**Executive Writeup about UnityX as an Accelerator**

**UnityX** as an Accelerator is used for Azure AD (Entra ID) Application Certificate Lifecycle Management. Prevent SSO outages while automating certificate expiry governance., enabling safe self-service.

Azure AD / Microsoft Entra ID application certificates (including SAML signing and encryption certificates and applicable OIDC certificates) are a common root cause of unplanned authentication outages when renewals are missed or poorly governed. These failures typically surface late, require emergency intervention, and create avoidable downtime for business-critical applications.

The UnityX Certificate Lifecycle Management Accelerator delivers a governance-driven, self-service capability to centrally manage application certificates across Entra ID. It provides a unified inventory of certificates with expiry visibility, proactive renewal notifications to application owners and IAM teams, controlled activation of renewed certificates during approved change windows, and standardized evidence generation for operational and audit compliance.

By institutionalizing certificate lifecycle ownership and approvals, the accelerator significantly reduces operational overhead on IAM teams, accelerates renewal turnaround times, and materially lowers the risk of authentication outages caused by expired or unmanaged certificates across the enterprise application landscape.

**1) Summary**

Azure AD/Entra ID application certificates (SAML signing/encryption certs, OIDC-related certs where applicable) are a frequent cause of **unplanned outages** when they expire without timely renewals. This introduces the **UnityX Certificate Lifecycle Management Accelerator**, a self-service and governance-enabled capability that provides a unified inventory of expiring certificates, proactive notifications to app owners and IAM teams, controlled production activation during approved change windows, and standardized evidence for audit and operational compliance.

The accelerator reduces operational burden on IAM teams, improves renewal turnaround times, and materially lowers risk of authentication outages caused by expired certificates across enterprise applications.

**2) Purpose**

- **Eliminate certificate-expiry-driven authentication outages** by ensuring every app owner and IAM team gets advance warning and guided renewal workflows.
- Create a **single pane of glass** for certificate expiry posture across all Azure AD enterprise applications.
- Standardize renewal processes with **controlled production activation** aligned to change management.
- Enable **safe self-service** renewals in lower environments to reduce IAM operational overhead.
- Provide **audit-ready evidence** (who changed what, when, and which certificate versions were used).

**3) Target Audience**

This is designed for organizations that have a large SSO footprint and multiple app integrations:

1. **IAM / Entra ID Operations Team**
    - Owns tenant configuration, enterprise apps, access governance, and identity risk controls.
2. **Application Owners / Application Custodians**
    - Own app integrations, SSO configurations, certificates, and business continuity.
3. **Change Management / Release Management**
    - Governs production change windows, approvals, and rollback discipline.
4. **Security & Compliance / Internal Audit**
    - Needs evidence of controls, renewal process discipline, and prevention of avoidable outages.
5. **SRE/Operations**
    - Responsible for service reliability, incident reduction, and operational resilience.

**4) UnityX Overview**

The UnityX Accelerator delivers the following core capabilities:

**A. Proactive notification & communications**

1. **Configurable scheduled email delivery** to Application Owners and IAM team with advance notice of certificate expiry
2. **Customizable email templates** (branding, tone, escalation, distribution lists)

**B. Unified visibility and discovery**

1. **Central view of all Azure AD apps with certificate expiry** (days to expiry, status, owner mapping)
2. **Search and filter** by:
    - **App name**
    - **Integration protocol:** OIDC / SAML

**C. Controlled certificate lifecycle operations**

1. **Upload / re-upload certificate** and **activate only during production change window** (governed process)
2. **Download current and uploaded certificate versions** for sharing with app teams and for documentation

**D. Self-service enablement (with guardrails)**

1. **Self-service renewal controls for lower Azure AD environments** (Dev/Test/UAT) to reduce IAM load and allow pre-validation before production.

**E. Portal experience (core support requirements)**

- **UnityX portal SSO enabled**
- **Branding support** (logo, colors, standard templates, consistent enterprise experience)

**5) Detailed Approach (Delivery & Operating Model)**

**Phase 1: Discovery & Design (Week 1)**

**Activities**

- Identify tenants/subscriptions, enterprise app inventory scope, and protocol split (SAML vs OIDC).
- Confirm ownership mapping (App Owner, Application Custodian, IAM Admin group).
- Define expiry notification policy: lead times (e.g., 90/60/30/15 days), reminder cadence, escalation path.
- Define governance for production: change window rules, approvals, rollback/verification checklist.

**Deliverables**

- Target architecture & integration plan
- RACI matrix (IAM vs App Owner vs Change Manager)
- Notification policy & template requirements document
- Pilot shortlist (e.g., Top 20 critical apps)

**Phase 2: Build & Configure Accelerator (Week 2)**

**Activities**

- Configure UnityX portal with SSO and enterprise branding.
- Integrate with Entra ID to ingest enterprise apps and certificate metadata.
- Configure search/filter logic (App name, protocol).
- Configure scheduled email jobs and email templates.
- Enable certificate upload/re-upload workflow and certificate download feature.

**Deliverables**

- Configured UnityX tenant instance
- Email templates and schedules
- Dashboard views (expiry posture)
- Role-based access configuration (IAM vs App Owners)

**Phase 3: Pilot & Validation (Week 3)**

**Activities**

- Run pilot for selected apps and validate:
    - correctness of expiry detection
    - correct routing of notifications
    - upload/download workflows
    - lower environment self-service renewals
- Define production activation workflow aligned to change management.
- Train IAM team and App Owners (short enablement sessions).

**Deliverables**

- Pilot report and lessons learned
- Updated runbooks and SOPs
- Operational dashboards and KPIs baseline

**Phase 4: Scale & Go-Live (Week 4)**

**Activities**

- Expand to full tenant / full app scope.
- Activate production governance flow.
- Set monthly hygiene reporting and operational review cadence.
- Hypercare and stabilization.

**Deliverables**

- Full rollout completion
- Operational handbook + support model
- Monthly reporting cadence established

**6) Technology & Architecture (High-Level)**

**Core components**

- **UnityX Web Portal**
    - SSO-enabled for enterprise users
    - Role-based access (IAM Admin, App Owner, Auditor/Read-only)
- **Entra ID Integration Layer**
    - Reads application metadata, certificate details, expiry dates, protocol attributes
    - Supports inventory refresh and near-real-time views (configurable)
- **Scheduler / Notification Engine**
    - Configurable rules for:
        - expiry thresholds (90/60/30/15)
        - reminder schedules
        - escalation recipients
    - Uses customizable email templates (HTML)
- **Certificate Management Module**
    - Upload/re-upload certificate to app record
    - Controlled activation pathway for production (change window gating)
    - Certificate version history and download support
- **Audit & Evidence Logging**
    - User actions, timestamps, before/after certificate versions
    - Exportable reporting for audits and incident postmortems

**Optional integrations (recommended)**

- **ITSM integration** (e.g., ServiceNow) to link activation to change requests and approvals.
- **SIEM integration** to forward audit logs/events for monitoring and compliance.

**7) Why UnityX matters**

1. **Availability / Business Continuity**

    - Prevent avoidable SSO outages caused by certificate expiry.
2. **Security & Control**
    - Reduce risky last-minute changes; enforce change windows and governance.
3. **Operational Efficiency**
    - Reduce IAM team workload by enabling safe self-service in lower environments.
4. **Compliance & Audit Readiness**
    - Provide repeatable process, evidence trails, and demonstrable control maturity.
5. **Standardization**
    - Standard communications and workflows reduce confusion and improve accountability.

**8) Business Outcomes (Measurable impact)**

**Operational outcomes**

- Target **near-zero certificate-expiry incidents**
- Improved proactive posture: fewer emergency change requests
- Reduced time-to-renew (lead time increases, last-minute rush decreases)

**Governance outcomes**

- Clear ownership and accountability per application
- Consistent production change activation discipline

**Security outcomes**

- Reduced exposure due to mismanaged or expired certs
- Improved auditability (who/what/when evidence always available)

**Efficiency outcomes**

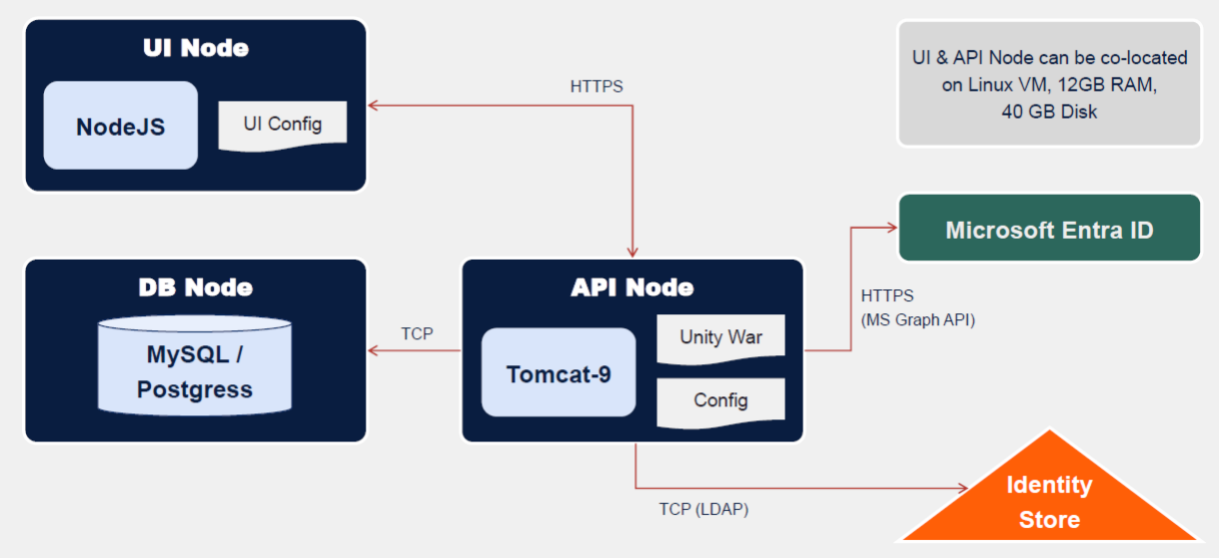
- IAM team spends less time on follow-ups and manual trackers

- App owners can validate renewals earlier in non-prod environments

**9) Value Adds**

1. **Single pane of glass** for all app certificate expiry posture (visibility)
2. **Automated, configurable communications** reduces missed renewals
3. **Protocol-aware discovery** (OIDC/SAML) improves routing and troubleshooting speed
4. **Self-service with guardrails** reduces IAM bottlenecks while maintaining control
5. **Change-window-controlled activation** reduces operational risk and aligns with ITIL practices
6. **Certificate download/versioning** improves coordination and evidence sharing
7. **SSO-enabled, branded portal** improves adoption and reduces training friction

**10) UnityX Deployment Topology**




The UnityX Accelerator is designed as a modular, secure, and enterprise-grade platform architecture that integrates seamlessly with Microsoft Entra ID and existing identity stores, while remaining lightweight and operationally efficient.

The solution follows a **three-tier architecture**—Presentation, Application, and Data—ensuring clear separation of responsibilities, scalability, and ease of governance.

**Presentation Layer (UI Node)**

The UI layer provides a secure, intuitive, browser-based user interface built on Node.js. It enables application owners, identity administrators, and governance teams to view certificate inventories, track expirations, receive actionable alerts, and initiate renewal workflows. All UI interactions are secured over HTTPS, ensuring encrypted communication end-to-end.

**Application Layer (API Node)**

The core business logic resides in the API layer, deployed on Apache Tomcat 9 and hosting the UnityX application services. This layer acts as the orchestration engine, enforcing governance controls, validation logic, approval workflows, and policy checks.
It integrates natively with **Microsoft Entra ID** using secure HTTPS connections via Microsoft Graph APIs to discover, monitor, and manage application certificates. Where required, the platform also supports secure LDAP connectivity to enterprise identity stores, enabling hybrid identity alignment.

The UI and API components can be co-located on a hardened Linux virtual machine (12 GB RAM, 40 GB storage), simplifying deployment while maintaining enterprise performance and availability standards.

**Data Layer (Database Node)**

The data layer supports industry-standard relational databases such as MySQL or PostgreSQL. It securely stores certificate metadata, ownership information, audit logs, approval records, and compliance evidence. Communication between the application and database layers occurs over controlled TCP connections, ensuring data consistency and integrity.

**Security, Governance, and Compliance by Design**

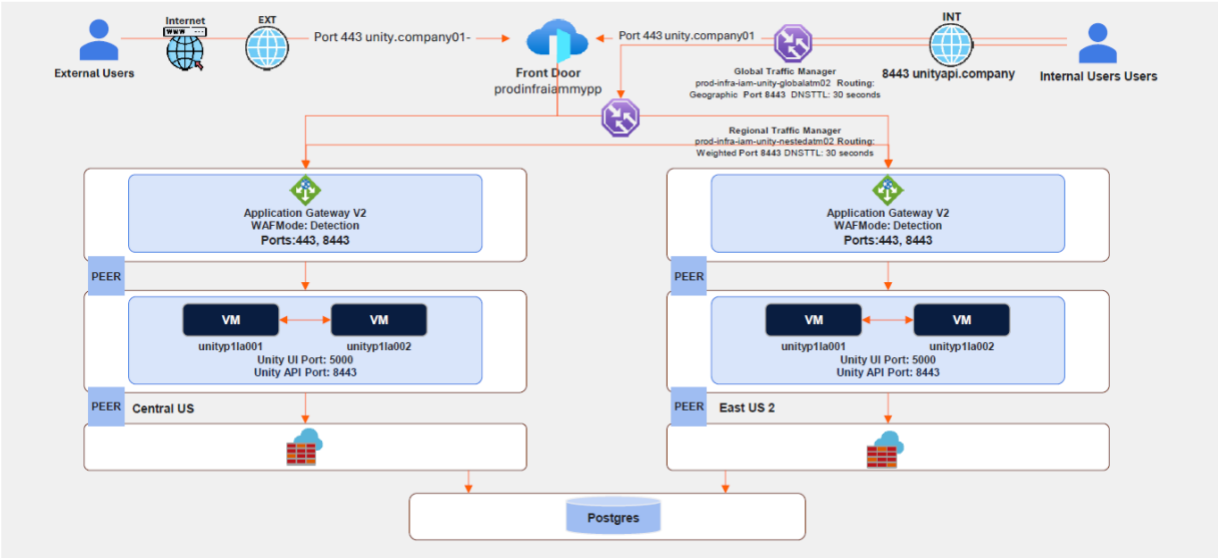
The architecture is designed with security and auditability as first-class principles:

- Encrypted communications across all layers (HTTPS / secure TCP)
- Strict separation of UI, application, and data workloads
- Controlled production activation through approved change windows
- Persistent audit trails and standardized evidence generation for operational and regulatory compliance

**Business Value**

This architecture enables centralized visibility across Entra ID application certificates, reduces dependency on manual IAM operations, and prevents certificate-driven authentication outages. At the same time, it aligns with enterprise IT, security, and compliance expectations—making the UnityX Accelerator suitable for regulated environments and large, distributed application landscapes.

**11) UnityX Deployment – High Availability**




The UnityX Accelerator is deployed on a secure, cloud-native, multi-region architecture designed to deliver high availability, global performance, and enterprise-grade security. The architecture follows a defense-in-depth and resilience-by-design approach, ensuring consistent user experience for both internal and external users while minimizing operational and outage risks.

**Secure Global Access and Traffic Management**

All user traffic—external and internal—is routed securely over HTTPS (Port 443) through Azure Front Door, providing a single global entry point with built-in TLS termination, DDoS protection, and accelerated global access.
Front Door integrates with Azure Traffic Manager, enabling intelligent routing based on geographic proximity and health checks. This ensures users are automatically directed to the nearest healthy region, with a defined DNS TTL to support rapid failover during regional disruptions.

**Perimeter Security and Web Application Protection**

Regional ingress traffic is protected by Azure Application Gateway v2 with Web Application Firewall (WAF) operating in detection mode. This layer defends against common web threats (OWASP Top 10), enforces secure ports (443/8443), and provides controlled exposure of UnityX services while maintaining strong perimeter security.

**Regional Application Tier (Active-Active Design)**

The UnityX application layer is deployed across multiple Azure regions (Central US and East US 2) in an active-active configuration.
Each region hosts a pair of hardened virtual machines running UnityX UI and API services, enabling:

- Horizontal scalability
- Zero single-point-of-failure at the application layer
- Seamless regional failover without user disruption

Secure VNet peering ensures controlled, low-latency communication between components while preventing unnecessary lateral exposure.

**Service Segmentation and Controlled Access**

UnityX UI services operate on an internal application port, while UnityX API services are exposed on a secured API port (8443), enforcing logical separation between presentation and orchestration layers. This segmentation supports tighter access controls, easier policy enforcement, and reduced blast radius during incidents.

**Centralized and Resilient Data Layer**

The platform leverages a centralized PostgreSQL database, serving as the system of record for certificate metadata, application ownership, audit logs, and governance evidence. Database connectivity is restricted to application tiers over secured network paths, ensuring data integrity, consistency, and compliance with enterprise security standards.

**Built-in Resilience, Governance, and Compliance Readiness**

The architecture is purpose-built to support regulated and mission-critical environments by providing:

- Multi-region high availability and automated traffic failover
- Encrypted communications across all layers

- Centralized logging, traceability, and audit-ready data persistence
- Alignment with enterprise security, change management, and operational governance requirements

**Business Outcome**

This architecture ensures that the UnityX Accelerator delivers continuous availability, predictable performance, and strong security posture, even during regional outages or demand spikes. It minimizes operational risk, supports compliance and audit obligations, and provides a scalable foundation for enterprise-wide certificate lifecycle governance.

**12) Dashboarding**

UnityX provides an administrative dashboard designed for managing application policies, supporting various login methods including Local, SAML, and OIDC based SSO. The platform integrates with source systems like Okta and target systems such as Azure AD/Entra ID to import, manage, and provision identity policies efficiently.

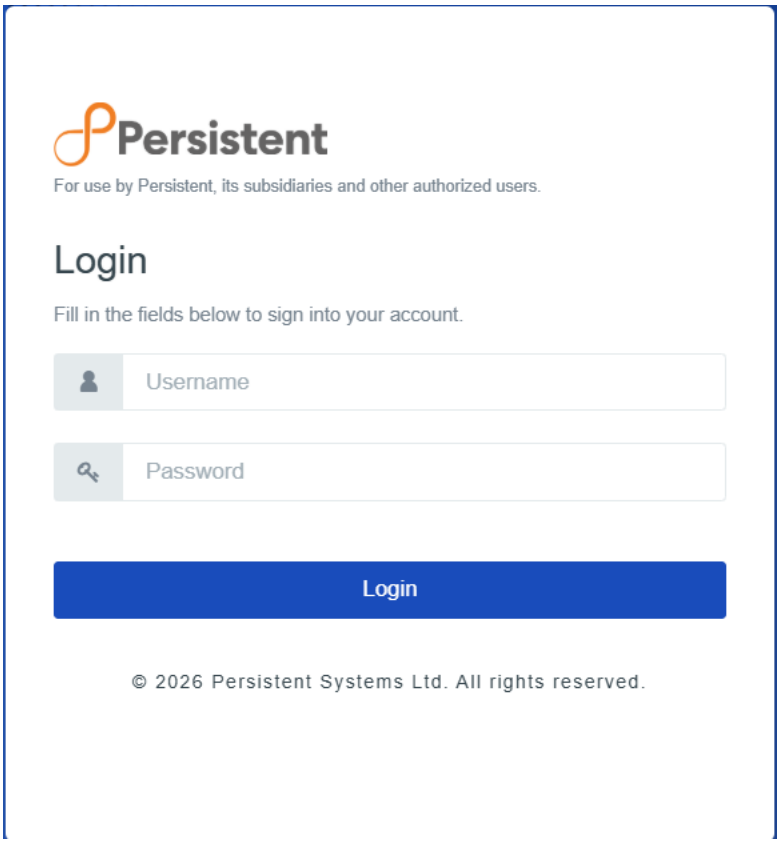
• **Dashboard and User Roles:** The UnityX main dashboard offers two wizards for admin users to view application statistics and manage policies, while non-admin users have limited access to their own policies. The dashboard supports live reporting of policy integration types such as SAML and OAuth in the target environment.

• **Policy Management and Lifecycle:** UnityX allows importing existing policies from source environments like Okta by uploading JSON files, supporting both SAML and OAuth policies. Admins can create new applications from templates, edit, provision, rollback, or delete policies with enforced lifecycle management moving from lower to production environments.

• **Configuration, Reporting, and Documentation:** The platform supports detailed configuration for source and target environments, provisioning, and UI settings. It includes multiple out-of-the-box policy templates and reporting features such as import, audit, and alert reports. Admins can export policy details and integration artifacts as PDFs or email them directly to application teams.

**UnityX sign-in screen**

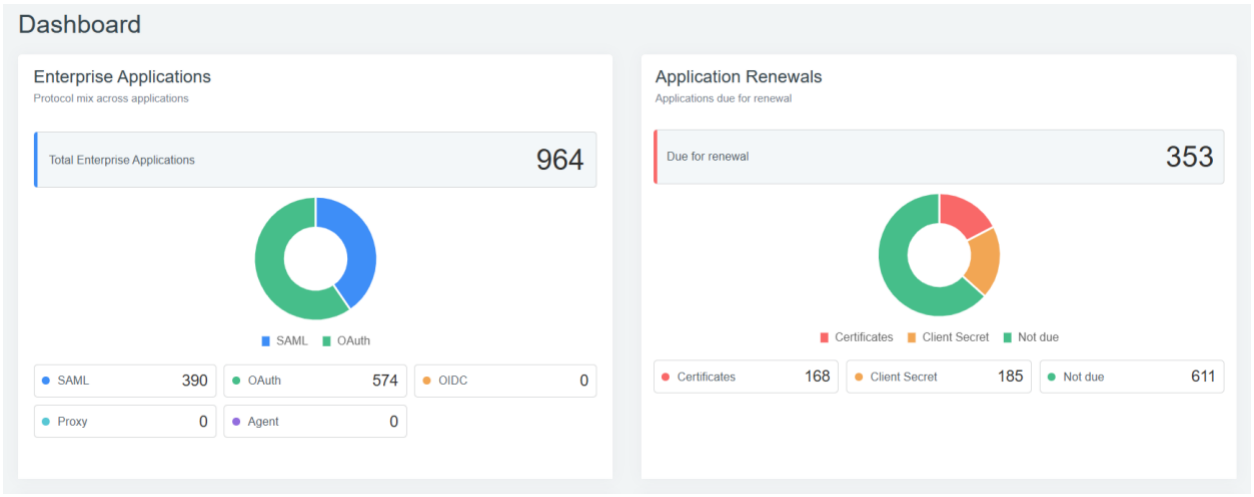
Use this screen to authenticate to UnityX using Local credentials, SAML-based SSO, or OIDC-based SSO.

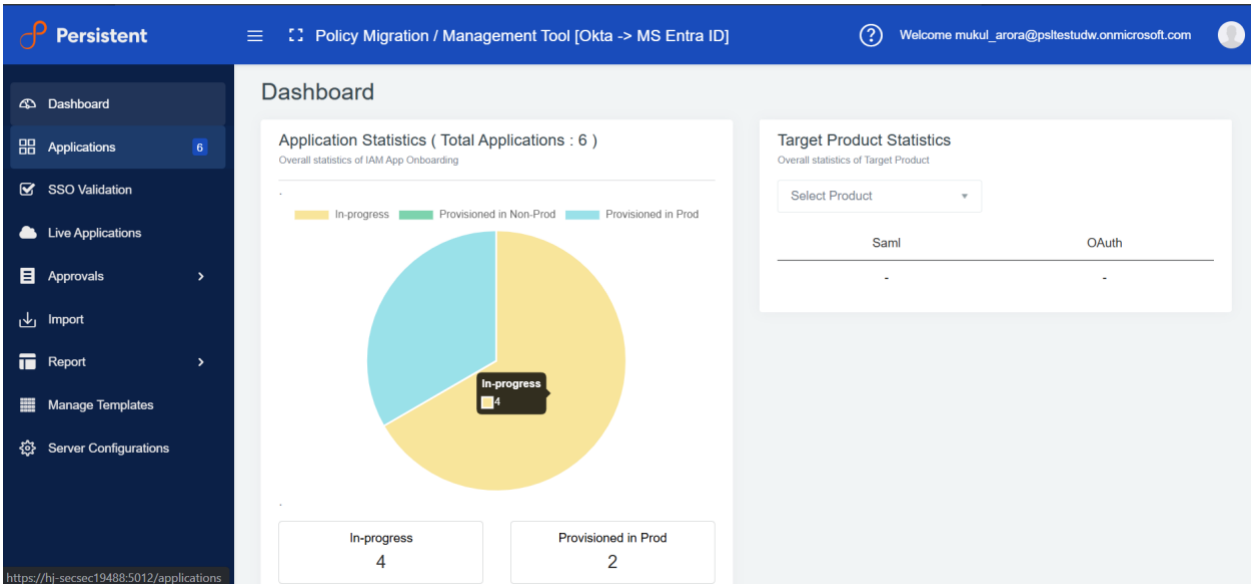


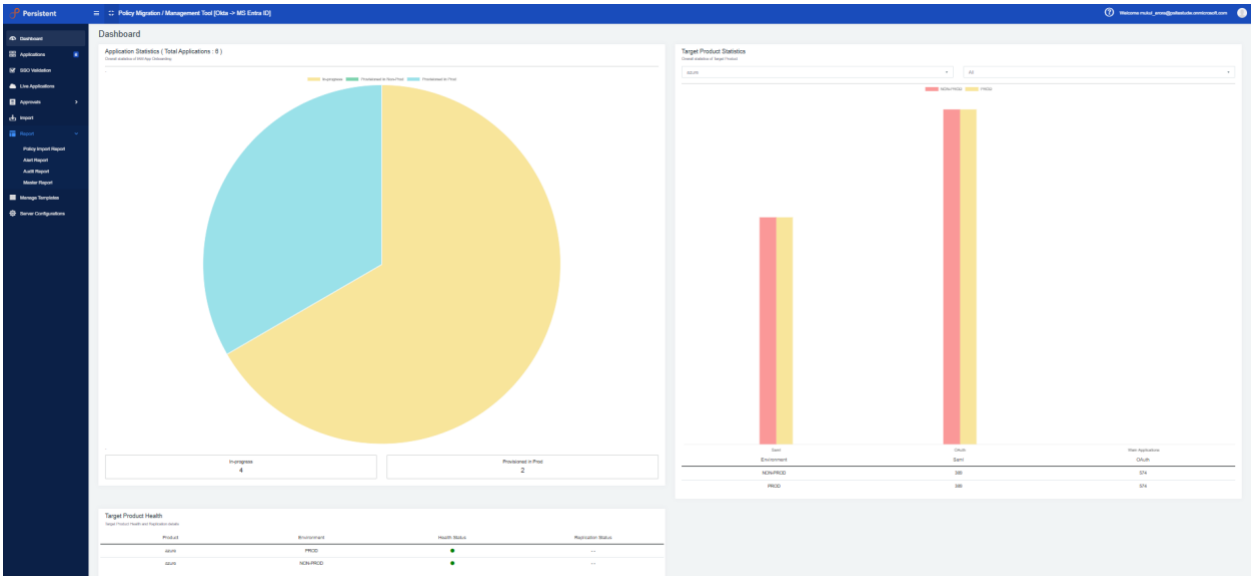

**UnityX main dashboard (Admin)**

This dashboard is available to users with UnityX administrator permissions.

On landing, UnityX displays two guided wizards. Use **Application Statistics** to review applications that are either imported from a source system or managed directly in UnityX.

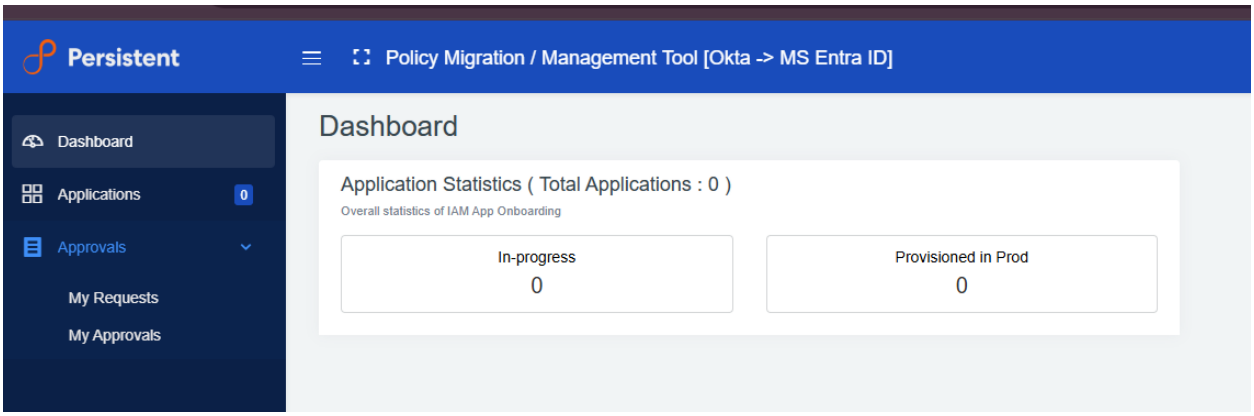

Dashboard
Enterprise Applications
Protocol mix across applications
Total Enterprise Applications
964
SAML
OAuth
SAML 390
OAuth 574
OIDC 0
Proxy 0
Agent 0
Application Renewals
Applications due for renewal
Due for renewal
353
Certificates
Client Secret
Not due
Certificates 168
Client Secret 185
Not due 611


Persistent
Policy Migration / Management Tool [Okta -> MS Entra ID]
Welcome mukul_arora@psltestudw.onmicrosoft.com
Dashboard
Applications
6
SSO Validation
Live Applications
Approvals
Import
Report
Manage Templates
Server Configurations
Dashboard
Application Statistics ( Total Applications : 6 )
Overall statistics of IAM App Onboarding
In-progress
Provisioned in Non-Prod
Provisioned in Prod
In-progress
4
In-progress
4
Provisioned in Prod
2
Target Product Statistics
Overall statistics of Target Product
Select Product
Saml
OAuth
-
-
https://hj-secsec19488:5012/applications



**User dashboard (non-admin)**

Non-admin users have limited access and can manage only the policies assigned to them.

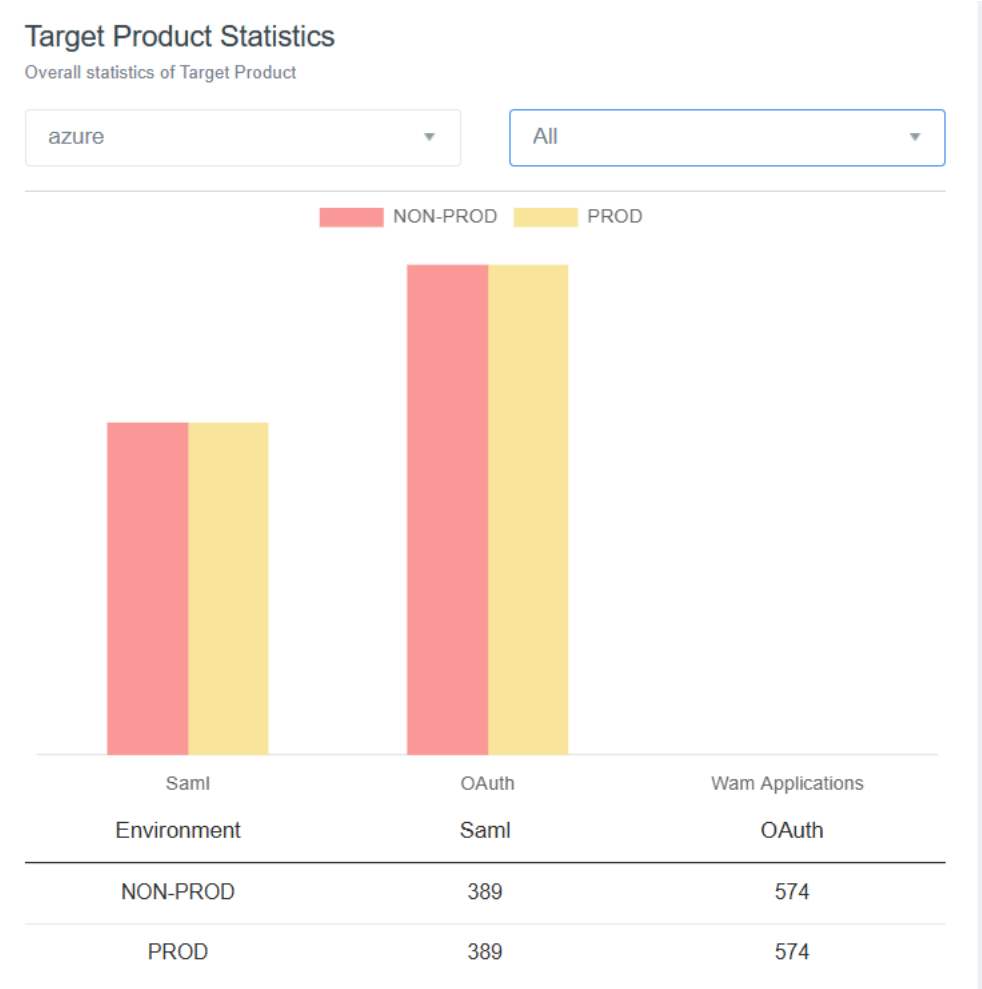



**Current Entra ID policy snapshot**

**Target Product Statistics**

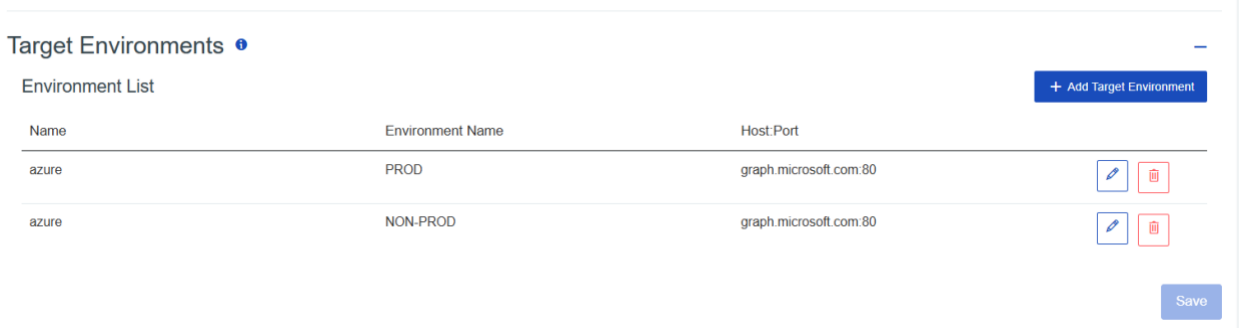
This section provides a live view from the selected target product and environment. It summarizes configured policy/integration types (for example, SAML and OAuth) detected in

the target.




| Environment | Saml | OAuth |
|---|---|---|
| NON-PROD | 389 | 574 |
| PROD | 389 | 574 |

UnityX reads the target product and environment from **Configuration Management**. In the example below, the target is configured as **Azure AD / Entra ID**.



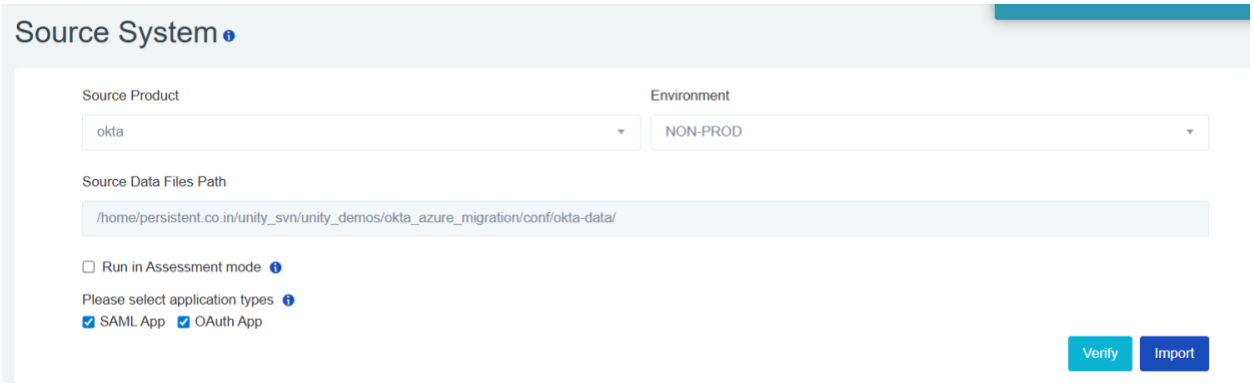
**Source Environment configuration**

Configure the source system that UnityX connects to for importing existing policies. In the example below, the source is configured as **Okta**.


**Import from source system**

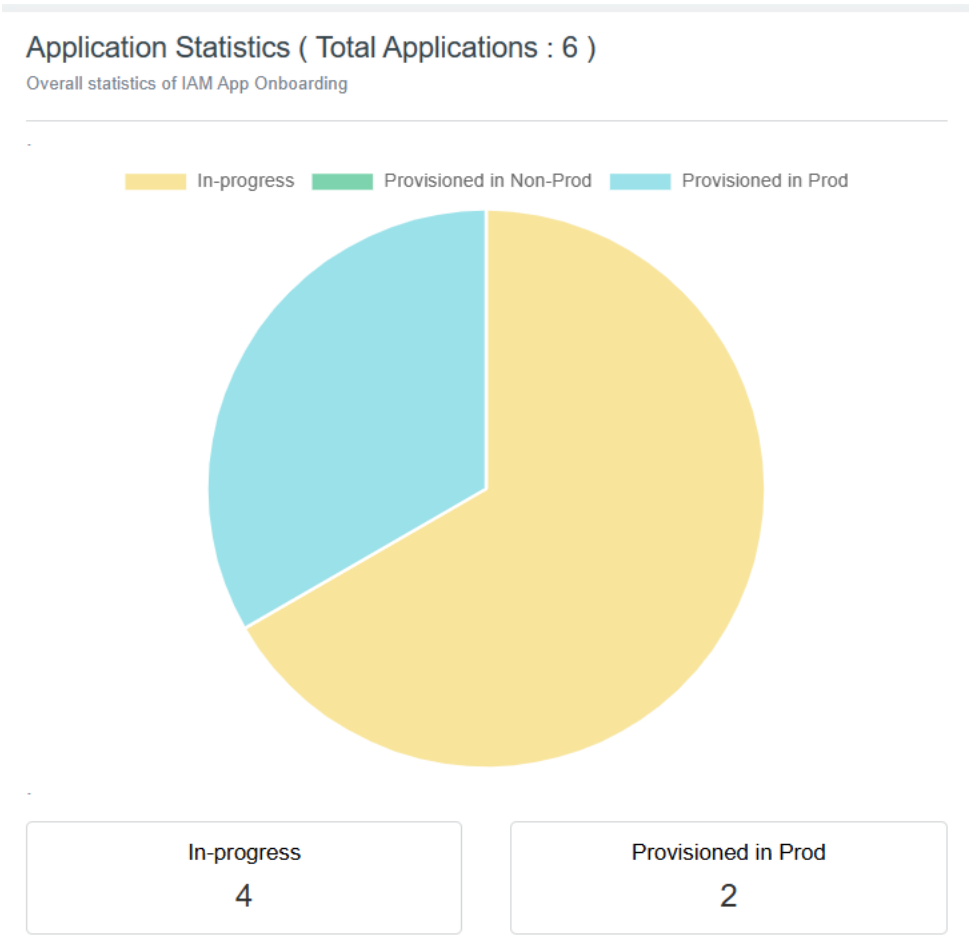
Use import to bring existing policies into UnityX from the configured source system. To control scope, UnityX currently requires you to upload the application JSON exported from Okta and place it in the configured **Data File Path**.

You can choose to import **SAML** policies, **OAuth/OIDC** policies, or **both**.



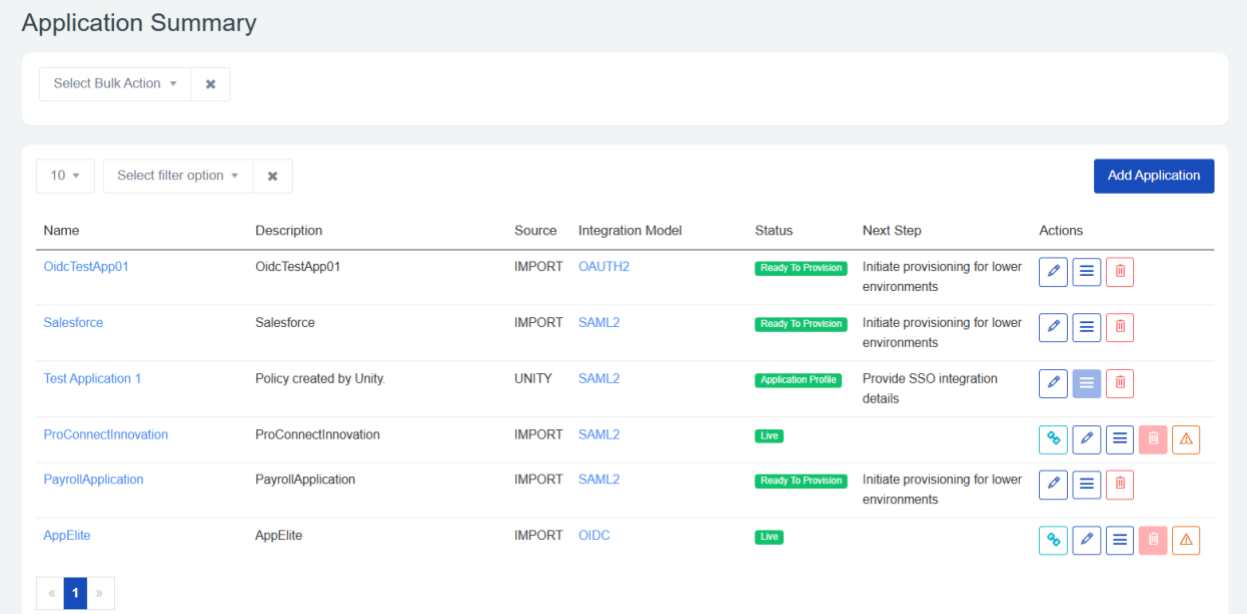

**Application Statistics**

Imported policies and newly created policies are listed under **Application Statistics**. Policies are grouped by status (for example, In Progress, Provisioned in Non-Prod, and Provisioned in Prod).



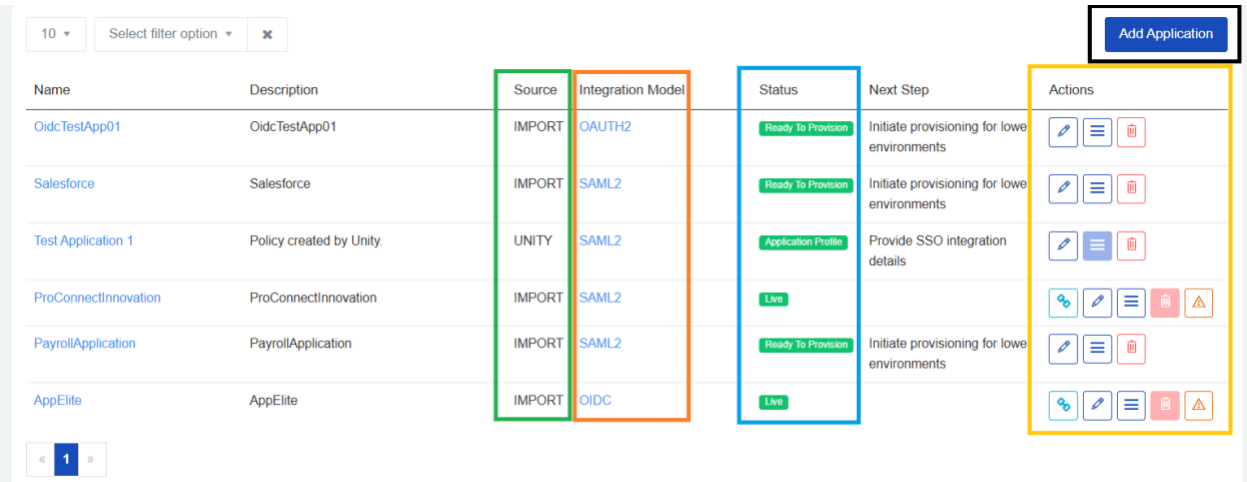

**Application Summary**

**Application Summary** lists all policies managed by UnityX. From this page, admins perform key lifecycle tasks such as editing imported policies, provisioning, rollback, and deletion. The grid supports pagination for large policy sets and shows the policy source (Imported or Created in UnityX) and integration model (OAuth2, OIDC, or SAML2).

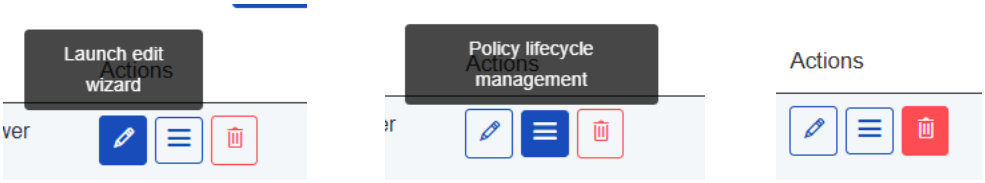



This page shows each policy's source, integration model, current status, and available actions.

Admins can also create new applications using out-of-the-box templates.

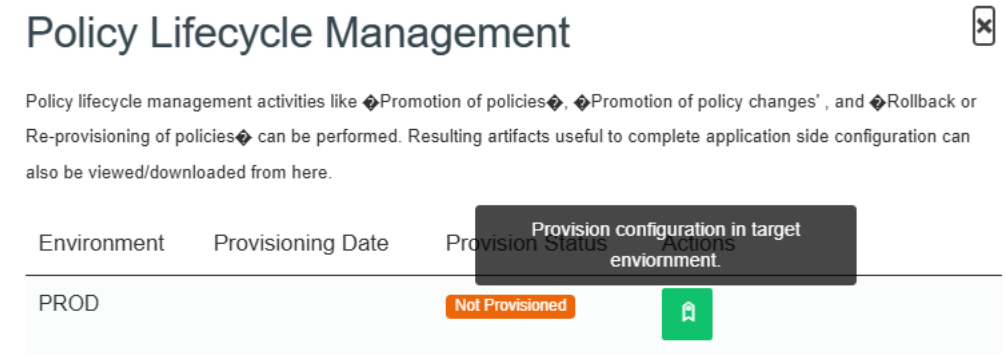



**Actions**: Edit Policy | Lifecycle Management | Delete Policy




**Policy provisioning**

After you complete the required policy updates, provision the policy to the target system. UnityX enforces promotion from lower environments to production environments.

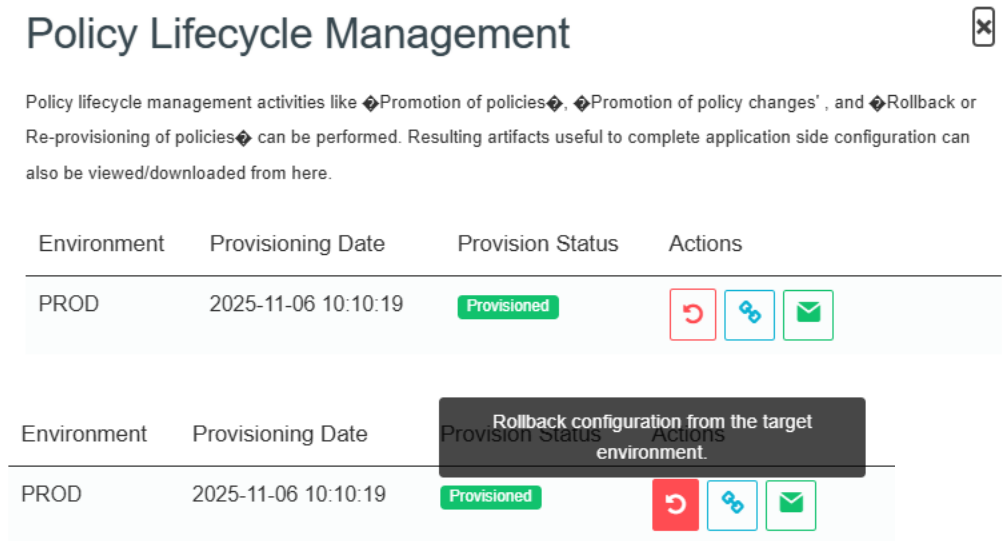



**Live policy actions**

Use **Rollback** to remove a provisioned policy when it is no longer required. This workflow rolls back all policy-related artifacts from the target system.

Use **Edit** to update a provisioned policy and then **Re-provision** to apply changes to the target system.

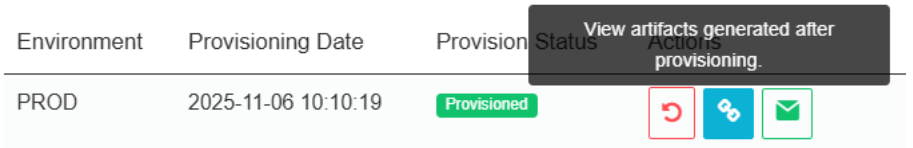
Use **Delete** to remove a policy from UnityX only if it is not provisioned to any target environment.



### Integration artifacts

Use **Integration Artifacts** to generate a PDF package for a policy. The package can include the policy details, metadata, IdP public certificate, and the client ID and client secret (as applicable).

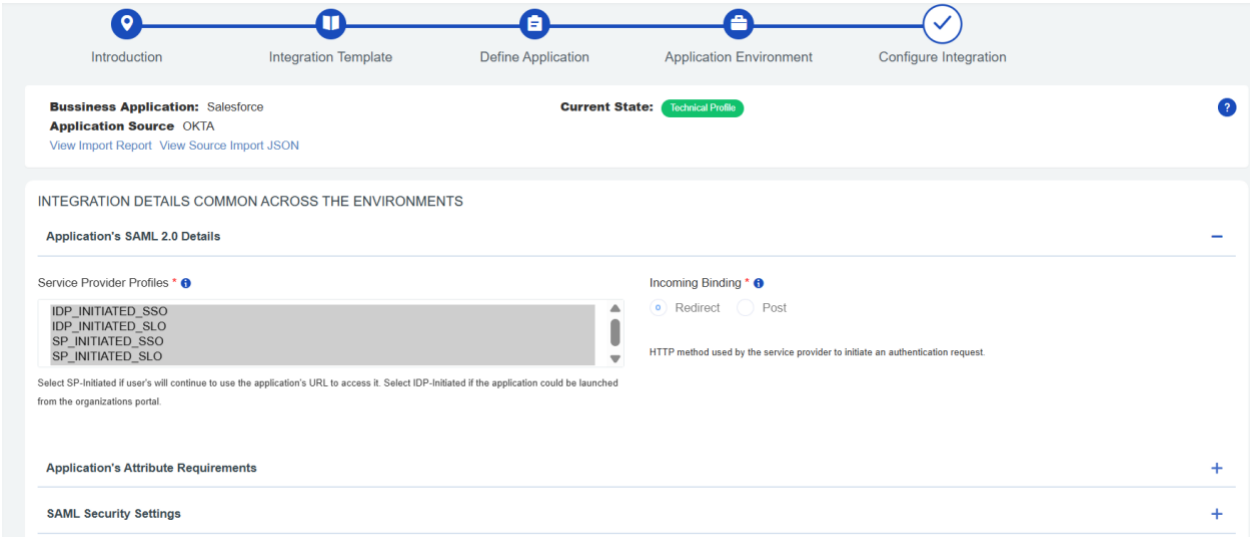
You can also email the artifacts directly to the application team distribution list (DL) configured in UnityX.

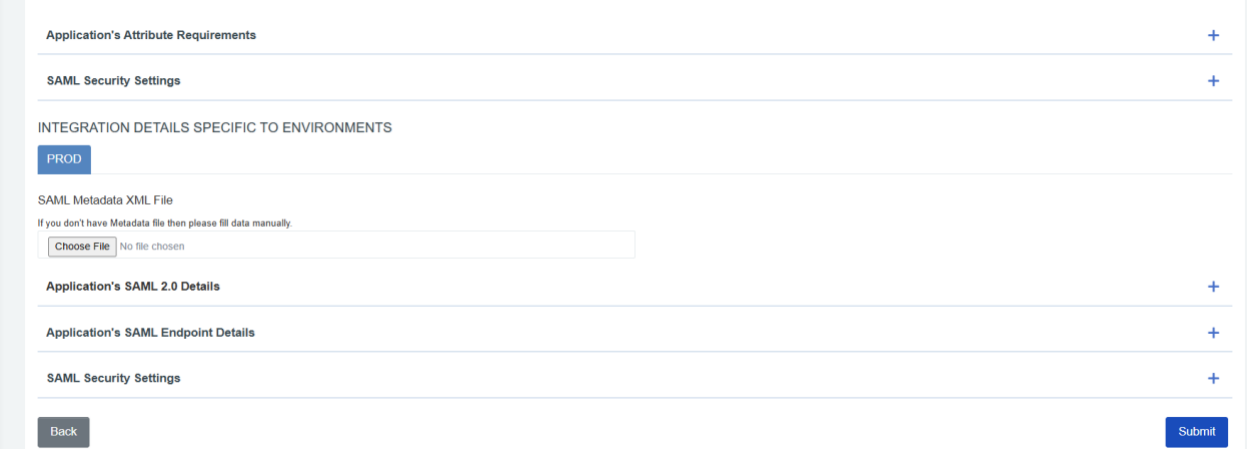




### SAML-based policy

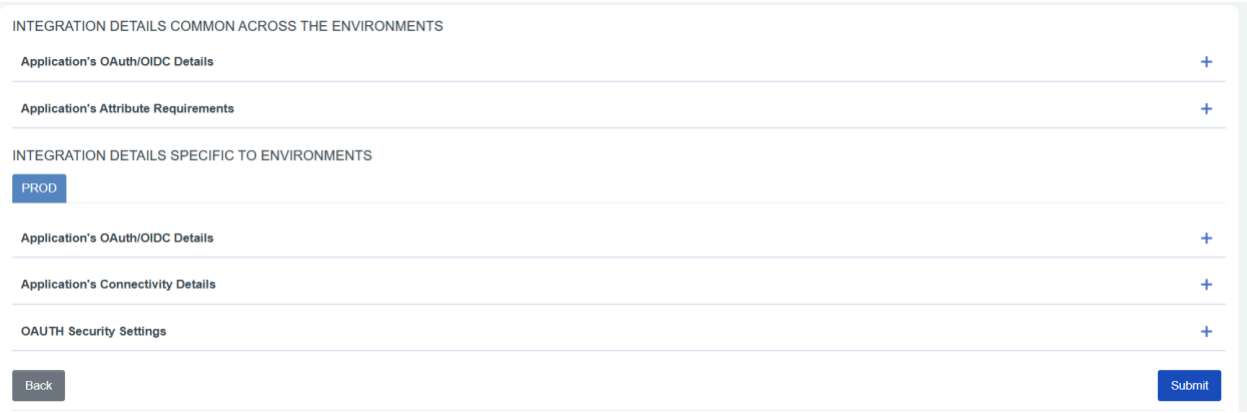
This page provides a detailed view of a SAML policy (read-only with editable sections as applicable). Information is organized into logical sections to simplify administration.





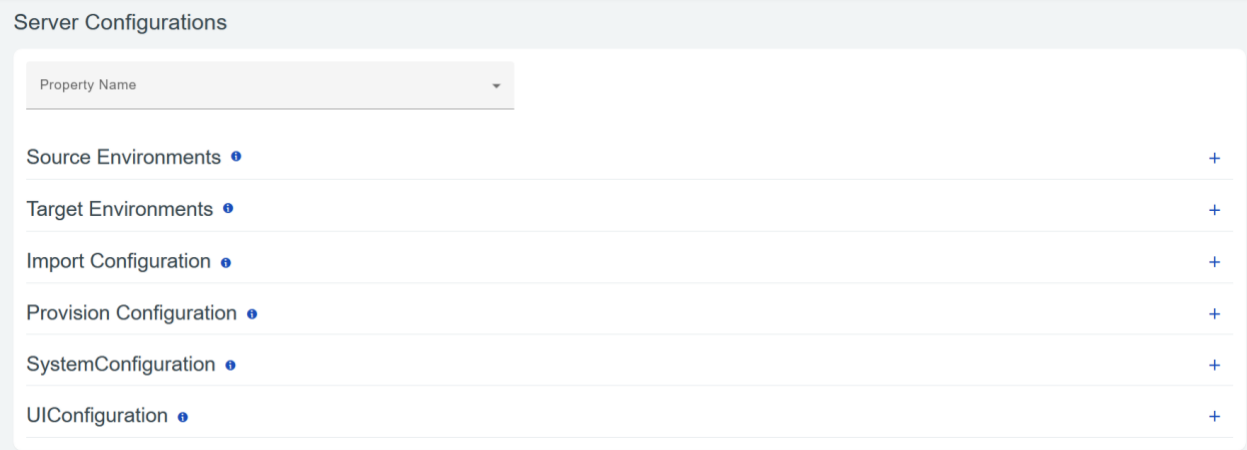

**OAuth / OIDC policy**

Similar to SAML, the OAuth/OIDC policy page displays all configured policy details for review and updates.



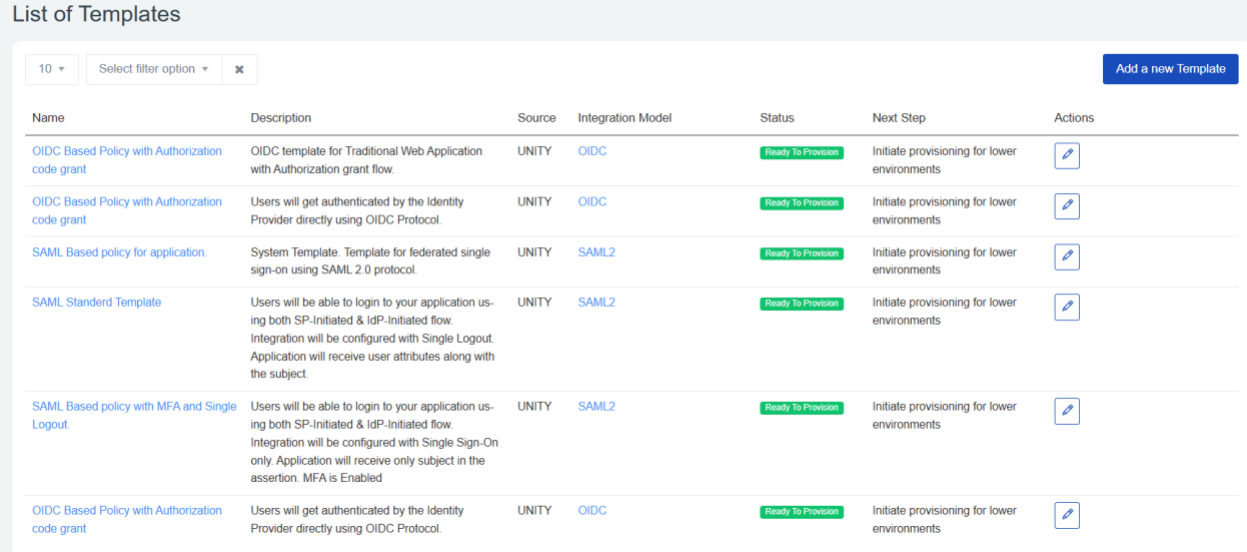

**UnityX configuration**

After installation, configure UnityX for your organization by setting up source and target environments, import settings, provisioning settings, and system/UI configuration. This is a critical setup step before you begin importing or provisioning policies.



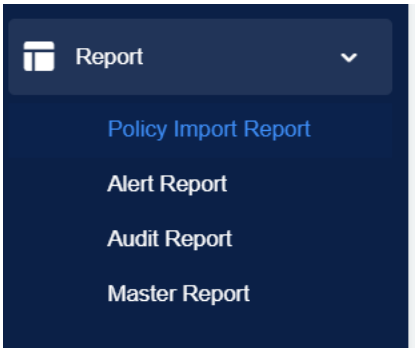

**Policy templates**

UnityX provides multiple out-of-the-box policy templates. Admins can also create custom templates based on organizational requirements.




**Reports**

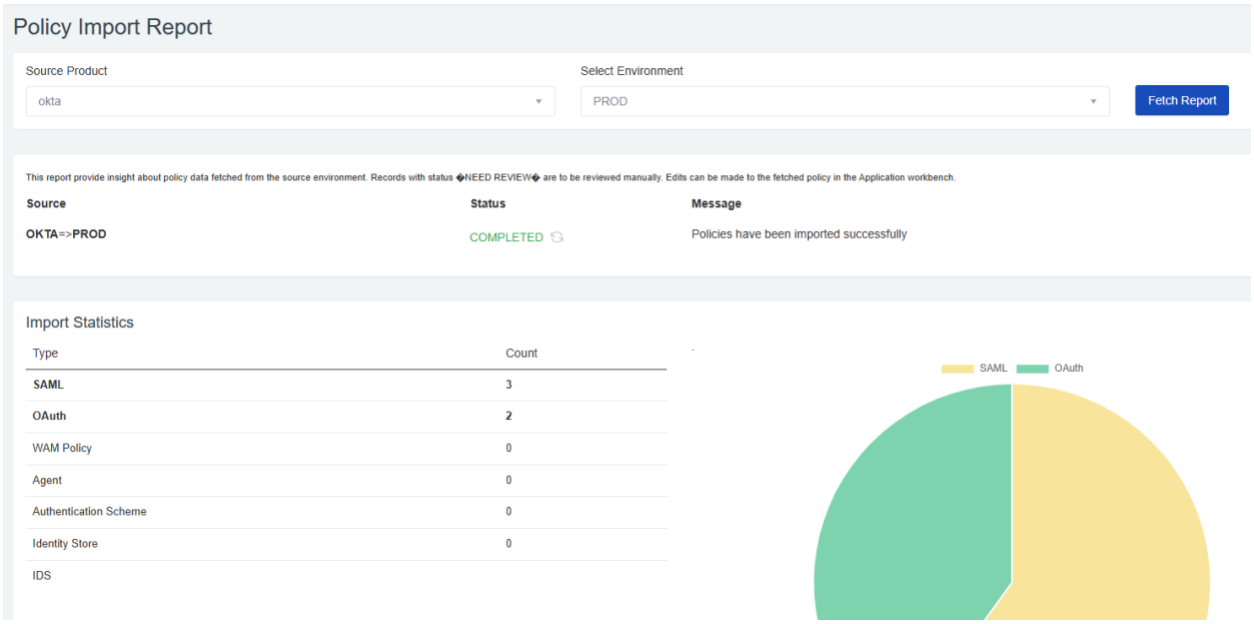
UnityX provides built-in reports, including the Policy Import Report and Audit and Alert reports.



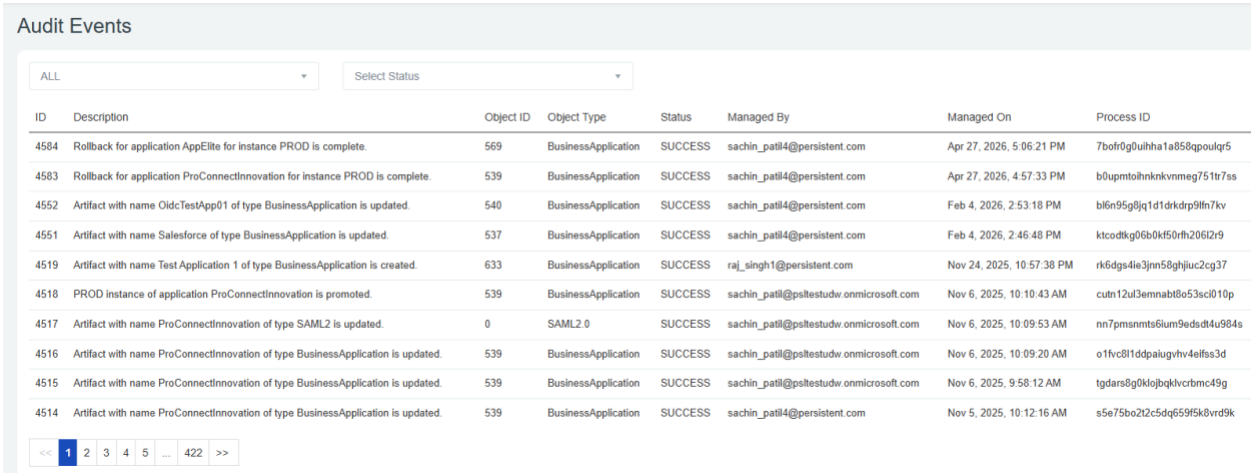

## Approvals


## Import report

The latest import report provides policy counts by type, current status, and the source system used for policy import.



## Audit Events:




| ID | Description | Object ID | Object Type | Status | Managed By | Managed On | Process ID |
|---|---|---|---|---|---|---|---|
| 4584 | Rollback for application AppElite for instance PROD is complete. | 569 | BusinessApplication | SUCCESS | sachin_patil4@persistent.com | Apr 27, 2026, 5:06:21 PM | 7bofr0g0uihha1a858qpoulqr5 |
| 4583 | Rollback for application ProConnectInnovation for instance PROD is complete. | 539 | BusinessApplication | SUCCESS | sachin_patil4@persistent.com | Apr 27, 2026, 4:57:33 PM | b0upmtoihnknkvnmeg751tr7ss |
| 4552 | Artifact with name OidcTestApp01 of type BusinessApplication is updated. | 540 | BusinessApplication | SUCCESS | sachin_patil4@persistent.com | Feb 4, 2026, 2:53:18 PM | bl6n95g8jq1d1drkdrp9lfn7kv |
| 4551 | Artifact with name Salesforce of type BusinessApplication is updated. | 537 | BusinessApplication | SUCCESS | sachin_patil4@persistent.com | Feb 4, 2026, 2:46:48 PM | ktcodtkg06b0kf50rfh206l2r9 |
| 4519 | Artifact with name Test Application 1 of type BusinessApplication is created. | 633 | BusinessApplication | SUCCESS | raj_singh1@persistent.com | Nov 24, 2025, 10:57:38 PM | rk6dgs4ie3jnn58ghjiuc2cg37 |
| 4518 | PROD instance of application ProConnectInnovation is promoted. | 539 | BusinessApplication | SUCCESS | sachin_patil@psltestudw.onmicrosoft.com | Nov 6, 2025, 10:10:43 AM | cutn12ul3emnabt8o53sci010p |
| 4517 | Artifact with name ProConnectInnovation of type SAML2 is updated. | 0 | SAML2.0 | SUCCESS | sachin_patil@psltestudw.onmicrosoft.com | Nov 6, 2025, 10:09:53 AM | nn7pmsnmts6ium9edsdt4u984s |
| 4516 | Artifact with name ProConnectInnovation of type BusinessApplication is updated. | 539 | BusinessApplication | SUCCESS | sachin_patil@psltestudw.onmicrosoft.com | Nov 6, 2025, 10:09:20 AM | o1fvc8l1ddpaiugvhv4eifss3d |
| 4515 | Artifact with name ProConnectInnovation of type BusinessApplication is updated. | 539 | BusinessApplication | SUCCESS | sachin_patil@psltestudw.onmicrosoft.com | Nov 6, 2025, 9:58:12 AM | tgdars8g0klojbqklvcrbmc49g |
| 4514 | Artifact with name ProConnectInnovation of type BusinessApplication is updated. | 539 | BusinessApplication | SUCCESS | sachin_patil4@persistent.com | Nov 5, 2025, 10:12:16 AM | s5e75bo2t2c5dq659f5k8vrd9k |

<< 1 2 3 4 5 ... 422 >>