

Quick Reference Guide - Approving Privileged Access Requests (Approver Point of View)

Process Overview - Approver POV

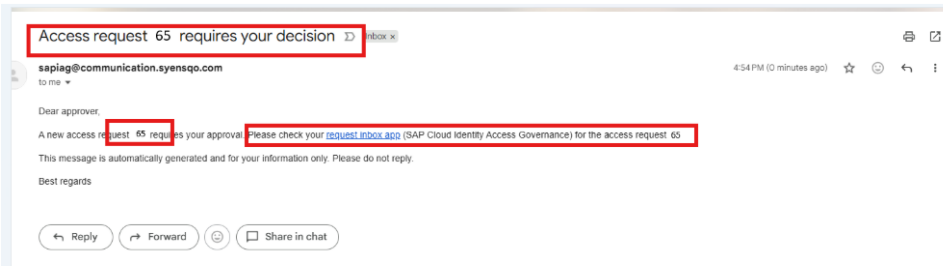
- [Step 1: Receive Approval Notification](#)
- [Step 2: Login to IAG](#)
- [Step 3: Open Access Request Inbox](#)
- [Step 4: Review Request Details](#)
- [Step 6: Validate Request](#)

Note: Access requests, including PAM (Privileged Access Management), provide elevated permissions and must be approved only for valid business or emergency needs.

- *Approvers are responsible for validating the **reason, scope of work, and expected activities.***
- *Requests with insufficient or incomplete information **must be rejected.***

Step 1: Receive Approval Notification

- Approver will receive an **email from IAG** indicating a pending access request.



Step 2: Login to IAG

- Click the link in the email or open the **IAG portal**, <https://syw-iag-dev-eu10.sapciag-ee.cfapps.eu10.hana.ondemand.com/cp.portal/site#Shell-home>

Step 3: Open Access Request Inbox

- Click **Access Request Inbox**.
- Pending approval work items assigned to you will be displayed.

The screenshot shows the SAP Access Request Inbox. The table has the following columns: Request Number, Escalated, Reason for Request, Requested For, Priority, Role Owner, Delegated By, and Pending Days. The first row is highlighted in yellow.

Request Number	Escalated	Reason for Request	Requested For	Priority	Role Owner	Delegated By	Pending Days
65	No	Need for S443 Application	Sanjiva Latha (P000001)	High	Role Owner		0
33	No	Access Request for Change Access	Sanjiva Latha (P000001)	High	Role Owner		29
33	No	Access Request for Change Access	Shruthi Kumaravil (P000005)	High	Role Owner		80

Step 4: Review Request Details

- Select the request to review.
- Verify the following information:
 - **Requestor Name**
 - **Requested User**
 - **Role Requested**
 - **Reason / Justification / Scope of Work**
 - **Duration of access requirement**

Ensure the request is **complete and accurate**. The following PAM roles require the requester to provide a valid justification and specify the assignment duration before the approver can grant access.

SAP Ariba PAM Roles

Ariba Template Manager – Creates and maintains sourcing templates.

Ariba User Admin – Monitors correct user provisioning from IAG to Ariba.

Ariba Master Data Manager – Reviews integration of master data into Ariba.

Ariba System Admin – Super user for exceptional tasks or defect fixes.

Icertis PAM Roles

IT Icertis Master Data Admin – Manages master data only; no system/workflow access.

IT Icertis User Management Admin – Administers users, groups, orgs, and technical role assignments; no transactional data access.

IT Icertis Admin Extended – Same as Support + access to transactional data (excluding confidential contracts).

IT Icertis Config Admin – Full system configuration control; no access to contracts or transactional data; technical roles assigned via User Management Admin.

Step 6: Validate Request

- Confirm the request is for a **valid, active user**.
- Ensure the request aligns with requester's role ownership responsibilities and understand for any impacts of changes in the production system for the access requested.
- Based on validation, approve or reject the request with appropriate comments. The corresponding access decision will be communicated to the user via email notification.

The screenshot shows the SAP Approve Requests interface for a PAM for SAAS Application. The interface is divided into several sections:

- Request Summary:** Shows the request ID (05), priority (High), and status (Updated 0 days ago). It also displays the requester's name (Sumbha Lakha) and department (Sumbha Lakha).
- Risks:** Shows 0 SoD Risks and 0 Critical Access risks, with 0 Risks Mitigated.
- Access Requested (1):** A table showing the requested access. The table has columns for Access, Access Type, Action, Validity Period, Risks, and Approve or Reject Access. The row shows 'PAM Ariba System Admin' with 'Business Role' access type, 'Add' action, validity period from 'Dec 12, 2025' to 'Dec 25, 2025', and 'No Risk'.
- Existing Assignments (14):** A table showing existing assignments. The table has columns for Access, Access Type, Validity Period, and Risks. The rows list various assignments such as 'IAG_WF_MANAGER', 'SelfService ConfigKey Admin Group', 'IAG_WF_DEFAULT', 'Procurement Excellence', 'Icertis Dev application', and 'SAP Ariba Development system'.