IBM Security Access Manager for Enterprise Single Sign-On

Deliver secure, convenient access to endpoints in enterprise, virtual and mobile environments

Highlights

- Increase security through strong authentication to a variety of endpoints, including laptops, tablets, kiosks and virtual desktops
- Reduce password-related help-desk costs with fewer password reset calls
- Facilitate compliance by tracking and auditing fine-grained user access to information
- Improve mobile workforce productivity with convenient single sign-on access to Apple iPad devices
- Realize a fast time to value and lower total cost of ownership (TCO) with an easy-to-deploy-and-manage virtual appliance option
- Streamline access to critical applications such as electronic medical records (EMR) solutions

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. And now, with the rising popularity of bring-your-own-device (BYOD) programs, the access needs to be safely extended to mobile devices.

In order to access corporate data and applications, employees are typically expected to remember a 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 and mobile 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, strong two-factor authentication, session management, centralized identity and policy management, security workflow automation, fast user switching, and user access tracking and auditing 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 single sign-on 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 endpoints, including laptops, tablets, 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 a personal iPad device.

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.

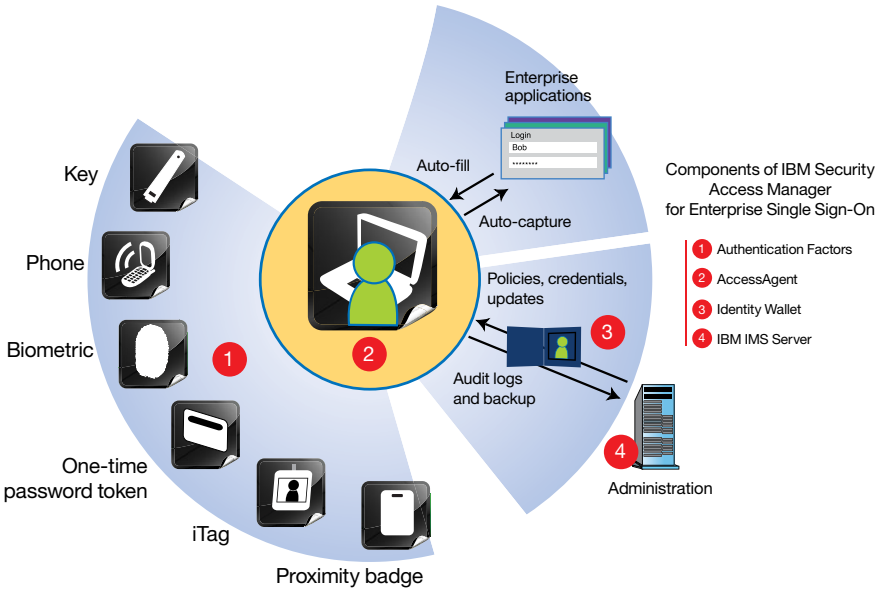
Security Access Manager for Enterprise Single Sign-On can be configured to detect password changes and auto-generate strong passwords for each application. Because it remembers and enables single sign-on with these strong passwords, users never have to remember or manage these passwords themselves, providing 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.

In addition, Security Access Manager for Enterprise Single Sign-On can be extended to manage passwords for iPad devices. The Wallet Manager for iPad provides a secure password store on the device for all the user's enterprise (and personal) usernames and passwords. Security Access Manager for Enterprise Single Sign-On can be synchronized with this wallet, so users can switch from their PCs to their iPads and continue to use the same passwords.

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 compliant with public-key cryptography standards 11 (PKCS#11) or Microsoft cryptographic application programming interface (MS-CAPI), and any serial ID device, such as your building access badge or photo badge. Also, it provides out-of-the-box support for third-party applications including EMR solutions from vendors such as Epic and enterprise-resource planning (ERP) solutions from vendors such as SAP.



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.

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 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 helps 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 related to monitoring events such as application access and usage inside the virtual desktop.

Improve mobile productivity

With Security Access Manager for Enterprise Single Sign-On, you can now extend password management and single sign-on access to users of iPad devices. The software provides two key capabilities for iPad users:

- *Secure browser:* Enables iPad users to save time with single sign-on access to corporate data and applications
- *Wallet manager:* Provides a secure password store on the iPad device for all of the user's enterprise (and personal) usernames and passwords

The Security Access Manager for Enterprise Single Sign-On server automatically synchronizes with the wallet manager, so users can seamlessly switch between their PCs and iPads—only signing into resources once. As a result, organizations can increase mobile workforce productivity and improve security as mobile users access their corporate data and applications. Users no longer need to type their passwords on the iPad device; the Security Access Manager for Enterprise Single Sign-On agent will do it for them.

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, IBM 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, and then send the information 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 lifecycle 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 deprovisioned, this tight integration ensures that access via Security Access Manager for Enterprise Single Sign-On will automatically be denied.

Integrating IBM Security 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 access management solutions deliver 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 integrated solution enables security-rich, single sign-on access 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	
Hardware	At least 1 GB of memory for Windows 7 and Windows 8 At least 512 MB of memory for Windows XP At least 500 MB free hard disk space for AccessAgent At least 300 MB free hard disk space for AccessAgent
Operating systems	Microsoft Windows 8 (x86 and x64) Microsoft Windows 7 SP1 (x86 and x64) Microsoft Windows XP Professional SP3 (x86)
Software	AccessAgent v8.2.1 Microsoft .NET Framework 2.0 for Windows XP Professional only Microsoft .NET Framework 2.0 Language Pack for Windows XP Professional only
Virtualization	Citrix XenApp v6.0 and v6.5 (x64) Citrix XenDesktop v5.5 and v5.6 (x86 and x64) Citrix ICA Client and Web plugin v12.x (x86) Citrix Receiver for Windows v3.x VMware View v4.6 (x86 and x64) and v5.1 (x64) Microsoft App-V v4.6 (x86 and x64)
Web browsers	Microsoft Internet Explorer v9 and v10 Mozilla Firefox ESR v10 and v17

Security Access Manager for Enterprise Single Sign-On at a glance	
IMS server requirements	
Hardware	For IBM DB2®: 2 GB RAM and 20 GB disk space For IBM WebSphere® Application Server Network Deployment: 2 GHz processor, 8 GB disk space and 3 GB RAM For IBM HTTP Server: 1 GB RAM and 1 GB disk space
Virtualization	For VMware vSphere Hypervisor (ESXi) v5.1: 2 virtual processors and 4 GB virtual RAM
Operating system	Microsoft Windows Server 2008 R2 Enterprise Editions SP1 (x64) Microsoft Windows Server 2008 Enterprise Editions SP2 (x86 and x64)
Middleware for application server and web server	WebSphere Application Server (Base and Network Deployment Edition) IBM HTTP Server – v8.5 (x64) and v7.0 (x64)
Middleware for database server	DB2 (Workgroup and Enterprise Server Edition) with DB2 JDBC driver v4.0 – v10.1 on Windows (x86 and x64) and v9.7 on Windows and IBM AIX® (x86 and x64) Oracle Database – v11g R2 (x86 and x64) and v11g R1 (x86 and x64) Microsoft SQL Server – 2008 R2 (x86 and x64) 2008 R1 (x86 and x64)
Middleware for directory server	Microsoft Windows Active Directory – 2008 R2 SP1 (x64), 2008 R1 (x86 and x64) and 2003 (x86) IBM Tivoli Directory Server – v6.3 (x86 and x64)
Middleware for reporting tool	IBM Tivoli Common Reporting – v2.1.1

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.

Why IBM?

Security Access Manager for Enterprise Single Sign-On is part of a broad portfolio of threat-aware identity and access management solutions from IBM. These solutions are designed to help clients manage and secure identities as a key line of defense across multiple perimeters, providing secure online access in mobile, cloud and social environments. As a result, organizations can improve identity assurance, facilitate compliance, and reduce operational costs by enforcing secure user access to data, applications and infrastructure across the extended enterprise.

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 solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
November 2013

Please Recycle

TID10298-USEN-05