

Quick Reference Guide - Request Privileged Access (Requester Point of View)

Process Overview - Request Privileged Access (Requester POV)

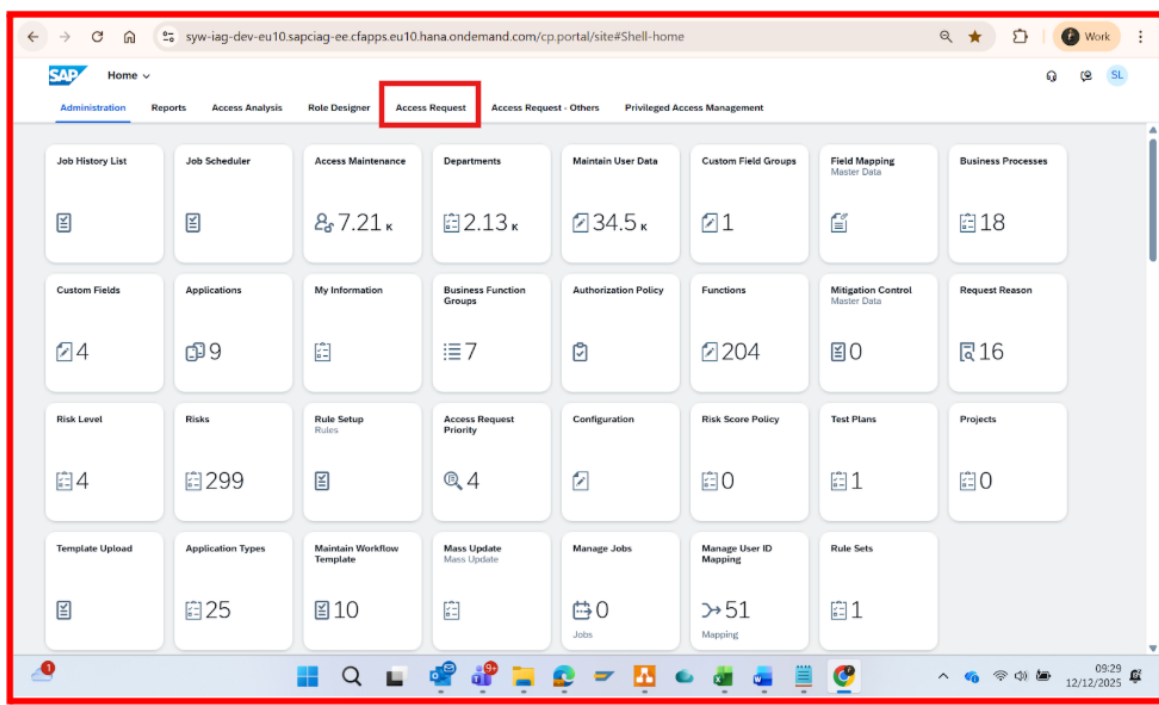
- Step 1: Login to IAG to raise the access request
- Step 2: Navigate to Access Request
- Step 3: Select Role and Create Request
- Step 4: Fill Request Details
- Step 5: Submit Request
- Step 6: Receive email notification for submission
- Step 7: Receive email confirmation for approval status
- Step 8: Login and Use of Privileged Access in Target Applications

Note: Use of PAM from requester Point of View

- PAM access provides elevated permissions and must be requested only for valid business or emergency needs.
- **Clearly document the reason, scope of work, and expected activities when raising the request.** Requests with **insufficient or incomplete information will be rejected.**
- All user activities are logged and monitored, and users are responsible for their actions. During the hypercare period, access will **automatically expire within one week** according to the default duration, until the Release 4 solution is implemented for Release 2.
- If reviewer challenges, users must explain why access was used, confirm approvals for any direct production changes, and provide accurate details including before and after values where applicable

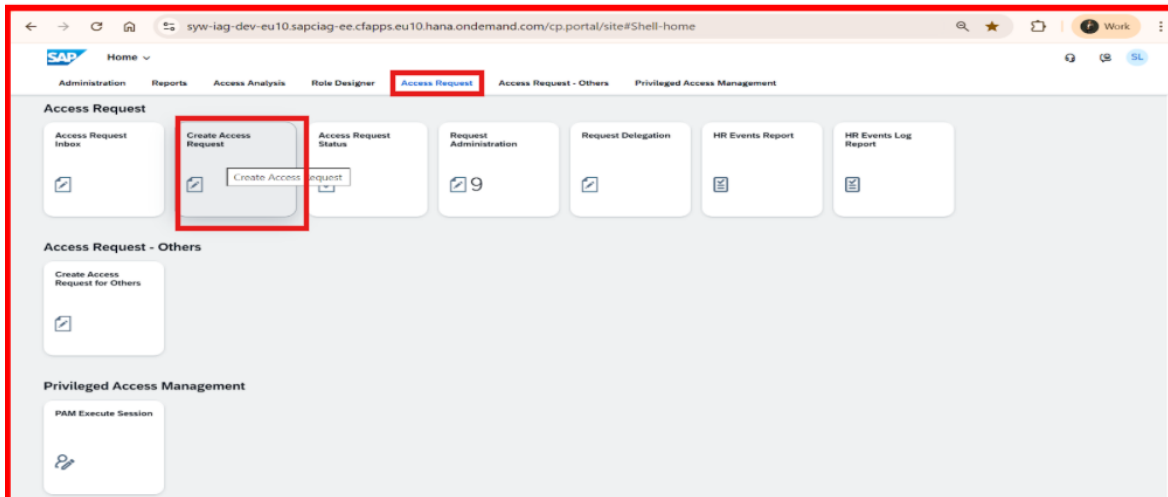
Step 1: Login to IAG to raise the access request

- <https://syw-iag-prd-eu10.sapciag-ee.cfapps.eu10.hana.ondemand.com/cp.portal/site#Shell-home>
- Based upon the access application would be visible here

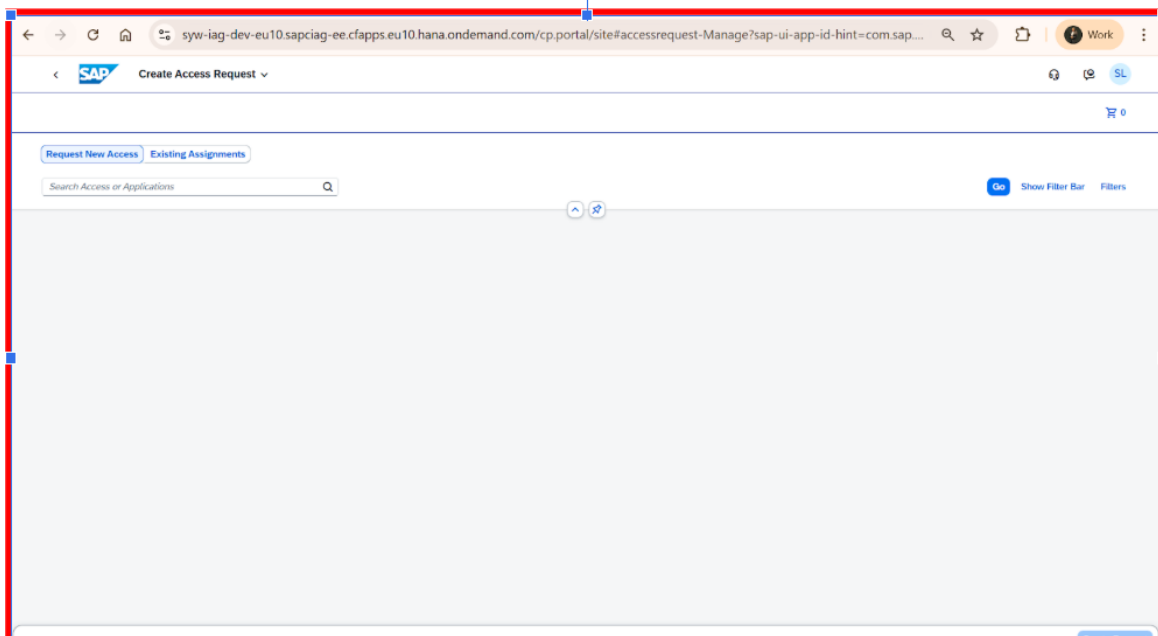


Step 2: Navigate to Access Request

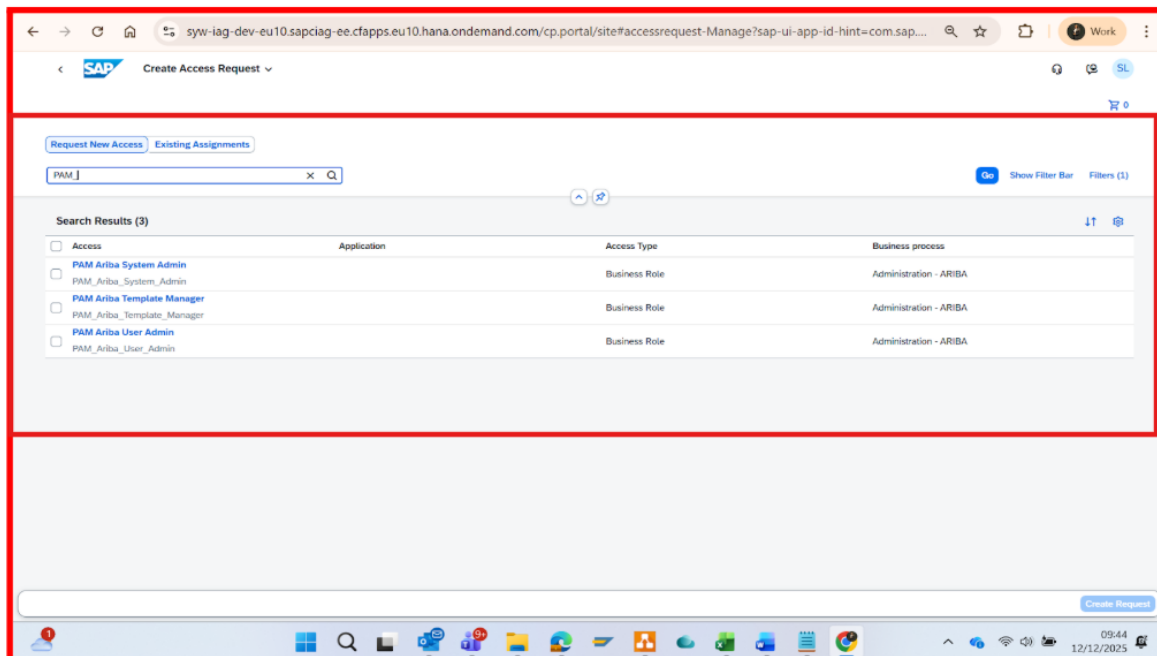
- Go to the **Access request** tab and click on the 'Create Access Request' application



- Create Access Request page will appear.



- In Search Access or Application , search the role by prefix string **PAM_** and all PAM related Business roles will be visible here.



Step 3: Select Role and Create Request

Choose from the available PAM roles as below with justification explained in the description section after PAM role selection

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.

- Select the appropriate **PAM role** and click on the Create request.

Step 4: Fill Request Details

- Below page will be displayed after clicking on the Create Request button.

Provide the below information for the PAM access request.

- **Reason for Request:** PAM for SAAS Application
- **Priority:** Select High, Medium, Low as per the urgency basis
- **Description:** Why emergency access request is raised and what will be done in the system(**mandatory for approval**)
- Duration of access requirement in the description section(**Mandatory for approval**)
- Manager and Email address will be populated automatically.

syw-iag-dev-eu10.sapciag-ee.cfapps.eu10.hana.ondemand.com/cp.portal/site#accessrequest-Manage?sap-ui-app-id-hint=com.sap...

Review Request

Requested By: Sumitra Lohiya (P000007)
Requested For: Sumitra Lohiya (P000007)
Department: SAP System Support

Request Details **Access Requested** **User Details** **Attachment**

Request Details

Reason for Request: PAM for SAAS Application
Priority: High

User Details

Manager: P000043 Satya Madasu
User Email: sumitra.lohiya-ext@syensqa.com

Access Requested

Provide validity dates for each requested access that belongs to application type 'S4HANA' or 'ERP'. You can also remove an individual access or add more access.

Access (1)

Access	Application	Access Type	Action	Validity Period
PAM Ariba System Admin		Business Role	Assign	Dec 12, 2025 - Dec 31, 9999

User Details

Job:
User Group:
Company: Syensqa
Location:
Division: IAG

Submit Request **Cancel**

Step 5: Submit Request

- Click on the Submit Request

syw-iag-dev-eu10.sapciag-ee.cfapps.eu10.hana.ondemand.com/cp.portal/site#accessrequest-Manage?sap-ui-app-id-hint=com.sap...

Review Request

Requested By: Sumitra Lohiya (P000007)
Requested For: Sumitra Lohiya (P000007)
Department: SAP System Support

Request Details **Access Requested** **User Details** **Attachment**

Request Details

Reason for Request: PAM for SAAS Application
Priority: High

User Details

Manager: P000043 Satya Madasu
User Email: sumitra.lohiya-ext@syensqa.com

Access Requested

Provide validity dates for each requested access that belongs to application type 'S4HANA' or 'ERP'. You can also remove an individual access or add more access.

Access (1)

Access	Application	Access Type	Action	Validity Period
PAM Ariba System Admin		Business Role	Assign	Dec 12, 2025 - Dec 31, 9999

User Details

Job:
User Group:
Company: Syensqa
Location:
Division: IAG

Confirmation

Do you want to submit this access request?

Yes **No**

Submit Request **Cancel**

09:49 12/12/2025

- Click on OK, to check request status

Review Request

Requested By: Sumitra Lohiya (P000007)
Requested For: Sumitra Lohiya (P000007)
Department: SAP System Support

Request Details

Reason for Request: PAM for SAAS Application
Priority: High

User Details

Manager: P000043 Satya Madan
User Email: sumitra.lohiya-ext@syensqo.com

Access Requested

Provide validity dates for each requested access that belongs to application type

Access	Application	Access Type	Action	Validity Period
PAM Ariba System Admin		Business Role	Assign	Dec 12, 2025 - Dec 31, 9999

User Details

Job:
User Group:
Company: Syensqo
Location:
Division: IAG

[Submit Request](#) [Cancel](#)

- Check request status for access request information.

Access Request Status

My Requests (37)

Search using Request No.

PAM for SAAS Application 0 Days Ago In Process
Request #: 65
Created By: Sumitra Lohiya
1 Pending

PAM for SAAS Application 0 Days Ago Cancelled
Request #: 64
Created By: Sumitra Lohiya
1 Cancelled

Access Request for Change Access 2 Days Ago Completed
Request #: 63
Created For: Dhiraj ...
1 Approved

Access Request for Change Access 3 Days Ago Completed
Request #: 62
Created For: Micha...
1 Approved

Access Request for Change Access 3 Days Ago Completed
Request #: 61

Details

PAM for SAAS Application

Request #: 65 Status: In Process
Priority: High Updated: 0 Days Ago
Created By: Sumitra Lohiya (P000007) Created For: Sumitra Lohiya (P000007)

Access Requested

Access	Approver	Provisioning Action	Stage	Last Updated	Status
PAM Ariba System Admin	2 Approvers	Add	Role Owner	Dec 12, 2025	Pending

Additional Details

User Details

Job:
User Group:
Company: Syensqo
Location:
Division: IAG
Position:

[Cancel Request](#)

Step 6: Receive email notification for submission

- The user receives an email notification confirming that the access request has been submitted successfully.

Your access request 65 has been successfully submitted [Inbox](#)

sapiag@communication.syensqo.com
to me

13:18 (1 hour ago)

Dear Sumitra Lohiya

Access request 65 has been successfully submitted for approval. You can check its status in the [Access Request Status](#) app (SAP Cloud Identity Access Governance).

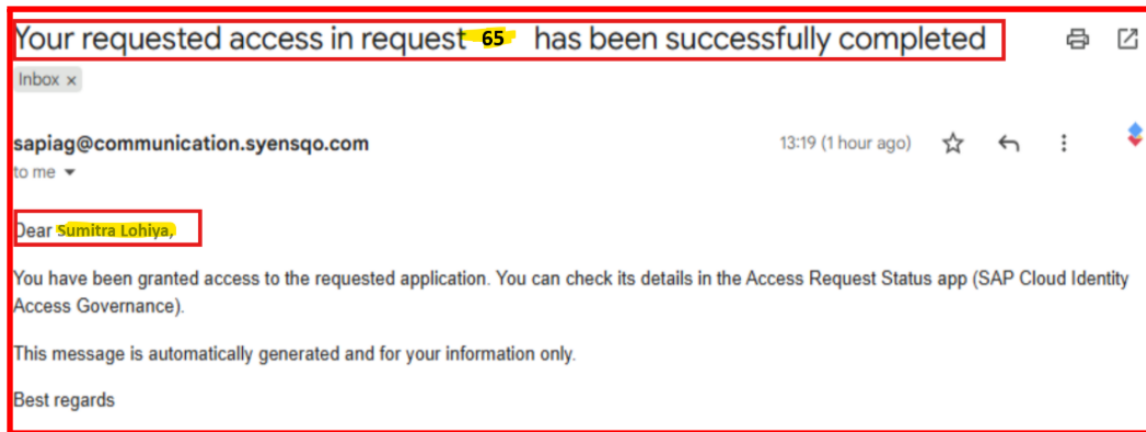
This message is automatically generated and for your information only.

Best regards

[Reply](#) [Forward](#) [Share in chat](#) [More](#)

Step 7: Receive email confirmation for approval status

- The user receives an email confirmation on the approval or rejection status of the access request.



Step 8: Login and Use of Privileged Access in Target Applications

- Once the access request is approved and provisioned, the user may log in to the respective application, such as SAP Ariba or Icertis, and perform activities using the granted privileged access.