click **Select** to activate the user or group. The **Add Assignment** page updates for Users.

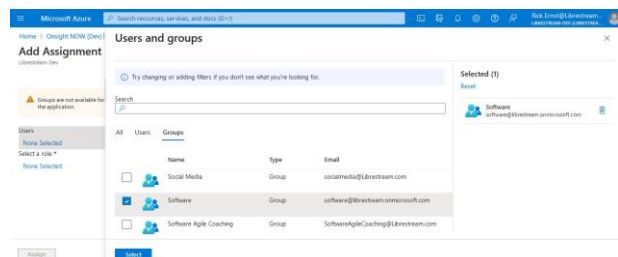


Figure 2-14 Add Assignment

- Locate **Select a role** and click the **None Selected** link. The **Select a role** popup appears.

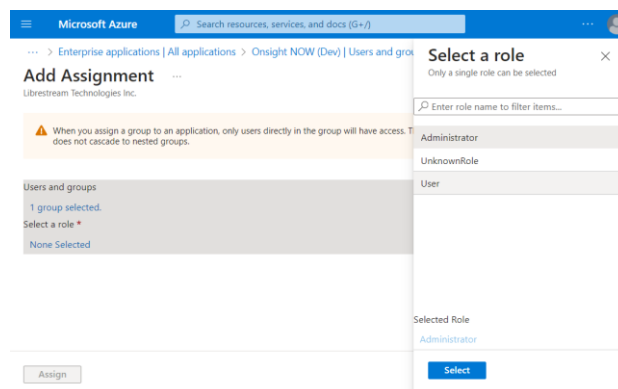


Figure 2-15 Select a Role

10. Choose a role to assign to the selected users and/or groups. For example, select Administrator or User and click **Select** to activate the role.

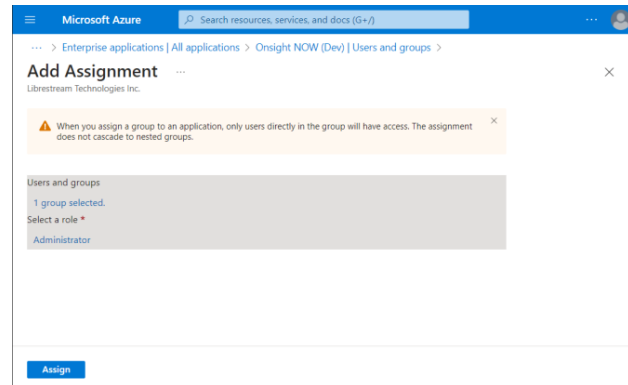


Figure 2-16 Select a Role

11. Click **Assign** to finalize user and group assignment.

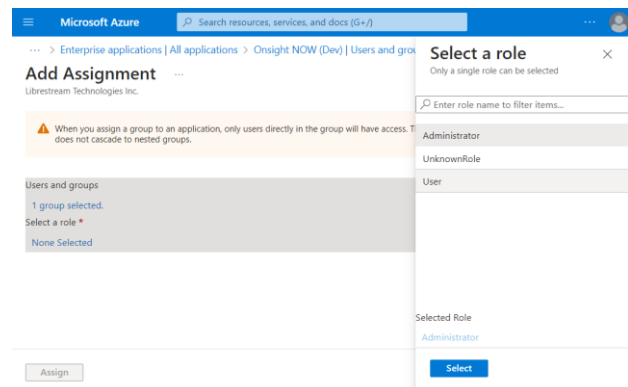


Figure 2-17 Finalize User & Group Assignment

12. The Users and groups page reappears with a message stating Application assignment succeeded.

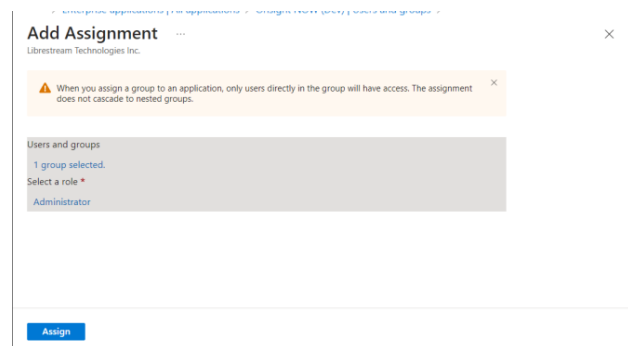



Figure 2-18 Finalize User & Role Assignment

13. You must log out and log in to Onsight NOW to see the role change in affect. This completes the procedure.

2.3 External Users

External users are necessary to support different partnerships, parts suppliers, inspections, etc. An administrator must log in to their Azure tenant and invite external users to support people outside their organization.


The recipient must accept the invitation, sign in to the target tenant, and log in using Microsoft's login process like any other user. Once an external user logs in, they can access Onsite NOW and any shared Microsoft resources to which they've been authorized. Shared resources include SharePoint drives, collections, contacts, roles, and assignments. Additionally, external users can upload, download files, create meetings, and send invitations to join them.

 **Note:** If allowed, any user can invite people outside their organization to use Onsite NOW as a guest. External users must log in using their credentials to access Onsite NOW. In contrast, guest users don't need to log in but have limited access to Onsite NOW functionality and cannot access shared Microsoft resources.


2.3.1 Inviting External Users Using Microsoft Entra ID

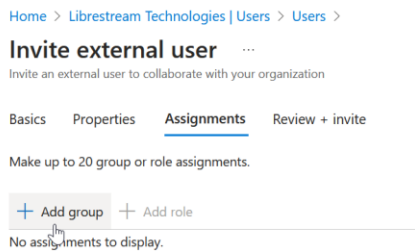
To invite an external user through [Microsoft Entra ID](#), an administrator will need to:

1. Log in to the Azure portal.
2. Click **Users > New User** and choose **Invite external user** from the drop-down menu.
3. Provide an email address for the external user.
4. Enter information within the **Given Name**, **Surname**, and **Display Name** as these properties will be used within Onsite NOW. Enter more information as necessary.

 **Tip:** To ensure you receive a copy of the email, you may also use the carbon copy (cc:) option.

5. Click **Invite** to continue.
6. Click **Review + Invite** to finalize and send.
7. When you invite an external user, a message stating: "User invitation in progress" will appear. An email invitation will automatically be sent to the newly added external user.
8. This completes the procedure.

 **Note:** In the **Invite external user** page, you may also use the 'Add Group' button on the Assignments tab to assign the application to an external group. As seen below:



2.3.2 Signing Into a Different Organization as an External User

An admin must set up the account for the external user in advance, and the tenant will automatically send an email invitation to the external user.

Advise the external user that they will receive an email invitation and will need to:

1. Click the **Accept invitation** link.
2. Launch a web browser and enter the Onsite NOW URL. For example, `app.onsightnow.com`
3. Choose the **Sign in using a different organization** link.
4. Enter the organization's name and click the **Sign in with Microsoft** button.
 - a. If prompted, pick an account to use for login.
 - b. Follow any prompts to complete the Microsoft login process.
5. The external user will be redirected to the Onsite NOW Home page.
6. This completes the procedure.

3 Organization Settings

The Organization settings allow you to configure the Microsoft permissions required for the application, upload licenses and manage license pools, and manage divisions.

3.1 Microsoft Permissions

The super administrator must configure and grant admin consent for the Microsoft permissions needed based on the features they wish to use. This requires that the previous sections have been completed and that the user:

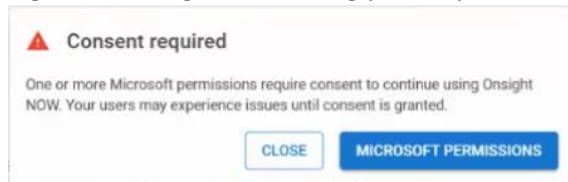
- Is assigned the Super Administrator Onsign NOW app role so they can access tenant settings.
- Has privileges in Entra to grant consent for user delegated permissions for their organization.

Once admin consent is granted for the chosen permissions, users will not see a Microsoft consent prompt when signing in. This is a one-time operation unless an IT administrator subsequently wants to change their permissions.

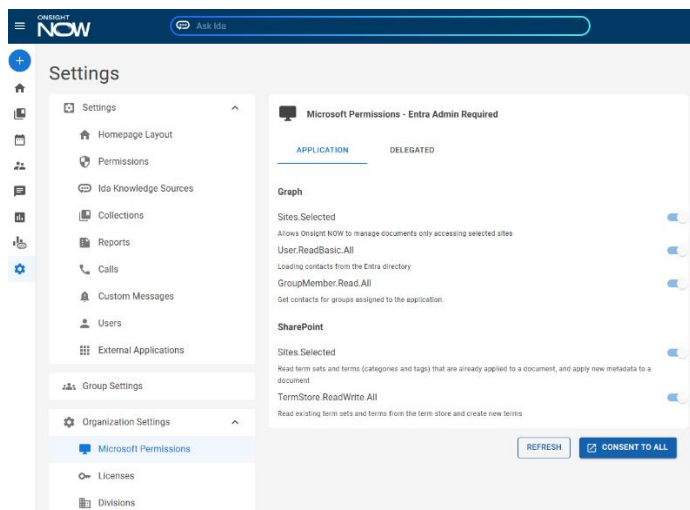
Until this step is performed, users in the tenant will not have access to calendar, contacts, files on SharePoint, email search, etc.

3.1.1 Consent to Permissions

1. Sign-in to Onsign NOW using your Super Administrator account. You will see this notification.

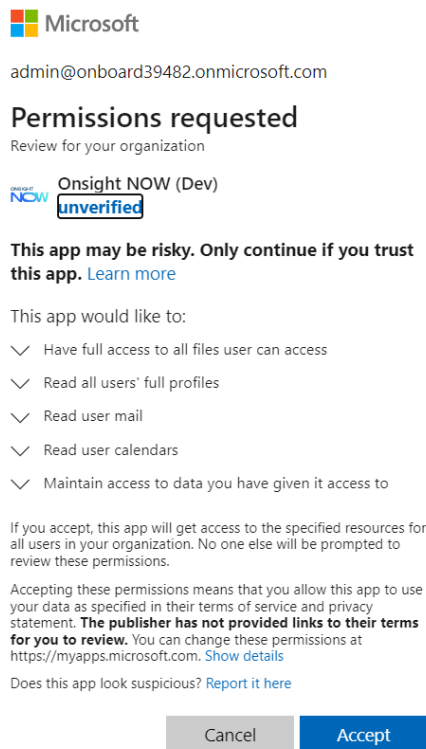


2. Open the Settings page and go to Settings – Organization Settings - Microsoft Permissions.

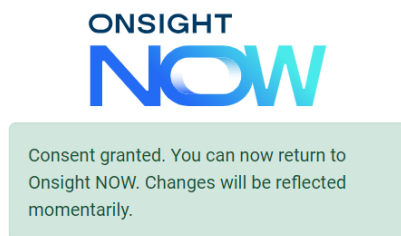


3. On the APPLICATION tab, click CONSENT TO ALL. A new tab will open prompting you to consent for your organization. After completing this you can return to the app. You can click refresh to view the updated state of the application permissions in Onsign NOW (**IMPORTANT:** These changes may take up to 5 minutes for their state to update).
 - a. **IMPORTANT:** All Application permissions must be consented to initially, if required, after the initial consent is granted you can revoke specific Application permissions from within Entra.

4. Click on the DELEGATED tab. Select the permissions that you want to grant use of (Review section [2.1.1](#) for additional details). Once your required permissions are selected, click CONSENT. A new tab will open prompting you to consent to these permissions for your organization. After completing this you can return to the app. It may take up to a minute for these changes to take effect
 - i. **IMPORTANT:** Refer to section [4.12.1](#) to complete the Sites.Selected permission setup by a SharePoint administrator.
5. Click Consent to open the Microsoft application consent page in a new browser tab. The chosen permissions should be listed and explained.



6. After clicking **Accept**, they will be returned to a status page confirming the permissions are available. They may close this tab and return to Onsite NOW.



7. The features that depend on those permissions should now be shown and available.

3.1.2 Revoking Permissions

This section describes the process the customer administrator would follow to disable and revoke consent for one or more Microsoft permissions. This requires that the previous sections have been completed and that the user:

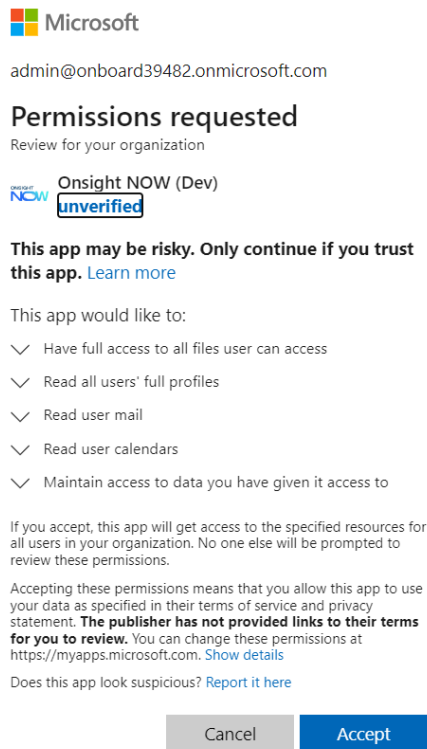
- Is assigned the Administrator Onsite NOW app role so they can access tenant settings.
- Has privileges in Entra ID to grant consent for user delegated permissions for their organization.

This process has two steps:

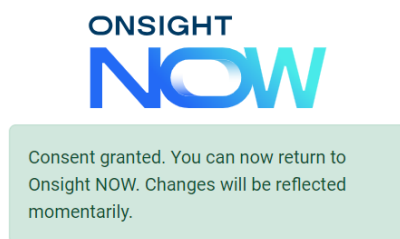
- Disabling the permission in Onsite NOW.
- Revoking the permission in Microsoft Entra ID.

3.1.3 Disabling Permissions in Onsite NOW

1. Sign-in to Onsite NOW as an Administrator.
2. Go to the Settings -> Microsoft Permissions page.
3. Disable one or more optional permissions. For example, Mail.Read.
4. Click Consent to open the Microsoft application consent page in a new browser tab. The chosen permissions should be listed and explained.



5. After clicking **Accept**, you will be returned to a status page confirming the permissions are available. You may close this tab and return to Onsite NOW.



6. The Onsite NOW functionality depending on the disabled permission(s) should now be disabled or hidden.

3.1.4 Revoking Permissions in Entra ID

After following the steps in ‘Disabling Permissions in Onsign NOW’, the app will no longer request disabled permissions. Customers should also revoke the consent in Entra so they are ensured Onsign NOW can no longer access those resources.

NOTE: The customer administrator MUST disable the permission(s) in Onsign NOW following the previous section first before revoking permissions in Entra. Otherwise, they may not have access to Microsoft resources and will need to repeat the ‘Microsoft Permissions ’ section.

To revoke permissions an Entra ID administrator must complete these steps.

1. Login to your enterprise’s Azure Portal
2. Go to Enterprise Applications -> Onsign NOW -> Permissions.
3. Select the ‘...’ menu next to the permission(s) disabled in ‘Disabling Permissions in Onsign NOW’ and select

Revoke Permission.

Onsign NOW (Dev) | Permissions

Overview, Deployment Plan, Diagnose and solve problems, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Self-service, Custom security attributes, Security, Conditional Access, Permissions, Token encryption, Activity, Sign-in logs, Usage & insights, Audit logs

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). [Learn more.](#)

You can review, revoke, and restore permissions. [Learn more.](#)

Grant admin consent for Onboard 39482

Admin consent | User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by	
Microsoft Graph						
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 yo...	Delegated	Admin consent	An administrator	...
Microsoft Graph	Files.ReadWrite.All	Have full access to all files ...	Delegated	Admin consent	An administrator	...
Microsoft Graph	People.Read	Read users' relevant peopl...	Delegated	Admin consent	An administrator	...
Microsoft Graph	Mail.Read	Read user mail	Delegated	Admin consent	An administrator	...
Microsoft Graph	Calendars.Read	Read user calendars	Delegated	Admin consent	An administrator	...
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator	...

3.2 External Users

External users are necessary to support different partnerships, parts suppliers, inspections, etc. An administrator must log in to their Azure tenant and invite external users to support people outside their organization.

The recipient must accept the invitation, sign in to the target tenant, and log in using Microsoft's login process like any other user. Once an external user logs in, they can access Onsign NOW and any shared Microsoft resources to which they've been authorized. Shared resources include SharePoint drives, collections, contacts, roles, and assignments. Additionally, external users can upload, download files, create meetings, and send invitations to join them.

Note: If allowed, any user can invite people outside their organization to use Onsign NOW as a guest. External users must log in using their credentials to access Onsign NOW. In contrast, guest users don't need to log in but have limited access to Onsign NOW functionality and cannot access shared Microsoft resources.

3.2.1 Inviting External Users Using Microsoft Entra ID

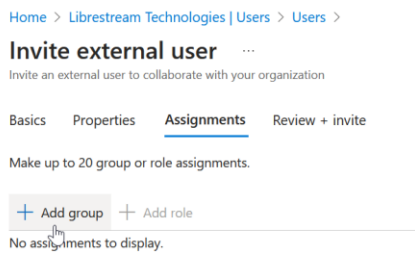
To invite an external user through [Microsoft Entra ID](#), an administrator will need to:

9. Log in to the Azure portal.
10. Click **Users > New User** and choose **Invite external user** from the drop-down menu.
11. Provide an email address for the external user.
12. Enter information within the **Given Name**, **Surname**, and **Display Name** as these properties will be used within Onsight NOW. Enter more information as necessary.

Tip: To ensure you receive a copy of the email, you may also use the carbon copy (cc:) option.

13. Click **Invite** to continue.
14. Click **Review + Invite** to finalize and send.
15. When you invite an external user, a message stating: "User invitation in progress" will appear. An email invitation will automatically be sent to the newly added external user.
16. This completes the procedure.

Note: In the **Invite external user** page, you may also use the 'Add Group' button on the Assignments tab to assign the application to an external group. As seen below:



3.2.2 Signing Into a Different Organization as an External User

An admin must set up the account for the external user in advance, and the tenant will automatically send an email invitation to the external user.

Advise the external user that they will receive an email invitation and will need to:

7. Click the **Accept invitation** link.
8. Launch a web browser and enter the Onsight NOW URL. For example, `app.onsightnow.com`
9. Choose the **Sign in using a different organization** link.
10. Enter the organization's name and click the **Sign in with Microsoft** button.
 - a. If prompted, pick an account to use for login.
 - b. Follow any prompts to complete the Microsoft login process.
11. The external user will be redirected to the Onsight NOW Home page.
12. This completes the procedure.

4 Organization Settings

The Organization settings allow you to configure the Microsoft permissions required for the application, upload licenses and manage license pools, and manage divisions.

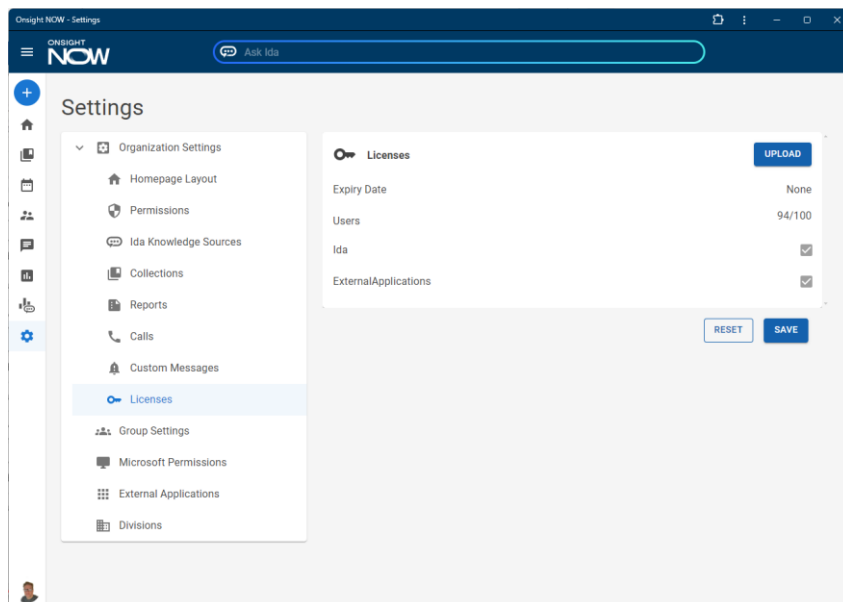
Microsoft Permissions

4.1 Licenses

The Licenses page is where you upload the license file for your organization. It also indicates the expiry date for the licenses, and which extended features have been enabled for your organization.

New customers (and newly created divisions) will automatically have a 90-day expiry date applied to their tenant. This will allow sufficient time to get license files from Librestream and upload them to your organization. License files will be supplied as part of the onboarding process.

Once you've received your license file from Librestream press the UPLOAD button and select it from your file system. The licenses will be added to the tenant and the number of licenses will be displayed along with the Expiry Date.



4.2 Divisions

Divisions can be created to provide multi-tenancy for self-hosted (on-premises) environments. Most SaaS customers will not need Divisions. Divisions can be considered independent tenants. License pools can be created for the purpose of managing the number of licenses allocated to each division.

Please Refer to the OnSight NOW Divisions App Note for more information.

5 Settings

Onsight NOW administrators can access application setting options by clicking the **Settings** within the **Navigation** bar. Application setting options allow an administrator to display and manage settings for:

- **Homepage Layout**
- **Permissions**
- **Ida Knowledge Sources**
- **Collections**
- **Reports**
- **Calls**
- **Custom Messages**
- **Users**
- **External Applications**

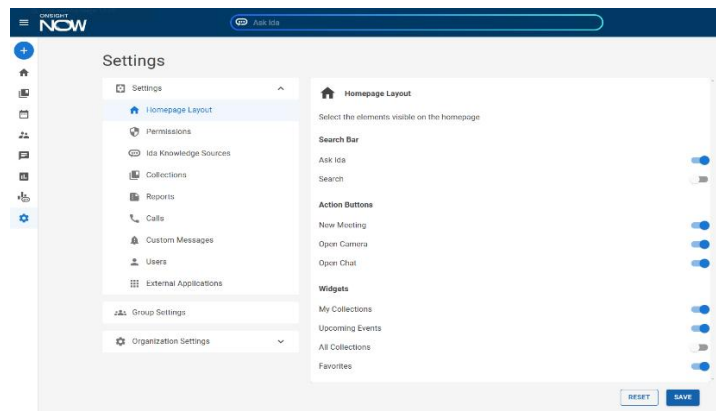


Figure 4-1 Settings

Click a category within **Settings** on the left-side pane to reveal all corresponding settings on the right.

5.1 Homepage Layout

Click **Settings > Homepage Layout** to customize the layout for all users within an organization. The Homepage layout allows an administrator to enable options that activate key features from the Homepage including actions and widgets.

Use this section to control which elements appear on the Homepage Layout.

Click to **Enable** only those elements to display.

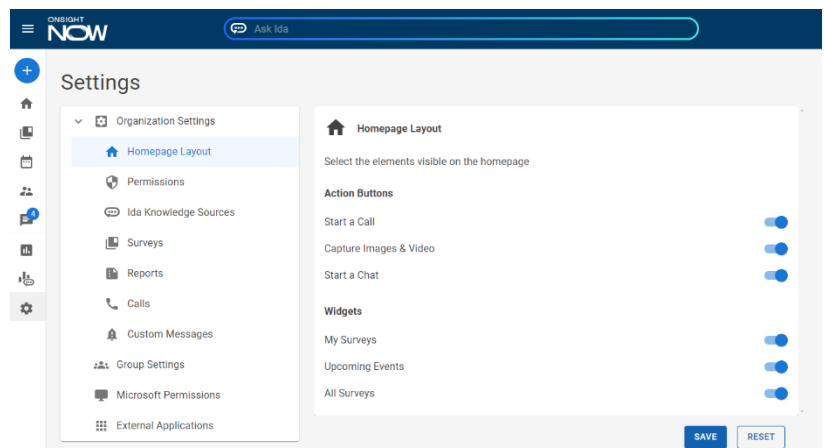


Figure 4-6 Organization Settings — Homepage Layout

Choose from:

Action Buttons

Users within your organization can use this section to control the permitted actions. Click to **Enable** only those elements to display. Choose from:

- **Start a Call** — When enabled, users can call using Onsight NOW.
- **Capture Images & Video** — When enabled, users can capture images and video.
- **Start a chat** — When enabled, users can send messages via chat.

Widgets

Widgets allow an administrator to control which sections appear on the Homepage. Choose from:

- **My collections** — Enable to display the user's collections.

- **Upcoming Events** — Enable to display future events.
- **All Collections** — Enable to display all collections.

Settings can be assigned differently to mobile and desktop users. Enable **Mobile** to apply setting changes to cell phone users. Enable **Desktop** to apply setting changes to personal computer (PC) and tablet users.

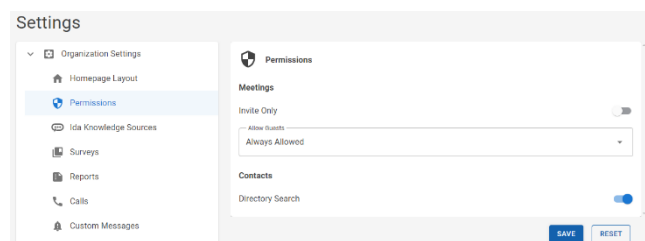
Click **SAVE** to display these changes immediately within the application. Click **RESET** to revert to the default home page layout.

5.2 Permissions

5.2.1 Meetings

Click **Settings > Permissions > Invite Only**. Enable this option to only allow invitees to attend scheduled meetings. Only contacts from the directory and included in the original invite can attend. (Guests and sharing of the meeting link are not allowed.)

Click **Settings > Permissions** to **Allow Guests**. Enable this option to allow guests to attend calls. Disable this option to prevent guests from joining calls.



There are 4 options:

1. Never Allowed – users cannot invite guests.
2. Always Allowed – users can invite guests.
3. Default Allowed – users have the option to invite guests and the default setting for the meeting is 'guests allowed'.
4. Default Not Allowed - users have the option to invite guests but the default setting for the meeting is 'guests not allowed'.

5.2.2 Contacts

Contacts displays the system level contacts from your Entra directory.

Click **Settings > Permissions > Directory Search**. Enable this to allow users to search the full directory.

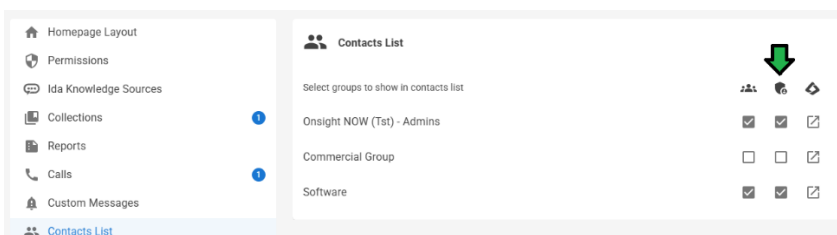
Click **SAVE** to finalize all changes. Click **RESET** to restore all default settings.

5.2.3 Guest Contacts

If **Allow Guests** is enabled, the personal guest contact list is enabled by default. This allows users to keep a personal list of frequently invited guests.

When enabled, guests can be added to a user's personal contact list or to a group contact list. The group contact list is shared by all group members. The group contact list is for use cases such as Support or Call Centers for sharing guest contacts between agents.

To enable the sharing of a guest contact list on a group basis (e.g. for the Call Center use case) go to **Settings – Group Settings**, select a group to edit. Go to **Contacts List** and enable the Guest Contacts list checkbox beside the groups for which you want a shared contact list. Selecting multiple groups will share the guest contact list between the groups.



Click **SAVE** to finalize all changes. Click **CANCEL** to revert to the previous settings.

5.3 Ida Knowledge Sources

Onsight NOW uses a chatbot called the *Industrial Digital Assistant (Ida)*. Ida utilizes *Azure AI Search* and an Azure storage account to provide this functionality. The customer can host this information using SharePoint or their Azure storage *Binary Large Object (BLOB)*, or Librestream can host this information segregated by tenant.

To choose which sources Ida references when responding, click **Settings > Ida Knowledge Sources** to enable the Ida knowledge sources. You can use Chats, Calls, Collections, Collection Files, Images, and Documents.

Note: Guest contacts are exclusively used when scheduling meetings by sending guest invites. Guests cannot be called directly.

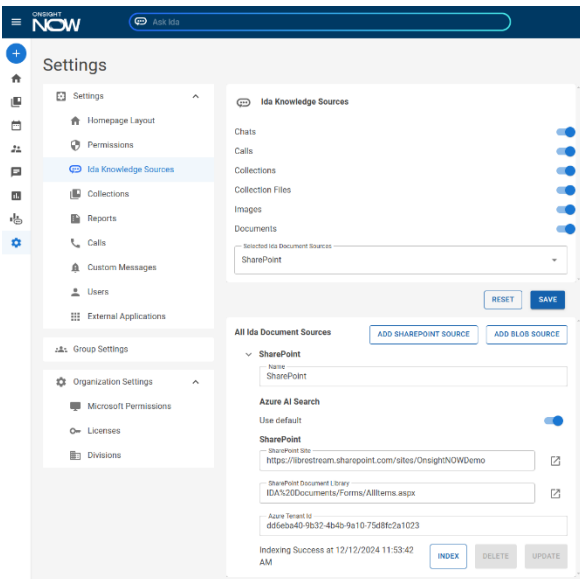



Figure 4-3 Settings — Ida Knowledge Sources

5.3.1 Add SharePoint Source

Click the ADD SHAREPOINT SOURCE button and enter the following information:

1. **Name** – Enter a name for your SharePoint source. Give meaningful names so that you can understand how they're used. E.g. 'Field Service Ida Documents'.
2. **Azure AI Search** — Leave as 'Use Default' unless you want to use host your own Azure AI Search index. 'Use Default' will store the Ida document index in Librestream's Azure AI Search. If hosting your own Azure AI Search engine, an administrator must enable this service by entering the **Endpoint** (URL) and **Key** parameter credentials.
3. **SharePoint** - An administrator can enable this service by entering the **SharePoint Site** (URL), **SharePoint Document Library** and **Azure Tenant ID** parameter credentials. Press **SAVE**.
4. **Index** – Once the credentials have been saved, press INDEX to manually start the indexing of the Site.
5. **Indexing Success** represents the most recent date and time the indexing routine ran.
6. **Selected Ida Document Sources** – this drop down allows you to set which Ida Knowledge Sources will be referenced for the Organization or Groups. To set the Ida Document Source for a group go to Group Settings.

 **Tip:** After adding new documents to the Azure Storage Account, the administrator can force the index to regenerate by clicking the **INDEX** button.

Click **SAVE** to finalize all changes. Click **RESET** to restore all default settings.
See Section 4.8 for additional information on setting up Ida Knowledge Sources.

5.3.2 Add Azure Storage BLOB Source

Click the ADD BLOB SOURCE button and enter the following information:


1. **Name** – Enter a name for your SharePoint source. Give meaningful names so that you can understand how they're used. E.g. 'Field Service Ida Documents'.
2. **Azure AI Search** — Leave as 'Use Default' unless you want to use host your own Azure AI Search index. 'Use Default' will store the Ida document index in Librestream's Azure AI Search. If hosting your own Azure AI Search engine, an administrator must enable this service by entering the **Endpoint** (URL) and **Key** parameter credentials.
3. **Azure Storage Account** - An administrator can enable this service by entering the **Document Container Name** (URL) and **Connection String** credentials. Press **SAVE**.
4. **Index** – Once the credentials have been saved, press INDEX to manually start the indexing of the Storage.
5. **Indexing Success** represents the most recent date and time the indexing routine ran.

5.3.3 Supported Document Types for Indexing

Indexing for Ida can support the following document types:

- Portable Document Format (PDF)
- Plain text files

5.4 Collections

Collections group content related to a specific industrial workplace function or task, such as documents, emails, photos,  Onsite NOW embraces flexibility by allowing organizations to use appropriate labels that fit their use case. For example, a support organization may want to use "cases" or "tickets", whereas an inspection company may prefer "inspections".

Click **Settings > Collections** to define collection and SharePoint options. Administrators can:

1. Auto Tag Images – enables computer vision processing to auto tag images with detected objects and text.
2. Enable GPS location on images – when enabled location is included with saved images.
3. Select a **Collections Label Descriptor** from the drop-down menu that includes the following options:

- Cases
- Collections
- Tickets

- Inspections
- Surveys

Tip: The **Label Descriptor** drop-down will replace all references to collections within the User Interface when referring to the Librestream Collections feature.

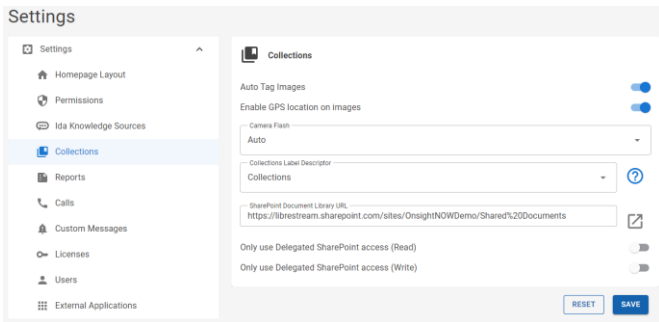


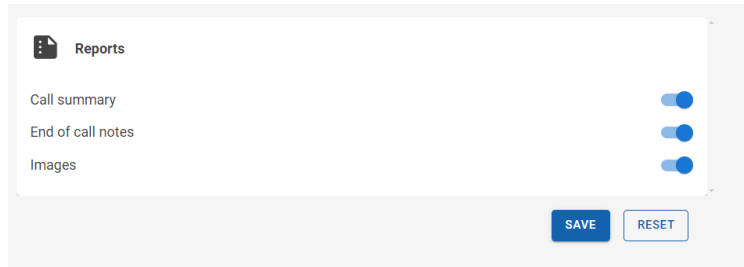
Figure 4-2 Application Settings — Collections


4. Specify a **SharePoint Document Library URL**
 — All content at this level and below is accessible by `username/collections`, and anyone invited to participate in the meeting has read/write permissions to add to the collection. See [Section 4.7](#) for more information on setting up the SharePoint directory for Collections.
5. Enable 'Only use Delegated SharePoint access (Read)' if you only want Standard users to be able to Read content from Collections to which they have permission. For example, an Entra External user joining a meeting would not be able to open images or recording from a collection if this is enabled. If disabled, then Read access via the application token is allowed and an External user who does not have direct SharePoint access, will be able to view thumbnails, images and documents in collections that are shared with them. Otherwise, they will not be able to view those items.
6. Enable 'Only use Delegated SharePoint access (Write)' if you only want Standard users to be able to Write content to Collections to which they have permission. For example, an Entra External user joining a meeting would not be able to capture or record video if this is enabled. If disabled, then Write access via the application token is allowed and an External user who does not have direct SharePoint access, will be able to upload images/files, and rename or delete images/files in collections that are shared with them. Otherwise, those operations will be denied.
7. Click **SAVE** to finalize all changes. Click **RESET** to return to previous settings.

5.5 Reports

Use the following settings to define which items are included in Collection generated reports. Note that the following settings must be enabled prior to including them in the generated reports:

- 'Calls - End of call notes'
- 'Calls - Call Transcription – Summarization'
- Images



 **Tip:** Press the Generate Report button in a collection to export a pdf of the collection.

5.6 Calls

Click **Settings > Calls** to enable the following capabilities:

- **Team Ad Hoc Calling** — Enables users to call Microsoft Teams contacts directly and call into a Teams meeting using Onsignt NOW.
- **End of Call notes** — Enables the ability to add Call notes after the call has ended.
- **Captions** — Enables Onsignt NOW to generate closed captions for audio in real-time using the language spoken by the participants in the meeting.
- **Translation** — Allows users to view captions in another language if it is different from the system call language.
- **Per-user spoken language** – Allows users to speak in a language that is different from the system call language.
- **System Call Language** – Captions, transcripts, and summaries will be generated in this language for all calls and meetings.
- **Recording** – Allows users to record calls or meetings.
- **Transcription** — Enables Onsignt NOW to transcribe all dialogue from the call as defined by the **Closed Captions > System Call Language** drop-down menu.
- **Summarization**— Enables Onsignt NOW to use transcription to generate a call summary.

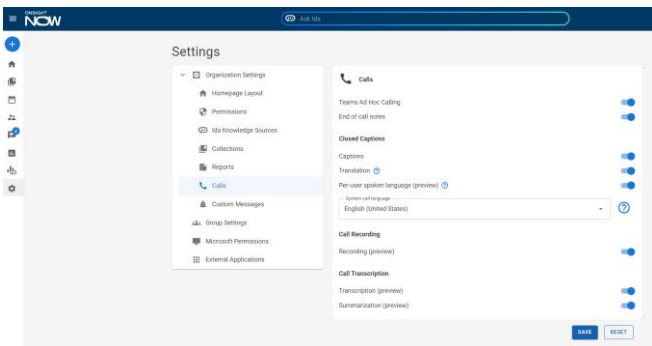




Figure 4-4 Application Settings — Calls


 **Note:** Transcription, translation, summarization, and captions are closely related functions.


1. When enabled, transcription, translation, and summarization will automatically use the **System Call Language** setting as the input language.

2. Summarization is supported for the following languages: Chinese-Simplified, English, French, German, Hebrew, Italian, Japanese, Korean, Polish, Portuguese and Spanish. For the most up-to-date information, please refer to [Language Support for Document & Conversation Summarization](#).
3. [Azure Government Cloud \(GC\)](#) and On-premises installations do NOT support call transcription and summarization.

- **End of call notes** — This option allows one user at a time to create, edit, and save a note from a call. When a user edits a note, the note turns blue and locks for all other users to prevent further editing. Click the **Edit Note**  icon to enter and modify notes as text.

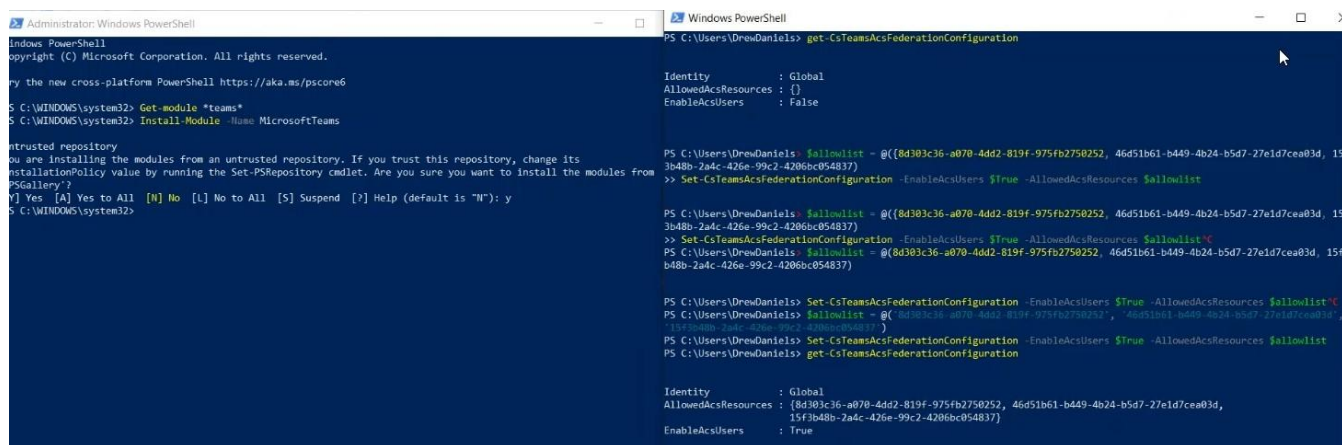
 **Tip:** The note will remain locked until the user clicks **SUBMIT** or **DISMISS**. There is a five-second delay before the note unlocks, and it's available for further edits.

 **Note:** For more information on enabling Teams calling and chat interoperability, please refer to Microsoft's [Teams Interoperability: Calling and chat > 3. Enable tenant configuration](#). Provide the **ACS Immutable ID**, which is 15f3b48b-2a4c-426e-99c2-4206bc054837.

 **Tip:** The ACS Immutable ID is called `IMMUTABLE_RESOURCE_ID` in the Microsoft document.

Click **SAVE** to finalize all changes. Click **RESET** to restore all default settings.

5.6.1 Tenant Setup for Teams Ad Hoc Calling via PowerShell & ACS Immutable ID



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Get-Module *teams*
PS C:\WINDOWS\system32> Install-Module -Name MicrosoftTeams

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
PSGallery?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\WINDOWS\system32>

PS C:\Users\DrewDaniels> get-CsTeamsAcsFederationConfiguration
Identity : Global
AllowedAcsResources : {}
EnableAcsUsers : False

PS C:\Users\DrewDaniels> $allowlist = @((8d303c36-a070-4dd2-819f-975fb2750252, 46d51b61-b449-4b24-b5d7-27e1d7cea03d, 15f3b48b-2a4c-426e-99c2-4206bc054837)
>> Set-CsTeamsAcsFederationConfiguration -EnableAcsUsers $true -AllowedAcsResources $allowlist

PS C:\Users\DrewDaniels> $allowlist = @((8d303c36-a070-4dd2-819f-975fb2750252, 46d51b61-b449-4b24-b5d7-27e1d7cea03d, 15f3b48b-2a4c-426e-99c2-4206bc054837)
>> Set-CsTeamsAcsFederationConfiguration -EnableAcsUsers $true -AllowedAcsResources $allowlist

PS C:\Users\DrewDaniels> $allowlist = @((8d303c36-a070-4dd2-819f-975fb2750252, 46d51b61-b449-4b24-b5d7-27e1d7cea03d, 15f3b48b-2a4c-426e-99c2-4206bc054837)
>> Set-CsTeamsAcsFederationConfiguration -EnableAcsUsers $true -AllowedAcsResources $allowlist

PS C:\Users\DrewDaniels> get-CsTeamsAcsFederationConfiguration
Identity : Global
AllowedAcsResources : {8d303c36-a070-4dd2-819f-975fb2750252, 46d51b61-b449-4b24-b5d7-27e1d7cea03d, 15f3b48b-2a4c-426e-99c2-4206bc054837}
EnableAcsUsers : True
  
```

Figure 4-5 PowerShell & ACS Immutable ID

The administrator will need to run a series of commands in PowerShell.

1. Run the following commands:
 - `Get-Module *teams*`
 - `Install-Module -Name MicrosoftTeams`
2. Connect to the tenant using `Connect-MicrosoftTeams` and log in using the credentials.
3. Use the `get-CsTeamsAcsFederationConfiguration` to verify the following settings:
 - Identity: Global
 - AllowedAcsResources: {}
 - EnableAcsUsers: False



Note: These results verify that Onsignt NOW is disabled and unable to call.

4. Utilize the `Set-CsTeamsAcsFederationConfiguration` to enable ACS users as `$True` and `$allowlist`

5. Run `get-CsTeamsAcsFederationConfiguration` again and confirm that:

- Identity: Global
- AllowedACSResources: {Series of numbers and the ACS Immutable ID: 15f3b48b-2a4c-426e-99c2-4206bc054837}
- EnableACSUsers: True

For more information on enabling Teams calling and chat interoperability, please refer to Microsoft's [Teams Interoperability: Calling and chat > 3. Enable tenant configuration](#). Provide the **ACS Immutable ID**, which is 15f3b48b-2a4c-426e-99c2-4206bc054837.

5.6.2 Teams Ad Hoc Calling – Microsoft Teams Phone License Assignment

For Teams Ad Hoc calling you must assign Microsoft Teams Phone license, follow these steps:

1. Assign a Microsoft Teams Phone Standard license to Teams identity of the user(s).
2. Using PowerShell run the following command:

```
Set-CsPhoneNumberAssignment -Identity <String> -EnterpriseVoiceEnabled <Boolean>
```

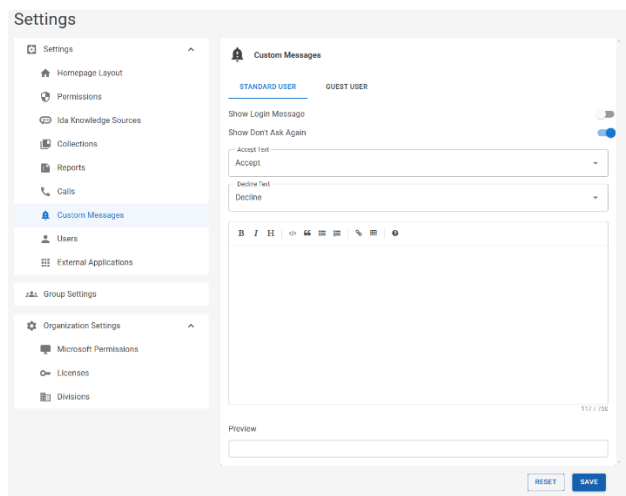
For further details refer to the Microsoft documentation:

- <https://learn.microsoft.com/en-us/microsoftteams/setting-up-your-phone-system>
- <https://learn.microsoft.com/en-us/powershell/module/teams/set-csphonenumassignment?view=teams-ps>

5.7 Custom Messages

Add and manage custom messages that users will see at login. These messages can be an effective way to communicate important information such as terms and conditions, updates, or alerts directly to users as they access the system. If enabled the message will be shown immediately after login. You can give the option to the user to select 'Don't Ask Again'. And you may pick the text used on the message buttons so that they match the intent of the message. Use Markdown language to format your messages. Custom Messages are supported for both Standard and Guest users.

Note that users will be logged out of the application if they press Decline, Cancel, or Log Out. The intent of this behaviour is to ensure the user accepts the conditions before using the application.



5.8 Users

The Users page lists all users who have been assigned the application. The administrator can Activate/Inactive licenses for each user from this page.

5.9 Group Settings

Groups in Entra (Azure) serve as a method for managing user roles and permissions. Within Entra, administrators manage group memberships by assigning users to appropriate groups.

Within Entra, groups are assigned to specific enterprise applications, like Onsight NOW, to manage application settings and permissions. Using Entra groups provides a flexible yet controlled environment where group-specific settings enhance the functionality and security of enterprise applications. Onsight NOW uses the defined Entra group membership to control user access and settings. Assigning Onsight NOW to Entra groups is discussed in [section 2.1.5](#).

Within Onsight NOW, groups can have specific settings applied to them. These settings are configured allowing for tailored functionality for each group.

To apply groups settings the following Microsoft Permissions must be enabled within Onsight NOW:

Group Settings

Application.Read.All

Read groups assigned to the application for Group Settings management

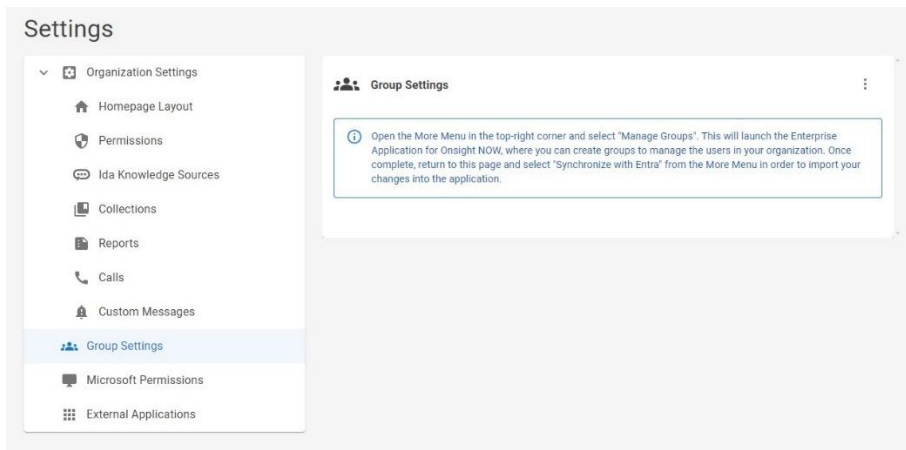
GroupMember.Read.All

Get contacts for groups assigned to the application

5.9.1 Entra Group Synchronization

Entra groups must be synchronized with Onsight NOW using the synchronization feature that updates group membership data from within Onsight NOW. This ensures that only relevant groups are considered when users log in, based on their Entra group memberships. Press 'Synchronize with Entra' to import the groups into Onsight NOW. After synchronization is completed all Entra groups that were assigned Onsight NOW as an enterprise application will appear in the group list.

If you haven't previously synchronized with Entra you'll be prompted to complete the following steps (Note: this will only be visible for Onsight NOW admins with Entra admin permissions):





1. Click on the more menu (...) in the top-right corner.
2. Select "Manage Groups".
3. You will be directed to the Enterprise Application for Onsite NOW in Entra.
4. If necessary, create groups to manage your organization's users and assign Onsite NOW to the groups.
5. Return to Onsite NOW.
6. Click on the More Menu and select "Synchronize with Entra".
7. This step imports your groups into the application.

You are now ready to assign group settings within Onsite NOW.

5.9.1.1 Assigning Setting to Groups

Administrators can view and change settings directly from the Group Settings interface. If settings are not assigned to a group, the group will inherit the default 'Using Organization Settings'.

1. Go to Settings - Group Settings. 
2. Press the edit button beside the group name.
3. Select each checkbox beside the setting you wish to customize for the group.
 - 3.1. Homepage Layout
 - 3.1.1. Action Buttons – Start a Call, Capture Images & Video, Start a Chat.
 - 3.1.2. Widgets – My Collections, Upcoming Events, All Collections
 - 3.2. Ida Knowledge Sources
 - 3.2.1. Set the sources you want Ida to use as a source of information. (Chat, Calls, Collections, Images, Documents, Selected Ida Document Sources).
 - 3.2.2. All Ida Document Sources – see section 3.9.1.2 Ida Document Sources for details.
 - 3.3. Collections:
 - 3.3.1. Enable GPS location on images.
 - 3.3.2. Camera Flash – Auto, Disabled.
 - 3.3.3. Collections Label Descriptor – Sets the name for Collections in the system.
 - 3.3.4. SharePoint Document Library URL – Sets the location for the SharePoint collection storage.
 - 3.4. Calls:
 - 3.4.1. Closed Captions – System call language – Sets the language that captions, transcripts, and call summaries are generated for all calls and meetings.
 - 3.5. Contacts List – Select groups to show in the contacts list of the current group. Each selected group will show up as contacts in the directory for each group member of this group.  Click the Entra button to go directly to MS Azure Entra to manage the group.
4. Enter the information or select the setting you wish to apply for the group.
5. Click SAVE to apply the new setting to the group.

Note: Setting Entra ID Guest access to "Restricted" results in guests not being able to view any Group Contacts. They must be set to at least "Limited" access to see the Group Contacts.

5.9.1.2 Ida Document Sources

Industrial Digital Assistant™, Ida, can use multiple SharePoint Document Libraries as an information source for its responses.

5.9.1.3 Assigning Group Priority

Group priority enables you to distinguish which settings take precedence when a user belongs to multiple groups. Settings will be applied in the order of the groups in the list where the highest priority is at the top.

1. Click on the more menu (...) in the top-right corner.
2. Select "Reorder Group Priority".
3. Order groups based on the order of the setting you wish to take priority when being applied.

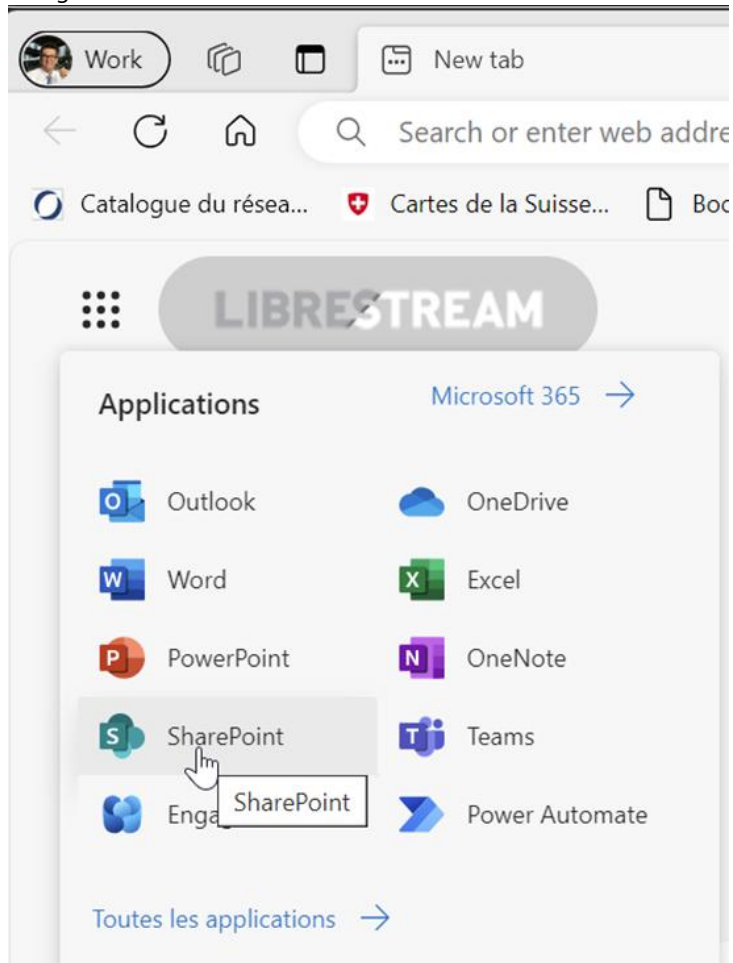
5.10 SharePoint Configuration

5.10.1 Collections - SharePoint Configuration

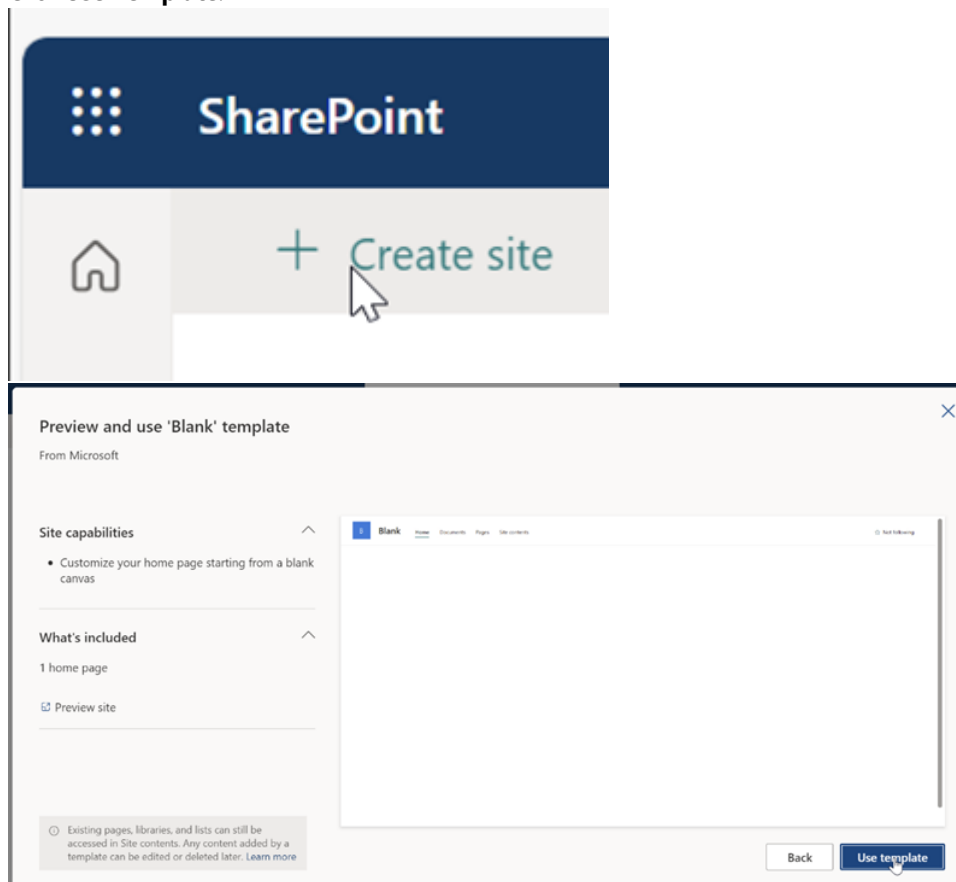
Your SharePoint administrator will need to create a SharePoint site with document libraries where we can store documents and Collection data. The Onsight NOW application will also need to be given permission to read and write to this site. Simply send us the URL for the libraries and we will configure one library to store documents you want accessible to Ida, and one to store Collections data (images, videos, transcripts, notes, etc. from the field). This section gives an overview of the steps a customer administrator should perform to enable SharePoint access.

5.10.2 Creating a new Onsight NOW SharePoint site

1. Navigate to SharePoint



2. Create a new SharePoint site and select **Communication site**. Choose the Blank Template or Standard Communication template. Click **Use Template**.



3. Enter a site name (e.g. Onsign NOW) and a description (e.g Storage for Onsign NOW Collections and Documents).

Give your site a name

Decide on a unique name that follows your organization's naming standards. The description is optional, but useful for people to understand what your site is for.

Blank [Change template](#)

Site name *

Onsign NOW

The site name is available.

Site description

Tell people the purpose of your site

Site address *

https://librestream.sharepoint.com/sites/ OnsignNOW

The site address is available.

Back Next

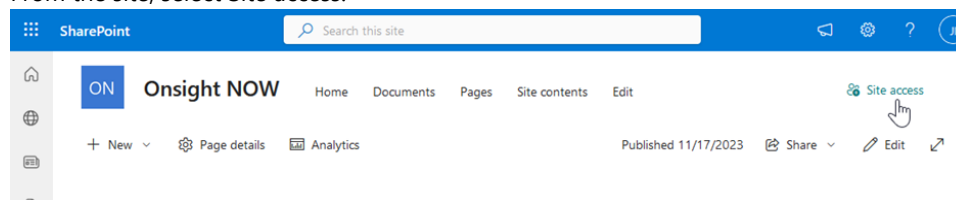
4. Note the URL of the site, such as https://{Customer Domain}.sharepoint.com/sites/onsightnow. Click **Create site** to finish creating the site.

Site address *

https://librestream.sharepoint.com/sites/ OnsignNOW

The site address is available.

5. From the site, select Site access.



6. Give access to users/groups who will be using Onsign NOW. Select Everybody to allow access to all. Give the selected users **Edit Control**. Note: this can be limited to the Entra groups that are granted access to Onsign NOW app.

Site access ×

Add users, Microsoft 365 Groups, or security groups to give them access to the site.

E

Everyone except external users

Search Directory

Site visitors - no control ⓘ

Share

Cancel

Site access ×

Add users, Microsoft 365 Groups, or security groups to give them access to the site.

E

Everyone except external users

Read ▾

×

1 g Full control

Se... Edit

7. Deselect **Send email** to avoid sending an invite to all selected users (Optional). Click **Share**

Site access ×

Add users, Microsoft 365 Groups, or security groups to give them access to the site.

E

Everyone except external users

Edit ▾

×

1 group will be invited.

☒

 Send email

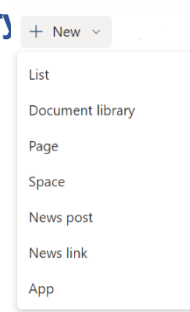
Add a message

5.10.3 Create SharePoint Document Libraries

SharePoint Document Libraries are used to store content in Collections and as a repository for Ida Knowledge Sources. In this section we will create the two libraries: Collections and Ida Knowledge Sources.

5.10.3.1 Create the Collections Document Library

1. Navigate to the Onsite NOW SharePoint Site.
2. Create a New 'Document Library'.
3. Select 'Blank Library'.
4. Enter 'Collections' as the library name. Note: you can name the library to accommodate your process. E.g. 'Cases'.
5. Write a description, e.g. 'Onsite NOW Collections'.
6. Click 'Create'.
7. Note the URL of the newly created document library, you will be entering this in the Onsite NOW application under *Settings – Collections – SharePoint Document Library URL*.



5.10.3.2 Create the Ida Documents Library

1. Navigate to the Onsite NOW SharePoint Site.
2. Create a New 'Document Library'.
3. Select 'Blank Library'.
4. Enter 'Ida Knowledge Sources' as the library name. Note: you can name this to accommodate your process. E.g. 'Knowledge Base'.
5. Write a description, e.g. 'Onsite NOW Ida Sources'.
6. Click 'Create'.

5.10.4 Collections Folder Structure

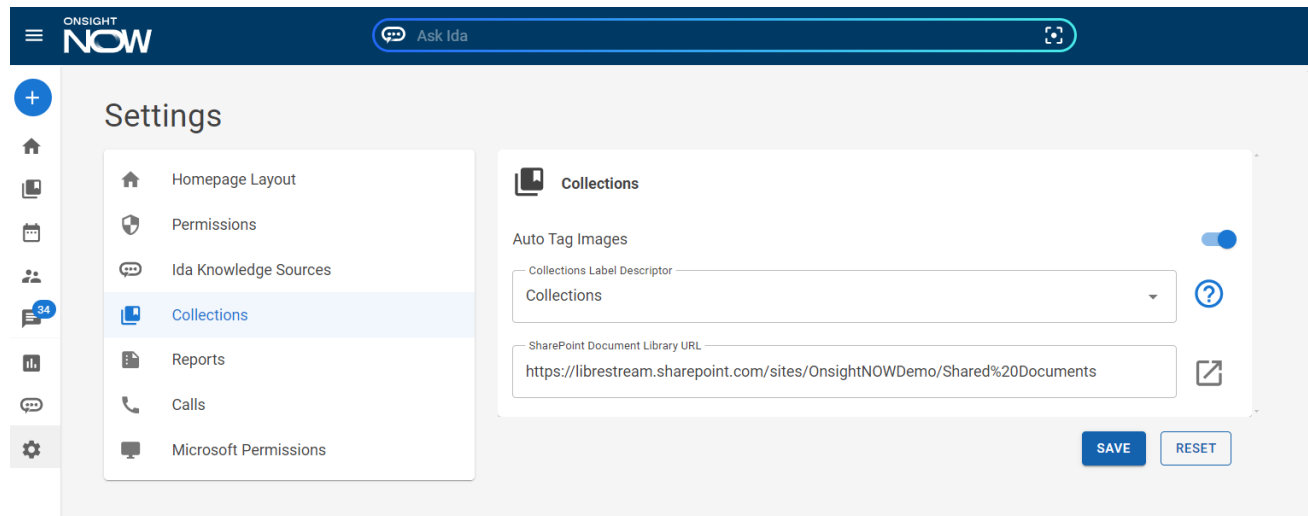
Collections will be created in SharePoint using the following folder structure:

- \KnowledgeCollections\{AuthorName}\{CollectionId}
 - Author name is the name of the user that "creates" the collection. This could be the user that explicitly created it, or the first person to join a meeting or call.
 - CollectionId is a UUID that is generated for the collection by the Knowledge Collection API.
 - Images in the collection folder are stored as "image-{date}-{time}.jpeg"
 - \KnowledgeCollections\{AuthorName}\{CollectionId}\Files
 - Contains files that were uploaded to the collection.
 - \KnowledgeCollections\{AuthorName}\{CollectionId}\Recordings
 - Contains recordings that were saved to the collection.
- \IDA Documents\Forms\{Subfolder}
 - A repository for documents that Ida will index as a source for responding to questions.

5.10.5 Configure SharePoint Drive in Onsight NOW

1. Copy the document library URL the following instructions in the previous section.
2. Login to Onsight NOW as an Administrator.
3. Go to Settings -> Collections and paste the SharePoint Document Library URL Directory into the field. Click Save.

Note: New settings and list structure have been added and so requires a new screenshot of this



4. Set the Collections default label, you may leave it as 'Collections' or any of the available options, e.g. Cases, Tickets, Inspections, or Surveys. The label change will be reflected in the Onsight NOW UI.
5. Users can now add calls, transcripts, and images to Collections.

5.10.6 Configure SharePoint for Onsight NOW Tagging

This guide will detail the steps required to configure Onsight NOW to allow applying tags and categories to Knowledge Collections items such as images, recordings and documents.

5.10.6.1 Categories

In Onsight NOW, a category is similar to a key-value pair that can be used to describe or categorize an item with Onsight NOW. Categories are appropriate when the possible values are structured, or known ahead of time, and may either be user-defined (for example, a case or ticket number), or admin-defined (such as a job role or business unit).

- Ticket #
 - o C1234, C7890
- Asset #
 - o SN3462
- Region
 - o NA, EMEA, APAC

Categories may accept a single value or multiple values, depending on the configuration of that category.

5.10.6.2 Tags

Tags are freeform values defined by users that otherwise do not fit into a particular category.

- “important”
- “TODO”
- “blue team”

5.10.6.3 SharePoint Term Store

Onsight NOW uses the SharePoint Online Term Store (<https://learn.microsoft.com/en-us/sharepoint/managed-metadata>) as a repository for tags and categories, allowing organizations to take advantage of existing managed metadata that is already used across their enterprise.

The terminology used in SharePoint differs slightly, but can be directly mapped to the concepts in Onsight NOW as follows:

Onsight NOW	SharePoint Term Store
Category Name	Term Set – a collection of related Terms that can be used to categorize content
Category Values	Term – individual items with a Term Set
Tag	Enterprise Keywords –a special case of a Term Set that is intended to accept arbitrary Terms

5.10.6.4 Required API Permissions

Tagging support in Onsign NOW requires the use of the SharePoint Online CSOM API (<https://learn.microsoft.com/en-us/sharepoint/dev/sp-add-ins/sharepoint-net-server-csom-jsom-and-rest-api-index>) in order to manage Term Sets and Terms and apply them to documents in your Knowledge Collection document library.

Two new Application-scoped API permissions must be consented to for the Onsign NOW Enterprise application for your organization:

- **Office 365 SharePoint Online - Sites.Selected (Application)**
 - o Allows Onsign NOW to read Term Sets and Terms (categories and tags) that are already applied to a document, and to set / apply new metadata to a document
 - o Note that this is a separate API permission from Microsoft Graph – Sites.Selected (Application) and must be consented to separately for your Enterprise Application.
 - o You will also need to grant Read/Write permission for your Enterprise Application to the SharePoint site. Refer to **Grant read/write permissions to the Onsign NOW SharePoint site** in the Onsign NOW Administrator Guide. If you have already completed this step for the Graph API permissions, it does not need to be done again.
- **Office 365 SharePoint Online - TermStore.ReadWrite.All (Application)**
 - o Allows Onsign NOW to read existing Term Sets and Terms from the Term Store, and to create new Terms.
 - o This permission will grant access to the Term Store for the entire organization and cannot be scoped to a single SharePoint site at this time.

5.10.6.5 Configuring The Document Library

To support applying tags and categories to document in your Knowledge Collections, some setup is required on the Document Library in SharePoint. These steps must be performed by someone with admin privileges on the Document Library.

5.10.6.5.1 Enable Tags (Enterprise Keywords)

Tags can be enabled for a Document Library by enabling the Enterprise Keywords setting. Currently this must be done directly in SharePoint.

1. Navigate to the Document Library used for Knowledge Collections in SharePoint.
2. Choose **Settings > Library Settings > More library settings**
3. Under **Permissions and Management**, choose **Enterprise Metadata and Keywords Settings**:

Permissions and Management

- ▣ [Manage files which have no checked in version](#)
- ▣ [Workflow Settings](#)
- ▣ [Enterprise Metadata and Keywords Settings](#)

4. On the next screen, enable Enterprise Keywords.

Enterprise Keywords

- ☒ [Add an Enterprise Keywords column to this list and enable Keyword synchronization](#)

Press OK.

This will add an Enterprise Keywords column to the Document Library. Documents can be now be tagged directly in SharePoint by viewing the **Details** of the document and adding free form tags to the **Enterprise Keywords** column. For example:

Enterprise Keywords

Security

Note: Use '**Change default column value**' to assign a default value for a folder, this will apply to all sub folders and files for any new additions.

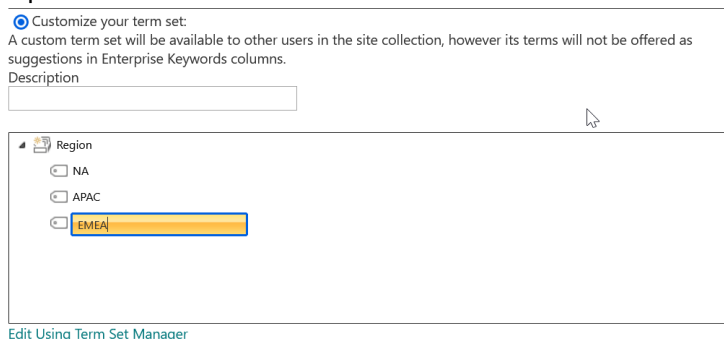
5.10.6.5.2 Enable Categories

Categories can be enabled for a Document Library by adding Managed Metadata columns to the Document Library that are mapped to a Term Set. Currently this must be done directly in SharePoint.

1. Navigate to the Document Library used for Knowledge Collections in SharePoint.
2. Choose **Settings > Library Settings > More library settings**
3. Under **Columns**, choose **Create column**
4. Choose a **Name** for the column.
 - a. The name you choose will be displayed within SharePoint in the document Details section. This can be different than the name of the Term Set mapped to the column.
 - b. Onsite NOW will display the name of the Term Set.
5. For column Type, choose **Managed Metadata**.
6. Choose whether the column / Category should allow multiple values by configuring the **Multiple Value** field,
7. Under **Term Set Settings**, choose to use either an existing Term Set, or to create a new Term Set for this column.
 - a. To use an existing term set, choose **Use a managed term set**.
 - i. Choose an existing Term Set from either the SharePoint organization or site collection



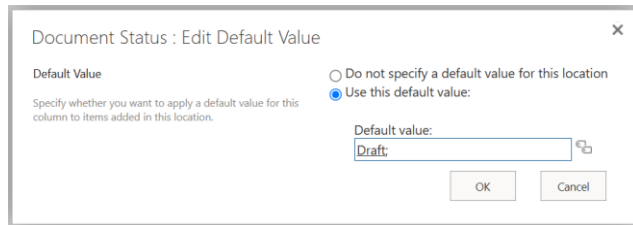
- b. To create a new Term Set, choose **Customize your term set**.
 - i. Using the built-in Term Set management control, you can rename the new Term Set and pre-populate it with Terms. New Terms can be added to the Term Set later in Onsite NOW.



- Click **OK** to create the column. This will add a column with the name you chose to the Document Library. Values for the column can be set on a document directly in SharePoint by viewing the Details of the document and adding or choosing values for the column. For example:



- To assign a default value for a folder, Choose **Settings > Library Settings > More library settings > Column default value settings**.
- Select the Column to which you want to add the default value. Set the value and click OK.



- This will apply to all folders, sub folders, and files for any new additions.

5.10.6.6 Managing Categories and Tags in Onsight NOW

After the configuration in the previous sections has been completed, Tags and Categories will now be available for management within Onsight NOW. Note that it may take some time for the API permissions changes to take effect after applying them.

Within Onsight NOW, tags and categories can be applied to a document through either the embedded viewer or via the Info panel for the document.

5.10.6.6.1 Add Tags and Categories from the Document or Image Viewer

Tags and Categories for a document can be managed in Onsight NOW using the built-in image or document viewer. Note that this is currently only available for Knowledge Collection items, and not Ida documents.

- For Images, Documents or Videos / Recordings in a Knowledge Collection, choose **View** to open the in-app document viewer. The Tags and Categories for the document will be shown at the top of the viewer, as follows:



- To apply an existing Category value to a document:
 - Click the **+ Add** button next to **Categories**.
 - Begin typing the value for the category (for example, the Item # or Case #) you wish to apply to the document and choose from the suggested list of values in the autocomplete menu. You can narrow your search to a specific category by selecting from the filter chips above.
 - Click the category value or select it using the arrow keys and press Enter. This will immediately apply the category value to the document.

3. To apply an existing Category value to a document:
 - a. Click the **+ Add** button next to **Categories**.
 - b. Type the value for the category (for example, the Item # or Case #) you wish to apply to the document.
 - c. Choose the category that this new value will apply to by selecting from the filter chips above.
 - d. Press Enter. This will add the category value (Term) to the category (Term Set) and immediately apply the category value to the document.
4. To apply a Tag to a document:
 - a. Click the **+ Add** button next to **Tags**.
 - b. Begin typing the value for the you wish to apply to the document.
 - i. If a suggested tag matches the one you wish to add, choose from the suggested list of values in the autocomplete menu.
 - ii. If no suggested tag matches the one you wish to add, finish typing in the tag and press Enter.
 - c. The tag will immediately be applied to the document
5. From the Info panel for the document
 - a. Categories are separated for clarity

5.10.6.6.2 Add Tags and Categories from the Info Panel

Tags and Categories for a document, including those documents that cannot be viewed directly in Onsite NOW, can also be managed via the Info panel for that document. Note that this is currently only available for Knowledge Collection items, and not Ida documents.

1. Using the context menu in the item's thumbnail, choose Info.
 - a. Alternatively, press the Info button on the document viewer.
2. This will open the Info panel for the document.
3. Use the Info panel to apply Tags and Categories just as you would from the document viewer.

5.11 Ida Knowledge Source Configuration

Ida™ is an AI chat interface that functions as your Industrial Digital Assistant™. Users can ask complex questions and receive responses parsed from volumes of information and different data systems across the enterprise.

There are two knowledge sources that Ida can use for generating responses, SharePoint, and Azure Blob Storage. Document indexing gives Ida the ability to search for document chunks that have been indexed into Azure AI Search. This is done by creating an index/indexer that will consume documents from a SharePoint site. Documentation can also be indexed from Azure Blob Storage, this section will describe how to configure both knowledge sources for Ida to use.

Once created, indexes/indexers that are created by the APIs in this section will run automatically every 24 hours or an index operation can be started by pressing the INDEX button on the page.



LibreStream will work with customer administrators to configure Ida document indexing.

5.11.1 Ida Document Indexing from SharePoint [Optional]

5.11.1.1 Customer Prerequisites

- A customer representative that has Azure Entra Administrator access in order allow the Onsite NOW indexer to read the contents of the site for indexing.
 - The Entra ID roles that should be sufficient for this process are **Privileged Role Administrator** and **Global**

Administrator.

- A customer representative that has **SharePoint Site Administrator** access in order allow the Onsign NOW indexer to read the contents of the site for indexing.

5.11.1.2 SharePoint Site

A SharePoint site is required to host the documents for the indexer to consume. Customers can host the documents in their own SharePoint site.

5.12 Granting Onsign NOW Sites.Selected permissions to the SharePoint

For security reasons, the Onsign NOW enterprise application will request the **Sites.Selected** API permission. This permission will grant the application access to selected SharePoint sites that a SharePoint Site administrator will allow. The initial grant to the **Sites.Selected** will not actually give any permissions to a SharePoint site until the **SharePoint Site Administrator** performs the steps in the next section.

A customer representative that has Azure Entra Administrator access to allow the Onsign NOW indexer to read the contents of the site for indexing is required.

NOTE: The Entra ID roles that should be sufficient for this process are **Privileged Role Administrator** and **Global Administrator**.

Granting the **Sites.Selected** permission can be done through the Onsign NOW enterprise application in Azure by the **SharePoint Site Administrator** (or equivalent Entra role). This procedure was outlined in section [Granting Consent to Onsign NOW Permissions](#) :

Home > Enterprise applications | All applications > Onsign NOW

Onsign NOW | Permissions

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

<< Refresh Review permissions Got feedback?

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). [Learn more.](#)

You can review, revoke, and restore permissions. [Learn more.](#)

To configure requested permissions for apps you own, use the [app registration](#).

Grant admin consent for Librestream Technologies Inc.

Admin consent

User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by	
Microsoft Graph						
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator	***
Microsoft Graph	Mail.Read	Read user mail	Delegated	Admin consent	An administrator	***
Microsoft Graph	offline_access	Maintain access to data you h...	Delegated	Admin consent	An administrator	***
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator	***
Microsoft Graph	Files.ReadWrite.All	Have full access to all files us...	Delegated	Admin consent	An administrator	***
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	People.Read	Read users' relevant people li...	Delegated	Admin consent	An administrator	***
Microsoft Graph	Calendars.Read	Read user calendars	Delegated	Admin consent	An administrator	***
Microsoft Graph	Files.Read.All	Read all files that user can acc...	Delegated	Admin consent	An administrator	***
Microsoft Graph	Sites.Selected	Access selected site collections	Application	Admin consent	An administrator	***

44

4 - Settings

5.12.1 Grant read/write permissions to the Onsight NOW SharePoint site using Graph Explorer

Once the **Sites.Selected** permission has been granted to the Onsight NOW enterprise application, the **SharePoint Site Administrator** must use the Microsoft Graph API to grant **read/write** access to the Ida documents and the Collections document libraries in the Onsight NOW SharePoint site.

The following steps can be done using the [Microsoft Graph Explorer](#). The **SharePoint Site Administrator** must log using their Microsoft company credentials.

Obtain the SharePoint Site ID

In Graph Explorer run a GET request to the <https://graph.microsoft.com/v1.0/sites> API (graph.microsoft.com is graph.microsoft.us for Government Cloud customers). For example, <https://graph.microsoft.com/v1.0/sites/librestream.sharepoint.com/sites/TestSite>. If successful, the result should show the properties of the site. Copy the value under **id**, this is the SharePoint site ID.

Grant Read/Write Permissions to the SharePoint site

In Graph Explorer start a POST request to the <https://graph.microsoft.com/v1.0/sites/{siteid}/permissions> API. Replace **{siteid}** with the Site ID retrieved from the previous step.

Paste the following json under the **Request Body**:

```
{
  "roles": ["read", "write"],
  "grantedToIdentities": [{
    "application": {
      "id": "{Onsight NOW enterprise application ID}",
      "displayName": "Onsight NOW"
    }
  ]
}
```

Note: The id can be found at Azure Portal -> Entra ID -> Enterprise Applications -> Onsight NOW -> Overview -> Application ID

The user may have to grant Graph Explorer access to make this call:

➤ Request body

📄 Request headers

⚙️ Modify permissions

🔑 Access token

Permissions

One of the following permissions is required to run the query. If possible, consent to the least privileged permission.

Permission	Description	ⓘ Admin consent required	Status	ⓘ Consent type
Sites.FullControl.All ⓘ	Allow the application to have full control of all site collections on your behalf.	Yes	ⓘ Unconsent	🔄

Run the POST command to the permissions API.

5.12.1.1.1 Azure AI Search

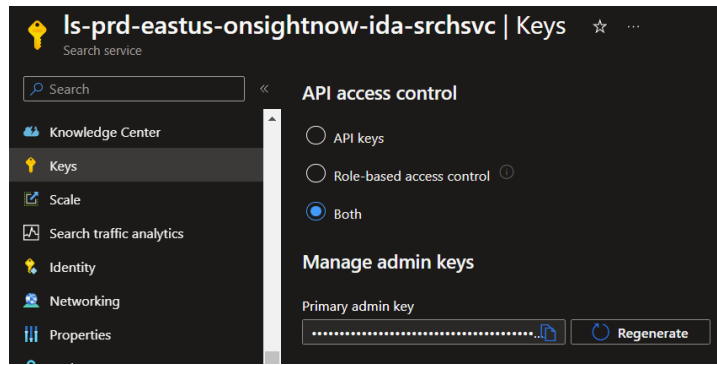
An Azure AI Search resource is required to be able to index the documents stored in the Azure storage container. Librestream can host the Azure AI Search resource and indexes/indexers, or the customer can host their own Azure AI Search resource.

Librestream Hosted Azure AI Search

The Librestream hosted Azure AI Search resource is pre-configured. No action is required.

Customer Hosted Azure AI Search

If you prefer to host your own Azure AI Search resource, provide the endpoint and access key for the Azure AI Search resource to Librestream. For example:



Creating an Index and Indexers

Using your Azure AI Search endpoint and access key, Librestream will create and configure the Index and Indexers.

Adding Documents

After Librestream has completed the initial creation of the source and index for a customer, you can add more documents to the index at any time by uploading documents to the SharePoint site. The created indexes will automatically run every 24 hours to index any new document in the container.

The customer's tenant administrators can also run the index operation in the Onsignt NOW tenant admin settings page.

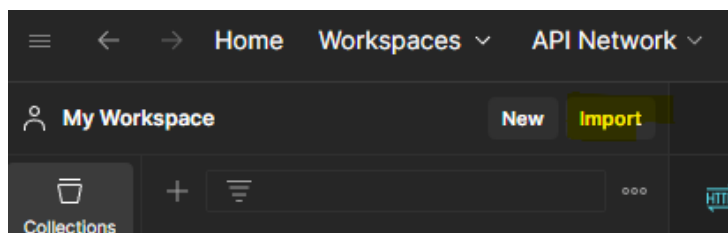
5.12.2 Grant read/write permissions to the Onsignt NOW SharePoint site using Postman

Use these instructions if you do have access to the MS Graph Explorer. (Skip this section if you have granted SharePoint permissions using the MS Graph Explorer.)

Once the **Sites.Selected** permission has been granted to the Onsignt NOW enterprise application, the **SharePoint Site Administrator** must use the Microsoft Graph API to grant **read/write** access to the Ida documents and the Collections document libraries in the Onsignt NOW SharePoint site.

The following steps can be done using the [Postman API Platform](#). The **SharePoint Site Administrator** must log using their Microsoft company credentials.

1. Refer to the Onsignt NOW [Postman collection](#) for more documentation and examples obtaining and using tokens.
2. Get the Onsignt NOW postman json file from Librestream.
3. Download Postman Windows 64-bit [Download Postman | Get Started for Free](#)
4. Sign in or create an account. Use your work email.



5. Once in, click **Import**, **files**, click on the json file then **Open**.
6. Create a SharePoint site in Azure then go back to Postman.
7. Click on **SharePoint sites.selected** then **Variables**.

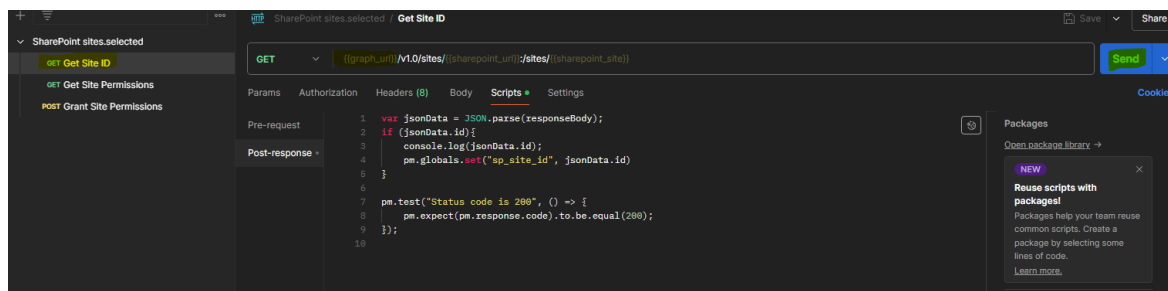
Variable	Initial value	Current value
<input checked="" type="checkbox"/> login_url	https://login.microsoftonline.com	https://login.microsoftonline.us
<input checked="" type="checkbox"/> login_scope	https://graph.microsoft.com/default	https://graph.microsoft.us/default
<input checked="" type="checkbox"/> graph_url	https://graph.microsoft.com	https://graph.microsoft.us
<input checked="" type="checkbox"/> tenant_id	dd6eba40-9b32-4b4b-9a10-75d8fc2a1023	b981f6dd-71f7-4079-9ad1-07578ee8d3b6
<input checked="" type="checkbox"/> client_id	b27baac1-3f93-4cf1-9427-692216305075	b47ca74-888b-4ee6-beb5-9dc35c38acaf
<input checked="" type="checkbox"/> client_secret	j908Q-1327KBLNEJfukI3xktExyUxR0Tn5Jdkx	k9.yRSQ2wXvgbn99Z-o_mb07-8Tp9gfoQ
<input checked="" type="checkbox"/> onsigntnow_client_id	9e7e9e91-d73c-4882-b492-e56b3c278c94	454ca8ee-bcfc-4b41-8c2b-76582c3af02f
<input checked="" type="checkbox"/> onsigntnow_client_name	Onsight NOW	Onsight NOW
<input checked="" type="checkbox"/> sharepoint_url	librestream.sharepoint.com	rmsecho.sharepoint.us
<input checked="" type="checkbox"/> sharepoint_site	TestSite	OnsightDemo

8. Change the Current Value to correct value
 - a. tenant_id – get this from your Azure Entra ID.
 - b. client_id – go to Entra, app registrations, new registration. Once the application has been created go to API permissions, then add a permission, Microsoft Graph, Application permissions, search for Site then select the permission required.
Then go to Enterprise Application, click on the app you created. Grab the **Application ID**
 - c. client_secret – go to Entra, App registrations, click on the App you created, Certificate & secrets, New client secret. Once secret is created grab the **Value**
 - d. onsigntnow_client_id – TBD where do you get the id from?
 - e. sharepoint_url

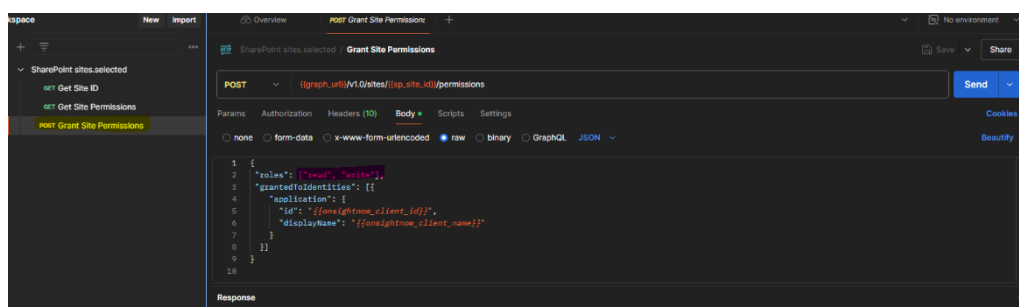
<https://rmsecho.sharepoint.us/sites/OnsightDemo/Shared%20Documents/Forms/AllItems.aspx>

- f. Sharepoint_site

<https://rmsecho.sharepoint.us/sites/OnsightDemo/Shared%20Documents/Forms/AllItems.aspx>



9. Get Site ID.
10. Post Grant Site Permissions – change the **roles**.
11. Go to Azure, Users and groups, add the user need to manage the OnsightNOW settings and assign **Administrator** role
12. Go to app.onsightgov.us, Microsoft Permissions, select the permission needed then hit Grant.



13. Test

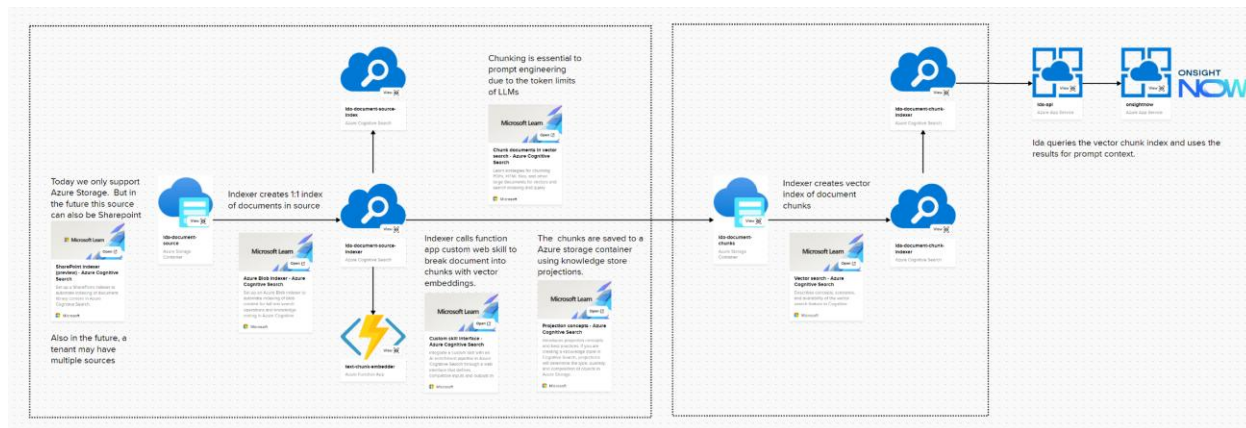
- Login the user and try to upload a picture or go to onsite Sharepoint site and make sure you can access the document library.

5.12.3 Ida Document Indexing from Azure Blob Storage [Optional]

Document indexing gives Ida the ability search for document chunks that have been indexed into Azure AI Search. This is done by creating an index/indexer that will consume documents from an Azure storage container.

Once created, indexes/indexers that are created by the APIs in this section will run automatically every 24 hours or an index operation can be requested manually through the APIs.

Librestream will work with customer administrators to configure Ida document indexing.



Azure Storage Account and Container

An Azure Storage Account and container are required to host the documents for the indexer to consume.

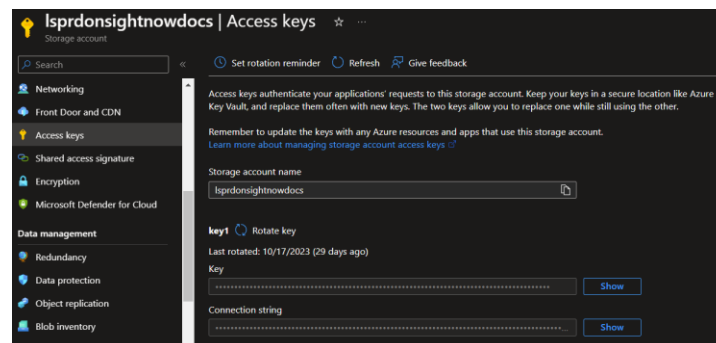
- Librestream can host these documents for a customer, or
- Customers can host the documents in their own Azure Storage Account and container.

Librestream Hosted Storage Account and Container

Librestream will configure the storage container and OnSight Now application on your behalf.

Customer Hosted Storage Account and Container

The customer administrator must provide the connection string for the Azure Storage Account to Librestream. For example:



Azure AI Search

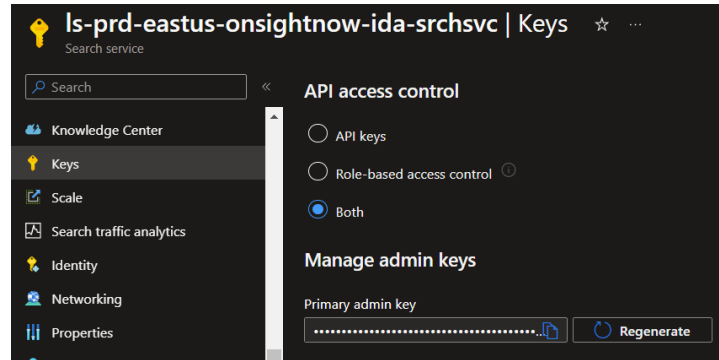
An Azure AI Search resource is required to be able to index the documents stored in the Azure storage container. Librestream can host the Azure AI Search resource and indexes/indexers, or the customer can host their own Azure AI Search resource.

Librestream Hosted Azure AI Search

Nothing to be done. The Librestream hosted Azure AI Search resource is pre-configured.

Customer Hosted Azure AI Search

The customer administrator must provide the endpoint and access key for the Azure AI Search resource to Librestream. For example:



Creating an Index and Indexers

Using your Azure AI Search endpoint and access key, Librestream will create and configure the Index and Indexers.

Adding Documents

After Librestream has completed the initial creation of the source and index you can add more documents to the index at any time by uploading documents to the SharePoint site. The created indexes will automatically run every 24 hours to index any new document in the container.

The customer's tenant administrators can also run the index operation in the Onsignt NOW tenant admin settings page.

5.13 External Applications

Configure an External Application to use Onsignt NOW APIs from your application. Refer to our Postman collection for more information, example requests, and authorization methods. This configuration is required to authenticate and obtain access tokens that are needed to make Onsignt NOW API requests.

Onsignt NOW supports standard OIDC/OAuth 2.0 flows to authenticate and obtain user or application tokens. The Onsignt NOW APIs authorize requests using the standard Bearer token authorization scheme.

5.13.1 Application Registration

The application that will integrate and make use of Onsignt NOW APIs must be registered and configured. You must have the Onsignt NOW **Administrator** role to perform this configuration.

1. Sign-in to Onsignt NOW and go to **Settings > External Applications**
2. Select Add New Application. The **External Applications** registration form will be available.
3. The **Application ID** is generated when the External Application registration is created. This will be needed to configure your application (see 5.13.2).
4. Provide details for your application:
 - a. **Application Name:** Short display name
 - b. **Application Description:** Optional description of your application
 - c. **Grant Types:** Select one or both of the supported OIDC/OAuth grant types.
 - i. **Client Credentials:** Suitable for service-to-service requests. Your application will obtain tokens issued to the application and not an end-user. This requires a Client Secret to obtain tokens in place of user credentials. Use this flow if you do not want your users to need to sign-in to Onsignt NOW before making API requests.
 - ii. **Authorization Code:** Suitable for requests made on behalf of an Onsignt NOW user. This flow requires an interactive Onsignt NOW sign-in by the end user to obtain initial tokens. Use this flow if you want Onsignt NOW API requests to be made on behalf of the end user.
 - d. **Require PKCE:** Enable to require [Proof Key for Code Exchange \(PKCE\)](#). This is applicable to the Authorization Code flow only and improves security for public clients.
 - e. **Redirect URL:** add your application URL(s) that will receive authorization codes from Onsignt NOW during the Authorization Code flow.
 - i. This must match exactly the [redirect_uri parameter](#) included by your application in the authorization code request.
 - ii. Upon successful sign-in, Onsignt NOW authorization services will redirect back to this URL with the issued authorization code. The code can be then exchanged for an access token.
 - iii. You may add several Redirect URLs for different applications or deployments.
 - f. **Post Logout URL:** add any application URL(s) that will receive callback from an [OIDC single logout](#). This is only applicable to the Authorization Code flow.

- g. Secret:** add one or more Client Secrets. A secret is required for the **Client Credentials** flow.

Settings

Use the information from the Onsignt NOW **Settings** > **External Applications** registration to configure your application to authenticate and retrieve tokens needed to call Onsignt NOW APIs.

Onsight NOW uses standard OIDC/OAuth flows for authorization and obtaining tokens used to call APIs. The implementation details for performing this flow are beyond the scope of this document. Depending on the architecture, frameworks, and languages utilized by your

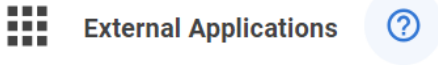
- [oidc-client](#): Javascript npm package
- [IdentityModel](#): Helper library for claims-based identity, OIDC/OAuth. Contains useful utilities for handling Identity Provider metadata (OpenID Configuration).
- [Microsoft ASP.NET Libraries](#): .NET libraries for OIDC/OAuth for web applications
- [Other providers](#)

If none of these are suitable, the Client Credentials and Authorization Code flows are relatively simple to implement.

Typically, your OAuth client will require standard configuration elements available from your application registration:

- **Authority:** the base URL of the Onsignt NOW authorization server. For example: <https://login.onsightnow.com>.
- **OIDC Metadata Endpoint:** the URL of the Onsignt NOW authorization server's well known OIDC JSON metadata document. For example: <https://login.onsightnow.com/well-known/openid-configuration>.
- **Client ID:** your registration's **Application ID**.
- **Client Secret:** needed for **Client Credentials** flow.
- **Scopes:** space-separated list of application scopes identifying Onsignt NOW API resources. The scopes vary depending on the authorization flow used.
 - **Client Credentials:** meeting_api collection_api
 - **Authorization Code:** onsignt openid offline_access
 - The offline_access scope is optional. If requested, a Refresh token will be included in the authorization response. The refresh token can be used with the OAuth Refresh Token flow to obtain a new short-lived access token without requiring user interaction.

Click the '?' button on the External Applications page for more details.



5.13.3 Obtaining and Using Tokens

Upon a successful authorization exchange your application will receive one or more tokens that can be used to access Onsite NOW APIs and resources.

Example authorization response. Some fields are shortened.

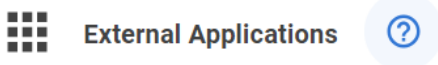
```
{
  "id_token": "eyJhbGciOiJSUzI1NiIsImt...",
  "access_token": "eyJhbGciOiJSUzI1NiIsIm...",
  "expires_in": 3600,
  "token_type": "Bearer",
  "refresh_token": "81F0787058F6B259168AA3C97EDD33794BB72E22018D060AF1D975CC5D6F9F0D-1",
  "scope": "openid profile onsite offline_access"
}
```

- **id_token:** User identity token. Contains Onsite NOW user claims and information. This is not needed to call Onsite NOW APIs and is only issued when using the **Authorization Code** flow.
- **access_token:** This token must be included in Onsite NOW API requests. It must be placed in the Authorization HTTP header, using the Bearer scheme. For example:
 - Authorization: Bearer eyJhbGciOiJSUzI1NiIsIm...
 - The access_token is short-lived and is valid for 1 hour.
- **expires_in:** The number of seconds from issuance to when the access_token expires. After expiry, it will no longer be valid for API requests. It must be renewed using a **refresh_token** (if available) or the authorization flow must be repeated to obtain a new token.
- **refresh_token:** Can be used with the OAuth Refresh Token flow to obtain a new access token. The refresh token is valid for approximately 30 days.
- **token_type:** Indicates the type of access token. Should always be Bearer.
- **scope:** The resource scopes the **access_token** is valid for.

Refer to the [Onsite NOW Postman collection](#) for more documentation and examples obtaining and using tokens.

5.13.4 Using External Applications Resources

Links to the Onsite NOW Postman Workspace and individual Swagger pages are available from the Onsite NOW Settings > External Applications > Help '?' panel.



Using External Applications

Configure an External Application to use Onsight NOW APIs from your application. Refer to our Postman collection for more information, example requests, and authorization methods.

OAuth endpoints used for configuring your application and getting a token.

Authority
https://login.onsightnow.com

Authorization Endpoint
https://login.onsightnow.com/connect/authorize

Token Endpoint
https://login.onsightnow.com/connect/token

Explore APIs and additional documentation with our Postman Workspace.

[Postman Collection](#)

View Swagger documentation and retrieve Open API (OAS) specifications.

[Meetings](#)

[Collections](#)

CLOSE

Post Logout URL

Explore APIs and additional documentation with our Postman Workspace.

<https://www.postman.com/onsightnow/workspace/onsight-now/collection/10195276-10bc1513-d721-469a-9af2-b0c31ede0236>

View Meetings Swagger documentation and retrieve Open API (OAS) specifications.

<https://ls-prd-eastus-onsightnow-chat-api-svc.azurewebsites.net/swagger/index.html>

View Collections Swagger documentation and retrieve Open API (OAS) specifications.

<https://ls-prd-eastus-onsightnow-knowledge-api-svc.azurewebsites.net/swagger/index.html>

6 Analytics

Administrators can access the Analytics page for usage reports on Logins, Calls, Chats, and Collections (the Knowledge base).

7 Ida Dashboard

The Ida Dashboard is where you access information about Ida usage and where you curate Ida Document sources for inclusion in Ida responses. You must have the Curator role applied to your user account in order to access the Content panel on the dashboard.

Once a user has been assigned the Curator role, they will have access to the 'Ida Dashboard – Content' tab.

The screenshot shows the OnSight NOW interface. At the top is a dark blue header with the 'ONSIGHT NOW' logo and a search bar labeled 'Ask Ida'. Below the header is a sidebar with various icons, including a plus sign, home, document, calendar, people, and a chat icon with a '36' badge. The main content area is titled 'Ida Dashboard' and has two tabs: 'CONTENT' (selected) and 'ANALYTICS'. Under the 'CONTENT' tab, there is a search bar with 'python' entered and a 'Sources' dropdown menu set to 'SharePoint'. Below this is a table with the following columns: Name, Last Feedback Date, Toggle Ida Status, and Analytics. The table contains two rows of document entries. The first row is for 'python-crash-course-2nd-edition-pdf.pdf' with a last feedback date of 'Wednesday, October 16, 2024', a status of 'INCLUDED', and analytics showing 3 thumbs up and 0 thumbs down. The second row is for 'pythonlearn.pdf' with the same last feedback date, a status of 'INCLUDED', and analytics showing 2 thumbs up and 0 thumbs down. At the bottom of the table, there is a pagination bar showing 'Rows per page 10', '1-2 of 2', and navigation arrows.

Name	Last Feedback Date	Toggle Ida Status	Analytics
python-crash-course-2nd-edition-pdf.pdf Document	Wednesday, October 16, 2024	INCLUDED	3 0 ...
pythonlearn.pdf Document	Wednesday, October 16, 2024	INCLUDED	2 0 ...

- Use the Search field to filter for specific documents.
- Use the Sources drop down menu to select different Ida Knowledge sources (as configured in Settings – Ida Knowledge Sources).
- Use the Arrow icon to go directly to the document source.
- Use 'Toggle Ida Status' to include or exclude documents from Ida responses.
- The Thumbs up/down totals indicate user votes for each response that cited the document.
- The more menu contains a 'View' option for the document.

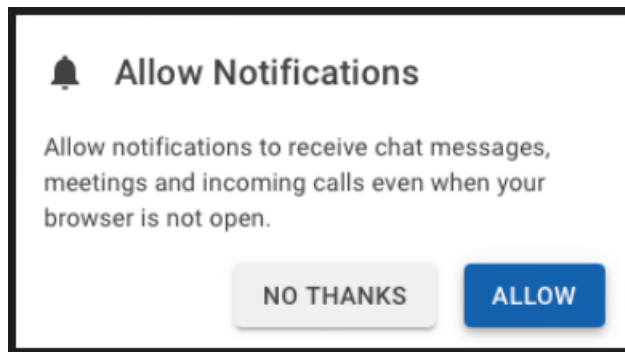
8 Web Browser Notifications

8.1 How to Receive Web browser notifications

Users must follow the browser instructions on their devices to receive notifications for Chats, Calls, and Meetings. The instructions will be displayed when they log in to <https://app.onsightnow.com>.

8.1.1 For PC's and Android devices

- Web browser must be opened.
 - Web notifications must be enabled in your browser.
 - For PC's, system notifications must be enabled E.g. Windows: System > Notifications > Enabled, or System > Privacy & security > Notifications.
 - Accept permissions to Allow notifications from Onsite NOW.
 - When logging into a browser for the first time, you will see a prompt like the following:
-
- Press ALLOW to get the browser-specific prompt to enable push notifications.
 - If you choose "No Thanks", you can enable them later by navigating to the Onsite NOW profile menu, pressing the up arrow, and choosing User Settings then pressing ALLOW NOTIFICATIONS.



8.1.2 Mac/iOS (Safari and Chrome)

For Mac/iOS (Safari and Chrome) to receive notifications the web app needs to be installed as a Progressive Web app (PWA) i.e., added to the home screen. This will place a shortcut on the home screen that links directly to the Onsite NOW web app. PWAs have the appearance of a locally installed application but are in fact a web application. Note that PWAs do not contain the standard browser menu bar, they will only display the web application's menu bar.

- When running the web app directly through the browser, you will receive a prompt to Install it.
- If you choose to install, you will be shown instructions on how to get to the 'Add to Home Screen' option in the browser's menu.
- Once installed, you can launch the web app from the Home Screen and will be prompted to allow notifications for chat messages, meetings, and incoming calls.

9 Support

For Support inquiries:

- **Email:** support@librestream.com
- **Web:** <https://librestream.com/contact-us-support/>
- **Phone:** 1.800.849.5507 or +1.204.487.0612



Figure 5-1 Contact Support QR Code