



Основные преимущества

- Разверните надежный веб-браузер, который защищает корпоративные данные и повышает эффективность работы на устройствах iOS, Android и Windows Phone
 - Используйте платформу централизованного управления, которая предоставляет вашим сотрудникам защищенный доступ к сайтам и внутренним корпоративным сетям без использования VPN
 - Контролируйте возможности доступа в Интернет с мобильных устройств, используя детализированные политики безопасности
 - Предотвращайте атаки и заражение вредоносным кодом с мошеннических веб-сайтов
 - Преодолейте проблемы, связанные с работой в Интернете с мобильных устройств, которые охватывают широкий спектр бизнес-потребностей
-

IBM MaaS360 Secure Mobile Browser

Используйте весь потенциал данных вашего предприятия и сократите уязвимости, связанные с опасными веб-сайтами

Управление сетевым доступом на мобильных устройствах

IBM® MaaS360® Secure Mobile Browser предоставляет сотрудникам защищенный доступ к внутренним корпоративным сайтам и сетям без использования VPN.

Также можно снизить уязвимость мобильных устройств по отношению к опасным веб-сайтам, которые могут содержать вредоносный код, нарушать политики отдела кадров или просто тратить ценное рабочее время пользователей.

С помощью MaaS360 Secure Mobile Browser организации могут указывать категории контента, доступ к которому следует ограничить, включая сайты социальных сетей, сайты загрузок и сайты для взрослых. Есть более 60 категорий критериев фильтрации, включающих миллионы URL-адресов.

Можно указать определенные URL-адреса для фильтрации доступа к соответствующим веб-сайтам. С помощью политик и черных списков IBM® MaaS360® Device Management можно отключать встроенные и сторонние браузеры.

MaaS360 Secure Mobile Browser может отправлять администраторам сообщения по электронной почте практически в реальном времени, предупреждая их о попытках доступа к таким сайтам.

Возможности, предоставляемые MaaS360 Secure Mobile Browser:

- Платформа централизованного управления на основе облака
- Простое создание политик и их дистанционное назначение по беспроводной сети
- Защищенный доступ к внутренним корпоративным сайтам и сетям без использования VPN устройств
- Мобилизация данных SharePoint, JIRA, внутренних вики-страниц, систем ERP предыдущих поколений и т.п.
- Постоянная защита путем перехвата трафика браузера
- Ограничение URL-адресов по категориям и предоставление доступа к определенным URL-адресам
- Блокировка известного вредоносного кода и опасных веб-сайтов, используя механизм сканирования и базу данных репутации
- Отключение cookie-файлов, печати, загрузок файлов, а также копирования и вставки
- Настраиваемые параметры блокировки, уведомлений практически в реальном времени, исключений и отчетности

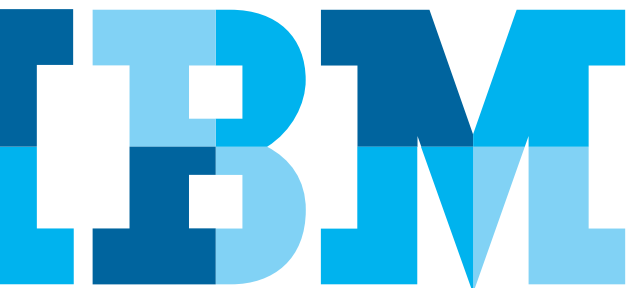




Рис. 1. Пример MaaS360 Secure Mobile Browser на различных мобильных устройствах

Управление возможностями доступа в Интернет на мобильных устройствах

MaaS360 Secure Mobile Browser — это надежный веб-браузер для смартфонов и планшетов. Его интуитивно понятный пользовательский интерфейс включает вкладки для просмотра, закладок, поиска, обмена и истории. MaaS360 Secure Mobile Browser позволяет организации снизить уязвимость мобильных устройств пользователей, предотвратить нарушение политик отдела кадров или сосредоточить внимание пользователей.

- **Медицинские устройства с общим доступом:** Обеспечьте защиту медицинских записей пациентов и оптимизируйте использование общих устройств медицинскими сотрудниками, сосредоточившись на справочных медицинских сайтах и веб-сайтах медицинских учреждений, а также предоставляя доступ к внутренним сайтам без необходимости подключения устройств по VPN.
- **Специализированные терминалы в пунктах розничных продаж (POS):** Повысьте эффективность работы торговых сотрудников и защитите данные в устройствах, разрешив доступ POS-терминалов только к указанным веб-сайтам для расчета, поиска по складскому запасу или проверки наличия товара в интернет-магазине.
- **Совместно используемые обучающие устройства:** Сосредоточьте внимание учащихся, ограничив доступ к определенным веб-сайтам с совместно используемых обучающих устройств в классе. Это приоритетная задача для образовательных учреждений при выполнении требований закона «О защите детей в Интернете» (CIPA).
- **Устройства консьерж-службы в гостиницах:** Повысьте эффективность работы персонала в гостиницах, ограничив возможности устройств регистрацией и выпиской гостей, просмотром услуг и доступом к местным метеослужбам и диспетчерским транспортным службам.
- **Демонстрационные устройства на мероприятиях:** Повысьте эффективность работы сотрудников на выставках, разрешив в информационном киоске доступ только к небольшому числу определенных веб-сайтов.

Параметры настройки браузера

- Настройка в качестве браузера по умолчанию
- Применение политик безопасности в отношении контейнеров MaaS360
- Отключение cookie-файлов и загрузок файлов
- Ограничение копирования, вставки и печати
- Включение режима информационного киоска в браузере
- Настройка домашней страницы по умолчанию и пользовательских закладок



Рис. 2. Пример настроек браузера в консоли MaaS360

Параметры фильтрации веб-сайтов

- Выбор категорий URL-адресов для разрешения, блокировки и отслеживания
- Возможность выбора из более чем 60 категорий, содержащий миллионы URL-адресов
- Поддержка исключений на основе имени домена или URL-адреса
- Черный список веб-сайтов



Рис. 3. Пример параметров фильтрации категорий веб-сайтов на портале

Параметры уведомлений пользователей и администраторов

- Отправка собственных тестовых или HTML-уведомлений пользователям при попытке доступа к запрещенному URL-адресу
- Перенаправление пользователей на определенный URL-адрес в случае нарушения политик
- Отправка уведомления администратору в случае блокировки пользователя
- Определение количества блокировок пользователя до отправки уведомления администратору

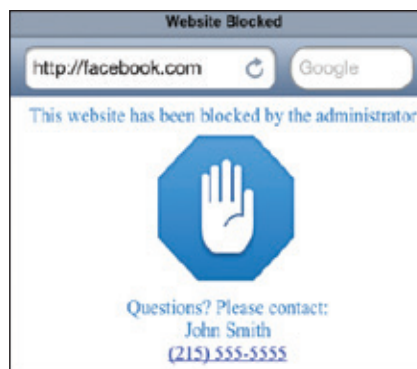


Рис. 4. Пример уведомления для пользователя в браузере при блокировке веб-сайта

Отчеты по устройствам и компании

- Просмотр обзорных графических отчетов по категориям и истории блокировки и отслеживания доменов
- Доступ к подробным отчетам по блокировке определенного устройства и истории отслеживания доменов



Рис. 5. Пример отчета о нарушениях для браузера устройства

Превентивная безопасность в Интернете

MaaS360 Secure Mobile Browser защищает данные и повышает производительность труда, контролируя доступ к общедоступным веб-сайтам и внутренним корпоративным сайтам на устройствах iOS и Android.

Этот браузер ограничивает или разрешает доступ пользователей к веб-сайтам на основе указанных категорий, включая следующие:

- Рекламные объявления и всплывающие окна
- Анонимайзеры
- Бот-сети
- Чат
- Преступные действия
- Знакомства и светская хроника
- Сайты загрузки
- Развлечения
- Порнография
- Форумы и новостные группы
- Азартные игры
- Игры
- Хакинг
- Обмен фотографиями
- Мгновенный обмен сообщениями
- Вредоносный код
- Новости
- Одноранговые сети
- Фишинг и мошенничество
- Покупки
- Социальные сети
- Спорт
- Потокное мультимедиа и загрузки
- И так далее

Легкость управления:

- Гибкая среда создания политик
- Настраиваемое назначение политик
- Интеграция с MaaS360 Mobile Device Management для оптимизации управления (необязательно)

Чтобы узнать подробнее о решении IBM MaaS360 и начать 30-дневный бесплатный период пробного использования, посетите веб-сайт www.ibm.com/maas360



© Copyright IBM Corporation 2016

IBM Восточная Европа/Азия

123317, Москва
Пресненская наб., 10
Тел.: +7 (495) 775-8800
Факс: + 7 (495) 258-6468, 258-6404
ibm.com/ru

Подготовлено в США.
Февраль 2016 г.

IBM, логотип IBM, ibm.com и X-Force являются товарными знаками International Business Machines Corporation, зарегистрированными во многих юрисдикциях мира. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® и устройство, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, MaaS360 Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360® и We do IT in the Cloud.™ и устройство являются товарными знаками или зарегистрированными товарными знаками Fiberlink Communications Corporation, компании IBM. Другие названия продуктов и услуг могут являться товарными знаками IBM или других компаний. Текущий список товарных знаков IBM доступен в разделе «Авторские права и товарные знаки» на веб-сайте по адресу ibm.com/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch и iOS являются товарными знаками или зарегистрированными товарными знаками компании Apple Inc. в США и других странах.

Microsoft, Windows, Windows NT и логотип Windows являются товарными знаками Microsoft Corporation в США и (или) в других странах.

Этот документ актуален на дату первоначального опубликования и может быть изменен IBM в любое время. Некоторые предложения могут быть недоступны в странах, где IBM ведет свою деятельность.

Данные о производительности и примеры заказчиков приведены в документе только в качестве иллюстрации. Фактическая производительность может зависеть от конкретной конфигурации и условий эксплуатации. Ответственность за оценку и проверку работы любого другого продукта или программы вместе с продуктами и программами IBM лежит на пользователе.

ИНФОРМАЦИЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИИ ИЛИ УСЛОВИЯ КОММЕРЧЕСКИХ КАЧЕСТВ, ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ ИЛИ НЕНАРУШЕНИЯ ЧЬИХ-ЛИБО ПРАВ. Гарантия на продукты IBM определяется условиями и положениями соглашений, действующих для продуктов в момент продажи.

Ответственность за выполнение требований всех действующих законов и нормативов несут заказчики. Корпорация IBM не предоставляет юридических консультаций и не дает гарантии, что ее продукты и услуги соответствуют требованиям каких бы то ни было законов.

Заявления относительно направления действий и намерений компании IBM в дальнейшем могут быть изменены или аннулированы без предварительного уведомления и представляют собой только цели и задачи.

Заявление о добросовестных практиках безопасности. Безопасность ИТ-систем включает в себя защиту систем и информации путем предотвращения, обнаружения и реагирования на несанкционированный доступ в рамках предприятия и за его пределами. Несанкционированный доступ может приводить к изменению, уничтожению или неправоначальному присвоению информации либо к повреждению или недопустимому использованию ваших систем, включая атаки на другие системы. Ни одна ИТ-система или продукт не может считаться абсолютно защищенным, и ни один продукт или мера безопасности не может быть полностью эффективной в предотвращении несанкционированного доступа. Системы и продукты IBM разрабатываются как часть комплексного подхода к обеспечению безопасности, который будет в обязательном порядке включать в себя дополнительные оперативные процедуры и для наиболее эффективного функционирования может требовать наличия других систем, продуктов или сервисов. Компания IBM не гарантирует неуязвимость этих систем и продуктов по отношению к злоумышленным или незаконным действиям любой стороны.



Подлежит переработке и вторичному использованию