ORACLE MANAGED CLOUD SERVICES - STRONG AUTHENTICATION SERVICE

Enterprises need to address a growing number of security threats targeting their cloud based applications, and meet various compliance requirements, and at the same time be able to provide easy access to legitimate users.

Oracle Managed Cloud Services - Strong Authentication Service provides Managed Cloud Services customers with a cost effective, managed, multi-factor authentication service to protect their managed cloud application environments against unauthorized access, deliver real-time web fraud detection and prevention, and enable compliance with strong authentication requirements.

Overview

The type of strong authentication solution that is a de-facto security standard for online banking, financial services, and healthcare portals is now available as a managed service for Managed Cloud Services customers. Powered by Oracle Adaptive Access Manager and Oracle Access Manager, the Oracle Managed Cloud Services - Strong Authentication Service provides web fraud protection and a multi-factor authentication solution for companies seeking to protect the confidentiality and integrity of sensitive data they make available via the cloud.

With nothing to install on the customer network or client machine, and nothing additional to carry, the Strong Authentication Service offers rapid deployment, ease of use and a low cost to support end-user authentication. The Strong Authentication Service is available for Oracle web applications that are certified for integration with Oracle Access Manager and are managed by Oracle Managed Cloud Services.

Real Time Identity Protection and Fraud Prevention

Oracle Managed Cloud Services - Strong Authentication Service allows customers to select between Two Factor (user and device), Three Factor (user, device, location), and Four Factor (user, device, location, behavior pattern/risk score) authenticated access to their protected applications. Use of personalized images, phrases and timestamps on login screens helps thwart phishing attacks. Use of virtual authentication devices allows customers to effectively combat threats from keystroke loggers in real time.

Virtual authentication devices are 100% server based features, provided without any client-side software or logic, and thereby, offering protection against password theft by keystroke loggers, click-loggers or other malicious software.

Unique technology used by the service enables device fingerprinting every time a user attempts to authenticate to access a protected application. Information about the device is compared with the user’s profile and history. This information can then be used to take action such as issuing a security challenge question if the user has logged in from a new device.

The service is effective in protecting against social engineering, various malware, and web application exploits. Risk based policies are used to evaluate in real time, the risk profile of a given authentication transaction. This is done utilizing a combination of parameters, such as
the number of previously failed login attempts, whether the user has used the device before, the user’s IP address or location and behavioral factors. Depending on the risk-based rules configuration and the risk score, the service may permit or block access to the applications, trigger alerts, or challenge a user with a Knowledge Base Authentication (KBA) Challenge Question.

Access to the user-friendly, service dashboard provides customers’ security analysts and helpdesk analysts with real-time metrics, activity information, case management and security/forensic investigations.

**Rapid Deployment and Ease of Use of a Managed Service**

Customers of the Oracle Managed Cloud Services - Strong Authentication Service benefit from implementation support provided as part of the service. Detailed analysis of the your security and functional requirements are translated into the configuration of service policies/alerts and actions.

You can select from hundreds of built-in policies and KBA challenge questions. You can also specify KBA answer rules, such as minimum length for answers, answer uniqueness and the degree of leniency allowed in answer matches to account for typos.

Oracle Managed Cloud Services - Strong Authentication Service, powered by Oracle Adaptive Access Manager and Oracle Access Manager, does not require installation or management of any hardware or software on your network. No client software needs to be installed on the end-users’ computers. No key fobs, smart cards or card readers need to be used. Application users find it easy and intuitive to access protected applications. The implementation service also includes assistance with the development of training materials for end users and your helpdesk analysts.

Using predefined rule sets, KBA challenge questions and answer validation rules allows rapid deployment of Oracle Managed Cloud Services - Strong Authentication Service with the certified applications. Use of third party implementation or consulting services is not necessary.

**Conclusion**

As companies aggressively embrace the cloud for sales, self-service, profile management and many other functions, online cloud based security is an increasing urgency.

Consumers need to be well protected while using the web and other channels to access sensitive data and transactions, and compliance mandates exist to ensure that companies respond.

In addition, as organizations are aiming to enable online access for their partners and mobile employees, they are facing a strong need to better protect their Internet environments and to proactively manage risks associated with remote access to critical business applications.

To address the growing security expectations for both consumer-facing and partner/employee-facing environments, Oracle Managed Cloud Services - Strong Authentication Service, powered by Oracle Adaptive Access Manager and Oracle Access Manager, provides secure, yet flexible protection for businesses and their end users by strengthening login processes, providing risk-based challenge methods and harnessing real-time fraud prevention/detection strategies.

**Contact Us**

For more information about Oracle Managed Cloud Services –Strong Authentication Service, visit oracle.com/managedcloudservices or call +1.800.ORACLE1 to speak to an Oracle representative.
 Oracle is committed to developing practices and products that help protect the environment.

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Hardware and Software, Engineered to Work Together