

SOLUTION SCENARIO / AS OF 2026-10-02

# Keycloak application SSO, with lifecycle ownership

One access journey, from approved arrival to verified removal.

ILLUSTRATIVE / PROPOSED SELECTIONS / MODELED FINANCIAL RESULTS

This example uses its own size and budget; figures are illustrative, not customer results or quotes.

## Scenario and intended outcome

ENVIRONMENT

Illustrative 50-user professional-services firm with six applications that can support the selected federation pattern.

OBJECTIVE

Reduce repeated application login administration and establish explicit enrollment, recovery, privilege and removal responsibilities.

SCOPE

Application SSO and lifecycle design for the pilot applications. Network admission and device management remain separate scopes.

MODEL BOUNDARY

Six-application SSO component for 50 synthetic users, not a full managed IT subscription.

## A repeatable selection method

START WITH THE REQUIREMENT

Map the business workflow, data classification, integrations, scale, recovery objectives, operator skills and support hours. Treat eligibility, security and mandatory features as pass/fail gates before scoring price.

COMPARE SUITABLE CANDIDATES

For candidates that pass the gates, score functional fit 30%, operational maintainability 25%, integration and data portability 20%, three-year total cost 15%, and supplier/support resilience 10%. These are proposed weights, not completed vendor test results.

PROVE THE CHOICE

Run a representative pilot, negative tests and recovery exercise. Price hosting, retention, patching, engineering, support, training and exit. A lower license bill wins only when the complete solution meets the requirement.

## Proposed selections and alternatives

Illustrative options for evaluation; selection does not represent a completed vendor test or an actual quote.

### FIRST, PASS THE GATES

Map the business workflow, data classification, integrations, scale, recovery objectives, operator skills and support hours. Treat eligibility, security and mandatory features as pass/fail gates before scoring price.

### PROPOSED SCORING WEIGHTS AFTER THE PASS/FAIL GATES

For candidates that pass the gates, score functional fit 30%, operational maintainability 25%, integration and data portability 20%, three-year total cost 15%, and supplier/support resilience 10%. These are proposed weights, not completed vendor test results.

| PROPOSED DIRECTION                                                                                                                                                                                                      | ALTERNATIVE TO TEST                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Proposed: Keycloak for suitable application federation</b><br><br>Pilot the open-source identity layer using the supported OIDC/SAML interfaces, with a maintained production configuration.                         | Prefer an existing licensed identity platform if it already meets the requirement at lower incremental total cost. Protocol support does not prove an application integration. |
| PROPOSED DIRECTION                                                                                                                                                                                                      | ALTERNATIVE TO TEST                                                                                                                                                            |
| <b>Proposed: retain the customer's authoritative directory</b><br><br>Define the source of identity and role ownership; keep privileged and emergency paths explicit.                                                   | A second directory is justified only by a documented requirement. Keycloak alone is not endpoint management or a complete identity-governance program.                         |
| PROPOSED DIRECTION                                                                                                                                                                                                      | ALTERNATIVE TO TEST                                                                                                                                                            |
| <b>Proposed: protected database, backup and supported operations</b><br><br>Budget TLS, persistence, patching, monitoring, recovery and specialist support. Rehearse the recovery and application logout/removal paths. | A supported commercial distribution or managed identity service may reduce operator burden. License savings are tested against the complete operating cost.                    |

### PROOF BEFORE CHOICE

Run a representative pilot, negative tests and recovery exercise. Price hosting, retention, patching, engineering, support, training and exit. A lower license bill wins only when the complete solution meets the requirement.

# Architecture flow and delivery path

The sequence below follows the supplied scenario flow and implementation stages.

## Architecture flow

**01****Directory -> approved identity lifecycle**

The customer approves identity, roles and removal; operators apply the agreed changes.

**02****Identity provider -> supported applications**

Federation connects a representative application and verifies required claims and authorization.

**03****Lifecycle -> evidence**

Access, recovery and removal tests produce an acceptance record and accountable exceptions.

## Implementation stages

|                     |                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------|
| 01 Map dependencies | Inventory applications, protocols, groups, local accounts and existing license entitlements.                            |
| 02 Define and pilot | Approve roles and recovery, configure one representative app and use synthetic identities.                              |
| 03 Stage migration  | Move applications in agreed batches; preserve a tested emergency path and rollback to the previous trusted integration. |
| 04 Accept and train | Test authorized and denied access, session behavior, removal and restore; train primary and backup operators.           |

# Acceptance and operating handoff

Acceptance evidence is scoped to the illustrative component described in this brief.

## Acceptance checks

01

### Acceptance check 1

An approved identity receives only the intended application role.

02

### Acceptance check 2

Wrong audience/issuer or unauthorized access is rejected by the application.

03

### Acceptance check 3

Removal and relevant sessions behave according to the agreed policy.

04

### Acceptance check 4

Recovery restores the service without bypassing documented authority.

## Common handoff

01

### Handoff 1

Customer owns approvals and business priorities; L8DT owns only the operating tasks and access authority in the signed schedule.

02

### Handoff 2

Deliver versioned configuration, asset/data-flow registers, escalation and recovery runbooks, license obligations, known gaps and an acceptance record.

03

### Handoff 3

Rehearse the operator workflow and restore before acceptance. Record owners, backup owners, training attendance, support hours and supplier escalation.

04

### Handoff 4

Review coverage and evidence monthly; revisit capacity and access quarterly. Define export, credential removal and retention at termination.

## 36-month economics

Synthetic scenario inputs and calculated model outputs. These values are not a quote or realized savings.

### Monthly assumptions and setup

| Input                         | Illustrative commercial comparator | Illustrative L8DT model |
|-------------------------------|------------------------------------|-------------------------|
| One-time setup                | \$7,000                            | \$9,500                 |
| License / month               | \$600                              | \$0                     |
| Infrastructure / month        | \$100                              | \$250                   |
| Service / month               | \$600                              | \$800                   |
| Monthly cash total            | \$1,300                            | \$1,050                 |
| Customer effort / month       | 6 hours                            | 8 hours                 |
| Customer hourly value         | \$65                               | \$65                    |
| Customer effort value / month | \$390                              | \$520                   |

### Calculated totals across 36 months

| 36-month total                        | Commercial comparator | L8DT model |
|---------------------------------------|-----------------------|------------|
| Cash TCO (setup + monthly cash)       | \$53,800              | \$47,300   |
| Customer-effort value                 | \$14,040              | \$18,720   |
| Economic TCO (cash + customer effort) | \$67,840              | \$66,020   |

### Modeled comparison outputs

|                                                    |                                                                                    |                                                   |
|----------------------------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------|
| NET CASH AVOIDANCE<br><b>+\$6,500</b>              | COST AVOIDANCE<br><b>12.08%</b>                                                    | CASH ROI<br><b>13.74%</b>                         |
| ECONOMIC BENEFIT<br><b>+\$1,820</b>                | PRETAX PROFIT DELTA: YEAR 1 / STEADY<br><b>Y1 +\$500</b><br><b>steady +\$3,000</b> | PAYBACK<br><b>10 months</b>                       |
| L8DT EXTRA CUSTOMER TIME / MONTH<br><b>2 hours</b> | SENSITIVITY ADD-ON / MONTH<br><b>\$240</b>                                         | SENSITIVITY NET CASH AVOIDANCE<br><b>-\$2,140</b> |

# Model definitions, boundaries and references

Use the links and source notes for review. Public destination routes are targets; deployment was not verified for this package.

Definitions: cost avoidance = net cash avoidance / commercial 36-month cash TCO; cash ROI = net cash avoidance / proposed L8DT 36-month cash TCO. Economic benefit = commercial economic TCO minus L8DT economic TCO; economic TCO adds customer effort valued at the stated hourly input. Valued time is not payroll saving. Sensitivity applies the stated additional monthly L8DT operating cost for all 36 months.

**REALIZED OUTCOMES**

Realized ROI: NOT PROVIDED | Realized profit: NOT PROVIDED. These are not provided as customer results.

**INTERPRETATION LIMIT**

Illustrative scenario only. Proposed selections, input costs and modeled values are not actual customer results, completed vendor test results, or supplier quotes.

**HYPOTHETICAL PROFIT-DELTA ASSUMPTION**

Year-one pretax profit delta uses the modeled recurring cash difference less any incremental setup; steady-year delta uses 12 times the recurring cash difference. The model assumes costs are recognized as operating expenses with equal revenue and other costs. Capitalization, depreciation and tax treatment can differ.

## Out of scope for this model

Application licenses, endpoint/MDM, network AAA, application rewrites, privileged-access software, data migration and taxes are excluded equally. Production availability and support commitments require scoped engineering.

**WHAT TO PROVE AND PRICE**

Run a representative pilot, negative tests and recovery exercise. Price hosting, retention, patching, engineering, support, training and exit. A lower license bill wins only when the complete solution meets the requirement.

## Official project and product references

|                                                                 |
|-----------------------------------------------------------------|
| <a href="#">Keycloak project and guides</a><br>www.keycloak.org |
| <a href="#">Keycloak production guides</a><br>www.keycloak.org  |

Source data as of 2026-10-02.

## Related L8DT destinations

|                                                                                                                   |                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <a href="#">Experience story</a><br><a href="/experience/identity-readiness/">/experience/identity-readiness/</a> | <a href="#">Solution detail</a><br><a href="/solutions/identity-readiness/">/solutions/identity-readiness/</a> |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|

Website: <https://www.layer8defensetechnologies.com/>