Evidian

Web Access Manager and Office 365

With more and more businesses hosting applications externally, –Software as a Service (SaaS) subscriptions gradually overruns licenses-based software delivery model.

This trend towards the cloud has prevailed with a global growth of the cloud infrastructure services market by more than 30% per year according to several analysts.

COVID-19 impacts are also accelerating this phenomenon, especially considering remote working's wider application.

This model offers a greater agility to organizations which can react faster and more efficiently. In addition, the use of "as a Service" applications allows them to anticipate, smooth and sometimes defer expenses.

However, this paradigm shift broadens the security perimeter of organizations, for which it is necessary to adopt a strict access control posture, which includes the following elements:

- Offer a strong authentication strategy to remove or limit password use
- Reduce the complexity and integrate seamlessly the access and management to both worlds
- Increase the users' productivity by giving easy access to the best-in-class SaaS application portfolio at the right time.
- Enable a User Identity lifecycle, compatible with on premises applications and Cloud applications, for employees, contractors or customers
- Decrease the cost of unused licenses and optimize application related expenses
- Deploy an active governance process at the center of all application accesses, and establish a compliance plan.

Evidian Web Access Manager (WAM) is an Identity Provider and Service Provider

Authentication & security

Context-Aware Authentication or Adaptive authentication is the basic mechanism for determining the risk of the user's session before his authentication. The right secure authentication policy is triggered depending on the user's context.

Single Sign-On

Authentication is a burden for users. Internal applications, from SaaS applications, to Web applications or Mobile applications authentications are required everywhere. Removing intelligently this burden increases security and the productivity.

Self-Service

By letting your users reset their own passwords, enroll stronger authentication methods, and deploy their SaaS or on premise accounts whenever they request them or need them, you can drastically cut your costs.

Facilitates compliance

Quickly list the access rights to your information system your authenticated users own. Easily obtain the report of IT resource access rights for all your listed users.

Learn how Evidian Web Access Manager (WAM) allows you to meet these challenges

Increase the security without impacting users

The major international SaaS vendors are also major security researchers and innovators, therefore security byconstruction is at the core of their offers. But as often, people remain the weakest link in the SaaS security chain. Using your same usual password anywhere, trusting any web server, from your professional trusted applications to your less trustable personal applications, exposes you and your enterprise to security breaches.

Fortunately, SaaS vendors fully understand how passwords can be a risk for the enterprise. It would be nonsensical to let users access professional SaaS applications without giving the real owner – the enterprise – the tools to address the who, when and how, of applications access. Enterprises must deploy their own Identity Providers and Identity Governance and Access management. Wherever users come from, internal or external network, at any time, the enterprise manages its assets through federation mechanisms.

Atos

Business Oriented – Ready to use

Adaptive and multi-level Authentication

Passwords are forgotten, and even worse, they are corrupted. Only strong, long, complex and hard to remember passwords can resist. Fortunately there is no reason to use them anymore. Multi-factors, multi-level authentication, using tokens, OTP, or QR code crypto-keys can effectively replace them in any situation. Identification and authentication now rely on what you know and what you own. If you do not use your usual device, additional authentication steps are triggered: it is the Context-Aware Authentication or Adaptive Authentication. Your geo-location, your device, your access time, your IP are used to compute a risk before opening sessions that will define the minimal level of the required authentication method. This level will let you choose an authentication method accordingly to the authentication means you own. It is a more convenient way in a heterogeneous population of users (employees, partners, customers) to provide different authentication means, and, for instance, to consider that an intranet Kerberos authentication has the same level as a twofactor authentication from an Internet partner. Evidian Web Access Manager supports all kinds of authentications from simple credential authentication to multistep multi-factor, with browser fingerprinting and Context-Aware Authentication. WAMprovides many off-the-shelf authentication means. It provides a simple configuration tool for combining them as multi-factormulti-step authentication methods. If built-in methods are not strong enough for your needs, WAM is also able to use on-premise external authentication services or SaaS authentication servers like Gemalto-SafeNet Authentication Service.

Single Sign On

With only one single login, give access to all your applications, even when they use different identities or credentials. You can also disconnect all applications with the click of a single button. Your internal Web applications still use login/password? Never mind, Web Access Manager will keep them secure without exposing them to the user's browser. No need to modify the protected application, Evidian WAM will turn any application into a service provider and will play the application authentication cinematic. SaaS applications and internal Web applications will be reached seamlessly, without any additional authentication step by the users. One single login opens securely the doors to all allowed applications, powering up the user's productivity and reducing help-desk costs.

Self-Services

The shift to SaaS forces changes how users access and consume IT applications — meaning our heuristics and best practices must evolve. Web Access Manager gives users complete autonomy for resetting passwords, activating authentication means, enrolling phones and stronger authentication methods, filling secondary accounts, editing profiles, requesting access rights — using IGA — , ... WAM provides simple, customizable Welcome pages, and easy integration points in your own custom welcome portal. Once again, you will reduce your help-desk costs.

Cost-Efficient SaaS Provisioning

Dormant accounts are a risk for on premise IT. When part of your IT is distributed in the Cloud, in SaaS applications, dormant accounts are not only risky but they also generate additional costs: welcome to the shadow IT. Without Access Governance, it is very difficult to identify these accounts among active accounts. Decreasing the number of unused licenses is one of the key objectives of the IT cost reduction when moving to SaaS. Cost efficient SaaS provisioning is an exclusive Evidian feature that provisions the SaaS accounts at the exact time users need to access SaaS applications, for the first time.

With Office365

A practical use case of this is Office365. Creating federated users, provisioning accounts, bulk-importing CSV identity files, assigning licenses, syncing directories, and writing endless power-shell command lines, are usually the first steps of the Office365 move. It can be made simpler and cheaper with WAM and IGA, by using the Cost- Efficient provisioning and access management. When a user tries to access Office365, he is redirected to your Identity Provider; WAM, which issues a strong context-aware authentication. Once authenticated, if the user is granted access to Office365, IGA will dynamically create the federated identity in Office365, and will request WAM to authorize the access for this user and his newly federated identity. An Office365 license will be assigned to this new user. Users have an instant access to their Office365 accounts, with strong adaptive authentication, Single Sign-On across all

other applications of your on-premise IT, and Self-service to request the rights to use applications. When a user loses his right to use Office365, as defined by your policy, IGA will transparently unprovision the SaaS account and will release the unused license. No more expensive dormant accounts. IT administrators may generate reports about use, identify active accounts, handle the policy and role management, deploy approval workflows, and let approvers validate the user's self-service requests. WAM manages the access of Office365 Web applications, Mobile applications and Desktop applications. All your Office365application accesses are managed by your own Identity Provider applying your own policy rules with optimized costs.

- WAM: Web Access Manager 9 Evolution 2: WAM may be used separately or in association with IGA. Visit www.evidian.com for more details about WAM features.
- IGA: Identity Governance and Administration 10: IGA may be used separately or in association with WAM or other products. Visit www.evidian.com for more details about IGA features.
- Cost-efficient provisioning initiated by Identity Provider, is protected by the Patent WO2015173517. This feature requires WAM and IGA.

Request a demonstration of WAM with Office365 and Cost-Efficient Provisioning at www.evidian.com or self-create an account on **https://iam-portal2.evidian.com**

PowerPoint 2016 Office365 on Mac OSX.

The default Context-Aware Authentication panel proposed by WAM as Identity Provider.

For more information: **www.evidian.com**

Atos, the Atos logo, Atos|Syntel, and Unify are registered trademarks of the Atos group. © Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.