Brochure

Managing Identities & Access for your Business Ecosystem

Thales OneWelcome Identity Platform: The only true B2B IAM solution to streamline collaboration and enhance security

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Effective collaboration with business partners, vendors, and your supply chain is essential for the success of your business. As you provide them with portals to enhance this collaboration, the complexity of managing numerous identities and access permissions becomes apparent. Traditional identity management models are struggling to keep up with the demands of today's business. They often entail labor-intensive administrative processes, slow response times, and, inadvertently, introduce security vulnerabilities and user experience friction.

Recognizing Your B2B IAM Challenges

Onboarding and offboarding new business partners and effectively managing them within the context of their organizational structure, mirroring their organization's lifecycle, presents a significant complexity.

While delegating identity management to your business partners can reduce administrative burdens – they know their employees better than you – it introduces the challenge of ensuring they follow security best practices and maintain data integrity.

Managing users conventionally through individual user access assignment to a policy-based approach can be more efficient and offers better control. However, it requires careful planning and coordination to ensure that access is granted or revoked based on user attributes and roles.

Verifying users through tracking dynamic user attributes, such as certifications or clearances, and incorporating them into access control can be complicated and time-consuming.

Meeting compliance requirements, especially when dealing with external users, demands robust reporting and control mechanisms from your DPO and CISO to prevent fraud and penalties.

Making new apps and portals quickly available while maintaining security can be challenging, especially when developers need to leverage identity APIs and concentrate on business functionality without introducing vulnerabilities.

The B2B IAM User Groups

Ensuring seamless collaboration and data security across your network relies heavily on providing proper access and authorization for your B2B user groups, their employees, as well as potential applications and resources.

Business-to-Business collaboration can include a variety of users: Business customers, suppliers, supply chain manufacturing, co-engineering or projects, researchers, on-demand workforce and business outsourcing, temporary staff in the gig-economy, distribution channels with dealers, brokers, and shop-in-shop.

That's why you need a hybrid approach that accounts for your diverse B2B user groups.

The Thales OneWelcome Identity platform, equipped with cutting-edge B2B IAM capabilities, is the only IAM platform designed to explicitly address your challenges offering a swift deployment in just a few weeks. With our purpose-built, cloud-based B2B IAM solution you can cater to the full range of your B2B user groups – whether they are customers, suppliers, or anyone in between.

Furthermore, we understand the significant risk posed by incomplete offboarding processes within many organizations. Neglecting to revoke access for former employees can leave your organization vulnerable to breaches. Our solution addresses this challenge proactively.

With the Thales **OneWelcome Identity Platform**, you gain:

- **Organizational Structures:** Tailored access levels per department, business unit, or relationship to cater to the unique needs of your stakeholders and partners.
- **Precise Access Control:** Attribute and Role-based access to minimize the risk of unauthorized entry, enhancing security.
- **Mitigated Threat Impact:** Prevent potential threats by restricting unnecessary access, bolstering your defense mechanisms.
- **Efficient Collaboration:** Safely promote teamwork across internal teams, partners, and contractors for seamless project execution.
- **Compliance and Auditing:** Ensure regulatory compliance with meticulous tracking of user activities, giving you peace of mind.
- **SaaS Scalability:** Deploy an on-demand B2B IAM platform that scales effortlessly to meet your evolving business demands.

Using our Application Launchpad

Partners will be able to access a secure application launchpad for accessing business apps enabled for their role or organization. It provides a centralized and controlled gateway for employees to access various business applications, ensuring that sensitive data and systems are protected from unauthorized access and cyber threats. Here's a description of a typical secure application launchpad:

User Authentication and Authorization

Users must first authenticate themselves through a multi-factor authentication (MFA) process, which could include something they know (password), something they have (smart card or token), and something they are (biometric data like fingerprint or facial recognition). Once authenticated, the system verifies the user's authorization level and role to determine which applications they are allowed to access.

Single Sign-On (SSO)

The launchpad often offers SSO functionality, allowing users to access multiple applications with a single set of credentials. This enhances convenience and reduces the risk of password-related security breaches.

Application Catalog

Users are presented with an organized catalog of business applications that they have permission to use. This catalog may include web apps, desktop apps, and virtualized applications.

Access Control Policies

The launchpad enforces access control policies, ensuring that users can only access the applications and data they are authorized to view or modify.

Role-based access control (RBAC) is commonly used to determine which users can access which resources.

Integration with Identity and Access Management (IAM)

Integration with IAM systems ensures that user identities and permissions are consistently managed across the organization.

Compliance and Reporting

The launchpad assists organizations in meeting regulatory compliance requirements by collection consent, generating reports and providing data for compliance audits.

In summary, a secure application launchpad is a central hub that prioritizes security while simplifying and streamlining user access to business applications. It plays a pivotal role in protecting sensitive data, reducing the attack surface, and ensuring that only authorized personnel can access critical systems and information.

Why Thales?

Thales has a tradition and referenceable reputation in Digital Identity and Security. Thales' B2B IAM solution was designed from the ground up to cater to the full range of B2B user groups and drive business collaboration. Thales has a long history of serving industries with the highest security requirements. Security is in our DNA. This extends to our IAM solutions, where the world's leading brands place their trust in our expertise, backed by a dedicated team of over 15,000 specialists in the field and multiple references.

Let us explore how our approach can reinforce your identity management strategy and enhance your partner engagement procedures, ensuring your organization remains resilient and secure in an ever-changing digital landscape.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com