INDEED ID

WHITE PAPER

INDEED ACCESS MANAGER

Централизованная аутентификация и контроль доступа пользователей

Содержание

Надежная аутентификация и централизованное управление доступом

Защита доступа к корпоративным ресурсам является одной из основных задач информационной безопасности компании. Важными элементами решения этой задачи являются надежная аутентификация пользователя и централизованное управление доступом.

Выбор технологии аутентификации

Выбор технологии надежной аутентификации зависит от нескольких параметров:

- Применимость - пользовательские сценарии могут существенно ограничивать выбор технологий аутентификации. Например, большинство удаленных сценариев делают нецелесообразным применение подключаемых к рабочей станции пользователя устройств аутентификации.

- Безопасность - на сколько технология аутентификация отвечает потребностями организации в области ИБ. Например, одноразовые пароли обеспечивают адекватный уровень защиты для большинства удаленных сценариев, с другой стороны, организация может быть вынуждена применять иные технологии для соответствия внешним требованиям, таким как требования регуляторов или отраслевые стандарты.

- Удобство - насколько конечным пользователям будет комфортно применять ту или иную технологию в условиях их работы. Например, доступ к рабочему столу с использованием одноразовых паролей может быть неудобен, т.к. потребует генерировать и вводить пароль много раз в течение рабочего дня.

- Стоимость использования технологии аутентификации складывается из нескольких составляющих: стоимость внедрения; возможность использования имеющегося парка устройств аутентификации; стоимость владения; сложность интеграции технологии аутентификации с целевыми информационными системами.

Централизованное управление доступом

Сотрудники имеют доступ к широкому перечню информационных систем, контролируемых разными группами администраторов (Active Directory, базы данных, прикладные системы). Для управления таким доступом требуется специализированное централизованное решение, которое позволит:

- Собрать информацию по доступным для пользователя информационным системам в одном месте;
- Реализовать механизм единого входа - Single Sign-On;
- Определять какие технологии аутентификации должны быть использованы для входа в каждую информационную систему;
- Запрещать доступ к информационным системам;
- Вести журнал получения сотрудником доступа

Централизация достигается использованием различных технологий и протоколов интеграции в части аутентификации пользователей, в зависимости от того, что поддерживает целевая система. Из-за большого разнообразия приложений и используемых ими технологий, единого механизма интеграции не существует. Поэтому важно, чтобы система управления доступом поддерживала разные механизмы и протоколы интеграции с целевыми приложениями, что позволит охватить

максимальное число информационных систем.

Indeed Access Manager

Программный комплекс Indeed Access Manager (Indeed AM) представляет собой платформу для построения системы централизованного управления доступом пользователей к информационным ресурсам компании.

Indeed AM реализует возможность использования технологий строгой и многофакторной аутентификации пользователей при доступе к информационным ресурсам. Такие технологии сокращают риски информационной безопасности, дополняя или заменяя пароли. Поддерживаются различные способы аутентификации, за счет этого Indeed AM адаптируется к требуемым сценариям доступа и в каждом конкретном случае предлагает пользователям оптимальную технологию аутентификации.

Помимо различных технологий аутентификации, Indeed AM использует широкий спектр технологий интеграции, которые позволяют подключить целевые приложения к системе аутентификации. Такие технологии включают реализацию подхода Single Sign-On (web и enterprise sso), стандартизированные протоколы аутентификации и агентские модули. Indeed Access Manager позволяет организовать контролируемый доступ к информационным ресурсам как из внутренней сети компании, так и к системам, доступным из внешней сети, таким как почта, VPN, VDI и web-порталы. Такой подход позволяет построить централизованную систему предоставления доступа, которая охватывает все используемые целевые системы, минимизирует количество обращений пользователей в службу help desk, сокращает расходы на сопровождение инфраструктуры и повышает эффективность работы пользователей.

Платформа Indeed Access Manager

В основе платформы лежат базовые модули, которые реализуют бизнес-логику системы и обеспечивают функционирование серверной инфраструктуры и инструментов управления (рис. 1). К базовым модулям Indeed AM относятся:

Сервер аутентификации и управления Indeed AM. Сервер является ядром системы и обеспечивает функционирование всей платформы, он выполняет аутентификацию пользователей и реализуют бизнес-логику решения. Сервер представляет собой ASP .Net приложение и поддерживает установку в режиме кластера, позволяя обеспечить высокий уровень производительности и отказоустойчивости вне зависимости от масштабов внедрения.

Политики доступа определяют правила доступа, какие технологии аутентификации и для каких приложений должны быть использованы, а также задают область действия прав операторов и администраторов системы.

Роли определяют полномочия при работе в консоли управления Indeed AM. В системе имеется три роли:

- Администратор — имеет полный доступ ко всем функциям и настройкам.
- Оператор — имеет полномочия на работу с пользователями системы.
- Инспектор — имеет доступ на чтение.

Права с помощью ролей могут быть выданы как на всю системы целиком, так и в рамках отдельных политик.

Хранилище данных. Все данные системы хранятся в едином хранилище, к которому напрямую обращается только сервер. Хранение и передача данных к/от сервера производится в зашифрованном виде. Хранилище может быть расположено либо в каталоге Active Directory (расширение схемы не производится), либо в SQL СУБД.

Журнал событий. Все события изменения настроек и получения доступа фиксируются в едином журнале, который расположен на выделенном сервере. Журнал может хранится в формате Windows Event Log, либо в собственном формате Indeed AM в SQL СУБД, кроме этого, поддерживается отправка событий в сторонний журнал по протоколу syslog.

Консоль управления выполнена в формате web-приложения, в котором администраторы AM могут просмотреть и изменить параметры системы и настройки пользователей, а также просмотреть журнал системы.

Консоль пользователя дает возможность зарегистрировать или изменить аутентификационные данные (смарт-карты, генераторы одноразовых паролей, отпечатки и др.), а также просмотреть историю входов.

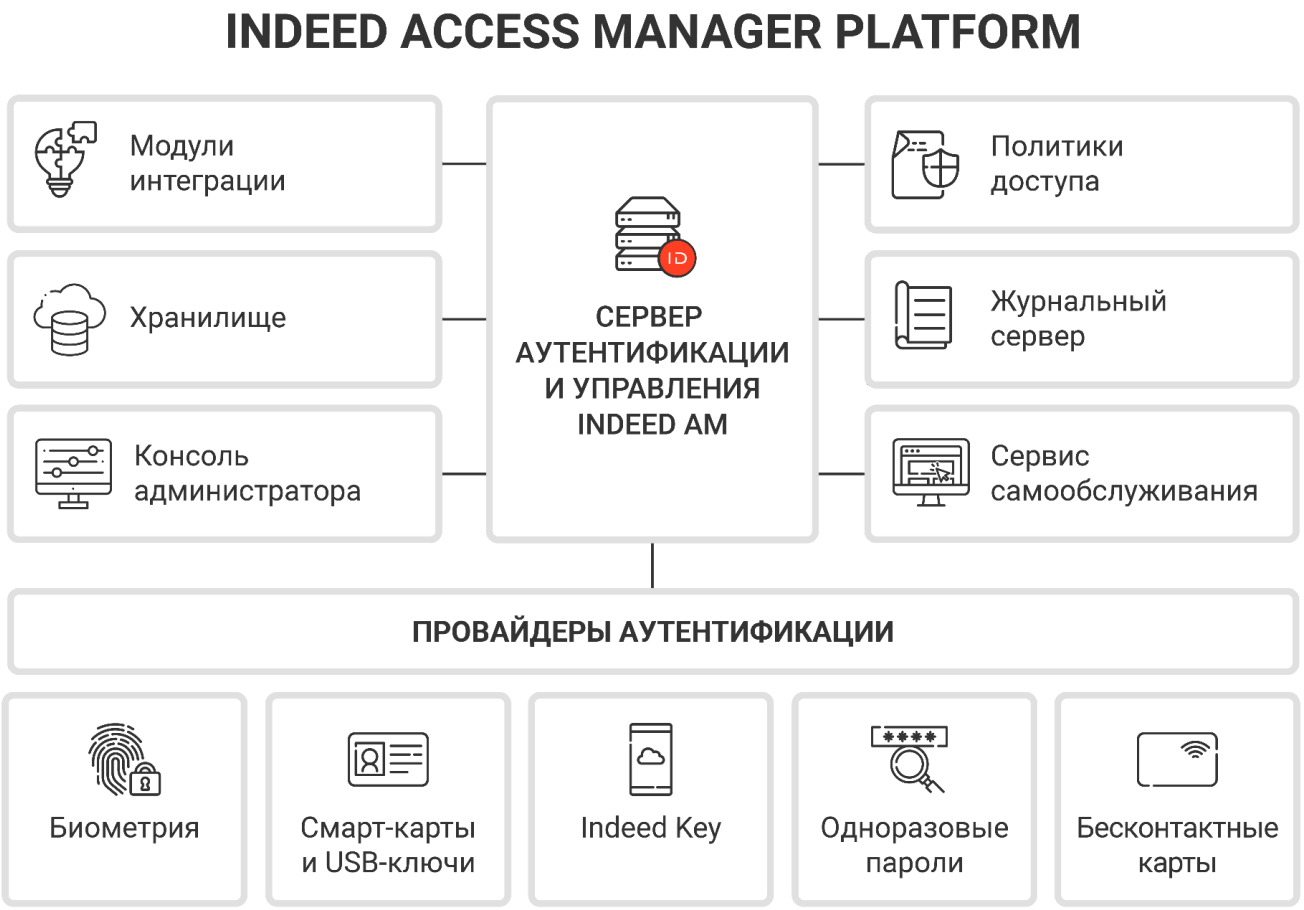

Рисунок 1. Платформа Indeed Access Manager

Провайдеры аутентификации обеспечивают Indeed AM возможность работы с технологиями аутентификации пользователей. Провайдер аутентификации предоставляет системе унифицированный интерфейс для выполнения операций по работе с конкретной технологией аутентификации: получение аутентификационных данных от пользователя для хранения, а также верификацию (проверку) данных. Indeed Access Manager поддерживает следующие технологии аутентификации:

- Криптографические смарт-карты и USB носители, такие как Рутокен, eToken, JaCarta и др.

- Бесконтактные RFID карты (используемые в качестве пропуска в СКУД системах) форматов EM-Marin, HID iClass, HID Proximity, Mifare.
- Аппаратные и программные токены генерации одноразовых паролей по протоколам OATH TOTP и HOTP.
- Одноразовые коды, высылаемые по SMS или Email.
- Биометрические технологии - отпечатки пальцев, рисунок вен ладони, изображение лица.
- Out-of-band аутентификация с использованием мобильного приложения и push-уведомлений на базе продукта Indeed Key. Мобильное приложение Indeed Key доступно для операционных систем iOS и Android. Используя Indeed Key, пользователь подтверждает операцию входа в приложении на смартфоне. Детали операции отображаются на экране смартфона, где пользователь может убедиться, в какую именно систему выполняется вход. Кроме этого, Indeed Key поддерживает генерацию одноразовых паролей по протоколу TOTP.

Различные технологии можно объединять в один способ аутентификации, реализуя таким образом мультифакторную аутентификацию (MFA).

Модули интеграции

Каждый модуль интеграции может использоваться отдельно и предназначен для решения задачи по защите доступа и аутентификации пользователей в конкретных приложениях. Модули спроектированы для совместной работы, что позволяет создавать любые конфигурации системы аутентификации, адаптируя ее под текущие нужды и ландшафт информационных систем предприятия.

Программный комплекс Indeed Access Manager включает в себя следующие модули интеграции с целевыми информационными системами:

Indeed AM SAML Identity Provider

Для организации многофакторной аутентификации и сквозного доступа в web-приложения (web single sign-on, WebSSO) используется модуль Indeed AM SAML Identity Provider (SAML IDP). Для интеграции с целевыми решениями этот модуль использует открытый международный стандарт аутентификации SAML 2.0 (Security Assertion Markup Language), что гарантирует совместимость с широким спектром коммерческих систем. Применение SAML избавляет пользователя от необходимости запоминать множество учетных данных, для доступа во все интегрированные системы требуется только один комплект учетных данных. Аутентификация выполняется централизованно на стороне SAML Identity Provider (IDP, поставщик удостоверений). Indeed AM SAML IDP выполнен в формате web-приложения и разворачивается в инфраструктуре заказчика. В процессе получения доступа, целевое приложение перенаправляет пользователя на страницу IDP для аутентификации, после чего, в случае успеха, пользователь перенаправляется обратно на целевое приложение с признаком “аутентифицирован”, где ему открывается его сессия.

Интеграция по протоколу SAML выполняется на серверной стороне, что дает возможность использовать MFA и WebSSO подход на любых устройствах, где есть браузер: ПК, смартфон или планшет.

Indeed AM SAML IDP поддерживает следующие технологии аутентификации пользователей в любых сочетаниях: доменный пароль, одноразовые пароли OATH TOTP и HOTP, одноразовые коды через SMS и EMail, out-of-band аутентификация с использованием мобильного приложения Indeed Key.

В контур WebSSO и MFA могут быть включены как корпоративные on-premise приложения, поддерживающие SAML (например, решения от компаний SAP, Citrix и др.), так и облачные сервисы,

такие как Office 365, Salesforce, Slack, Google Workspace (ранее G Suite) и другие.

Рисунок 2. Модули интеграции Indeed Access Manager

Indeed AM Windows Logon

Indeed AM Windows Logon (Windows Logon) представляет возможность получать доступ в Windows с использованием технологий строгой аутентификации в среде Microsoft Active Directory. Для этого на рабочие места пользователей устанавливается агент Windows Logon. Инсталлятор агента реализован как стандартный пакет установщика MSI (Microsoft Windows Installer). Это позволяет оперативно производить установку и обновление системы в массовом порядке с использованием различных инструментов, таких как групповые политики Active Directory, Microsoft System Center Configuration Manager (SCCM) и др.

Для интеграции с операционной системой Windows используются стандартный механизм для реализации собственного интерфейса аутентификации пользователей - Credentials Provider. Данная технология позволяет сторонним разработчикам интегрировать собственные технологии аутентификации с интерфейсом Windows, предоставляет возможность не только выполнять вход в

Windows с помощью технологии Indeed AM, но и аутентифицироваться с помощью Indeed Access Manager внутри ОС, например, при доступе к доменным ресурсам, веб-приложениям и др.

В Windows Logon поддерживаются все технологии аутентификации, доступные в Indeed Access Manager (смарт-карты, RFID карты, OTP, биометрия и др.).

Оффлайн режим

Для повышения отказоустойчивости, Windows Logon может создавать локальный кеш на ПК пользователя. Такой кэш содержит аутентификационные данные и используется в моменты, когда отсутствует связь с серверной инфраструктурой (оффлайн режим), например, вследствие обрыва связи или в командировке. Время жизни локального кэша можно ограничить количеством дней или календарной датой, кэш создается только для тех пользователей, для кого это явно разрешено администратором Indeed AM. Для защиты локальных данных используется технология Windows Data Protection API.

Режим замещения сотрудника

Indeed AM Windows Logon поддерживает режим замещения сотрудника, для этого администратор имеет возможность назначить заместителя для определенного пользователя. В таком режиме заместитель, с помощью своих аутентификационных данных (карты, отпечатка и др.) может выполнить вход в ОС от имени замещаемого пользователя. При этом в журнале системы будет содержаться информация о том, что вход выполнил именно заместитель. Такой режим полезен, когда необходимо срочно выполнить какое-то действие (например, отправить годовой отчет) от имени пользователя, который в данный момент недоступен (болен, находится в отпуске). Период замещения можно ограничить календарными датами.

Автоматическая идентификация пользователей (режим киоска)

Данный режим характерен тем, что одно рабочее место используется большим числом сотрудников и переключение между их рабочими сессиями должно выполняться оперативно. Для максимального удобства в данном режиме рекомендуется использование бесконтактных (RFID) или контактных PKI смарт-карт, в этом случае сценарий доступа выглядит следующим образом:

1. Для идентификации пользователям не требуется указывать имя пользователя, достаточно предъявить смарт-карту. Для этого киоск оборудуется считывателем карт.
2. Система может требовать наличие карты на считывателе в течение всего времени работы на ПК, при убирании карты текущая сессия может быть заблокирована или завершена.
3. При прикладывании к считывателю новой смарт-карты, текущая сессия может либо завершаться, либо переключаться на сессию подошедшего сотрудника.
4. К карте может быть добавлена биометрическая аутентификация для дополнительной защиты доступа (например, бесконтактная биометрия с использованием рисунка вен).

Управление паролями пользователей Active Directory

Indeed Access Manager не заменяет штатную систему аутентификации Active Directory, а автоматизирует управление паролями пользователей. В такой конфигурации парольная аутентификация становится внутренним механизмом, который используется только на программном уровне. Администратор Indeed Access Manager может настроить систему таким образом, чтобы в момент регистрации для пользователя первого аутентификатора его пароль автоматически меняется на случайное значение, которое не сообщается ни пользователю, ни администратору системы. Таким образом, доступ в домен становится возможным только с использованием Windows Logon. В дальнейшем пароль пользователя меняется автоматически либо по требованию операционной

системы, либо по заданному расписанию.

Indeed AM RDP Windows Logon

Модуль Indeed AM RDP Windows Logon (RDP Windows Logon) используется для реализации двухфакторной аутентификации при подключениях по протоколу RDP. В этом случае первым фактором выступает доменный пароль, а вторым - одноразовый пароль (one-time password, OTP) или подтверждение входа в мобильном приложении Indeed Key. OTP может быть либо сгенерирован на стороне пользователя в приложении на смартфоне или с помощью специального брелока (OTP-токена), либо отправлен ему по SMS или Email.

RDP Windows Logon следует устанавливать на конечный терминальный сервер, куда выполняет вход пользователь. Установка каких либо компонент на клиентский ПК не требуется. Поддерживается конфигурация с Remote Desktop Gateway.

Indeed AM Enterprise Single Sign-On (Enterprise SSO)

Indeed AM Enterprise Single Sign-On (Enterprise SSO) реализует подход single sign-on для унаследованных приложений, которые не поддерживают механизмы SSO. Система централизованно хранит пароли пользователя от всех приложений, требующих ввода учетных данных и автоматически подставляет их в экранные формы, когда приложение того требует. Технология Enterprise SSO может быть применена для любых типов приложений (windows, java, web, .net), независимо от архитектуры: одно-звенная, двух-звенная, трех-звенная, “толстый” клиент, “тонкий” клиент, терминальные приложения.

Enterprise SSO избавляет сотрудников от запоминания и хранения паролей в секрете, от ручного ввода паролей с клавиатуры, от периодической смены паролей согласно парольным политикам безопасности.

Для этих целей на рабочей станции пользователя устанавливается Enterprise SSO агент, который отслеживает запуск приложений и выполняет перехват форм аутентификации, когда они появляются на экране. Агент также включает в себя расширения для популярных браузеров (Internet Explorer, Google Chrome, Mozilla Firefox), что позволяет работать с веб-приложениями.

Принцип интеграции Enterprise SSO с целевыми системами

Enterprise SSO позволяет настраиваться на работу с приложением без программного вмешательства в серверную или клиентскую части данного приложения. Поддержка нового приложения подразумевает создание специального шаблона xml-формата, реализация которого выполняется на внутреннем языке Indeed AM Enterprise SSO скриптового типа. Язык позволяет указать, на какие формы приложения необходимо определить реакцию. Реакция Enterprise SSO может включать в себя повторную строгую аутентификацию пользователя, заполнение полей регистрационными данными (например, логин, пароль), нажатие необходимых элементов управления (например, нажатие кнопки “Вход”), запись события в аудит-журнал и т.п.

Смена пароля в целевом приложении

В целях минимизации рисков информационной безопасности, большинство информационных систем поддерживают возможность требовать от пользователя изменить значение пароля сразу после того, как пользователь осуществил первый вход в систему, либо по истечении заданного времени жизни пароля. Enterprise SSO обрабатывает данную ситуацию и позволяет в автоматическом режиме (прозрачно для пользователя) заблокировать на этот момент доступ пользователя к окну смены

пароля, сгенерировать новое значение, заполнить поля формы “новое значение” и “подтверждение”, нажать кнопку “OK”. Дождавшись от целевой системы уведомления об успешной смене пароля, Enterprise SSO агент сохраняет новое значение в базе данных Indeed AM. С этого момента ни пользователь, ни администратор не знают новое значение пароля и, следовательно, не могут войти в целевую систему в обход Enterprise SSO.

Возможность обрабатывать ситуацию смены пароля появляется только в том случае, если ESSO шаблон приложения поддерживает реакцию на появление данного типа окна.

Поддержка терминальной среды исполнения

Indeed AM Enterprise SSO адаптирован к работе в терминальной среде, позволяя избавить сотрудников от явного использования своих паролей в моменты, когда работа с приложением происходит внутри терминальной сессии. Для этого агент Enterprise SSO должен быть установлен на терминальном сервере.

В некоторых ситуациях, в момент получения доступа к особо критичным приложениям, от сотрудника может потребоваться пройти дополнительную процедуру аутентификации. Если технология предполагает использование внешнего оборудования, подключенного к ПК сотрудника (например, сканер отпечатка пальца), то между агентом Enterprise SSO терминального сервера и оборудованием возникает коммуникация. Enterprise SSO осуществляет коммуникацию по протоколам Microsoft RDP или Citrix ICA. Это означает, что на стороне ПК сотрудника не требуется установка дополнительного программного обеспечения за исключением драйвера и набора run-time библиотек, необходимых для работы оборудования.

Indeed AM ADFS Extension

Web-приложения на базе сервера Internet Information Services (IIS) могут быть интегрированы с программным комплексом Indeed AM с использованием механизма ADFS и компонента Indeed AM ADFS Extension. Компонент ADFS Extension реализует провайдер мультифакторной аутентификации для сервера Microsoft ADFS, добавляя в процесс получения доступа второй фактор. Такой подход дает возможность интегрироваться с целевыми приложениями без их модификации: при входе в приложение пользователь перенаправляется на веб страницу аутентификации ADFS, где через провайдер аутентификации Indeed AM ADFS Extension у него запрашивается второй фактор, после успешной аутентификации пользователь возвращается в целевое приложение.

Технологию ADFS поддерживают веб-приложения Microsoft, такие как Outlook Web Access, Sharepoint, Skype for Business и др..

Indeed AM ADFS Extension в качестве второго фактора поддерживает аутентификацию с помощью одноразовых паролей OATH TOTP и HOTP, одноразовых кодов через SMS и EMail и out-of-band аутентификации с использованием мобильного приложения Indeed Key.

Indeed AM IIS Extension

Для аутентификации в web-приложениях, использующих Internet Information Services (IIS), и не поддерживающих механизм ADFS, нами разработан специализированный модуль интеграции Indeed AM IIS Extension. Данный модуль устанавливается на веб-сервер, где развернуто целевое приложение и позволяет обеспечить двухфакторную аутентификацию без вмешательства в его программный код. Модуль перехватывает попытки аутентификации и после ввода имени и пароля, пользователь перенаправляется на отдельную страницу, где должен подтвердить себя с помощью

одноразового пароля.

Также поддерживается режим однофакторной аутентификации. Такой режим востребован для приложения Exchange ActiveSync (EAS) и позволяет исключить доменный пароль из схемы аутентификации. Для доступа к EAS в этом случае используется недоменный пароль, который по сути представляет собой так называемый application password, используемый только для EAS. Этот пароль вводится пользователем в мобильном клиенте для доступа к корпоративной почте.

IIS Extension может использоваться для любых web-приложений на базе IIS, например Outlook Web Access, RD Web Access, Exchange ActiveSync и др.

Indeed AM NPS RADIUS Extension

Indeed AM NPS RADIUS Extension (RADIUS Extension) представляет собой модуль расширения Microsoft Network Policy Server (NPS, входит в состав Windows Server) и позволяет реализовать для RADIUS-совместимых сервисов и приложений технологию двухфакторной аутентификации. Для этого требуется:

- Развернуть в сети предприятия NPS сервер, который предоставляет возможность аутентификации по протоколу RADIUS с использованием учетных данных пользователей каталога Active Directory.
- Настроить целевое приложение на аутентификацию пользователей по RADIUS протоколу на сервере NPS.
- Установить на NPS сервер расширение Indeed AM NPS RADIUS Extension, которое будет обрабатывать запросы на аутентификации и требовать от пользователя второй фактор аутентификации.

Аутентификация по второму фактору выполняется на сервере Indeed Access Manager и результат проверки через NPS сервер транслируется в целевое приложение.

Indeed AM NPS RADIUS Extension в качестве второго фактора поддерживает аутентификацию с помощью одноразовых паролей OATH TOTP и HOTP, одноразовых кодов через SMS и EMail и out-of-band аутентификации с использованием мобильного приложения Indeed Key.

Аутентификация по RADIUS протоколу может быть использована во многих VPN и VDI решениях, например, в программных продуктах компаний Cisco, Citrix, Check Point, VMWare, C-Терра.

Indeed AM API

Indeed AM API представляет собой программный интерфейс формата REST API для интеграции со сторонними системами и приложениями. API может быть использован для двух целей:

- Реализация двухфакторной аутентификации. В случае, когда целевое приложение не поддерживает ни один из стандартов аутентификации, двухфакторная аутентификация может быть добавлена в него путем встраивания вызовов Indeed AM API. Такой подход может быть использован для приложений собственной или заказной разработки, когда есть возможность их доработки.
- Интеграция со смежными системами. Такая интеграция позволяет реализовать дополнительные сценарии по автоматизации работы с учетными данными или контролю доступа пользователей. Примерами таких сценариев являются интеграция с системами управления правами и учетными данными пользователей (Identity Management, IDM) и системами контроля физического доступа (СКУД).

Интеграция с Identity Management системами

Интеграция позволяет в автоматическом режиме создавать и наполнять профиль доступа пользователя для модуля Indeed AM Enterprise SSO. Коннектор к IDM системе позволяет в автоматическом режиме синхронизировать учетные данные пользователей в базе данных Enterprise SSO. Учетные данные создаются при помощи IDM-коннекторов к целевым системам и тут же сохраняются в подсистеме Indeed AM Enterprise SSO, избавляя сотрудника от запоминания и ручного ввода паролей. Интеграция позволяет получить такие преимущества:

- Повышение уровня информационной безопасности компании за счет полной автоматизации жизненного цикла паролей пользователей (пароли создаются, изменяются и вводятся полностью в автоматическом режиме, без участия пользователей и администраторов)
- Минимизация шагов в предоставлении и получении доступа сотрудниками. После занесения нового пользователя в исходную систему (например, HR-систему) и выполнения синхронизации (в автоматическом режиме), пользователь получает беспарольный доступ во все необходимые ему системы.

Схема интеграции Indeed AM Enterprise SSO с IDM

Рассмотрим схему работы на примере бизнес-операции принятия нового сотрудника на работу и использования для аутентификации при доступе к рабочему столу USB-ключа. Весь процесс можно условно разделить на 5 крупных шагов.

1. Сотрудник отдела кадров регистрирует запись о новом сотруднике в системе учета персонала (HR система).
2. После этого, данные о новом сотруднике попадают в базу данных IDM через коннектор к HR системе.
3. На основе этого события IDM выполняет операцию синхронизации, создавая для пользователя учетные записи во всех приложениях, согласно должности (бизнес-роли) сотрудника. Для данной операции используются специальные IDM-коннекторы.
4. По такому же принципу реализован коннектор к Indeed AM Enterprise SSO, который на заключительном шаге синхронизации создает профиль доступа сотрудника в БД Enterprise SSO, копируя в него учетные данные пользователя.
5. На данном шаге сотрудник имеет все необходимое для работы. После получения доступа к своему рабочему столу, агент Indeed AM Enterprise SSO обеспечивает для сотрудника прозрачный доступ во все необходимые приложения, подставляя учетные данные пользователя в формы входа в приложения.

Интеграция с СКУД

Интеграция с системами контроля и управления физическим доступом (СКУД) дает возможность Indeed AM учитывать местоположение сотрудника в момент его аутентификации. Это позволяет реализовывать, например, такие сценарии доступа:

- Разрешить доступ только при нахождении сотрудника внутри периметра здания (например, вход через проходную №1, №2 и №3);
- Разрешить доступ только в определенном кабинете (например, только в кабинете №5, не имеет значения, каким маршрутом сотрудник в него попал);
- С любого компьютера определенной зоны (например, к любому компьютеру 3 этажа).

О компании Индид

Компания «Индид» (indeed-id.ru) – российский разработчик программных комплексов в области информационной безопасности. За 10 лет компания самостоятельно разработала 4 программных комплекса для повышения уровня информационной безопасности и корпоративного использования в компаниях разных отраслей экономики. Результат внедрения продуктов компании не ограничивается только решением отдельных задач информационной безопасности. Программные комплексы обеспечивают выполнение требований регуляторов и реализацию соответствия нормативным документам (ГОСТ, ФСТЭК и др.), а также включены в Реестр отечественного ПО, что имеет важное значение для реализации требований программы импортозамещения в РФ. ПО внедрено на территории РФ и стран СНГ во многих компаниях разных отраслей экономики, а также в странах Европы и Азии.