Magnit™

The Evolution of Work™

App Integration

February 2024

IT/Developer Guide

TABLE OF CONTENTS

SUMMARY

Within our Magnit 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 the Magnit 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 stores the refresh and access 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.

INTEGRATION ACCESS TYPES

Magnit VMS offers two types of integrations:

- **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 the Magnit VMS permission to access domain accounts defined by their Microsoft application Access Policy rather than authentication by each individual user.

PERMISSIONS

The table below outlines the permissions the Magnit VMS uses to perform required functions.

Application	Description	Scope	Authentication	User-Consent	Admin-Consent
Microsoft 365 / Outlook	Read profile Read/write calendar Read meeting room information	https://graph.microsoft.com/v1.0/me https://graph.microsoft.com/v1.0/me/calendar/getschedule https://graph.microsoft.com/v1.0/me/calendar/events https://graph.microsoft.com/v1.0/me/calendarview https://graph.microsoft.com/v1.0/me/events office365_Admin_scope = https://graph.microsoft.com/.default	OAuth 2.0	Yes	Yes
Microsoft Teams	Read/write calendar	offline_access%20OnlineMeetings.ReadWrite Admin Scope = Magnit passes as default. https://graph.microsoft.com/.default	OAuth 2.0	Yes	Yes
Google Calendar	See primary Goggle Account email address See personal information, including any personal information that is made publicly available	"https://www.googleapis.com/auth/userinfo.email" "https://www.googleapis.com/auth/userinfo.profile" "https://www.googleapis.com/auth/calendar"	OAuth 2.0	Yes	No

	See, edit, share, and permanently delete all calendars that can be accessed using Google Calendar				
Cisco WebEx	Retrieves the meeting lists and details Create, manage, or cancel scheduled meetings	*meeting:schedules_write*	OAuth 2.0	Yes	No

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, Magnit 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 does store the access and refresh tokens.

For admin-consent integration, please contact your Client Services representative or Magnit Global Services & Support Center.

STORING ACCESS & REFRESH TOKENS

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

CALENDAR INTEGRATION | MANAGED SERVICE PROVIDER (MSP) ACCOUNT ACCESS

By integrating a 3rd-party calendar account with the Magnit VMS, you acknowledge and confirm that an MSP user assigned to represent your organization may have access to view your calendar availability (Free/Busy visibility only, not calendar details).

The authorized MSP will have access to create, modify, cancel interview meetings with the integrated calendar account for the hiring manager assigned to the staffing request.

The account owner will have full visibility to their calendar details within the VMS. Also, the authorized MSP user will have visibility to the account owner's free/busy schedule within the VMS.

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

By integrating your 3rd-party video conferencing account with the Magnit 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

Magnit 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 Magnit 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 Magnit Global.

- Client administrator is 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

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 Magnit 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 “Magnit VMS” -AppIds “{{magnit application id}}” -Description “Magnit VMS Microsoft Teams Access”
```

Grant Access Example

```
Grant-CsApplicationAccessPolicy -PolicyName “MagnitVMS -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 Magnit 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 MAGNIT 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 Magnit VMS system.

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** > **Calendar Sync** or **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
Zoom	https://support.zoom.us/hc/en-us/articles/4413265586189-Allowing-Apps-access-to-shared-access-permissions
Cisco WebEx	https://help.webex.com/en-us/article/osit0i/Revoke-Third-Party-Integrations-from-a-Cisco-Webex-Meetings-Account

MAGNIT VMS SECURITY & COMPLIANCE

Independently audited security certifications, including SOC 1 Type II, SOC2 Type II, CSA Star Level 2, Privacy Shield (EU and Swiss), ISO 27001:2013, 27701:2019, 27017:2015, 27018:2014 (US & EU).

MAGNIT VMS PRIVACY POLICY

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