IBM Security
Data Sheet

IBM MaaS360 Secure Mobile Browser

Unlock your enterprise data and reduce vulnerabilities from risky websites

Key benefits

- Deploy a robust web browser that protects corporate data and increases productivity for iOS, Android and Windows Phone devices
- Use a centralized management platform that provides your employees with protected access to corporate intranet sites and networks with no VPN required
- Control the mobile internet experience through granular security policies
- Prevent attacks and malware from malicious websites
- Overcome your mobile web challenges that cover a wide range of business needs

Control access to the Web on mobile devices

IBM® MaaS360® Secure Mobile Browser gives your employees protected access to corporate intranet sites and networks with no VPN required.

You can also reduce the vulnerability your mobile devices have to risky websites that may contain malware, violate Human Resources (HR) policies or simply waste your users' precious time.

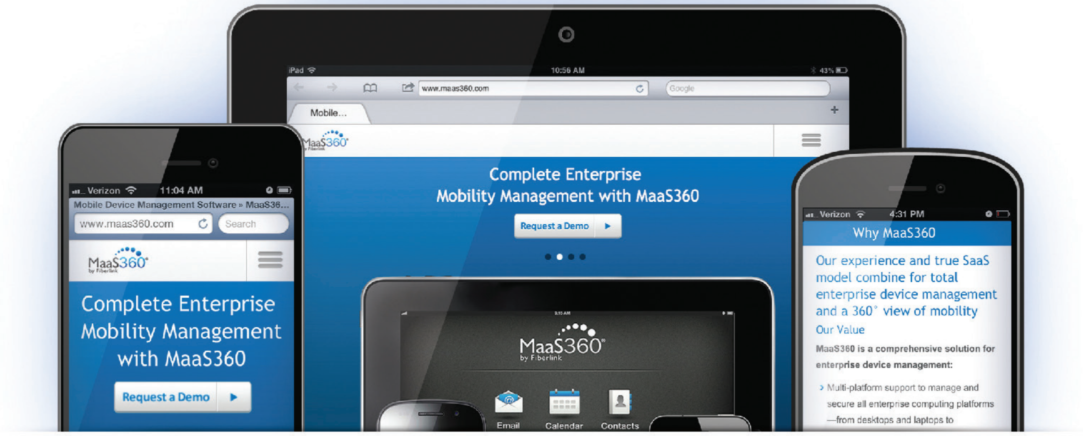
With MaaS360 Secure Mobile Browser, organizations can specify categories of content that they want to prevent users from accessing, including social networking sites, download sites, and explicit sites. It has 60+ categories of filtering criteria, with millions of URLs categorized.

Specific URLs can be set to filter access to appropriate websites. Through IBM® MaaS360® Device Management policies and blacklisting, native or third-party browsers can be disabled.

MaaS360 Secure Mobile Browser can send emails to administrators in near real time, alerting them of attempts to access these sites.

With MaaS360 Secure Mobile Browser you get:

- A cloud-based, centralized management platform
- Easy-to-use policy creation and remote over-the-air (OTA) assignment
- Protected access to corporate intranet sites and network without device VPN
- Mobilization of SharePoint, JIRA, internal wikis, legacy ERP systems and more
- Continuous protection via interception of browser traffic
- Restriction of URLs by category and allowing access to specific URLs
- Blocking of known malware and malicious websites using a scanning engine and reputation database
- Disabling of cookies, printing, file downloads, and copy and paste
- Customizable blocking, near real-time notification, exception and reporting options



Our experience and true SaaS model combine for total enterprise device management and a 360° view of mobility

Our Value

MaaS360 is a comprehensive solution for enterprise device management:

› Multi-platform support to manage and secure all enterprise computing platforms —from desktops and laptops to

Figure 1: Example of MaaS360 Secure Mobile Browser on various mobile devices

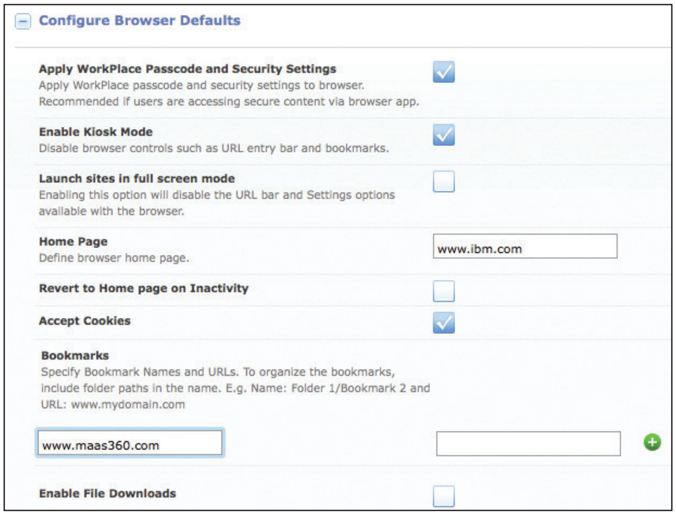
Control the mobile internet experience

MaaS360 Secure Mobile Browser is a robust web browser for smartphones and tablets. It has an intuitive user interface that includes tabbed browsing, bookmarks, search, share and history features. There are many ways to build on MaaS360 Secure Mobile Browser in your organization to reduce the vulnerability of your users' mobile devices, prevent violations to HR policies or focus user attention.

- **Shared healthcare provider devices:** Safeguard patient records and optimize utilization of shared devices by your health workers by focusing on medical reference and point-of-care websites, and by providing access to intranet sites without needing a device VPN connection.
- **Dedicated retail point-of-sale (POS) devices:** Improve the productivity of your retail staff and protect on-device data by locking down your POS devices to specific websites for checkout, inventory lookup or web store availability.
- **Shared teaching devices:** Focus student attention by restricting access to explicit websites for shared learning devices in the classroom, a priority for educational institutions to comply with the Children's Internet Protection Act (CIPA) regulations.
- **Hospitality concierge devices:** Increase the efficiency of your hospitality staff by limiting devices to checking in or out, viewing facility amenities and accessing local weather or traffic.
- **Event demo devices:** Boost the utility of your demo staff by allowing access to only a few, select websites at your kiosk.

Browser configuration settings

- Configure as the default browser
- Apply MaaS360 container security policies
- Disable cookies and file downloads
- Restrict copy, paste and printing
- Enable browser kiosk mode
- Set a default home page and custom bookmarks



Configure Browser Defaults

Apply WorkPlace Passcode and Security Settings ☑
Apply WorkPlace passcode and security settings to browser. Recommended if users are accessing secure content via browser app.

Enable Kiosk Mode ☑
Disable browser controls such as URL entry bar and bookmarks.

Launch sites in full screen mode ☐
Enabling this option will disable the URL bar and Settings options available with the browser.

Home Page www.ibm.com
Define browser home page.

Revert to Home page on Inactivity ☐

Accept Cookies ☑

Bookmarks
Specify Bookmark Names and URLs. To organize the bookmarks, include folder paths in the name. E.g. Name: Folder 1/Bookmark 2 and URL: www.mydomain.com

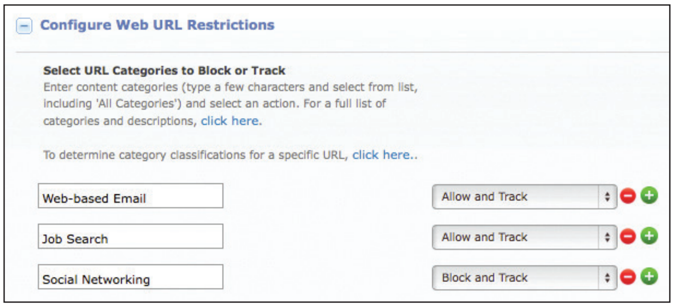
www.maas360.com

Enable File Downloads ☐

Figure 2: Example of the browser settings in the MaaS360 console

Website filter settings

- Select URL categories to allow, block and track
- Choose from 60+ categories with millions of URLs
- Allow exceptions based on the domain name or URL
- Blacklist specific websites



Configure Web URL Restrictions

Select URL Categories to Block or Track
Enter content categories (type a few characters and select from list, including 'All Categories') and select an action. For a full list of categories and descriptions, click here.

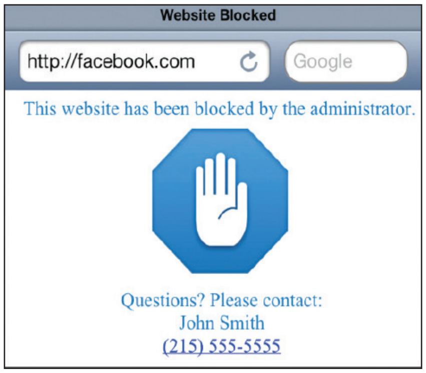
To determine category classifications for a specific URL, click here..

Web-based Email	Allow and Track
Job Search	Allow and Track
Social Networking	Block and Track

Figure 3: Example of website category filter settings in the portal

User and administration notification settings

- Send custom text or HTML notifications to users when they try to access a prohibited URL blocked
- Redirect users to a specific URL when policies are violated
- Send a notification to your administration when a user is blocked
- Define how many times a user can be blocked before the administration notification is sent



Website Blocked

http://facebook.com

Google

This website has been blocked by the administrator.

Questions? Please contact:
John Smith
(215) 555-5555

Figure 4: Example of a user notification in the browser when a website is blocked

Device-specific and company reports

- View summary, graphical reports of category and domain blocked and tracked history
- Access detailed reports of specific device block and tracked domain history

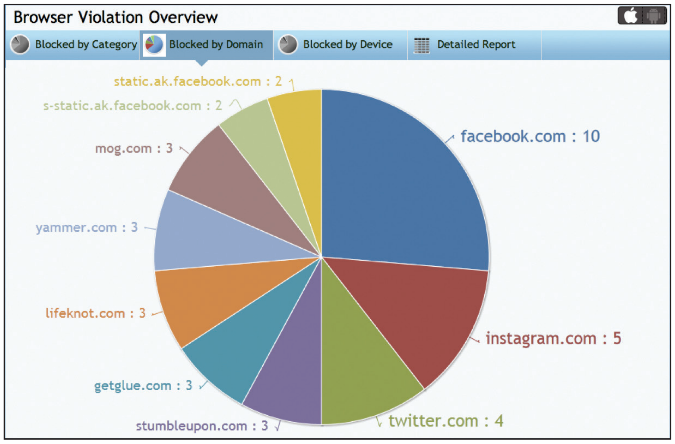


Figure 5: Example of device browser violations report

Proactive web security

MaaS360 Secure Mobile Browser protects data and increases productivity by controlling access to public websites and corporate intranet sites for iOS and Android devices.

It restricts or allows users to access websites based on categories you specify, including:

- Advertisements and pop-ups
- Anonymizers
- Botnets
- Chat
- Criminal activity
- Dating and personals
- Download sites
- Entertainment
- Explicit
- Forums and newsgroups
- Gambling
- Games
- Hacking
- Image sharing
- Instant messaging
- Malware
- News
- Peer-to-peer
- Phishing and fraud
- Shopping
- Social networking
- Sports
- Streaming media and downloads
- And more

Enjoy ease of management:

- Flexible policy creation framework
- Customizable policy assignment
- Integration with MaaS360 Mobile Device Management for optimized control (optional)

For more information on IBM MaaS360, and to start a no cost 30-day trial, visit www.ibm.com/maas360

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2016

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.