IBM Security Access Manager for Web

Secure user access to web applications and data

Highlights

- Implement centralized user authentication, authorization and secure session management for online portal and business initiatives
- Protect enterprise-wide web applications against advanced threats with the ability to scale to tens of millions of users
- Deliver consistent web single sign-on and sign-off across heterogeneous web applications and services, including IBM® WebSphere®, Microsoft and SAP
- Choose either a hardware or virtual appliance form factor for faster time to value and higher return on investment
- Provide context-aware access control enforcement via integration with IBM Security Access Manager for Cloud and Mobile[1]

Advanced web threats and increased incidence of web fraud are compelling organizations to seek improved solutions for managing user access and securing web applications. IBM Security Access Manager for Web (formerly IBM Tivoli® Access Manager for e-business) can help organizations address the growing incidence of advanced web threats and risks associated with mobile, social and cloud access while complying with security regulations. Security Access Manager for Web provides security-rich access management that enables employees, customers and partners to safely access online resources.

Security Access Manager for Web combines user access and web application protection into a highly scalable user authentication, authorization and web single sign-on (SSO) and sign-off solution. The product includes a reverse proxy that can be placed in front of web applications to centrally manage security threats. Alternatively, authorization and authentication plug-ins can be added directly into the protected web server or application servers. From any of its flexible enforcement configurations, Security Access Manager for Web provides a single point of flexible authentication, authorization and secure session management, making it easy to enable policy-driven, advanced protection for your applications.

Security Access Manager for Web integrates with online business applications out of the box for highly secure, unified and personalized online business experiences. The software's scalable reverse proxy acts as an identity firewall. The authentication, authorization and administration interfaces simplify integration with common application platforms to help you secure access to business-critical applications and data spread across the extended enterprise.

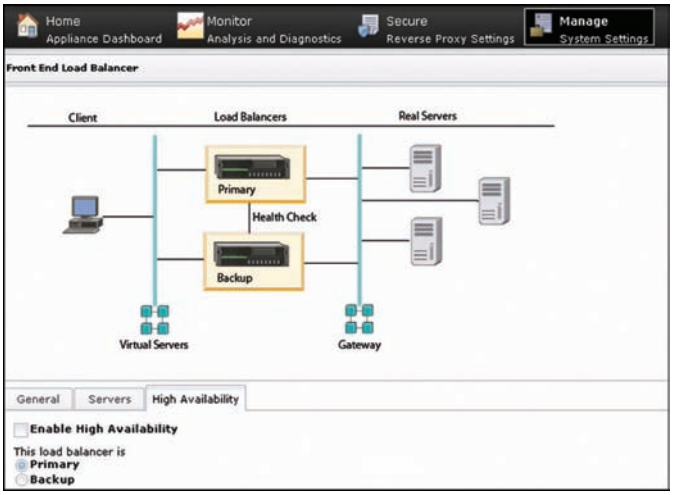
Adding IBM Tivoli Federated Identity Manager Business Gateway (with support for OAuth 1.0 and 2.0) to your environment can provide additional business-to-customer authorization capabilities. The integrated solution provides federated SSO across business affiliates, which can help increase user productivity and reduce password management costs. The solution's risk-based access enforcement services can more precisely identify the risk associated with anytime, anywhere mobile access to enterprise systems.

Simplify operations with highly configurable appliances

Security Access Manager for Web is offered as a virtual appliance for the reverse proxy (WebSEAL) component. The virtual appliance offers a standalone-mode option through the integrated policy server and local user registry. In addition, an integrated front-end load balancer provides high availability and workload distribution to the virtual appliance for smoother operation.

Security Access Manager for Web is also available as part of the IBM Security Web Gateway Appliance. This appliance provides access, authentication and session management for web applications, as well as protection from external threats. Highly scalable and configurable to support a wide variety of application environments, the Security Web Gateway Appliance serves as a proxy-based solution located between users and application servers. Security Web Gateway Appliance provides a web-based, graphical Local Management Interface (LMI), which enables users to easily configure the appliance and reverse proxy. The LMI also provides a dashboard that enables administrators to view the overall health of the appliance.

Security Access Manager for Web virtual and hardware appliances help protect web applications against vulnerabilities such as cross-site scripting, SQL injection and other threats. These appliances contain the IBM Security Intrusion Protection Protocol Analysis Module. Powered by IBM X-FORCE® vulnerability research and development, this module can be configured to scan incoming and outgoing HTTP and HTTPS requests for threats.



The IBM Security Web Gateway Appliance displays how high availability and workload distribution for the virtual appliance is provided by an integrated front-end load balancer.

Enjoy significant ease of use in a massively scalable solution

To manage users and groups as well as related access policies, Security Access Manager for Web offers a web-based administration tool. Administrators can leverage the tool to delegate application management and security administration where appropriate.

The centralized reverse-proxy based architecture and authentication services of Security Access Manager for Web can be provided to Java applications, ASP.NET applications and C/C++ applications for simplified enterprise-wide deployment. Security

Access Manager for Web supports many open industry standards and common IT operational deployment requirements, including:

- Lightweight Directory Access Protocol (LDAP) for storing user and group information plus supported user directories such as IBM Tivoli Directory Server (included in the product license), Oracle Directory Server Enterprise Edition, Novell eDirectory and Microsoft Active Directory
- Meta-directory implementations, including IBM Tivoli Directory Integrator, which helps synchronize user information across numerous registries, directories, databases and other repositories without adding yet another repository to your IT environment
- X.509 V3 client certificates for strong authentication to web-based resources; support for many certificate providers, including VeriSign and Entrust
- Mutually authenticated and confidential component interactions through Secure Sockets Layer (SSL) or Transport Layer Security (TLS)
- Integration with existing identity management systems, such as IBM Security Identity Manager, for importing users and roles, synchronizing passwords between the two products and enabling cost savings through integrated user provisioning and lifecycle management
- Integration with IBM WebSphere DataPower® service-oriented architecture (SOA) appliances for seamless SSO and user session management for Web 2.0 and Web Services environments
- Upgrading to Tivoli Federated Identity Manager for federated SSO and business-to-consumer user self care to expand user access to on- and off-premises applications, Software as a Service and cloud-based services

Protect user access to web applications and services

Security Access Manager for Web can manage and enforce user access to a wide variety of web applications and services, from SSO to more highly scalable application security infrastructure deployments. It enables organizations to cope with the growth and complexity of new application deployments and the escalating costs associated with securing large numbers of web applications across the enterprise. Security Access Manager for Web can help:

- Simplify the implementation of consistent security policies across a wide range of web and application resources; it centrally manages access control policies for numerous enforcement points by placing a reverse proxy in front of web applications, or through authorization and authentication plug-ins directly into web or application servers
- Secure the interaction of authorized users with web applications and servers to deliver a secure and unified business experience
- Safeguard user access to business-critical applications and data spread across the extended enterprise, allowing highly available, scalable transactions with partners, customers, suppliers and employees

Implement policy-driven web access management and enforcement

Security Access Manager for Web enables users to define comprehensive web access control policies and enforce security controls based on access control lists—giving employees, partners, suppliers and end users role-based access that is appropriate to each user's responsibilities. You can group users and assign permissions to groups, thereby simplifying administration of access control across multiple applications and resources.

Security Access Manager for Web provides both HTTP reverse proxy and web server plug-in mechanisms to suit a broad variety of web security infrastructures. Compared to the web server plug-in approach, this highly secure, advanced reverse proxy model helps minimize overall hardware requirements and reduce application development and maintenance costs.

Improve web security at the application level

Security Access Manager for Web addresses issues related to securing applications against common threats and vulnerabilities. As organizations open their environments for user access to corporate and Internet applications, the need to secure access and improve web security becomes paramount. The Security Access Manager for Web reverse proxy acts as an identity firewall to support secure deployments of web applications and works with IBM Security AppScan® to address key application vulnerabilities. Security Access Manager for Web can help remediate these vulnerabilities once they are detected by creating a secure, persistent user-to-application tunnel and providing stronger authentication and session management support for suspected applications. Security Access Manager for Web also contains an Internet Content Adaptation Protocol client that enables integration of its reverse proxy component with a data loss prevention or malware scanning service.

Increase scalability and performance

To help you achieve highly scalable deployments, Security Access Manager for Web supports modular proxy-based implementation, integrates with commercial load balancers and performs intelligent load balancing over replicated servers. It supports tens of millions of users and is proven to scale to hundreds of millions of users. It also takes advantage of SSL accelerator card technology, and it provides a failover capability that enables automatic switchover to backup web servers. To further enhance scalability, configurable administrative domains make it possible to support multiple instances of the reverse proxy components (WebSEAL) on a single directory/LDAP server. The domains also ease replication across the deployment lifecycle and help configure clustering support across multiple WebSEAL instances.

Furthermore, Security Access Manager for Web helps you deliver enhanced session management to keep track of what users are doing—even across multiple concurrent sessions. When users log out once, the software can log them out everywhere to avoid concurrent logons. The software can also enforce policies about inactivity timeouts and other options across multiple enforcement points. The virtual appliance also contains a front-end load balancer with configurable scheduling algorithms, enabling you to deploy your web servers and applications in a configuration that is highly scalable and easy to deploy and manage.

Security Access Manager for Web includes a centralized session management service that can improve performance in several ways:

- The number of sessions users create can be limited on a policy basis, so that new login requests will be blocked once the maximum number has been reached.
- A dynamic configuration feature eliminates session management server restarts.
- High availability is built in by allowing multiple session management server instances via IBM WebSphere Application Server Network Deployment.

Deliver highly secure, unified user experiences

IBM works with leading application providers to offer and maintain out-of-the-box integration with third-party software solutions. With authentication and access control services for online business and enterprise applications and resources, you can secure customer, supplier, employee and partner connectivity across:

- Web servers
- XML and web services
- User repositories
- Platform and traffic management
- Directory services
- J2EE-based application servers
- XML firewalls and gateways

- Ajax-based rich Internet applications
- A growing list of industry-leading web server plug-ins and applications including:
  - Apache Tomcat
  - JBoss
  - CA eTrust Directory
  - IBM Worklight
  - IBM Cognos® Business Intelligence
  - IBM Content Manager
  - IBM FileNet® P8 Platform
  - IBM Lotus® Domino® and IBM Lotus Sametime®
  - Documentum eRoom and Webtop
  - Microsoft .NET, Exchange, Internet Information Server, Office Communications Server and SharePoint
  - Oracle Database, eBusiness Suite, Internet Directory, PeopleSoft and WebLogic Server
  - SAP NetWeaver ABAP and Java, Internet Transaction Server
  - SecurIT
  - Siebel
  - Sun ONE Web Server

Security Access Manager for Web accommodates a broad range of possible user authentication mechanisms, including user IDs and passwords, client-side certificates, risk-based authentication with soft certificates, tokens, biometrics, mobile and wireless identities, and smart cards for physical and network access.

The software can also designate the authentication levels required for access to protected resources and enforce a "step-up" policy in which users must provide the next level of authentication. The authentication mechanism is completely configurable and can also be extended internally. Plus, an external authentication interface enables strong authentication requests to be offloaded to an external server. You can use this feature to enable:

- Interaction with users during multi-factor authentication requests
- Authentication checking against multiple user repositories (directory chaining)
- Separation of policy and user repositories
- Many other types of external, third-party strong authentication integration, including risk and adaptive solutions

About IBM Security Systems software

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 Security Access Manager for Web at a glance	
Platform support for reverse proxy component (WebSEAL) and infrastructure*	• IBM AIX® • Sun Solaris on Sun SPARC • Microsoft Windows Server • SUSE Linux Enterprise Server for x86_64 and IBM System z® • Red Hat Enterprise Server for x86_64 and System z
Other support	• Mozilla Firefox and Microsoft Internet Explorer web browsers

* The product documentation and release notes can be found in the IBM Security Product Information Center: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp
IBM customers can view the latest platform support matrix at: http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.jsp

Why IBM?

IBM Security access management solutions provide centralized authentication, policy management and access control services for web resources, systems and hosted applications. Now you can more securely manage access to critical applications and data, while providing your users with fast, convenient access to the information they need. IBM has also extended user access protection to mobile and cloud environments. Federated SSO, user authentication and context-based access management for mobile devices help prevent users from inadvertently exposing your sensitive IT assets in an insecure environment.

IBM Security Access Manager for Web enables you to enforce security policies over a wide range of web and application resources. It can help you address the growing incidence of advanced web threats and risks associated with mobile, social and cloud access and demonstrate compliance with security regulations. It can help simplify the management of web application environments, control escalating management costs and address the difficulties of implementing security policies across a wide range of web and application resources. With Security Access Manager for Web, you can manage and enforce policy-based access control and web security across the extended enterprise and support highly available, scalable transactions with partners, customers, suppliers and employees.

For more information

To learn more about IBM Security Access Manager for Web, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

[1] The IBM Security Access Manager for Cloud and Mobile software solution comprises IBM Tivoli Federated Identity Manager Business Gateway and IBM Tivoli Security Policy Manager.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2012

Please Recycle

TID14016-USEN-02