Magnit

App Integration

September 2025

IT/Developer Guide

TABLE OF CONTENTS

SUMMARY

Within our [redacted] VMS product ('VMS', 'application'), we help our clients with all aspects of their interview process, including candidate scheduling.

Through our web application, clients will grant permission to their calendar and/or video conferencing service. The system will then allow the user to schedule a new meeting and generate a meeting link through [redacted] VMS with the convenience of seeing their business calendar to avoid any conflicts.

- Only meetings created through the VMS will be modified or deleted on the user's calendar or video conferencing service.
- The VMS securely stores access and refresh tokens so it can request the user's calendar details, create a meeting, and generate a meeting link.
- Client Administrators or users can revoke access at any time.
- Integrations can only access active VMS user account calendar information.

INTEGRATION ACCESS TYPES

[redacted] VMS offers two types of integration:

- **User-Consent** – This option allows a user with the Manager role to integrate their individual account with the VMS system, if allowed by their organization.
- **Admin-Consent** - This option allows the Client's IT Administrator to grant [redacted] VMS permission to access domain accounts rather than authentication by each individual user.
    - With Microsoft Teams, IT Administrators can control access to domain accounts through their Microsoft application Access Policies.

PERMISSIONS

The table below outlines the permissions [redacted] VMS uses to perform required functions. Permissions are granted for either Admin Consent or User Consent, but not both.

- User-Consent = Delegated Permissions
- Admin-Consent = Application Permissions

Application	Description	Scope	Authentication
Microsoft 365 / Outlook **"User-Consent"**	Read profile Read/Write calendar	Calendars.ReadWrite Allows the app to create, read, update, and delete events in user calendars.	OAuth 2.0

Microsoft 365 / Outlook **“Admin-Consent”**	Read profile Read/write calendar	Calendars.ReadWrite Allows reading, creating, updating, and deleting calendars and their events for all users without a signed-in user.	Application Permission
Microsoft Teams	Read/write calendar	OnlineMeetings.ReadWrite Allows the app to read all transcripts of online meetings, on behalf of the signed-in user.	OAuth 2.0
Microsoft Teams “Admin-Consent”	Read/write calendar	OnlineMeetings.ReadWrite.All Allows the app to read all transcripts of all online meetings, without a signed-in user.	Application Permission
Google Calendar	View and read calendar events	/calendar/api/v3/reference/events	OAuth 2.0
Cisco WebEx	Retrieves the meeting lists and details Create, edit, or cancel scheduled meetings	meeting:schedules_write	OAuth 2.0

REFERENCES

- Microsoft Outlook: https://learn.microsoft.com/en-us/graph/api/resources/calendar?view=graph-rest-1.0
- Google: https://developers.google.com/identity/protocols/oauth2/scopes
- Microsoft Teams: https://learn.microsoft.com/en-us/graph/api/application-post-onlinemeetings?view=graph-rest-1.0&tabs=http
- Cisco WebEx: https://developer.webex.com/docs/integrations#scopes

AUTHENTICATION

For user-consent integration, [redacted] VMS leverages the corresponding applications OAuth 2.0 workflow to allow the user to authenticate. When the user initiates the integration, the VMS will direct the user to the browser to enter their credentials.

- The VMS does not store the user’s credentials.
- The VMS securely stores access and refresh tokens.

For admin-consent integration, please contact your Client Services representative or [redacted] Services & Support Center.

STORING ACCESS & REFRESH TOKENS

[redacted] VMS securely stores the users' access and refresh tokens within the database. It will be used for the following functions:

Calendar Integration

- Allow the user to create, modify, and cancel meetings through the VMS web application.
- Allow delegates who schedule interviews for a manager, to see their free/busy (no calendar details.)
- Allow the user to create, modify, and cancel meetings through the VMS mobile application.

Video Conferencing Integration

- Allow the user to create, modify, or delete meeting links through the VMS web application.
- Allow the user to create, modify, or delete meeting links through the VMS mobile application.
- Allow MSP to create, modify, or delete meeting links through the web application.

VIDEO CONFERENCE INTEGRATION | MANAGED SERVICE PROVIDER (MSP) ACCOUNT ACCESS

By integrating your 3rd-party video conferencing account with the [redacted] VMS, you acknowledge and confirm that an MSP user assigned to represent your organization may generate a meeting link from your video conferencing account when they create meeting requests on your behalf.

The authorized MSP user will have access to generate or delete video meeting links with the integration video conferencing account for the hiring manager assigned to the staffing request.

VIDEO CONFERENCING SYNC | MICROSOFT TEAMS ADMIN CONSENT

[redacted] VMS (VMS) offers the ability to integrate with Microsoft Teams with administrator consent for the interview scheduling functionality. Admin consent allows the Client's IT Administrator to grant the [redacted] VMS permission to access domain accounts defined by their Microsoft application Access Policy rather than authentication by each individual user.

> The VMS will only request permissions related to user profile and online meetings. The user's VMS login must match the client's domain account for a successful integration.

Provide Admin Consent Integration URL to Client

The client organization needs to click on the Microsoft Teams admin consent integration URL provided by [redacted] Global.

- Client administrators are prompted to log in using their admin credentials.
- The administrator consents to the requested permissions.
- The administrator receives a message stating "Admin Consent Successful". Your admin consent has been successfully provided to the app'.

Create Client Application Access Policy (Microsoft Teams Only)

The client administrator needs to log into their Microsoft 365 tenant and create a client application access policy. This will control applications, such as the [redacted] VMS, and define the domain accounts the application will be authorized to access and act on behalf of.

Please refer to the following Microsoft documentation

- Microsoft New-CsApplicationAccessPolicy Documentation
- Microsoft Grant-CsApplicationAccessPolicy Documentation

Create Example

```
New-CsApplicationAccessPolicy -Identity [redacted] VMS" -AppIds [redacted] application id}}" -Description
[redacted] VMS Microsoft Teams Access"
```

Grant Access Example

```
Grant-CsApplicationAccessPolicy -PolicyName [redacted] -Identity "{{user azure object id}}
```

Manager Role – No Additional Configuration

After the client administrator has provided admin consent and the MSP Admin has enabled Microsoft Teams in the configuration, users with the Manager role are able to create an interview request using the Microsoft Teams method with no additional configuration.

By integrating your 3rd-party video conferencing account with the [redacted] VMS, you acknowledge and confirm that an MSP user assigned to represent your organization may generate a meeting link from your video conferencing account when they create meeting requests on your behalf.

The authorized MSP will have access to generate or delete video meeting links with the integrated video conferencing account for the hiring manager assigned to the staffing request.

REVOKE ACCESS WITHIN [redacted] VMS

As a user with the manager role, using the un-sync function in the User Profile Settings will revoke access to the integrated account. This option will delete the stored refresh/access tokens for the integration, and it will no longer be available within the [redacted] VMS system.

For video conference integrations, un-syncing also revokes access for an authorized MSP user. To revoke access, log into the Manager version of the VMS, click **Profile** > **User Profile** > **Video Conference Sync**, and click **Un-sync**.

As a user with the MSP Admin role, disabling the app integration at the Client-Configuration level will not revoke access to the integrated account. This option will remove the option from being visible within the VMS.

Disabling at the client-configuration level will not delete stored access/refresh tokens if a user has previously authorized the integration.

REVOKE ACCESS FROM YOUR BUSINESS APPLICATION

To permanently remove an integration from your organization, please use the following references.

Application	Documentation
Microsoft 365 / Outlook	https://learn.microsoft.com/en-us/powershell/module/skype/remove-csapplicationaccesspolicy?view=skype-ps
Google Calendar	https://support.google.com/accounts/answer/3466521?sjid=4314463268678627614-NA
Microsoft Teams	• User-consent: https://support.microsoft.com/en-us/office/manage-your-apps-ff207d1f-e071-40a3-8388-0c3d5a3b456a • Admin-consent: https://learn.microsoft.com/en-us/microsoftteams/manage-apps
Cisco WebEx	https://help.webex.com/en-us/article/osit0i/Revoke-Third-Party-Integrations-from-a-Cisco-Webex-Meetings-Account

[redacted] VMS SECURITY & COMPLIANCE

[redacted]

[redacted] VMS PRIVACY POLICY

https://prowand.pro-unlimited.com/privacy_policy.jsp