IBM Security Access Manager

Take back control of access management with an integrated platform for web, mobile and cloud

Highlights

- Protect critical assets with risk-based and multi-factor authentication
- Secure consumer identities and deliver convenient access experiences at scale
- Facilitate a secure application programming interface (API) ecosystem by enabling user authentication
- Unify access control and security between on-premises and cloud environments
- Manage hybrid identity-as-a-service deployments via pre-integration with IBM® Cloud Identity Connect
- Enforce mobile access control policies that integrate with mobile device management, application development and risk detection solutions
- Simplify web and mobile user experiences with single sign-on (SSO)

As organizations undergo digital transformation, nearly every part of a business is now—or soon will be— available digitally. The majority of businesses today must offer digital experiences tailored to their users that are available across a wide range of devices—from traditional PCs to mobile and an ever-growing list of other connected gadgets. Access management is the key to delivering personalized experiences and maintaining security in the rapidly evolving digital world.

IBM® Security Access Manager allows organizations to deliver the access management required to embrace this digital transformation without sacrificing security. It helps enforce risk-based access policies that provide minimal friction during authentication when the user is known and stronger, multi-factor authentication if the risk is elevated. It enables enforcing security polices consistently across multiple channels, letting users interact with the devices they choose with a consistent experience.

IBM Security Access Manager is a modular platform for web, mobile, and cloud access management, multi-factor authentication, risk-based authentication, web-application protection, and identity federation. Its integrated appliance form factor allows for flexible, automated deployment on-premises or in the cloud. This includes taking advantage of Docker container orchestration frameworks like Kubernetes.

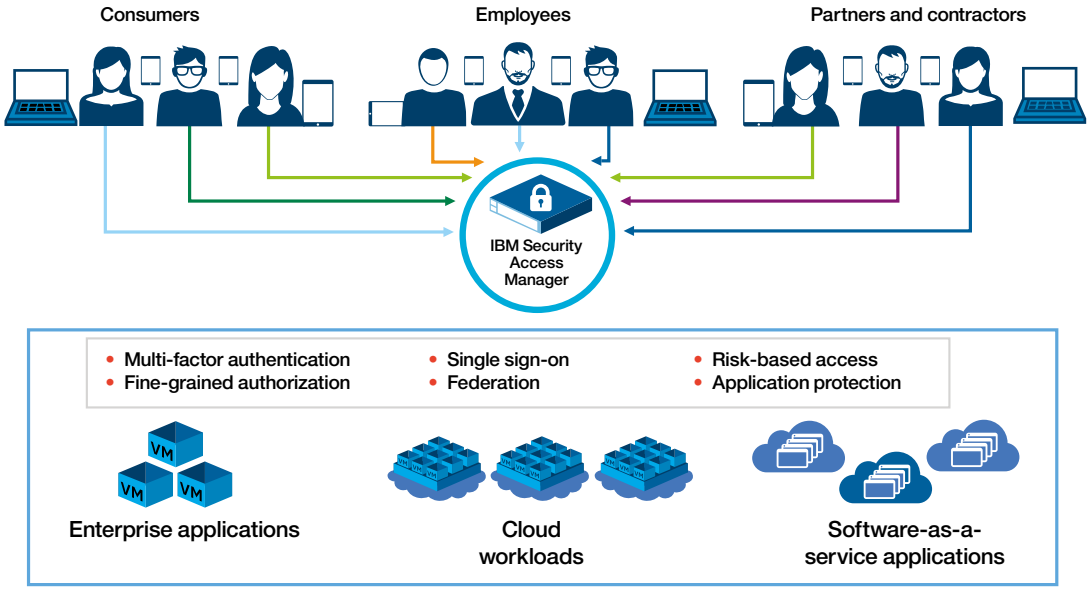
Authentication methods are always changing. Integrations available on IBM Security App Exchange allow administrators to easily integrate third-party authentication mechanisms—such as biometrics and hardware tokens—from pre-certified business partners into IBM Security Access Manager, without custom coding.

IBM Security Access Manager is delivered using a security appliance designed to secure user access and protect content against common web attacks. Key benefits include:

- A centralized integration platform for user access security, allowing organizations to avoid having to modify application code when access or authentication requirements change
- Better protection from advanced threats including the top 10 web application risks documented by the Open Web Application Security Project (OWASP)
- Enhanced user productivity with secure user access to web and mobile applications through SSO, session management, multi-factor authentication and context-based access policy enforcement
- A low-friction, security-focused, consumer identity infrastructure to facilitate user adoption of digital channels
- Federated SSO, which helps enhance user productivity and facilitates trust through the delivery of SSO across separately managed domains, including easily configurable connections to popular software-as-a-service (SaaS) applications
- Integration with IBM MaaS360® and IBM Trusteer® solutions for providing the risk context used in access decisions

IBM Security Access Manager is structured as a platform with two optional add-on modules. All required code is included with the base appliance; users enable an add-on module's functionality by entering the appropriate activation keys. This allows users the flexibility to more easily support multiple usage scenarios while minimizing the additional software required.

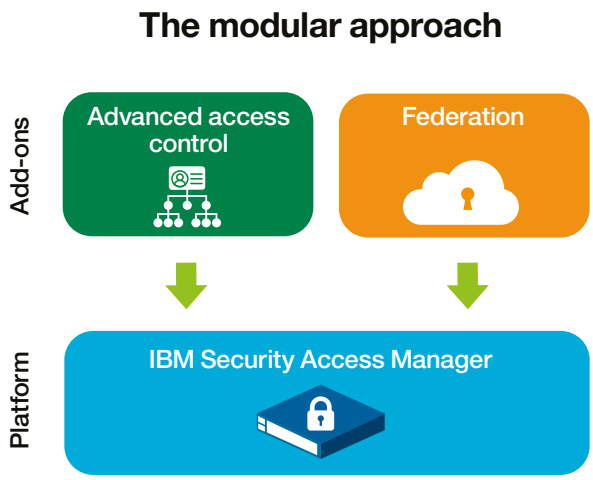
Take back control of access management



One platform offering, with easily consumable add-on modules

IBM Security Access Manager is a modular, integrated access management appliance that helps secure access to web, mobile and cloud applications and APIs. The integrated appliance form factor allows for easier, more flexible and automated deployment and maintenance on-premises or in the cloud. It is offered as a physical appliance, a virtual appliance that runs on a number of popular hypervisors, or as a Docker image.

According to the OWASP top 10 list of web vulnerabilities, external hackers use SQL injections, broken authentication and cross-site scripting (XSS) as common methods to gain unauthorized access into web applications.[1] Utilizing research from the IBM X-Force® threat research team, IBM Security Access Manager delivers the ability to help block OWASP top 10 web vulnerabilities before they reach the targeted application.



IBM Security Access Manager Advanced Access Control Module

Identity fraud, bring-your-own-device (BYOD) initiatives and increasing regulatory requirements for authentication are increasing security challenges for enterprises undergoing a digital transformation.

In the face of these challenges, it is important to provide increased intelligence to authentication and authorization. The Advanced Access Control Module for IBM Security Access Manager allows the solution to use detailed contextual information (for example, geographic location, device fingerprint, browser type or application data) in assessing the risk of a user when making access decisions.

Additional key capabilities of the Advanced Access Control Module include:

- Multi-factor authentication with the IBM Verify mobile application for authentication, supporting fingerprint verification on compatible devices as well as time-based, email and SMS one-time password mechanisms
- IBM Mobile Access SDK for building authentication into custom-developed mobile applications on the Google Android and Apple iOS platforms
- Risk scoring engine to enforce context-aware authorization using information about the users, their mobile devices and other transactions-based information
- More secure mobile transactions with a graded level of trust designed to allow and deny access using mobile device fingerprinting, geographic location awareness and IP reputation
- Integration with MaaS360 to enforce corporate security policies when making access decisions for enterprise mobile devices
- Integration with Trusteer solutions, allowing IBM Security Access Manager to use sophisticated indicators of identity, behavior, malware, device and fraud risk in making access decisions
- A graphical policy management interface that supports authoring complex policies

IBM Security Access Manager Federation Module

Collaboration between organizations is a central tenet of business. In some cases, users from collaborating organizations require secure access to each other's applications. And increasingly, internal users need access to externally hosted services, including cloud-based SaaS and business partner applications.

Federated access helps enable these scenarios by delivering a secure, seamless sign-on experience to external applications, helping eliminate the need for providing multiple user IDs and passwords. This may lead to gains in user productivity and user experience, as well as reductions in the cost of administration. In a federated environment, users authenticate once, then obtain access to applications inside and outside their network infrastructure.

The Federation Module for IBM Security Access Manager accelerates an organization's adoption of third-party enterprise SaaS applications by enabling out-of-the-box connectors to popular applications. Using these connectors, the organization can rapidly give users access to an application without creating an additional set of logins. The Federation Module also helps increase security and visibility by linking a user's enterprise identity to the identity at the third-party application provider.

IBM Security Access Manager Federation Module provides key capabilities that include:

- Federated SSO for users across multiple applications
- Support for SAML 2.0 and OpenID Connect protocols for federated access
- Pre-integrated federation connectors to popular cloud applications
- Security token service for identity token validation and mediation

IBM Security Access Manager at a glance	
Physical characteristics of hardware appliance:	• 1U form factor • H x W x D: 44.2 mm x 430.2 mm x 650 mm (1.74 in. x 16.9 in. x 25.6 in.) • Management interface: 10/100/1000 • Application interface: 10/100/1000 (IPv6 supported) • Supported physical media types: RJ-45 • Redundant power supplies • Solid-state storage • 100 – 240 V, full range
Machine specifications for hardware appliance:	• Intel Core E3-1275 processor • 64 GB memory • 800 GB solid-state drive • 6 network ports*
Platform support for virtual appliance:	• VMware ESX environment • IBM Cloud Bare Metal • Amazon Web Services (AWS) • Citrix XenServer • Kernel-based Virtual Machine (KVM) • Microsoft Azure • Microsoft Hyper-V • Docker
Supported web browsers:	• Google Chrome • Microsoft Edge • Mozilla Firefox
Performance data:†	• Throughput: Up to 1.3 Gbps or 42,000 requests per second • Latency: Down to 0.8 ms • Large-packet throughput: Up to 1.3 Gbps • Small-packet throughput: Up to 42,000 requests per second • Authentication throughput: Up to 2,400 logins per second

Why IBM?

IBM Security solutions are trusted by organizations worldwide for identity and access management. The proven technologies enable organizations to protect their most business-critical resources from the latest security threats.

Going beyond traditional point solutions, IBM Security Access Manager integrates with many other IBM Security solutions to provide next-generation access management for a multi-perimeter world. Organizations can use IBM QRadar® Security Intelligence Platform to get actionable insights that can help them stay a step ahead of new types of attacks—while helping facilitate regulatory compliance. Out-of-the-box consumption of context data from IBM Trusteer Mobile SDK and IBM MaaS360 Secure Mobile Browser enables users to create comprehensive access policies that include fraud and malware detection without modifying applications. IBM Security Access Manager also provides built-in support for MaaS360 developed mobile applications by enabling seamless authentication and authorization of users along with risk-based access enforcement.

As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

For more information

To learn more about IBM Security Access Manager and start your 90-day, no-cost trial, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/identity-access-management

About IBM Security solutions

IBM Security offers one of the most advanced portfolios of enterprise security products and services, to help organizations holistically protect their people, infrastructures, data and applications. Backed by world-renowned X-Force research and development, IBM Security offerings cover identity and access management, endpoint management, network security and more, and with solutions 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 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2018

Please Recycle

* Two of these ports are dedicated to appliance management.

† Performance data quoted for IBM Security Access Manager for Web is based on testing with HTTP and HTTPS traffic that is intended to be reflective of typical live traffic. Environmental factors such as protocol mix and average packet size will vary in each network, and measured performance results will vary accordingly. IBM Security Access Manager for Web throughput was determined by pushing traffic through the appliance and measuring how much throughput was achieved with zero packet loss and low response times. For benchmark testing, IBM Security Access Manager for Web appliances were configured with worker-threads = 300 and maximum-cached-persistent-connections = 300; large-file throughput was measured with multiple clients requesting 50 Kb.

[1] "IBM Security Access Manager: Web Application Protection, Performance, Federation & Risk-Based Access Evaluation," *Tolly Enterprises, LLC*, Commissioned by IBM Security, June 2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03120USEN