



关键优势

- 部署稳健的网络浏览器，以保护企业数据并提高 iOS、Android 和 Windows Phone 设备的生产效率
 - 使用集中管理平台为员工提供受保护的企业内部网站和网络访问，无需 VPN
 - 通过精细安全策略控制移动互联网体验
 - 防止攻击和来自恶意网站的恶意软件
 - 克服涵盖各种业务需求的移动网络挑战
-

IBM MaaS360 Secure Mobile Browser

释放您的企业数据并减少访问风险网站带来的安全隐患

控制通过移动设备进行的 Web 访问

IBM® MaaS360® Secure Mobile Browser 使您的员工受保护地访问企业内部网站和网络，无需 VPN。

您还可以降低使用移动设备访问风险网站带来的安全隐患，这可能包括恶意软件，违反人力资源 (HR) 政策或仅仅是浪费用户的宝贵时间。

借助 MaaS360 Secure Mobile Browser，组织可以指定他们希望阻止用户访问的内容的类别，包括社交网站、下载网站和具体站点。它有 60 多种过滤条件，将数百万 URL 进行分门别类。

它可以设置具体 URL，以过滤对相应网站的访问。通过 IBM® MaaS360® Device Management 策略和黑名单，可以禁用本机或第三方浏览器。

MaaS360 Secure Mobile Browser 可以近乎实时地发送电子邮件给管理员，提醒他们注意试图访问这些站点的行为。

借助 MaaS360 Secure Mobile Browser，您将获得：

- 基于云的集中管理平台
- 易于使用的策略创建和远程空中传送 (OTA) 分配
- 受保护的企业内部网站和网络访问，无需设备 VPN
- SharePoint、JIRA、内部维客、原有 ERP 系统等的移动化
- 通过浏览器流量拦截实现的持续保护
- 通过类别和允许对具体 URL 进行访问实现的 URL 限制
- 使用扫描引擎和声誉数据库阻止已知恶意软件和恶意网站
- 禁用 Cookie、打印、文件下载、复制和粘贴
- 可自定义的阻止、近乎实时的通知、意外情况和报告选项





图 1: MaaS360 Secure Mobile Browser 在各种移动设备上的示例

控制移动互联网体验

MaaS360 Secure Mobile Browser 是适用于智能手机和平板电脑的稳健网络浏览器。它拥有直观的用户界面，其中包括选项卡式的浏览、书签、搜索、共享和历史记录特性。目前有很多方法可在您组织的 MaaS360 Secure Mobile Browser 上进行构建，以降低用户移动设备的安全隐患，防止违反人力资源政策或集中用户注意力。

- 共享医疗保健提供方设备：通过关注医疗参考和医疗点网站以及在不进行设备 VPN 连接的情况下提供对内部网站点的访问，保护患者记录并优化医务人员共享设备的利用。

- 专用零售销售点 (POS) 设备：将您的 POS 设备锁定到具体网站，以进行结账、库存查找或了解网上店铺的可用性，从而提高零售员工的生产效率并保护设备上的数据。
- 共享教学设备：通过限制教室中共享教学设备对具体网站的访问来集中学生注意力，使遵守《儿童互联网保护法》(CIPA) 的规定成为教育机构的重点。
- 酒店礼宾设备：通过使设备仅能办理入住或退房手续，查看酒店的康乐设施以及访问当地天气或交通情况，来提高酒店员工的效率。
- 事件演示设备：通过在信息亭仅允许访问一些精选的网站来提升您演示员工的效用。

浏览器配置设置

- 配置为默认浏览器
- 采用 MaaS360 容器安全策略
- 禁用 Cookie 和文件下载
- 限制复制、粘贴和打印
- 支持浏览器信息亭模式
- 设置默认主页和定制书签

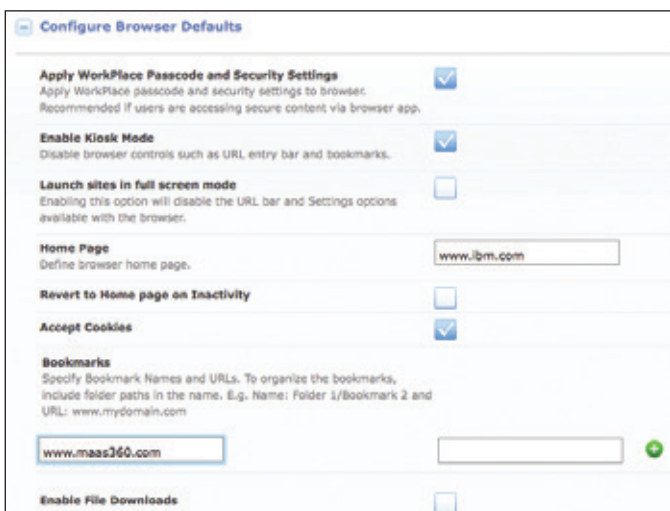


图 2: MaaS360 控制台中的浏览器设置示例

网站过滤器设置

- 选择 URL 类别进行允许、阻止和跟踪
- 从数百万 URL 形成的 60 多种类别中进行选择
- 基于域名或 URL 的允许例外情况
- 将特定网站列入黑名单



图 3: 门户中的网站类别过滤器设置示例

用户和管理通知设置

- 当用户试图访问被阻止的禁止 URL 时，向他们发送自定义的文本或 HTML 通知
- 当违反策略时，将用户重定向至特定 URL
- 当用户被阻止时向您的管理者发送通知
- 定义用户被阻止多少次后才发送管理通知

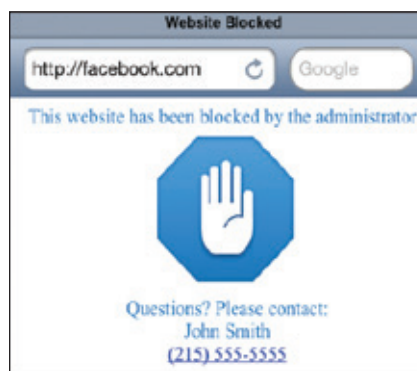


图 4: 网站被阻止时浏览器中的用户通知示例

设备特定和公司报告

- 查看概要、类别的图形报告，以及域名被阻止和被跟踪的历史记录
- 具体设备阻止和被跟踪域名历史记录访问详情报告

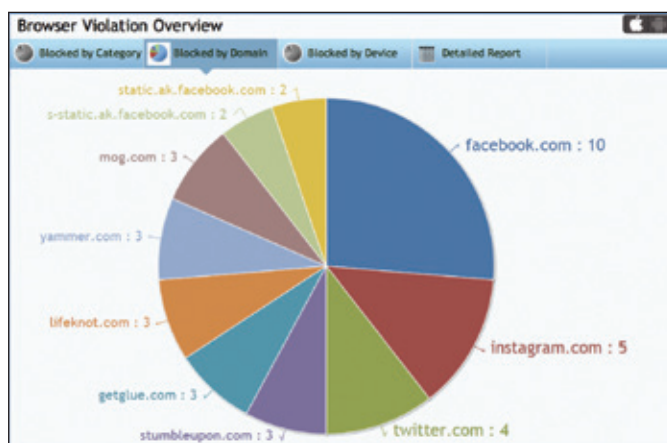


图 5: 设备浏览器违规报告示例

主动的网络安全性

MaaS360 Secure Mobile Browser 通过控制 iOS 和 Android 设备对公共网站和企业内部网站点的访问来保护数据并提高生产效率。

它基于您指定的类别限制或允许用户访问网站，包括告和弹出窗口

- 匿名网站
- 僵尸网络
- 聊天
- 犯罪活动
- 约会和交友
- 下载站点
- 娱乐
- 显式
- 论坛和新闻组
- 赌博
- 游戏
- 黑客
- 图片共享
- 即时消息
- 恶意软件
- 新闻
- 对等网络
- 钓鱼和欺诈
- 购物
- 社交网络
- 体育运动
- 流媒体及下载
- 等等

易于管理：

- 灵活的策略创建框架
- 可定制的策略分配
- 与 MaaS360 Mobile Device Management 集成以实现最佳控制（可选）

如要了解有关 IBM MaaS360 的更多信息并开始 30 天的免费试用，请访问 www.ibm.com/maas360



© Copyright IBM Corporation 2016

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美国印制 2016 年 2 月

IBM、IBM 徽标、ibm.com 和 X-Force 是 International Business Machines Corp. 在全球许多司法辖区的注册商标。BYOD360™、Cloud Extender™、Control360®、E360®、Fiberlink®、MaaS360®、MaaS360® 及设备、MaaS360 PRO™、MCM360™、MDM360™、MI360®、Mobile Context Management™、Mobile NAC®、Mobile360®、MaaS360 Productivity Suite™、Simple. Secure. Mobility®、Trusted Workplace™、Visibility360® 和 We do IT in the Cloud.™ 及设备是 IBM 旗下 Fiberlink Communications Corporation 的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的最新列表在以下网址的“版权与商标信息”处提供：
ibm.com/legal/copytrade.shtml

Apple、iPhone、iPad、iPod touch 和 iOS 是 Apple Inc. 在美国和其他国家/地区的注册商标或商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家/地区的商标。

本文档为初始发布日时的最新文档，IBM 可能随时对其进行更改。IBM 并未在每个开展业务的国家/地区提供所有产品/服务。

所引用的性能数据和客户示例仅供参考。实际性能结果可能会有所不同，具体取决于特定的配置和操作条件。对于与 IBM 产品和程序配合使用的其他任何产品或程序，用户应负责相关的评估与验证工作。

本文档中的信息“按原样”提供，不带任何明示或暗示的保证，包括不带任何适销性、对特定用途的适用性的保证，以及任何不侵权的保证或条件。IBM 产品根据提供这些产品时所依据协议的条款与条件进行保证。

客户负责确保遵守适用的法律和法规。IBM 不提供其服务或产品能确保客户符合所有法律或法规的法律意见、声明或保证。

关于 IBM 未来方向和意向的声明仅表示目标和目的，可能随时更改或撤销，恕不另行通知。

良好安全实践声明：IT 系统安全包括通过防范、检测和响应来自企业内部和外部的不正当访问，从而保护系统和信息。不正当访问可导致信息被更改、销毁或盗用或导致系统被破坏或滥用，包括攻击其他系统。没有任何 IT 系统或产品是完全安全的，而且在防范不正当访问方面，也没有任何单个产品或安全措施是完全有效的。IBM 系统和产品的设计旨在作为全面安全方案的组成部分，其中必然涉及其他操作程序，可能会要求其他系统、产品或服务具有最高的效率。IBM 不保证其系统和产品可免受任何一方的恶意或非法行为影响。



请回收利用