SYMBEEO

PUBLIC

DESIGN STUDY

Identity and PAM for 4,000 staff, passwordless in 12 months

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Security	Life Sciences	Life-sciences company
DOCUMENT	**VERSION**	**DATE**
SEC-006	1.3	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SEC-006	Version	1.3
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.2, Sep 27, 2026
Capability	Security	Industry	Life Sciences
Author	David Morgan	Role	Principal Security Architect
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 6
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 8
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's own current page on Sep 18, 2026 · [S*] figure from the vendor's page summary where the page itself could not be opened · [A] design assumption for the typical buyer, to be confirmed by the signing engineer · [T] design target taken from the design's stated outcome or derived from it. Every figure carries one tag. No figure comes from any prior engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 18, 2026	1.0	First issue.
Sep 20, 2026	1.1	Public implementations added; figures reconciled with published sources.
Sep 27, 2026	1.2	Figures and platform details rechecked against published sources.
Oct 10, 2026	1.3	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.

1 · Scope

Who it is for. The CISO of a life-sciences company with GxP obligations, whose staff sign in with passwords and SMS codes, whose administrators share standing privileged accounts, and whose laboratory instruments sit on the same network as the office, who has 12 months to reach passwordless and just-in-time privilege without stopping research.

Typical buyer [A]. A life-sciences company with two research sites and a plant: 4,000 staff (3,200 office and research, 800 plant), 120 IT and OT administrators, 600 laboratory instruments and instrument PCs, 200 privileged Azure and Windows Server targets, an existing Microsoft 365 tenant with Entra ID, Cisco campus switching and wireless at all three sites.

What is in. Phishing-resistant passwordless sign-in on Entra ID with FIDO2 security keys for every member of staff; privileged access through just-in-time role activation with session recording; network access control with posture on the laboratory and plant segments through Cisco ISE; the 12-month rollout sequence. **What is out.** The GxP validation package itself; instrument vendor firmware; the plant's DCS; third-party contractor identities beyond the guest flow.

Assumptions. Microsoft is the identity and privileged-access vendor [A]; Cisco is the network access control vendor [A]. Staff have Windows 11 devices joined to Entra ID [A]. Laboratory instruments cannot run an agent and cannot do 802.1X [A]. Entra ID P2 and Entra ID Governance licensing is in place for the 4,000 staff [A].

Related documents, read Sep 18, 2026. Microsoft Entra passkeys (FIDO2) concept, https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passkeys-fido2 · Plan a phishing-resistant passwordless deployment, https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-deploy-phishing-resistant-passwordless-authentication · What is Privileged Identity Management, https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure · Azure Bastion session recording, https://learn.microsoft.com/en-us/azure/bastion/session-recording · Cisco ISE 3.5 release notes, https://www.cisco.com/c/en/us/td/docs/security/ise/3-5/release_notes/cisco-ise-release-notes-35.html · Cisco Secure Network Server 3800 Series datasheet, https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/secure-network-server-3800-series-ds.html · Microsoft Inside Track, Windows Hello for Business and day-one authentication at Microsoft (Mar 5, 2026, updated Aug 14, 2026), read Sep 20, 2026, https://www.microsoft.com/insidetrack/blog/getting-started-with-windows-hello-for-business-and-day-1-authentication-at-microsoft/ · Microsoft Inside Track, protecting elevated-privilege accounts at Microsoft (Mar 25, 2019, updated Aug 14, 2026), read Sep 18, 2026, https://

© 2026 Symbeeo. All rights reserved. · Public

www.microsoft.com/insidetrack/blog/improving-security-by-protecting-elevated-privilege-accounts-at-microsoft/ ·
Cisco ISE Secure Wired Access Prescriptive Deployment Guide (Jan 21, 2021, edited Nov 3, 2025), read Sep 20, 2026, https://community.cisco.com/t5/security-knowledge-base/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515.

1c · Public implementations this design follows

Deployment rows are real public deployments, each dated. Where no public deployment matches, the row is Vendor documentation: the vendor's document that this design, Symbeeo's own, is built on.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Deployment. Microsoft's own workforce onboarded to Windows Hello for Business and security keys on day one through an internal identity-pass flow: 30-day verified identity proof, Temporary Access Pass, Conditional Access; password-reset volume fell 80 %	Microsoft · Mar 5, 2026, updated Aug 14, 2026	R5, R7 and §4.2: identity proofing, then TAP, then key and Windows Hello registration in one session is the vendor's own production flow; the record gives no headcount, so it settles the sequence, not the 12-month pace	https://www.microsoft.com/insidetrack/blog/getting-started-with-windows-hello-for-business-and-day-1-authentication-at-microsoft/
Deployment. Microsoft's own administrators (more than 40,000) hold no persistent admin group membership; privileges are elevated just in time for four to eight hours from secure admin workstations under Conditional Access	Microsoft · Mar 25, 2019, updated Aug 14, 2026	R10 and §4.4: eligible-not-active roles with time-bound activation for the 120 administrators is the vendor's own practice at more than 300× the scale	https://www.microsoft.com/insidetrack/blog/improving-security-by-protecting-elevated-privilege-accounts-at-microsoft/
Vendor documentation. Cisco ISE Secure Wired Access Prescriptive Deployment Guide on Catalyst 9300: monitor mode, then low-impact mode, then closed mode; 802.1X first, MAB for headless endpoints, load-balanced PSNs for large sites	Cisco · Jan 21, 2021, edited Nov 3, 2025 (ISE 2.4)	R4, §4.5 and §4.6: the report-only period before enforcement per wave and MAB with profiling for instruments follow the vendor's prescribed three-stage rollout; the guide predates ISE 3.5, so posture features in R12 rest on the 3.5 release notes	https://community.cisco.com/t5/security-knowledge-base/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Staff passwordless on Entra ID	4,000, with FIDO2 security keys	[T]
R2	Time to reach R1	12 months	[T]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R3	Privileged access	just-in-time, no standing privileged accounts except two break-glass accounts (§5), every session recorded	[T]
R4	Laboratory systems	behind ISE posture checks	[T]
R5	Credential type by persona	FIDO2 security keys for admins and highly regulated users; Windows Hello for Business as the local credential	[S] Microsoft deployment plan
R6	Enforcement control	Conditional Access "Require Authentication Strength – Phishing-resistant MFA"	[S] Microsoft deployment plan
R7	Onboarding credential	Temporary Access Pass to bootstrap the first portable credential	[S] Microsoft deployment plan
R8	Attestation	enforced in the passkey profile; only device-bound passkeys allowed when enforced	[S] Microsoft passkeys concept
R9	Windows Hello for Business	cloud Kerberos trust; Windows 11 22H2 minimum; up to 10 users per device	[S] Microsoft deployment plan
R10	Privileged roles	just-in-time, time-bound, approval and MFA on activation, access reviews, downloadable audit history	[S] PIM
R11	Session recording	Azure Bastion Premium SKU records all RDP and SSH graphical sessions through the host to a storage-account blob container	[S] Bastion session recording
R12	NAC platform	Cisco ISE 3.5 with continuous posture reassessment, USB disk-encryption condition, grace periods	[S] ISE 3.5 release notes
R13	NAC appliance	SNS-3855: 24 cores, 128 GB; 100,000 endpoints as dedicated PSN, 50,000 shared	[S] SNS 3800 datasheet
R14	Endpoints under NAC	4,000 staff devices + 600 instruments + 1,200 plant and IoT = 5,800	[A]
R15	Rollout waves	admins month 1–2; research site A month 3–5; research site B month 6–8; plant month 9–11; enforcement month 12	[A]
R16	Security keys issued	4,400 (4,000 plus 10 % spares)	[A] derived from R1

Sixteen rows; nine carry a vendor figure, three are design assumptions, four are design targets.

© 2026 Symbeeo. All rights reserved. · Public

3 · Architecture overview

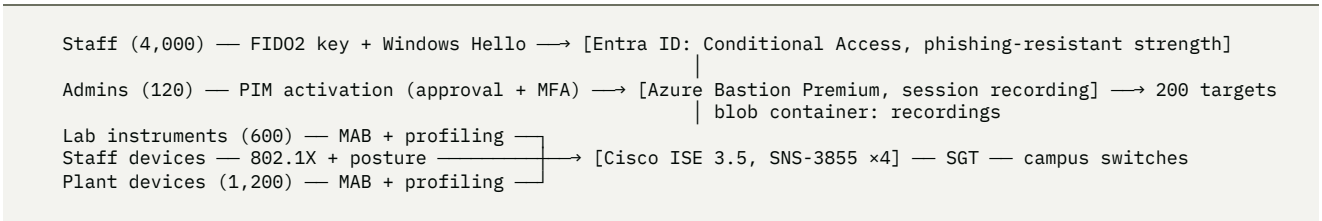


Figure 1. Identity, privileged access and admission

Entra ID carries sign-in for everyone with phishing-resistant enforcement; PIM and Bastion carry privileged access with recording; ISE carries network admission for the laboratory and plant.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
Identity and Conditional Access	Microsoft Entra ID (P2 licensing assumed)	4,000 users	—	Existing tenant; phishing-resistant authentication strength control [S]
Portable credential	FIDO2 security key, Microsoft-attested vendor from the Entra list	4,400	1 per person + 10 % spare [A]	Recommended for admins and highly regulated users [S]; extended to all staff here [T]
Local credential	Windows Hello for Business, cloud Kerberos trust	4,000 devices	—	Recommended local credential [S]
Privileged role management	Microsoft Entra Privileged Identity Management	120 admins	—	Just-in-time, approval, MFA, audit history [S]
Session recording	Azure Bastion, Premium SKU	2 (one per subscription region)	200 targets [A]	Records all RDP/SSH sessions through the host [S]
NAC	Cisco ISE 3.5 on Cisco SNS-3855	4 (2 PAN/MnT, 2 PSN)	5,800 of 100,000 endpoints per dedicated PSN [A]/[S]	Continuous posture reassessment in 3.5 [S]

4 · Design by subsystem

4.1 Passwordless sign-in.

Two personas from the vendor plan [S]: admins and highly regulated users (here, all research and QA staff under GxP) and non-admins (here, plant and office staff). Both receive a FIDO2 security key [T]; Windows Hello for Business is the local credential on every Windows 11 device [S]. Attestation enforced so only device-bound passkeys register (R8) [S]. Rejected: Authenticator app passkeys as the primary credential — shared laboratory PCs and plant kiosks have no personal phone in the room [A].

4.2 Onboarding.

New starters and each rollout wave receive a Temporary Access Pass after identity proofing [S], register the key and Windows Hello in one session, and the password is set to a random value the user never sees [A]. Helpdesk holds the

© 2026 Symbeeo. All rights reserved. · Public

spare keys (R16).

4.3 Enforcement.

Conditional Access policy "Require Authentication Strength – Phishing-resistant MFA" [S] applied in report-only mode per wave, then enforced per wave (R15); month 12 removes the report-only exception for the last group. SMS and voice methods disabled at month 12 [A].

4.4 Privileged access.

All 120 administrators hold eligible, not active, roles in PIM; activation requires approval and MFA, is time-bound, and is reviewed quarterly by access review [S]. Server and Azure targets are reached only through Azure Bastion Premium, which records every session to the storage-account container [S]; retention of recordings 13 months for GxP audit [A]. Rejected: standing local administrator accounts — replaced by the PIM path; rejected: a third-party credential vault — PIM and Bastion leave no standing privileged credential to vault [A].

4.5 Network access control.

ISE 3.5 on four SNS-3855 [S]: two PAN/MnT, two PSNs, one PSN per research site, plant served from site A's PSN over the WAN with the second as fallback [A]. Staff devices: 802.1X certificate authentication plus posture with continuous reassessment and the USB disk-encryption condition [S]. Instruments: MAB with profiling, placed in a laboratory SGT that reaches only the instrument-data servers [A]. Plant devices: MAB with profiling in a plant SGT [A]. Posture failure moves the device to a remediation SGT after the grace period [S].

4.6 Rollout sequence.

R15 waves; each wave has a 2-week report-only period before enforcement. Laboratory segments go under ISE enforcement in the same wave as their site's staff so that a posture rule and a sign-in change never land on a researcher in the same week [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Security key lost	User signs in with Windows Hello on the enrolled device; helpdesk issues a spare key after identity proofing with a new TAP	[S] TAP, [A] process
Entra ID unreachable from a site	Cached Windows Hello sign-in continues on enrolled devices; cloud apps unavailable until connectivity returns	[A]
PIM approval unavailable out of hours	Break-glass accounts, two, excluded from Conditional Access, keys in a physical safe, use alerted	[A]
Bastion host down	Privileged sessions blocked; no unrecorded path exists by design; second Bastion in the other region	[A]
ISE PSN down	Switches fail to the second PSN; on total ISE loss, critical-auth VLAN keeps existing sessions	[A]
Instrument fails posture it cannot take	Instruments are MAB-profiled, not postured; a misprofiled instrument lands in remediation and is re-profiled by the helpdesk	[A]

© 2026 Symbeeo. All rights reserved. · Public

6 · Limits

- Licensing for Entra ID P2, Entra ID Governance and Bastion Premium is assumed, not costed here.
- Laboratory instruments are admitted on MAB and profiling, which is identity by MAC address; the laboratory SGT limits the damage but does not authenticate the instrument.
- ISE endpoint figures are from the SNS datasheet at ISE 3.4 patch 4 and later [S]; the 3.5 figure is confirmed with the vendor before order.
- Session recording covers RDP and SSH through Bastion; console access to plant systems is not recorded by this design.
- The 12-month schedule has no slack for a wave that slips; the enforcement month is the buffer.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

David Morgan

Principal Security Architect

CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

SEC-006 · Version 1.3 · Oct 10, 2026