LM01_KDD007 - External Collaboration

Status	DECIDED
Owner	Eric Triffaux
Stakeholders	James Kyndt, Damien Avril, Frank Bolata, Boris Foiselle, Owen Pettiford

Decision: Option 5: B2B + Entitlement Management

Decision made by: Damien Avril, Owen Pettiford

Date: 07 Jan 2026

Online Meeting: M365 Key Decision - External Collaboration

Why B2B Guest Collaboration is the Path Forward

The Challenge: Outdated and Unsecure Collaboration

Historically, our approach to external collaboration relied on simple domain whitelisting. While this allowed some level of interaction with partners, it came with significant limitations and risks:

- Lack of Control: No granular management of who could access what information.
- Security Risks: Unrestricted sharing increased the risk of data leaks and unauthorized access.
- Inefficient Collaboration: Partners and external stakeholders faced barriers, slowing down projects and innovation.

The Opportunity: Embracing B2B Guest Collaboration

As we migrate from Google Workspace to Microsoft 365, we have a unique opportunity to modernize how we collaborate externally. B2B Guest Collaboration offers a structured, secure, and flexible way to work with partners, suppliers, and customers:

- Granular Access Control: Assign specific permissions to each guest, ensuring the right people have access to the right resources—no more, no less.
- Enhanced Security: Monitor and manage external access, reducing the risk of data breaches and ensuring compliance with internal and external regulations.
- Seamless Collaboration: External partners can securely access shared documents, participate in Teams meetings, and contribute to projects as if they were part of our organization—without compromising our data.
- Scalability: Easily onboard and offboard guests as projects evolve, maintaining agility without sacrificing control.

The Vision: Towards Entitlement Management

Our long-term goal is to implement Entitlement Management—a system that automates and governs access rights for both internal and external users. This will allow us to:

- Automate Access Lifecycles: Grant, review, and revoke access based on business needs and project timelines.
- Ensure Compliance: Maintain a clear audit trail and demonstrate compliance with industry standards.
- Empower Business Owners: Enable project leaders to manage access without IT bottlenecks, accelerating innovation.

Conclusion

By moving away from unsecure, manual processes and embracing B2B Guest Collaboration, Syensqo positions itself as a modern, agile, and secure organization—ready to drive scientific breakthroughs through seamless and trusted partnerships.

Personas

Guests Are external users outside of Syensqo who only require access to content shared in M365 (e.g. Sharepoint), and to collaborate with Syensqo users on this content. Their work is generally not carried out using Syensqo IT systems, and their work is generally not directed by Syensqo employees or governed by Syensqo policies and procedures.

Examples of External Users could be:

- an external auditor
- an employee of a customer of Syensqo collaborating on product specifications
- an Account Executive of an IT outsourcing provider collaborating with Procurement on an IT Services contract
- external legal counsel

Contingent workers are non-employee workers who are represented in the SuccessFactors org structure and may fulfil a number of different roles at Syensqo. They *do* require access to IT systems beyond M365 in order to perform their work, and their work is generally directed by Syensqo personnel and carried out in accordance with Syensqo policies and procedures.

Examples of External Users could be:

- contractors who are back-filling a permanent employee on long-term leave
- Employees of an IT outsourcing provider performing work in Syensqo IT systems, such as consultants working on projects such as SyWay or LEAP
- Employees of a 3PL provider working in the warehouse owned by the 3PL, but processing logistics transactions using Syensqo systems.
- User who need to access a syensqo asset such as server or workstation.
- User who need to get elevated privileges.

By definition, Guest users and Contingent workers are non-overlapping sets. All, or the vast majority of, the ~3,966 people in SuccessFactors flagged as 'External' are by definition *not* External users as per above.

Because they perform work in Syensqo systems other than M365, and are subject to Syensqo policies (thus requiring access to learning systems, The Hub intranet, etc.), they will require a proper Syensqo EntraID account and some kind of M365 license.

The exact type of license can be determined based on need, and we should not assume that an E5 license is needed by default. Lower-cost licenses such as F3 may suffice for their work.

Recommendation

Scenario 5: B2B + Entitlement Management

Background & Context

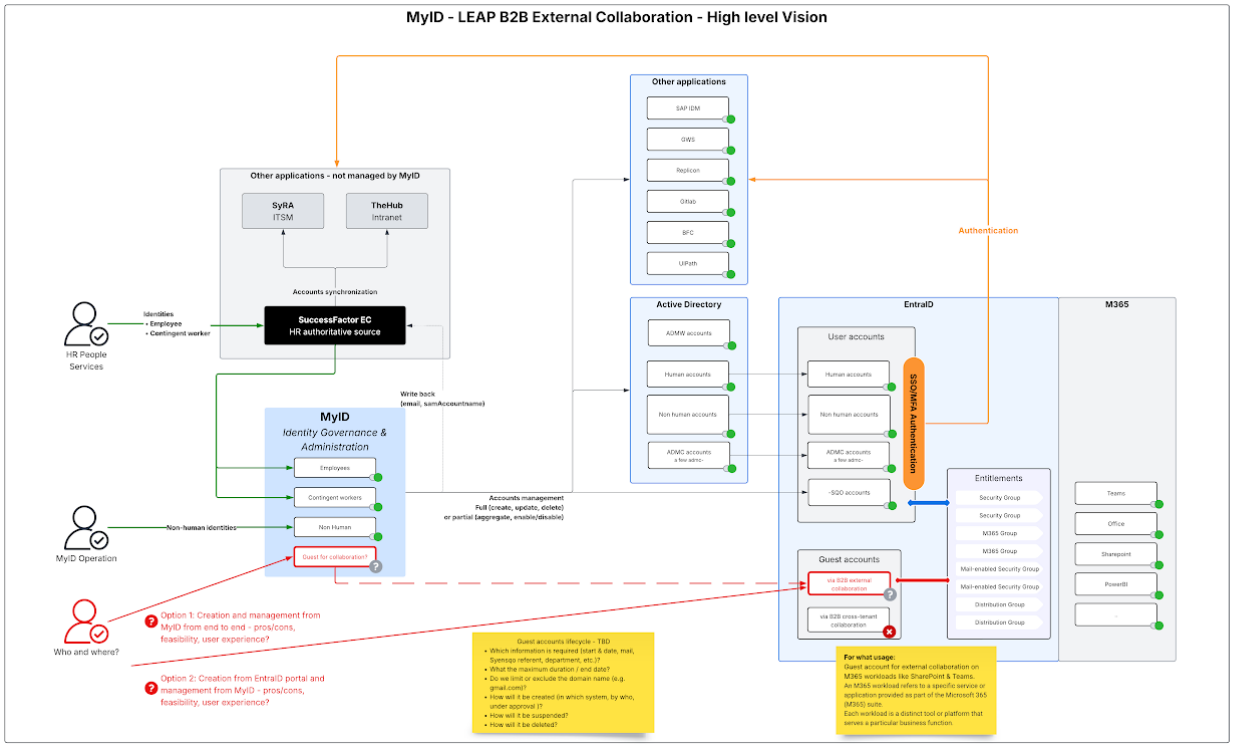
No information on Google personal MyDrive document sharing with externals.

154 domains whitelisted between AODocs and Shared Drive.
That represent **External sharing with 1572 users**, not covered by contingent worker identity (**Guests**)

.
In addition **2368 contingent worker users covered by a microsoft license.**

- **2368 Contingent users = $2,64M$/4y** potential optimisation on some F3 moving to Guest and few E5
- **1572 Guest Users** eligible to B2B collaboration

F3	GRP-License-M365 F3 Foundation	1568
	GRP-License-U_K-Lab-Accounts-DYNAMIC	0
	GRP-License-Entra ID P1-Shared mailbox	0
E5	GRP-License-M365 E5 Foundation	710
	GRP-License-M365 E5 Power BI Pro Only-Manual Assignment	12
	GRP-License-M365 E5_Full-Manual Assignment	8
	GRP-License-M365 Teams-User-Manual Assignment	4
P2	GRP-License-Entra ID P1 For external users	54
	GRP-License-Entra ID P1-Other users	12
	GRP-License-Entra ID P2	0
	Only -Ext	**2368**



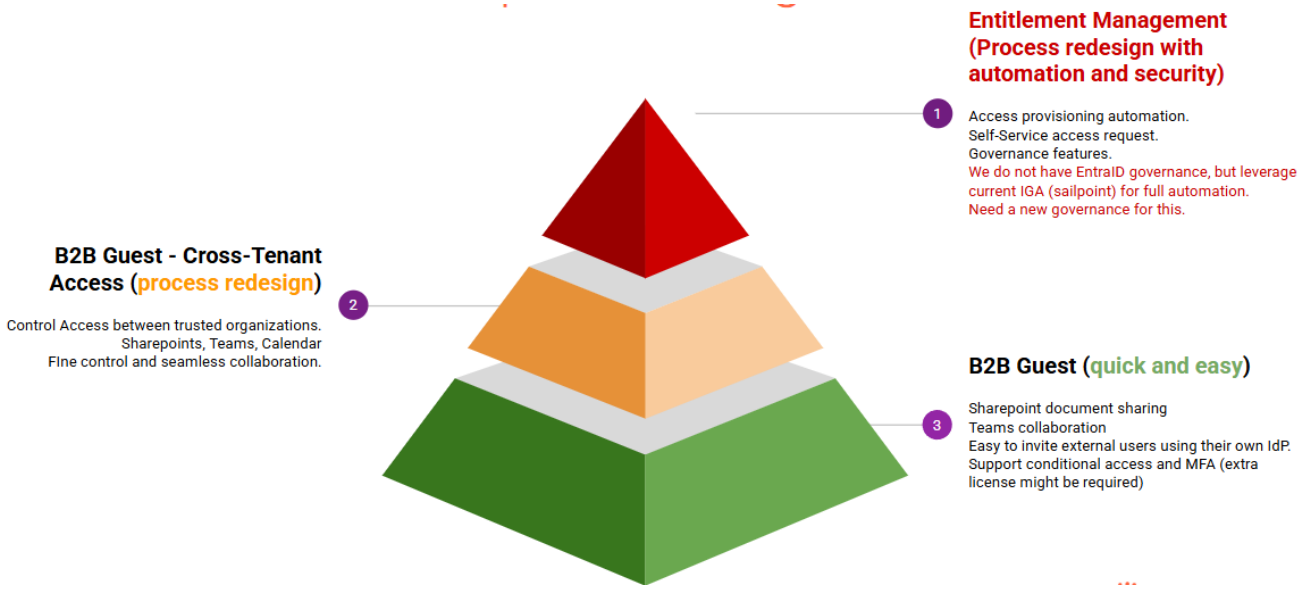
	Eligible applications						
Human Identity type	**AD/EntraID**	**Syensqo MFA**	**Mailbox**	**On-premise applications**	**SaaS applications**	**M365 workload**	**Comment**
Employee	Yes	Yes	Yes	Yes	Yes	Yes	Same as today
Contingent worker	Yes	Yes	Yes	Yes	Yes	Yes	Same as today Mandatory for external requiring access to onpremise application or applications integrated with SSO, except M365
Guest for collaboration	No	Maybe - depending if default guest authentication flow is acceptable in terms of security - need to deep dive	No	No	No except in certain cases where the application supports multiple types of usernames for authentication and account provisioning	Yes under condition (lifecycle management, secured authentication flow with MFA or at least security approval, access management RACI/process)	For external collaboration - not to replace all contingent workers i.e. equivalent to Google external sharing

Identities

Human Identity type	**AD/EntraID**	**Syensqo MFA**	**Mailbox**	**On-premise applications**	**TPA / Workstation**	**SaaS applications**	**M365 workload**	**Comment**
Employee	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Same as today
Contingent worker*	Yes	Yes	Yes	Yes	Yes if non Saas application.	Yes	Yes	Mandatory for external requiring access to on-premise application or applications integrated with SSO, except M365
Guest for collaboration	No	Maybe – depending if default guest authentication flow is acceptable in terms of security – need to deep dive	No	No	No	No	Yes (under condition: effective license management, secured authentication with MFA or at least security approval, access management/ACL/process)	For external collaboration – not to replace all contingent workers, equivalent to Google external sharing

*some contingent worker might be eligible to Guest, while only using GWS / M365 platform.
No need to provide a workstation.
No need to access other Syensqo applications.

Collaborate with 3rd parties using M365?



Options considered

Option 1: no external sharing Solution by default without consensus

- **a.** Major Business impact

Option 2: TODAY in GWS (uncontrolled sharing and domain whitelisting*)

- **a.** Major Security risk (domain whitelisting only)
- **b.** Teams chat need an account to collaborate
- **c.** Sharepoint will rely on anonymous or link-based sharing with very limited control (no Conditional Access, no MFA, no lifecycle management).

Option 3: External using contingent worker identity only

- **a.** Expensive

Option 4: B2B + DLP Integration

- **a.** Not improving the security risk of external sharing and guest management
- **b.** Reduce the cost while not obliged to provide license to all externals

Option 5: B2B + Entitlement Management

- **a.** Requires new processes and governance to manage the guest collaboration
- **b.** Improve licenses : 1600 external guest users and an additional 1600 contingent workers who might not need Syensqo accounts.

Why: Option 5: B2B + Entitlement Management

The decision was made to select **Option 5**, as it ensures the same level of security and collaboration. Additionally, during the transition from GWS to M365, we will be able to achieve stronger security through measures such as disabling anonymous sharing, blocking external sharing, and enforcing sharing link expiration.

This is only the beginning of the external collaboration journey, referred as **Phase 1: Foundation & Risk Mitigation**, and it serves as a directional guide for the future.

The subsequent phases — **Phase 2: Controlled B2B Pilot, Phase 3: Operationalization & Governance, and Phase 4: Expansion & Application Access** — represents the path toward the target operating model and require deeper and broader analysis, which is outside the scope of the M365 Migration project.

Phase 1: Foundation & Risk Mitigation

Objective: Replace legacy domain whitelisting

Actions:

- Audit current external sharing practices
- Disable anonymous sharing and Block Onedrive external sharing
- Implement baseline for guest sharing
  - Put in place Domain whitelisting & blacklisting as intermediary step and allow guest only on specific sharepoint sites
  - Sharing Link Expiration policy
  - Conditional Access + Guest Lifecycle
- Begin DLP policy design for external collaboration
  - Allow external sharing only on public document

Phase 2: Controlled B2B Pilot

Objective: Enable secure collaboration for Guest

Actions:

- Enable Microsoft Entra B2B to accept guests
- Restrict access to M365 suite only (Teams, SharePoint, OneDrive)
- Apply DLP policies to shared content
- Collaborate with SYWAY to identify any impact on OnOffboarding

Phase 3: Operationalization & Governance

Objective: Institutionalize B2B collaboration
Extend to (RFP/project-based)

Actions:

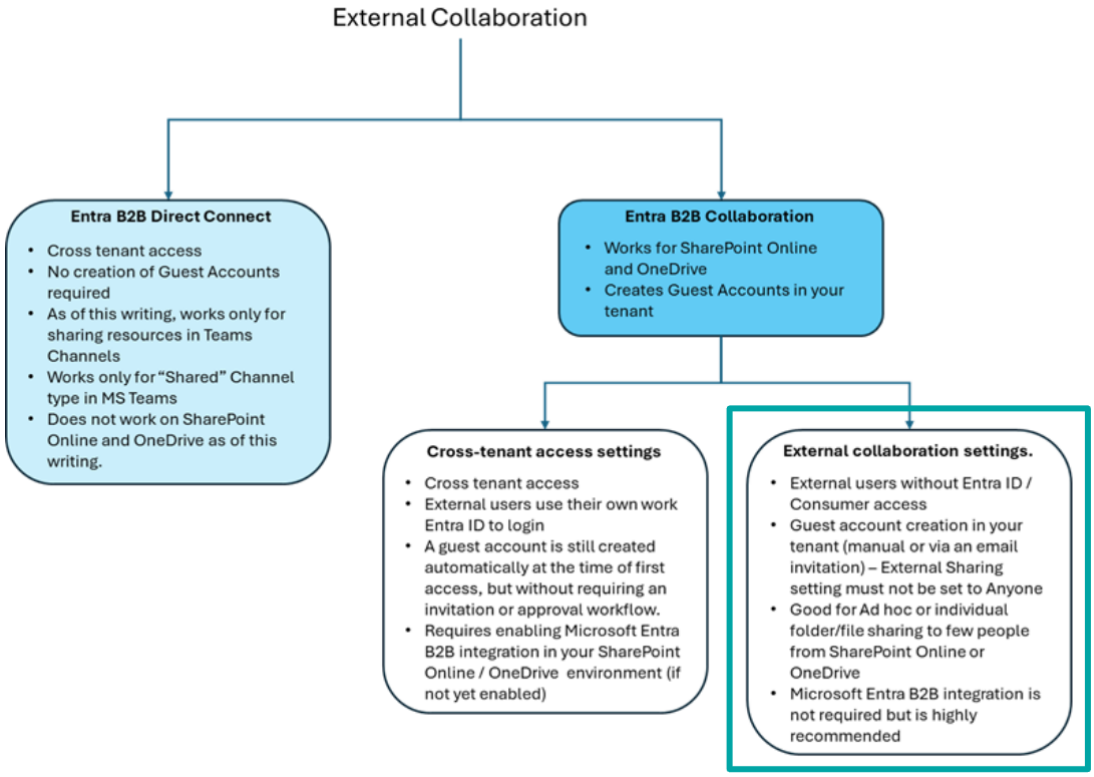
- Define the governance model for entitlement management and access package. Time-Bound Access Packages
- Integrate with SYWAY for full lifecycle management
- Establish reporting & compliance dashboards
- Enforce Supplier control to optimise M365 licenses.
- Communicate new process

Phase 4: Expansion & Application Access

Objective: Broaden guest access to additional apps

Actions:

- Define application access tiers for guests
- Extend Conditional Access and DLP to other applications.
- Monitor usage and refine policies
- Evaluate license impact and optimize



Reference Material from Avanade:

SailPoint & Entra ID Entitlement Management

HOW	WHO	WHAT
• Entra ID Connector is used to access and manage identities, including those of Guests. • SailPoint retrieves access package assignments and incorporates them into a governance process.	• Entitlement Management handles the onboarding and offboarding of guests, as well as managing access packages. • SailPoint conducts access certifications for guest accounts and enforces policies, including Segregation of Duties (SoD) checks.	• Upon invitation of a guest through Entitlement Management, SailPoint identifies the new user and enforces governance policies. • SailPoint is capable of deprovisioning users if certification is not passed or if policies are breached.

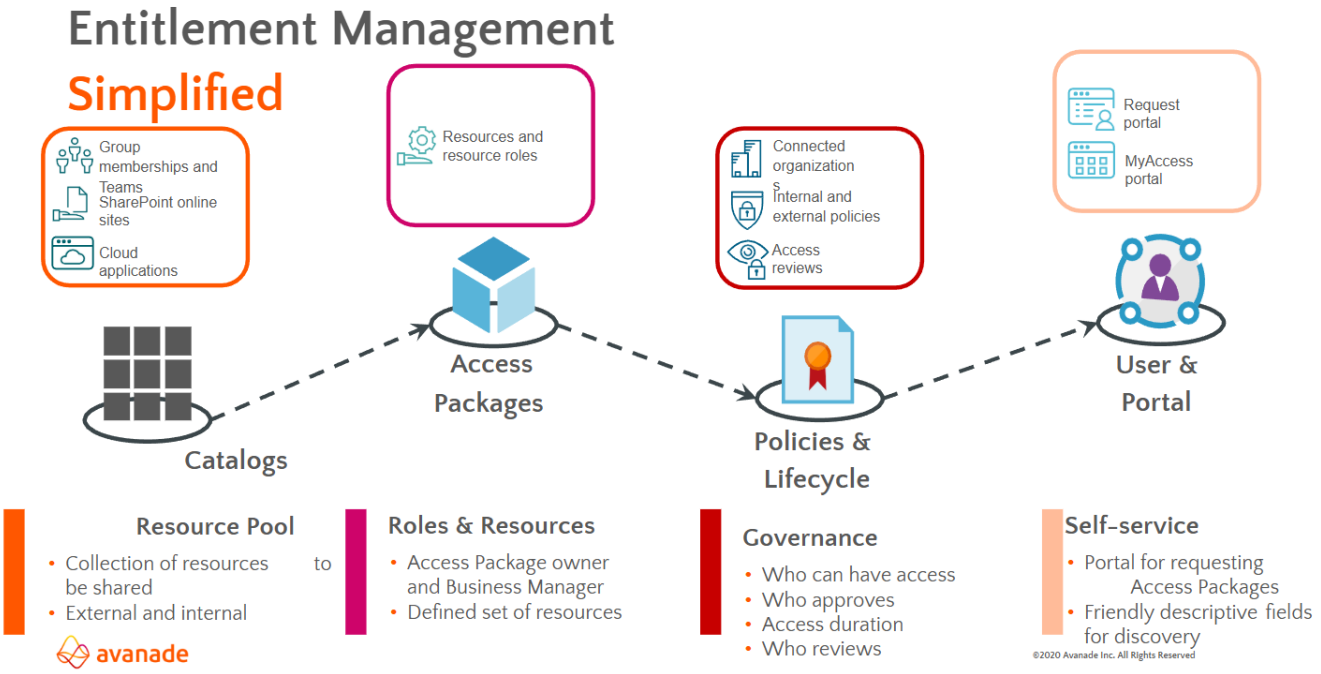
SYENSQO

SailPoint & Entra ID Entitlement Management

Dimension	TODAY with SailPoint	TOMORROW with Entitlement Management	Added Values
Time Savings	Lifecycle automation across hybrid systems, but manual effort may remain for Microsoft-specific workflows	Native automation of access packages, approvals, and entitlement workflows directly in Microsoft 365/Azure	Faster onboarding/offboarding, reduced manual approvals, streamlined access requests
Operational Efficiency	Strong governance and compliance, but workflows may require custom integration with Microsoft apps	Out-of-the-box integration with Microsoft ecosystem (Teams, SharePoint, Azure AD)	Simplified operations, fewer integration scripts, smoother collaboration
Financial Impact	Investment in governance tools, but potential hidden costs in manual provisioning and audits	Reduced administrative overhead, fewer audit penalties, lower integration costs	Cost savings from automation, reduced compliance risk, optimized licensing usage
User Experience	Governance is strong but user-facing processes may feel complex	Self-service access requests via Entra ID portals with automated approvals	Improved employee productivity, fewer IT helpdesk tickets
Compliance & Risk	Certification campaigns and audit trails managed centrally	Reinforced least-privilege enforcement with entitlement workflows	Lower risk of over-provisioning, stronger audit readiness
Scalability	Handles large-scale identity governance	Optimized for Microsoft cloud scalability	Easier expansion as Microsoft services grow

SYENSQO

12



See also

The following section describes relevant documentation:

Description	Repository
TDA External Collaboration Slide deck	https://docs.google.com/presentation/d/1UrysXwzm0eeTsaiBCxiKaWVHC80xTjEwUPJBPHmiFyQ/edit?slide=id.g36e7d99f663_0_0#slide=id.g36e7d99f663_0_0

M365 Key Decision - External Collaboration - meeting minutes	https://docs.google.com/document/d/13toX_XWHxZPxBSPqAEGEbx4KrCl4bgFrI5LtzLhCdjg/edit?tab=t.fwsr6ea1xvl4

Version	Published	Changed By	Comment
CURRENT (v. 24)	**Feb 19, 2026 11:49**	**CHUDZIAK-ext, Aleksander**	
v. 23	Feb 19, 2026 11:13	**CHUDZIAK-ext, Aleksander**	
v. 22	Feb 19, 2026 11:13	**CHUDZIAK-ext, Aleksander**	
v. 21	Feb 18, 2026 12:39	**CHUDZIAK-ext, Aleksander**	
v. 20	Feb 06, 2026 16:13	**CHUDZIAK-ext, Aleksander**	

Go to Page History

LM01_KDD001 - Migration Strategy