Этот документ входит в комплект поставки продукта.
Информация, содержащаяся в этом документе, может быть изменена разработчиком без уведомления пользователя.

Контактная информация:

+7 (495) 640-06-09
Москва
+7 (812) 640-06-09
Санкт-Петербург

inbox@indeed-id.com
почта

8 800 333-09-06
support@indeed-id.com
техническая поддержка

Indeed-Id Events Analyzer

Руководство по эксплуатации

версия 6.3.0

Содержание

Условные обозначения **2**

О компоненте Indeed-Id Events Analyzer **2**

Работа с Indeed-Id Events Analyzer **3**

Запуск приложения 3

Виды отчетов 4

Использование способов входа пользователями 5

Диаграмма использования способов входа 5

Неудачные попытки входа 6

Использование пароля для входа в Active Directory 7

Действия пользователя 8

Смена пароля пользователя 10

Автоматическая смена пароля пользователя 11

События входа пользователя в SSO-приложение 11

Обработка ошибок Indeed-Id Events Analyzer **13**

Условные обозначения

В Руководстве используются следующие условные обозначения:

Важная информация
Указания, требующие особого внимания при развертывании, настройке, работе или обновлении продукта.

Дополнительная информация
Указания, способные упростить развертывание, настройку, работу или обновление продукта.

О компоненте Indeed-Id Events Analyzer

Компонент Indeed-Id Events Analyzerпредназначен для сбора и наглядного анализа информации о событиях Indeed EA/ESSO и дополнительных подсистем. Собранные статистические данные представляются в виде отчета в формате .htm или .jpg (если тип отчета предусматривает построение диаграммы). Indeed-Id Events Analyzer позволяет создавать отчеты следующих типов:

- Использование способов входа пользователями
- Диаграмма использования способов входа
- Неудачные попытки входа
- Использование пароля для входа в Active Directory
- Действия пользователя
- Смена пароля пользователя
- Автоматическая смена пароля пользователя
- События входа пользователя в SSO-приложение

Работа с Indeed-Id Events Analyzer

Запуск приложения

Откройте файл **LogAnalyzer.hta**, включенному в каталог \Events Analyzer дистрибутива Indeed-Id Admin Pack (Рисунок 1). Для получения отчета:

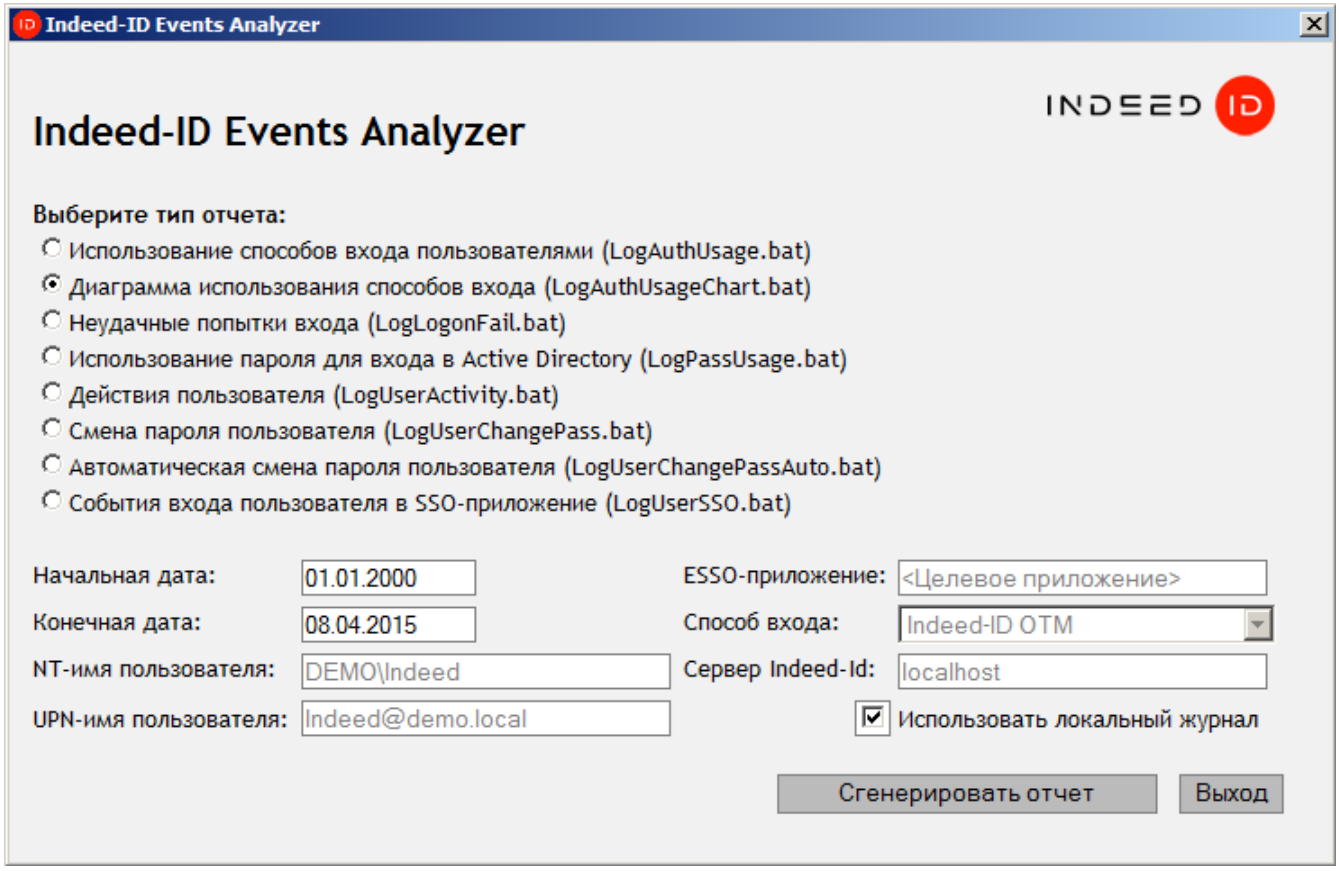

Рисунок 1 – Окно Indeed-Id Events Analyzer.

1. Выберите тип отчета.
2. Укажите период отчета (начальную и конечную дату).
3. Укажите дополнительные параметры.
4. Укажите сервер Indeed EA/ESSO, с которого необходимо получать события.

> По умолчанию события в отчет поступают из журнала машины, на которой запущен Events Analyzer. Для изменения сервера необходимо отключить опцию **Использовать локальный журнал** и указать имя (Computer Name или Full Computer Name) рабочей станции, с установленным сервером Indeed EA/ESSO. Для сбора сведений с нескольких серверов укажите их имена через запятую.

5. Нажмите **Сгенерировать отчет**.
6. Файл отчета сохраняется в каталоге приложения Indeed-Id Events Analyzer в формате .htm или .jpg (если тип отчета предусматривает построение диаграммы).

Создание отчета выполняется при наличии в журнале соответствующих категорий событий и доступности каталога приложения Indeed-Id Events Analyzer для записи. Для построения диаграмм необходимы компоненты **Microsoft Office Web Components**, являющиеся частью Microsoft Office. Если эти компоненты отсутствуют на рабочей станции, Вы можете установить их с помощью исполняемого файла owc10.exe, включенного в состав дистрибутива Indeed-Id Events Analyzer.

Для сбора информации о событиях системы по умолчанию используется журнал Indeed-Id. Если журнал Indeed-Id отсутствует, сообщения о событиях системы сохраняются в стандартном журнале Application. В этом случае перед запуском приложения необходимо внести изменения в файл SetIIDLogSource.bat, включенный в состав дистрибутива Indeed-Id Events Analyzer:

1. Откройте файл **SetIIDLogSource.bat** для редактирования.
2. В строке **if not defined IIDLogSource Set IIDLogSource=Indeed-Id** вместо значения Indeed-Id введите значение **Application** и сохраните изменения.

Виды отчетов

Indeed-Id Events Analyzer позволяет создавать отчеты следующих типов:

- **Использование способов входа пользователями** – отчет о частоте использования одного из доступных способов аутентификации за указанный период.
- **Диаграмма использования способов входа** – отчет о соотношении частоты использования доступных способов аутентификации.
- **Неудачные попытки входа** – отчет о количестве неуспешных попыток входа в систему по паролю Active Directory или аутентификатору, совершенных пользователями за указанный период.
- **Использование пароля для входа в Active Directory** – отчет о количестве успешных попыток входа в систему по паролю Active Directory за указанный период.
- **Действия пользователя** – отчет об успешных действиях пользователя (управление аутентификаторами, вход в систему, вход в SSO-приложение, блокировка/разблокирование рабочей станции, смена пароля) за указанный период.
- **Смена пароля пользователя** – отчет о количестве попыток смены пароля пользователю за указанный период.
- **Автоматическая смена пароля пользователя** – отчет о количестве успешных и неуспешных попыток автоматической смены пароля пользователю за указанный период.
- **События входа пользователя в SSO-приложение** – отчет о количестве успешных попыток входа пользователя в SSO-приложение за указанный период.

Использование способов входа пользователями

Отчет **Использование способов входа пользователями** (AuthUsage.htm) представляет собой таблицу, содержащую список пользователей Indeed EA/ESSO и количество попыток использования аутентификатора (в данном случае – одноразовой матрицы ОТМ), совершенных пользователями за указанный период (Рисунок 2).

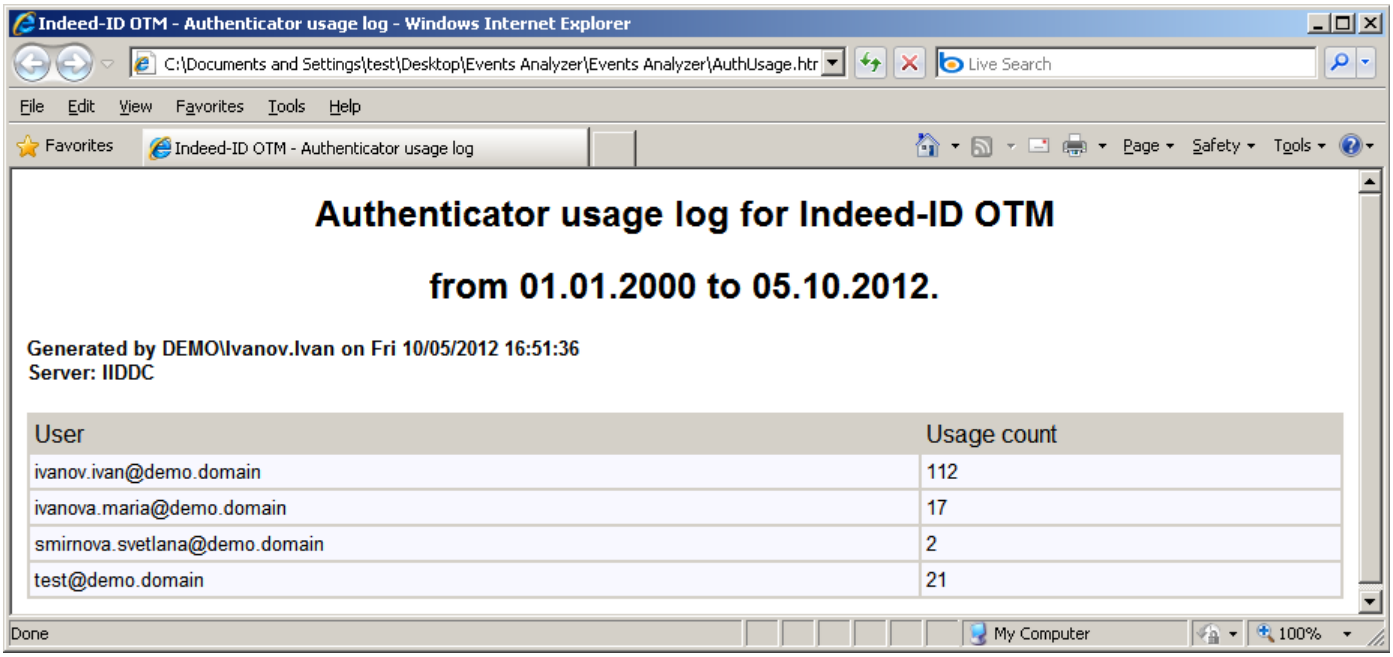

Рисунок 2 – Использование способов входа пользователями.

При создании отчета учитываются следующие события:

1000 – Пользователь был успешно аутентифицирован по предоставленному аутентификатору.

2001 – Успешная аутентификация пользователя по аутентификатору.

2009 – Успешное разблокирование компьютера пользователем с использованием аутентификатора.

1040 – Пользователь выполнил вход по идентификатору.

Событие **1040 – Пользователь выполнил вход по идентификатору** в отчете отображается отдельной строкой от остальных событий аутентификации пользователя, т.к. указывает на использование механизма автоматической идентификации пользователя.

Диаграмма использования способов входа

Отчет **Диаграмма использования способов входа** (AuthUsageChart.jpg) представляет собой изображение, иллюстрирующее соотношение частоты использования доступных способов входа. Для каждого способа входа указывается количество попыток использования (Рисунок 3).

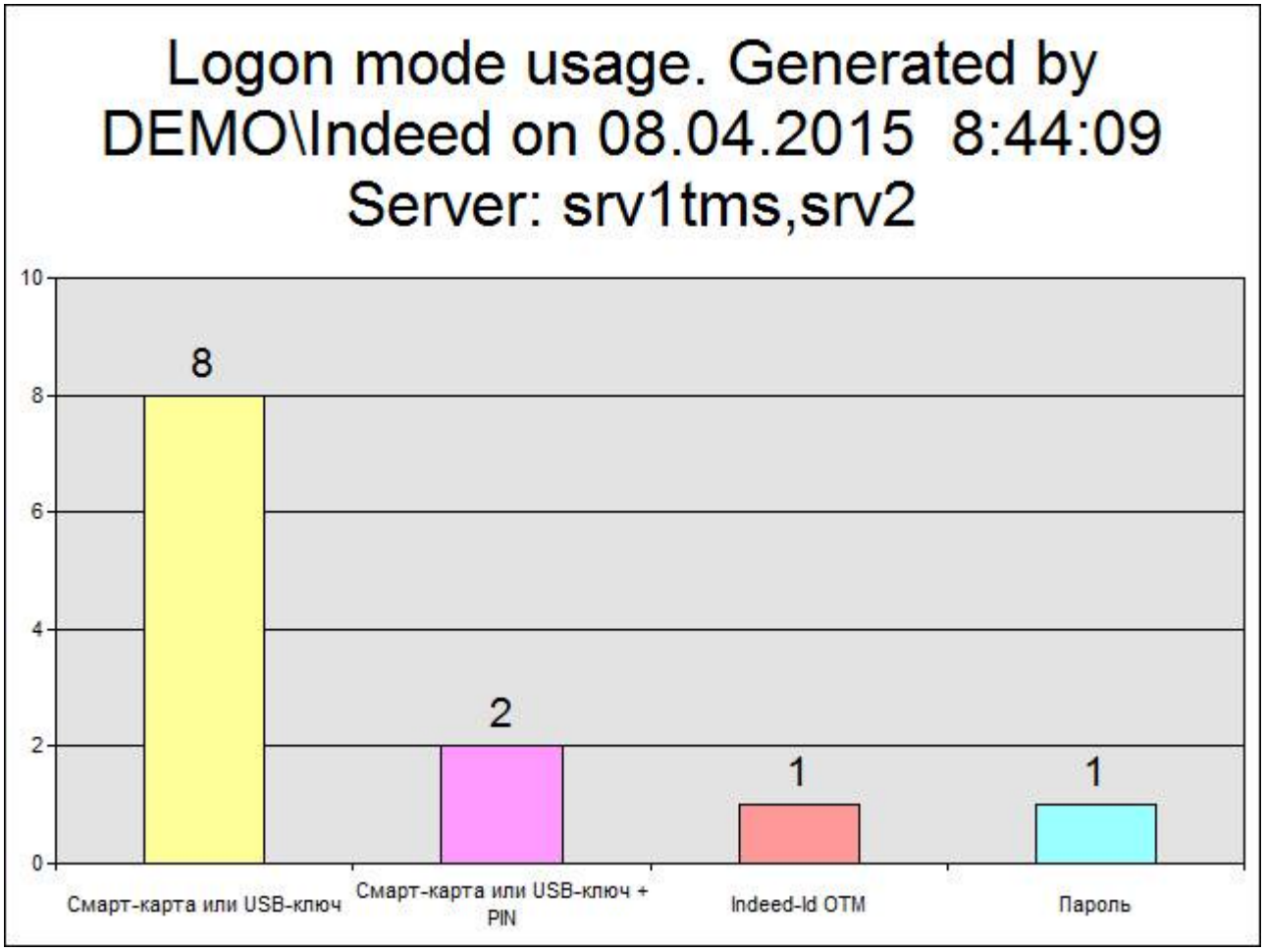

Рисунок 3 – Диаграмма использования способов входа.

При создании отчета учитываются следующие события:

1000 – Пользователь был успешно аутентифицирован по предоставленному аутентификатору.

1001 – Пользователь был успешно аутентифицирован по паролю.

Неудачные попытки входа

Отчет **Неудачные попытки входа** (LogonFail.htm) представляет собой таблицу, содержащую список неуспешных попыток входа в систему по паролю Active Directory или аутентификатору, совершенных пользователями за указанный период (Рисунок 4).

Рисунок 4 – Неудачные попытки входа.

При создании отчета учитываются следующие события:

1000 – Пользователь был успешно аутентифицирован по предоставленному аутентификатору.

1001 – Пользователь был успешно аутентифицирован по паролю.

Использование пароля для входа в Active Directory

Отчет **Использование пароля для входа в Active Directory** (PassUsage.htm) представляет собой таблицу, содержащую список пользователей Indeed-Id и количество успешных попыток использования пароля Active Directory для входа в систему (Рисунок 5).

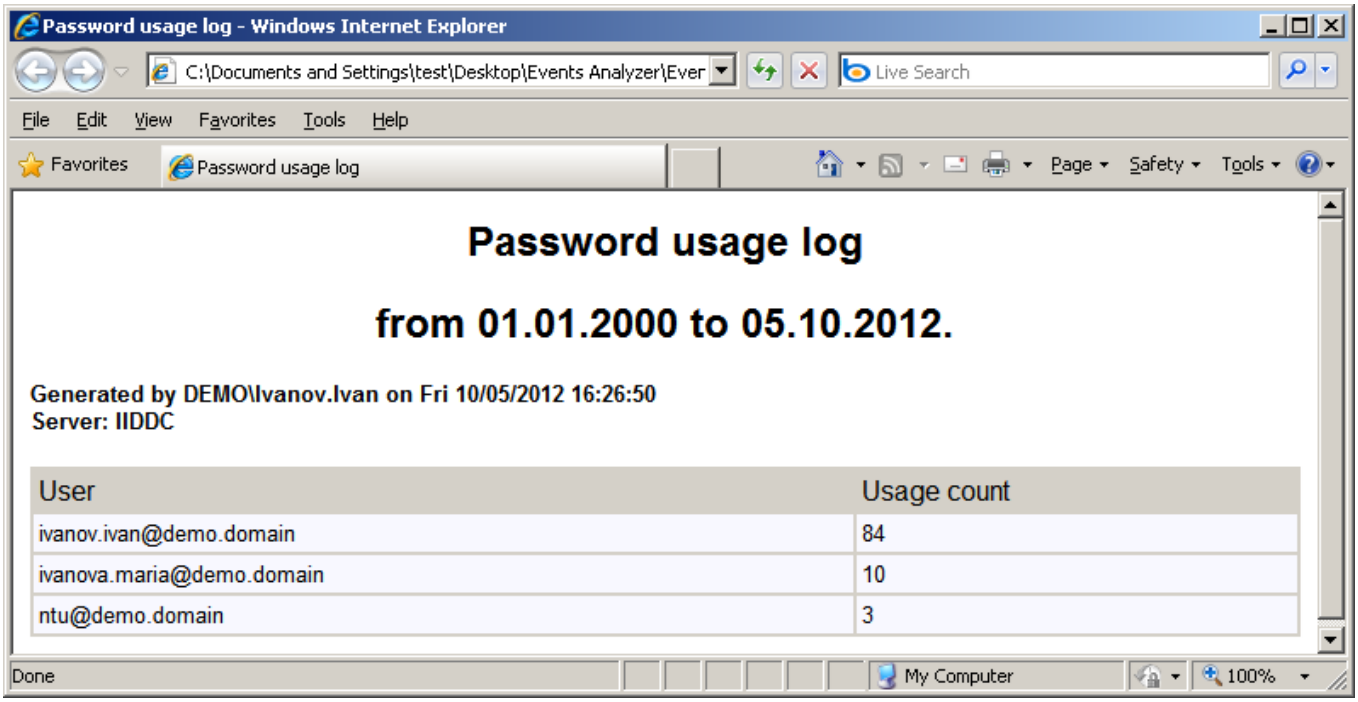

Рисунок 5 – Использование пароля для входа в Active Directory.

При создании отчета учитываются следующие события:

1001 – Пользователь был успешно аутентифицирован по паролю.

Действия пользователя

Отчет **Действия пользователя** (UserActivity.htm) представляет собой таблицу, содержащую успешные действия пользователя (вход в систему, управление аутентификаторами, блокировка/разблокирование рабочей станции, вход в SSO-приложение, смена пароля в SSO-приложении и др.) за указанный период (Рисунок 6).

Для получения отчета **Действия пользователя** необходимо указать имя пользователя в формате NT и UPN в соответствующем поле в окне Indeed-Id Events Analyzer.

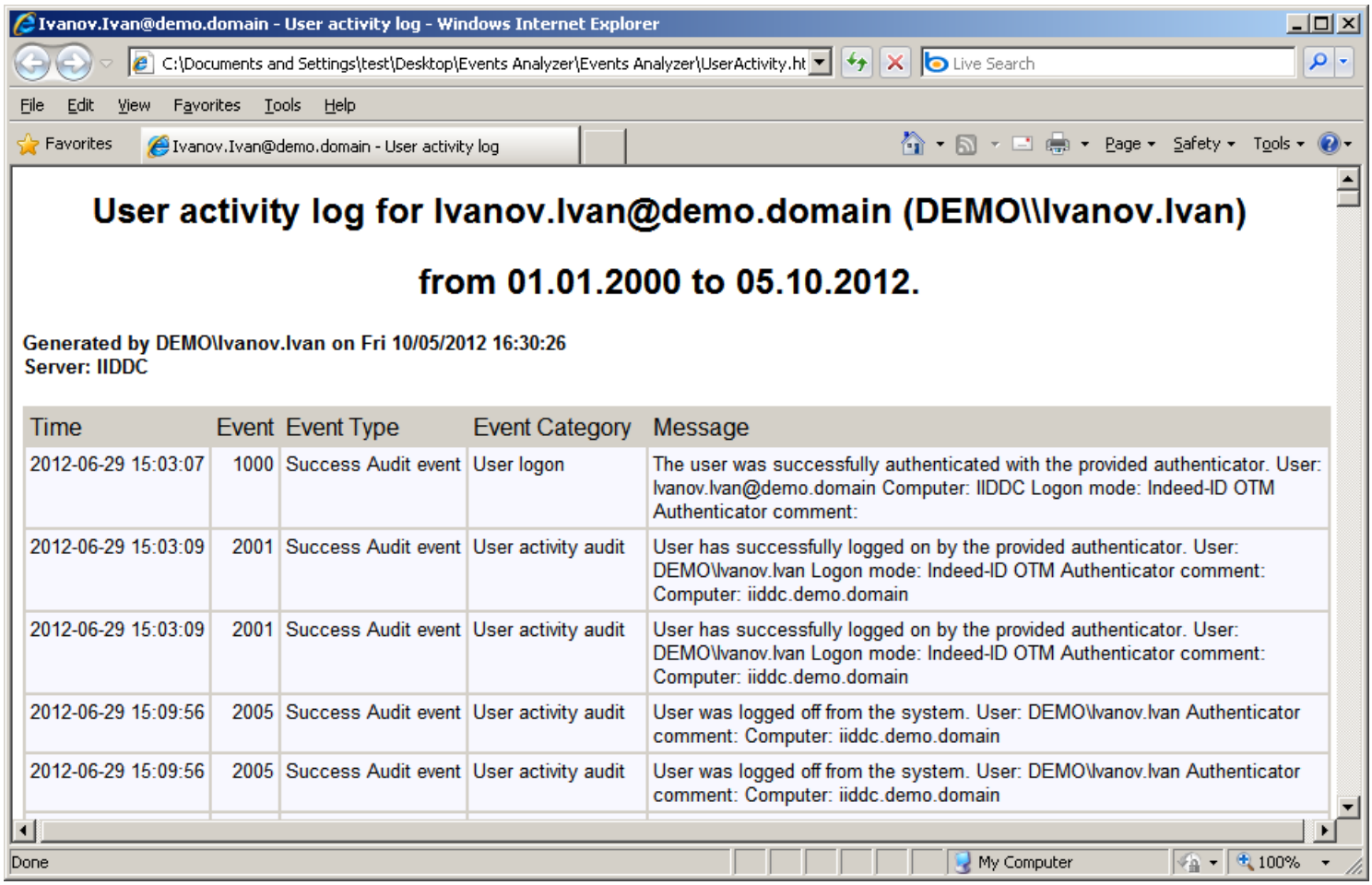

Рисунок 6 – Действия пользователя.

При создании отчета учитываются следующие события:

1000 – Пользователь был успешно аутентифицирован по предоставленному аутентификатору.

1001 – Пользователь был успешно аутентифицирован по паролю.

1004 – Аутентификатор пользователя был успешно обучен.

1005 – Аутентификатор пользователя был успешно переобучен.

1106 – Комментарий аутентификатора пользователя был успешно изменен.

1006 – Аутентификатор пользователя был успешно удален.

1007 – Список аутентификаторов пользователя был успешно очищен.

2001 – Пользователь успешно выполнил вход по предоставленному аутентификатору.

2002 – Пользователь успешно выполнил вход по предоставленному паролю.

2003 – Пользователь заблокировал компьютер.

2004 – Пользователь убрал устройство входа. Компьютер заблокирован.

2005 – Пользователь вышел из системы.

2006 – Пользователь убрал устройство входа. Сессия завершена.

2008 – Пользователь разблокировал компьютер по предоставленному паролю.

2009 – Пользователь разблокировал компьютер по предоставленному аутентификатору.

10006 – Пользователь выполнил вход в приложение.

10007 – Пароль пользователя был успешно сгенерирован и сменен.

10008 – Ошибка при сохранении пароля пользователя в базе данных Indeed-Id ESSO.

Смена пароля пользователя

Отчет **Смена пароля пользователя** (ChagePass.htm) представляет собой таблицу, содержащую успешные и неуспешные события смены пароля пользователю за указанный период (Рисунок 7).

Для получения отчета **Смена пароля пользователя** необходимо указать имя пользователя в формате NT и UPN в соответствующем поле в окне Indeed-Id Events Analyzer.

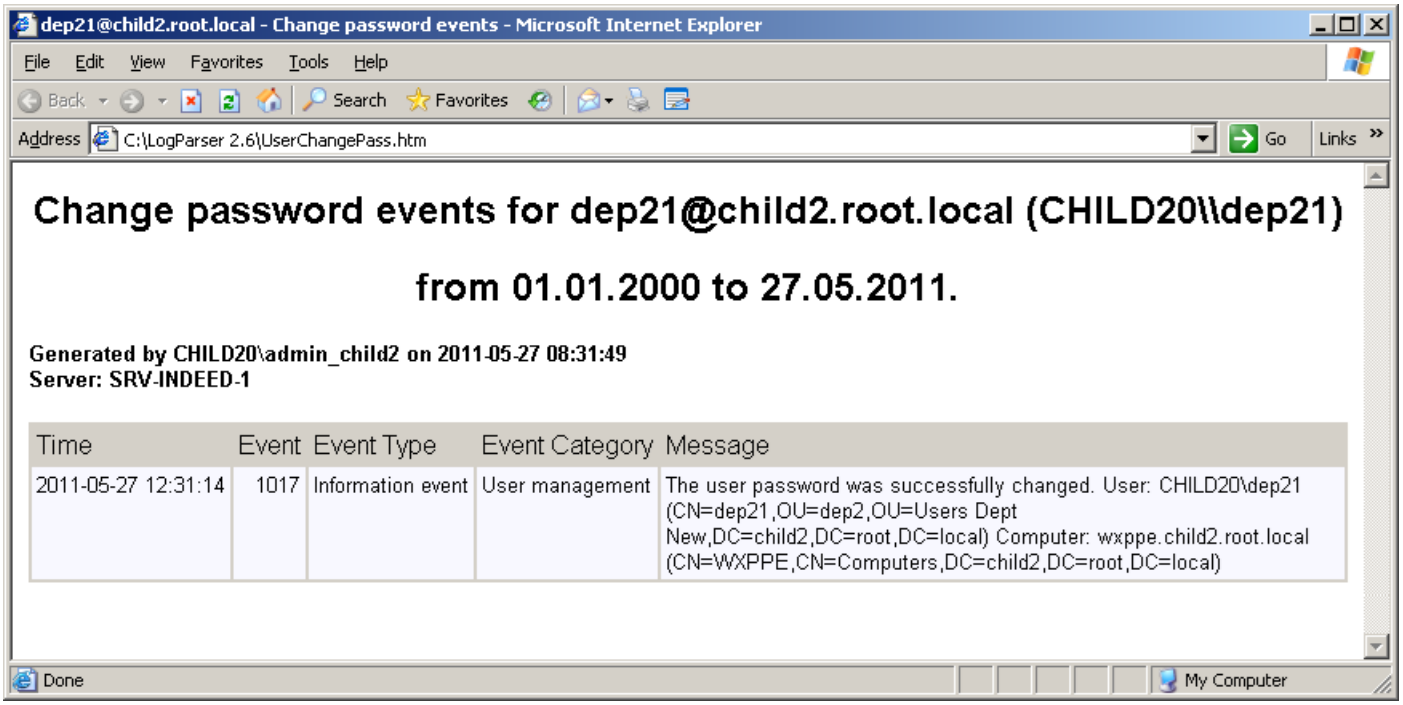

Рисунок 7 – Смена пароля пользователя.

При создании отчета учитываются следующие события:

1017 – Успешное событие. Пароль пользователя был успешно сменен.

1017 – Ошибка. Неуспешная попытка смены пароля пользователя.

Автоматическая смена пароля пользователя

Отчет **Автоматическая смена пароля пользователя** (UserChangePassAuto.htm) представляет собой таблицу, содержащую успешные и неуспешные события автоматической смены пароля пользователю за указанный период (Рисунок 8).

Для получения отчета **Автоматическая смена пароля пользователя** необходимо указать имя пользователя в формате NT и UPN в соответствующем поле в окне Indeed-Id Events Analyzer.

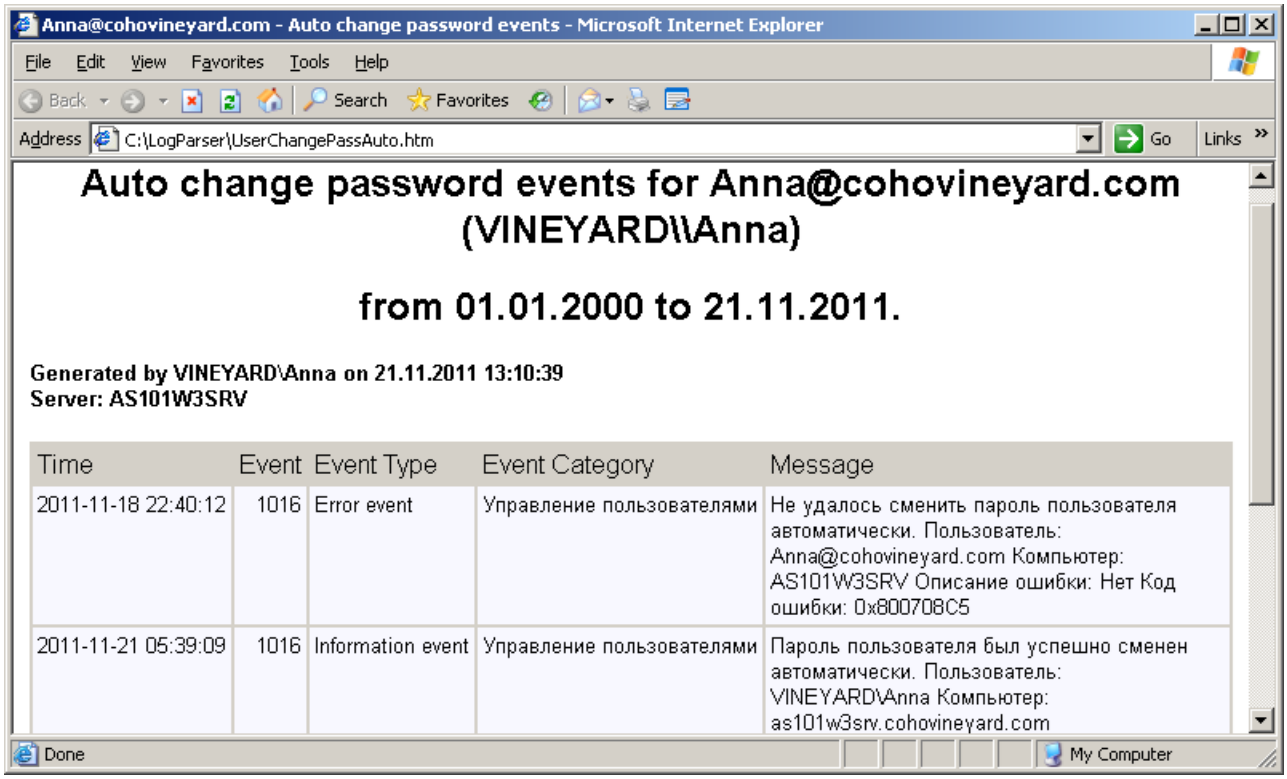

Рисунок 8 – Автоматическая смена пароля пользователя.

При создании отчета учитываются следующие события:

1016 – Пароль пользователя был успешно сменен автоматически.

1016 – Не удалось сменить пароль пользователя автоматически.

События входа пользователя в SSO-приложение

Отчет **События входа пользователя в SSO-приложение** (UserSSO.htm) представляет собой таблицу, содержащую успешные события аутентификации пользователя в SSO-приложении (Рисунок 9).

Для получения отчета **События входа пользователя в SSO-приложение** необходимо указать имя пользователя в формате NT и UPN в соответствующем поле в окне Indeed-Id Events Analyzer.

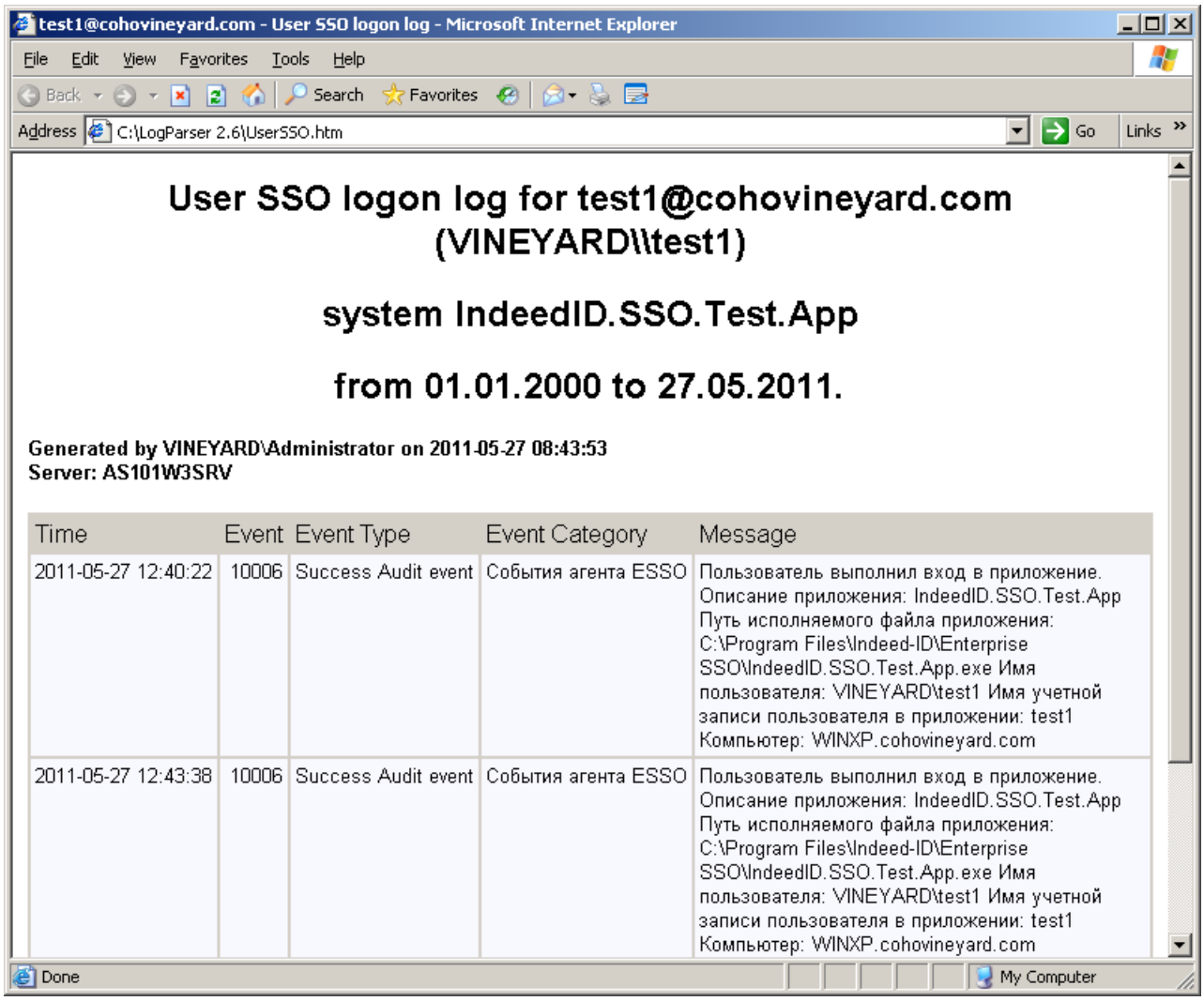

Рисунок 9 – События входа пользователя в SSO-приложение.

При создании отчета учитываются следующие события:

10006 – Пользователь выполнил вход в приложение.

Обработка ошибок Indeed-Id Events Analyzer

Раздел содержит информацию о решении известных проблем. Если проблемы нет в списке, обратитесь в службу технической поддержки.

Ошибка записи отчета
При попытке создания отчета отображается сообщение об ошибке **Не удалось сгенерировать отчет** (Рисунок 10).

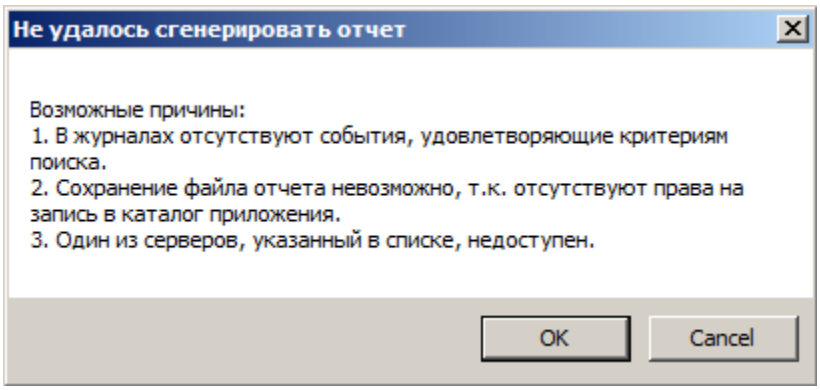

Рисунок 10 – Ошибка создания отчета.

Возможные причины:

- Журнал не содержит событий, соответствующих выбранному типу отчета.
- Каталог приложения Indeed-Id Events Analyzerнедоступен для записи.
- Не установлены компоненты Microsoft Office Web Components, необходимые для создания диаграмм.
- Один или несколько серверов Indeed недоступны или их имена указаны неверно.

Действия по устранению:

- Проверьте наличие нужных событий в журнале Indeed-Id. Если вместо журнала Indeed-Id используется стандартный журнал Application, перед запуском приложения необходимо внести изменения в сценарий поиска событий.
- Установите разрешение на запись для каталога приложения Indeed-Id Events Analyzer. Если разрешение на запись установить не удается, это может быть связано с **известной проблемой Microsoft**. В таких случаях для удаления атрибута **Только чтение** необходимо выполнить команду **attrib –r <с>:\<имя каталога>**.
- Выполните установку Microsoft Office Web Components.
- Проверить правильность указанных имен серверов Indeed EA/ESSO и их доступность с рабочей станции, на которой запущен Indeed-Id Events Analyzer.

Ошибка просмотра отчета-диаграммы
При попытке просмотра отчета-диаграммы в Microsoft Windows Server 2008 отображается сообщение об ошибке печати изображения (Рисунок 11).

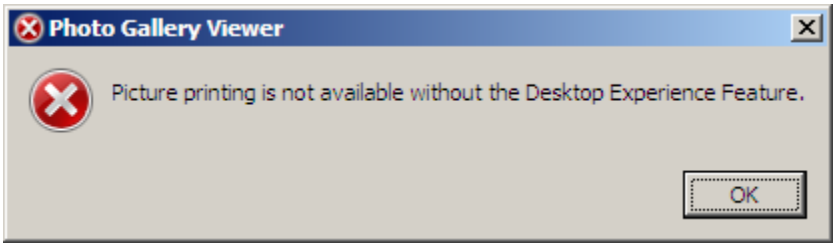

Рисунок 11 – Ошибка просмотра отчета.

Возможные причины:
Для отображения отчета-диаграммы в операционных системах Microsoft Windows Server 2008/2008R2 и 2012/2012R2 необходимо наличие установленного компонента **Возможности рабочего стола** (Desktop Experience). По умолчанию данный компонент отключен.

Действия по устранению:
Для включения функции Desktop Experience выполните следующие действия:

Windows Server 2008/2008R2

1. Перейдите в **Диспетчер серверов** (Server Manager).
2. В разделе **Компоненты** (Features Summary) нажмите **Добавить компоненты** (Add Features).
3. В открывшемся окне **Мастера добавления ролей** должна быть выбрана опция **Возможности рабочего стола** (Desktop Experience). Нажмите **Далее** (Next), затем **Установить** (Install).
4. Дождитесь завершения установки и выполните перезагрузку операционной системы.

Windows Server 2012/2012R2

1. Перейдите в **Диспетчер серверов** (Server Manager).
2. В разделе **Роли и компоненты** (Roles and Features) нажмите **Добавить компоненты** (Add Features) и перейдите в раздел **Компоненты** (Features)
3. В открывшемся окне **Мастера добавления ролей** разверните пункт **Пользовательские интерфейсы и инфраструктура** (User Interfaces and Infrastructure) и отметьте опцию **Возможности рабочего стола** (Desktop Experience).
4. Дождитесь завершения установки и выполните перезагрузку операционной системы.