thalescpl.com

THALES

Access Management Handbook

Contents

An Introduction

Over the years, you may have heard a lot about access management. In fact, we tended to use the terms “authentication” and “access management” pretty much to mean the same thing. But in fact there are differences between the two. While authentication validates a user’s identity, access management determines that a user has the permission to access a certain resource and enforces the access policy that has been set up for that resource.

Access management is very important when it comes to managing access to cloud resources. Nowadays, a person typically has to access numerous cloud apps throughout the day. This is a hassle for both users and IT: Users have to remember countless passwords; while IT need to endlessly reset forgotten passwords. The solution to this problem is SSO: By having one credential for all cloud apps, users can easily login once to several apps while IT saves precious time over password resets.

Since that single identity is only as secure as the authentication used to verify it, the method of verifying users’ identities becomes paramount to maintaining cloud access security. To this end, access management solutions and single-sign on solution offer granular control over the access policies defined per application. By requiring an additional authentication factor in high risk situations, a frictionless user experience is maintained.

Glossary of Access Management Terms

Authentication and Access Management

Authentication and Access Management solutions are composed of Identity Governance and Administration (IGA) functionality and Access Management (AM) functionality. IAM solutions provide a methodic framework for granting (and requesting) access to applications (IGA),

enforcing access controls (AM) and ensuring visibility into access events (AM). Given that most organizations deploy the IGA and AM components separately of each other, these disciplines are being increasingly evaluated as distinct, standalone solution families, rather than as composite functionalities of a single Authentication and Access Management suite

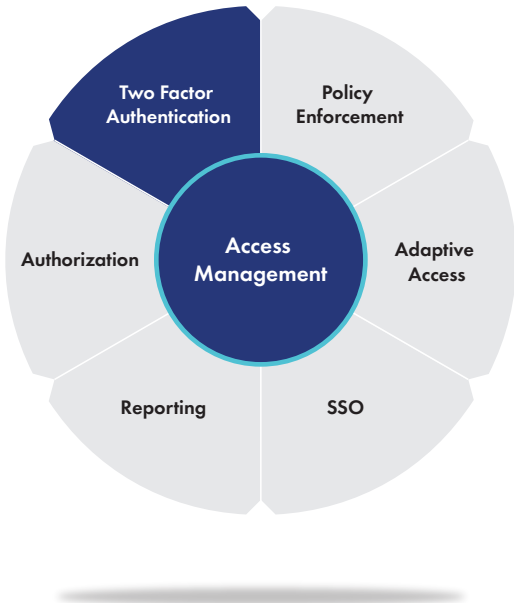
Access Management

Access management is a functionality that enables determining whether a user has permission to access a certain resource, and enables the enforcement of the access policy that has been set up for that resource.

Access management is implemented based on access policies that are defined by IT administrators and include such information as which groups of users (e.g. Sales, R&D, HR) are allowed access to which cloud applications (e.g. Salesforce, Office 365, Jira, Taleo), as well as the set of user attributes required to access each application (e.g. trusted network, password, OTP).

The access policy can require more or less user attributes to be assessed depending on the sensitivity of a cloud application. These attributes are assessed using risk-based or context-based authentication, which is central to enforcing the different access policies defined for each cloud application. (For more details, see context-based authentication.)

Also central to cloud access management is single sign-on, which enables the use of a single username-and-password set or 'identity' to log in to all one's cloud applications. (For more details, see single sign-on.)

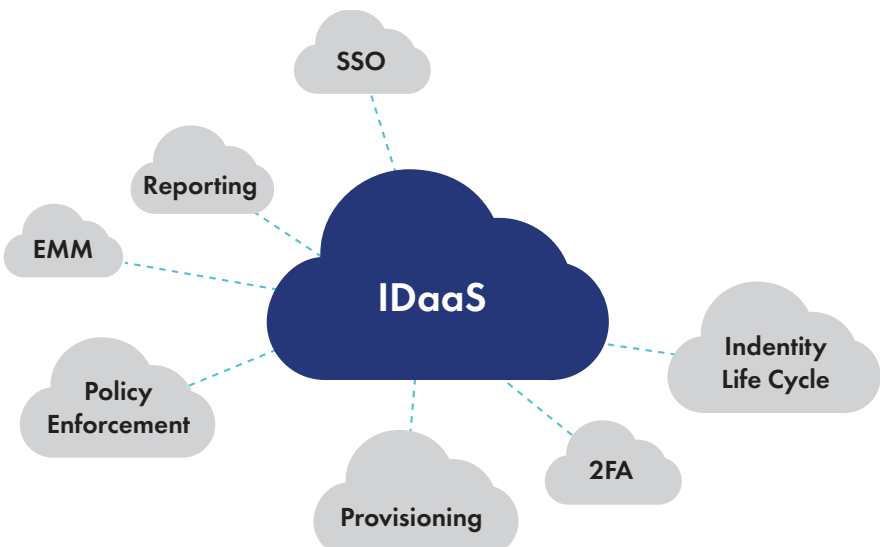


IDaaS

IDaaS stands for IAM-as-a-Service, also called identity-as-a-service, to describe Identity and Access Management (IAM) solutions that offer a cloud-based as-a-service delivery model for Access Management and Authentication. While IDaaS has been reviewed as a separate market in recent years, given recent market trends, going forward it will be treated as two separate disciplines—that of Access Management and IGA, whose delivery methods include on-premises installations, software or cloud-based platforms.

Identity Governance and Administration (IGA)

Identity Governance and Administration (IGA) solutions help answer the questions, "Who should receive access, or who is 'entitled access,' to which application?" and "Who in practice was granted access to which application, by whom and when." For example, an IGA solution may help establish that R&D staff are entitled access to certain development applications, such as GitHub, Jira and Confluence. An IGA solution can automatically provision access to these applications, based on their R&D group membership. The R&D user may also request to be provisioned access to other applications, a request which would then go through a management approval process that is supported by some IGA solutions.



Identity Federation

With identity federation, a single system called a trusted Identity Provider ("IdP") governs the authentication of users, with cloud apps relaying the authentication process to the Identity Provider each time a user attempts to access them. Federated identity solves the challenges and frustrations of managing credentials for numerous web apps separately, whether internal or external to an organization. Identity federation relies on federation protocols such as SAML and Open ID Connect, as well as proprietary protocols such as Microsoft's WS-Federation.

Federated Login

Federated login is a function of federation protocols, such as SAML, Open ID Connect and others, which use an Identity Provider model to authenticate users and relay that authentication information to the target system in the form of an "authentication assertion." The assertion contains an 'accept' or 'reject' response, resulting in the user being denied or granted access.

Federated login allows users to sign in once in order to concurrently gain access to all their cloud applications. Instead of logging in to separate cloud applications using different username-and-password sets, or "identities," federated login lets users log in to office 365, Salesforce, AWS etc. with the same identity they use to log in to the corporate network in the morning, or the VPN at night.

With identity federation, a single system called a trusted Identity Provider governs the authentication of users, with cloud apps relaying the authentication process to the Identity Provider each time a user attempts to access them.

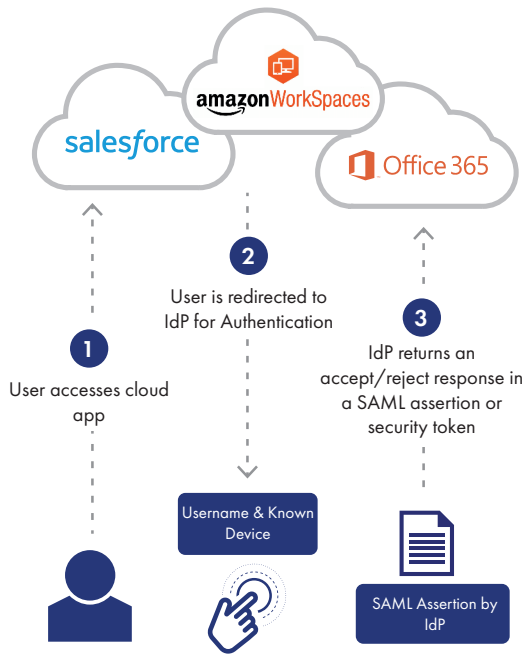
Identity Provider

SAML, and other identity federation protocols which enable the safe exchange of identity data between unaffiliated websites, are based on an Identity Provider (IdP) and Service Provider model. When a user accesses a Service Provider (cloud-based service), they are redirected to the trusted Identity Provider for authentication and/or authorization data. The Identity Provider verifies the user's authentication data (e.g. user's cookie, device, network, OTP) and produces an "accept" or "reject" response which is then sent to the Service Provider. Authorization data may include the permission to access such information as email addresses from a webmail account or names of friends from a social network account.

For example, SafeNet Trusted Access acts as an identity provider when users access cloud applications as in the scenario described above.

Security Token Services

Identity Provider models are also called Token-based Authentication, or Security Token Services. A Security Token Service (STS), is equivalent to an Identity Provider, and a Relying Party (RP) is equivalent to a Service Provider. And instead of exchanging SAML assertions, these are called Security Tokens. Different names, same concept.

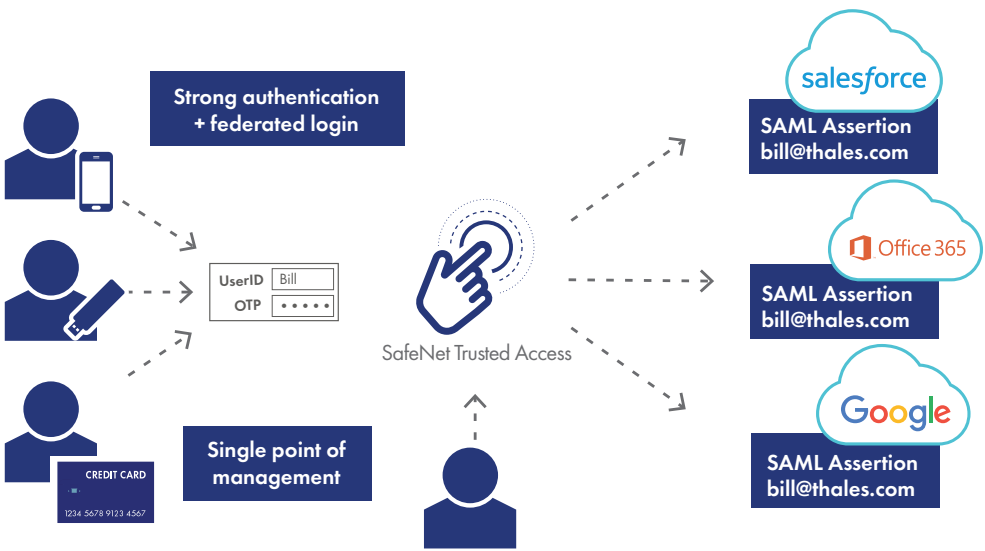


SAML

SAML, pronounced 'sammel,' stands for Security Assertion Markup Language, which is an XML-based open standard for exchanging authentication data between unaffiliated websites, a capability also called identity federation or federated authentication. Identity federation means the ability to extend users' current enterprise identities to the cloud, enabling them to log in to their cloud applications with their current enterprise identity. Federated authentication to cloud apps with SAML allows users to log in to all their cloud applications with their current enterprise identity, so that instead of maintaining 5 or 25 username-and-password sets, they can maintain just one.

How SAML Works

When a user attempts to log in to a cloud-based application, they are redirected to a trusted Identity Provider for authentication. The Identity Provider collects the user's credentials, for example, their username and one-time-password, and it returns a response to the cloud application being accessed. This response is called a SAML assertion, and the SAML assertion contains an accept or reject response. Based on this response, the Service Provider, e.g. Salesforce, Office 365 or DropBox, blocks or grants access to the application.



WS-Fed

WS-Federation Services, or WS-Fed, is Microsoft's proprietary identity federation protocol. WS-Fed works with Microsoft's Active Directory Federation Services, or AD FS, to extend identities stored in Active Directory to Microsoft cloud applications such as Office 365 and Azure. Like SAML, WS-Fed users an Identity Provider model. When accessing a Microsoft cloud application, the user is redirected for authentication to AD FS, based on whose response the cloud application grants or denies the user access.

OAuth

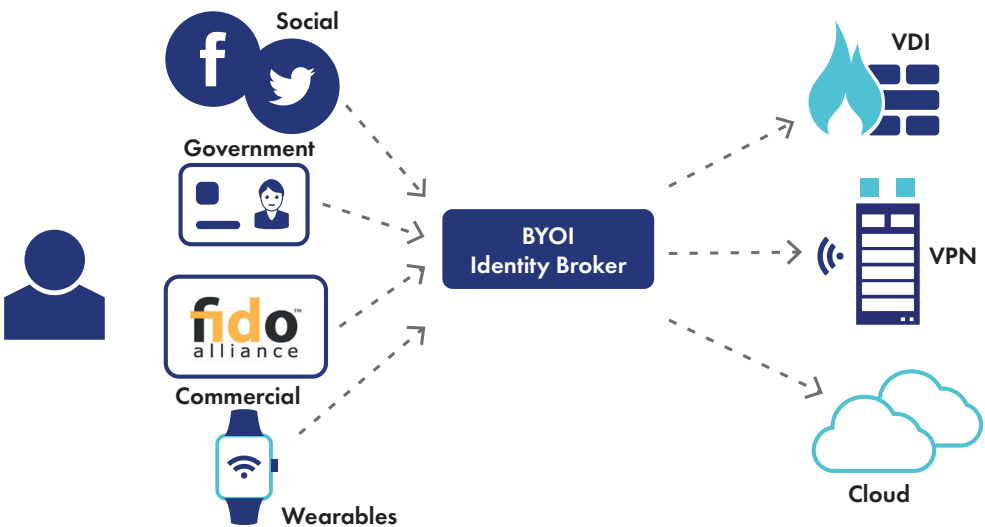
OAuth, pronounced “oh-auth,” stands for Open Authorization, and it is an open standard for federated, or ‘token-based’ authentication and authorization between unaffiliated websites. As with other identity federation protocols, such as SAML, Open ID Connect and WS-Fed, OAuth enables logging into an application with an identity that is verified by a trusted identity provider. OAuth goes beyond federated authentication to enable users to authorize relying party websites to access certain account information such as contact names and email addresses. For example, OAuth is the protocol used by social network websites to access your webmail contacts and ask you if you’d like to invite your webmail contacts into your social networks.

Open ID Connect

Like SAML, OpenID Connect is an open standard identity federation protocol that uses an Identity Provider model. However, unlike SAML, which works using a cookie and therefore only works with applications that open in a browser ('browser-based applications'), OpenID Connect provides a single-sign on framework that enables the implementation of single sign-on across browser-based applications, native mobile apps and desktop clients (such as rich clients and some VPNs). So while most single sign-on implementations today support only cloud and browser-based apps, as more identity providers adopt OpenID Connect, we'll be able to authenticate just once in order to concurrently gain access to all our resources - be they desktop clients, browser-based applications or native mobile apps.

Bring Your Own Identity (BYOI)

In the identity management space, vendors and organizations are looking to enable employees and partners to use their own identity to access corporate resources. This identity could theoretically be any identity that provides a sufficient level of identity assurance – for example, government-issued identity cards, healthcare smart cards, as well as online identities, such as social identities, professional network identities and commercially-available identities such as FIDO. The enterprise and consumer worlds are merging closer together, with enterprise security teams under increasing pressure to implement the same type of authentication methods typically seen in consumer services.



Single Sign-On (SSO)

Single sign-on (SSO) provides the capability to authenticate once, and be subsequently and automatically authenticated when accessing various resources. It eliminates the need to separately log in and authenticate to individual applications and systems, essentially serving as an intermediary between the user and target applications. Behind the scenes, target applications and systems still maintain their own credential stores and present sign-on prompts to the user's system. SSO responds to those prompts and maps the credentials to a single login/password pair. (Source: Gartner)

SSO, whether in a standalone solution or a broader access management solution, can be achieved through a range of identity federation protocols. These include open-source protocols such as SAML 2.0 and Open ID Connect, proprietary protocols such as Microsoft's WS-Federation, and other technologies such as password vaulting and reverse proxies.

Password Vault

Password vaults, also called password managers, are a simple way to create a single sign on (SSO) experience when a target application does not support identity federation protocols, for example, a legacy or custom application. Password vaults are systems that work by storing and encrypting the passwords of different websites. Instead of logging to each application with a dedicated password, the user can simply authenticate with a master password (which in turn decrypts the password vault), eliminating the need to maintain disparate passwords.

Authorization

Authorization is a process that ensures that properly authenticated users can access only the resources which they are allowed to access, as defined by the owner or administrator of that resource. In the consumer world, Authorization may also refer to the process whereby a user ensures that a cloud-based application (for example, a social network) accesses only certain information from a non-affiliated website (for example, the user's webmail account).

Authentication

Authentication is a process in which a user's identity is validated or verified based on the the credentials that the user provides when logging in to an application, service, computer or digital environment. Most authentication credentials consist of something the user has, for example a username, and something the user knows, for example a password. If the credentials provided by the user, match those that are stored by the underlying application or Identity Provider, the user is successfully authenticated and granted access.

Context-based Authentication

Context-based authentication verifies the identity of users by assessing a range of supplemental information at the time a person logs into an application. The most common type of contextual information include a user's location, time of day, IP address, type of device, URL and application reputation. Context-based authentication, also called risk-based or adaptive authentication, is central to the world of SSO and access management where the objective is to make the authentication journey as transparent and painless as possible.

By assessing a user's login attributes, be they contextual (device, role, location) or behavior based (e.g. typing speed, page view sequence), single sign on and access management solutions can continuously match the level of authentication required from the user with the access policy defined for each application. In this way, authentication is applied granularly—in the most frictionless manner possible—per an application's access policy, rather than as a blanket, uniform rule for all enterprise resources.

Continuous Authentication

With a token, a password or a fingerprint – authentication is basically a yes / no decision: The system validates a user's identity and either allows or denies them access to an application.

But thanks to newer technologies, such as context-based authentication or behavioral biometrics (for example, typing pattern and other physical traits), authentication can become a more continuous process. By assessing a range of attributes such as IP address, mobile parameters, known device, operating system etcetera, contextual or risk based authentication can continuously verify a person's identity each time they log into an application. In fact, it can do so without the user even knowing.

Contextual authentication offers many frictionless ways of verifying a person's identity. And this is really what allows us to balance user convenience with the ability to apply granular access controls for numerous cloud applications. And this is why the concept of continuous authentication—which is based on context-based authentication—is a foundation of cloud access management.

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalescpl.com <