

From: Wood, Caroline

Sent: 2/19/2020 12:41:23 PM

To: TTAB EFiling

CC:

Subject: U.S. Trademark Application Serial No. 88210547 - ACCESS MANAGEMENT - 569.336 - Request for Reconsideration Denied - Return to TTAB - Message 9 of 12

Attachment Information:

Count: 12

Files: a8-2.jpg, a8-3.jpg, a8-4.jpg, a9-1.jpg, a9-2.jpg, a9-3.jpg, a9-4.jpg, a9-5.jpg, a11-1.jpg, a11-2.jpg, a11-3.jpg, a12-01.jpg

By using or further navigating this website, you agree to Omada's use of cookies. [Click here](#) to see our cookie policy.

Close

[Read Privacy Policy](#)

30% of employees leaving the enterprise typically do not have all access rights removed promptly
Enterprise-wide transparency of access rights is unavailable
'Least privilege' principle is often not implemented
Monitoring toxic combinations of accumulated access rights is difficult
Failure to control separation of duty (SoD) may lead to fraud and financial losses
Complex and insecure authentication of users for password resets

Identity Management System

Omada Identity Suite is an identity and access management solution that



By using or further navigating this website, you agree to Omada's use of cookies. [Click here](#) to see our cookie policy.

Close

[Read Privacy Policy](#)

reduces the need for custom development, decreasing deployment time, so ROI is achieved fast.

The solution offers end-to-end user provisioning and access management. Key functionality of our identity management system includes:

- ✓ Identity lifecycle management
- ✓ Provisioning
- ✓ Self-service processes
- ✓ Password management
- ✓ Approval workflows
- ✓ Segregation of duties (SoD)
- ✓ Role management
- ✓ Audit reporting.



What is identity and access management?

By using or further navigating this website, you agree to Omada's use of cookies. [Click here](#) to see our cookie policy.

Close

[Read Privacy Policy](#)

Managing identity and access is a complex task that is essential for ensuring that only authorized users have access to.

By using Omada Identity Suite, permissions can be granted manually and automatically, depending on the user's assigned role in the company. Using Omada software to prevent data and information breaches, complying with domestic and international legislation is easier than ever.

Learn more about the essential identity management functionality of Omada Identity Suite:

[Learn more](#)

By using or further navigating this website, you agree to Omada's use of cookies. [Click here](#) to see our cookie policy.

Close

[Read Privacy Policy](#)



Security

Improve your IT security and manage access across all systems.



Compliance

Ensure Compliance with built-in automated access rights policies.



Efficiency

Automate processes, boost efficiency, and enable your business.

access across all systems

[Learn more](#)

automated access rights policies

[Learn more](#)

enable your business

[Learn more](#)

By using or further navigating this website, you agree to Omada's use of cookies. [Click here](#) to see our cookie policy.
[Read Privacy Policy](#)

[Close](#)

Download: Omada Identity Suite - Solution Overview

[Download](#)

[See office locations](#)



Crown
Commercial
Service
Supplier

By using or further navigating this website, you agree to Omada's use of cookies. [Click here](#) to see our cookie policy.
[Read Privacy Policy](#)

[Close](#)

Solution

Omada Identity Suite
Overview
Cloud Delivered IGA

Resources

Solution Sheet
EU GDPR Guide
Cases

Company

Career
Contact
Omada Partner Program

Legal

Privacy Policy
Disclaimer

By using or further navigating this website, you agree to Omada's use of cookies. [Click here](#) to see our cookie policy.
[Read Privacy Policy](#)

[Close](#)

[Skip to main content](#)



Become a BizTech Insider | Sign up today to receive premium content! [Sign Up](#)

To stay ahead of your storage,
you need Dell Technologies™ and
IT Orchestration by CDW™

[LEARN MORE](#)



BizTech

INDUSTRIES ▾ TOPICS ▾ STATES TIPS & TACTICS VOICES FEATURES VIDEO IT

[LOG IN](#)

SEP
07
2019

SECURITY

3 Reasons to Deploy an Identity

Latest Articles



Big Tax Deductions For Tech
Purchases

Identity and Access Management Solution

Providing users with secure access can be challenging, but identity and access management solutions deliver improved security, as well as cost and time savings.

by BizTech Staff

▶ LISTEN 04:26

Users demand quick and easy access to systems and information whether they're located in the office, at home or on the road.

Most organizations recognize the need for this access but realize they must balance user demands against difficult security requirements. Cybercriminals know that organizations must support remote users and attempt to exploit enterprise identity systems through the use of social engineering attacks that allow them to **compromise the credentials of legitimate users and gain access to enterprise systems**. In recent years, social engineering has grown into an increasingly common and effective attack vector.

The **demand for secure access poses a serious challenge** to IT professionals. The IT team must simultaneously meet the needs of a diverse landscape of users across numerous, disparate applications. Many scenarios arise on a daily basis that require modifications to access permissions. New users are hired and need their access provisioned quickly during their onboarding process. At the same time, current users leave an organization as part of planned retirements or sudden terminations, and they must have their access revoked. Other users change roles within an enterprise because of transfers and promotions and need their access rights updated to reflect their new positions, while removing the permissions they no longer require.

Meeting these demands across a variety of on-premises and cloud applications requires the use of agile and flexible identity and access management solutions. Identity and access management (IAM) products must be able to handle access rights for many different categories of individuals who are using a variety of devices to access different types of data and workloads. Access control systems must be able to integrate with a wide variety of existing and future information systems, allowing users access to the information they need, wherever it is stored.



Making The Most Of Mobile Collaboration



A Good Security Story Can Make All The Difference

Is Perimeter-Based Network Security Dead?



SOFTWARE

Computer Clean Up: What Is Bloatware, and How to Get Rid of It



Adding to the complexity of the modern identity and access management challenge, business data now exists far beyond the traditional network perimeter. While firewalls and intrusion prevention systems continue to play an important role in network security, **organizations cannot depend on them to protect sensitive information** that exists outside the traditional network perimeter. The risks of cloud computing and mobile devices are that these technologies spread data across a much broader area and increase the challenge of protecting access to an organization's information.

What Is IAM, and Why Is It Important?

Identity and access management is the information security discipline that allows users access to appropriate technology resources, at the right time. It incorporates three major concepts: identification, authentication and authorization. Together, these three processes combine to ensure that specified users have the access they need to do their jobs, while unauthorized users are kept away from sensitive resources and information.

When a user attempts to access a system or data, he or she first makes a claim of identity, typically by entering a username into the system. The system must then verify this claim of identity through an authentication process. Authentication may use basic knowledge-based techniques, such as passwords, or rely upon advanced technologies, such as biometric and tokenbased authentication. Once a user successfully completes the authentication process, the IAM system must then verify the user's authorization to perform the requested activity. **The fact that a user proves his or her identity is not sufficient to gain access** — the system must also ensure that users perform actions only within their scope of authority.

Without a centralized approach to IAM, IT professionals must manage authentication and authorization across a large number of increasingly heterogeneous technology environments. These environments support many different business functions, some customer-facing and some meeting internal requirements. To work effectively in such an environment, the security professionals managing IAM solutions must understand not only business operations but also the ways that access to IT systems enables those operations.

Effective IAM solutions help enterprises facilitate secure, efficient access to technology resources across these diverse systems, while delivering a number of important benefits:

Improved data security: Consolidating authentication and authorization functionality on a single platform provides IT professionals with a consistent method for managing user access. When a user leaves an organization, IT administrators may revoke their access in the centralized IAM solution with the



DIGITAL WORKSPACE

6 Steps to a Successful Migration to a New Workplace Collaboration Tool

ADVERTISEMENT

To elevate your office, you need VARIDESK® and IT Orchestration by CDW®.



VARIDESK
NEW DESK

PEOPLE
BUY
GET IT

Trending Now



Digital Transformation Starts In The Data Center

In The Cloud, IT Teams Remain Responsible For Performance

confidence that this revocation will immediately take effect across all of the technology platforms integrated with that IAM platform.

Reduced security costs: Using a single IAM platform to manage all user access allows administrators to perform their work more efficiently. A security team may have some additional upfront work integrating new systems into an IAM platform but may then dedicate time to the management of that platform, saving time and money.

More effective access to resources: When users receive access through a centralized platform, they benefit from the use of single sign-on (SSO) technology that limits the number of interactions they have with security systems and increases the likelihood that their legitimate attempts to access resources will succeed.

These three benefits combine to demonstrate the importance of centralized identity and access management to the modern enterprise.

Learn more about IAM solutions by downloading the white paper, "IAM: Overcoming the Authentication Challenge."

PX300ZTHN3STOCK



**Get More Insights Delivered
Right to Your Inbox.**

[Sign Up Now →](#)

More On [SECURITY](#) [IDENTITY MANAGEMENT](#) [IDENTITY MANAGEMENT](#)

Related Articles





Security

A Good Security Story Can Make All the Difference

Security

Is Perimeter-Based Network Security Dead?

Security

How to Mitigate Cyber-Risk While Empowering a Modern Workforce

BizTech

Technology Solutions That Drive Business

[About Us](#) [Contact Us](#) [Privacy](#) [Terms & Conditions](#) [Site Map](#)

BIZTECH:

CDW:

VISIT SOME OF OUR OTHER TECHNOLOGY WEBSITES:

EdTech **FedTech** **StateTech** **HealthTech**



Get BizTech in your Inbox

[Browse Email Archives](#)





Subscribe to BizTech Magazine


[Browse Magazine Archives](#)




[BACK TO TOP](#)





Ask "What cloud developer tools do you" 

 View Accounts

Try Oracle Cloud Free Tier


Oracle Fusion Middleware / Identity Management /

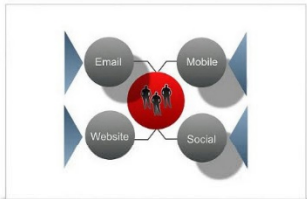
Oracle Access Management

Comprehensive Access Management for Applications, Data, and Web Services





Delivers risk-aware end-to-end user authentication, single sign-on, and authorization protection, enabling enterprises to secure access from mobile devices and seamlessly integrate social identities with applications.

Download Oracle Identity Management 12c and 11g

 [Data Sheet \(PDF\)](#)



Oracle Access Management enables you to provide a secure anytime, anywhere experience.



Overview

Features

Resources

- Seamless single sign-on to any application from any device
- Lower helpdesk-related support costs and

- Context-aware, real-time, adaptive security policies enhanced user productivity
- Real-time external authorization based on XACML, ABAC, and RBAC for a broad variety of platforms and environments
- Accelerated application lifecycle and simplified evolution of fine-grained security policies for applications, middleware, and databases
- Risk-based authentication and proactive real-time fraud prevention
- Standards-based identity propagation across vendors, customers, partners, and social networks
- Context aware computing—automatically collect, propagate, and leverage identity and device context for personalization and authorization across web, web services, and application tiers

[See all features and benefits](#)



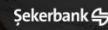
Oracle Adaptive Access Manager Ensured Secure Internet Banking with Oracle

The Video Cloud video is not playable.

Error Code: VIDEO_CLOUD_ERR_NOT_PLAYABLE
Session ID: 2020-02-19-1824324483367755af2af525 Player Element ID: vclid-7755af2af525-483679

“Oracle met our timeframe and exceeded our expectations. The fraud management system is easy to manage and has received good feedback from our customers.”

—Sansal Nuray, senior officer,
ŞekerBank



OK

Related Products

Oracle Identity Governance

Oracle Directory Services

Oracle Enterprise Single Sign-On

Oracle API Gateway

Get Started

Contact Sales

Resources for

Developers

Startups

Students and Educators

Partners

Oracle PartnerNetwork

Find a Partner

Log in to OPN

Emerging Technologies

Artificial Intelligence

Internet of Things (IoT)

More Solutions

How We Operate

Corporate Security Practices

Doing Business with Oracle

Oracle@Oracle

Contact Us

US Sales: +1.800.633.0738

Global Contacts

Subscribe to emails

Country/Region

© 2020 Oracle

Site Map

Privacy / Do Not Sell My Info

Cookie Preferences

Ad Choices

Careers

12 Best Access Management Software & Tools

If you want to make sure that users on the network have access to the right tools and want to have appropriate restrictions in place, there is nothing more powerful than access management software. We'll show you the best tools available in 2020.



STEPHEN COOPER

@VPN_News UPDATED: January 14, 2020



What is access management?

Access Management (AM), also known as Identity and Access Management (IAM), is the practice of ensuring people in an organization have appropriate access to technology.

Popular Posts

- 10 Best Network Monitoring Tools & Software of 2020**
March 18, 2019 / by Tim Henry
- 11 Best Free TFTP Servers for Windows, Linux and Mac**
February 28, 2019 / by John Kovalick
- The 19 Best Free SFTP and FTPS Servers for Windows and Linux**
February 21, 2019 / by John Kovalick
- NetFlow - Ultimate Guide to NetFlow and NetFlow Analyzers**
January 23, 2019 / by John Kovalick
- Best Bandwidth Monitoring Tools - Free Tools to Analyze Network Traffic Usage**
December 21, 2018 / by John Kovalick

