RSA ADAPTIVE FEDERATION
Identity Federation as a Service

ESSENTIALS

Secure access to SaaS applications
- Federated Single Sign-On (FSSO) for both identity provider (IdP) and service provider (SP) models
- Fine-grained, centralized access controls
- RSA SecurID® integration for two-factor authentication

Lower identity-federation costs
- Cloud-based federation service reduces deployment and operating costs
- Leverages your existing MS Active Directory infrastructure
- Third-party IdP support to leverage existing enterprise infrastructure

Increase user productivity and satisfaction
- Easy, one-click, on-demand user access

FEDERATED SSO TO SaaS APPLICATIONS

As use of Software as a Service (SaaS) applications increases, organizations require strong and transparent identity-access controls in the cloud. Secure authentication and authorization assure that the right users have the right access, right now, to business-critical resources and sensitive data.

RSA® Adaptive Federation enables secure and convenient access from the cloud, increasing IT agility and end-user productivity for faster delivery of new products and services. This cloud-based solution also lowers deployment and operating expenses.

To align access controls with your standard security policies, RSA Adaptive Federation provides easy-to-use, federated single sign-on (FSSO) to cloud-based applications. A user portal controlled by centralized access policies increases the security, control, and accountability of access to information in the cloud.

SIMPLE AND SECURE DEPLOYMENT FROM THE CLOUD

Deployment is fast and easy. As a cloud-based service, RSA Adaptive Federation provides flexible, scalable support without additional hardware, software, agents, or data stores. In addition, existing user credentials can be extended securely to the cloud without leaving your enterprise.

ANYWHERE, ANYTIME USER ACCESS

With RSA Adaptive Federation, users get easy, on-demand FSSO access to cloud applications whenever needed, increasing their productivity and simplifying their overall experience. The product also lowers security risks; reduces help desk calls for reset, lost, and weak passwords; and lowers cost of ownership of SaaS applications.

A centralized application catalog delivers users a single view of all cloud applications to which a user is entitled. Users simply select pre-populated applications for a self-
service experience that reduces IT costs and simplifies the experience.

**MOBILITY CONVENIENCE**

Because they increasingly use cloud applications both inside and outside the organization, employees must maintain many credentials. RSA Adaptive Federation eliminates the need for employees to remember sign-on credentials for each cloud application. Employees are also finding more efficient ways to work by leveraging mobile devices such as tablets and Smartphones. With RSA Adaptive Federation, employees can safely use any browser-enabled mobile device for access to and interaction with cloud applications.

**MULTI-FACTOR AUTHENTICATION**

RSA Adaptive Federation directly integrates with and securely authenticates to existing Microsoft Active Directory services without externally exposing user credentials. For step-up authentication, RSA Adaptive Federation also integrates with the world’s leading two-factor authentication, RSA SecurID®.

With RSA Adaptive Federation, users get easy, on-demand FSSO access to cloud applications whenever needed, increasing their productivity and simplifying their overall experience.

**EFFECTIVE POLICY MANAGEMENT**

RSA Adaptive Federation gives administrators granular policy control, including the ability to easily define access by users, groups, and roles. Administrators can then specify which users have access to which applications and generate application-usage reports to improve audit and license management. With a click, administrators can also remove a user's application access.
SECURE ADMINISTRATION
Via a central, multi-tenant console, administrators can manage user identities and access to applications, as well as policies and reporting. RSA Adaptive Federation also enables separation of duties via delegated administration, supporting roles that provide granular access such as managing users, organizations, and applications. The administrator console is a "super administrator" able to create, manage, and report on tenant end-user computing.

JUST-IN-TIME USER PROVISIONING
RSA Adaptive Federation supports just-in-time provisioning of user credentials. Administrators can automatically provision user credentials to cloud-based applications through a centralized web portal. Unauthorized users can be quickly and easily removed to reduce IT discovery and risk.

LEVERAGE EXISTING ENTERPRISE INFRASTRUCTURE
RSA Adaptive Federation can connect to on-premise, enterprise-based Microsoft Active Directory, allowing administrators to extend, but not externally expose, user profiles outside the firewall. The service comes with an enterprise connector, an on-premise virtual appliance which centralizes authentication and authorization and facilitates communication without changing or disrupting existing directory architectures. RSA Adaptive Federation provides an intuitive deployment template for quick access to cloud-based applications.

CLOUD ARCHITECTURE
STANDARDS-BASED
RSA Adaptive Federation supports industry standard OAuth 2.0, SAML 1.1, SAML 2.0, and WS-Fed 1.2, enabling easy integration with popular SaaS applications.

HOSTED DATA CENTER
RSA Adaptive Federation is a hosted service that resides in high availability/disaster recovery, load-balanced, secure, SAS 70 Type II-compliant data centers. A Network Operations Center monitors physical and digital performance and security 24x7x365.
PRODUCT SPECIFICATIONS

WEB BROWSER

- Windows XP - Internet Explorer 8; Firefox; Safari 5; Chrome
- Windows Vista - Internet Explorer 8 and 9; Firefox
- Windows 7 – Internet Explorer 8 and 9; Firefox; Safari 5; Chrome
- Mac OS X through 10.7 – Firefox; Safari 5; Chrome

MOBILE BROWSER

- Google Chrome
- Apple Safari
- Internet Explorer

ENTERPRISE CONNECTOR (VIRTUAL APPLIANCE)

- Hypervisor compatibility: vSphere 4.0 and later
- Minimum Hardware Requirements for the Server
  - Processor: 1 Intel Xeon Dual Core, 3.0GHz, 4MB cache
  - Memory: 4GB DDR2 667MHz, ECC registered
  - On-board LAN: One10/100 /1000 Base-TX ports
  - Storage: 15GB
- Recommended Resource Requirements
  - Memory: 2GB RAM
  - Processor: 1vCPU
  - Storage: 15GB (recommended 20GB)
- Network Configuration Settings
  - Inbound firewall port (443) opened from RSA Adaptive Federation Service to Connector Appliance
  - Also note that the Connector Appliance needs to have the following ports opened to Active Directory: typically ports 389 and 636.

SUPPORTED IDENTITY STORES

- LDAP compliant identity stores
- RSA Adaptive Directory 6.0

CONTACT US

To learn more about how RSA products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

www.EMC.com/rsa

EMC2, EMC, the EMC logo, RSA, the RSA logo, and SecurID are registered trademarks or trademarks of EMC Corporation in the United States and other countries. © Copyright 2012 EMC Corporation. All rights reserved. Published in the USA. 07/12 Data Sheet H10932
EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.