Indeed Enterprise SSO
Сквозная и строгая аутентификация в корпоративных приложениях

Введение

Indeed Enterprise SSO помогает повысить производительность пользователей, сократить риски информационной безопасности, минимизировать количество обращений в службу help desk, сократить расходы на сопровождение инфраструктуры.

Indeed Enterprise SSO реализует подход single sign-on в масштабе предприятия. Система централизованно хранит пароли пользователя от всех приложений требующих аутентификации и автоматически подставляет, когда приложение того требует. Технология Indeed 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.

Indeed 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.

Список терминов и определений

Персональный профиль доступа сотрудника (профиль доступа сотрудника или esso-профиль) - перечень приложений и сетевых ресурсов, в которые система Indeed Enterprise SSO обеспечивает доступ. Для каждого ресурса фиксируется набор параметров и правил, уточняющих или ограничивающих предоставление доступа. Профиль доступа сотрудника может быть персональным, ролевым или смешанным.

Ролевой профиль доступа (сокращенно **роль**) - перечень приложений и сетевых ресурсов, которые типичны для определенной категории сотрудников (например, для сотрудников финансового отдела или сотрудников центрального офиса). Ролевой профиль может быть закреплен как за отдельным сотрудником, так и за целой группой сотрудников. Допускается определять сотруднику несколько ролей.

Смешанный профиль - профиль пользователя, составленный из объединения ролевого профиля и персонального профиля сотрудника.

Состав Indeed Enterprise SSO

В состав Indeed Enterprise SSO входят три базовых компонента:

- Indeed Enterprise SSO Агент
- Indeed Enterprise Server
- Indeed Enterprise Management Console

Indeed Enterprise SSO Агент (сокращенно ESSO Агент или Агент) - ПО, устанавливаемое на рабочее место сотрудника. В момент своей работы ESSO Агент запрашивает с сервера Indeed Enterprise Server перечень систем и учетных данных, которые составляют персональный профиль доступа сотрудника. Как только сотрудник запускает ярлык приложения, требующего ввода логин-пароль, ESSO Агент перехватывает регистрационное окно приложения, скрывает его от пользователя, автоматически заполняет (подставляет имя учетной записи и пароль полученные с сервера) и контролирует процедуру получения доступа в среду приложения. По результату операции в журнале событий системы фиксируется факт выполнения успешной или неуспешной попытки доступа.

Indeed Enterprise Server (сокращенно Сервер) - серверный компонент инфраструктуры Indeed Enterprise SSO. Сервер обеспечивает централизованное хранение и защиту данных пользователей, осуществляет процедуру аутентификации сотрудника с использованием методов, поддерживаемых решением, осуществляет прием и обработку запросов со стороны ESSO Агента или Консоли администратора.

Наличие сервера гарантирует пользователю доступность данных своего профиля с любого ПК организации. Сервер дает возможность администратору создавать, модифицировать или блокировать профиль и параметры доступа сотрудника (или группы сотрудников), вносить глобальные изменения в систему.

Indeed Enterprise Management Console (сокращенно Консоль) представляет собой web-приложение, доступное с любого ПК домена. С помощью консоли администраторы управляют настройками системы, параметрами (и правилами) доступа пользователей.

Дополнительно к основным компонентам, Indeed Enterprise SSO может комплектоваться следующими элементами, расширяющими возможности и функциональность системы:

Indeed ESSO TMS/SAM Connector - Расширение, обеспечивающее интеграцию системы управления жизненным циклом ключевых носителей SafeNet Authentication Manager с системой Indeed Enterprise SSO.

Коннектор позволяет совместить момент выпуска электронного ключа eToken, сертификата и паролей сотрудника, минимизируя за счет этого количество действий как it-администраторов, так и рядовых пользователей.

Indeed ESSO IdM Connector - Коннектор к Identity Management системам[1], позволяющий в автоматическом режиме синхронизировать учетные данные пользователей в базе данных Indeed ESSO. Учетные данные создаются при помощи IdM-коннекторов и тут же сохраняются в системе Indeed Enterprise SSO, избавляя сотрудника от запоминания и ручного ввода паролей. Интеграция позволяет получить следующие преимущества:

1. 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)
2. Минимизация шагов в предоставлении и получении доступа сотрудниками. После

[1] Для каждой IdM-системы применятся отдельный специально разработанный модуль интеграции.

занесения нового пользователя в исходную систему (например, HR-систему) и выполнения синхронизации (в автоматическом режиме), пользователь получает беспарольный доступ во все необходимые ему системы.

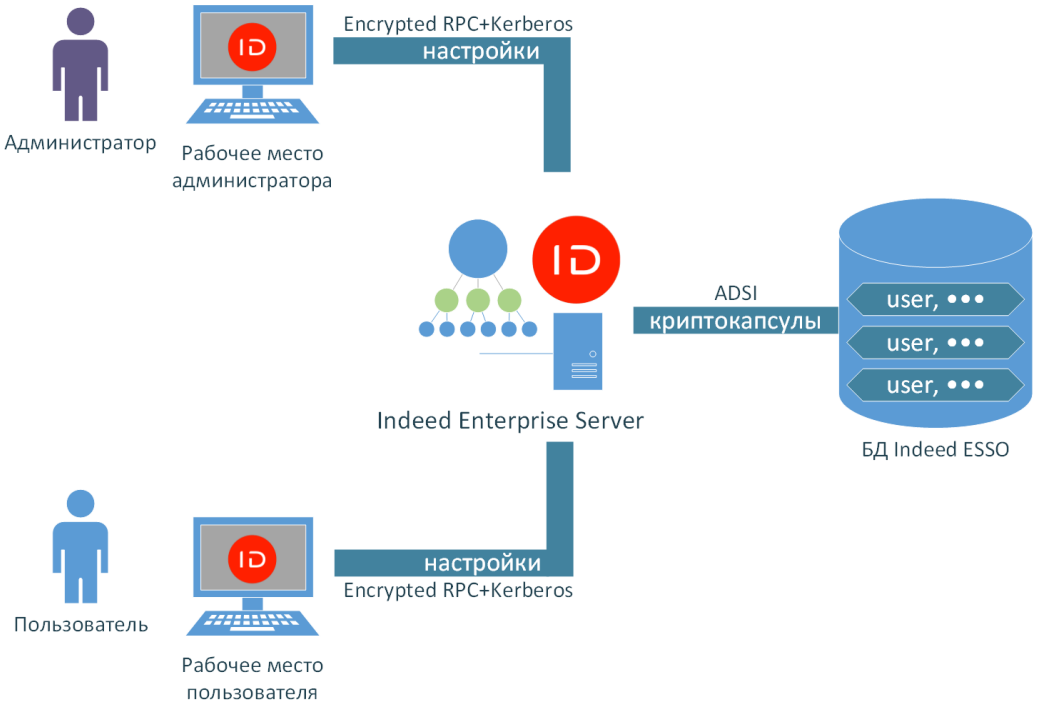
Протоколы коммуникации, хранение и защита данных

Для хранения данных Indeed Enterprise Server использует каталог Microsoft Active Directory (модификация схемы не требуется). Это обеспечивает резервирование и доступность данных для всех узлов системы.

Каждый раз когда требуется сохранить блок данных, Indeed Enterprise Server выполняет процедуры шифрования, хеширования и электронной подписи, обеспечивая тем самым конфиденциальность и контроль целостности записываемой информации. Это означает, что данные, курсирующие в направлениях “от” сервера или “к” серверу всегда передаются в защищенных “капсулах”. Распаковка и запаковка данных происходит внутри процесса Indeed Enterprise Server.

Для защиты данных Indeed Enterprise Server используются алгоритмы криптографического преобразования, входящие в состав CSP, установленного на сервере. По умолчанию используются алгоритмы CSP, встроенного в операционную систему Microsoft Windows Server. При наличии альтернативных CSP (например, КриптоПро), сервер может быть перенастроен на его использование.

Коммуникация Indeed Enterprise SSO Агента с сервером Indeed Enterprise Server осуществляется с использованием стандартного протокола Encrypted RPC, входящего в состав Windows-систем. Encrypted RPC обеспечивает защиту и контроль целостности передаваемого по сети трафика за счет встроенных в протокол алгоритмов. Encrypted RPC широко используется в Windows-среде, (например, в моменты репликации данных Active Directory) и, как правило, не требует дополнительных действий по настройке брандмауэров на ПК сотрудников.



Следует различать работу системы в режимах, когда Indeed Enterprise Server доступен ESSO Агенту (on-line, обычный режим работы сотрудника в офисе) и не доступен (off-line, режим работы сотрудника в командировке). При активации для конкретного сотрудника off-line режима,

Indeed Enterprise SSO Агент запрашивает с сервера и сохраняет копию профиля пользователя на локальном ПК, обеспечивая защиту уязвимых данных с использованием технологии Microsoft Protected Storage.

Поддержка методов надежной аутентификации

Дополнительно к классической технологии аутентификации, реализованной в большинстве single sign-on систем - с использованием универсального пароля (мастер-пароля), Indeed Enterprise SSO поддерживает свыше двадцати альтернативных технологий аутентификации. К ним относятся двух-факторная аутентификация, биометрия, смарт-карты и USB-ключи, бесконтактная карта, одноразовый пароль, одноразовая матрица, sms-технология и другие.

С точки зрения Indeed Enterprise SSO, каждая уникальная категория пользователей может использовать собственную, оптимальную для этой группы пользователей технологию аутентификации. Администратор системы имеет возможность предписать, какую технологию аутентификации должен использовать конкретный пользователь или группа пользователей.

Существуют ситуации, когда сотруднику может быть разрешено использовать несколько технологий:

- резервная технология на случай отказа основного способа
- временный способ с ограниченным сроком действия
- технология, адаптированная для работы в удаленном режиме
- комбинация технологий (мульти-факторная аутентификация)

Принцип интеграции Indeed Enterprise SSO с целевыми системами

Indeed Enterprise SSO позволяет настраиваться на любой тип приложений 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 Enterprise SSO скриптового типа. Язык позволяет указать, на какие формы приложения необходимо определить реакцию. Реакция Indeed Enterprise SSO может включать в себя повторный запрос аутентификации пользователя, заполнение полей регистрационными данными (например, логин, пароль), нажатие необходимых элементов управления (например, нажатие кнопки Вход), запись события в аудит-журнал и т.п.

Для упрощения процедуры создания шаблонов Indeed Enterprise SSO предоставляет набор инструментов, включающий визуальный редактор. С их помощью шаблон для типовой формы авторизации может быть создан в течение нескольких минут.

Большинство популярных систем уже интегрированы с Indeed Enterprise SSO: 1С Предприятие, Банк-Клиенты, IBM Lotus Notes, SAPGui, IBM Tivoli, Oracle eBusiness Suite, Novell Клиент, Microsoft Dynamics AX, Дело, Siebel, CSBI Банкир, Microsoft Outlook, Google Mail и др. Шаблоны для поддержки данных систем можно найти в библиотеке готовых шаблонов.

Обработка ситуации “смена пароля при первом входе в приложение”

В целях минимизации рисков информационной безопасности, большинство it-систем поддерживают возможность требовать от пользователя изменить значение пароля сразу после того, как пользователь осуществил первый вход в систему. Indeed Enterprise SSO Агент 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 “ОК”. Дождавшись от целевой системы уведомления об удачной смене пароля, Indeed Enterprise SSO Агент синхронизирует новое значение на сервере Indeed Enterprise Server. С этого момента ни пользователь, ни it-администратор не знают новое значение пароля и, следовательно, не могут войти в it-систему в обход Indeed Enterprise SSO.

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

Обработка ситуации “пароль устарел”

Еще одной мерой минимизации рисков информационной безопасности в современных ИТ-системах является ограниченный срок действия пароля. По окончанию данного интервала времени система требует от пользователя выполнить смену значения пароля. Indeed Enterprise SSO Агент реагирует на подобный запрос системы и в автоматическом режиме (прозрачно для пользователя) выполняет смену пароля. Механизм работы полностью аналогичен обработке ситуации “смена пароля при первом входе” (см. выше).

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

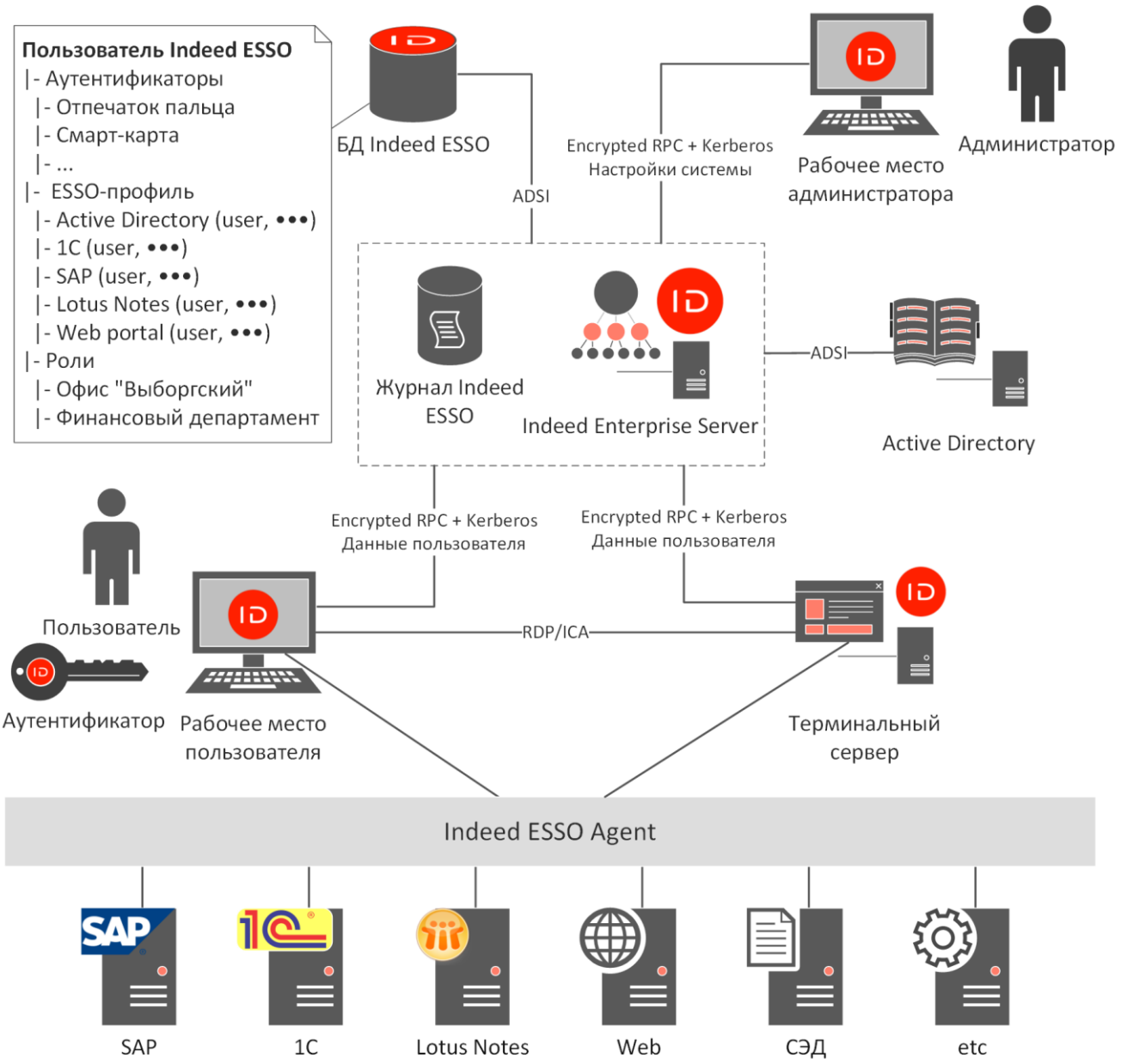
Поддержка терминальной среды исполнения

Indeed 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 Indeed Enterprise SSO Агент 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 Indeed Enterprise SSO Агентом терминального сервера и оборудованием возникает коммуникация. Indeed 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.

В составе решения Indeed Enterprise SSO имеется ряд технологий надежной аутентификации пользователей специально адаптированных под использование в терминальной среде. Некоторые из них не предполагают наличие дополнительного оборудования. Это положительно отражается на свободе перемещения сотрудников и позволяет работать даже с “неподготовленного” компьютера. Также, это позволяет вместо традиционного ПК использовать тонкого клиента Windows CE, Linux, Wyse и т.п.

Общая схема взаимодействия компонент Indeed Enterprise SSO



Аудит и отчетность

Все события, возникающие в системе Indeed Enterprise SSO, сохраняются в центральном аудит журнале формата Windows Event Log. Журнал фиксирует дату, время, имя пользователя, имя учетной записи Active Directory, имя учетной записи целевой системы, факт использования учетных данных, факт входа в целевые системы и т.п. В журнале фиксируется каким способом и с применением какой технологии аутентификации сотрудник получал доступ в систему.

Интеграция с Identity Management системами

Indeed ESSO поддерживает интеграцию с системами управления жизненным циклом и правами учетных записей пользователей (Identity Management, IdM). Интеграция позволяет в автоматическом режиме создавать профиль доступа пользователя в Indeed ESSO с необходимыми параметрами. Коннектор к IdM системе позволяет в автоматическом режиме

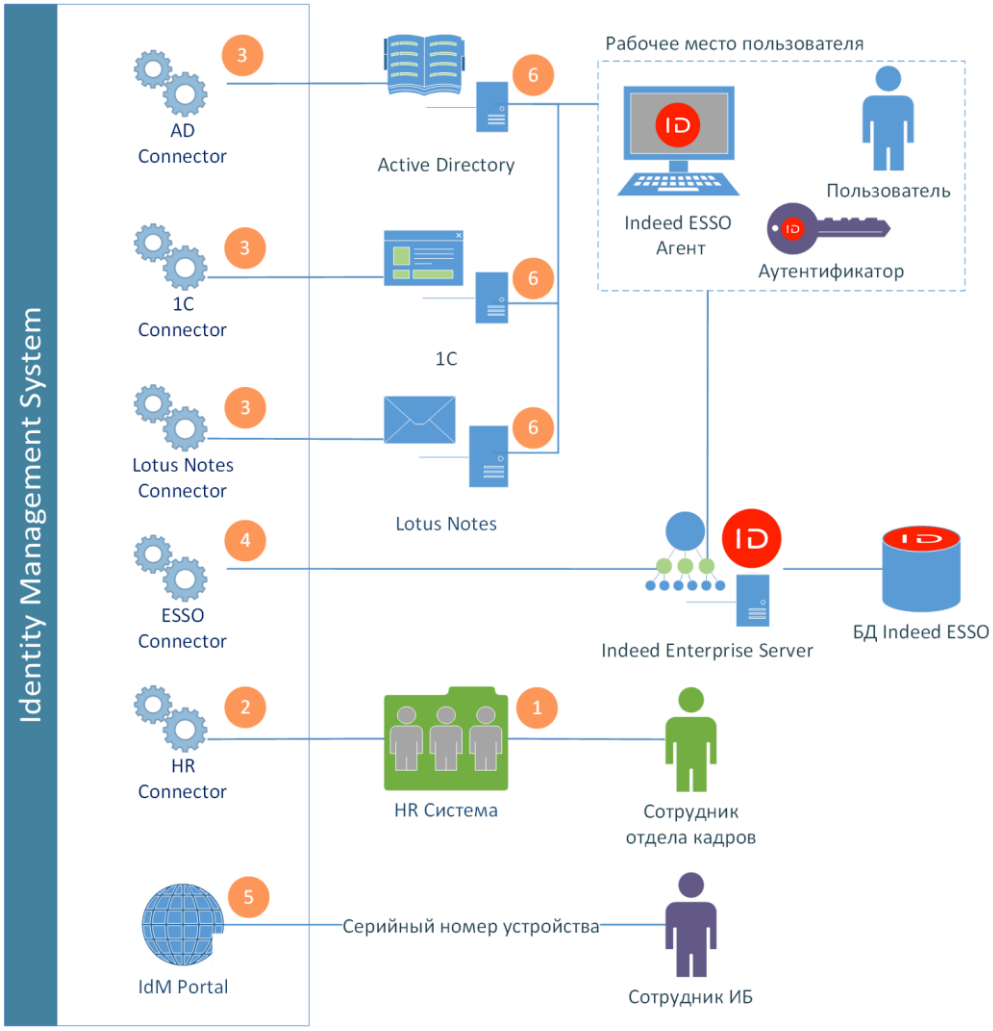
синхронизировать учетные данные пользователей в БД сервера Indeed Enterprise Server. Учетные данные создаются при помощи IdM-коннекторов и тут же сохраняются в системе Indeed Enterprise SSO, избавляя сотрудника от запоминания и ручного ввода паролей.

Цели интеграции Indeed Enterprise SSO с IdM

1. 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)
2. 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.
3. В случае использования аппаратных средств аутентификации, вынесении операции добавления аутентификатора в БД Indeed ESSO на сторону портала IdM (зависит от возможностей IdM).

Схема интеграции Indeed 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 6 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 коннекторы.

4. По такому же принципу реализован Indeed IdM Connector, который на заключительном шаге синхронизации создает профиль доступа сотрудника в БД Indeed Enterprise SSO, копируя в него учетные данные пользователя.

5. Дополнительно к учетным данным пользователя, в базе Indeed ESSO, может быть зарегистрирован аппаратный аутентификатор пользователя. Таким аутентификатором, например, может являться USB-ключ (eToken, ruToken и т.п.). Серийный номер ключа сотрудник информационной безопасности заносит через интерфейс специальной формы на портале IdM. Серийный номер ключа регистрируется в БД Indeed ESSO в качестве аутентификатора сотрудника.

   Примечание: Шаг 5 может быть пропущен, если аутентификация с использованием ключа не требуется (например, сохраняется стандартная схема ввода логин-пароля учетной записи Active Directory).

6. На данном шаге сотрудник имеет все необходимое для работы. Для доступа к рабочему столу он указывает имя своей доменной учетной записи, подключает USB-ключ и вводит PIN-код ключа. После выполнения успешной аутентификации, Indeed Enterprise SSO Агент обеспечивает для сотрудника прозрачный доступ во все необходимые приложения, подставляя учетные данные пользователя в формы входа в приложения.

Интеграция с Card Management System

Интеграция с системами управления ключевыми носителями (Card Management System, CMS) позволяет связать жизненный цикл смарт-карт и токенов с учетными данными пользователей. При этом носитель, выпускаемый сотруднику в системе CMS, автоматически регистрируется в базе данных Indeed ESSO. На данный момент уже реализованы модули интеграции с системами:

- Indeed Card Management (модуль входит в стандартную поставку)
- SafeNet Authentication Manager (SAM)
- JaCarta Management System.

Полный перечень продуктов Indeed ID

AirKey	**Indeed AirKey Cloud (Indeed AK Cloud)** Облачная платформа, реализующая операции электронной подписи, строгой аутентификации и доставки защищенных сообщений на смартфоне пользователя. **Indeed AirKey Enterprise (Indeed AK Enterprise)** Виртуальная смарт-карта, представляющая собой программную реализацию традиционной смарт-карты и позволяющая выполнять полный набор операций, доступный аппаратным ключевым носителям.
Card Management	**Indeed Card Management (Indeed CM)** Система управления жизненным циклом ключевых носителей и цифровых сертификатов.
Web Authentication	**Indeed Web Authentication (Indeed WA)** Система усиленной и двухфакторной аутентификации в web-приложениях и организации web single sign-on доступа.
Enterprise Authentication	**Indeed Enterprise Authentication (Indeed EA)** Доступ пользователей Active Directory к информационным ресурсам организации с использованием технологий строгой аутентификации. **Indeed EA Authentication providers** Библиотека модулей сопряжения системы Indeed EA (коннекторов) с устройствами аутентификации. Поддерживаются более 20 разных технологий аутентификации, в том числе технологии смарт-карт, биометрия, одноразовые пароли. **Indeed Rules System СКУД Connector** Интеграция с системами контроля и управления физическим доступом. Предоставляет дополнительный фактор (местоположение сотрудника на территории предприятия) при доступе к информационным системам.
Enterprise Single Sign-On	**Indeed Enterprise SSO (Indeed ESSO)** Организация сквозной и строгой аутентификации при доступе пользователей в информационные системы компании без необходимости модификации данных систем. **Indeed ESSO IdM Connector** Интеграция с системами управления жизненным циклом учетных записей: Microsoft FIM 2010, IBM Tivoli IdM, Trustverse КУБ, 1IDM, Sailpoint IdentityIQ. **Indeed ESSO TMS/SAM Connector** Интеграция жизненного цикла ключевых носителей eToken и жизненного цикла учетных данных пользователей.

Контактная и дополнительная информация

Наши контакты:

- inbox@indeed-id.com
- 8 (800) 333-09-06 (звонок по России бесплатный)
- +7 (495) 640-06-09 Москва
- +7 (812) 640-06-09 Санкт-Петербург

Интернет ресурсы о наших продуктах и технологиях:

- сайт indeed-id.ru
- блог blog.indeed-id.ru
- база знаний community.indeed-id.com
- подборка видеоматериалов youtube.com/user/IndeedID