# Application Architecture SAP Identity Tooling

| | |
|---|---|
| **Status** | Approved |
| **Owner** | LOHIYA-ext, Sumitra |
| **Stakeholders** | HEALY-ext, Michael RUFFINONI, Francois CICHELLA, Domenico |
| **LeanIX Link** | SAP Identity Access Governance (IAG)<br>SAP Identity Provisioning Service (IPS)<br>SAP Identity Authentication Service (IAS) |


- Syensqo Identity Architecture — SAP Tooling Overview
  - 1) Purpose
  - 2) Scope
  - 3) Guiding Principles
  - 4) Landscape Overview
  - 5) Core Services (Responsibilities)
    - 5.1 SAP Cloud Identity Access Governance (IAG)
    - 5.2 SAP Cloud Identity Services (CIS)
    - 5.3 SAP BTP Connectivity & Cloud Connector (SCC)
- Key Decisions and Requirements
- Provisioning Architecture
  - Overview
    - IAG Subaccount Model
  - Application Architecture Components
  - Global User ID integration
- Network Architecture
- System Landscape
- System Access
  - Work Zone
    - System Access User Flow
- Application Security
  - Authentication Approach (SPInitiated SSO)
    - Human, SPInitiated SSO
    - Human, IdP-Initiated SSO
    - AI Agents
    - NonInteractive / ServicetoService & Destinations
  - Authorisations
  - Communication Security
  - Data Security
  - Other Controls
- Operation Architecture
  - Change and Configuration Management
  - Sizing
  - High Availability & Disaster Recovery
  - Maintenance Plan
- Exceptions
- See also
  - Terminology
- Change log


## Syensqo Identity Architecture — SAP Tooling Overview

### 1) Purpose

Provide a clear architectural overview of the SAP tools that enable identity and access management (IAM) across Syensqo's cloud and onpremise applications.

### 2) Scope

- SAP identity governance and provisioning across cloud and onpremise systems
- Standard joiner/mover/leaver (JML) processes and access request governance
- Risk and Segregation of Duties (SoD) control framework
- Periodic access certifications
- Connectivity, security, and operations considerations for the above

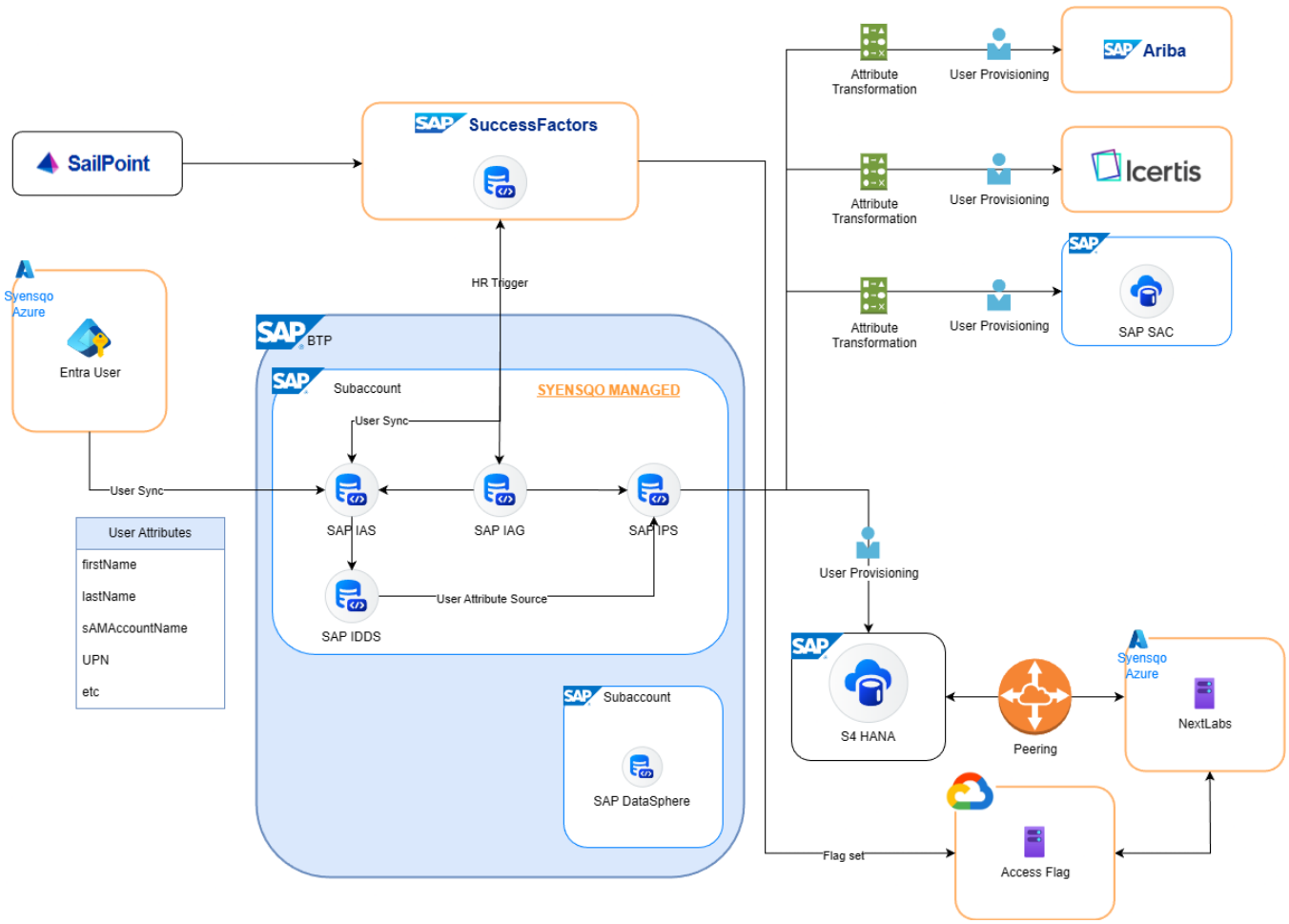
Implementation details for the various interfaces will be covered in the relevant specifications rather than in this document.

## 3) Guiding Principles

- **Cloudfirst:** Prefer SAP SaaS services on SAP Business Technology Platform (BTP).
- **Single source of identity:** SuccessFactors as the workforce truth; Cloud Identity Services as the identity broker.
- **Businessrole model:** Assign access through business roles; avoid direct technical role assignment.
- **Least privilege with controls:** SoD, risk analysis, and periodic certifications are builtin gates.
- **Standardsbased integration:** Use SCIM and established SAP connectors wherever possible.
- **Environment isolation:** Strict separation (DEV/TEST/PROD) for predictable promotion and auditability.

## 4) Landscape Overview

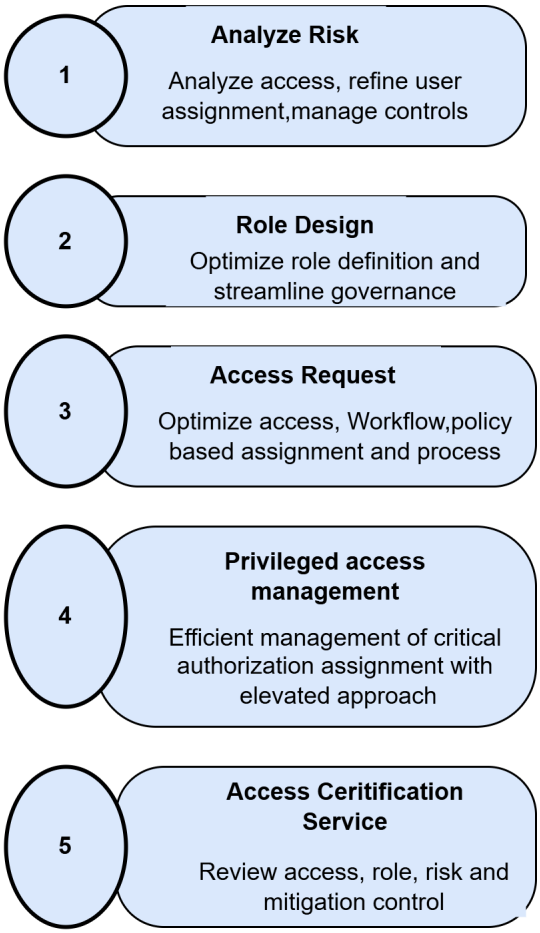
At the center is **SAP Cloud Identity Access Governance (IAG)**, delivered as a SaaS tenant on **SAP BTP**. IAG integrates with **SAP Cloud Identity Services (CIS)**—notably **Identity Authentication Service (IAS)**, **Identity Provisioning Service (IPS)**, and **Identity Directory**—to authenticate users, propagate identity data, and orchestrate provisioning to target applications.




## 5) Core Services (Responsibilities)

### 5.1 SAP Cloud Identity Access Governance (IAG)

- **Access Request & Workflow:** Central entry point for requesting and approving access for R2 Release. For future releases this will change to automated triggers from SuccessFactors for business roles.
- **Access Risk Analysis:** Builtin SoD and criticalaccess checks before and after assignment.
- **Role Design:** Businessrole centric design aligned to functions and processes.
- **Privileged Access:** Controlled elevation for critical activities (emergency access).
- **Access Certification:** Campaignbased periodic reviews for ongoing entitlement validation.
- **Audit & Reporting:** Endtoend traceability of requests, approvals, and provisioning events.




### 5.2 SAP Cloud Identity Services (CIS)

- **Identity Authentication Service (IAS):** SSO and authentication. Federates to Microsoft Entra ID; supports riskbased and MFA policies.
- **Identity Provisioning Service (IPS):** Orchestrates identity and role provisioning between sources (e.g., SuccessFactors) and targets (e.g., IAG, Ariba, SAC).
- **Identity Directory:** Central store for user and group objects used by IAS/IPS and downstream systems.

### 5.3 SAP BTP Connectivity & Cloud Connector (SCC)

- **Connectivity Service (BTP):** Managed egress from IAG to enterprise networks.
- **SAP Cloud Connector (SCC):** Secure reverse tunnel from onpremise to BTP so IAG can reach S/4HANA APIs without opening inbound firewall ports

## Key Decisions and Requirements

| Description | Rationale |
|---|---|
| Future Proofing | A strategic decision was made to future-proof Syensqo's identity management platform. SAP has made it clear that its primary investment focus lies in its SaaS offerings. **SAP IAG** and **CIS** are the flagship IAM solutions within this model, providing a broad range of capabilities for SAP landscapes. Aligning with SAP's strategic direction ensures long-term product viability and continued vendor support over the next 10–20 years. |
| Standardisation | "**Standard by default**" is the overarching architectural principle. Standard integrations should always be prioritised over custom developments. Customisation will only be considered when standard functionality cannot meet a **critical business requirement** necessary for process continuity. |

## Provisioning Architecture

### Overview

SyWay's SAP IAG landscape is delivered as a SaaS tenant on SAP Business Technology Platform, with the ability to connect to both cloud and on-premise systems. Environment alignment (DEV, INT, UAT, TRG, PRD) is achieved via dedicated IAG tenants in matching landscapes, ensuring consistent SoD enforcement and predictable deployments across stages. The architecture is cloud-first and region-agnostic, maintaining strict isolation of access-governance activities per environment while using SAP-delivered SCIM connectors for supported cloud apps (e.g., Ariba, SuccessFactors, iCertis, Work Zone). Integration with SAP Cloud Identity Services (IAS/IPS) standardizes provisioning flows.

### IAG Subaccount Model

**Runtime:** SAP IAG is delivered as a SaaS service on **SAP Business Technology Platform** (multi-tenant, no direct runtime selection).

**Naming:** syw-<area>-<env>-<region> (e.g., syw-iag-dev-eu10)

**Environment codes:** dev, int, uat, trg, prd

## Application Architecture Components

| Component | Description | Deployment |
|---|---|---|
| **SAP IAG Tenant** | Core SaaS service on SAP BTP delivering access requests, risk analysis, provisioning workflows, and audit reporting. | Cloud (SAP BTP, multi-tenant) |
| **Connectors** | Pre-delivered integration content for SAP cloud applications (SuccessFactors, Ariba, iCertis SCIM, Work Zone, S/4HANA). Uses SCIM or application APIs. | Configured per IAG tenant |
| **Acceus Risk & Policy Content** | Delivered by SAP to check Segregation of Duties (SoD) conflicts and critical access; extendable by customers. | Cloud (within IAG tenant) |
| **Workflow Engine** | Manages approval flows for access requests; configurable per tenant. | Cloud (within IAG tenant) |
| **Reporting & Audit Logs** | Provides access request history, provisioning logs, and risk analysis results. | Cloud (within IAG tenant) |
| **SAP Cloud Identity Services – IAS/IPS** | IAS: Authentication/SSO, federation. IPS: User provisioning between source identity and IAG/target systems. | Cloud (separate services, integrated with IAG) |
| **SAP Cloud Connector** | Secure reverse tunnel from onpremise to BTP so IAG can reach S/4HANA APIs without opening inbound firewall ports | On Prem |

## Global User ID integration

As Syensqo continues to modernize its operations and expand its digital ecosystem, SAP solutions are playing an increasingly central role across multiple business domains. With the organization's landscape becoming more cloud-based and integrated, maintaining a consistent identity framework across systems is essential. The Global User ID is an essential concept for this integration and is used by SAP to consistently identity a user across different applications, which each may have different native user ID formats.

SyWay uses the Person ID from SuccessFactors as the value for the Global User ID.

Please refer to the User ID and Attribute Mapping for Release 2 link for a complete overview of the user ID mapping across all landscapes.

# Network Architecture

All of the tools in the SAP Identity Suite are delivered as SaaS, and integrated to S/4HANA and other systems behind the Syensqo firewall via the SAP Cloud Connector, as described in Network and Infrastructure Architecture DD-TEC-070

# System Landscape

SAP IAG will have a 3-tier landscape: Development, Test and Production. Each landscape will connect to below applications.

The SAP IAG development environment will be integrated with the respective development target systems, including S/4HANA Dev, Ariba Development Tenant, and other applicable applications.

**Upstream Sources (into IAG)**

| Source | Purpose | Protocol / Feed | Key Attributes | Notes |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| SuccessFactors (HR) | Workforce lifecycle (join/move/leave), manager, org | OData/API feed to identity layer consumed by IAG | Person ID, Employment Type, Manager, Cost Center, Country | HR remains golden source for demographics; IAG consumes normalized identities |
| Entra ID | Directory groups / device or context attributes (optional) | Graph API / CSV (if used) | UPN, mail, groups | Not authoritative for provisioning; used for context enrichment only |

**Connected Applications (via IPS)**

**Correlation:** All targets must match on externalId = globalUserId. Where externalId is not supported, use a stable custom attribute (documented per connector).

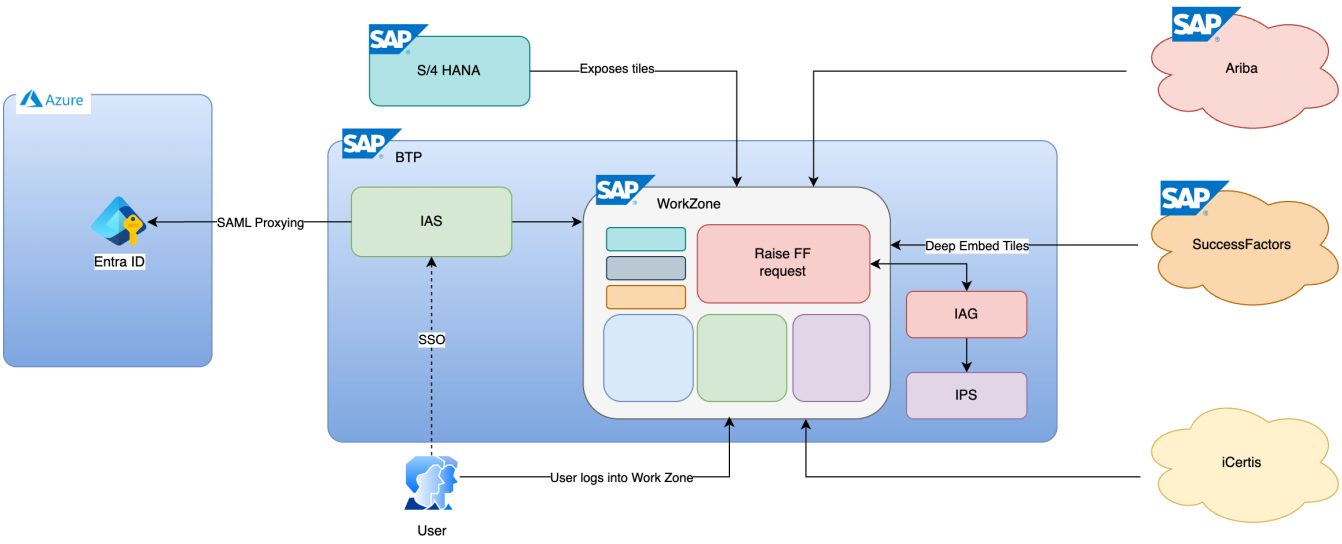
| Application | Category | Connector / Protocol | Provisioned Objects | SSO | UAR Reviewer | Remediation Mode | Notes |
|---|---|---|---|---|---|---|---|
| Ariba | SAP Cloud (Procurement) | SCIM 2.0 | Users, Groups/Roles & Realm assignments | SAML via IAS | App Owner | Auto via IPS | Map company codes / purchasing orgs via role attributes |
| iCertis | CLM | SCIM 2.0 | Users & Groups | OIDC/SAML via IAS | App Owner | Auto via IPS | Validate group permission mapping with Legal |
| SAC – Reporting /Planning | SAP Analytics Cloud | SCIM 2.0 | Users, Teams & Roles | SAML via IAS | Role Owner | Auto via IPS | Team/role design aligned to BI governance |
| Build WorkZone | SAP BTP | SCIM 2.0 | Users & Groups | SAML via IAS | App Owner | Auto via IPS | Align with corporate portal taxonomy |
| Advanced Financial Cockpit (AFC) | Finance | SCIM 2.0 | Users & Roles | SAML via IAS | Role Owner | Auto via IPS | Sensitive finance roles 2stage review |
| PAPM Cloud | Profitability & Performance Mgmt | SCIM 2.0 | Users & Roles | SAML via IAS | Role Owner | Auto via IPS | Ensure environment/tenant scoped roles |
| RAM (Risk & Assurance Management) | Risk Management | SCIM 2.0 / API | Users & Roles | SAML via IAS | App Owner | Auto via IPS | Confirm role hierarchy with Plant ops |
| Asset Performance Management (APM) | EAM analytics | SCIM 2.0 | Users & Roles | SAML via IAS | Role Owner | Auto via IPS | Tag sensitive telemetry access |
| Global Track & Trace (GTT)Logistics | | SCIM 2.0 | Users & Roles | SAML via IAS | App Owner | Auto via IPS | Geo access scoping (regions /partners) via attributes |
| S/4HANA + GTS (Embedded) | SAP Private Cloud (via RISE) | IPS CIC Cloud Connector SAP | Users, Roles (PFCG) | SAML for Fiori; SAPGUI SSO | Role Owner | Auto via IPS (where supported) | GTS cohosted; use plant /company filters; RFC/SNC secured |
| SAP IAG (Identity &Access Management) | SAP Identity Management | SCIM 2.0 | Business Roles | SAML via IAS | Role Owner | Auto via IPS | |
| SAP BTP SubAccounts | BTP | SCIM 2.0 | Users & Roles | SAML via IAS | Role Owner | Auto via IPS | |

# System Access

## Work Zone

All user access to SyWay systems will have one central landing zone in the form of SAP WorkZone.

### System Access User Flow




# Application Security

## Authentication Approach (SPInitiated SSO)

SyWay standardizes Single Sign-On (SSO) across the SAP Business Technology Platform (BTP) using region-specific SAP Identity Authentication Service (IAS) tenants federated with Microsoft Entra ID. Each BTP subaccount designates its respective IAS tenant as the trusted identity provider, ensuring consistent and secure user authentication.

All interactive user logins are by default **Service Provider (SP)–initiated**:

- Authentication between BTP subaccounts or services and IAS uses OpenID Connect (OIDC).
- Federation from IAS to Microsoft Entra ID is established via SAML 2.0.

For **non-interactive authentication** and **system-to-system communication**, SyWay adopts modern standards based on the target system's capability:

- **OAuth 2.0** (including Client Credentials Grant)
- **OAuth2 SAML Bearer Assertion**
- **Mutual TLS (mTLS)**

**Basic authentication** is permitted only as an exception where modern protocols are not supported; such cases must be formally documented and approved. **Principal Propagation** is enabled wherever supported to maintain user context across connected systems.

### Human, SPInitiated SSO

| System / SaaS (in scope) | Audience | SPInitiated | App IAS Protocol | IAS Entra Protocol | Notes |
|---|---|---|---|---|---|
| **SAP BTP Cockpit & Subaccounts** | End users / Admins | Yes | OIDC | SAML 2.0 | IAS is default IdP per region. |
| **SAP Build Work Zone** | End users | Yes | OIDC (preferred) or SAML 2.0 (per capability) | SAML 2.0 | Choose OIDC where supported. |
| **SAP Business Application Studio (BAS)** | Developers | Yes | OIDC | SAML 2.0 | Same IdP path as end users. |
| **SAP Integration Suite (Cloud Integration UI)** | Admins | Yes | OIDC (preferred) or SAML 2.0 | SAML 2.0 | Runtime APIs handled in Matrix 2. |
| **SAP API Management (Designer/Portal UI)** | Admins / Devs | Yes | OIDC (preferred) or SAML 2.0 | SAML 2.0 | |
| **SAP Analytics Cloud** | Analysts | Yes | SAML 2.0 | SAML 2.0 | Typical pattern is SAML via IAS. |
| **SAP SuccessFactors** | HR / Managers | Yes | SAML 2.0 | SAML 2.0 | SAML from Entra |
| **SAP Ariba Procurement and Sourcing** | Procurement | Yes | SAML 2.0 | SAML 2.0 | SAML from Entra |
| **SAP S/4HANA + GTS (Embedded) Cloud (private)** | Business users | Yes | SAML 2.0 | SAML 2.0 | Typical pattern is SAML via IAS. |

## Human, IdP-Initiated SSO

| System / SaaS (in scope) | Audience | SPInitiated | App IAS Protocol | IAS Entra Protocol | Notes |
|---|---|---|---|---|---|
| **SAP Ariba Network** | Procurement | No | SAML 2.0 | SAML 2.0 | SAP Ariba Network does not support SP-initiated SSO. |

## AI Agents

At the time of writing, SyWay has not identified any AI agents which are required to be deployed. However, the aim is to ensure that this architecture is future-proof and supports AI agents which could be deployed in the future.

Details of how authentication and authorization of AI Agents will be managed in the SyWay landscape is described in more detail in the Security Approach. OIDC (OpenID Connect) is the preferred authentication protocol for both two-legged and three-legged authentication scenarios, and is natively supported by SAP IAS, and thus this architecture. SAP AI Agents rely heavily on the use of the Global User ID, which is also implemented in this architecture. For details on the Global User ID, please refer to User ID and Attribute Mapping.

## NonInteractive / ServicetoService & Destinations

| Scenario / Target | Authentication Pattern | Protocol / Grant | Credentials / Tokens | Secret Storage & Controls | Principal Prop |
|---|---|---|---|---|---|
| BTP app  SAP SaaS API (e.g., SuccessFactors OData, Ariba APIs) | Servertoserver | **OAuth 2.0 Client Credentials** (preferred) or **OAuth2 SAML Bearer Assertion** | Client ID/secret; JWT or SAML assertion | BTP **Destination** service or **Credential Store**; rotation & vaulting | N/A |
| BTP app  SAP S/4HANA (onprem) via Cloud Connector | Enduser context | **Principal Propagation** (user JWT X.509 / ticket) | Shortlived userbound credential | Managed by Cloud Connector trust; cert rotation | **Yes** (preferred) |
| BTP service  BTP service (intraplatform) | Servicetoservice | **OAuth 2.0 Client Credentials** | JWT access token | Service key / Credential Store | N/A |
| API Management  Backend | Gatewaytoservice | **mTLS** and/or **OAuth 2.0** | Client certificate and/or JWT | Certificate management with rotation | Optional |
| Legacy/3rdparty target lacking modern auth | Exception path | **Basic Auth** (documented exception) | Username /password | Destination service with strong rotation; CA compensating controls | No |

**Conditional Access Policies**

Conditional Access policies TBD. Nothing currently in scope.

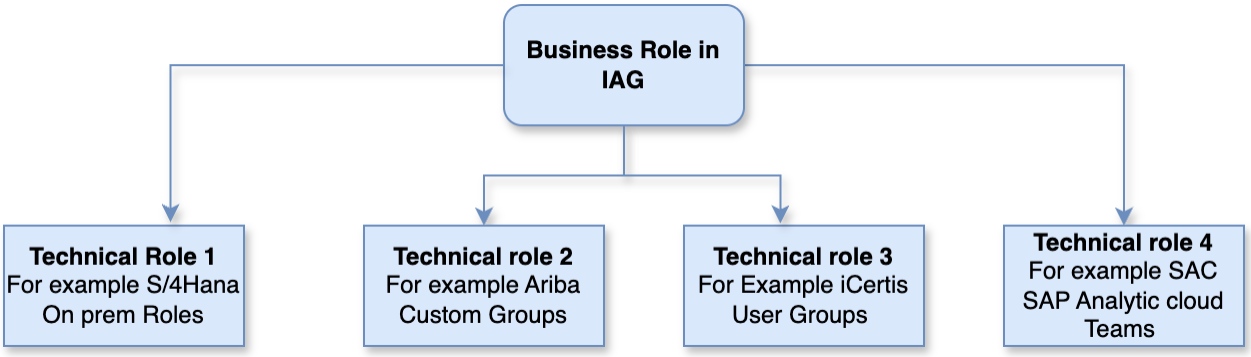
# Authorisations

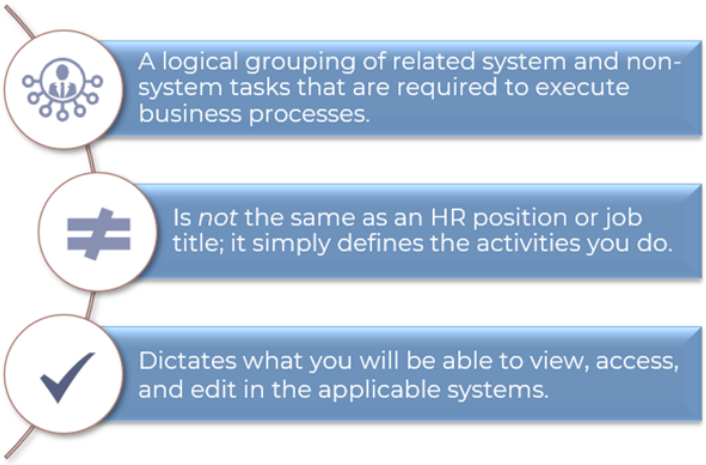
Business roles represent a high-level grouping of access aligned to specific job functions or responsibilities within the organization. Instead of assigning individual permissions or technical roles directly to users, business roles provide a simplified and standardized way to manage access. Each business role will bundle the necessary access components required to perform a particular role, supporting consistency, ease of provisioning, and alignment with governance and compliance requirements.

Business Roles should be defined to act as process driven components that deviate from HR job titles.

Key benefits:

- Supports modelling of business roles that aggregate technical roles or permissions from multiple systems
- Roles can be built to reflect job functions, departments, or business processes
- The service performs real-time SoD checks during role creation or modification
- Designed roles can go through workflow approvals before activation.




## Benefits of Business Roles:

- Better role provisioning/user role request or assignment
- Better role change management
- Address business role transfers

## Communication Security

The below table shows the in scope systems for Syway and the encryption protocols used to secure communication between each system.

| System / Integration | User/Web (HTTP [S]) — Encryption Protocol | SystemtoSystem — Encryption Protocol | SAPSAP (RFC/IDoc/HTTP) — Encryption Protocol | Authentication & Notes (summary) |
|---|---|---|---|---|
| **Ariba** | TLS 1.3 / TLS 1.2 | TLS 1.3 / TLS 1.2 + mTLS (for inbound B2B /API) | Via HTTP only TLS 1.3 / TLS 1.2 | SSO via IAS (SAML/OIDC). APIs through SIS with OAuth 2.0; cXML /REST over HTTPS. |
| **SuccessFactors** | TLS 1.3 / TLS 1.2 | TLS 1.3 / TLS 1.2 (OData /SFAPI) | HTTP only TLS 1.3 / TLS 1.2 | SSO via IAS. System calls use OAuth 2.0 (client credentials) via SIS. |
| **SAP BTP (subaccount & services)** | TLS 1.3 / TLS 1.2 | TLS 1.3 / TLS 1.2; BTPSCC tunnel uses mTLS | To onprem ABAP via SCC: TLS 1.3 / TLS 1.2 | SSO via IAS; servicetoservice tokens (JWT/OAuth). |
| **iCertis SAP** | N/A (enduser in iCertis) | TLS 1.3 / TLS 1.2 + mTLS | To S/4 via HTTP: TLS 1.3 / TLS 1.2 | OAuth 2.0 to SAP APIs via SIS; avoid raw RFC. |
| **SAP SuccessFactors** | N/A | TLS 1.3 / TLS 1.2 (OData) | HTTP only TLS 1.3 / TLS 1.2 | OAuth 2.0 via CIS. |
| **IAS Entra (federation)** | TLS 1.3 / TLS 1.2 (browser redirects) | N/A | N/A | SAML 2.0 (signed; encrypt assertions where supported) or OIDC (JWS; JWE optional). |
| **PAPM Cloud (BTP)** | TLS 1.3 / TLS 1.2 | TLS 1.3 / TLS 1.2; mTLS to onprem via SCC | To S/4 via HTTP: TLS 1.3 / TLS 1.2 | OAuth 2.0; principal propagation via SCC when needed. |
| **Asset Performance Management (APM, BTP)** | TLS 1.3 / TLS 1.2 | TLS 1.3 / TLS 1.2; mTLS to onprem via SCC | To S/4 via HTTP: TLS 1.3 / TLS 1.2 | OAuth 2.0; events/APIs via SIS. |
| **Global Track & Trace (GTT, BTP)** | TLS 1.3 / TLS 1.2 | TLS 1.3 / TLS 1.2 + mTLS (B2B endpoints) | To S/4 via HTTP: TLS 1.3 / TLS 1.2 | OAuth 2.0; IP allowlisting on B2B endpoints. |

| | | | | |
|---|---|---|---|---|
| **S/4HANA + GTS (Embedded)** (ABAP) | TLS 1.3 / TLS 1.2 (ICM) | HTTP APIs: TLS 1.3 / TLS 1.2 | SNC (CommonCryptoLib) for RFC/DIAG (privacy protection); IDoc via TLS 1.3 / TLS 1.2 or RFC+SNC | SSO via IAS (SAML) or SPNEGO; STRUST PSEs hardened. |
| **SAP Analytics Cloud (SAC)** | TLS 1.3 / TLS 1.2 | Live connections via SCC /Web Dispatcher: TLS 1.3 / TLS 1.2 | To S/4HANA onprem via SCC: TLS 1.3 / TLS 1.2 | SSO via IAS; principal propagation as applicable. |

**Legend**

**TLS 1.2+** = TLS 1.2 or higher (prefer TLS 1.3 where supported) • **mTLS** = Mutual TLS (client + server certs) • **SNC** = SAP Secure Network Communications (CommonCryptoLib) for RFC/DIAG • **IAS** = SAP Identity Authentication Service • **Entra** = Microsoft Entra ID (Azure AD) • **SCC** = SAP Cloud Connector • **SIS/CPI** = SAP Integration Suite (Cloud Integration) • **PP** = Principal Propagation

## Data Security

Data security in our landscape is about enforcing **least privilege** so that only authorized users can perform approved actions on the specific data they' re entitled to see. We will implement a **layered accesscontrol model** that combines **RBAC, ABAC, and Groups**. **RBAC** will define business roles and the precise permissions each role grants (the *what* a user can do). **ABAC** will add finegrained, contextaware rules that filter data by attributes such as Nationality, location, company code, region, business unit, asset, or document owner (the *which* records a role can act on and *under what conditions*). **Groups**—managed centrally in the IdP—will streamline assignment and lifecycle (the *who* gets which roles), support separation of duties, and simplify provisioning and reviews. Together, this model delivers defenceindepth: roles gate capabilities, attributes constrain data scope, and groups keep access manageable, auditable, and adaptable as the organization changes.

| System | RBAC | ABAC | Groups /Teams | Notes (how it's enforced) |
|---|---|---|---|---|
| **Ariba** | | | | Permissions are assigned via **user groups**; access is controlled by groupbased permissions (RBAC via groups). (SAP Help Portal) |
| **iCertis** | | | | **Security groups & role–action mapping** govern feature/data access; groups are the primary container. (iciwikiapac.icertis.com) |
| **SAC – Reporting/Planning** | | | | Roles/privileges + **teams**; **Data Access Control** and model privacy apply **dimensionmember (rowlevel) restrictions**. (SAP Help Portal) |
| **Build Work Zone** | | | | BTP **role collections** + Work Zone roles; **groupbased** space/content permissions across components. (SAP Learning) |
| **Advanced Financial Cockpit (AFC)** | | | | **Static role templates** and scoped user roles; *owner groups* used in process governance. (SAP Help Portal) |
| **PAPM Cloud** | | | | BTP role templates + **data/analytic privileges** (e.g., region/team) and **teams**; finegrained data locks. (SAP Help Portal) |
| **RAM (Risk & Assurance Management)** | | | | Rolebased access within RAM; organizations typically map **IdP groups** to roles/controls. (SAP) |
| **Asset Performance Management (APM)** | | | | Standard role collections + **AttributeBased Access Control Role Template** for data scoping (site/asset, etc.). (SAP Help Portal) |
| **Global Track & Trace (GTT)** | | | | Role collections and **attributebased authorization for document access** (e.g., party /shipper). (SAP Help Portal) |
| **S/4HANA + GTS (Embedded)** | | | (opt) | **PFCG roles** + **authorization objects with orglevel fields** |
| **SAP IAG** | | | | Role/authorization policies inside IAG; **IAS/IdP groups** commonly used to assign business roles. (SAP Help Portal) |
| **NextLabs** | | | | **ABAC** is the core (policydriven, attributecentric); |

**Legend**

**RBAC**: role templates/role collections/authorization objects; **ABAC**: attribute or dimensionbased rules (e.g. location, nationality, etc); **Groups** : application or IdP (IAS/Entra) groups/teams used for membership/sharing/role assignment.

## Other Controls

NAA

# Operation Architecture

## Change and Configuration Management

In SAP IAG, the configuration and integration of target applications must be carried out manually across all landscapes, including Development, Quality, and Production systems.

Business Rules and Business Roles will be set up in the Development system and then transported by exporting the configurations from Development and importing them into the Quality and Production systems.

# Monitoring

## Sizing

All of the systems described in this document are delivered as SaaS components by SAP, with sizing being managed by SAP Cloud Ops.

## High Availability & Disaster Recovery

The Availability SLAs provided by SAP for the components of the SAP Cloud Identity suite are as follows:

| Component | Availability SLA | Comment |
|---|---|---|
| SAP Cloud Identity Access Governance (IAG) | 99.9% | default SAP SLA BTP services, as per the SAP Business Technology Platform Service Description Guide |
| SAP Identity Provisioning Service (IPS) | 99.95% | as per the SAP Business Technology Platform Service Description Guide |
| SAP Identity Authentication Service (IAS) | 99.95% | as per the SAP Business Technology Platform Service Description Guide |

# Backup/Restore

- **Platform-managed:** For SAP-managed BTP services(SAP IAG), backups are handled by SAP; restore is service-specific and generally not customer-operated. Guidance is outlined in the BTP admin help (“Data Backups Managed by SAP”).
- **Audit evidence:** BTP **Audit Log Service** stores subaccount audit data for 90 days by default; export/forward logs if longer retention is needed.

## Maintenance Plan

Even though IAG is cloud-managed, there is still a “maintenance plan” that Syensqo using IAG must follow internally to stay secure, compliant, and effective. Key responsibilities:

- **Tenant & subscription management.** When subscribing to IAG,  set up sub-accounts/tenants on SAP BTP (test vs. production), assign entitlements, and manage role collections for administrators. refer to the link https://help.sap.com/docs/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE/e12d8683adfa4471ac4edd40809b9038/f16bc311b1d544d3a0687e7c453a49ec.html?state=DRAFT&version=2205
- **Integration and connectivity maintenance.** To connect IAG to on-premise systems, cloud apps, or other SAP services (e.g. via cloud connectors, provisioning),  must ensure connectivity, destination configuration, and correct provisioning setup.
- **User/role lifecycle and governance operations.** Even though IAG provides features like Access Request, Role Design, Access Certification, and Privileged Access Management —  need to keep the user/role data up to date, run periodic reviews (e.g. access recertification), manage segregation-of-duties (SoD) rules, mitigation controls, and ensure correct workflow configuration.
- **Audit logging & compliance reporting.** While IAG logs events, access changes and so on, the organization needs to define and enforce retention policies as well as regularly review logs, reports, and audit data, to comply with internal or external regulations.
- **Planning for changes & revalidations.** If business processes change — e.g., new applications, changed workflows, additional risk rules, integrations —  must periodically review and adjust the IAG configuration (roles, connectors, policies) accordingly.

SAP Cloud Service – Maintenance Window for SAP Cloud Identity Access Governance

| Regular Maintenance | Major Upgrades |
|---|---|
| Start time in UTC per region: Americas SUN 4am | Time frame in UTC per region: Americas SAT 1pm – 7pm |
| Up to once every month | Up to four times a year |

| | |
|---|---|
| Duration: 4 hours | Duration: 4 hours |

To view the maintenance windows for CIS, you can follow the below steps:

- **Link:** SAP for Me - Systems & Provisioning
- **Navigation:** Go to **Systems & Provisioning** > **Availability**
- **What to look for:** Search for your specific Cloud Identity Services tenant (usually starts with `ias` or `ips`). It will list upcoming "Planned Events" and maintenance.

# Exceptions

# See also

SyWay Security Approach

Network and Infrastructure Architecture DD-TEC-070

## Terminology

| Term / Acronym | Full Form / Description |
|---|---|
| **SAP IAG** | *SAP Cloud Identity Access Governance* – A SaaS solution on SAP BTP that automates provisioning, SoD analysis, access requests, and certifications. |
| **SAP BTP** | *SAP Business Technology Platform* – Cloud platform where IAG and other SAP SaaS services are hosted. |
| **IAS** | *SAP Identity Authentication Service* – Provides Single Sign-On (SSO), authentication, and federation with external identity providers like Microsoft Entra ID. |
| **IPS** | *SAP Identity Provisioning Service* – Automates user and role provisioning between source and target systems (e.g., SuccessFactors  IAG  S/4HANA). |
| **CIS** | *SAP Cloud Identity Services* – Umbrella suite including IAS, IPS, and Identity Directory for centralized identity management. |
| **SCIM** | *System for Cross-domain Identity Management* – Open standard protocol for automating user provisioning and deprovisioning between cloud systems. |
| **SoD** | *Segregation of Duties* – Governance principle ensuring no user can perform conflicting business functions that could lead to fraud or error. |
| **HR Trigger** | Event in HR system (e.g., hire, transfer, termination) that initiates an identity or access workflow in IAG. |
| **JML** | *Joiner, Mover, Leaver* – Framework defining user lifecycle events: onboarding, role changes, and offboarding. |
| **SCC** | *SAP Cloud Connector* – Secure reverse proxy linking SAP BTP cloud services to on-premise systems like S/4HANA. |
| **S/4HANA** | *SAP S/4HANA Enterprise Suite* – Core ERP system integrated with IAG for access governance and provisioning. |
| **Entra ID** | *Microsoft Entra ID (formerly Azure AD)* – Enterprise identity provider used for authentication and federation with IAS. |
| **Access Request** | Workflow-based process in IAG for requesting and approving system access. |
| **Access Certification** | Periodic review of user access to validate ongoing need and ensure compliance. |
| **Business Role** | Logical grouping of multiple technical roles across systems representing a job function or responsibility. |
| **Technical Role** | Application-specific role or authorization object providing actual system access (e.g., PFCG roles in S/4HANA). |
| **Connectivity Service** | SAP BTP service enabling IAG to communicate with on-prem systems through the Cloud Connector. |
| **Identity Directory** | Central repository within SAP Cloud Identity Services storing user and group information for provisioning and authentication. |
| **Workflow Engine** | Component in IAG managing approval steps for access requests and certifications. |
| **Access Risk Analysis** | IAG process that checks access assignments against SoD and critical access rules. |

| | |
|---|---|
| **Campaign (Access Review)** | A scheduled access certification exercise involving reviewers and approvers. |
| **IPS Job** | Scheduled provisioning job that synchronizes user and role data across systems. |
| **BTP Subaccount** | Logical container within SAP BTP hosting applications and services, isolated per environment (e.g., dev, int, prd). |
| **Principal Propagation** | Mechanism that forwards a user's authenticated identity across service layers for secure end-to-end communication. |

# Change log

| Version | Published | Changed By | Comment |
|---|---|---|---|
| **CURRENT (v. 105)** | **Apr 10, 2026 07:01** | **WENNINGER-ext, Sascha** | |
| v. 104 | Apr 10, 2026 06:26 | **WENNINGER-ext, Sascha** | |
| v. 103 | Apr 01, 2026 15:34 | **WENNINGER-ext, Sascha** | |
| v. 102 | Dec 10, 2025 13:25 | **WENNINGER-ext, Sascha** | added stakeholders |
| v. 101 | Dec 10, 2025 10:32 | **HEALY-ext, Michael** | |
| v. 100 | Dec 10, 2025 10:11 | **HEALY-ext, Michael** | |
| v. 99 | Dec 10, 2025 10:09 | **HEALY-ext, Michael** | |
| v. 98 | Dec 09, 2025 17:16 | **HEALY-ext, Michael** | |
| v. 97 | Dec 09, 2025 14:02 | **HEALY-ext, Michael** | |
| v. 96 | Dec 09, 2025 14:00 | **HEALY-ext, Michael** | |

Go to Page History

# Workflow history

This view shows the 5 most recent entries. The complete workflow log is available from the 'Document Activity' menu item.

| Apr 30, 2026 | Actor | Type | Activity | Version |
|---|---|---|---|---|
| Approved | WENNINGER-ext, Sascha | State | changed state to Approved at 8:37 am | v105 |
| Pending SteerCo Review | WENNINGER-ext, Sascha | State | gave *Final Approval* approval at 8:37 am<br>*Approved by Frank Bolata. Minutes of meeting attached* | |
| **Apr 10, 2026** | | | | |
| | WENNINGER-ext, Sascha | State | changed expiry date to '24 Apr, 2026 07:03 am' at 7:03 am | |
| | | State | changed state to Pending SteerCo Review at 7:03 am | v105 |
| Edited following Stakeholder Review | WENNINGER-ext, Sascha | State | gave *Minor change* approval at 7:03 am<br>*updated with section on AI Agent authentication as per feedback from Frank* | |
| | | Edit | updated the page at 7:01 am | |

| | | | | |
|---|---|---|---|---|
| | State | changed state to Edited following Stakeholder Review at 6:26 am | | v104 |
| **From Apr 01, 2026 to Apr 10, 2026** | | | | |
| Pending SteerCo Review | WENNINGER-ext, Sascha | Edit | updated the page at 3:34 pm | |