SOLUTION BRIEF

RSA External Authentication Method (EAM) for Microsoft Entra ID

Reduce risk and accelerate Zero Trust with RSA and Microsoft

Security teams using Microsoft Entra ID often seek additional capabilities to enhance their protection, simplify compliance, and extend coverage across all organizational resources, particularly in highly regulated and complex environments.
Using Microsoft's External Authentication Methods (EAM), RSA® ID Plus integrates RSA identity security capabilities directly into existing Microsoft setups. This helps organizations maximize their investment in Microsoft while benefiting from deep RSA expertise in secure access, covering everything from desktops to data centers.

Understanding EAM

EAM allows organizations to create an additional security layer from RSA ID Plus to protect their Microsoft resources. EAM helps satisfy multi-factor authentication (MFA) needs for various Microsoft policies, including conditional access, risk-based conditions, Privileged Identity Management (PIM), and applications requiring MFA. Unlike federation methods, which manage user identities externally, EAM keeps identity management centralized within Microsoft Entra ID. *(Note: A Microsoft Entra ID P1 license or higher is required to use EAM.)*

Why organizations choose RSA ID Plus EAM

Enhanced security

RSA EAM provides reliable and flexible identity security, keeping your Microsoft environment protected even as your needs evolve. RSA complements Microsoft's security capabilities with trusted methods that proactively reduce risk:

- The RSA Authenticator App for iOS and Android devices provides convenient, secure access.
- In air-gapped environments or BYOD scenarios, where installing company apps isn’t an option, RSA hardware authenticators, such as the RSA iShield Key 2 Series or DS100, deliver phishing-resistant authentication and comprehensive protection for every user.

Protecting Microsoft GCC High environments

For government contractors and organizations handling sensitive information, achieving compliance with Microsoft GCC High standards is crucial. The RSA EAM integration meets these stringent requirements while maintaining flexibility for users accessing Azure and Office environments from non-GCC endpoints.

“A transformative solution” for CNA

“We have been able to successfully authenticate using our RSA tokens to our Azure environment now…so far this looks like a transformative solution for us, and will allow us to provide much more flexibility for users accessing our Azure/Office environment from non-CNA endpoints.”

Brandon Hoffman
Deputy Director, Cloud Solutions & Systems, CIO, CNA

Increased resilience

Protect your business operations and maintain continuity by using RSA ID Plus Hybrid Failover across all your Microsoft Entra ID resources in cloud, hybrid, and on-premises environments. RSA and Microsoft together ensure comprehensive security coverage and disaster recovery readiness.

Expanded coverage

RSA identity security capabilities can extend beyond Microsoft to cover your entire IT landscape, including non-Microsoft solutions and legacy systems. This unified approach ensures consistent security management across your entire organization.

RSA and Microsoft: Layered security

Microsoft updates can change defaults and configuration settings, which can inadvertently introduce risk. By using RSA EAM, organizations can maintain their security settings with predictable, transparent security operations that:

- Ensure predictable security defaults and configurations, minimizing the risk of unexpected changes common in Microsoft environments.
- Add an extra validation step that prevents users from being redirected to phishing sites after authentication, offering built-in phishing-resistant safeguards.
- Provide a separate, robust authentication layer to reduce the risk of a single point of compromise and enhance the resilience of the entire identity infrastructure.

Compliance

RSA simplifies compliance with clear and auditable identity processes aligned with standards such as CMMC, DORA, and NIS2. This approach helps ensure that regulatory requirements are met and security audits are streamlined.

RSA + Microsoft: United by Zero Trust

RSA and Microsoft together help reduce organizational risk and develop Zero Trust maturity with:

- **Enhanced security**: Flexible security approaches that organizations trust.
- **Increased resilience**: Effective business continuity and disaster recovery capabilities.
- **Expanded coverage**: Comprehensive identity protection across Microsoft, non-Microsoft, and legacy systems.

Bill Gates with an RSA authenticator at RSA Conference in 2006.

A proven partnership

RSA and Microsoft have a strong, 20-year history of joint innovation and collaboration, specifically highlighted by RSA serving as a launch partner for Microsoft's External Authentication Methods. This ongoing partnership continues to provide organizations with secure, reliable, and advanced identity solutions.

Fortify your Microsoft environment with RSA

Contact us to see how RSA capabilities can complement Microsoft environments with additional security solutions.

About RSA

RSA provides mission-critical cybersecurity solutions that protect the world's most security-sensitive organizations. The RSA Unified Identity Platform provides true passwordless identity security, risk-based access, automated identity intelligence, and comprehensive identity governance across cloud, hybrid, and on-premises environments. More than 9,000 high-security organizations trust RSA to manage more than 60 million identities, detect threats, secure access, and enable compliance. For additional information, visit our website to contact sales, find a partner, or learn more about RSA.