


Ключевые преимущества бизнес-решений ESET NOD32

Надежность Усовершенствованная система сканирования, обеспечивающая эффективную защиту персональных данных в корпоративной сети.	Быстродействие Низкие системные требования и интеллектуальные алгоритмы сканирования обеспечивают высокую производительность.	Минимальные системные требования Экономичное потребление ресурсов не перегружает систему, обеспечивая стабильную работу.
--	---	--

Защита рабочих станций и файловых серверов и мобильных устройств

	ESET NOD32 Smart Security Business Edition Комплексное решение для бизнеса. Мгновенно реагирует на попытки проникновения вредоносных программ, отражает сетевые атаки, блокирует нежелательную почту. Компоненты: ESET Endpoint Security ESET File Security для Microsoft Windows Server ESET File Security для Linux/BSD/Solaris ESET Mobile Security Business Edition/ ESET Endpoint Security для Android ESET Remote Administrator
--	--



ESET NOD32 Antivirus Business Edition

Бизнес-решение для централизованной антивирусной защиты рабочих станций и файловых серверов от интернет-угроз и вредоносных программ. Обеспечивает высокий уровень безопасности корпоративной сети без снижения ее быстродействия.

Компоненты:

ESET Endpoint Antivirus
ESET File Security для Microsoft Windows Server
ESET File Security для Linux/BSD/Solaris
ESET Mobile Security Business Edition/ ESET Endpoint Security для Android
ESET Remote Administrator



ESET Endpoint Security

антивирус | антишпион | антиспам | DEVICE-контроль | WEB-контроль | HIPS | файервол

Эффективная защита рабочих станций корпоративной сети от всех типов угроз. Обеспечивает оптимальный уровень безопасности и высокую производительность работы, при минимальных системных требованиях.

Ключевые особенности

Высокий уровень безопасности данных

- выявление всех типов сложных угроз
- оперативное противодействие атакам киберпреступников
- проверка репутации приложений до запуска
- сканирование веб-контента
- предотвращение заражений рабочих станций и эпидемии в корпоративной сети

Защита от неизвестных угроз

- детектирование угроз на основе облачного сервиса ESET Live Grid
- распознавание ранее неизвестных угроз по принципу технологии эвристического анализа ThreatSense®
- поведенческий анализ потенциально опасного ПО
- блокирование вредоносных ссылок в интернете

Контроль съемных носителей

- автоматическое сканирование содержания подключаемых внешних устройств
- настройка правил работы со съемными носителями информации для каждого пользователя
- контроль доступа пользователей по типу устройства и заданным атрибутам
- идентификация съемных устройств
- ограничение подключения USB-принтеров, LPT/COM портов, модемов, Card reader, а также устройств по сети Bluetooth

Системные требования

Поддерживаемые ОС:


Microsoft Windows® 8/7/Vista/XP/2000 (32-bit и 64-bit версии)


Microsoft Windows® Server 2008 R2/ 2008/ 2003 /2000 (32-bit и 64-bit версии)

Microsoft Windows Small Business Server 2003/ 2003 R2/ 2008/2011

Microsoft® Windows® 2000, XP, Server 2003

Microsoft® Windows® 7, Vista, Home Server, Server 2008

	<p><i>Linux (RedHat, Mandrake, SuSE, Debian, FreeBSD 4.X, 5.X и 6.X, NetBSD 4)</i></p> <p><i>Sun Solaris 10</i></p> <p><i>Mac OS X 10.5.x (Leopard), Mac OS X 10.6.x (Snow Leopard), Mac OS X 10.7.x (Lion), Mac OS X 10.8.x (Mountain Lion)</i></p> <p><i>Требования к оперативной памяти 512 MB</i></p> <p><i>Необходимое свободное место на жестком диске 60 MB (для установки 320 MB)</i></p>
	<p>ESET Endpoint Antivirus антивирус антишпион DEVICE-контроль HIPS</p> <p>Решение для проактивной защиты рабочих станций от всех типов вредоносного ПО. Проводит оперативное сканирование, блокирует работу запрещенных приложений, исключает вероятность утечки конфиденциальной информации.</p> <p>Ключевые особенности</p> <ul style="list-style-type: none"> • Высокий уровень безопасности данных • Защита от неизвестных угроз • Контроль съемных носителей • Разграничение прав доступа к интернету • Защита от внешних вторжений и фильтрация трафика • Проверка корпоративной почты • Защита виртуальной среды • Регулярное обновление • Дополнительные инструменты диагностики системы <p>Системные требования Поддерживаемые ОС:</p> <p><i>Microsoft Windows® 8/7/Vista/XP/2000/NT 4.0/ Home Server (32-bit и 64-bit версуи)</i> <i>Microsoft Windows® Server 2008 R2/ 2008/ 2003 /2000 (32-bit и 64-bit версуи)</i></p>

	<p><i>Linux (RedHat, Debian, Ubuntu, Suse, Fedora, Mandrake)</i> <i>Mac OS X 10.5.x (Leopard), Mac OS X 10.6.x (Snow Leopard), Mac OS X 10.7.x (Lion), Mac OS X 10.8.x (Mountain Lion)</i></p> <p><i>Требования к оперативной памяти 512 MB</i> <i>Необходимое свободное место на жестком диске 60 MB (для установки 320 MB)</i></p>
	<h3>ESET File Security для Microsoft Windows Server</h3> <p>Решение для обеспечения эффективной защиты файловых серверов от всех типов вредоносных программ для Microsoft Windows Server.</p> <ul style="list-style-type: none">• eShell(ESET Shell) Интегрированная командная строка позволяет расширить возможности управления решениями ESET, создавать скрипты для конфигурации продукта и выполнения действий.• Правила исключений Автоматическое обнаружение критических программ и файлов, которые могут нарушить работоспособность сервера.• Многопоточное сканирование без снижения производительности Минимальные системные требования и оптимизация работы в серверной среде обеспечивают безопасность файловых серверов без снижения их производительности. <p>Ключевые особенности</p> <p>Интеллектуальная фильтрация Сканирование и распознавание всех типов угроз, мгновенная реакция на попытки проникновения вредоносных программ в корпоративную сеть компании</p> <p>Быстродействие Оптимизированный режим работы и фильтрации не влияют на производительность файлового сервера, не снижают вычислительные мощности для выполнения основных задач</p>

Настройка политик безопасности

Возможность установки правил на выполнение действий после обнаружения вредоносного кода – от перемещения зараженного объекта в карантин до полного его удаления

Информативные отчеты

Сбор полной статистики по работе ESET NOD32 File Security для Microsoft Windows с указанием логов, попыток заражения системы

Бесперебойная работа и простое управление

Необходимый набор инструментов и расширенные возможности конфигураций обеспечивают стабильную работу продукта и его удаленное администрирование с помощью консоли управления ESET Remote Administrator

Дополнительные инструменты диагностики системы

Ведение журналов об эффективности работы

Защита виртуальной среды

ESET NOD32 File Security для Microsoft Windows обеспечивает надежный уровень безопасности при работе на виртуальных машинах, подтвержденные сертификатом VMware.

Системные требования

Процессор: Intel or AMD x86/x64

Операционные системы:

Microsoft Windows Server 2000, 2003 (32 & 64 bit), 2008 (32 & 64 bit), 2008 R2

Microsoft Windows Small Business Server 2003, 2003 R2, 2008, 2011



ESET NOD32 File Security для Linux / BSD / Solaris

Обеспечивает безопасность файловых серверов **под управлением Linux / BSD / Solaris от всех типов вредоносного ПО и интернет-угроз** с минимальным воздействием на производительность и быстродействие системы.

Ключевые особенности

Расширенное сканирование

Тщательное сканирование альтернативных потоков данных (ADS) в файлах, мониторинг всей файловой системы и детектирование угроз в режиме реального времени

Улучшенный демон-службы в Linux

Повышенная устойчивость и эффективное сканирование службы Linux

Централизованное управление

Единая консоль администрирования ESET Remote Administrator позволяет удаленно настраивать политики и правила безопасности, контролировать работу и отслеживать события по обнаружению угроз

Проверка по требованию

Одновременное сканирование нескольких процессов и заданных файлов через командную строку

Пользовательские конфигурации


Возможность настройки для конкретных пользователей определенных правил сканирования и действий с потенциально опасными объектами

Расширенные функции карантина

Индивидуальное хранилище подозрительных и зараженных файлов каждого пользователя с возможностью управления через веб-интерфейс

Системные требования

Процессор: i386 (Intel® 80386), amd64 (x86_64)

	<p><i>Операционные системы:</i></p> <p><i>Linux (версия ядра 2.2.x, 2.4.x или 2.6.x, Glibc 2.2.5 или выше)</i> <i>FreeBSD 6.x, 7.x, 8.x</i> <i>NetBSD 4.x или выше Dazuko 2.0.0 или выше</i></p>
	<p>ESET Endpoint Security для Android</p> <p>Обеспечивает высокий уровень антивирусной защиты мобильных устройств под управлением ОС Android. Сочетает в себе широкий набор функций для обеспечения безопасности конфиденциальной информации, хранящейся на смартфонах или планшетах.</p> <p>Ключевые особенности</p> <p>Защита от потери конфиденциальных данных В случае утери мобильного устройства, определяет местонахождение по GPS-координатам, удаленно блокирует смартфон, удаляет контакты, сообщения с целью защиты от несанкционированного доступа.</p> <p>Надежная защита от известных и новых видов угроз Обнаруживает и удаляет интернет-угрозы и вредоносное ПО, которое распространяется по сети Bluetooth или Wi-Fi. Обеспечивает защиту приложений, файлов и карт памяти.</p> <p>Удаленное администрирование Проверка состояния защиты, настройка корпоративной политики безопасности и централизованное администрирование осуществляется удаленно, с единой консоли управления ESET Remote Administrator</p> <p>Основные возможности</p> <ul style="list-style-type: none">• Поведенческий анализ угроз• Антиспам• Дистанционная защита• Расширенное сканирование• Встроенный аудит безопасности

- Централизованное администрирование

Системные требования

Операционные системы:

Android 2.0 и выше (Функции Удаленная очистка и Защита паролем доступны для OS Android 2.2 и выше)

Свободное место: 1 Мб

Оперативная память: 128+ Мб

Свободное место внутренней памяти: 5+ Мб

SD-карта: рекомендуется

Экран: сенсорный (минимальный размер 240x320 пикс., рекомендуется 320x480 пикс.)

Процессор: 600+ МГц

Подключение к интернет-сети



ESET Mobile Security Business Edition

антивирус | антишпион | антиспам | файрвол

Решение для антивирусной защиты мобильных устройств под управлением ОС Windows Mobile и Symbian. Сочетает в себе широкий набор функций для обеспечения безопасности конфиденциальных данных от кражи злоумышленниками

Основные возможности

Защита в режиме реального времени

- мгновенное сканирование файлов и установленных приложений
- проверка всех объектов, загружаемых из Интернета по Wi-Fi, Bluetooth, GPRS и EDGE
- поведенческий анализ и детектирование ранее неизвестных угроз

SMS / MMS Антиспам

- блокировка нежелательных SMS и MMS-сообщений.

- настройка «черных» и «белых» списков контактов

Файервол

- мониторинг всех входящих и исходящих соединений на основе заданных правил
- автоматическая блокировка приема и передачи данных в роуминге

Встроенный аудит безопасности

- проверка мобильного устройства по расписанию
- отчетная информация о состоянии системы, включая данные о заряде батареи, Bluetooth, свободной памяти и подключенных устройствах.

Remote Wipe

Специализированная SMS-команда позволяет удаленно стереть все персональную информацию с телефона, включая контакты, сообщения и данные на карте памяти

Централизованное администрирование

Управление и применение политик безопасности корпоративной сети с помощью единой консоли ESET Remote Administrator

Системные требования

Операционные системы:

Symbian S60 3rd Edition Feature Pack 1 или 2 (только Nokia)

Symbian S60 5th Edition (Nokia только)

*Symbian3 (Nokia только) **

Windows Mobile 5.0, 6.0, 6.1 и 6.5

Требования к оперативной памяти 1 MB



ESET REMOTE ADMINISTRATOR

ESET Remote Administrator

Централизованное администрирование и управление продуктами ESET NOD32 в корпоративных средах различной сложности. Повышает безопасность IT-инфраструктуры, обеспечивает бесперебойную работу защитных механизмов антивирусной системы.

Основные возможности:

Гибкое управление

Настройка политики безопасности и управление антивирусной системой компании с одного рабочего места.

Мониторинг

Отображение реального состояния безопасности и событий в отчетах.

Быстрая установка

Позволяет развернуть комплексную систему антивирусной защиты узлов корпоративной сети за минимальное время и с минимальными трудозатратами.

Ключевые особенности

- Централизованное управление антивирусной защитой
- Настройка политики безопасности
- Статистика и отчеты
- Удаленная установка
- Регулярные обновления
- Управление группами

Системные требования

Поддержка баз данных:

Поддержка баз данных: MS Access, MS SQL Server, MySQL и Oracle

Резервное копирование баз данных

ESET Remote Administrator Console:

Операционная система: Microsoft Windows® 8/ 7 / Vista / XP / 2008 R2 / 2008 / 2003 / 2000

ESET Remote Administrator Server

Операционная система: Microsoft Windows® 8/7 / Vista / XP / 2008 R2 / 2008 / 2003 / 2000 /NT4 (Service Pack 6)



ESET NOD32 Mail Security для Microsoft Exchange Server

Антивирус | Антишпион | Антиспам

Решение для защиты почтовых серверов от всех видов вирусов, интернет-угроз. Сканирует и фильтрует почту в режиме реального времени.

Ключевые особенности

- Интеллектуальная фильтрация
- Усовершенствованная защита от спама
- Многопоточное сканирование
- Быстродействие
- Бесперебойная работа и простое управление
- Защита виртуальной среды
- Настройка политик безопасности
- Мониторинг событий и производительности
- Правила исключений
- Расширенная статистика

Системные требования

Процессор

Intel or AMD x86/x64

Операционные системы

Microsoft Windows Server 2000, 2003 (32 & 64 bit), 2008 (32 & 64 bit), 2008 R2

Microsoft Windows Small Business Server 2003, 2003 R2, 2008, 2011

Microsoft Exchange

Microsoft Exchange Server 5.5 (SP3, SP4)

Microsoft Exchange Server 2000

(SP1, SP2, SP3)

Microsoft Exchange Server 2003 (SP1, SP2)

Microsoft Exchange Server 2007

(SP1, SP2, SP3)

Microsoft Exchange Server 2010 (SP1)



ESET NOD32 Mail Security для Linux / BSD / Solaris

Обеспечивает эффективную защиту почтовых серверов на платформах Linux/BSD/Solaris от всех известных и неизвестных ранее интернет-угроз, в том числе вирусов, современных модификаций вредоносных программ, червей, троянских программ, шпионского ПО, фишинга и спама.

Высокий уровень производительности и минимальное потребление ресурсов позволяют обеспечить безопасность почтовых Unix-серверов любого масштаба.

Ключевые особенности

Надежная защита

Двунаправленное сканирование всего входящего и исходящего трафика по протоколам POP3, SMTP, IMAP с целью обнаружения вирусов и потенциально опасного ПО

Многоуровневая защита

Применение нескольких методов фильтрации (нежелательных рекламных сообщений и спама)

Быстродействие

Небольшой размер пакетов регулярных обновлений сигнатурных баз и низкие системные требования не оказывают влияние на производительность почтового сервера под управлением Linux.

Правила защиты

Оптимизированный режим работы и фильтрации почты не влияет на производительность почтового сервера и не снижает вычислительные мощности для выполнения основных задач - таких, как обработка и доставка почты.

Гибкая политика безопасности

Определение индивидуальных параметров сканирования почты для группы пользователей и отдельных почтовых ящиков.


Простое управление

Удаленное администрирование с помощью консоли централизованного управления ESET Remote Administrator обеспечивает стабильную работу антивирусного решения.

Системные требования

Процессор: Intel или AMD x86/x64

Операционные системы

	<p><i>Linux – версия ядра 2.2.x, 2.4.x или 2.6.x; glibc 2.2.5 или выше</i></p> <p><i>FreeBSD 6.x, 7.x, 8.x</i></p> <p><i>NetBSD 4.x</i></p> <p><i>Sun Solaris 10</i></p>
	<p>ESET NOD32 Mail Security для IBM Lotus Domino</p> <p>Решение для почтовых серверов сканирует почтовый трафик и обеспечивает надежную защиту корпоративной почты от всех типов вредоносных программ и спама.</p> <p>Ключевые особенности:</p> <p>Передовая защита от спама</p> <p>Сочетание нескольких технологий анализа писем и точная настройка всех параметров защиты непосредственно из интерфейса пользователя обеспечивают максимальную защиту от нежелательной почты при минимальном потреблении системных ресурсов.</p> <p>Комплексная антивирусная защита</p> <p>Решение включает модуль резидентной защиты, осуществляет сканирование по требованию, анализирует трафик на уровне SMTP-шлюза, а также выполняет регулярные проверки архива писем в базе данных IBM Lotus Domino.</p> <p>Создание «серых» списков</p> <p>Дополнительный уровень защиты от спама за счет ограниченной доставки нежелательных писем, поступающих на сервер. Журнал «серых» списков отображает подробную информацию по заданным критериям.</p> <p>Улучшенный антиспам модуль</p> <p>Точная настройка всех параметров настройками непосредственно из интерфейса пользователя обеспечивает еще качественную и эффективную защиту от нежелательной почты.</p> <p>Журнал спама</p> <p>Отображает информация об отправителе, получателе, оценке спама, классификации и выполненных</p>

действий с файлом.

Дерево расширенных настроек

Интуитивная навигация для настройки управления всеми параметрами антивирусной защиты почтового сервера.

Исключения

Бесперебойная работа сервера обеспечивается за счет обнаружения и исключения критических файлов операционной системы.

Легкость установки и настройки

Расширенные параметры настроек, импорт / экспорт файлов конфигураций для удобства установки продукта.

Объединение лицензий

Возможность слияния лицензий с целью упрощения управления лицензиями в одной корпоративной сети.

Системные требования

Процессор

Intel или AMD x86/x64

Операционные системы

Microsoft Windows Server 2000, 2003 (32-bit & 64-bit), 2008 (32-bit & 64-bit), 2008 R2

Поддержка Lotus Domino

IBM Lotus Domino 6.5.x / 7.0.x / 8.0.x / 8.5.x



ESET NOD32 Antivirus для Kerio Connect

Решение для защиты почтовых серверов под управлением платформы Kerio. Обеспечивает современный уровень безопасности и противодействие вредоносному программному обеспечению до его проникновения в сеть.

Высокий уровень производительности и минимальная ресурсоемкость позволяют обеспечить безопасность почтовых Unix-серверов в компаниях любого масштаба.

Основные характеристики:

Надежная защита

Оперативное обнаружение и удаление всех типов известных и ранее неизвестных угроз в письмах, а также фильтрация вложенных файлов по имени, расширению или по типу MIME.

Защита клиент-сервер

Решение включает все инструменты для полноценного обеспечения безопасности сервера, в том числе резидентную защиту и сканирование по запросу.

Работа в фоновом режиме

Сканирование в фоновом режиме всего почтового потока данных позволяет снизить нагрузку на производительность сервера до минимума.

Минимальное влияние на работу сервера

Все задачи проверки и сканирования почтового трафика производятся по алгоритмам и технологии эвристического анализа на уровне ядра, что позволяет обеспечить быстродействие системы в целом.

Удаленное управление

Консоль централизованного управления ESET Remote Administrator позволяет актуализировать сигнатурные базы с локального зеркала обновлений сервера и предоставляет возможность администратору сети удаленно настраивать конфигурации, создавать правила безопасности и отслеживать работу каждого объекта сети.

Планировщик задач

Присутствует возможность настроить сканер для работы только на заданный период времени.

SelfDefense

Предотвращение попыток отключить или изменить статус безопасности сервера (в версии для Windows).

Поддержка различных платформ

Антивирус ESET NOD32 для Kerio Connect также поддерживает операционные системы Windows и Linux.

Системные требования*Процессор*

Intel или AMD x86/x64

Поддерживаемые почтовые серверы:

- *Под управлением Windows:*

- Kerio Connect 7.0 и более поздние версии до 7.5.x

- Kerio Mail Server 6.7.x и более поздние

- *Под управлением Linux:*

- Kerio Connect 7.0 и более поздние версии до 7.5.x

- Kerio Mail Server 6.1.2 и более поздние

Поддерживаемые ОС:

Microsoft Windows 2000 и более поздние (64-bit версии)

Linux: Linux Kernel версии 2.2.x, 2.4.x или 2.6.x/ glibc 2.2.5 и выше FreeBSD версии 5.x, 6.x и 7.x/NetBSD 4.x/ Sun Solaris 10

Защита шлюзов



ESET NOD32 Gateway Security для Linux / BSD / Solaris

Защита HTTP- и FTP-шлюзов от вирусов, червей, троянских и шпионских программ, фишинга и других интернет-угроз.

Ядро приложения основано на интеллектуальной технологии ThreatSense®, отличается высокой скоростью сканирования и эффективностью обнаружения компьютерных угроз.

Ключевые особенности

Проактивная защита

Интеллектуальные технологии обнаружения всех типов угроз и расширенное сканирование обеспечивают высокий уровень безопасности сети от проникновения вредоносных программ.

Сканирование данных

Проверка данных, транслируемых по протоколам HTTP, SMTP, POP3 и FTP, на наличие вредоносного кода.

Быстродействие

Оптимизированный режим работы и минимальные системные требования ESET NOD32 Antivirus для Kerio Control не влияют на производительность системы в целом.

Системные требования

Процессор: Intel или AMD x86/x64

Операционные системы

Linux версия ядра 2.2.x, 2.4.x или 2.6.x; glibc 2.2.5 или выше

FreeBSD – версия ядра 6.x, 7.x или 8.x

NetBSD – версия ядра 4.x

Sun Solaris – версия 10



ESET NOD32 Antivirus для Kerio Control

Решение для фильтрации всего трафика на уровне протоколов HTTP, FTP, SMTP и POP3 и своевременной защиты корпоративной сети от интернет-угроз, вирусов, троянских программ, шпионского ПО, руткитов и буткитов.

Ключевые особенности

Проактивная защита

Интеллектуальные технологии обнаружения всех типов угроз и расширенное сканирование обеспечивают высокий уровень безопасности сети от проникновения вредоносных программ.

Сканирование данных

Проверка данных, транслируемых по протоколам HTTP, SMTP, POP3 и FTP, на наличие вредоносного кода.

Быстродействие

Оптимизированный режим работы и минимальные системные требования ESET NOD32 Antivirus для Kerio Control не влияют на производительность системы в целом.

Настройка политики безопасности

Оперативное выявление вредоносных программ на уровне шлюза, предупреждение об инфицированных файлах и перемещение их в карантин.

Информативные отчеты

Возможность создания отчетов и осуществления контроля над работой пользователей.


Полная интеграция

Установка через конфигуратор Kerio и полная совместимость модулей «Антивирус» и «Антишпион».

Системные требования

Процессор

	<p><i>Intel или AMD x86/x64</i></p> <p><i>Поддерживаемые версии решений Kerio:</i></p> <ul style="list-style-type: none">• <i>Kerio Control 7.0 и выше, до версии 7.4.x</i>• <i>Kerio Winroute Firewall 6.6x и выше</i> <p><i>Поддерживаемые ОС:</i></p> <ul style="list-style-type: none">• <i>Microsoft Windows Server 2000, 2003 (32-bit и 64-bit версии), 2008 (32-bit и 64-bit версии), 2008 R2</i>• <i>Microsoft Windows 7/ Vista /XP/ 2000 (32-bit и 64-bit версии)</i>
--	--

	<p>ESET Secure Authentication</p> <p>Надежное и простое средство двухфакторной аутентификации При каждом подключении к корпоративной сети компании формируется дополнительный временный пароль для предотвращения утечки конфиденциальных данных Полностью программный продукт — нет необходимости в управлении аппаратными устройствами Никаких дополнительных затрат — продукт легко интегрируется в существующую инфраструктуру Идеальное решение для удаленных сотрудников Мультиплатформенное решение на базе мобильных устройств</p> <p>Ключевые особенности</p> <p>Безопасный доступ Двухфакторная аутентификация требует наличия двух элементов - постоянный пароль («то, что</p>
--	--

пользователь знает») и мобильный телефон («то, что пользователь имеет при себе»). Сочетание данных элементов обеспечивает более высокий уровень безопасности доступа к информационным ресурсам

Надежные пароли

Временные пароли формируются случайным образом и не могут быть подобраны или использованы повторно. Пользователь получает временный пароль в SMS сообщении или в приложении на его мобильном телефоне (подключение к интернету не требуется). Доступ к приложению дополнительно защищен PIN-кодом для предотвращения несанкционированного доступа

Простота и легкость внедрения

Продукт ESET Secure Authentication включает в себя приложение для мобильных устройств сотрудников компании и серверное приложение, которое легко интегрируется с MMC (Microsoft Management Console) и ADUC (Active Directory Users & Computers).

Совместимость с Web приложениями Microsoft

Продукт полностью поддерживает такие приложения, как Microsoft Outlook Web App, Microsoft Exchange, Microsoft SharePoint, Microsoft Dynamics CRM и Microsoft Remote Desktop Web Access

Поддержка VPN и VDI систем

Легкая интеграция в RADIUS-системы, в том числе: Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall, VMware Horizon View и Citrix XenApp

Пакеты API и SDK

Для внедрения в собственные системы аутентификации и системы дополнительного подтверждения действия пользователя доступны пакеты исходных кодов API (для систем, подключенных к Active Directory) и SDK на базе Java, PHP и Microsoft .NET (для систем, использующих, собственную базу данных).

Системные требования

Операционные системы:

Сервер: 32/64-битные версии Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2

Клиент: iOS 4.3 и выше, Android 2.1 и выше, Windows Phone 7 и новее, Windows Mobile 6, BlackBerry с 4.3 по 7.1 версии и 10 версия и выше, Symbian (все, поддерживающие J2ME), все мобильные устройства на базе J2ME

Поддерживаемые Web приложения Microsoft:

Microsoft Exchange 2007 (Outlook Web Access), Microsoft Exchange 2010 (Outlook Web App, Exchange Control Panel), Microsoft Exchange 2013 (Outlook Web App, Exchange Admin Center)

Microsoft SharePoint 2010, Microsoft SharePoint 2013

Microsoft Dynamics CRM 2011, Microsoft Dynamics CRM 2013

Microsoft Remote Desktop Web Access

Microsoft Terminal Services Web Access