IBM Security Access Manager for Enterprise Single Sign-On

Simplify password management, strengthen access security and demonstrate compliance

Highlights

- Achieve faster time to value and higher ROI with a virtual appliance form factor
- Reduce password-related help-desk costs with fewer password reset calls
- Track and audit fine-grained user access to information for improved compliance reporting
- Increase security through strong authentication to a variety of end-points such as personal computers, kiosks and virtual desktops
- Improve user productivity with convenient single sign-on to applications such as electronic medical records (EMR) solutions

A proven single sign-on solution to automate user access

With the advent of application and desktop virtualization, and an ever increasing number of enterprise applications and access points, organizations face the challenge of providing convenient user access while protecting IT resources. In order to access these resources, employees are typically expected to remember an ever-growing number of passwords—then update them frequently. When a forgotten password prevents a user from logging into an application, you have more than just a frustrated user. You have lost productivity and additional costs from password reset calls that burden overstretched IT help desks. Organizations must manage the trade-off of providing convenient user access while at the same time ensuring strong security, especially in shared workstation environments. They also need to ensure that only authorized users are accessing protected resources and to demonstrate their compliance with industry and security regulations.

By providing integrated single sign-on and access management capabilities, IBM Security Access Manager for Enterprise Single Sign-On addresses these needs and more. Security Access Manager for Enterprise Single Sign-On combines single sign-on (SSO), strong two-factor authentication, session management, centralized identity and policy management, security workflow automation, fast user switching, and user access tracking and audit with ***no change to the existing infrastructure***.

Security Access Manager for Enterprise Single Sign-On offers the power and flexibility that is needed in an enterprise SSO tool. With Security Access Manager for Enterprise Single Sign-On, employees authenticate once, and the software then detects and automates all password-related events for the employee, including:

- Logon
- Password selection
- Password change
- Password reset
- Automated navigation to any screen in the application where productive work can immediately begin
- Logoff

Security Access Manager for Enterprise Single Sign-On helps organizations reduce costs, strengthen security, improve productivity and address compliance requirements. This solution provides single sign-on for all your Microsoft Windows, web, Java, mainframe and teletype applications, and is available on all major network access points, including Windows desktops, laptops, shared kiosks, virtual desktops, Citrix servers, Microsoft Terminal Servers and web portals. This complete endpoint coverage allows users to sign on from anywhere to the enterprise network with one password and get single sign-on access to all applications, even if access is via a browser from an Internet café.

Improve password management with single sign-on

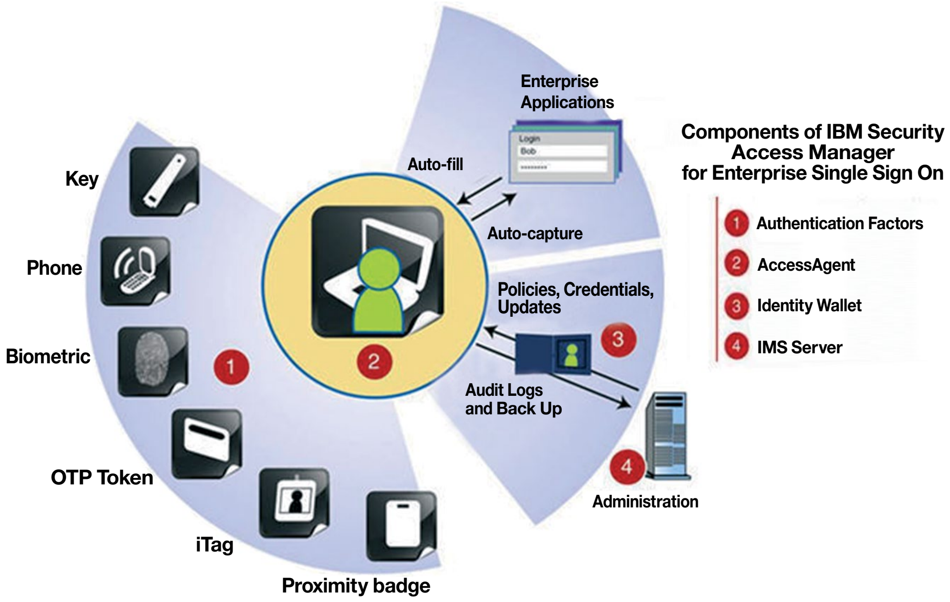
Security Access Manager for Enterprise Single Sign-On can reduce help-desk compliance and administration costs by streamlining password management and improving users' password behavior. When users have multiple user IDs and passwords, they typically write them down in unsecured locations, use easy-to-guess passwords and share their passwords with co-workers. Having only one password to remember can reduce these behaviors and lower the number of password-reset calls made to the help desk.

Security Access Manager for Enterprise Single Sign-On can be configured to detect password changes and auto-generate strong passwords for each application. Because it remembers and enables single sign-on with these strong passwords, users never have to remember or manage these passwords themselves, providing security while maintaining user productivity. To protect passwords and related data wherever they are located, the software uses Advanced Encryption Standard (AES) algorithms, some of the strongest cryptography available.

Use strong authentication to protect information

For added security, many organizations want to augment passwords with strong two-factor authentication methods to help meet compliance requirements. Security Access Manager for Enterprise Single Sign-On not only supports a wide choice of strong authenticators, such as USB smart tokens, smart cards, active proximity cards, passive proximity badges, one-time password tokens and fingerprint biometric devices, but also enables existing identification devices, such as building badges, photo badges and cell phones, to be used for authentication. Leveraging devices users already have and know how to use can accelerate implementation and reduce the total cost of ownership.

One of the strengths of Security Access Manager for Enterprise Single Sign-On is its ability to integrate with existing applications and authentication devices. For example, Security Access Manager for Enterprise Single Sign-On provides an open authentication device interface to easily integrate any smart card that is PKCS#11 or MS-CAPI compliant, and any serial ID device, such as your building access badge or photo badge.



IBM Security Access Manager for Enterprise Single Sign-On combines single sign-on, strong authentication, session management, automated navigation to any screen in the application and audit tracking with no change to the existing infrastructure.

Also, it provides out of the box support for 3rd party applications such as electronic medical records (EMR) solutions from vendors such as Epic and enterprise resource planning (ERP) solutions from vendors such as SAP.

Add security to virtual and shared desktops

Sharing kiosks, workstations and virtual desktops is a vital requirement in many industries such as manufacturing, healthcare, warehousing, retail and financial services. This convenience lets many users roam and access information from anywhere from a number of devices without having to return to their personal PCs. But shared work environments can pose severe security threats as users often walk away without logging off, potentially exposing confidential information to unauthorized access. Any attempt to tighten security, enforce unique user logons and comply with regulations can lead to users being locked out of workstations, resulting in a loss of productivity.

The session management and fast user switching capabilities within Security Access Manager for Enterprise Single Sign-On allow multiple users to share a computer simultaneously and switch between users without the need to log off or risk getting locked out. Users who want their desktops to "follow them" can use the software's roaming desktop support. Users can also maintain their private desktops while sharing workstations with co-workers. If a user walks away from a session without logging out, Security Access Manager for Enterprise Single Sign-On can be configured to enforce inactivity timeout policies such as configurable screen locks, application logout policies, graceful logoff of all applications, and more.

Security Access Manager for Enterprise Single Sign-On strengthens security for the virtual desktop by integrating with VMWare View, enabling users to access all their applications inside the virtual desktop with a single strong password. VMware View helps simplify and automate the management of thousands of desktops and to deliver desktop as a service to users from a central location or in the cloud. Once users are logged onto their workstation, Security Access Manager for Enterprise Single Sign-On automatically signs them into their virtual desktop. The Security Access Manager for Enterprise Single Sign-On agent for virtual desktops collects audit information that can be used to generate detailed reports for compliance and chargeback accounting purposes. The organization's regulatory and compliance requirements can be satisfied, especially those especially related to monitoring events such as application access and usage inside the virtual desktop.

Simplify fine-grained audit tracking and compliance reporting

Security Access Manager for Enterprise Single Sign-On also facilitates compliance with security and privacy regulations by leveraging centralized fine-grained auditing and reporting capabilities. To help address compliance requirements, the solution transparently logs all user log-on activities and centrally records them inside the system database. The software also enables customized tracking, allowing you to track and monitor activities not otherwise possible through your applications. The resulting consolidated user-centric logs provide the meta-information that can guide administrators to the right application logs for more detailed analysis when required. Integration with IBM Tivoli® Common Reporting provides flexible reporting options to meet your compliance reporting needs.

Simplify deployment and management

Security Access Manager for Enterprise Single Sign-On simplifies deployment and management with a new VMware ESX/ESXi virtual appliance configuration option. In addition, a wizard-driven graphical administrative web console walks administrators through all the tasks of configuration, deployment and administration.

Security Access Manager for Enterprise Single Sign-On ships preconfigured for many popular applications, and an even larger number of applications can be supported through an easy no-fee download of their access profiles. In addition, administrators can auto-generate access profiles for new applications through a simple wizard interface—without requiring the administrator to develop cumbersome scripts or costly connectors, or to make changes to the target applications or systems. More complex applications can be supported with visual profiling, a simple drag-and-drop graphical approach to configure automation and sign-on.

The software is designed to be centrally deployed and managed. Network administrators can deploy the client-side software from a central location using IBM Tivoli Configuration Manager or other software distribution solutions without having to involve employees in the installation process.

Once the software is up and running, administrators can use the administrative console to manage users individually or by group. From the central console, administrators can set password policies, system rules, user interface characteristics, re-authentication parameters and other options.

Leverage existing IT infrastructure and directory resources

Security Access Manager for Enterprise Single Sign-On is designed to work with minimal or no change to an organization's existing IT infrastructure. The solution works with any directory structure and does not require an expensive directory consolidation project prior to deployment. Unlike some competing single sign-on offerings, it does not require a directory schema extension or replication of directory data.

The solution stores user credentials, system settings and policies centrally in your corporate database, while interfacing with corporate directories such as Active Directory, NT Domain Controllers, Sun One LDAP, Tivoli Directory Server and Novell eDirectory for identity data. In addition, the solution accommodates Microsoft Internet Explorer and Mozilla Firefox browsers, offering the convenience and savings of single sign-on for users who use one browser or the other, or a combination of the two.

Centrally manage end-user and privileged identities

Administrators typically create accounts and credentials for each application, system or platform on behalf of employees, which they then send to employees by email or via paper. Not only does this manual creation and dissemination of credentials lower productivity, but employee handling of application credentials can compromise security.

Security Access Manager for Enterprise Single Sign-On integrates with best-of-breed user provisioning technologies and homegrown solutions to provide end-to-end, comprehensive identity life-cycle management. It accepts provisioning instructions from identity management solutions and enables you to pre-populate the employee's identity wallet with randomly generated application credentials.

This tight integration with provisioning solutions helps ensure that whenever an access right or password is changed through the provisioning system, Security Access Manager for Enterprise Single Sign-On user information is synchronized so that up-to-date application credentials are available. Similarly, when a user is de-provisioned, this tight integration ensures that access via Security Access Manager for Enterprise Single Sign-On will automatically be denied.

Integrating IBM Identity Manager and Security Access Manager for Enterprise Single Sign-On enables account sharing among a predefined group of users and provides single sign-on for each user in the group to a designated shared account, even as the account password is updated.

Enhance IBM access management solutions

Today, many customers are realizing the security benefits and convenience of single sign-on that IBM's Access Management portfolio delivers to web-based and federated applications. Security Access Manager for Enterprise Single Sign-On easily integrates into these environments to deliver its full set of client-focused capabilities. This IBM Security integrated solution enables security-rich single sign-on inside, outside and between organizations, providing a complete end-to-end single sign-on solution that is not available in other offerings.

Security Access Manager for Enterprise Single Sign-On at a glance

Client agent (AccessAgent and AccessStudio) requirements:

- Windows XP Professional SP3 (x86), Windows Vista SP2 (x86), Windows 7 SP1 (x86), Windows Server 2003 SP2 (x86), Windows Server 2008 SP2 (x86), Windows XP Professional SP2 (x64), Windows Vista SP2 (x64), Windows 7 SP1 (x64), Windows Server 2008 SP2 (x64), Windows Server 2008 R2 SP1 (x64)
- 600MHz Intel Pentium-based processor and 512 MB RAM for XP and 1 GB RAM for Windows Vista and Windows 7
- Disk space: At least 200 MB free hard disk space
- Microsoft Internet Explorer 7.0, 8.0, 9.0, Mozilla Firefox 3.5, 3.6
- Virtualization: Citrix XenApp version 5.0 and 6.0, Citrix ICA Client and Web plug in version 12.x, Microsoft App-V version 4.6 (x86 and x64), VMware View version 5 and 4
- Installation via Microsoft Installer (MSI) package requires Microsoft Windows Installer

Administrative console and server requirements:

- IMS Server requires Windows 2003 Service Pack 2 (x86) Standard, Datacenter and Enterprise Editions, Windows Server 2008 SP2 (x86 and x64) Standard, Datacenter and Enterprise Editions, Windows Server 2008 R2 SP1 (x64) Standard, Datacenter, and Enterprise Editions
- AccessAdmin requires Microsoft Internet Explorer 7.0 or higher with 128-bit encryption
- PC with an x86 or x64 bit processor, at least 2 GHz processor clock speed, minimum 3 GB physical memory (database not co-located), at least 8 GB free hard disk space (database not co-located)
- Hardware requirements (virtualization): VMware ESX and ESXi 3.5 or 4.0, 2 virtual processors, 4 GB virtual RAM
- Disk space: At least 3 GB free hard disk space
- Directory: Active Directory, NT Domain Controllers, Sun One LDAP, Tivoli Directory Server, Novell eDirectory, or other LDAP
- Application Server: IBM WebSphere® Application Server (Base and Network Deployment Edition) 7.0 (x86 and x64) with latest fix pack
- Web Server: IBM HTTP Server 7.0 (x86 and x64) with latest fix pack
- Reporting: IBM Tivoli Common Reporting 2.1 and 1.2
- Database: IBM DB2® Workgroup and Enterprise Server Edition 9.7 (x86 or x64), Oracle 10g R2 (x86 and x64), 11g R1 (x86 and x64), 11g R2 (x86 and x64), Microsoft SQL Server 2005 SP4 (x86 and x64), 2008 (x86 and x64), 2008 R2 SP1 (x64)

Certification:

- FIPS 140-2
- In evaluation for Common Criteria EAL3, which is given only to a select few products that can demonstrate that that they were methodically designed, tested and reviewed

Key components of Security Access Manager for Enterprise Single Sign-On

Authentication factors: Supports an open authentication device interface and a wide choice of strong authentication factors, including iTag—smart labels containing RFIDs that can be affixed to badges and other personal objects for flexible and cost-effective two-factor authentication.

AccessAgent and Plug-ins: Acts on the user's behalf for single sign-on and sign-off, authentication management and session management. JScript and VBScript plug-ins allow AccessAgent behavior to be customized.

Identity Wallet: Provides a personal, encrypted repository of user credentials. The identity wallet roams to the point of access and stores the user's personal identity profiles including log-in credentials, certificates, encryption keys and user policies.

IBM Integrated Management System (IMS™) Server: Provides centralized management of users and policies. All policies are defined centrally and enforced through the AccessAgent. The IMS Server also provides comprehensive backup of credentials, loss management, audit information and compliance reporting.

AccessStudio: Provides the interface used for creating AccessProfiles that enable sign-on or sign-off automation and fortified passwords.

AccessAdmin: Provides the management console that administrators and help-desk officers use to administer the IMS Server, manage users and manage policies.

AccessAssistant: Provides the web-based interface for password self-help. AccessAssistant can be used to obtain the latest credentials and to log on to applications. It also provides a web automatic sign-on feature to log on to enterprise web applications by clicking links instead of entering passwords.

AccessProfiles: Provides instructions to the AccessAgent on handling automation of single sign-on, sign-off, graceful logoff, etc. These can be customized using the AccessStudio to support a wide range of application automation actions.

For more information

To learn more about how IBM Security Access Manager for Enterprise Single Sign-On can help simplify password management for your users and IT administrators, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security

IBM Security provides the broadest, most advanced portfolio of enterprise security products, services, and expert consultants in the world. The portfolio provides the security intelligence to help organizations holistically protect its people, infrastructure, data and applications with a solution framework that covers all aspects of enterprise security, including identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates the world's broadest security research and development organization and delivery organization. This comprises nine security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM monitors 13 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
May 2012

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

♻ Please Recycle