

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

Process Overview - Approver POV

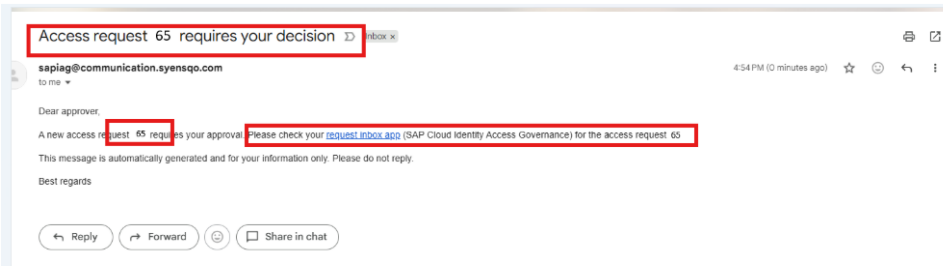
- Step 1: Receive Approval Notification
- Step 2: Login to IAG
- Step 3: Open Access Request Inbox
- Step 4: Review Request Details
- Step 6: Validate Request

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**.
- Dev/QA - <https://syw-iag-dev-eu10.sapciag-ee.cfapps.eu10.hana.ondemand.com/cp.portal/site#Shell-home>
- Production - <https://syw-iag-prd-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 My Inbox interface. A table lists access requests with columns: Request Number, Escalated, Reason for Request, Requested For, Priority, Stage, Delegated By, and Pending Days. The first row is highlighted in yellow.

Request Number	Escalated	Reason for Request	Requested For	Priority	Stage	Delegated By	Pending Days
65	No	PRD for S4H Application	Suresha Lakya (P000001)	High	Role Owner		0
18	No	Access Request for Change Access	Suresha Lakya (P000001)	High	Role Owner		29
19	No	Access Request for Change Access	Shubhi Kumaravelu (P000001)	High	Role Owner		30

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 displays the SAP PAM for SAAS Application interface. At the top, the title 'PAM for SAAS Application' is visible. Below it, a summary box shows 'Request: 05', 'Priority: High', 'Requested For: Sumitra Lohiya (P000007)', 'Requested By: Sumitra Lohiya (P000007)', 'Department: Risk', and 'Risks: 0 SoD Risks, 0 Critical Access, 0 Risks Mitigated'. The 'Access Requested' section shows a table with one entry: 'PAM Ariba System Admin' with 'Business Role' access type, 'Add' action, and a validity period of 'Dec 12, 2025 - Dec 31, 2025'. The 'Existing Assignments' section lists 14 assignments, including 'IAG_WF_MANAGER', 'SelfService ConfigKey Admin Group', 'IAG_WF_DEFAULT', 'Procurement Excellence', 'Icertis Dev application', and 'SAP Ariba Development system'.

Access	Access Type	Action	Validity Period	Risks	Approve or Reject Access
PAM Ariba System Admin	Business Role	Add	Dec 12, 2025 - Dec 31, 2025	No Risk	<input type="radio"/> Approve <input type="radio"/> Reject

Access	Access Type	Validity Period	Risks
IAG_WF_MANAGER IAS_DEV	Group		
SelfService ConfigKey Admin Group ICERTIS_SYW_DEV	Group		
IAG_WF_DEFAULT IAS_DEV	Group		
Procurement Excellence ICERTIS_SYW_DEV	Group		
IAS Dev IAS_DEV	Application		
Icertis Dev application ICERTIS_SYW_DEV	Application		
SAP Ariba Development system SAP_ARIBA_SYW_DEV	Application		