IBM MaaS360 Laptop Management for Windows

**Protect laptops, desktops, ultrabooks and tablets from a single screen**

**Manage Windows devices in the Cloud**

IBM® MaaS360® Laptop Management for Windows delivers a self-service, cloud-based solution that makes it easier and faster than ever for IT to support the entire Windows PC lifecycle.

It streamlines the process of securing today’s expanding suite of Windows computing devices, all from a single window – the same portal used for Mobile Device Management (MDM).

MaaS360 gives you an industry-leading solution for a unified approach to manage the many devices in your IT environment, from Windows devices to Mac laptops, as well as smartphones and tablets powered by iOS, Android, Windows Phone and BlackBerry.

**Just as simple as managing mobile devices**

Simple, over-the-air (OTA) enrollment (just like MDM) and a unified, consistent workflow, independent of device form factor, provide an easy-to-use portal for IT administrators.

MaaS360 Laptop Management for Windows delivers usable information across your laptops, desktops, ultrabooks and tablets. By collecting and correlating endpoint data from these devices, you get exceptional visibility into hardware and installed software, missing patches, outdated anti-virus signature files and so much more.

Mobility Intelligence™ dashboards and reports, including My Alert Center, help you to comply with corporate standards and government regulations.

---

**Key benefits**

- Make sure patches, third-party and software anti-virus signature files are kept up to date
- Push Microsoft patches and application updates to devices, independent of their location
- Push software to devices, independent of their location
- Locate the device
- Shut down or restart the device
- Stop/Start/Restart a service
- Send messages or lock devices
- Wipe the hard drive if the device is lost or stolen
- Demonstrate compliance for audits
- Consistent, unified workflows across device form factors
- OTA device enrollment
Gain visibility
MaaS360 Laptop Management for Windows shines a light onto hardware and software on Windows laptops, desktops, ultrabooks and tablets. A software agent runs continuously on managed devices for reporting and analysis.

- Hardware inventory
- Software inventory including application types (Win32 and Windows Store applications)
- Status information about security applications:
  - Anti-virus
  - Personal firewall
  - Anti-spyware
  - Data encryption
  - Backup and recovery
- Operating system (OS) details
- OS patch levels and information, including file size, severity level and how many users are missing each one
- Updates for Windows applications, i.e., Java and Adobe
**Take control**

MaaS360 Laptop Management for Windows extends visibility to help IT manage Windows devices across the organization. Through a centralized console, IT managers can perform a number of actions with unified workflows.

- Enroll devices over-the-air (OTA)
- Identify, schedule and install outstanding OS patches
- Locate, lock, shut down or restart the device
- Choose a service then stop, start or restart it
- Distribute packages with documents and apps to increase employee productivity while keeping your data safeguarded
- Send a message to the user

**Patch and application update distribution**

MaaS360 Laptop Management for Windows highlights the outstanding updates for Microsoft patches and security updates, along with updates for commonly used applications. It provides the ability to distribute and apply the updates to your devices from the same browser, whenever the device is connected to the Internet.

Payloads include:

- MSFT patches
- iTunes updates
- Adobe updates
- Operating systems
- Software inventory

---

*Figure 3: Example of the available actions for a Windows laptop*

*Figure 4: Examples of patch distribution settings*
Protect your Windows devices
MaaS360 supports Windows-based laptops, desktops and ultrabooks, in addition to smartphones and tablets. These types of devices can be managed through a single portal accessed through a web browser.

Build on the Cloud
Because MaaS360 is a cloud-based solution, it does not require you to install servers, deal with complex configurations or provide on-going maintenance. Deployment is quick and easy, and in just a few clicks you get instant visibility and control.

With MaaS360, IT can support and manage enterprise mobile computing devices, even when they are not connected to the corporate network.

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 performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on the specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM product and programs.

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.

Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 systems and products are immune from the malicious or illegal conduct of any party.