inbox@indeed-id.com
www.indeed-id.com

Indeed-ID Rules System. Интеграция с системой СКУД.

Краткое описание

Октябрь 2010

Введение

Архитектура сервера Indeed-ID Rules System универсальна и подразумевает расширение функциональности за счет реализации коннекторов к внешним системам. Такой коннектор позволяет с минимальными усилиями интегрировать Indeed-ID с любой системой. Примерами внешних систем могут служить система СКУД, HR, DLP, RMS и т.д.

Используя коннектор, способный получать доступ к журналу событий внешней системы, либо способный оставаться подписанным на происходящие в ней изменения, Indeed-ID Rules System получает возможность отслеживать и анализировать внешнюю ситуацию, формируя соответствующую реакцию внутри Indeed-ID: отказ в предоставлении доступа к ресурсам, полная или частичная блокировка профиля пользователя, выбор альтернативной конфигурации в зависимости от условий работы сотрудника, уведомление администратора и т.п.

Цели интеграции Indeed-ID с системой контроля и управления физическим доступом (СКУД)

1. Повышение уровня информационной безопасности компании за счет добавления нового фактора в схему предоставления доступа к информационным ресурсам (фактор местоположения сотрудника)
2. Управление правилами предоставления доступа к информационным ресурсам с учетом местоположения сотрудника
3. Унификация процедуры доступа в здание и доступа к информационным ресурсам с использованием единственной карты сотрудника (использование карты опционально)

Примеры сценариев

Интеграция Indeed-ID Rules System с системой СКУД позволяет на практике реализовать следующие бизнес-сценарии:

- **Предоставление доступа к данным**
  - только при нахождении сотрудника внутри периметра здания (например, вход через проходную №1, №2 и №3)
  - только в определенном кабинете (например, только в кабинете №5, не важно каким маршрутом сотрудник в него попал)
  - только при соблюдении определенного маршрута (например, турникет проходной > пункт контроля 3 этажа > кабинет №5)
  - с любого компьютера определенной зоны (например, к любому компьютеру 3 этажа)
- **Автоматическое изменение**

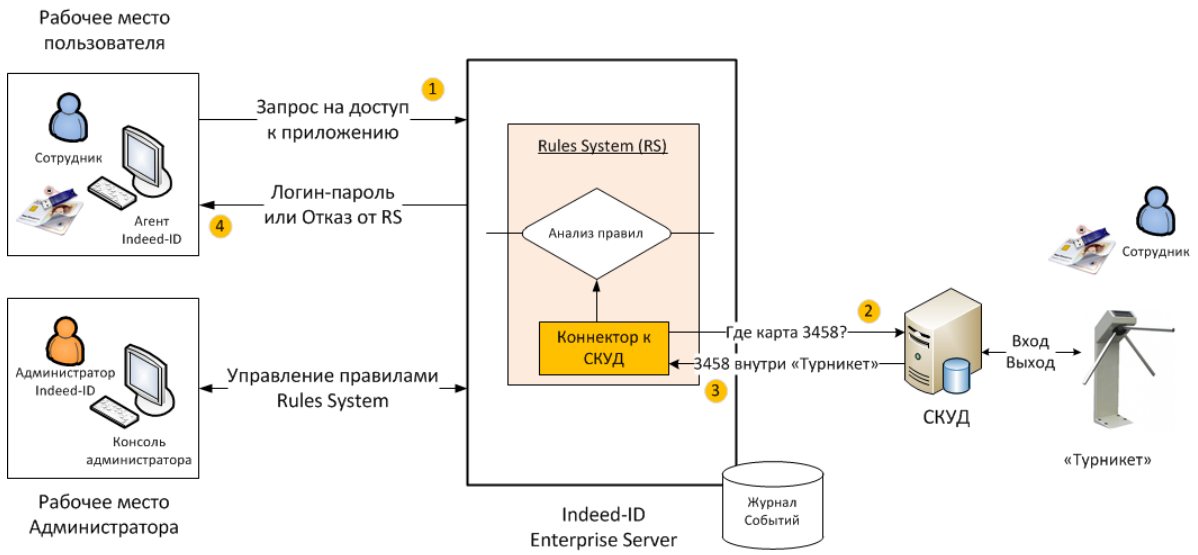
- параметров доступа в зависимости от местоположения сотрудника (внутри или снаружи здания, центральный офис или филиал и т.п.)
- настроек компьютера в зависимости от местоположения сотрудника в одном из офисов компании: Москва, Санкт-Петербург, Краснодар, Новороссийск и т.п.

- **Дополнительный уровень аудита**
  - запись в журнал событий Indeed-ID причины отказа в доступе к данным
  - запись в журнал событий Indeed-ID местоположения пользователя в момент получения доступа к данным
- **Автоматическая разблокировка**
  - рабочего стола Windows при входе в кабинет/переговорную
- **Автоматическая блокировка**
  - рабочего стола Windows при выходе из кабинета
  - профиля доступа при выходе сотрудника из офиса
- **другие**

Схема интеграции Indeed-ID Rules System и СКУД

Indeed-ID Rules System входит в состав Indeed-ID Enterprise Server, предоставляя интерфейс интеграции с внешними системами и одновременно выступая hosting-площадкой для коннекторов к этим системам. В данной схеме интеграция с системой СКУД достигается за счет реализации отдельного коннектора (Indeed-ID RS “СКУД” Connector). Коннектор является переходником между Indeed-ID Rules System и СКУД, скрывая особенности внутреннего протокола взаимодействия с системой СКУД (для разных СКУД могут требоваться разные коннекторы).

Рассмотрим схему работы на примере бизнес-операции получения пользователем доступа в информационную систему при помощи Indeed-ID ESSO Агента (далее Indeed-ID Агента), входящего в состав продукта Indeed-ID ESSO.



1. В момент получения доступа в информационную систему, Indeed-ID Агент, инсталлированный на рабочем месте пользователя, формирует запрос к серверу Indeed-ID Enterprise Server. В ходе

выполнения запроса от сотрудника может потребоваться пройти процедуру аутентификации (например, с использованием универсальной карты доступа с интегрированной радио-меткой).

2. Сервер Indeed-ID, получив запрос, извлекает из него информацию “от имени какой учетной записи” он пришел (например, от имени ivanov@domain.local). По имени учетной записи сервер находит соответствие между пользователем и идентификатором радио-метки его карты (предположим, что пользователю ivanov@domain.local соответствует идентификатор карты 3458). Далее запрос транслируется в подсистему Indeed-ID Rules System, которая через Коннектор обращается к журналу событий СКУД системы, определяя в какой зоне была зарегистрирована карта 3458.

3. Получив ответ содержащий идентификатор турникета (зоны) на котором зарегистрирована карта сотрудника, Коннектор передает ответ в подсистему Rules System, где происходит его анализ на соответствие правилам системы.

4. Если местоположение сотрудника соответствует настроенным правилам (эквивалентно тому, что Rules System одобрил запрос), Indeed-ID Enterprise Server возвращает данные, необходимые для доступа к информационной системе (как правило, логин-пароль). В противном случае, происходит отказ в доступе с указанием причины.

5. Результат и детали обработки запроса фиксируются в журнале событий Indeed-ID

Дополнительные выгоды от совместного использования технологии аутентификации “Aladdin eToken с интегрированной радио-меткой” в составе решения Indeed-ID Rules System

Следует обратить отдельное внимание на тот факт, что Indeed-ID Rules System не зависит от способа, которым пользователи подтверждают себя в информационных системах. На практике это означает, что разным категориям сотрудников могут быть назначены разные методы аутентификации (например, биометрика для топ-менеджеров, одноразовый пароль для администраторов, бесконтактная карта для рядовых сотрудников). Этот факт не вызовет никаких различий при обработке запросов на стороне Indeed-ID Rules System.

Однако, рассматривая ситуацию в обратную сторону, можно обнаружить, что наличие Indeed-ID Rules System способно существенно повысить привлекательность отдельных видов устройств и технологий аутентификации. Например, гибридное устройство Aladdin eToken с интегрированной радио-меткой и Indeed-ID Rules System позволяют совместить простоту “универсальной карты”, надежность технологий и защиту самых уязвимых мест систем безопасности - беспечное и халатное отношение пользователей (человеческий фактор).

Это достигается за счет комплекса мер:

- Визуальный контроль владельцев карт на проходной минимизирует риск передачи карт между сотрудниками и получения несанкционированного доступа “за” или “вместо” владельца карты (отсутствие отметки о регистрации карты на проходной будет автоматически выявлено Indeed-ID Rules System, соответственно карту нельзя пронести в кармане, не активируя при входе в офис)
- Автоматическая блокировка рабочего стола при выходе из кабинета (момент отключения eToken) с последующей автоматической блокировкой всего профиля пользователя (при

выходе за пределы разрешенной рабочей зоны: кабинет, этаж, офис и т.п.).

- N-факторная аутентификация (где N > 2). Наличие дополнительных факторов контроля местоположения сотрудника позволяет снизить требования к сложности PIN-кода ключа (на практике пользователи стараются уклоняться от использования сложных PIN-кодов, либо записывают их на бумажные носители)
- Совмещение в рамках концепции “универсальная карта” спектра современных технологий, детали которых скрыты от пользователей:
    - технология доступа в здание и отдельные помещения с применением радио-метки
    - технология доступа в сеть с использованием цифрового сертификата x.509
    - технология доступа в приложения по методу Single Sign-On с предварительной проверкой валидности сертификата x.509
    - технологии электронной цифровой подписи с использованием сертификата x.509
    - технологии предоставления логического доступа к информационным системам по сертификату, с учетом физического местоположения сотрудника

Полный перечень продуктов линейки Indeed-ID IAM

Аутентификация	Indeed-ID Authentication Providers (более 20 технологий) Indeed-ID Logon for Windows (Active Directory version)
Single Sign-On	Indeed-ID ESSO Indeed-ID ESSO - библиотека готовых шаблонов (более 30 систем) Indeed-ID ESSO Desktop Indeed-ID ESSO Outlook Web Access Indeed-ID ESSO ActiveSync
Identity Management	Indeed-ID Microsoft Forefront 2010 Connector Indeed-ID Sun IDM Connector Indeed-ID IBM TIM Connector
Card Management Systems	Indeed-ID Aladdin eToken TMS 2.0 Connector
Access Management	Indeed-ID Rules System Indeed-ID RS “СКУД” Connector
SDK	Indeed-ID Integration Pack