IBM MaaS360 Identity Management

Extending cognitive unified endpoint management with built-in cloud-based identity tools

Today’s enterprise IT teams oversee a complex web of hardware, software, privacy, security and networking needs. And the requirements for managing enterprise end-user device security continue to evolve; it’s been a long time since IT only had to keep track of hardware serial numbers or make sure passwords were up to date.

Contemporary responsibilities are wide-ranging: curating and deploying apps, enabling content access, maintaining shared resources, protecting data by containing leaks, watching for suspicious or anomalous data access, and sensing and responding to attacks and breaches. Complicating these requirements, today’s administrators must support users with a growing inventory of smartphones, tablets, laptops, desktops, wearables and Internet of Things (IoT) devices.

Perhaps the most critical task, though—one that underlies nearly every other aspect of enterprise IT—is authenticating and authorizing users. Provisioning new users, making apps and content available, guarding users from security breaches, and keeping employees happy with timely updates all require one thing: knowing that users are who they say they are.

IBM® Cloud Identity is a new identity-as-a-service (IDaaS) capability that extends the IBM MaaS360® with Watson™ cognitive UEM platform. IBM MaaS360 Identity Management gives administrators robust tools to manage identity for a full range of endpoints while providing users one-touch access to the apps and data they need.
Enterprise security starts with knowing your users, wherever they are

In the modern enterprise, it is critical to have secure, well-managed mobile access as well as secure access for static endpoints. MaaS360 Identity Management brings easy-to-use identity and access management (IAM) to UEM, helping MaaS360 administrators tackle their biggest, most critical device management needs—whether they are conducting one-time or ongoing administrative tasks.

From the very start of the data-access lifecycle, MaaS360 Identity Management helps smooth on-boarding for new users, provide SSO capabilities, and support built-in policy creation and enforcement tools. Access policies can be designed strategically based on business roles, enabling the IT team to define appropriate permissions even before on-boarding a new employee.

Identity federation, coupled with pre-populated connectors for popular SaaS apps such as Salesforce and Box, creates a smooth path between mobile users and the cloud-based apps they need for work—whether from a laptop, tablet or smartphone—while minimizing the need for new passwords. This federation occurs whether the device is owned by the enterprise or the employee.

---

IBM Cloud Identity: The full spectrum of identity as a service

Transform the enterprise with full identity and access management (IAM) from the cloud

Bridge from on-premises to cloud with born-in-the-cloud identity as a service (IDaaS)

Converge mobile device and identity management

Unify IAM between IBM and third-party cloud applications

IBM Cloud Identity, integrated with MaaS360 Identity Management, gives users simple, secure access to data resources and business-critical SaaS apps with prebuilt connectors.
**Consolidate real-world apps and security needs**

In an effort to support increasingly complex device and software ecosystems, the UEM capabilities offered by MaaS360 with Watson cover a wide range of devices and operating systems, with support for Apple iOS, Apple macOS, Google Android, and Microsoft Windows, including Microsoft Windows 10 and Microsoft Windows 10 Mobile. These capabilities also work with third-party identity management solutions.

Establishing identity is a crucial part of the security process, especially for mobile users—but it’s not the only part. MaaS360 helps administrators know relevant details, such as whether a user is connecting from a device that is fully patched against known security flaws, or whether the device’s operating system is up to date. MaaS360 Identity Management helps organizations implement conditional access, based on factors from user behavior to time of access, to restrict a user’s access. With conditional access, a user can be allowed to access a limited set of resources, or challenged with additional requirements for authentication, rather than simply accepted or rejected. With IBM Watson, MaaS360 uses risk data from IBM X-Force® Exchange to help enable conditional access.

Optional multi-factor authentication features—in tandem with conditional access—can further protect user access by requiring step-up authentication factors, including biometric identifiers and out-of-band login confirmation.

**Go beyond blocking access attempts**

One side of security is subtractive: closing ports, blocking malware, restricting users. While this kind of defense is important, the highly-evolved identity tools of IBM Cloud Identity, which powers MaaS360 Identity Management, instead help authorized users gain easy access to apps and content. In addition to offering secure, federated connectivity to enterprise data resources such as shared databases, the solution enables single-touch access to a user-friendly catalog of administrator-approved apps. Users aren’t burdened with separate accounts for these apps, and they aren’t stuck managing a password for each.

For software needs beyond the catalog of vetted apps, a self-service utility lets users easily request permission to add new apps. Device enrollment, too, can be approached with user-centric self-service tools. This flexibility helps turn identity management into a source of information administrators can use to understand the real-world needs of employees, and saves time for IT administrators. Administrators can save even more time by delegating app access management to line-of-business managers.

**Why IBM?**

While alternative solutions provide incomplete coverage across computing platforms, MaaS360 delivers cognitive UEM across all endpoint types including smartphones, tablets, laptops, desktops, devices designed for the IoT, ruggedized devices and wearables. And while competing solutions provide incomplete coverage of Windows devices, MaaS360 can support the full spectrum, from Microsoft Windows XP SP3 to Windows 10.

Traditional mobile device management systems were built in a simpler time for tactical purposes and disparate mobility projects. With the industry’s first cognitive UEM platform, MaaS360 delivers a single, strategic productivity and security solution with powerful insights and analytics from Watson technology, integrated IAM capabilities with IBM Cloud Identity, IBM X-Force Exchange threat intelligence, and cloud-sourced benchmarking data from its platform to help drive your organization’s digital business transformation.
For more information
To learn more about MaaS360 Identity Management, MaaS360 with Watson and IBM Cloud Identity, contact your IBM representative or IBM Business Partner, or visit: ibm.com/maas360

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 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 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

© Copyright IBM Corporation 2017
IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2017

IBM, the IBM logo, ibm.com, MaaS360, Watson, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle