

RSA® Sign-On Manager: Delivering on the Promise of Simple and Secure Access to Applications

This white paper explains how RSA® Sign-On Manager can be deployed to provide organizations and their end users with simple and secure application access. It describes the elements of the solution and shows how RSA Sign-On Manager can be implemented with different methods of authentication to meet an organization's business, security or compliance requirements.

Whether it is implemented in a password-only environment or deployed with strong, two-factor authentication, RSA Sign-On Manager allows the enterprise to: increase end-user satisfaction through simple and secure application access; reduce the burden of achieving regulatory compliance; slash the cost of password management, providing a quick ROI; and maximize its investment in RSA SecurID® and other RSA Security solutions.

TABLE OF CONTENTS

I. SUCCESSFULLY BALANCING SECURITY AND CONVENIENCE	1
II. AN OVERVIEW OF RSA SIGN-ON MANAGER	1
Enterprise Single Sign-on	1
Integrated Two-factor Authentication	1
Secure Self-service Emergency Access	2
Enterprise Management and Scalability	2
III. BENEFITS OF RSA SIGN-ON MANAGER	3
Increases End-user Satisfaction Through Simple and Secure Application Access	3
Reduces the Burden of Achieving Regulatory Compliance	3
Slashes the Cost of Password Management and Provides a Quick ROI	3
Maximizes an Organization's Investment in RSA SecurID® and Other RSA Security Solutions	4
IV. FACTORING-IN DIFFERENT AUTHENTICATION REQUIREMENTS	4
V. DEPLOYMENT SCENARIOS	5
Password-only Deployment	5
Strong Authentication	5
Leveraging an Existing RSA SecurID Infrastructure	6
ESSO for Diverse User Populations	6
V. SUMMARY	6
ABOUT RSA SECURITY	6

I. SUCCESSFULLY BALANCING SECURITY AND CONVENIENCE

Many organizations today are concerned with end-user dissatisfaction, weak security and high help desk costs associated with traditional password-based authentication to networks and applications. Whether as part of a regulatory compliance initiative or in an effort to protect sensitive company information, organizations are looking to impose stronger password requirements. These stronger policies come at the expense of end users, who are often struggling with remembering ten or more passwords. Recent research has shown that 9 out of 10 users surveyed expressed frustration with this password management headache. In response to this frustration almost 2/3 of all users write their passwords on sticky notes, in their PDA or in a file on their PC, thus actually weakening security.

Enterprise single sign-on (ESSO) solutions help to resolve this dilemma by providing organizations a way to provide simple *and* secure application access for their end users. ESSO solutions provide each user with a single method of authenticating his-or-her identity throughout the organization, and offer the organization the ability to make the method of authentication as strong as required to meet their business, security or compliance requirements.

RSA® Sign-On Manager—an ESSO solution that is integrated with two-factor authentication offerings from RSA Security—provides organizations with flexible, secure and cost-effective access to resources throughout the enterprise. By deploying RSA Sign-On Manager and two-factor authentication, organizations can simplify identity management, protect application and network resources, and build an infrastructure that both reduces complexity and increases security.

II. AN OVERVIEW OF RSA SIGN-ON MANAGER

RSA Sign-On Manager features can be grouped into four major functional areas: Enterprise Single Sign-On; Integrated Two-Factor User Authentication; Secure Self-Service Emergency Access; and Enterprise Management and Scalability.

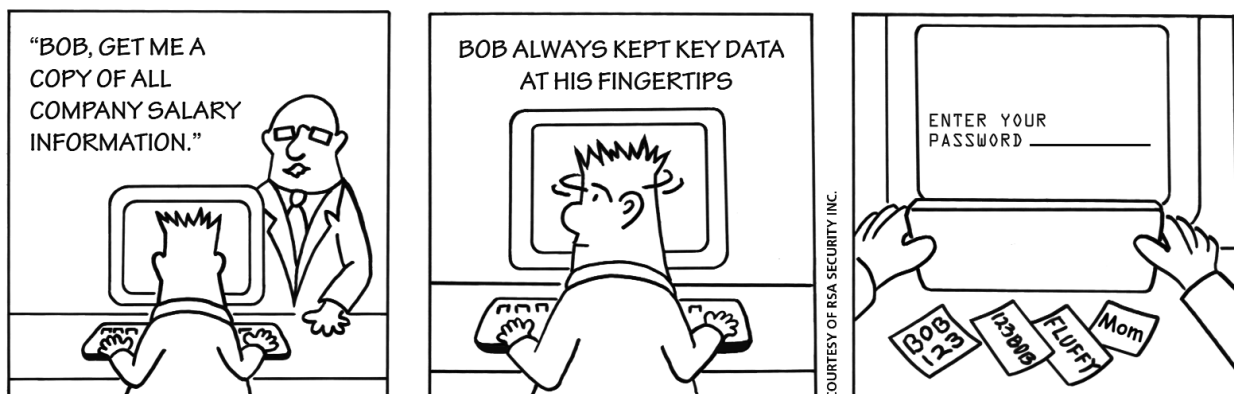
Enterprise Single Sign-on

RSA Sign-On Manager provides an automatic process to detect and respond to application logons and password change requests across a variety of software architectures—including client/server, web, Java™, host/mainframe and Citrix® distributed applications—without the need to make changes to any of the applications. RSA Sign-On Manager offers out-of-the-box support for a wide range of software applications, and organizations can easily add new applications without additional programming.

With RSA Sign-On Manager, IT can increase user satisfaction by allowing users to avoid having to remember multiple complex passwords. Users can authenticate once and move freely from application to application without the need to re-authenticate.

Integrated Two-Factor Authentication

As companies initiate ESSO deployments, it is essential that the initial logon is secure—protecting the “keys to the kingdom.” Tight integration with RSA Security’s best-in-breed two-factor authentication capabilities provides the extra layer of protection of desktop and application resources that many organizations require. Better still, companies may mix and match the strength of authentication to the security requirements of individual users or groups. This allows an organization to initially focus on tightly controlling the logon process for key groups (e.g. finance or human resources) while allowing for future migration from passwords to strong authentication for the rest of the user population.



INTELLIACCESS TECHNOLOGY: A CLOSER LOOK AT SECURE EMERGENCY ACCESS

IntelliAccess technology has taken self-service password reset and emergency access to an entirely new level, and this patent-pending technology offers the following major business advantages:

ENHANCED SECURITY: IntelliAccess technology moves beyond challenge/response technologies and delivers a secure and unique approach to virtually verify users before granting access to credentials. It starts with the use of pre-selected questions with sufficient randomness to prevent unauthorized users from “guessing” answers. Unique technologies evaluate the importance of specific questions and answers—going beyond a simple weighting or point system.

Administrators have the ability to determine the number of questions and configure the tolerance levels for answers to questions. For example, an administrator could determine whether all questions must all be answered correctly or if the system will tolerate a configurable number of unanswered questions, forgotten answers or possible user input errors. Identities are further protected through the use of encryption technologies, and administrators can also monitor IntelliAccess technology usage through RSA Sign-On Manager audit trails.

PRIVACY PROTECTION: Securing the identity and personal information of users is important to both employees and organizations. IntelliAccess technology increases end-user privacy by eliminating the need to store credentials or other personal information. Individual answers to challenge/response questions are never stored. Instead, the aggregate of verification information is compared—and secured with cryptographic methods—to ensure that unauthorized users cannot gain access to answers to the questions.

ANYTIME, ANYWHERE EMERGENCY ACCESS:

Whether in the office or on the road, users can gain emergency access to their credentials without calling the help desk. IntelliAccess can allow users to securely recover their credentials—whether it be a forgotten password or a lost SecurID token—regardless if they are on-line in the office or off-line on an airplane. This capability is unique to the RSA solution.

Secure Self-service Emergency Access

Embedded in the RSA Sign-On Manager solution, groundbreaking IntelliAccess™ technology—developed by RSA Laboratories—offers innovative self-service emergency access and password reset functionality. IntelliAccess technology delivers all the benefits of self-service password reset and emergency access plus innovative features that enhance security and protect end-user privacy. Unique to IntelliAccess technology is the ability to handle both forgotten passwords and lost RSA tokens—in both on-line and off-line situations—thus delivering to users anytime, anywhere access to their application resources.

Enterprise Management and Scalability

RSA Sign-On Manager includes centralized management for policy control, user enrollment, and automated credential backup. Automated backup ensures that the server has the most up-to-date user credentials, providing the mobility that end users require as they move from PC to PC. The intuitive web based interface enables delegation of administrative functions allowing organizations to segregate tasks such as the creation of password change policies and the setting of rules governing strong authentication—including the ability to enforce the use of two-factor authentication regardless of where the user attempts to login.

RSA Sign-On Manager can be run on clustered servers to provide for redundancy and fault tolerance, helping to ensure availability. Further helping to improve availability, performance and overall security, RSA Sign-On Manager leverages an organization’s replicated LDAP environment. As opposed to solutions that require each client to directly access the production directory, the RSA Sign-On Manager architecture provides one point of entry into the LDAP directory—thus allowing security administrators to easily lock down and monitor this connection.

Administrators can centrally establish, enforce and manage authentication policies matched to the security requirements of different classes of users. While password authentication may be sufficient for certain users, other classes of users may require strong, two-factor authentication. IT thus benefits from the flexibility to select the optimum means of authentication for each class of user. For environments using password-based authentication, the password change capabilities configured within the centralized RSA Sign-On Manager server allow organizations to have application passwords generated automatically. These passwords can be made more complex and therefore strengthened—without impacting the end user who never has to manually present these complex passwords to individual applications.

III. BENEFITS OF RSA SIGN-ON MANAGER

RSA Sign-On Manager benefits an organization by providing capabilities valued by both end users and IT.

Increases End-user Satisfaction Through Simple and Secure Application Access

Organizations can increase user satisfaction by eliminating multiple logons. Users no longer need to remember complex passwords or password policies that vary by application. They authenticate once and can move from application to application without the need to re-authenticate—and without having to waste any time looking for passwords or troubling the help desk to gain access.

The simplification of the user experience does not come at the expense of weakening security. The enterprise has maximum flexibility in selecting the most appropriate level of authentication to meet their security requirements. RSA Sign-On Manager can be deployed to support logon using passwords, while organizations looking for increased

security can enable two-factor authentication. Since RSA Sign-On Manager integrates and supports a range of authentication methods, an organization can easily transition their users from a Microsoft® Windows® password authentication to a stronger form of authentication without changing the applications or underlying ESSO architecture.

Reduces the Burden of Achieving Regulatory Compliance

An effective compliance program will involve improving access controls to critical applications in order to ensure adequate internal controls are in place to protect business information. This normally involves strengthening user authentication to existing applications within the company's network, often involving the implementation of strong password policies.

The unwanted by-product of these compliance initiatives is users committing passwords to sticky notes and thus actually decreasing overall security. As companies look to improve authentication capabilities in support of more positively validating user identities, doing so in a way that does not result in user backlash is critical. RSA Sign-On Manager allows organizations to mandate very strong password policies or implement two-factor authentication for the initial logon while not imposing draconian password requirements on an application by application basis.

Slashes the Cost of Password Management and Provides a Quick ROI

Forgotten passwords and misplaced tokens inevitably result in calls to the help desk and diminished user and IT help desk productivity. Organizations need to reduce the cost of managing passwords so they can drive down help desk calls and increase productivity.

Implementing RSA Sign-On Manager can significantly reduce the number of calls to the help desk caused by users trying to access individual applications. By automating the application logon process, RSA Sign-On Manager greatly reduces the chance that users will forget the credentials required to authenticate to any one application. Organizations will see a further reduction in calls to the help desk, since IntelliAccess™ technology allows users to access their credentials even if their authenticator is not available or if they have forgotten their initial Microsoft® Windows® password. IT can also completely automate the password change process for applications, thereby eliminating another source of calls to the help desk.

CRACKING THE COSTS OF PASSWORD MANAGEMENT

Passwords are not only difficult to remember, they are expensive for the organization to maintain. Password-related help desk calls may cost as much as \$30 per call, according to a Meta Group (now Gartner Group) study. Supporting the overhead of help desk calls is expensive when you take into consideration the lost productivity of the employee and the expenses associated with help desk personnel and their associated systems. Productivity is hurt each time a user gets locked out and has to call into the help desk for assistance.

Gartner estimates that password reset requests and user ID problems can account for 15 to 35 percent of all help desk call volumes.¹ This cost becomes a considerable portion of the help desk budget, particularly since according to industry statistics most users call the help desk with password-related issues more than three times a year.

¹ Justify Identity Management Investment With Metrics; R. Witty, K. Brittain, A. Allan; Gartner Research Note; February 23, 2004.

Maximizes an Organization's Investment in RSA SecurID® and Other RSA Security Solutions

Organizations which already use RSA SecurID solutions for remote access can add RSA Sign-On Manager to extend strong authentication to protect desktop, network and application resources. Sign-On Manager similarly extends the value of RSA Digital Certificate and RSA ClearTrust® Web Access Management solutions by providing a single-vendor solution for managing authentication.

RSA Digital Certificate solutions are a family of interoperable modules for managing digital certificates and creating an environment for authenticated, private and legally binding electronic communications and transactions. These keys and certificates can be used for authentication and also for digitally signing and encrypting documents and e-mail, and the enterprise can centrally manage them using RSA Sign-On Manager.

The RSA ClearTrust Web Access Management solution enables organizations to cost-effectively provide secure access to web applications within intranets, extranets and portals. RSA ClearTrust Web Access Management customers can extend their web single sign-on environment by deploying RSA Sign-On Manager to incorporate single sign-on to host/mainframe, client/server and other enterprise applications. By deploying RSA Sign-On Manager with RSA ClearTrust software, organizations can implement a complete SSO solution for the extended enterprise including employees, customers and business partners.

IV. FACTORING-IN DIFFERENT AUTHENTICATION REQUIREMENTS

Authentication—proving the identity of users—is designed to establish trust by ensuring that the participants are indeed who they claim to be. The most common form of authentication today is passwords, but many organizations seek greater security levels. While passwords are sufficient for some organizations or some classes of users, the enterprise has the option of complementing the use of passwords by deploying two-factor authentication.

Strong two-factor authentication allows organizations to better safeguard corporate information assets. Access to protected resources is granted only when the user is successfully authenticated using two factors:

- Something the user knows—a personal identification number (PIN) and
- Something the user has, such as an RSA SecurID authenticator or an RSA® Smart Card.

In addition to single factor password authentication, RSA Sign-On Manager supports two-factor authentication in conjunction with an RSA SecurID authenticator, RSA Smart Card or an RSA Security USB authenticator. These authentication devices can support a plethora of authentication methods, including the use of a One-Time Password (OTP), digital certificate or stored Microsoft® Windows® user names and passwords.

Unique to RSA Sign-On Manager is support for single sign-on to RSA SecurID Ready applications. Using either the SecurID software token or the dual use RSA SecurID SID800 token, users can seamlessly authenticate to the hundreds of popular applications (VPNs, Outlook® Web Access, etc.) that natively support RSA SecurID authentication.

Organizations interested in combining physical and logical access can turn to RSA® Smart Cards in conjunction with Sign-On Manager software. RSA Smart Cards allow users to securely store digital certificates, finger-based biometric templates, user names, and passwords allowing for authentication to the network and application resources when used with RSA Sign-On Manager. These same RSA Smart Cards can be used as employee identity cards—complete with a photograph of the employee. With support for proximity-based physical access solutions, RSA Smart Cards can become the single secure authenticator for organizations that want both ease-of-use for their users and enhanced security for protecting access to critical information.

V. DEPLOYMENT SCENARIOS

ESSO and two-factor authentication can be deployed as separate or complementary initiatives, with the combination of the two providing maximum value. There are many different deployment scenarios, giving an organization maximum flexibility for securing enterprise resources.

Password-only Deployment

An organization may be seeking to reduce password management overhead and improve user satisfaction via ESSO, but two-factor authentication may not yet be an immediate priority. By deploying RSA Sign-On Manager, this organization can simplify access to information, reduce help desk costs and increase user productivity while maintaining the flexibility to easily add enhanced security options in the future.

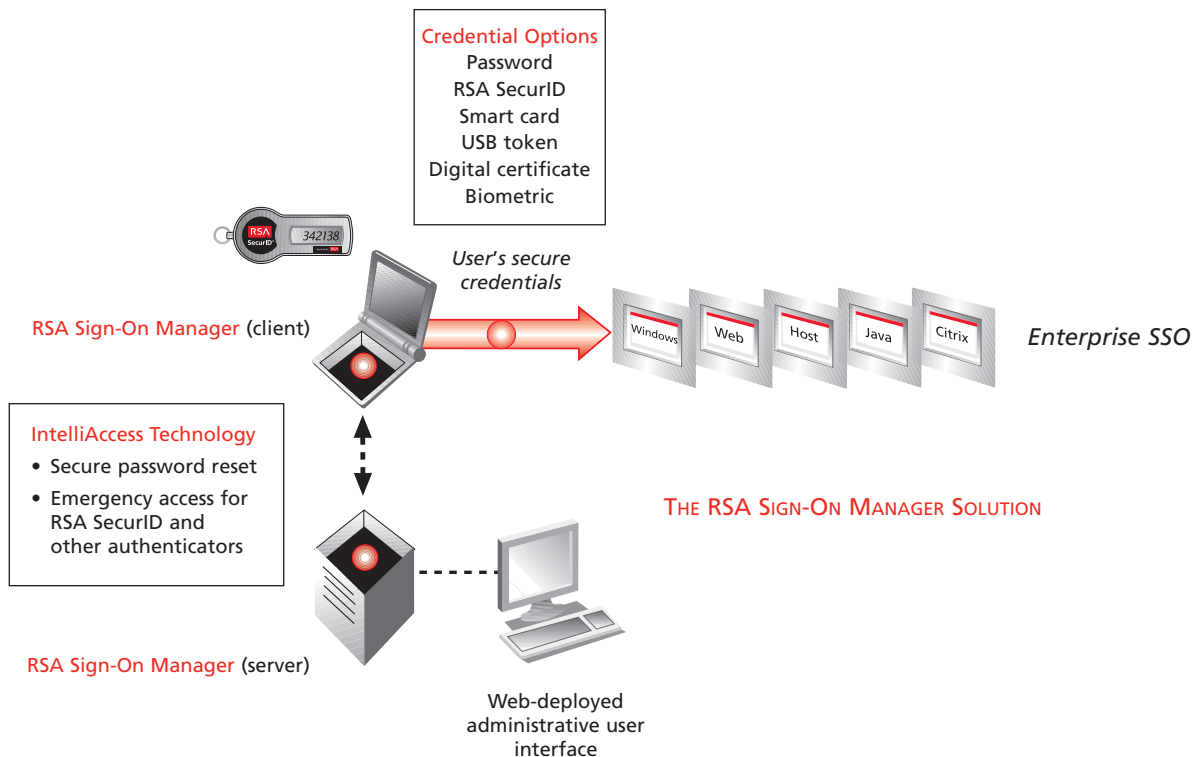
Users would simply authenticate at their desktops by entering a user name and password, and from that point on they could access applications without being prompted again to authenticate to the network. The users benefit from a secure self-service method to reset their Microsoft Windows password, and the organization avoids the overhead burden of password reset calls to the help desk. In the future, the organization can deploy strong two-factor authentication while leveraging the investment in ESSO.

Strong Authentication

In another scenario, an organization may be seeking a USB token authentication or smart card solution for two-factor authentication to the desktop or for support of digital certificates. ESSO may not be an immediate priority today with this organization, but it would like to deploy solutions that would easily allow for single sign-on in the future. By selecting solutions from RSA Security, this organization can protect investments in security by maintaining flexibility to meet future requirements.

For example, RSA Sign-On Manager could be deployed with RSA Smart Cards for environments that require digital certificate authentication used in conjunction with encrypted e-mail or digital signing solutions. These can then be extended to provide for single sign-on to a broader set of applications.

The RSA Sign-On Manager solution gives organizations the ability to deploy a single desktop package to end users without the need to integrate smart card software with enterprise SSO software. Administrator can manage all components from a single web deployed console—reducing the total cost of ownership for client deployment and administrative management.



Leveraging an Existing RSA SecurID Infrastructure

In a third deployment scenario, an organization may have already deployed strong authentication solutions from RSA Security to provide a remote workforce with two-factor authentication to access desktop and network resources. This existing RSA SecurID authentication customer can efficiently extend the investment to provide secure access to a wide range of applications.

By deploying RSA Sign-On Manager with SecurID solutions, employees may use their SecurID token to gain access to not only their Microsoft Windows environment, but to all of their enterprise applications as well. In this way the power of two-factor authentication is extended to protect a much broader set of company resources.

ESSO for Diverse User Populations

Many organizations have different authentication requirements for various groups of users, and RSA Sign-On Manager allows them to implement ESSO across a spectrum of authentication options. Sign-On Manager offers native support for a variety of authentication methods and the tools required to deploy and administer a heterogeneous environment.

VI. SUMMARY

RSA Security offers ESSO solutions that enable flexible access and authentication choices. RSA Sign-On Manager allows the enterprise to:

- Increase end-user satisfaction through simple and secure application access
- Reduce the burden of achieving regulatory compliance
- Slash the cost of password management and provide a quick ROI
- Maximize an organization's investment in RSA SecurID and other RSA Security solutions

The RSA Sign-On Manager solution combines enterprise single sign-on, integrated two-factor user authentication, secure self-service emergency access, and enterprise management to form a key component of an enterprise security program for identity and access management.

ABOUT RSA SECURITY

RSA Security is the expert in protecting online identities and digital assets. The inventor of core security technologies for the Internet, the company leads the way in strong authentication and encryption, bringing trust to millions of user identities and the transactions that they perform. RSA Security's portfolio of award-winning identity & access management solutions helps businesses to establish who's who online—and what they can do. With a strong reputation built on a 20-year history of ingenuity, leadership and proven technologies, we serve more than 18,000 customers around the globe and interoperate with over 1,000 technology and integration partners. For more information, please visit www.rsasecurity.com.

