Офисы Королевства
Великобритании и Ирландии
Север
1200 Century Way
Thorpe Park, Leeds
LS15 8ZA

Центральный офис: +44 (0)1134 860 123
Поддержка: +44 (0)1134 860 111
hq@swivelsecure.com

Юг
Pinewood
Chineham Business Park
Chineham, Basingstoke
RG24 8AL

Офисы в Америке
Сиэтл
Swivel Secure, Inc.
1001 4th Ave #3200
Seattle, WA 98154

+1 949 480 3626 (тихоокеанское время)
Бесплатная линия: 866 963 код (2884)
usa@swivelsecure.com

Офисы в Европе
Португалия
Estrada de Alfragide,
N.º 67, Alfrapark – Lote H,
Piso 0, 2614-519 Amadora

+351 215 851 487
portugal@swivelsecure.com

Испания
Calle Punto Mobi 4,
28805 Alcala de Henares
Madrid

+34 911 571 103
espana@swivelsecure.com

AuthControl Sentry®

Защита данных благодаря удостоверенной аутентификации

С технологией PINsafe® в основе для максимальной безопасности и Аутентификацией на основе пунктов, которое обеспечивает динамичное управление, удостоенный наград AuthControl Sentry® предоставляет интеллектуальное решение вместе с многофакторной аутентификацией для бизнеса

swivelsecure

www.swivelsecure.com

AuthControl Sentry® - Интеллектуальная многофакторная аутентификация.

Востребовано в более чем 52 странах и в разных предприятиях, в частности - правительство, здравоохранение, образование, производство. AuthControl Sentry® предоставляет организациям многофакторную аутентификацию, а также предлагает интеллектуальное решение для предотвращения взломов к приложениям и данным.

Просканируйте QR код чтобы увидеть всю диаграму AuthControl Sentry®, а также весь комплекс многофакторного решения.

AuthControl Sentry® с гибкостью подходит для поддержки ряд архитектурных требований, а также способнен обеспечить максимальное внедрение, с широким выбором факторов аутентификации. Не зависимо от того, используете ли вы мобильное приложение или же биометрию через считыватель отпечатков пальцев, AuthControl Sentry® зарекомендовал себя как ведущее решение в кибер-безопасности.

Что делает наше решение уникальным

- Запатентованная технология PINsafe® для максимальной безопасности - см. стр. 8
- Поддержка локальная и облачная для любой инфраструктуры
- Наше решение обеспечивает оптимизированную настройку и контроль.
- Аутентификация на основе пунктов и Технология единого входа как стандарт.
- Интегрирует с сотнями приложений
- Обеспечивает максимальное принятие с широким выбором методов аутентификации – до десяти факторов!

Аутентификация доступа к любому

фолдеру, будь то вход в Office 365, для проделки электронной комерции или же вход в ERP для контроля стока.

- ✓ Сотрудники
- ✓ Клиенты
- ✓ Поставщики

Архитектура

Поддержка облачных и локальных сетей для любой системы

AuthControl Sentry® не имеет ограничений. Предназначен для аутентификации доступа к локальным и облачным приложениям, для клиентов, работников или поставщиков запрашивающих доступ.

Локальная архитектура

Доступ к внутренним системам через наш Active Directory Agent, локально установленное программное приложение которое избавляет от необходимости делиться вашим Active Directory через Интернет, поддерживая синхронизацию учетной записи пользователя.

Облачная архитектура

Зафиксированный IP: Каждый клиент AuthControl получает выделенный фиксированный IP для своей виртуальной сети. Нет общего ресурса, нет API, нет портала общего доступа или же общей базы данных.

Специальное предложение: AuthControl в облаке выделяет вам специальную виртуальную машину, индивидуально только для вас, поэтому вы можете ожидать полное управление и контроль что означает гибкость настройки решения для удовлетворения ваших взыскательных потребностей.

Частный брандмауэр: Мы предлагаем межсетевой и отдельный экран для каждого клиента, что дает индивидуальную безопасность и доступ к контролю данных.

Выберайте AuthControl Sentry® для аутентификации:

- Заинтересованные стороны - сотрудники, поставщики, и клиенты
- Доступ к приложением, к таким как: Office 365, Salesforce или SAP
- Конкретный вертикальный рынок, например финансовые услуги

Особенности

swivelsecure

Как стандарт – Метод Единого Входа

Функция Метода Единого Входа для AuthControl Sentry® это предоставление пользователям

возможности доступа ко всем своим приложениям, с единой аутентификацией, обеспечивая пользователям эффективную работу без нарушения безопасность.

Непрерывная безопасность

Swivel Secure предоставляет Единый Портал который дает возможность

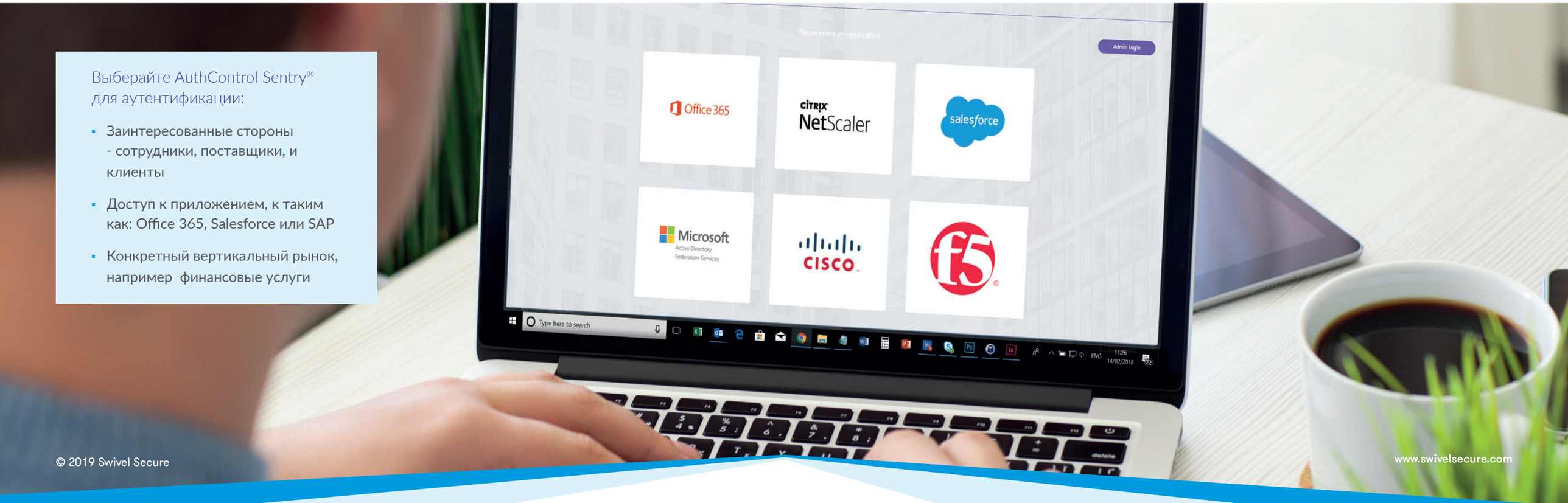
беспроблемного доступа для ваших пользователей. При использовании портала, необходимости каждого пользователя контролируемые, кроме того, в целях проведения аудиторских проверок, может быть отслежено, для повышенной безопасности и обеспечение подотчетности.

Рентабельный

Значительная экономия может быть достигнута за счет использования метода Единого Входа. Производительность увеличивается, так как при получении доступа к одному приложению, одновременно получают доступ ко всем остальным - экономия времени

Интуитивный

Метод Единого Входа был разработан для того чтобы дать пользователям возможность получить доступ ко всем приложениям при единой аутентификации, использовая механизм политики на основе баллов. Независимо от того, к каким приложениям пользователи хотят получить доступ, через VPN, по локальной сети или через облако, доступ будет автоматически направлен на аутентификацию с использованием Метода Единого Входа в Едином Портале



Особенности

Как стандарт – Аутентификация на основе пунктов

Аутентификация на основе пунктов (RBA) является особенностью AuthControl Sentry®, разработанная для автоматического запроса соответствующего уровня аутентификации для доступа к приложениям. Основан на параметрах, установленных заранее админом. RBA будет запрашивать соответствующий уровень аутентификации для доступа к приложениям на основе пользователя, их устройств и приложение.

Динамичный и умный

Адаптируется к обстоятельствам пользователя в том числе:

- К каким приложениям они пытаются получить доступ
- К какой групе пользователей они относятся
- Место нахождение при пролучения доступа
- Какое устройство они используют

Механизм политики

Основан на системе баллов, адаптивный механизм проверки подлинности позволяет админу устанавливать параметры для пользователя и приложений

- Группа пользователя
- Доступ к приложению
- IP Адрес
- Последняя аутентификация
- X.509 Cert
- Устройство
- Место нахождения (GeoIP)
- Geo Velocity

Аутентификация на основе пунктов: Пример 1

Сотрудница прилетела в Азию на встречу с поставщиком. Она только закончила обедать и вспомнила что забыла проверить некоторые пункты относительно встречи с поставщиком. Она думала что может быстро получить доступ к системе ERP используя мобильный телефон

Система ERP	
Система запрашивает 120 баллов	
LAN	0
Зарегестрированый ранее IP адрес	0
Устройство	50
Место нахождения (Asia)	-100
Требуется для аутентификации	
U&P	10
Мобильное приложение	60
Отпечаток пальца	20

Результат – В доступе отказано

Хотя она и использует телефон компании чтобы получить доступ к ERP, ее актуальное место нахождения не позволяет ей получить доступ, минус 100 пунктов. Она не сможет получить доступ даже при помощи многофакторной аутентификации

Аутентификация на основе пунктов: Пример 2

Менеджер по продажам находится в офисе и хочет получить доступ к CRM чтобы создать папку для новый клиентов. Он использует комьютер компании и пытается получить доступ к приложению по локальной сети.

Система CRM	
Система запрашивает 120 баллов	
LAN	50
Зарегестрированый ранее IP адрес	50
Устройство	50
Место нахождения (US)	50
Требуется для аутентификации	
U&P	10
Мобильное приложение	60
Отпечаток пальца	20

Результат – доступ разрешен

Менеджер по продажам без сомнений набрал нужное колличество баллов, чтобы получить доступ к системе CRM. Как только он прошел аутентификацию может использовать Метод Единого Входа чтобы получить доступ к другим приложениям. Ему звонит ассистент по закупкам и работник может предоставить всю необходимую информацию так как доступ к системе CRM было получено успешно.

Предельная гибкость и контроль

Механизм политики дает возможность создавать новые стандарты и объединять их с уже существующими.

Особенности

Портал Пользователя

Портал Пользователя является характерной особенностью AuthControl Sentry®, направленной для предоставления возможности администраторам настраивать опции решения.

Портал пользователя дает возможность администратором предоставлять пользователям прямой доступ к приложениям.

Предоставление мобильного приложения

Мобильное преложение может быть предоставлено так же просто, как и изменение или запрос нового пароля для пользователя. По электронной почте, пользователь получает пошаговую детальную инструкцию с использованием мобильного приложения, а также QR код для конфигурации. Так что пользователь сможет получить доступ ко всем своим приложения, используя: - одноразовый код (OTC) или - PUSH-уведомление

Самообслуживание

Самообслуживание Портала Пользователя уменьшает любые затраты связанные с поддержкой

Повышения эффективности

Портал Swivel Secure разработан, чтобы обеспечить полную безопасность для пользователей и выполняет основные требования, в том числе:

- Изменение пароля
- Сброс пароля
- Настройки мобильного приложения
- Повторная синхронизация Токена.

Ограничения могут быть введены для безопасности политики, которое гарантирует вам, что выполняемые действия соответствуют протоколу безопасности.

технология

swivelsecure

Запатентованная технология PINsafe®

PINsafe® - это запатентованная технология, которая поддерживает такие факторы аутентификации как изображение PINpad®, PICpad и TURing, все это в пределах диапазона факторов аутентификации, доступных в AuthControl Sentry®, - решение многофакторной аутентификации, разработанное для защиты организаций от несанкционированного доступа к приложениям, сетям или же данным.

Как работает PINsafe®?

Каждому пользователю выдается пароль - однако именно этот пароль никогда не вводится

Когда пользователю необходимо пройти аутентификацию для получения доступа, система автоматически отправляет пользователю 10-ти значную строку с цыфрами или буквами. Эта строка безопасности может быть получена в виде туринга, PINpad®, PICpad или же получена в виде смс на мобильный.

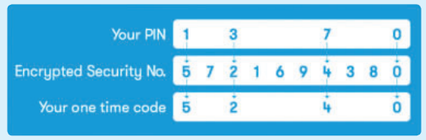
Зная пароль, ранее полученный админом можно извлечь из этой строки код для разового входа к приложениям.

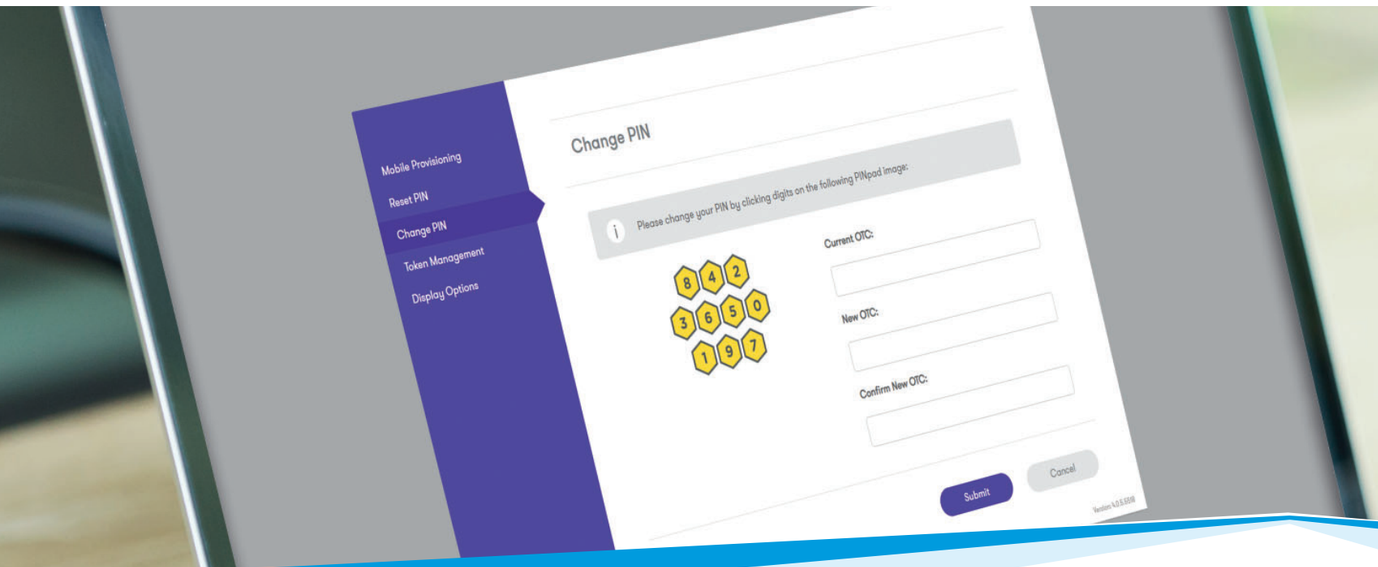
Можете привести пример?

Пример ниже - к примеру ваш пароль 1370. В соответсвии с 10-ти значной строкой безопасности 5721694380, ваш код для разового входа в систему 5240.

Эта строка безопасности интегрирует со многими устройствами и приложениями, в любом виде, включая:

- Вход в Windows
- Удаленный доступ к F5, Citrix Netscaler и Cisco VPN
- Веб-доступ к OWA, Apache и Microsoft ILS





С технологией PINsafe® нет необходимости ввода родного пароля, и это гарантирует полную безопасность от либо каких взломов системы, даннных и т.д.

Факторы

Факторы аутентификации

Swivel Secure предлагает широкий спектр факторов аутентификации, гарантируя, что каждая реализация приведет к максимальному внедрению во всей вашей организации.

Независимо от того используете вы мобильное приложение или токен для получение одноразового пароля, или отпечаток пальца, AuthControl Sentry® от Swivel Secure обеспечит максимальную безопасность, и может быть настроен в соответствии с потребностями безопасности вашего бизнеса.

AuthControl Mobile®: OTC (разовый код)

Каждый раз когда вам необходимо получить доступ, используйте разовый код в мобильном приложении. Так как вам предоставляется 99 разовых кодов, функция OTC достаточно универсальна при использовании офлайн. После ввода кода, вы получаете доступ к вашему приложению

Изображение PINpad®

Представлена в виде 10-значного кода в виде числовой сетки в браузере пользователя. Пользователь просто нажимает на изображения, которые соответствуют его паролю. Каждое нажатое изображение передает AuthControl Sentry® другой код ТС для аутентификации пользователь

Изображение PICpad

PICpad - это фактор аутентификации, который выходит за рамки обычных возможностей для языковой диверсификации как сотрудников, так и клиентов.

Используя те же принципы, что и PINpad®, PICpad состоит из символов вместо цифр.

AuthControl Mobile®: PUSH

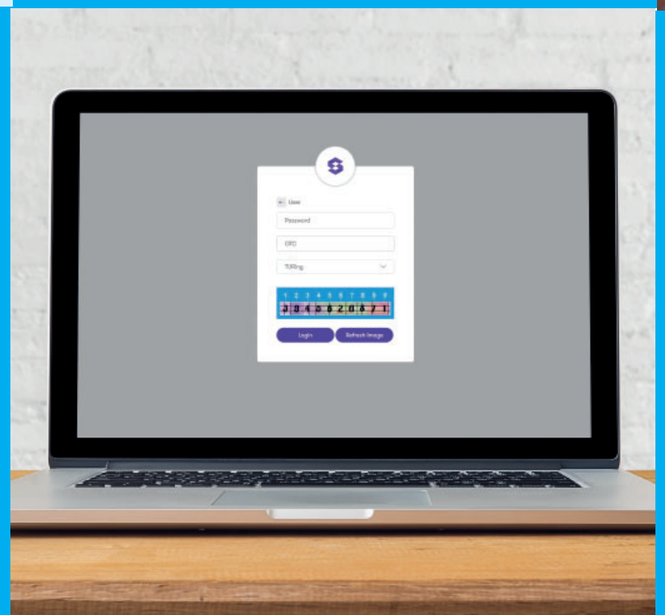
Просто нажав кнопку в приложении мобильного телефона, вы можете подтвердить аутентификацию с уведомлением, отправленным непосредственно на ваш мобильный.

Реализуйте функциональность One Touch® быстро и с минимальной конфигурацией

Изображение: TURing

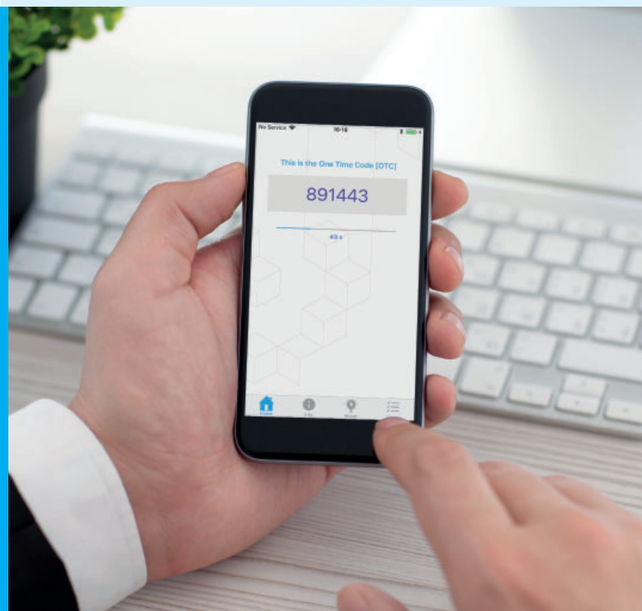
10-значный код представлен в виде прямоугольного изображения в браузере. Затем пользователь нажимает на цифры которые соответсвуют их паролю.

Пример: Если ваш пароль 1370, тогда нажмите на первую, третью, седьмую и десятую цифры на изображении



AuthControl Mobile®: OATH

OATH токен – это разовый код, который меняется через каждые 60 секунд. Код представлен в виде 6 знаков для аутентификации.



Телефон: СМС

Чтобы защитить ОТС (через SMS) от мошеннического перехвата, SMS защищен с помощью PINsafe®. Это означает, что SMS состоит из строки безопасности из двух буквенно-цифровых знаков, и в соответствии с родным паролем предоставляется доступ в систему.

Биометрия: Отпечаток пальца

Биометрия доступна для AuthControl Credential® Provider с использованием Windows 10,а также NITGEN. Пользователи могут проходить аутентификацию с помощью NITGEN контроллер отпечатков пальцев или с помощью встроенного считывателя отпечатков пальцев в ноутбуке.

AuthControl Voice

Позвонив пользователю, AuthControl Voice озвучивает либо одноразовый код (ОТС) или PUSH-уведомление (YES или NO) для аутентификации доступа к приложениям. При запросе нужно ввести код, полученный оператором по телефону.

Устройство Токен

С помощью токена, пользователь получает разовый код для доступа к приложениям компании. Каждый раз нажимая на токен, устройство отображает новый код для получения доступа к системе

swivelsecure

Интеграция

AuthControl Sentry® является одним из самых гибких решений, интегрирует с сотнями приложений и программным обеспечением через RADIUS, ADFS, SAML и наши собственные API - AgentXML.

Не зависимо от того, хотите ли вы получить доступ к Salesforce с помощью мобильного приложения, или получить доступ к Windows Credential Provider, используя аутентификацию в виде изображения, AuthControl Sentry® поддерживает широкий спектр приложений и устройств, обеспечивая полную безопасность для всей организация.

Лицензирование

Гибкие лицензионные планы, и по цене подходит любому предприятию. Одна лицензия предназначена одному пользователя.

Лицензия пользователя

Гибкие планы лицензирования, и цена подходящая для любой организации.

- Лицензия AuthControl Sentry® для определенного пользователя
- Каждая лицензия имеет все прелагаемые виды аутентификации
- MFA, SSO и RBA включены в AuthControl Sentry®
- Лицензирование на постоянной основе предлагает контракт на 1, 3, 5 или 7 лет

Локальная сеть

Лизензия на постоянной основе доступна для решений по локальной сети, а так же в облаке. Цена зависит от количество пользователей, начиная от 10 лицензий. Чем больше лецензий тем меньше цена. В идеале подходит для любых организаций

В Облаке

Лицензия на год доступна в Облаке и позволяет оганизациям соответствовать требованиям пользователей по мере изменения спроса. Никаких затрат заранее, выгодный договор, никаких штрафов. Идельное решение для организаций, которые хотят оптимизировать стоимость услуг с переменным числом пользователей.

Варианты лицензирования

Используйте приведенную ниже таблицу для сравнения вариантов локального и облачного лицензирования.

Лицензирование	На постоянной основе	В облаке
Аутентификация на основе пунктов	✓	✓
Интеграции (SAML/ADFS/RADIUS)	✓	✓
Лицензии на постоянной основе и Приложения в облаке	✓	✓
Все факторы аутентификации	✓	✓
AD Agent & AD Sync	✓	✓
Единый Портал вместе с Технологией единого входа	✓	✓
Уведомление	✓	✓
Оборудования (физическая и виртуальная машина)	✓	✗
Amazon AWS Image	✗	✓
24x7x365	По желанию	✓

Сервис и поддержка

Чтобы обеспечить организациям доступ к техническому обучению и новейшим функциям, мы предлагаем разные уровни поддержки: стандартный и премиум. У нас также есть профессиональные услуги по обновлению, развертыванию, миграции и комплексной интеграции

Договор о техническом обслуживании начального уровня

График Техподдержки: 8/5 доступ к software, апгрейд.

Стандартное соглашение об обслуживании

Часы поддержки: 24/5. Swivel Secure предлагает круглосуточную поддержу с пн. по пт

Договор о техническом обслуживании премиум

Техподдержка круглосуточно идеально подходит для бизнес-организаций, которым требуется немедленная экспертная поддержка.

Профессиональные услуги

Swivel Secure предлагает широкий спектр Профессиональных Услуг для организаций, нуждающихся в дополнительных услугах или технических ресурсах при развертывании многофакторной аутентификации, гарантируя совместимость с системами, подключениями и аппаратным обеспечением.

Услуги Менеджера по работе с клиентами по технической части

Наш сервис предлагает вам активное руководство и централизованное управление услугами, гарантирующее преимущества и приоритетную поддержку в рамках канала обслуживания.

Нужно обновить устройство Swivel Secure?

Swivel Secure известны проблемы, которые могут возникнуть во время апгрейда, и предлагает услугу обновления, что обеспечивает минимальное нарушения работы сервера.

Ваша сетевая инфраструктура очень сложная и требует многочисленных интеграций?

Наша команда опытных инженеров работает в тесном сотрудничестве с вашими техническими архитекторами и департаментом по закупкам, чтобы беспечить:

- Любая предложенная разработка адаптируется к вашей сетевой архитектуре.
- Разработка соответсвует вашим организационным архитектурным требованиям и требованиям контроля изменений

Вам нужно интегрировать новое устройство RADIUS или SAML без предварительной интеграции для работы?

Наша команда разработчиков программного обеспечения всегда готовы:

- Проанализировать и разработать любые новые интеграции
- Облегчить новые плагины
- Ответить на запросы по улучшению программного обеспечения