Product Brief

THALES

CYBERSECURITY

Thales Authenticator Lifecycle Manager

Centralize and Simplify FIDO Deployment in Enterprise

SIMPLE • SCALABLE • SECURE

cpl.thalesgroup.com

THALES

CYBERSECURITY

Modern enterprises need secure, phishing-resistant authentication, but large-scale FIDO hardware deployments bring challenges—complex manual processes, high operational burden, security gaps, and user frustration. Thales Authenticator Lifecycle Manager is a SaaS platform built to solve these issues, letting you take control of the full lifecycle of every FIDO authenticator from deployment to revocation. By offering centralized control, enhanced visibility, and streamlined operations, our solution empowers organizations to confidently implement and scale their passwordless authentication strategy, ensuring both security and compliance without compromising user experience.

The Authentication Challenge

Rising Phishing Threats

Traditional MFA methods remain vulnerable to sophisticated phishing attacks, putting enterprise credentials at risk.

Password Fatigue

Legacy authentication creates user friction and security gaps, hampering productivity and compliance.

Security Gaps

Insufficient visibility and control over authentication devices leave organizations exposed to compliance failures.

Organizations need phishing-resistant authentication with FIDO2 security keys to eliminate password vulnerabilities and achieve passwordless security. However, managing FIDO authenticators at enterprise scale presents significant operational challenges that demand a comprehensive lifecycle management solution.

Key Enterprise Pain Points

Deployment & Provisioning

Distributing, enrolling, and configuring FIDO keys for thousands of employees across diverse locations is complex and time-consuming.

Lifecycle Management

Managing the entire lifecycle of FIDO keys, including activation, suspension, revocation, and replacement, lacks a centralized process.

Visibility & Reporting

Lack of real-time visibility into FIDO key status, usage, and inventory hinders audit readiness and security posture assessment.

Integration Complexity

Integrating FIDO key management with existing identity providers and applications often requires significant custom development.

The Thales Solution & Key Capabilities

Our cloud-based admin console provides comprehensive FIDO2 authenticator lifecycle management. Designed for IT, Security, and Helpdesk teams, it ensures effortless deployment, policy enforcement, and audit-ready operations.

Key Features

Centralized Dashboard

Assign, revoke and reset authenticators quickly across your organization.

On-Behalf FIDO Key Registration

Registration, assignment, revocation, bulk configuration, and inventory tracking.

Policy Enforcement

Apply consistent security rules (like PIN length) that persist through the entire authenticator lifecycle.

Integration with leading IDPs

Easily integrate with multiple existing Identity Providers to enable FIDO key registrations from a single management console.

Comprehensive Auditing

Maintain full audit trails for compliance and security reviews.

Integrated Identity providers

- Microsoft Entra ID
- Thales SafeNet Trusted Access

Supported Authenticators

- Thales SafeNet FIDO 2.1 authenticators Standard and Enterprise Edition

Key Benefits

Simplified FIDO deployment in Enterprise

- Streamlined FIDO deployment at scale.
- Faster FIDO adoption across the organization

Simplified Administration

- Fewer support tickets thanks to on-behalf FIDO key registration
- Fewer errors thanks to intuitive administration

Increased Security Posture

- Phishing-resistant MFA
- Strengthened security policies persistent throughout authenticator lifecycle.

Implementation & Deployment

The Thales Authenticator Lifecycle Manager is designed for flexible, scalable, and secure enterprise-wide implementation, ensuring full security and operational benefits.

Architecture

Our hybrid architecture combines a secure, **SaaS service** that gives you a cloud-based admin console with lightweight local windows service for centralized control and efficient operations.

- **Cloud-Based Admin Console:** A single, secure web interface for FIDO2 authenticator management, policy setting, and monitoring.
- **Local service:** For secure communication, device discovery and provisioning,

This scalable architecture supports growth from pilot programs to large global deployments, with end-to-end encrypted communication.

System Requirements

- **Admin Console:** Modern web browser with internet connectivity.
- **Local service:** Available on Windows with web socket communication between the admin console and the local service

Integration

The platform seamlessly integrates with your existing identity ecosystem

- Identity Providers (IdP): Pre-defined templates for Microsoft Entra ID, and SafeNet Trusted Access to fetch user information
- SAML 2.0 & OIDC Support: Standard protocol support for other IdP solutions.
- API Integration: Comprehensive API for custom integrations and automation with HR, ITSM, or other security tools.

Rollout Strategy

A successful rollout involves careful planning to ensure user adoption and minimal disruption.

- Pilot Program: Test with a small group, start with one type of FIDO key, refine processes and gather feedback.
- Phased Deployment: Gradually expand to departments, managing onboarding and addressing issues proactively.
- Best Practices: Define clear policies, communicate benefits, and leverage various form factors based on different user personas.

Next Steps

Ready to simplify FIDO authenticator management and accelerate your passwordless journey?

Request a Demo:

hub-cpl.thalesgroup.com/iam/thales-authenticator-lifecycle-manager

About Thales OneWelcome Identity & Access Management Solutions

Thales' digital identity products and solutions empower billions of people and things with digital identities worldwide. The Thales OneWelcome Identity & Access Management portfolio enables organizations to build frictionless, trusted and secure digital journeys for customers, business partners and employees. The OneWelcome Identity Platform provides a variety of capabilities from identity verification, single sign-on, passwordless and multi-factor authentication to fraud management, adaptive access, dynamic authorization and consent & preference management for the highest levels of assurance. More than 30,000 organizations trust us with their IAM and data security needs, enabling them to deliver secure digital services to their users.

About Thales

In today's digital landscape, organizations rely on Thales to protect what matters most - applications, data, identities, and software. Trusted globally, Thales safeguards organizations against cyber threats and secures sensitive information and all paths to it — in the cloud, data centers, and across networks. Thales offers platforms that reduce the risks and complexities of protecting applications, data, identities and software, all aimed at empowering organizations to operate securely in the digital landscape. By leveraging Thales's solutions, businesses can transition to the cloud with confidence, meet compliance requirements, optimize software usage, and deliver exceptional digital experiences to their users worldwide.