SafeNet Trusted Access and One Identity Manager (IGA) + One Identity Manager On Demand (IDaaS)

Protecting and streamlining your IAM environment

Securing your Corporate Resources

Organizations need to ensure that the right users gain access to the right resources, at the right time and for the right reasons. As corporate assets get more distributed and the workforce gets more mobile, enabling access and then governing access rights becomes more challenging, often creating gaping holes in security.

Access Management and Identity Governance and Administration: Better Together

Perimeter-based security has inherent limitations that make it obsolete for modern threats. Organizations require the right solutions to help them develop an identity-centric security posture. SafeNet Trusted Access combined with Identity Manager or Identity Manager On Demand gives organizations the ability to leverage identity as the new perimeter.

Identity Governance and Administration

As organizations grow, their identity ecosystem becomes more and more complex. This complexity poses operational and security challenges for IT and security & risk management teams. On-boarding employees and provisioning the right tools and applications for them at joining is crucial for a welcoming user experience for the newcomers, rather than drowning them in manual and time-consuming approval processes. Larger enterprises that want to enable internal mobility find it challenging to update users' access rights appropriate for their roles, and revoking access to

Highlights

- **Identity lifecycle**
  Identity management software that secures user access and automates provisioning to any target on-premises or in the cloud.
- **Governance**
  Single platform for governance for visibility to who has access to data and apps, when, how and why.
- **Attestation**
  Empower line-of-business personnel to approve or deny user and group access and entitlements.
- **Self-service access**
  Enable users to request entitlements and group access via a shopping-cart selection menu.
- **Compliance Reporting**
  Satisfy compliance regulations with user- and privileged-access reporting.

avoid security threats. And finally, employee exits need to be smooth, while ensuring that their access to different applications and data is revoked. Identity Manager handles all these complexity to ensure that the joiner, mover and leaver events are handled through automated processes; with a detailed record for timely audit.

Access Management

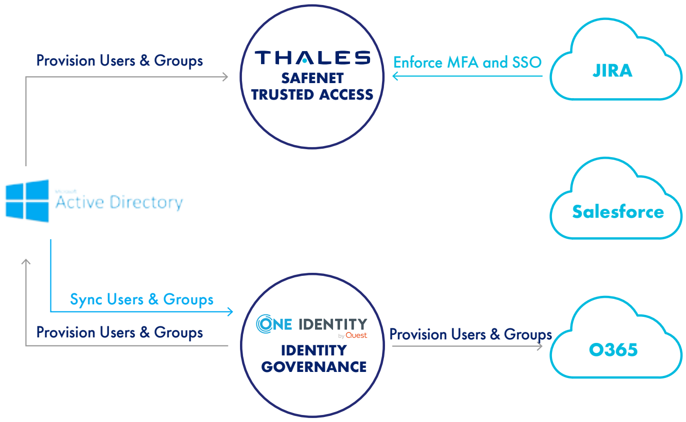
Based on user personas, organizations need to adjust the authentication journeys for their employees. A one-size-fits-all approach cannot be used for employees' access needs. IT and security teams require a flexible solution that allows them to implement flexible policies that adapt to the user needs and context. STA allows organizations to apply the right level of security at the time of access based on the user context and the nature of the application. Offering the broadest range of MFA capabilities, STA allows IT to choose the right authentication mechanism for the right use case.

Together, Identity Manager and STA allow organizations to implement a flexible and secure IAM framework from granting access rights to enforcing them. Whether your employees are working on-premises or remotely, One Identity and Thales ensure that the users have the right user experience in accessing applications that are crucial for their work; while ensuring that the IT, security and audit teams have peace of mind for their security and auditing needs. Perimeter-based security has inherent limitations that make it obsolete for modern threats. Organizations require the right solutions to help them develop an identity-centric security posture. SafeNet Trusted Access and Identity Manager and Identity Manager On Demand give organizations the ability to leverage identity as the new perimeter.

How the Joint Solution Works

STA and Identity Manager use a user directory, such as Active Directory, as a mechanism to sync user roles and groups. This allows both systems to work in tandem, with Identity Manager handling the identity governance and administration functions; and SafeNet Trusted Access handling the MFA, SSO and access management policies.

Additionally, users can leverage STA to enable MFA while signing in to Identity Manager. Depending on access policies defined in STA, users can be asked to use a second factor such as a smart card, mobile authenticator app (MobilePass+), OTP token or a soft token such as Gridsure.



Key Benefits

- Satisfy compliance and audit requirements
- Deploy an identity Zero Trust model
- Extend governance to cloud apps
- Unify policies to reduce risk exposure
- Lower operational costs
- Enhance user experience

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Their Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.com.

About Thales Access Management

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web, and cloud-based applications with a Zero Trust approach. Utilizing policy-based conditional access, rigorous SSO, and universal authentication methods, enterprises can effectively prevent breaches, migrate securely to the cloud and simplify regulatory compliance.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.