ERP-554 Integration Process - Provision users in ICertis from SAP Cloud IAG

Status	Approved
Owner	LOHIYA-ext, Sumitra
Stakeholders	
Jira Request ID	⚠ ERP-95 - Jira project doesn't exist or you don't have permission to view it.
Jira Development ID	⚠ ERP-554 - Jira project doesn't exist or you don't have permission to view it.

- High-Level Specification
  - Functional Overview
  - Technical Architecture Diagram
  - Process Flow Diagram
  - Design Assumptions
  - Security, Integrity and Controls
    - Access Control & Segregation of Duties
    - Service Account for System-to-System Calls
    - API Authentication & Gateway Enforcement
  - Configuration Requirements
  - Design Rationale
  - Data Structure
  - Identifier choice
  - Delta or Full Load Requirements
  - Monitoring
- Volumetrics
- Performance Consideration
  - Delta vs Full loads
  - Pagination & batch sizing
  - Attribute minimization & transformations
  - Rate Limits
    - Identity Provisioning Rate Limits
- Error Handling
- Testing
  - How to Test
  - Test Considerations/Dependencies
- Change log

High-Level Specification

Application System (Source)	SAP IAG
Application System (Target)	iCertis
Source System Interface	Standard APIs
Target System Interface	Standard APIs
Business Process Reference	13.03.01.01 User lifecycle Management

Functional Overview

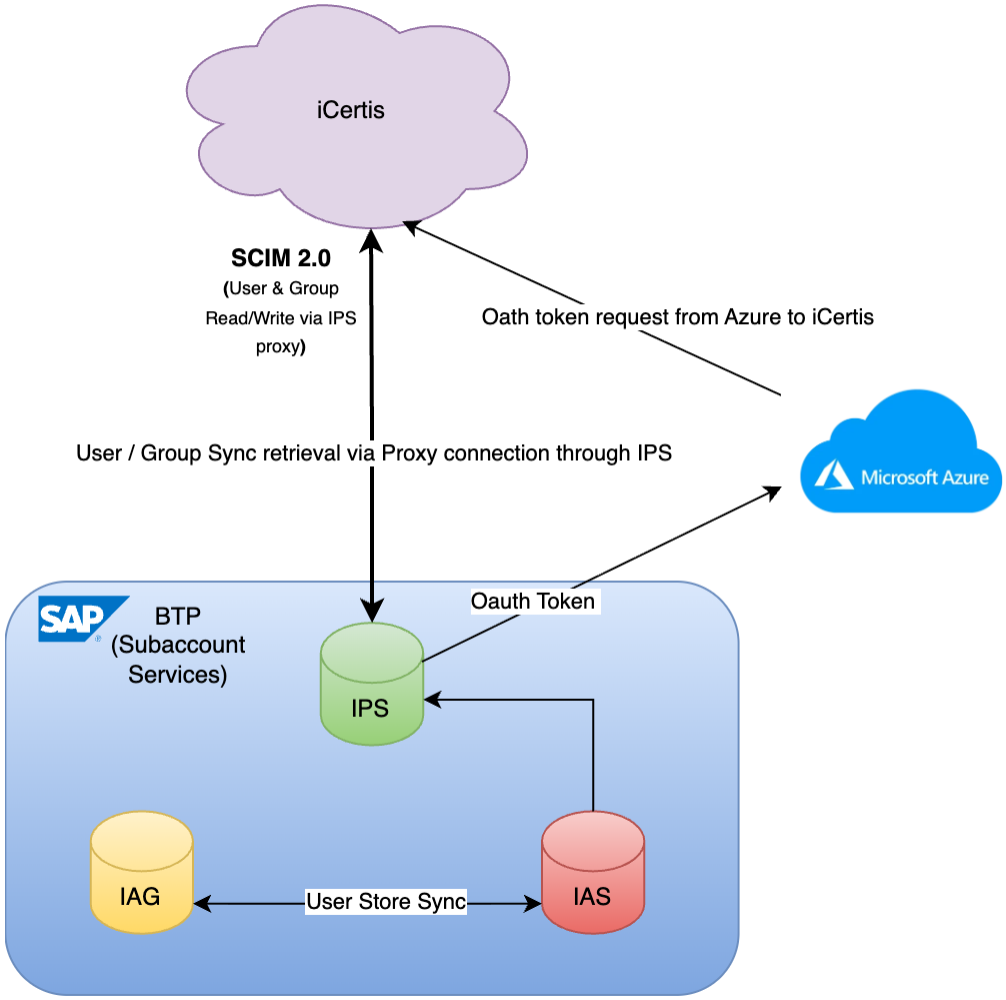
This specification outlines the detailed design for the integration between iCertis and SAP Identity Access Governance (IAG). The goal of this integration is to automate the provisioning, updating, and deprovisioning of user accounts, groups, and authorizations in iCertis through IAG. This ensures that access is consistently controlled, compliant, and properly aligned with organizational policies.

In this model, SAP IAG serves as the central system for user and role provisioning as well as Access Risk Analysis, while iCertis continues to manages the entire contract lifecycle, from creation and negotiation to execution and renewal. User accounts and group assignments will be provisioned from IAG to iCertis through SCIM-based connectivity, removing the dependency on manual user administration within iCertis.

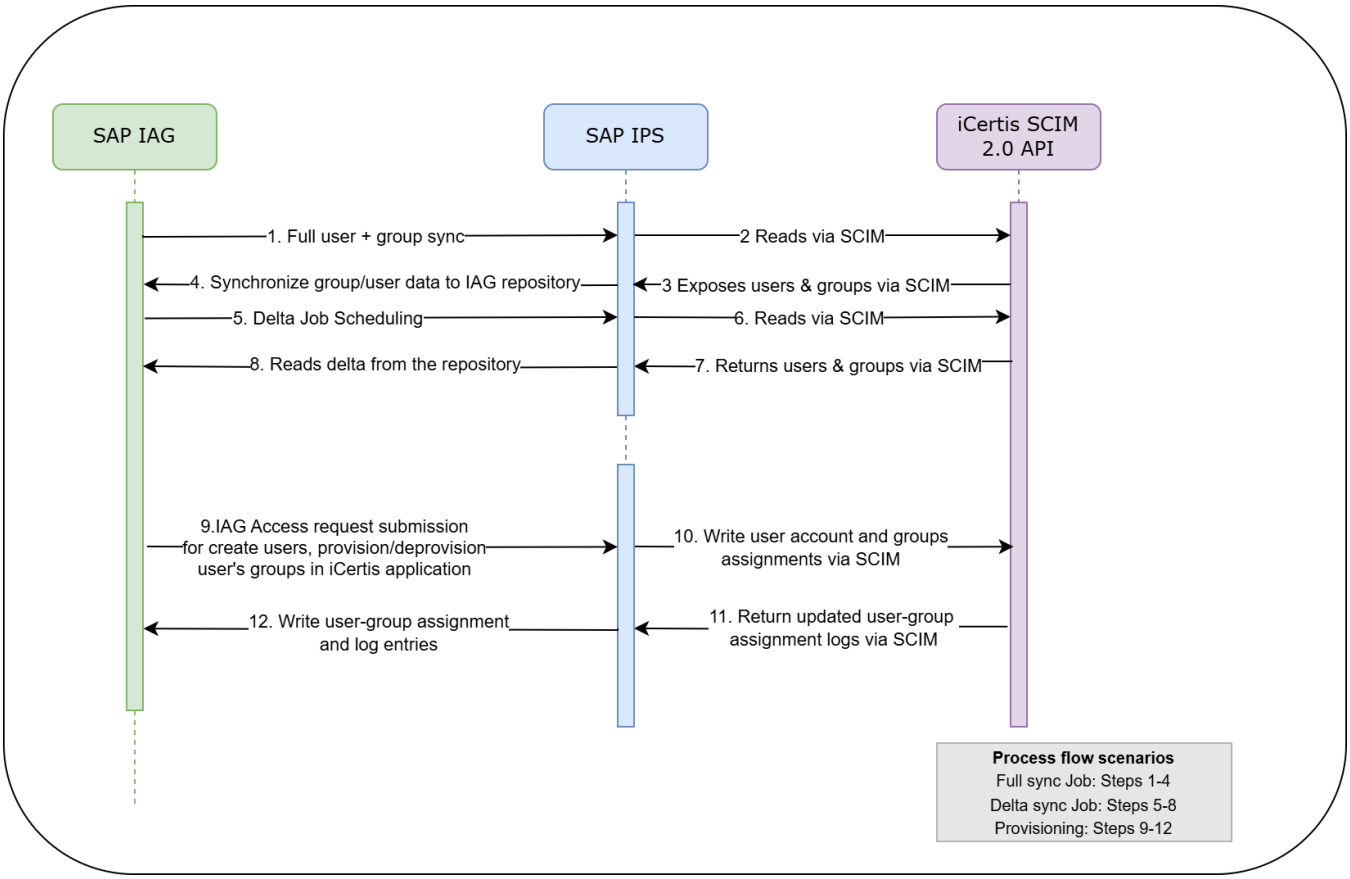
Scope and Objectives

Automate and govern iCertis user access via IAG to reduce manual effort. Also to populate user to group mapping to facilitate the SOD process for Risk Analysis.

Technical Architecture Diagram



Process Flow Diagram



Step	Description
1	Run full sync between to iCertis using IPS as the Proxy
2	Proxy connection from IPS to iCertis SCIM 2.0
3	SCIM exposes API
4	IAG reads data via SCIM
5	Delta job scheduled to run
6	SCIM exposes API
7	Returns users and groups from iCertis to IPS
8	IAG reads delta users and groups
9	IAG access request submission for user creation and group provisioning/deprovisioning in the target application.(Once the request is submitted, the IAG workflow (configured with no approval stage) is triggered. It then runs the background provisioning job, which sends the request to IPS (Identity Provisioning System) to perform the provisioning in the iCertis system.)
10	IPS picks up the request and provisions the access in the iCertis system.
11	Return updated user group assignment logs via SCIM
12	Write back to IAG to update the user record and add the corresponding log entries.

Design Assumptions

iCertis tenant exposes a **SCIM 2.0** endpoint for **Users & Groups** that is reachable from SAP IAG and supports the required ops (**GET/POST/PUT/PATCH** for delta updates), with a **unique, immutable identifier** available for mapping. This SCIM connector will be utilized by **SAP IAG & IPS** to provision users and groups to iCertis.

Dependencies

1. Request the SSO Operations team to provide the **Client ID**, **Client Secret**, and the **Azure OAuth 2.0 Token URL** required for authentication to the iCertis SCIM API. The Icertis App Registration Client Secret via AAD used for SCIM API authentication expires **two years** after its creation. The SSO team will be notified prior to the expiry to obtain new credentials, and updates will be coordinated to ensure uninterrupted integration.
2. Obtain the **scope** value that must be used when requesting OAuth tokens for the iCertis application.
3. Request the iCertis team to ensure that all iCertis Groups are published under the **/Groups** SCIM endpoint to support user and group synchronization.

Security, Integrity and Controls

Access Control & Segregation of Duties

- Security personnel must not manually create, modify, or delete users directly in the iCertis system. All identity changes must be executed exclusively through SAP IAG, with provisioning performed by the SAP Identity Provisioning Service (IPS) via the SCIM connector. This preserves clear control boundaries, auditability, and adherence to segregation of duties requirements.
- No iCertis end-user accounts are granted user-admin privileges.
- If emergency manual intervention is unavoidable, a break-glass procedure applies: raise an **Emergency Access request in IAG** under the PAM request for SAAS application request type obtain a documented exception, perform only the minimum required action, and ensure full post-event review is completed. (The Emergency Access procedure for Icertis can be referred from: KDD081 - Emergency Access Management (EAM) / Privileged Access Management (PAM) for SyWay - SyWay Project - Syensqo - Wiki knowledge base)

Service Account for System-to-System Calls

- The iCertis–IAG integration uses a dedicated technical (service) account registered in Azure AD with the least privileges required to obtain OAuth 2.0 access tokens for the iCertis SCIM API. This account is used by the SAP Identity Provisioning Service (IPS) to create and update users and groups in iCertis.
- The service account authenticates using a securely stored client secret; **Basic authentication is not used**.
- All communication between IPS (as part of the IAG provisioning flow) and the iCertis SCIM API is secured using HTTPS/TLS to ensure confidentiality and integrity in transit.

API Authentication & Gateway Enforcement

- All SCIM API calls are authenticated via **OAuth 2.0 Client Credentials (two-legged OAuth)**.
- APIs published on the **iCertis Portal** are protected by the API Gateway and OAuth.
- The Gateway validates the token associated with the registered client. Only requests with a valid token are accepted.
- Each API request must include a valid OAuth 2.0 access token issued to the client application.

Configuration Requirements

To build the integration of SAP IAG to iCertis application below steps needs to be performed:

- The SSO team registers the OAuth client in Azure AD and shares the **Client ID**, **Client Secret**, and **Token URL** required for configuring the iCertis SCIM connection in SAP Cloud Identity Services (IPS).
- Create the iCertis Proxy System in SAP Cloud Identity Services – Identity Provisioning (IPS) using the configuration details listed below.

Property Name	Value
URL	https://syensqo-dev-api.icertis.com/api/
User	client_id
Password	**********
ProxyType	Internet
OAuth2TokenServiceURL	https://login.microsoftonline.com/Tenant ID/oauth2/v2.0/token
Type	HTTP
OAuth2TokenScope	api://<application_id>/.default

- Refer to the link https://help.sap.com/docs/identity-provisioning/identity-provisioning/proxy-scim-system to set up the iCertis system in Identity Provisioning system.
- Create an application type for the SCIM API in the SAP IAG system, and then create the iCertis application under this application type. Refer to the SAP IAG documentation for the required configuration steps. https://help.sap.com/docs/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE/e12d8683adfa4471ac4edd40809b9038/37e4c466f8294eed88d284650d0c7070.html?state=DRAFT&version=2205
- Run the repository sync job in IAG to read the users and groups from iCertis system.

Design Rationale

Manual user provisioning within iCertis introduces operational risks, lacks scalability, and cannot enforce real-time approval workflows or segregation-of-duties (SoD) checks across systems.

Integrating iCertis with SAP IAG and IPS enables centralized and automated role-based provisioning, ensuring that access is granted only after the required approvals.

This integration further enhances security and auditability through compliant cloud-to-cloud communication, minimizes administrative overhead, and supports consistent access governance across the enterprise.

Why use SCIM via IPS?

- iCertis supports SCIM 2.0 APIs for user and group provisioning.
- SCIM is an industry-standard protocol for managing users, groups, and entitlements across systems. Since SAP IAG does not directly communicate with SCIM endpoints, the SAP Identity Provisioning Service (IPS) acts as the provisioning engine to connect IAG with the iCertis SCIM API.

Data Structure

The following fields will be used to provide the required data structure of the interface:

Attribute + Original Source	SyWay source - SAP CIS (IDdS)	Target Attribute (iCertis SCIM)	What is it used for	Is it Mandatory and why
(mail) - Entra	Email	Business email address	authentication and workflows.	Yes, needed for authentication and workflows
(firstName) - Entra	firstName	Name	To identify User Name	Not mandatory, but recommended for reporting and user display
	lastName	Name	To identify User Name	Not mandatory, but recommended for reporting and user display
EmployeeId - Entra	EmployeeId	Email	To identify ExternalUPN	Its Mandatory field of iCertis for user creation
orgUnitId (The attribute value is hard-coded in IPS(Identity Provisioning Services) for iCertis.)	orgUnitId	Static value as "Syensqo"	To identify OrganizationUnitId and OrgPathId	Its Mandatory field of iCertis for user creation Note: IAG is unable to provision the specific Org Unit for users. Instead, it only sends the top-level Org Unit value.
isAdmin (The attribute value is hard-coded in IPS(Identity Provisioning Services) for iCertis.)	isAdmin	Static value as "No"	To identify Administrator of iCertis	Its Mandatory field of iCertis for user creation Note :By default, IAG passes the Administrator attribute as “NO” to the iCertis application.
Business role(IAG)	IAG retrieves the user groups directly from iCertis.	User Groups	Assigns access and permissions in iCertis	Yes, to enable proper authorization and ensure users can perform their operational activities.

Identifier choice

The user’s email address will be used as the unique User ID in iCertis. This identifier is maintained in IAG and passed to iCertis through IPS during provisioning.

Username normalization

The iCertis user ID is email address and it is used as the unique username in iCertis. Since email IDs are already case-insensitive and uniquely maintained in SAP IAG, no additional normalization is required. The email value is provisioned to iCertis exactly as maintained in the source system.

Delta or Full Load Requirements

The initial synchronization performs a **full data load**, after which the repository sync job operates in **delta mode**, processing only incremental changes. In the event of a job failure, **system logs automatically generate alerts** to notify administrators. Administrators can **manually re-run the sync job** at any time, and the recovery process is **quick and straightforward**.

Monitoring

⚠ All provisioning logs are planned to be sent to the central **SIEM**. The central SIEM is yet to be confirmed but the current plan is to use the standard BTP Audit Log APIs to push logs to the SIEM.

If that's not possible we will look at a pulling mechanism once we confirm the SIEM.

Volumetrics

Job	Data	Estimated time
Full Sync	Users/roles/groups	1 to 2 hours
Delta sync	Users/roles/profiles	1 to 5 mins

Performance Consideration

Data transfer volumes are optimized by leveraging **incremental synchronization**, where only delta changes (new, modified, or deleted user records) are processed instead of full data loads. This approach reduces network usage and processing time while maintaining data accuracy and consistency between systems.

Batch sizes, job frequency(Every 3 hours), and retry intervals are configured based on the expected data volume and system load capacity to ensure timely provisioning without overloading the network or connected systems. IPS job scheduling is carefully aligned with system maintenance windows to avoid conflicts with other integrations or background jobs running in SAP IAG or iCertis.

Delta vs Full loads

To mitigate possible performance issues, we will only trigger full loads when necessary. A full load consume a whole lot of resources in IAG, so this is ran at the beginning only, then **delta reads** thereafter to reduce payloads and runtime. We aim to ensure small **timewindow overlap** in deltas to handle clock skew without duplicating work

Pagination & batch sizing

Not Applicable

Attribute minimization & transformations

IPS will only read the attributes that are needed. Within the transformation we will drop / filter any unused fields to maintain performance.

Rate Limits

Identity Provisioning APIs implement rate limits to control the number of incoming requests for a given time.

The specific rate limit for **Icertis SCIM 2.0** is **5 API calls per minute**, which is a default setting within their API Management service

Identity Provisioning Rate Limits

Value	Description
150	Allowed requests per minute. When the limit is reached, the requests are slowed down.
200	Maximum requests per minute. When the limit is reached, further requests are immediately rejected.

The Identity Provisioning rate limits are enforced at tenant level to the total number of incoming requests (that is, incoming calls for real-time provisioning and proxy systems).

Error Handling

To help support Error Handling, the below table can be reviewed to help with the typical error codes that may be experienced if a SCIM connector fails.

Typically these errors will only be viewable to the IPS admin who has access to the job log in BTP.

Please refer to the below link to get more details on error.

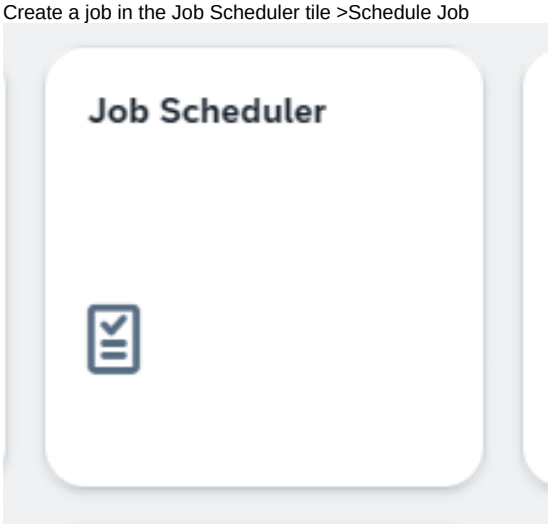
https://help.sap.com/docs/cloud-identity-services/cloud-identity-services/error-messages

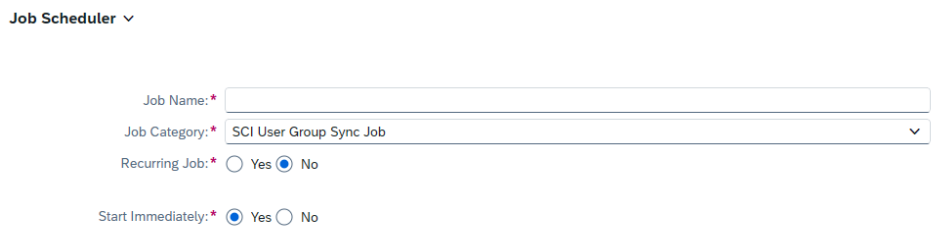
If the **iCertis system is unavailable**, the **recurring synchronization jobs** (scheduled every 3 hours) will **retrieve all delta users and groups** once the system becomes available again.In the event of a job failure, **system logs automatically generate alerts** to notify administrators. Administrators can **manually re-run the sync job** at any time, and the recovery process is **quick and straightforward**.

Testing

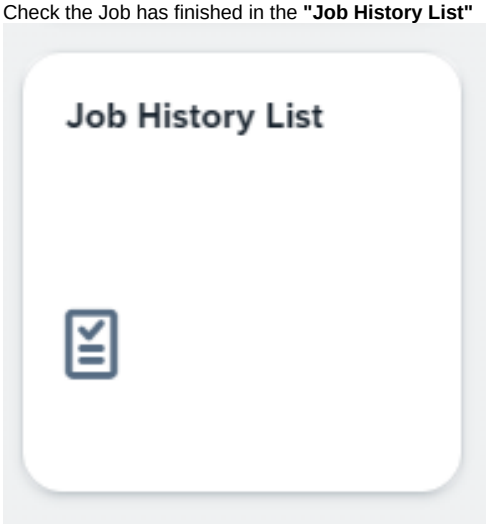
How to Test

- Create a job in the Job Scheduler tile >Schedule Job

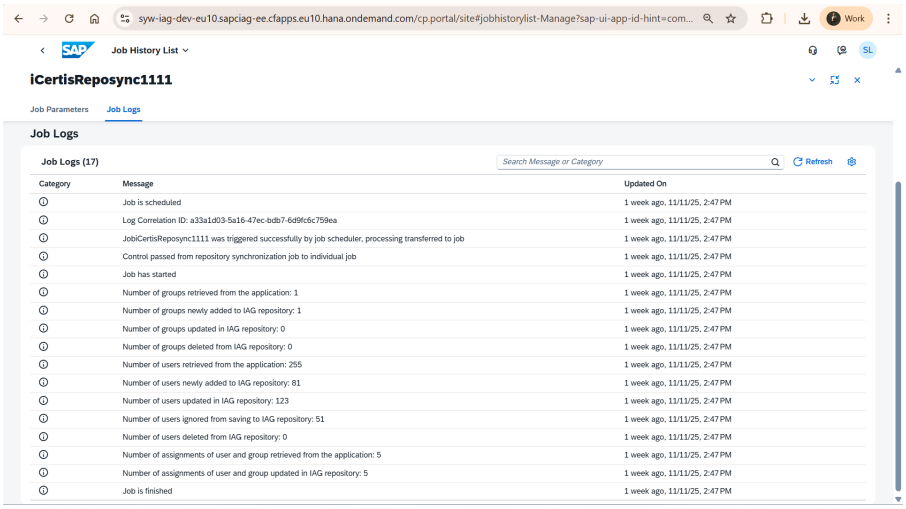




- Check the Job has finished in the **"Job History List"**



An example of a negative test can be seen below. If the job fails, there will be an error code visible in the list: - Below shows **Error 401**, when referenced about you can see this is related to **Bad/expired credentials or wrong OAuth/token setup to iCertis/IAS.**



Test Conditions and Expected Results

ID	Condition	Expected Results
01	Integration check between SAP IAG to iCertis system	The job status of the iCertis Repository Sync in SAP IAG should be monitored to ensure that all relevant data has been successfully synchronized. Negative test case: If the integration fails, the job status will be marked as **"Failed"** or **"Completed with Errors"**. For example, an **Err or 401** may occur, which typically indicates **bad or expired credentials** or an **incorrect OAuth/token configuration** for iCertis/IAS. This status signals that **data synchronization was unsuccessful** and requires investigation.
02	Number of users and roles check in IAG	• In the Access Maintenance app, all roles synchronized from the backend application can be viewed and validated. • In the Maintain Users app, detailed information about users can be accessed and reviewed.
03	User creation from SAP IAG to iCertis	User is created in the iCertis application with the correct group assignments.
04	Business role/iCertis groups assignment to users from SAP IAG to iCertis	The requested business role or group is assigned to the user.
05	Request in IAG to delete an iCertis group assignment from a user	Requested role/group is deprovisioned from the user in iCertis.
06	Request in IAG to terminate the user from the iCertis application	The user's assigned roles will be revoked, and the user account will be deactivated in iCertis.

Test Considerations/Dependencies

Not Applicable

Change log

Version	Published	Changed By	Comment
CURRENT (v. 69)	**May 08, 2026 07:53**	**WENNINGER-ext, Sascha**	
v. 68	Jan 08, 2026 14:38	**TORRES-ext, Benedict**	
v. 67	Jan 08, 2026 12:08	**LOHIYA-ext, Sumitra**	
v. 66	Jan 07, 2026 12:44	**LOHIYA-ext, Sumitra**	
v. 65	Jan 06, 2026 10:47	**LOHIYA-ext, Sumitra**	
v. 64	Dec 15, 2025 17:16	**LOHIYA-ext, Sumitra**	
v. 63	Dec 15, 2025 16:37	**LOHIYA-ext, Sumitra**	
v. 62	Dec 15, 2025 16:33	**LOHIYA-ext, Sumitra**	
v. 61	Dec 15, 2025 16:29	**LOHIYA-ext, Sumitra**	
v. 60	Dec 15, 2025 16:16	**LOHIYA-ext, Sumitra**	

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.

May 08, 2026	Actor	Type	Activity	Version
Approved	WENNINGER-ext, Sascha	State	changed state to Approved at 7:53 am	v69
Revision under Review	WENNINGER-ext, Sascha	State	gave *Minor change* approval at 7:53 am	
		State	changed state to Revision under Review at 7:53 am	v69
Revision in progress	WENNINGER-ext, Sascha	State	changed state to Revision in progress at 7:53 am	v69
Approved	WENNINGER-ext, Sascha	Edit	updated the page at 7:53 am	
Jan 09, 2026				
	TILBEE-ext, Amanda	State	changed state to Approved at 12:12 pm	v68