

UC Name	Semi-automated onboarding with verification after Discovery scan	
UC #	1	
Primary Actor	PAM administrator	
Use Case Story	Enables bulk onboarding of privileged accounts (executives, IoT, cloud) via CyberArk Discovery, reducing errors (20%) and time (70%), ensuring Zero Trust, AAA framework, and compliance with ISO27001/NIS2/RGPD/DORA.	
Trigger	New privileged account request from HR/IGA for executives, cloud, or IoT identities.	
Pre-Condition	1. Clear onboarding policy established, identifying privileged accounts and enforcing separation from standard accounts (IGA-managed for daily tasks).	
	2. Accounts registered in AD or target systems (multi-cloud: AWS/Azure/GCP, IoT devices).	
	3. Accounts belong to critical applications/servers.	
	4. Onboarding rules, platforms, and Safes configured.	
	5. Discovery Scan executed, results in Pending Accounts.	
	6. PAM Administrator performs verification process (rights, safes, platforms, Master Policy compliance).	
	7. Onboarding bulk initiated after verified accounts.	
Post-Condition	Accounts onboarded in CyberArk Safes, enabling secure actions via PSM. Ensures Zero Trust (continuous verification, least privilege), AAA (Authentication via IDP, Authorization via Master Policy, Accounting via audits), and compliance with ISO27001/NIS2/RGPD/DORA. Reduces errors (20%) and unmanaged accounts (150 in 2024).	
Primary Flow (PF)	Title: Semi-automated onboarding	
	Actor Action	System Response
	1) Navigate to Accounts > Pending Accounts	2) Display pending accounts from Discovery.
	3) Select accounts (bulk)	4) Highlights accounts, enables Onboard
	5) Click Onboard, define Safe/Platform/rotation	6) Pre-fills fields, launches onboarding
	7) Monitor Job Monitor	8) Shows "Onboarding completed", moves accounts to Account View.
Alternate Flow 1(AF1)	Title: Manual onboarding of privileged accounts	
	Trigger: Discovery unavailable.	
	Post-Condition: Account onboarded manually, compliant with Zero Trust/AAA, ISO27001/NIS2/GDPR/DORA.	
	Actor Action	System Response
	1) PAM admin navigates to Accounts > Add Account, enter details (platform, Safe), validates.	2) Validates and onboards to Safe.
Exception Flow (EF1)	Title: Failed onboarding	
	Trigger: Onboarding error (e.g., wrong platform, duplicate account).	
	Post-Condition: Failed accounts logged/alerted, no risks from incomplete onboarding.	
	Actor Action	System Response
		1) System keeps failed accounts in Pending.
	2) PAM admin retries or onboards manually	