

RSA ID Plus for Government

FedRAMP-authorized authentication

As federal agencies and public sector organizations move to the cloud and work to meet new Zero Trust directives and adopt technologies like FIDO2, RSA is committed to supporting their journey with industry-leading security solutions.

The FedRAMP-authorized RSA® ID Plus for Government identity and access management (IAM) solution provides the core capabilities that government agencies need to secure and accelerate the use of cloud services within a Zero Trust framework.

RSA ID Plus for Government helps US government agencies and Federal Systems Integrators move to the cloud faster, reduce costs, and enable compliance with federal policies and directives, including:

- Executive Order 14028, Improving the Nation's Cybersecurity
- OMB Memorandum M-22-09 on federal Zero Trust strategy
- FIPS 140-2 component validation

Moreover, RSA ID Plus for Government provides the capabilities federal agencies and integrators need to address a range of government use cases, such as:

- Workforce authentication
- Secure contractor access
- Remote and BYOD access
- Secure login for legacy systems
- Continuous diagnostics and mitigation (CDM) alignment
- Protecting Microsoft GCC High environments

What is FedRAMP?

FedRAMP (Federal Risk and Authorization Management Program) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring of cloud products and services. It aims to streamline the process of authorizing cloud services for use by federal agencies, ensuring a consistent level of security across the government. This is important because government agencies are assured FedRAMP-authorized security solutions meet the necessary security levels the government requires.

FedRAMP aligns with the goals of Executive Order 14208 by ensuring that cloud service providers meet stringent security requirements, which contributes to the overall security of federal systems.



Benefits of Moving to Cloud

Migrating IAM and other aspects of cybersecurity to the cloud can strengthen US government security by:

- Improving baseline security with enterprise-grade protections
- Enabling Zero Trust through strong authentication, including phishing-resistant multi-factor authentication (MFA)
- Supporting centralized dashboards to track adherence to security policies
- Establishing backup and redundancies for rapid recovery from incidents
- Building resilience against attacks through distributed cloud infrastructure

What is the focus of Executive Order 14028?

EO 14028 aims to modernize and strengthen the overall cybersecurity posture of federal agencies, including their use of cloud services. The order's primary focus is on improving the federal government's cybersecurity by addressing vulnerabilities, modernizing systems, and enhancing incident response capabilities. It pushes for the adoption of Zero Trust Architecture and standardized security practices.

What is Zero Trust?

Zero Trust describes an approach to security that never assumes trust, but instead always verifies whether someone or something seeking access is trustworthy before granting access. IAM in general and MFA in particular are critical to helping enforce the core "never trust, always verify" thinking behind the concept of Zero Trust, by enabling government agencies and integrators to continuously authenticate users and devices.

What is FIDO2?

FIDO2 is the open authentication standard that's designed to replace passwords with strong, phishing-resistant authentication. It's part of US government policy guidance through OMB M-22-09, which explicitly defines phishing-resistant MFA. (EO 14028, in contrast, sets broad policies for improving security without mentioning FIDO2 directly.)

RSA ID Plus for Government

RSA offers the most secure and comprehensive identity security platform to defend against the highest levels of cybersecurity risks and drive [Zero Trust](#). RSA ID Plus for Government is formally authorized by FedRAMP for use by any US government agency. RSA's mission is to help federal agencies secure and accelerate their adoption of cloud services, in accordance with EO 14028, which calls for more government agencies to quickly move toward secure cloud services.

Highlights of the complete, secure RSA ID Plus for Government platform include:

- A complete authentication and access solution
- Protecting Microsoft GCC High deployments with Microsoft External Authentication Methods (EAM)
- Extends across cloud, hybrid, and on-premises environments
- Multiple plans to ensure the right level of protection and controls
- Enhanced security layer for [Microsoft Entra ID](#)
- Part of the AI-powered RSA Unified Identity Platform
- Supports add-ons including [RSA® Risk AI](#), [RSA® Help Desk Live Verify](#), or [RSA® iShield Key 2](#) authenticators, based on specific needs
- Professional Services and Technical Support to deliver and maintain an optimal implementation
- A global network of trusted partners

FedRAMP Moderate security compliance

To meet specific FedRAMP Moderate security and privacy controls, RSA ID Plus for Government differs in the following ways from RSA ID Plus:

- The solution is hosted on Azure's Government Cloud for stronger security controls and compliance checks from Microsoft, rather than Azure's Commercial Cloud
- SMS and voice token codes are excluded from RSA ID Plus for Government

Ultimately, RSA ID Plus for Government provides the highest-level security solution that RSA ID Plus customers trust and rely on.

RSA ID Plus for government tech support

Customers who have purchased RSA ID Plus for Government are entitled to receive US Citizen on US Soil support. Additionally, for the convenience of customers who leverage this offering, we provide offshore support for general inquiries that do not involve controlled unclassified information (CUI) data. This allows customers to engage with our support team in a way that is comfortable and convenient for them.

Impact level/DoD impact level

RSA ID Plus for Government is FedRAMP Moderate Authorized by the Joint Authorization Board (JAB), with DoD IL2 reciprocity, making it an ideal solution for federal government agencies and Federal Systems Integrators with CUI requirements. The cloud-agnostic RSA iShield Key 2 Series hardware authenticators use an NXP security chip with a FIPS 140-3 Level 3 certification (certificate number 4679) which meets the NIST SP800-63B4 requirements of an AAL3 Authenticator (section 2.3). The combination of RSA ID Plus and iShield Keys provides the highest level of identity and authentication assurance, all from a single vendor. RSA ID Plus can also protect Microsoft GCC High environments via the Microsoft EAM integration.

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.

