RSA® SecurID® Access and Microsoft® Office 365

Secure and convenient access to enable workforce productivity

At A Glance

- Apply the same highly secure access levels for SaaS (like Microsoft Office 365) and mobile apps that you already provide on-premise
- Simplify user access with simple authentication options leveraging the user's mobile device and SSO capabilities
- Confidently access SaaS applications from any device, located inside or outside your network, while sensitive user credentials stay safe on-premise
- Discourage Shadow IT with integrations to all of your web applications
- Determine access using context sensitivity policies that look at application type, location of user and other factors

Nowadays, most organizations have users in the office and on-the-go. Microsoft Office 365 gives them the ability to create and share data from familiar business applications no matter where they are or what device they're using. It's in organizations' best interest to provide secure and convenient access to these applications to enable workforce productivity.

But, in today's world of SaaS applications (like Microsoft Office 365), and a mobile workforce, securely managing access has become nothing short of a herculean effort for IT. There are more users, more data, more devices, and the disappearance of the corporate perimeter with which to contend.

RSA SecurID Access answers these challenges by:

-**Consistently enforcing access controls** and strong authentication to Microsoft Office 365

-**Providing on-premise -levels of access protection** for all of your SaaS and on-premise web applications

-**Delivering a simple end user authentication experience** from iOS and Android mobile devices

-**Accommodating a wide range of requirements** for context-based access security

RSA SecurID Access: Secure, frictionless access to today's SaaS, enterprise, mobile and web apps

RSA SecurID Access seamlessly verifies user identities with policy-based contextual assessments and strong authentication SecurID smart mobile devices to deliver on demand, one-click SSO access to standard and non-standard SaaS, Web and mobile applications. A hybrid-cloud approach allows organizations to maintain control of the privacy and security of identities, combating one of the main hurdles to adopting a cloud solution.

RSA SecurID Access allows you to open the door to a new generation of SaaS, mobile and web applications, armed with the same confidence and security with which you deliver on-premise applications.

Strong, secure access with convenient SSO

RSA SecurID Access delivers higher security without forcing users to struggle through inconvenient authentication and access hoops. It ensures easy access to the many RSA SecurID Access-certified SaaS applications and to mobile, web and on-premise applications.

Intuitive user experience for mobile users. Users can access resources from any location through the RSA SecurID Access portal or directly when it's more convenient, regardless of where the data lives. By simply leveraging their mobile device, users can easily use step up authentication methods - TouchID, Shake/Tap to Approve, One Time Passcode – or Apple Watch or RSA SecurID®.

Flexible, context-based access allows you to create consistent, centrally enforceable access profiles based on user data such as what group they are in, application sensitivity, session and network info and device type. RSA SecurID Access automatically distinguishes between the access requirements of a finance director working at the office and an accounts payable specialist working from home. By making access simple, yet secure, RSA SecurID Access discourages departmental-level Shadow IT initiatives.

Single Sign-On (SSO) provides a streamlined experience for users, speeding access to resources from any location regardless of where the data lives. It eliminates the need to authenticate multiple times and removes roadblocks to user productivity without compromising security.

Regain control over a disrupted perimeter

Centralized control replaces multiple management silos. A single RSA SecurID Access management interface helps integrate SaaS access control with your existing web access management infrastructure, replacing existing, separate management interfaces.

Sensitive user credentials are inherently secure. RSA SecurID Access architecture delivers high security that pure SaaS access solutions cannot. Sensitive user credentials remain on-premise and are not transmitted to the cloud.
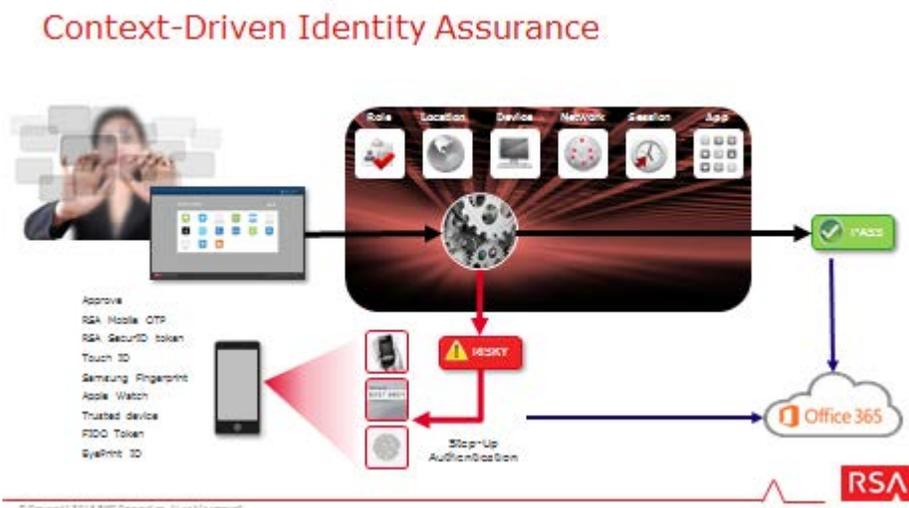
Tested and certified to work with *your* applications. RSA certifies SaaS applications, including Microsoft Office 365, for use with RSA SecurID Access to confirm that they, and your data, are fully protected.

Combats identity as a threat vector. RSA SecurID Access identities can be shared with RSA SecurID Lifecycle and RSA SecurID Governance, as well as other RSA offerings like SecurID, to form a coordinated response to identity threats.

Securely and easily connect to Microsoft Office 365

RSA SecurID Access enables secure and convenient access to Microsoft Office 365 by evaluating a set of identity attributes to determine whether to apply SSO or ask for an additional form of identity assurance. In this way, the application itself is protected but users are only interrupted if the situation requires additional authentication.

RSA SecurID Access embraces the Security Assertion Markup Language (SAML) standard to integrate securely and conveniently to Microsoft Office 365.