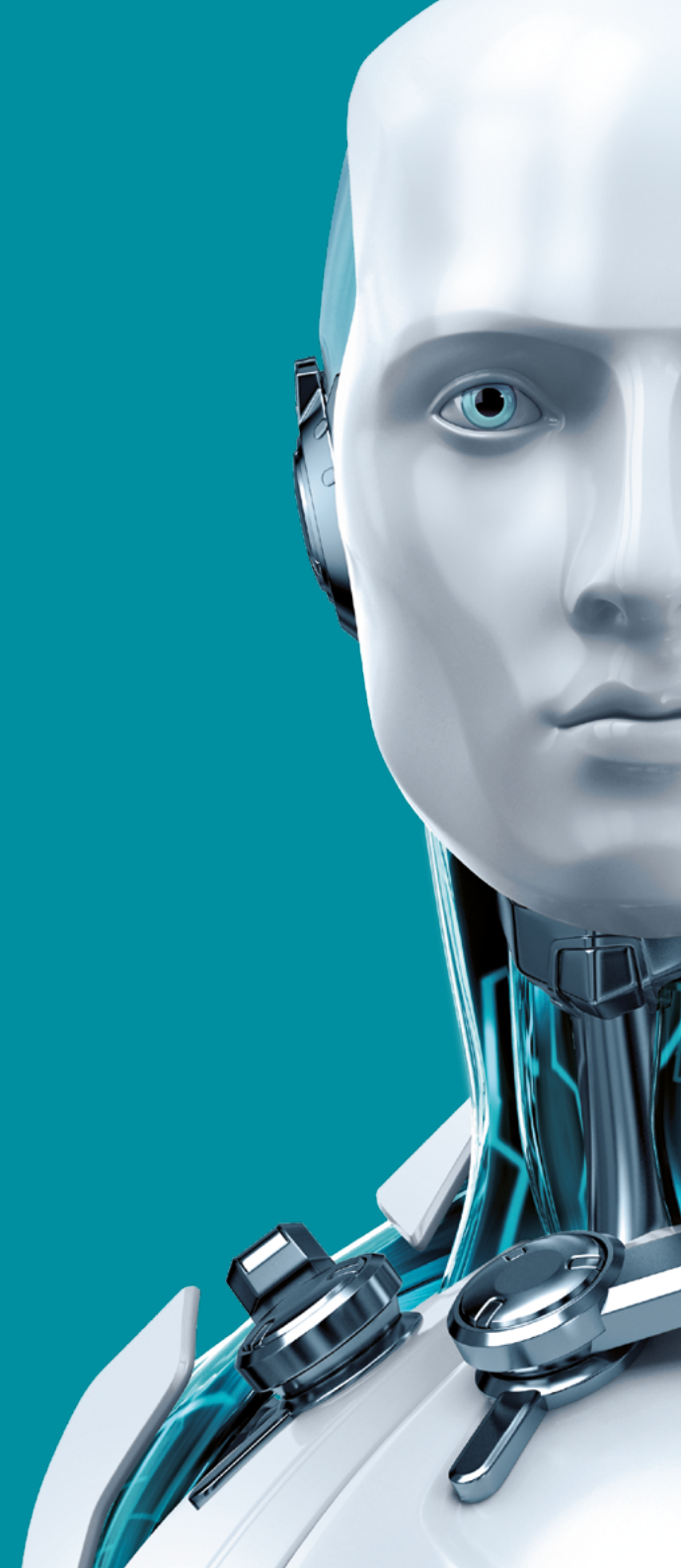
SECURE AUTHENTICATION

BUSINESS

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА



SECURE AUTHENTICATION

ESET Secure Authentication обеспечивает безопасный доступ к корпоративным данным организации. Решение позволяет компании за десять минут защитить подключение, что снижает риск утечки данных, обусловленный выбором ненадежных паролей.

Продукт включает серверную и клиентскую части, последняя представлена в виде мобильного приложения. Подтверждение аутентификации может осуществляться через push-аутентификацию или одноразового пароля. Рассылка пароля может производиться через мобильное приложение, SMS или любой аппаратный токен.

Двухфакторная аутентификация для сверхнадежной защиты информации

Вы можете использовать ESET Secure Authentication для:

- доступа к VPN компании
- удаленного доступа к ресурсам компании
- дополнительной защиты при входе в компьютер
- доступа к облачным сервисам через Microsoft ADFS 3.0 или 4.0, к таким приложениям как Office 365 и Google App
- защиты веб-приложений Microsoft, например, Outlook Web Access (OWA)
- доступа к Exchange Control Panel 2010 & Exchange Administrator Centre 2013, 2016
- просмотра VMware Horizon
- защиты VPN и VDI систем
- защищённого доступа к ресурсам системы 1С

Для внедрения в собственные системы аутентификации и дополнительного подтверждения действий пользователя доступны пакеты исходных кодов API и SDK.

Бизнес-преимущества

- При каждом подключении формируется дополнительный временный пароль для предотвращения утечки конфиденциальных данных
- Дополнительный уровень защиты от ненадежных паролей
- Выбор наиболее удобного пути доставки временного пароля (например, собственный шлюз для отправки SMS)
- Сокращение расходов на аппаратные средства защиты доступа
- Простота и легкость внедрения
- Поддержка аппаратных токенов
- Защита и поддержка облачных сервисов, таких как Office 365 и Google Apps.

ИТ-преимущества

- Пакеты API/SDK для легкой интеграции в собственные системы компании
- Приложение не требует подключения к интернету после загрузки
- Защита VPN-систем
- Мультиплатформенное решение на базе мобильных устройств
- Бесплатная круглосуточная техническая поддержка
- Готовое решение
- Увеличение производительности и снижение нагрузки на систему при подключении к проверенных адресов, благодаря функции список исключений IP
- Большое количество поддерживаемых систем

Техническая спецификация

Двухфакторная аутентификация	Решение для защиты доступа на базе мобильных устройств для высокого уровня безопасности
	Встроенная поддержка различных платформ (см. ниже обзор поддерживаемых платформ)
	Программный продукт – нет необходимости в дополнительной установке аппаратных устройств или токенов
	Подходит для удаленных сотрудников
	Поддержка аппаратных токенов
Клиент (мобильное приложение)	Установка в одно нажатие, простой и понятный пользовательский интерфейс
	Совместимость с любым устройством, которое поддерживает обмен сообщениями
	Поддерживаются актуальные мобильные платформы
	Доступ к приложению защищен паролем для предотвращения мошенничества в случае кражи или потери устройства
	Приложения доступны на нескольких языках: английский, немецкий, русский, французский, испанский, словацкий
Методы аутентификации	Одноразовый пароль формируется случайным образом, для его получения подключения к интернету не требуется
	Push-аутентификация – аутентификация одним нажатием на экран смартфона (данная функция доступна для устройств на базе операционных систем iOS и Android)
	Одноразовый пароль предоставляется в SMS
	Аппаратные токены (решение не требует для работы аппаратных токенов, но позволяет использовать любые аппаратные токены, работающие по стандарту OATH (Open Authentication) HOTP, FIDO)
	Другие каналы коммуникации (например, электронная почта)
Сервер	Готовое решение
	Простота и легкость настройки и установки (в два клика)
	Установщик автоматически распознает операционную систему и сам выбирает все необходимые компоненты
	Интерактивный установщик, встроенная установка в AFDS
Внедрение в собственные системы аутентификации	Для легкого внедрения в собственные системы аутентификации и системы дополнительного подтверждения действия пользователя доступны пакеты исходных кодов API или User Management API
	API и пакет SDK позволяют реализовывать внедрение системы для пользователей, которые не подключены к Active Directory
Централизованное управление	Управление серверной частью при помощи веб-консоли ESA или Microsoft Management Console (MMC)
	Полная интеграция в Active Directory
	ESET Secure Authentication расширяет функционал Active Directory Users & Computers (модуль ADUC) и включает дополнительные функции по управлению параметрами двухфакторной аутентификации для проверки подлинности пользователя компьютера

БЕСПЛАТНАЯ ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Экономьте свое время благодаря нашим специалистам.

Режим работы технической поддержки: круглосуточно, ежедневно, на русском языке.

Обзор поддерживаемых платформ

Для получения детальной информации по техническим требованиям пожалуйста обратитесь к руководству по продукту ESET Secure Authentication, которое доступно по ссылке: http://download.eset.com/manuals/eset_esa_product_manual_enu.pdf

Платформы для удаленного входа	**Протокол Remote Desktop** **Защита VPN** Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall	
Защита локального входа (Windows)	Windows 7 и более поздние версии Windows Server 2008 R2 и более поздние версии	
Active Directory Federation Services	Microsoft ADFS 3.0 или 4.0	
Платформы VDI	VMware Horizon View	Citrix XenApp
Веб-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 Exchange 2016	Outlook Web App Exchange Admin Center Microsoft Dynamics CRM 2011,2013,2015,2016 Microsoft SharePoint 2010, 2013,2016 Microsoft SharePoint Foundation 2010, 2013 Microsoft Remote Desktop Web Access Microsoft Terminal Services Web Access Microsoft Remote Web Access
Интеграция в собственную систему аутентификации	ESET Secure Authentication легко интегрируется в собственные RADIUS-системы. Интеграция осуществляется на основе адресной книги через ESET Secure Authentication API или User Management API. Пользователи, которые не используют Active Directory, могут использовать для установки API или пакет SDK.	
Операционная система (серверная часть)	Windows Server 2008,2008 R2, 2012, 2012 R2, 2016, 2019 Windows Small Business Server 2008, 2011 Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials, 2019 Essentials Средства управления поддерживаются также в операционных системах начиная с Windows 7.	
Платформы для мобильных устройств (клиент)	iOS 8 до iOS 11 Android™ 4.0.3 до Android 9.0 Windows Phone 8.1 до Windows 10 Mobile	