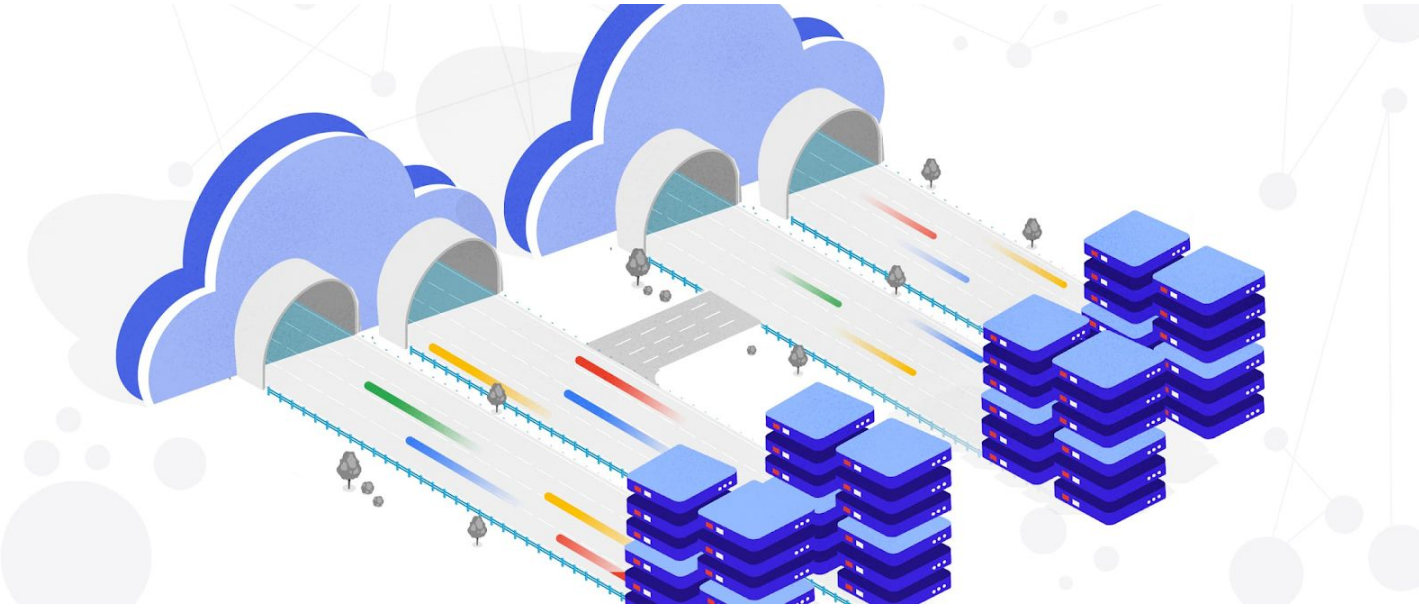
July 2020

G Suite & Office 365 coexistence overview



Google Cloud | Atos

Table of contents

1. About this document

This guide is intended to help customers better understand how to use and customize G Suite services and settings to coexist with Microsoft Office 365 users within the same company.

The information and recommendations in this document were gathered during our work with multiple clients and environments in the field. Thank you to our customers and partners for sharing their insights.

What's covered	• The experiences of G Suite and Office 365 users collaborating within the same example company. • All scenarios are from the G Suite perspective. • Helpful G Suite technical references to increase your knowledge.
What's not covered	• This document is not a technical configuration guide for setting up coexistence between G Suite and Office 365. • Each organization has its own history and own way of working, which might result in different approaches or configurations. Consult a Google partner, like Atos, who can support you with both G Suite and Office 365.
Primary audience	• IT leadership, change management consultants, and G Suite administrators.
IT infrastructure	• G Suite and Office 365 coexisting in a current IT environment.
Release notes	• July 20, 2020—Initial document release.
Feedback	• Google values your feedback. If you have comments or suggestions, use this contact form to provide us with remarks on the applicable section.

2. Background of the example company

Each organization has its own way of working. As a result, each company is unique and might make specific choices about how they leverage technologies.

In this chapter, an imaginary company is introduced as a consistent reference for the different scenarios throughout this paper. This example company might not be applicable to your organization, but hopefully it will help you select the best coexistence scenario for your situation.

As each company and their existing infrastructure is unique, this document is not a blueprint. We recommend you work with a Google partner who knows both G Suite and Office 365 to help you make the best decisions for your company.

About the company

The example organization, a company in the manufacturing sector, has approximately 25,000 employees globally with a presence in several countries/regions. Within each country/region, the organization has staff working in the office and on the factory floor. All countries/regions collaborate across every level of the organization, ranging from accountants to factory operations managers.

They previously used Microsoft Office 2016 software with on-premises versions of both Microsoft Exchange and Microsoft SharePoint. The company began their cloud journey in 2019.

Coexistence strategy

There are 2 ways G Suite and Office 365 can coexist:

1. **Split coexistence**—Deploy G Suite accounts to one user group and Office 365 accounts to a separate user group.
2. **Dual coexistence**—Deploy specific G Suite services for one purpose and Office 365 services for another. For example, use Google Meet and Google Drive to enhance collaboration with Microsoft Exchange Online as the mail client.

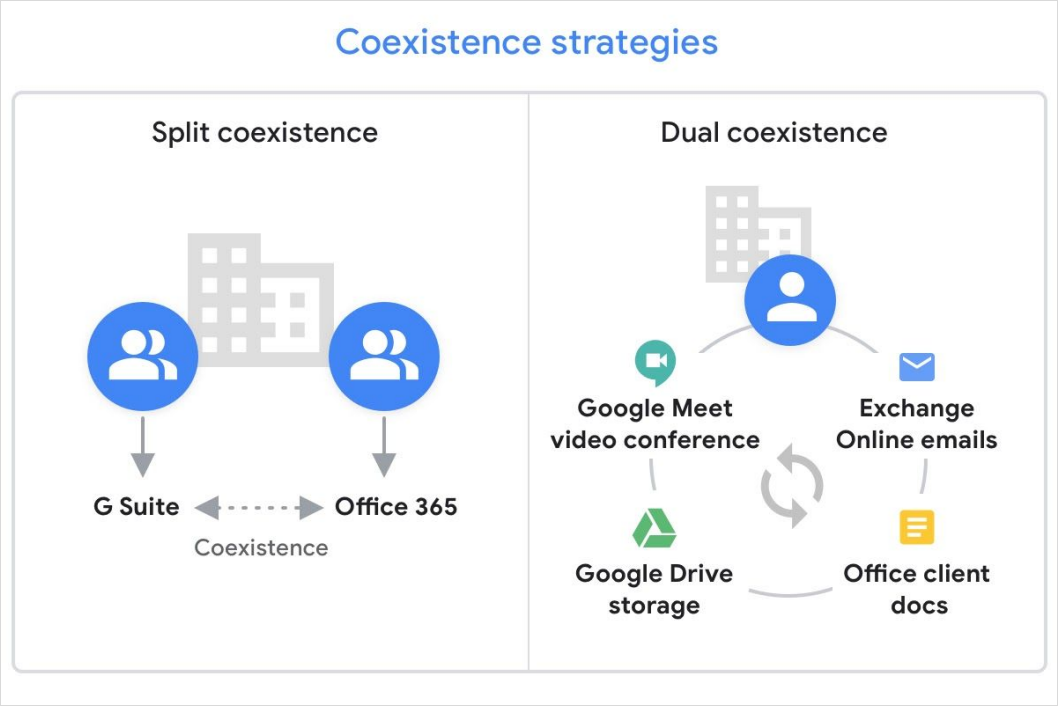


Figure 1: Architecture of the coexistence strategies

For the first part of this document, we'll use the split coexistence strategy where the company has users within both G Suite and Office 365 systems. With this cross-functional collaboration, employees use their specific platform to improve communication as they work toward common goals.

Dual coexistence, which offers users a combination of G Suite and Office 365 services, is discussed in chapter 5, G Suite Essentials.

Collaboration platforms

The decision to use either G Suite or Office 365 is made on a per country/region basis. The decentralization of IT decisions arose after several company acquisitions requested they remain on their current platform. This policy gives local management teams the power to select tools based on their markets.

This means some countries/regions use G Suite and others Office 365. As a result, the number of G Suite users (13,000) is about the same as those within Office 365 (12,000).

IT environment

In 2019, the company decided to move from a traditional IT environment to a modern IT deployment strategy. The current system eliminates operating system images on devices and replaces it with device OS configuration controlled from a central location. It also lets users install applications from the company's private store for Windows 10.

The company's network strategy also changed. Traditionally, employees needed Virtual Private Network (VPN) connections to access company applications. By moving to a zero-trust network policy, users no longer need VPN tooling.

As part of the modern IT deployment strategy, a wide range of devices are now allowed including Chromebooks, Microsoft Windows devices, and Apple MacBooks. The company also supports Bring Your Own Device (BYOD) to access the collaboration platforms.

IT management

Each country/region has its own IT department to manage local assets and a service desk to handle on-site support questions. Corporate headquarters manage all global tools, such as G Suite and Office 365. G Suite allows employees to work easily from any place and on any device.

Security and compliance

Enterprise security uses BeyondCorp for their workplace services. This zero-trust security model is used by Google to secure their own infrastructure.

For compliance, the company is subject to General Data Protection Regulations (GDPR) in the European Union and local compliance requirements (taxes, archiving of data, etc.) for specific countries/regions. Due to the items they manufacture, they must obey regulations to keep all relevant product content for 20 years. All sales contracts are kept for 10 years.

3. IT architecture of the example company

To provide a generic understanding of the company's IT environment, the most relevant components of the IT infrastructure are discussed in this chapter. Specific G Suite admin help resources are linked in the text for easy reference.

Directory synchronization

The company has on-premises Microsoft Active Directory for user provisioning in all systems but they want to sync all identities to the cloud. As a result, they chose the following architecture design:

- On-premises Active Directory is synced to Google Cloud using Google Cloud Directory Sync (GCDS).
- Google Cloud Identity is the central repository for all cloud-based applications and is also utilized for user provisioning.
- The on-premises Active Directory is synced with Microsoft Azure Active Directory using Azure Active Directory Connect sync services to provide identities to Office 365.

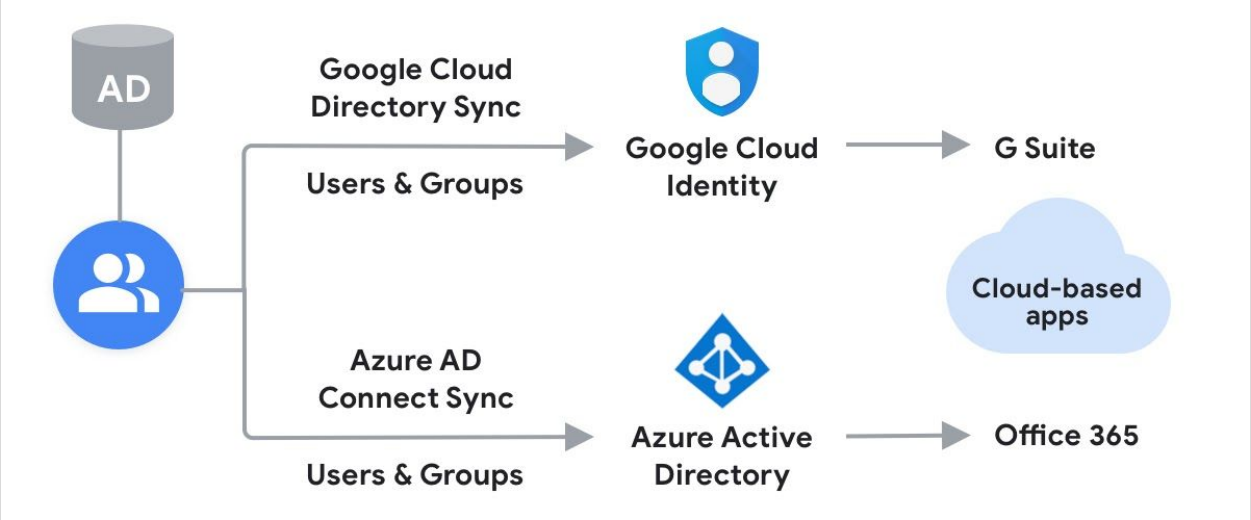


Figure 2: Directory synchronization flow

Security groups and mail distribution lists are maintained in the on-premises Active Directory. Those objects are synced to G Suite using GCDS and to Office 365 using Azure Active Directory Connect sync. Within G Suite, security groups and mail distribution lists are represented through Google Groups.

Access management

The company has a strategy to provide single sign-on (SSO) and encourages all users to adopt 2-Factor Authentication. They currently have 2 systems for access management:

- When on-site, users sign in with on-premises Active Directory.
- For cloud-based applications, they use the SAML features of Cloud Identity and G Suite. They also implemented SSO for Office 365 and other cloud applications.

Mail flow

Within the example organization, every employee can be reached through the corporate domain *example.com*, and on their country/region extension (for example, *example.nl*). The default mail address is the *example.com* domain.

For inbound mail, all Mail Exchange (MX) records point toward Google mail servers. Each server routes the mail toward Gmail, the customer relationship management (CRM) system, or Office 365 depending on the recipient address.

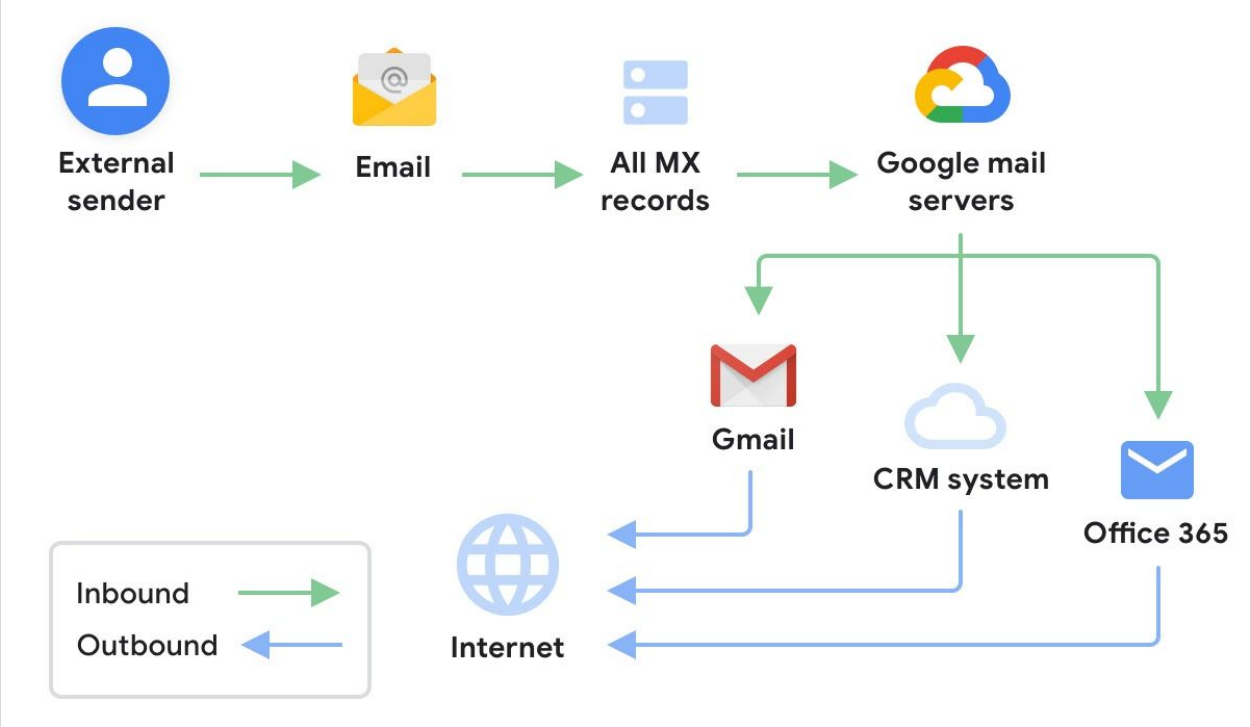


Figure 3: Mail flow

Each service (Gmail, the CRM system, or Office 365) sends all outbound mail directly to the internet. For security reasons, the Sender Policy Framework (SPF) records, DomainKeys Identified Mail (DKIM) records, and the Domain-based Message Authentication, Reporting, and Conformance (DMARC) records are created to prevent email spoofing.

The SPF record of the corporate domain (*example.com*) allows Gmail, the CRM system, and Office 365 to send mail on behalf of the company. The country/region domain extension (*example.nl*) only allows the specific service used (Gmail, the CRM system, or Office 365) to send mail. Learn more about SPF records, DKIM records, and DMARC records.

To assist with internal mail in Office 365, a relay rule points to Gmail servers. A similar configuration for Gmail is not necessary as Google routes all mail using MX records. For more information on setting up email coexistence between G Suite and Office 365, consult your Microsoft documentation.

Data loss prevention (DLP) policies are also employed in both G Suite and Office 365.

Calendar coexistence

The organization also implemented G Suite's Calendar Interop product. The configuration allows G Suite users to view the free/busy information of Office 365 users, and Office 365 users can view the free/busy information of G Suite users.

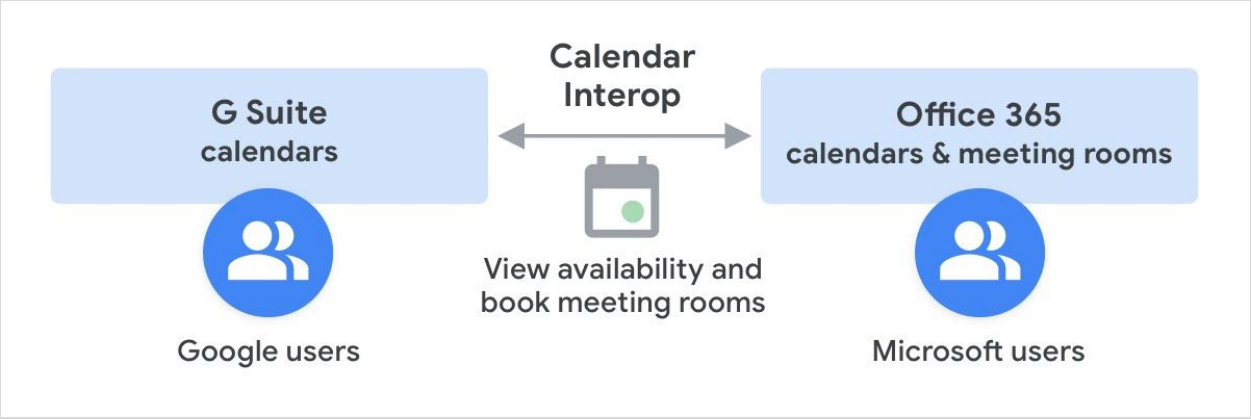


Figure 4: Calendar Interop workflow

Calendar Interop also supports Exchange calendar resources, such as meeting rooms. All calendar resources must be maintained in Office 365 to ensure resources can be booked from either collaboration platform.

Device management

In each country/region, local teams purchase devices. As a result, device management is also decentralized. Each country/region is in the process of applying modern IT management strategies using Google endpoint management or Microsoft Intune.

Countries/regions that adopted G Suite manage their Chromebooks and Windows 10 devices with the Google Admin console. Countries/regions using Office 365 manage their Windows and mobile devices with Intune.

Browser management

For several years the company has used the Chrome Browser as their default browser on all devices. The countries/regions that moved to G Suite now manage the Chrome Browser in the cloud. The organization previously used software package updates on Windows devices to manage the browser settings. The company also decided to buy Chrome Browser licenses for all employees using Office 365.

In the Chrome Browser, admins manage several settings and user experience controls. The home button navigates to the company's global intranet containing a central bookmark folder with subfolders for each country/region.

Context-Aware Access using endpoint verification

To support BYOD scenarios for employees and vendors with their own devices, the company uses the Chrome Browser to deploy endpoint verification to all BYOD devices. Windows and MacBook users installed the Endpoint Verification extension from the Chrome Web Store to maintain device access to company data. The extension also logs details in the Admin console about the device.

Context-Aware Access offers the ability to deploy company security policies on any device. Policy examples include:

- Only devices with storage encryption turned on can access Drive.
- Requiring a recent, supported version of the Chrome Browser to access all services.
- Restricting access to certain apps from outside the corporate network.

For Office 365 users, the company applies similar policies through Intune.

Storage

In moving to a cloud-based workplace, the organization migrated their file servers to the cloud. A Google Drive first strategy was chosen because the file servers were at the end of their lifecycle and their support contract was ending. To prevent access issues, the company decided to move these files to the cloud (Google shared drives or SharePoint). This migration proved advantageous as employees gained advanced search and collaboration features. Learn more about shared drives.

When sharing Drive files with Microsoft users, G Suite users can leverage all sharing options. To ensure Microsoft users can access Drive files, they must have a free Cloud Identity license within the Google Directory. Note that Drive supports built-in viewing and editing of Microsoft Office files.

Microsoft offers different options to let users share Microsoft OneDrive files with Google users. For more information, consult your Microsoft documentation.

Intranet and document management system

The company intranet has run on open source, on-premises software for many years. Besides acting as an intranet, the system is also used for enterprise document management.

As part of their cloud-first strategy, this joint server was recently migrated to the Google Cloud Platform (GCP). The new configuration relies on Cloud Identity for authentication.

Enterprise search

Google Cloud Search is used to manage enterprise search across all company content.

Cloud Search Connectors are used to index data and map authorizations. The company uses connectors for G Suite, Office 365, the intranet, the document management system, and the cloud-based CRM.

Online meetings

When all countries/regions moved to a cloud-based workplace, online meeting frequency increased significantly.

G Suite users can receive a Microsoft Teams invite and attend a Teams meeting (with or without the client installed). Similarly, Microsoft users can attend a Meet video meeting (without the client installed).

It's important that networks and VPNs are properly set up for both systems. For instance, Meet uses a set of dedicated IP address ranges and Office 365 has similar recommendations for Teams. For more information on Office 365 URLs and IP address ranges, consult your Microsoft documentation.

Online meetings can be scheduled using Google Calendar as it provides free/busy status interoperability between the 2 platforms. Learn more about calendar coexistence

Calendar resources, such as meeting rooms, within each country/region are not yet modernized. At the time of investment, video conferencing requirements using Meet and Teams were not discussed with the vendor. To integrate the current meeting rooms within Meet and Teams, the organization decided to deploy Pexip for integration.

Pexip is an approved Google and Microsoft vendor. They offer a service that can be deployed in GCP, Azure, or Amazon Web Services (AWS). The service also allows for on-premises deployments. Both deployment models offer scalability and management, along with cloud deployment automation.

When deploying the Pexip instance to G Suite, calendar meeting invites automatically include the necessary information for users joining from Teams, Skype for Business, Cisco Webex, etc. The solution also offers one-tap join capabilities from Cisco hardware.

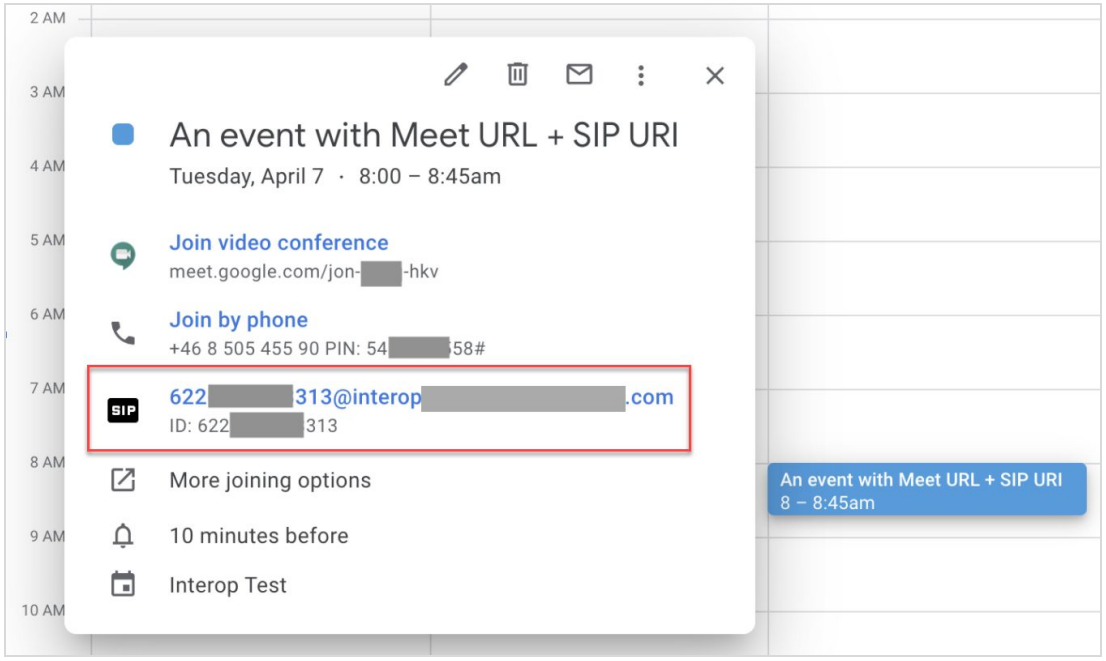


Figure 5: Pexip integration in a calendar invite

4. Sample user scenarios

This chapter contains typical scenarios for internal collaboration within the example organization. Each sample scenario starts from the viewpoint of the user and includes screenshots when applicable. Technical details and watchpoints are also listed.

The scenarios in this chapter surround 4 essential collaboration pillars:

- Connect
- Access
- Create
- Control

4.1 Connect

Within the example company, every employee needs to easily connect with their colleagues independently of the collaboration platform used. Based on this idea, the following coexistence scenarios are listed.

Scenario: Sending mail

All employees have an email address. On both collaboration platforms, employees are listed in the corporate directory with relevant details like phone number, job title, office location, and manager name.

User experience

1. Users start their mail client (Gmail or Outlook) and compose a new email message.
2. In the "To" field, as you begin entering text you can select a recipient from the corporate directory suggestions or enter an email address of a recipient.
3. The same applies when using mail distribution lists. These lists are identical on both platforms and some lists might contain a mix of both G Suite and Office 365 email addresses. This poses no problem as all email messages are delivered to the user's correct mailbox.
4. HTML formatting of email messages is used on both platforms. Different font types, font colors, font attributes, and emoji characters can be used to format the messages.
5. Security requirements like DLP are implemented on both platforms to make sure the same corporate policies are enforced for all users.

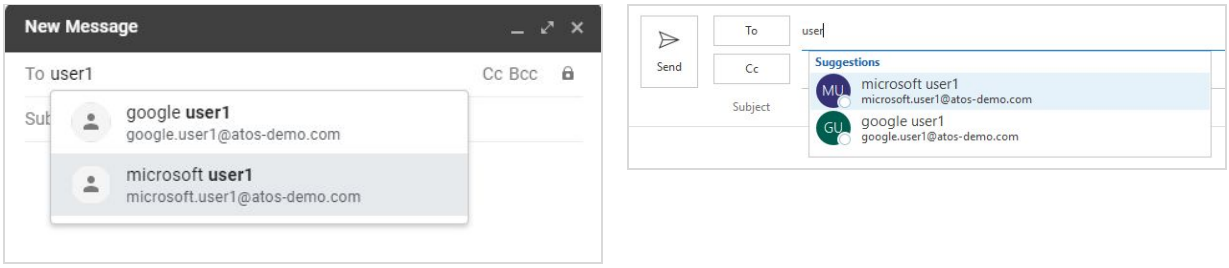


Figure 6: Suggested recipients when composing a message in Gmail (left image) and Outlook (right image). The corporate directory includes users on both platforms.

G Suite technical references

A technical description of directory sync between the Cloud Identity directory and the Azure Active Directory is described in the previous chapter. Mail distribution lists are maintained in the on-premises Active Directory. This ensures there's a single source of truth for all mailing lists.

- About Google Cloud Directory Sync—G Suite Admin Help
- Get started with Cloud Identity—G Suite Admin Help

Scenario: Booking a calendar appointment with the global team

Most departments within the company have an annual global meeting to align on their yearly objectives. Company headquarters organizes these meetings that can span multiple time zones across different countries/regions.

User experience

1. An invite is created in Google Calendar. Colleagues from either collaboration platform are added from the suggestions in the “Add guests” field.
2. For all employees, their free/busy status is visible through Calendar Interop so the event organizer can select a suitable time slot to accommodate everyone.
3. The event organizer adds a meeting room to the Calendar invite. The selected location exists in a factory that uses Office 365 exclusively. This has no implication on the free/busy status of the Office 365-held meeting room or the meeting’s visibility in Calendar.
4. All guests from both collaboration platforms receive the invite, can view all details including location information, and can accept or decline the meeting.

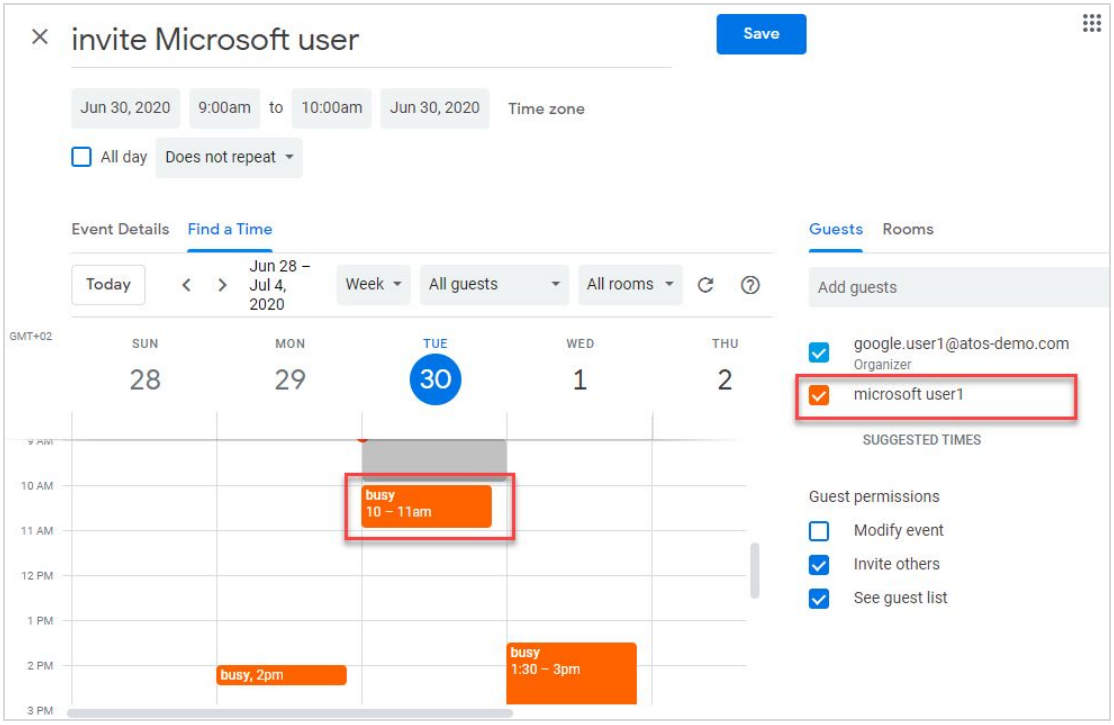


Figure 7: Calendar user can view the free/busy status of a Microsoft user

Watchpoints

All company users can view every meeting room and the free/busy status of every employee. While essential features for calendar interoperability are provided, the product does have the following limitations:

- Only the event organizer and users on the same platform (for example, G Suite) can view the status of guests who responded.
- Delegation of calendar access to users between platforms is not available.
- Some calendar options set by the event organizer do not transfer to users between platforms:
    - The Calendar option allowing guests to modify the event doesn't work for Outlook calendar users.
    - Working hours set in Calendar or Outlook are not visible to users between platforms.

While there are some limitations on the company's internal calendar coexistence, it's not a significant issue as the free/busy status on the primary calendar is available to all employees.

G Suite technical references

The company uses the Calendar Interop utility. An overview is provided in the previous chapter.

- Get started with Calendar Interop—G Suite Admin Help
- Allow Calendar users to book Exchange resources—G Suite Admin Help

Scenario: Hosting a video meeting (organizer on G Suite)

An employee at company headquarters using G Suite organizes a monthly event with the country/region leads (some of whom use G Suite and others Office 365). An invite is created in Calendar and a Meet video conference is added. In the event description, the meeting agenda is listed and a link to the meeting document stored on Drive is added.

User experience

1. Booking the monthly meeting is easy as the free/busy status of everyone is visible to all internal users through Calendar Interop.
2. The attached document has meeting topics, tasks, and meeting minutes. It's shared from Drive and any employee attending the meeting can open it in a browser.
3. Meeting guests using Office 365 can easily view the Meet video conference instructions in their invite message on Outlook. This means both external participants and users within the company can easily join the meeting.
4. The formatting of calendar events to include bold, italics, underscores, or bulleted lists is supported on both platforms.

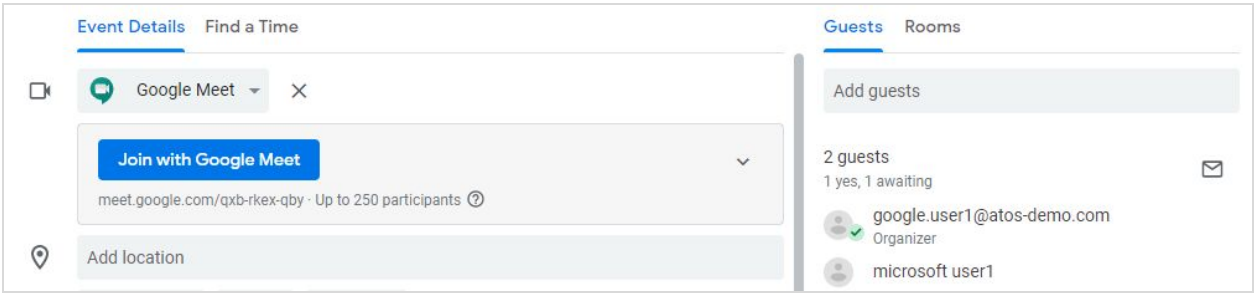


Figure 8: G Suite user hosting a video meeting with an Office 365 user. The invite includes a Meet video conference link.

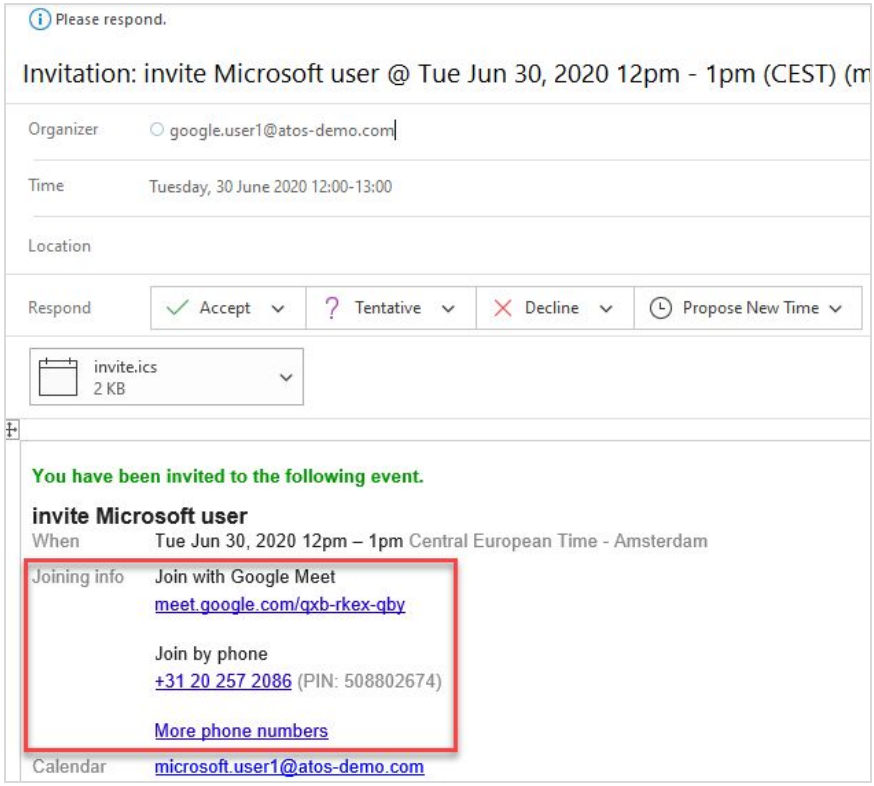


Figure 9: The invited Office 365 user can view the meeting info and Google Meet link in the description field

G Suite technical references

- Get started with Calendar Interop—G Suite Admin Help
- The company implemented a video meeting gateway to improve the user experience: Use Meet with 3rd-party video hardware systems—G Suite Admin Help

Scenario: Hosting a video meeting (organizer on Office 365)

An employee using Office 365 organizes a meeting with a colleague who uses G Suite. The purpose of the meeting is to discuss data captured in a Microsoft Excel spreadsheet. The file is attached to the Outlook calendar invite.

User experience

1. Selecting a meeting time slot in Outlook is easy as free/busy information is visible to all internal users through Calendar Interop.
2. The video meeting is facilitated through Teams and instructions are provided in the email. Participants can attend the Teams meeting without having to install extra tools. This is beneficial as Teams is not installed on G Suite user devices.

3. The meeting organizer drafts the agenda in the description field of Outlook and formats some numbers for discussion during the meeting. This information is visible to a Google Calendar user.
4. The Excel document is attached directly to the invite by the meeting organizer and is also visible to a Google Calendar user. The file can be viewed in Google Sheets as G Suite document editors support built-in viewing and editing of Microsoft Office files. The Office 365 user could have also shared the file with the meeting attendees instead of attaching it.
5. Before the meeting begins, a newer version of the Excel file is distributed through email. This newer version is not attached to the calendar invite.

G Suite technical references

- Get started with Calendar Interop—G Suite Admin Help
- Work with Microsoft Office files—Docs Editors Help

Scenario: Delegation strategies

Within the organization, managers and their personal assistants use mail, calendar, and contact delegation to complete tasks. For delegation to work, both users must have accounts on the same collaboration platform. Managers can then delegate the relevant service to their assistant.

User experience

For simplification, only the Google Calendar experience is explained here. However, delegation in Gmail and Google Contacts operates in a similar manner.

1. In Calendar, a user can share their primary calendar or another calendar.
2. To be valid, the user must select a colleague that also uses Calendar, as delegation between collaboration platforms is not supported.
3. The colleague receives an email about the delegation. After accepting, the delegated calendar is accessible and automatically added in Calendar.

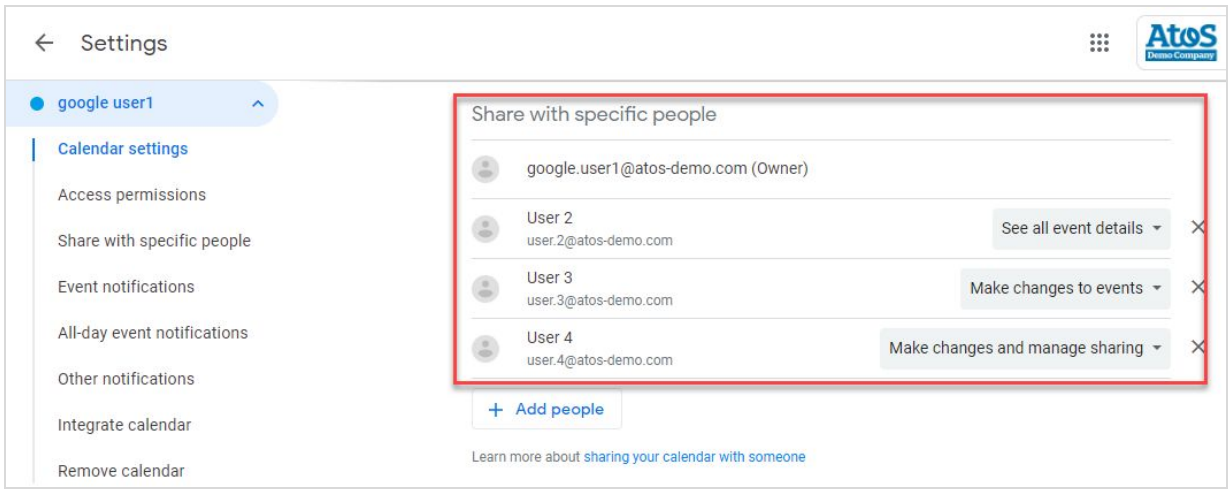


Figure 10: G Suite user delegating a Calendar to G Suite colleagues

Delegation in Outlook calendar uses a different approach. Users can share their calendar in an email or set more advanced access permissions using Outlook calendar properties. For more information on sharing Outlook calendars, consult your Microsoft documentation.

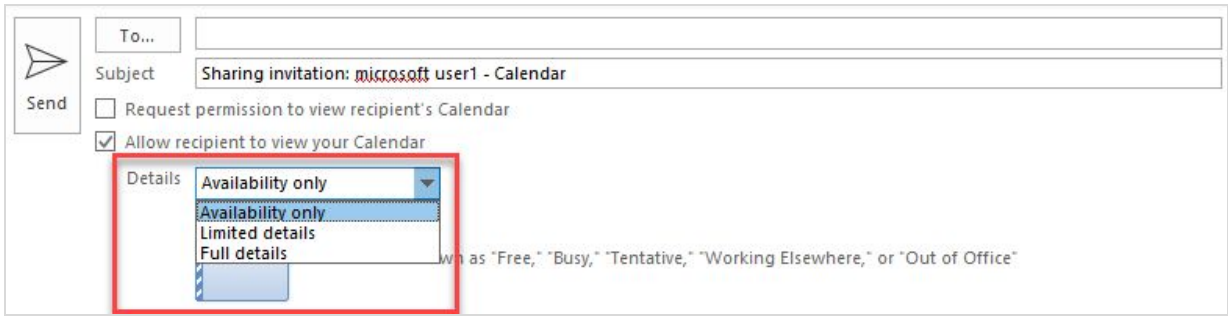


Figure 11: Office 365 user delegating to Office 365 colleagues in an email

Workaround

- There's no feature in G Suite or Office 365 that supports delegation across collaboration platforms. As a consequence, delegated users must be on the same platform.
- A possible workaround is to provision a second identity. For example, an assistant on Office 365, who needs to manage a calendar (or mailbox or contact list) of a manager on G Suite, would need a G Suite license. Mail and calendar routing still goes to the assistant's mailbox on Office 365, but the assistant can sign in to their G Suite account to view the manager's Google Calendar (or other delegated) service. Since it's a second identity, the assistant needs to sign in with separate credentials.

- However, for the best everyday experience, it's recommended that both users have the same collaboration platform.

G Suite technical references

- Share your calendar with someone—Calendar Help
- To support the workaround, a second identity can be hidden in the Google directory: Hide a user from the Directory—G Suite Admin Help

Scenario: Communities

The organization wants to give certain projects and company departments the ability to use specific communities or collaboration spaces.

In G Suite, Google Groups are created for these departments. Team collaboration spaces can be created in either Google Currents, Google Chat rooms, shared drives, or Google Sites. The company is letting departments choose the best option to organize themselves.

In Office 365, company departments use the Teams environment. There's no specific coexistence feature in place. If some projects have both G Suite and Office 365 users, the company might need to give G Suite users an Office 365 license to access Teams.

User experience

1. The project lead is using G Suite and can create a group for the specific project directly in Groups. Self-service creation of groups is a feature permitted by the G Suite admin.
2. All group members receive an automatic email when added to the project's group.
3. The project lead decides to use a Drive folder to share project files and Sheets to organize tasks.
4. Any project members using Office 365 can access the Drive files without requiring a temporary G Suite license.
    a. If the project uses Currents, Chat rooms, Sites, or Calendar, a G Suite license is required.
    b. If a G Suite license is needed, Office 365 users would have the license added to their account so they can use all G Suite services, except Gmail. While they can access the project team's Google Calendar, they cannot view their personal Outlook calendar within Calendar.

G Suite technical references

- When using Google Groups for Business, admins enforce the "Add a suffix to groups created by users" option when Groups for Business are created. This allows G Suite

users to create groups but it appends an identifying word or phrase to the end of the group's email address. This ensures user-created groups are recognizable by their unique email address. For more information, go to Set Groups for Business sharing options—G Suite Admin Help.

- Some G Suite services are available to Cloud Identity users: What is Cloud Identity?—Cloud Identity Help

Scenario: Chat

All employees have access to chat. Employees with G Suite use Google Chat and those with Office 365 use Teams. There's no integration between the 2 collaboration platforms.

A third-party, cloud-based communications tool is used for telephony on both G Suite and Office 365. This solution has a chat feature to bridge user communication between collaboration platforms.

User experience

1. Both platforms (G Suite and Office 365) offer tight integration of their built-in chat tool in their respective platform services. Employees mostly use their platform's built-in chat features. Since employees use chat platforms with no coexistence features, it means they cannot view their colleague's online presence on the opposite platform.
2. To start a chat between collaboration platforms, the third-party chat client is used.

G Suite technical references

- Get started with Google Chat—Google Chat Help

Scenario: Telephony (cloud and on-premises)

The company offers employees an integrated communication experience with telephony added into the workplace environment.

For telephony infrastructure (PBX), they chose a third-party, cloud-based telephony solution that integrates with G Suite and Office 365. It's available in all relevant countries/regions. Since G Suite has the Google Voice cloud-based telephony solution, they're considering a switch in the future.

User experience

1. Every telephone number listed on a webpage changes to a URL which users can call with the cloud telephony client.

2. Employees can call directly using the computer's Chrome Browser extension that is installed by default.
3. Employees on their mobile phones use a dedicated third-party mobile application. For G Suite users, the app is available through the enterprise-managed apps section of managed Google Play (Android) or can be installed using a Google Device Policy app (iOS).

G Suite technical references

- Set up managed apps for Android devices—G Suite Admin Help
- Use the Google Device Policy app on iOS—G Suite Learning Center

4.2 Access

Within the organization, all employees need to access documents independently of the collaboration platform used. Based on this idea, the following coexistence scenarios are listed.

Scenario: Internal collaboration on G Suite documents

G Suite users create and edit documents directly in Drive. This is done using one of the Google Docs editors (Docs, Sheets, or Slides) or with a third-party editor approved by the company for use on Drive (for example, AutoCAD, Lucidchart, or Sketchboard). These documents are available for internal collaboration and can be easily shared with partners and customers.

User experience

1. Sharing a file on Drive with a colleague is done using the Share button.
2. As you start entering text, you can select the name of any person in the company from the suggestions.
3. The colleague (either on G Suite or Office 365) receives an email message with a sharing notification and can directly open the document from the message.
4. Depending on the sharing security settings, the collaborator can read, comment, and edit the document.

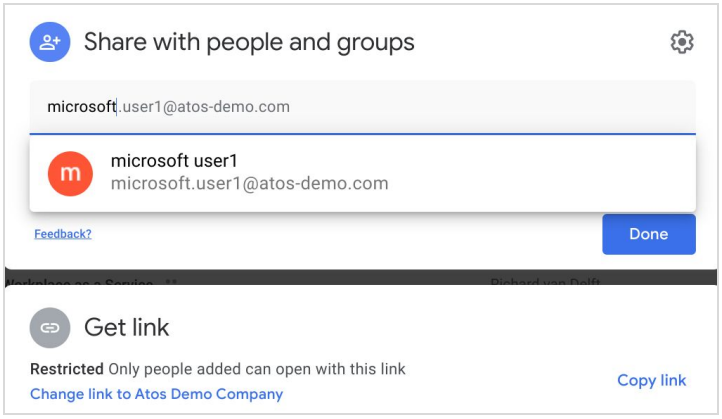


Figure 12: G Suite user sharing a document with a colleague using Office 365

Notes

- Drive also natively supports external sharing. A file or folder stored in Drive can be securely shared with partners and customers using a Google Account.
- Visitor sharing in Drive is another way to invite users to collaborate on G Suite files using verification codes. Visitors with a code can view, comment, suggest edits, and directly edit documents, as well as other file types like PDFs and Office files. Learn more

G Suite technical references

- All employees with a G Suite or a Cloud Identity license are listed in the Google Directory. This ensures they have access to Drive content using an identity controlled by the company. Learn more
- Choose which third-party apps users can install in Drive from the G Suite Marketplace. Learn more
- Share files from Google Drive—Google Drive Help

Scenario: Internal collaboration on Office 365 documents

Documents created in Office 365 can be shared from OneDrive or Teams with G Suite users. This means employees using Office 365 can collaborate on documents with users on G Suite.

User experience

1. Employees using Office 365 share a document or OneDrive folder with their G Suite colleagues.

Additional considerations

- For this scenario to work, the identity of the G Suite user might need to be provisioned in Office 365 and a license might be needed.

Scenario: Locate documents across platforms

As a manufacturer, the company creates lots of documentation. This content is stored in Drive, Teams, SharePoint, OneDrive, Salesforce, or the on-premises enterprise document management system.

The organization uses Cloud Search as their enterprise search system. They selected this search solution based on its ability to connect to many different content repositories, its artificial intelligence and machine learning capabilities, and the different languages supported.

The company used Cloud Search to index and integrate multiple content repositories:

- G Suite, including Gmail, Drive, and shared drives
- Office 365, including Outlook, OneDrive, and Teams
- A cloud-based CRM
- An on-premises intranet
- An on-premises enterprise document management system

User experience

1. All employees can use the search homepage (*https://search.example.com*). After authorization, the Cloud Search page offers access to all indexed content the user is permitted to view.
2. Cloud Search is also loosely integrated into other applications. While it could replace an application's built-in search feature, the company opted to add a Cloud Search button in the application's search result pages. This way the application's built-in search can be used with the Cloud Search application to improve search results from other sources with just one click. After integration, this coexistence strategy resulted in the best user feedback.
3. A custom search application was built for support engineers. The search application only finds technical documentation in the on-premises enterprise document management system.

The advantage of coexistence between built-in application search and Cloud Search is that within Cloud Search company data from multiple data sources is combined into a single result

page. Assist cards in the Cloud Search results page highlight the relevant answer to search queries based on the indexed information.

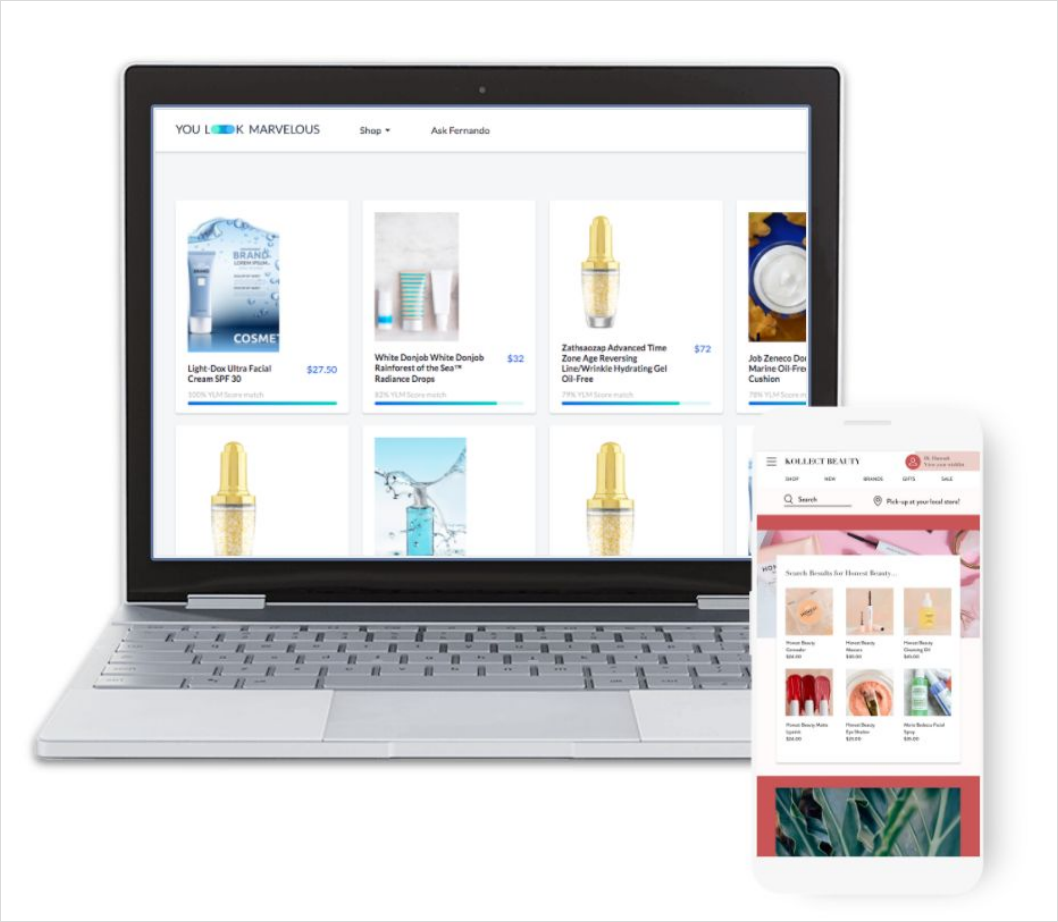


Figure 13: Custom Cloud Search application with assist cards on a third-party site

G Suite technical references

- Cloud Search is part of G Suite services but can be obtained separately. Licensing is based on the indexed content, search queries, and number of custom search applications created.
- The search results page shows assist cards next to the content returned. Information displayed on the cards is from one or more data repositories. For more information, go to Cloud Search Help
- For the custom search application built for support engineers, a Cloud Search interface was created.

4.3 Create

Inside the organization, all employees need to create and store documents independently of the collaboration platform used. Based on this idea, the following coexistence scenarios are listed.

Scenario: Edit existing Office 365 documents in G Suite

Within the company, most of the existing files were created in Office 365. Drive offers built-in support to open, comment, and edit existing Microsoft Word, Excel, and PowerPoint files. No technical setup is required in the Admin console to support Office file formats. Learn more

Files created in Drive can also be shared in Office file format using the G Suite document editor menu option Email as attachment. These files can also be downloaded in Office file format using the menu option Download as (in case you need to upload an Office file to a website).

User experience

1. Office files are uploaded to Drive or exist there after files were migrated into Drive.
2. When opening a document in Office file format from Drive, a preview is provided. To edit the document, the option “Open with Google” is available.
3. The Office document is edited in the G Suite document editors and a visual indicator next to the filename indicates the document is in Office file format (for example, .docx).
4. Some Office file formats are not supported in the G Suite document editors. Unsupported items are listed in a dialog when editing.

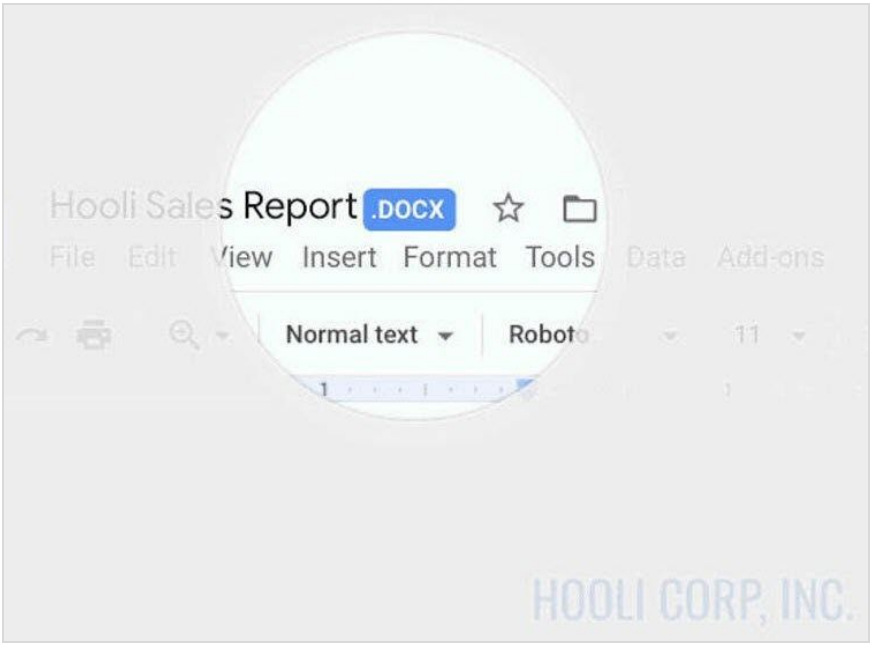


Figure 14: Word document in Google Docs editor

G Suite technical references

- Work with Microsoft Office files—Google Drive Help
- Guides for Switching from Microsoft - G Suite Learning Center

Scenario: Access departmental drives

The organization deployed Drive File Stream on Windows and Mac devices. This allows employees to save their files on Drive similar to a network file server. Within computer applications, employees can use a network drive to find files on Drive and open them.

User experience—Drive File Stream within an application

A marketing employee collaborates with an external video company to create a video. The large video files are stored in Drive. This provides flexibility for the employee as these large files (up to 5 TB) can be stored and shared with the external vendor.

1. The marketing employee opens a video editor on a Windows PC.
2. From the video editor, the employee can use the file selector to navigate to a file (served up using Drive File Stream), select it, and click Open.
3. The video opens in the video editor. Edits are saved directly to the file on Drive.

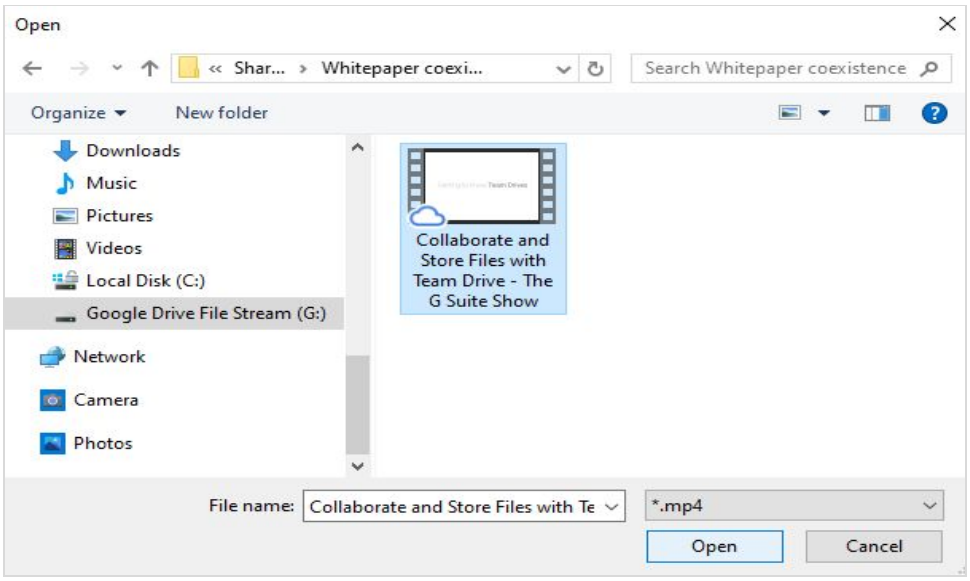


Figure 15: Drive File Stream with video file

User experience—Drive within a browser

1. The marketing employee navigates to a file in Drive.
2. The employee double clicks the video file. The file opens in the Drive file viewer and the video starts playing automatically. Drive offers many online viewers for common file formats.
3. When the employee wants to edit the file, they can use “Open with” in the viewer to select a video editor.

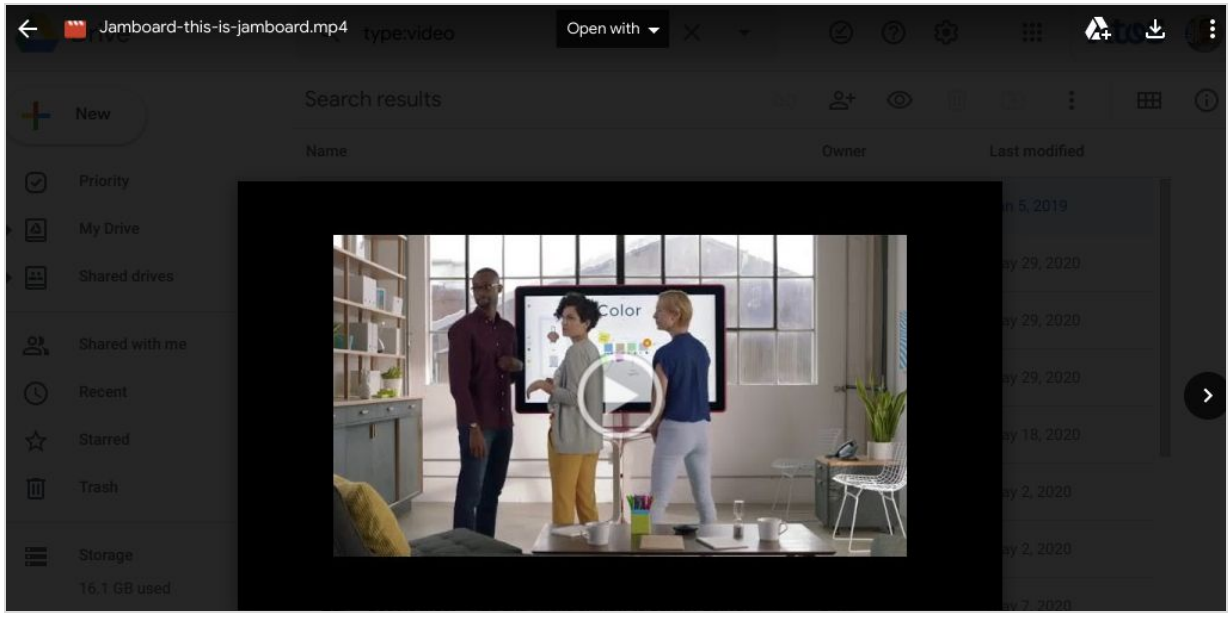


Figure 16: Drive file viewer plays video without opening an app

G Suite technical references

- Use Drive File Stream with work or school—Google Drive Help
- Any file type (up to 5 TB in size) can be stored in Drive. For file sizes and supported file types, go to Files you can store in Google Drive—Google Drive Help.
- While not used by the company, the Chrome Browser extension Application Launcher for Drive can be installed to open Drive files directly from the browser within compatible applications on the computer. Learn more

Scenario: Company style guide

The company has a branding style guide for their documents, presentations, and spreadsheets. Employees are responsible for applying the branding style guidelines on all documents, both internally and externally. To provide consistent document structure, the organization offers several templates for document creation ranging from a simple memo template to more advanced ones for technical documentation. Templates are all provided in the company standard language of English. Besides corporate templates, specific department-level templates are also provided.

User experience—G Suite

- Employees begin file creation in Drive where they can select a template from the template gallery of the specific G Suite document editor (Docs, Sheets, Slides, or Forms).

The template gallery shows an overview of all available templates, categorized by intended use.

- Templates in Drive contain the text structure and utilize the branding guidelines.

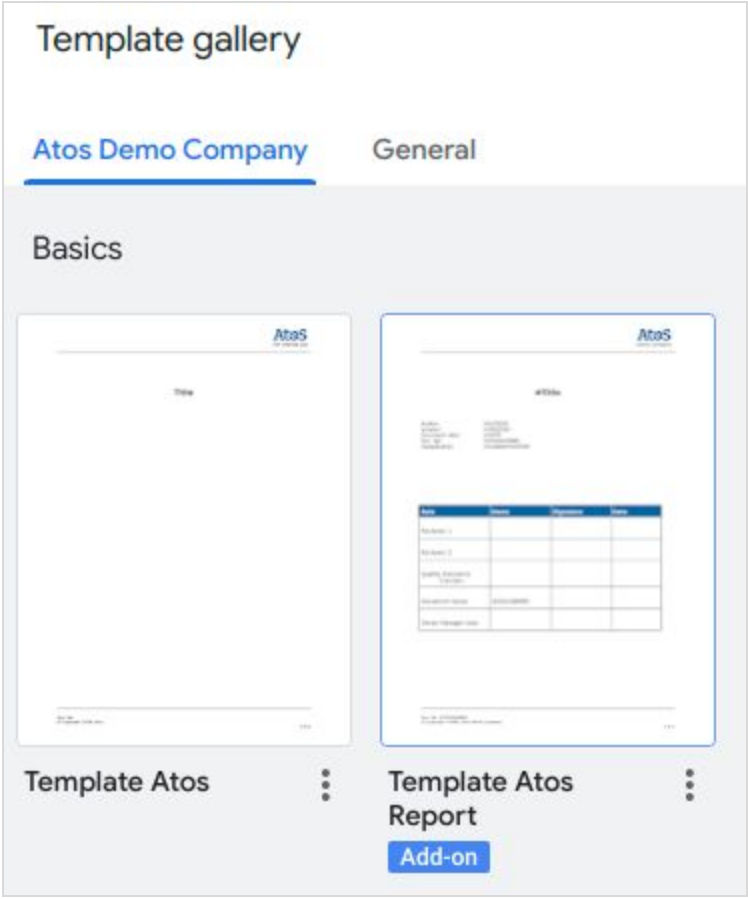


Figure 17: Company template gallery

User experience—Office 365

- The company uses traditional file shares to make company templates available that users can open and reuse in their Office 365 applications.

User experience—cross-platform, department-level templates for Corporate Communications

- Since corporate templates are needed on both platforms, the Corporate Communications department maintains all platform templates.

- New template files, or edits to existing templates, are completed within the G Suite editors or Office editors. This ensures the branding guidelines are correctly applied and it prevents conversion formatting issues.
- While not in use at the company, there are third-party tools available to provide a single template gallery for both G Suite and Office 365 users.

G Suite technical references

- Create custom Drive templates—G Suite Admin Help

Scenario: Preserve documents for archiving compliance

Certain files must be archived within the company for 20 years. This compliance regulation is for documentation related to the products they manufacture. These documents are typically stored in the enterprise document management system in PDF format.

Employees also sometimes need to work with existing PDF documents (for example, PDFs sent by customers).

User experience—save as PDF files

- A G Suite user creates a document using a G Suite document editor.
- After collaboration and finalization, the document needs to be saved as a PDF file in the enterprise document management system.
- In the document editor, a Google Docs add-on is available to store the document directly in the document management system as a PDF file. On save, the required metadata is requested.
- Alternatively, the user can select File > Download > PDF Document in the G Suite document editor to download the file.

User experience—open PDF files

- Every G Suite employee can open PDF documents accessible in Drive. The file can either be opened in the built-in Drive viewer or within a local PDF application (for example, Adobe reader) depending on the user's preferences. If the PDF contains form fields, the user can fill them in.
- To edit a PDF, the G Suite user can open it in Docs. It uses Optical Character Recognition (OCR) capacities to convert the document into text so it can be edited.

G Suite technical references

- View Drive items like videos, PDFs, Office files, audio files, and photos: View & open files—Google Drive Help

- Convert PDF and photo files to text—Google Drive Help
- Fill out PDF forms in Google Drive—Google Drive Help

4.4 Control

For administration and security, it's not just coexistence but also making sure both systems are set up consistently with the same security features and reporting options. This provides users on both platforms with a similar user experience.

The following section describes the G Suite setup of certain company policies.

Scenario: Device management

The company has a BYOD policy. Each collaboration platform comes with a mobile device management solution. The current IT strategy means devices are maintained either as part of the Google platform or as part of the Microsoft platform.

Every company mobile device with G Suite or Office 365 uses G Suite's basic endpoint management solution. This ensures Office 365 users always have the minimum security in place if they utilize G Suite on their mobile devices. And since G Suite's basic endpoint management doesn't require an agent on the device, it can be used with different mobile device management solutions.

For global reporting of mobile device management, multiple platform reports are exported and integrated into a single spreadsheet to provide insights on mobile device use.

Devices running Windows 10 and Office 365 within factories are managed using Intune to ensure a modern workplace management system. The Admin console is used to manage Windows 10 devices for G Suite users. The company also deployed Chromebooks for G Suite users, with the Chrome OS managed in the Admin console.

Note: Chrome endpoint verification is mandatory on all devices when accessing G Suite services through the browser. Google endpoint management lets the admin view information about the device and control access to apps based on location, device security status, or other attributes.

User experience

1. When an employee adds their enterprise email address as an account on their personal device, the basic mobile device management profile is applied. Admins do not need to approve the device.

   a. The basic mobile device management profile makes sure the device has password protection turned on. It also allows IT management to lock or remove corporate data from lost or stolen devices directly from the Admin console.
2. G Suite users get a mandatory work profile on their Android device. For iOS devices, employees get a mandatory Google Device Policy app.
3. G Suite mobile device management offers many policies for Android and iOS devices. The following were applied:
   a. Devices are encrypted.
   b. Devices are not compromised, meaning no iOS jailbreaking.
   c. Only apps on the allowlist can be installed on the device. This is not limited to Google apps but can be applied to any other app, including those from Microsoft.
   d. Corporate data cannot be copied to non-corporate applications or stored in iCloud.

G Suite technical references

- Set up basic mobile device management—G Suite Admin Help
- Automate mobile management tasks with rules—G Suite Admin Help
- Enforce advanced policies for compromised devices and device encryption: Apply advanced settings—G Suite Admin Help
- Control how users interact with their Android device by applying a work profile and verifying apps: Apply settings for Android mobile devices—G Suite Admin Help
- Enforce advanced policies for data protection and iCloud storage on managed iOS devices: Apply settings for iOS devices—G Suite Admin Help
- Overview: Windows management settings—G Suite Admin Help
- Overview: Manage devices with Google endpoint management—G Suite Admin Help

Scenario: Identity Management

For a great user experience in a coexistence situation, it's vital to create a central identity management repository. There are many identity management solutions available to provide synchronization with other directory services.

The company kept their on-premises Active Directory to unify identity management. By centralizing the directory for all systems, they have one source of truth for corporate identities. This strategy also had minimal impact on existing on-premises applications and hardware such as printers, which still rely on the on-premises Active Directory.

Requests to get a new identity, change an existing account, or remove an account are automated using the IT service management (ITSM) portal. The portal creates the account in the on-premises Active Directory, which is synced to G Suite and Office 365. Depending on the

requested access rights, one or more approval workflows might be generated before the account is authorized. These workflows are managed outside of G Suite or Office 365.

User experience

1. A department manager must provide information using the ITSM. They list the account information, application authorizations, and device requirements.
2. The account is created within the on-premises Active Directory and added to the proper security groups.
3. The account is automatically synced into the Google Directory using the provided server solution Google Cloud Directory Sync (GCDS). This product also supports account updates and deletes from Active Directory to Google Directory. It can also sync groups, resources, and contacts.
4. A similar sync workflow is used from Active Directory to Office 365 using Azure Active Directory Connect.

G Suite technical references

- About Google Cloud Directory Sync—G Suite Admin Help

Scenario: Access management

In user authentication, 2 architectural approaches are possible:

1. **Relying on a cloud-based identity provider**—G Suite comes with Cloud Identity which offers built-in authentication functionality like password lifecycle, 2-Factor Authentication, risk management, and alerts. Cloud Identity can be set up as the unique cloud-based identity provider for any SAML 2.0-based application. With Secure LDAP, Cloud Identity can also connect to legacy on-premises LDAP apps. Lastly, Cloud Identity can provide password vaulting help for old web apps that do not have SAML 2.0 compatibility.
2. **Setting up SSO between an on-premises identity provider, G Suite, and Office 365**—This is also a popular option since both G Suite and Office 365 can offer SSO through Active Directory Federation Services or any other SAML 2.0 identity provider. These tools allow for a standardized authentication flow among different cloud providers. However, it can add overhead to the network infrastructure as it requires redundancy, high availability, and low latency.

In our scenario, the company decided to embrace Cloud Identity as the new baseline for secured on-premises and cloud authentication. While most of the existing on-premises apps are still signing in with Active Directory or Active Directory Federation Services, the goal is to migrate them to Cloud Identity. Office 365 was already set up to sign in against Cloud Identity.

As part of their security framework, the organization implemented Context-Aware Access to check any device accessing G Suite against current company security policies. Only encrypted devices running an updated operating system are authorized. Learn more

User experience

1. A user (on either G Suite or Office 365) navigates to a business cloud solution (for example, a cloud CRM solution).
2. The CRM asks the user to sign in with SSO.
3. The default Google sign-in box with 2-Factor Authentication is provided.
4. Context-Aware Access verifies the device before granting access to the CRM solution.

G Suite technical references

- Cloud Identity now provides access to traditional apps with secure LDAP—Google Cloud Blog
- Automated user provisioning for SAML apps—G Suite Admin Help
- Context-Aware Access overview—G Suite Admin Help
- Control which third-party & internal apps access G Suite data—Cloud Identity Help
- Endpoint Verification—Chrome Web Store
- Set up endpoint verification on your computer—G Suite Learning Center

Scenario: Groups and organizational units

Google Admin console settings can be set at the organizational unit level or assigned to a Google Group. The company uses both organizational units and groups.

Organizational units are only used for users with different licenses. For example, frontline workers are in a different organizational unit than inside office workers. Google Groups are used to apply specific security access settings to certain applications. By assigning application access to a specific group, the administrator makes sure members of the group have access to the app even if the organizational unit doesn't grant this access.

The on-premises Active Directory contains all users and groups. Active Directory syncs to G Suite (and other systems, like Office 365). Some groups are also used within the Admin console to apply a specific G Suite set up or to provide access to an application.

User experience

1. A user needs access to a project management planning application and requests the application in the ITSM portal.

2. The portal automatically adds the user account to an Active Directory group.
3. The Active Directory group is synchronized to the Cloud Identity directory as a Google Group.
4. The user gets access to the SAML-based application as the Google Group is now set up to provide access.

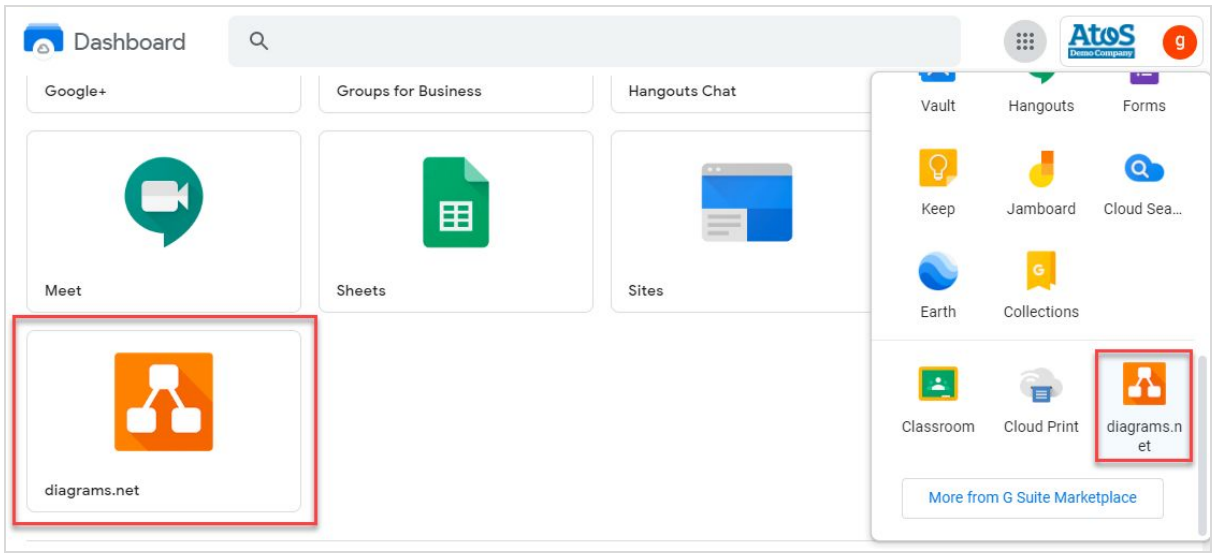


Figure 18: SAML-based applications in the G Suite Dashboard. (Note that extra application authorizations are visible in the dashboard and under the profile button.)

G Suite technical references

- Set up your own custom SAML application—G Suite Admin Help

5. G Suite Essentials

Google recently introduced a new G Suite edition called G Suite Essentials. This edition offers Google Meet for secure video meetings; Google Drive for cloud storage; Google Docs, Sheets, and Slides for content creation; and administrative controls. You also get many of the features of other G Suite editions but without the cost of services you might not need, like Gmail and Calendar.

There are 2 offerings: G Suite Essentials and G Suite Enterprise Essentials, which provides advanced security and Meet features. Compare key features

This whitepaper focuses on the split coexistence scenario where the example company decides to equip some users with G Suite and others with Office 365. G Suite Essentials introduce a new coexistence scenario called dual coexistence. Here is an example:

- A company chooses to deploy Office 365, or some dedicated Microsoft cloud products, to all the employees. These products include Exchange Online with an Outlook client to send and receive emails, and rich Office clients to view and edit Office files.
- The same company also wants to use a web-based, responsive, and easy to deploy collaboration solution with Drive for file storage and sharing, and Meet for secure video meetings. They use G Suite Essentials along with Office 365 for a coexistent solution.

User experience

- Google offers an Outlook add-on to make it easy to add a Meet video conference in an Outlook calendar invite.
- Office files can be stored in Drive and opened locally with a rich Office client. They can also be previewed and edited within the G Suite document editors (without format conversion).
- An Office file opened with a G Suite document editor receives the same benefits as a regular Google Doc, including easy and secure sharing, real-time collaboration, offline work mode, auto saving, file versioning, etc.

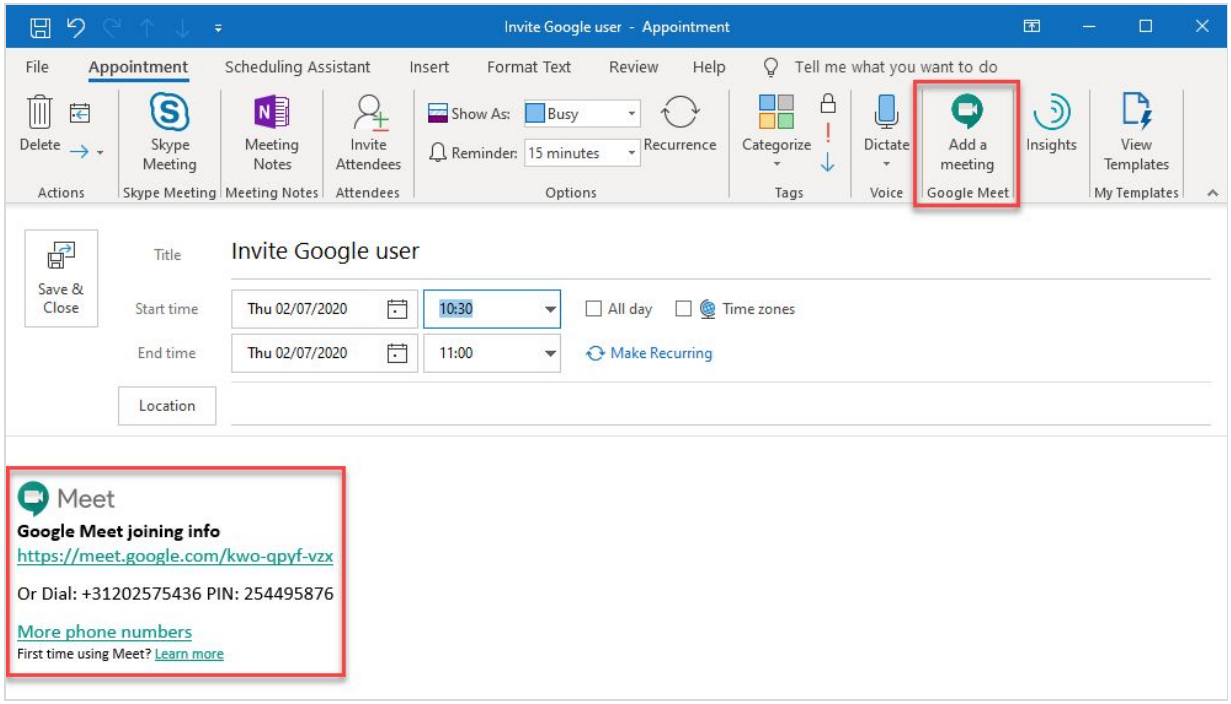


Figure 19: How a Meet video meeting invite appears in Outlook for an Office 365 user

G Suite technical references

- G Suite Essentials: The Simplest Way for Teams to Work Together
- G Suite Essentials edition—G Suite Admin Help
- Add Meet video meetings to Outlook—Google Meet Help

6. Additional resources

For more information on how G Suite services are designed with collaboration, privacy, and availability of data in mind, go to:

- G Suite Help Center
- Guides for Switching from Microsoft
- G Suite Data Protection Implementation Guide
- Trusting your data with G Suite
- Google security whitepaper
- Google Cloud & the GDPR