

**Руководство
пользователя
BioLink IDenium
для Active Directory**



© 2013 BioLink Solutions

Содержание

Часть I Авторские права	1
Часть II Предисловие	3
1 Комплект документации	3
2 Используемые обозначения	3
3 Контактная информация	4
Часть III Введение в BioLink IDenium Client	5
1 Компоненты BioLink IDenium	5
2 Назначение IDenium Windows Logon	5
3 Назначение IDenium Password Vault	6
4 Как прикладывать палец к окну сканера отпечатков пальцев	6
Часть IV Регистрация на APM пользователя	9
1 Первый вход пользователя	9
2 Общие рекомендации по регистрации на APM пользователя	10
3 Вход в Windows XP по отпечатку пальца	11
4 Вход в Windows XP по паролю	12
5 Вход в Windows XP с помощью смарт-карты	13
6 Вход в Windows Vista / 7 / 8 по отпечатку пальца	14
7 Вход в Windows Vista по паролю	15
8 Возможные сообщения об ошибках при регистрации на APM пользователя	17
Часть V Управление биометрическими идентификаторами и паролями	19
1 Учетные данные пользователя	19
2 Как ввести в систему отпечатки пальцев	21
3 Очистка кэша	26
4 Изменение пароля пользователя	28
Часть VI Работа со сценариями IDenium Password Vault	30
1 Запись сценариев BioLink IDenium Password Vault	31
2 Выполнение сценариев Password Vault	35
3 Изменение сценариев BioLink IDenium Password Vault	36
4 Удаление сценариев BioLink IDenium Password Vault	38
5 Публичные сценарии и параметры BioLink IDenium Password Vault	39

Часть VII Сведения о программе

40

1 Авторские права

© 2013 BioLink Solutions. Все права защищены.

Данное программное обеспечение (далее "Программа") является собственностью BioLink Solutions. Программа защищена законами и международными соглашениями об авторских правах, а также другими законами и договорами, регулирующими отношения авторского права. Запрещается производить декомпиляцию или восстановление исходного кода Программы.

Настоящий документ может быть изменен без уведомления в результате совершенствования или изменения Программы. Содержащаяся в документе информация является интеллектуальной собственностью BioLink Solutions и передается клиенту на конфиденциальной основе. BioLink Solutions не гарантирует отсутствие неточностей и опечаток в данном документе. При обнаружении неточностей в документации, сообщайте о них, пожалуйста, в службу технической поддержки.

Настоящий документ может содержать ссылки на веб-сайты, которые были действительны на момент публикации документа, но могут быть изменены или стать неактивными впоследствии. Настоящий документ может содержать ссылки на сайты в Интернет, принадлежащие и поддерживаемые сторонними организациями. BioLink Solutions не несет ответственности за содержимое сайтов сторонних организаций.

Любое воспроизведение, копирование, сохранение или передача данной публикации полностью или частично, в любой форме и с использованием любых средств: электронных, механических, фотокопировальных и др. без предварительного письменного согласия со стороны BioLink Solutions запрещено.

BioLink® является товарным знаком BioLink Solutions. U-Match® является зарегистрированным товарным знаком BioLink Solutions. Любые товарные знаки, упомянутые в данном руководстве, являются либо товарными знаками, либо зарегистрированными товарными знаками соответствующих владельцев. BioLink Solutions признает все права компаний, имеющих зарегистрированные товарные знаки.



Биолинк Солюшенс

125493, Россия, г. Москва,

ул. Авангардная, 3

Тел: +7 (495) 645-87-03 (-04,-05)

Техническая поддержка: +7 (495) 645-87-03 (-04,-05)

Контактная информация
службы технической поддержки:

support@biolinksolutions.com
Веб-сайт: <http://support.biolinksolutions.com>

2 Предисловие

Добро пожаловать в BioLink IDenium для Active Directory! Система биометрической аутентификации пользователей BioLink IDenium (далее IDenium) позволит эффективно использовать стандартные средства защиты операционных систем семейства Windows благодаря использованию одной из самых эффективных технологий распознавания пользователей - по отпечатку пальца.

Эта глава знакомит с сокращениями и системой условных обозначений, используемых в данном документе, и содержит ссылки на дополнительные источники знаний о продукции BioLink Solutions и контактную информацию для оперативной связи с представителями компании в случае необходимости. Также в этой главе содержится информация о документации, сопровождающей систему.

2.1 Комплект документации

Настоящий документ является частью комплекта документации BioLink IDenium для Active Directory, состоящего из следующих документов:

- **Руководство пользователя** (настоящий документ). Содержит подробные инструкции по работе пользователя с компонентом BioLink IDenium Client
- **Руководство администратора**. Детально описывает все аспекты функционирования системы BioLink IDenium Active Directory Edition, включая основные понятия Active Directory, концепцию работы системы IDenium и ее администрирование.
- **Руководство по установке**. Содержит инструкции по установке и развертыванию системы BioLink IDenium для Active Directory.

2.2 Используемые обозначения

Прежде чем приступить к работе с Руководством, рекомендуем ознакомиться с принятыми типографскими соглашениями по стилевому оформлению данного документа.

Вид форматирования	Тип информации
Заголовок процедуры	Пошаговые процедуры. Следуйте этим инструкциям для выполнения конкретной задачи.
Специальный	Элементы интерфейса, которые необходимо выбрать,

полужирный	например, пункты меню, кнопки команд или элементы списка.
<i>Курсив</i>	Важная информация, на которую необходимо обратить внимание или которая используется для обозначения переменных выражений, например, параметров.
ПРОПИСНЫЕ	Названия клавиш на клавиатуре, например, SHIFT, CTRL, ALT.
SHIFT+CTRL	Комбинация клавиш, при которой следует нажать и удерживать на клавиатуре сначала одну клавишу и затем нажать другую. Например: CTRL+P или ALT+F4.
Моноширинный	Текст исходного кода программы.

2.3 Контактная информация

Дополнительную информацию о компании BioLink Solutions можно найти в Интернете по адресу:

[для русской версии документации] <http://www.biolink.ru>

[для английской версии документации] <http://www.biolinksolutions.com>

За технической поддержкой обращайтесь:

<http://support.biolinksolutions.com>

3 Введение в BioLink IDenium Client

Эта глава содержит информацию о компонентах BioLink IDenium для Active Directory, о назначении и об основных функциях компонента BioLink IDenium Windows Client. Также, прочитав эту главу, вы сможете узнать, как правильно прикладывать палец к сканеру отпечатков пальцев.

3.1 Компоненты BioLink IDenium

Реализованная на базе клиент-серверной технологии, система BioLink IDenium для Active Directory включает в себя:

- серверную часть, состоящую из **сервера BioLink IDenium**, отвечающего за поиск и сравнение биометрических идентификаторов, и **Компонентов для контроллера домена**, позволяющего синхронизировать данные об учетных записях пользователей между Active Directory и сервером BioLink IDenium;
- клиентскую часть, состоящую из компонента **BioLink IDenium Client**, позволяющего пользователям применять биометрическую идентификацию для доступа к защищенным программам и ресурсам, и компонента **BioLink IDenium Admin Pack**, предназначенного для администраторов.

Вся информация об администрировании IDenium для Active Directory и работы с компонентом **BioLink IDenium Admin Pack** представлена в **Руководстве администратора IDenium**.

Данный документ целиком и полностью посвящен работе обычного пользователя и, соответственно, компоненту BioLink IDenium Client, который состоит из следующих двух модулей:

- BioLink Windows Logon;
- BioLink Password Vault.

3.2 Назначение IDenium Windows Logon

Модуль BioLink IDenium Password Vault позволяет решить задачу контроля доступа к автоматизированным рабочим местам (АРМ) или сетевым ресурсам с помощью биометрической идентификации, обеспечивая выполнение следующих операций пользователя:

- вход в систему по отпечатку пальца (или, если необходимо, по имени и паролю пользователя);
- блокирование/разблокирование АРМ пользователя;

- самостоятельный ввод/изменение пользователем своих биометрических идентификаторов.

3.3 Назначение IDenium Password Vault

Модуль BioLink IDenium Windows Logon позволяет записывать последовательность действий пользователя в окнах приложений в виде сценариев и впоследствии воспроизводить их автоматически при открытии этих окон.

Как правило, данная функциональность особенно полезна в случае, когда приложение требует авторизации пользователя для выполнения каких-либо действий. Таким образом, пользователь может записать для каждого такого диалогового окна свой сценарий BioLink IDenium Password Vault. После записи сценария, пользователю больше не нужно будет вводить имя пользователя и пароль.

С помощью BioLink IDenium Password Vault можно выполнять следующие действия:

- записывать сценарии для последующего выполнения;
- выполнять сценарии;
- изменять параметры сценариев;
- удалять сценарии.

3.4 Как прикладывать палец к окну сканера отпечатков пальцев

Отличительной особенностью Windows Logon является возможность применения биометрического сканера, позволяющего системе определять пользователей по отпечаткам пальцев. Для успешной работы с Windows Logon с самого начала необходимо ознакомиться с рядом простых правил по использованию биометрического сканера:

1. Выберите палец, по отпечатку которого система будет определять ваши права доступа

Вы можете использовать для верификации любой палец любой руки. Если к компьютеру подключен сканер BioLink U-Match, удобнее использовать указательный палец. Но следует помнить, что каждый из пальцев обладает своим уникальным отпечатком, не похожим на отпечатки других пальцев. Поэтому, если, например, в системе зарегистрирован отпечаток большого пальца правой руки, то и прикладывать к сканеру нужно именно этот палец.

2. Проверьте состояние пальца

Палец должен быть чистым, сухим и нормальной температуры.

3. Приложите палец к окну сканера

Оптимальное положение



Используйте всю поверхность окна сканера

Используйте всю максимально возможную площадь сканера, ориентируясь по изображению отпечатка на экране компьютера.

Размещайте кутикулу по центру окна сканера

Перекошенный, смещенный в какую-либо сторону палец не может быть корректно зарегистрирован в системе и может стать причиной отказов в распознавании или существенного снижения скорости идентификации. Старайтесь прикладывать палец таким образом, чтобы кутикула находилась в центре окна сканера.

Старайтесь прикладывать палец полностью и не разворачивать его относительно поверхности сканера

Не прикладывайте палец боком или частично. Это резко снижает качество отпечатка и рассматривается программой как ошибка.

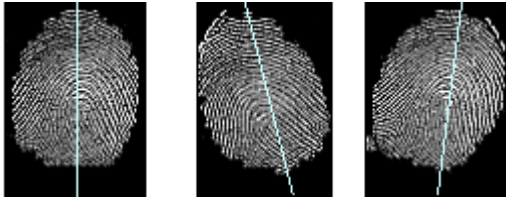
Необходимо учитывать, что смещение или поворот пальца относительно поверхности сканера приводит к ошибкам распознавания отпечатка пальца.

Не прижимайте палец слишком сильно или слишком слабо

Если палец прижат слишком сильно, то оттиск будет иметь вид однородного темного пятна. Ослабьте силу нажатия.

Если палец прижат слишком слабо, то вместо четкой картины капиллярных линий будут видны отдельные точки и отрезки. Увеличьте силу нажатия.

Рекомендуется слегка поворачивать палец при вводе отпечатка пальца пользователя в систему. Например, сначала расположить палец так, чтобы ось пальца и ось симметрии сканера совпадали по центру, затем слегка повернуть палец влево, потом - слегка вправо.



4 Регистрация на АРМ пользователя

4.1 Первый вход пользователя

Способ первого после установки BioLink IDenium Windows Logon на АРМ пользователя входа одинаков для всех операционных систем и может быть следующим:

Если отпечатки пальцев пользователя уже внесены в базу данных (БД) программного комплекса BioLink IDenium (пользователь присутствовал при создании своей учетной записи в локальной сети), то для того, чтобы зайти на АРМ пользователя в первый раз, приложите свой палец к окну сканера отпечатков пальцев.

Если отпечатки пальцев пользователей отсутствуют в БД, необходимо обратиться к системному администратору, чтобы он передал пользователю пароль для первого входа.

Если ПИН-код смарт-карты уже введен в БД BioLink IDenium, и отпечатки пальцев внесены в БД, вставьте смарт-карту в считыватель и, после появления приглашения ввести ПИН-код, приложите палец к сканеру отпечатков пальцев.

Внимание! В зависимости от политик BioLink IDenium, возможно, что пользователь не сможет использовать какой-либо из вышеупомянутых способов. Необходимо обратиться к системному администратору в случае возникновения каких-либо затруднений.

Обратите также внимание, что если учетная запись пользователя была зарегистрирована до установки BioLink IDenium, то первый вход пользователя должен быть, либо по имени пользователя и паролю, либо с помощью смарт-карты. Чтобы войти в систему по отпечаткам пальцев, пользователь должен попросить администратора сменить (сбросить) пароль пользователя. Это необходимо для того, чтобы пароль попал в БД сервера BioLink IDenium.

4.2 Общие рекомендации по регистрации на АРМ пользователя

Раньше вам приходилось каждый раз вводить пароль (и иногда имя пользователя) для входа в операционную систему и доступа к защищенным ресурсам. Если вы использовали смарт-карту для входа в операционную систему, то вам приходилось запоминать, и каждый раз вводить ПИН-код своей карты.

Теперь, после установки BioLink IDenium, достаточно приложить всего лишь палец к сканеру отпечатков пальцев.

Разработчики BioLink IDenium настоятельно рекомендуют пользоваться только биометрическим входом в систему после установки BioLink IDenium Windows Logon.

Пользователь может также войти в операционную систему, предъявив имя и пароль своей учетной записи.

Это может оказаться полезным в следующих случаях:

- палец пользователя поврежден, и результат сканирования отпечатка пальца не совпадает с его эталоном;
- сканер отпечатков пальцев не установлен или работает некорректно.

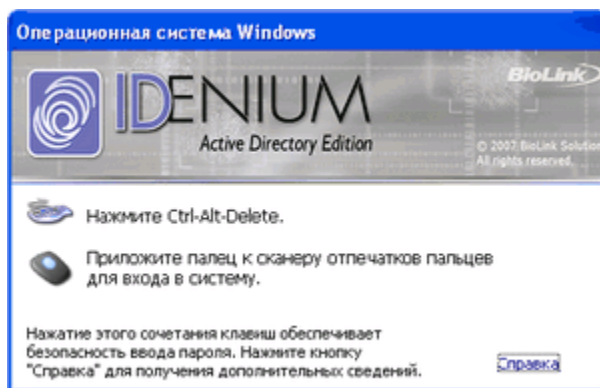
Администратор может обязать вас использовать многофакторную идентификацию. Это значит, что для входа в операционную систему вам придется и приложить палец к сканеру отпечатков пальцев, и ввести имя пользователя и пароль своей учетной записи Windows.

4.3 Вход в Windows XP по отпечатку пальца

Чтобы войти в Windows XP по отпечатку пальца, выполните следующие действия:

1. Включите компьютер.
2. После загрузки операционной системы на экране появится окно «Операционная система Windows» с приглашением приложить палец к окну сканера отпечатков пальцев.

Окно «Операционная система Windows XP»



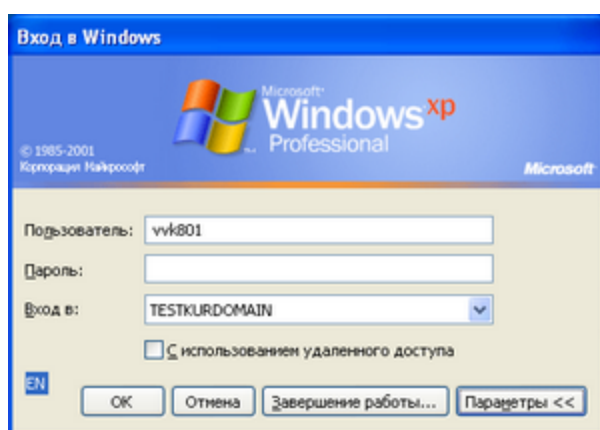
3. Приложите палец к окну сканера, как вы это делали в процессе ввода в систему эталонов отпечатков пальцев. Если вы ввели в систему несколько отпечатков пальцев, то используйте любой из них.
4. После успешного распознавания вас по отпечатку пальца запустится операционная система.
5. Вы можете также использовать имя и пароль своей учетной записи для входа в операционную систему. Впоследствии вы можете использовать эти идентификаторы, например, в том случае, если палец поврежден, и новый отпечаток пальца не соответствует какому-либо эталону, хранящемуся в БД BioLink IDenium.

4.4 Вход в Windows XP по паролю

Данная процедура не отличается от стандартной процедуры входа в операционные системы семейства Windows. После включения и загрузки операционной системы появится окно «Вход в Windows», в котором необходимо указать требуемую идентификационную информацию о пользователе.

Замечание! Конкретные шаги пользователя при входе в операционную систему Windows по паролю зависят от настроек политик, определяемых администратором сети/домена.

Окно «Вход в Windows»



При входе в операционную систему пользователь должен указать имя и пароль своей учетной записи Windows. После развертывания BioLink IDenium, характеристики данной учетной записи расширяются за счет добавления в нее биометрической информации (эталон отпечатков пальцев) и других служебных данных, необходимых для корректного функционирования BioLink IDenium.

После успешной авторизации пользователя запустится операционная система.

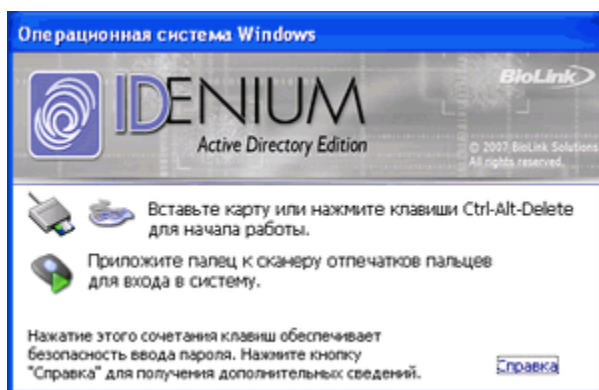
После входа в операционную систему рекомендуется создать эталон отпечатка пальца в БД BioLink IDenium, чтобы при следующем входе в операционную систему вам было достаточно приложить палец к окну сканера отпечатков пальцев для идентификации вас как пользователя.

4.5 Вход в Windows XP с помощью смарт-карты

Чтобы войти в Windows XP с помощью смарт-карты, выполните следующие действия:

1. При появлении на экране Windows окна «Операционная система Windows» вставьте смарт-карту в считыватель карт.
2. В ответ на соответствующее приглашение ввести ПИН-код приложите палец к сканеру отпечатков пальцев, как вы это делали в процессе ввода в BioLink IDenium эталонов отпечатков пальцев. Если вы ввели в BioLink IDenium несколько отпечатков пальцев, то используйте любой из них.
3. После успешного распознавания вас по отпечатку пальца запустится операционная система.

Вход в систему с помощью смарт-карты



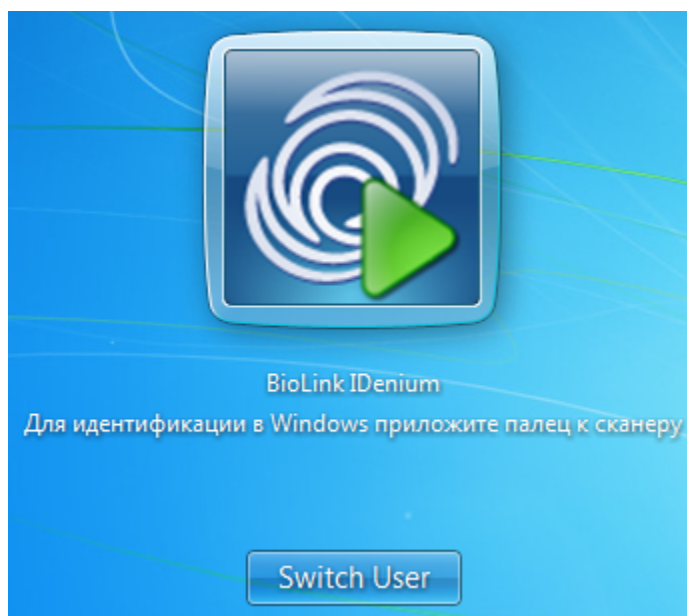
Заметьте, вам больше не надо вводить ПИН-код карты. ПИН-код карты будет подставлен автоматически после предъявления отпечатка пальца.

4.6 Вход в Windows Vista / 7 / 8 по отпечатку пальца

Чтобы войти в Windows Vista / 7 / 8 по отпечатку пальца, выполните следующие действия:

1. Включите компьютер.
2. После загрузки системы на экране появится окно «BioLink IDenium» с приглашением приложить палец к окну сканера отпечатков пальцев

Приглашение входа по отпечатку пальца в Windows 7



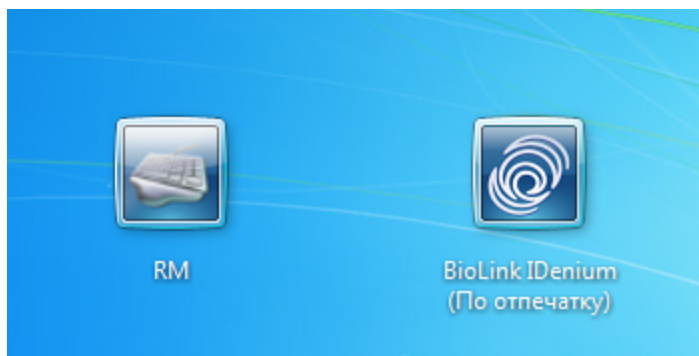
3. Приложите палец к окну сканера, как вы это делали в процессе ввода в BioLink IDenium эталонов отпечатков пальцев. Если вы ввели в BioLink IDenium несколько отпечатков пальцев, то используйте любой из них.
4. После успешного распознавания вас по отпечатку пальца запустится операционная система.

4.7 Вход в Windows Vista по паролю

Чтобы войти в Windows Vista / 7 / 8 по паролю, выполните следующие действия:

1. Включите компьютер.
2. После загрузки системы на экране появится приглашение приложить палец к окну сканера отпечатков пальцев.
3. Нажмите кнопку **«Сменить пользователя»**.
4. В окне выбора способа доступа в Windows Vista выберите режим **«BioLink IDenium (по имени и паролю)»**.

Окно выбора способа доступа в Windows 7



5. В окне «BioLink IDenium» введите ваши учетные данные в следующем виде:

- имя_домена\имя_пользователя (например, tesdomain\testuser),
- пароль.

Окно «BioLink IDenium»



1. Нажмите клавишу ENTER. После успешного распознавания вашего имени пользователя и пароля запустится операционная система.

4.8 Возможные сообщения об ошибках при регистрации на APM пользователя

Возможные сообщения об ошибках при регистрации на APM пользователя:

«Ошибка идентификации»

Причина: Предъявленные отпечатки пальцев не найдены в БД BioLink IDenium.

Если программный комплекс BioLink IDenium не распознал отпечаток пальца, для которого был создан эталон в БД, воспользуйтесь следующими рекомендациями для решения данной проблемы:

а) Проверьте положение пальца

Поворот или смещение пальца относительно его эталонного расположения на окне сканера рассматривается программой как ошибка сканирования. Попробуйте разместить палец на окне сканера так, как это делали в процессе обучения.

б) Проверьте состояние пальца

Протрите пальцы сухой материей, если они слишком влажные. Согрейте пальцы, если они слишком холодные.

в) Очистите поверхность сканера

Для очистки поверхности сканера от пыли или жира используйте клейкую ленту.

г) Войдите в систему по паролю

Если в БД BioLink IDenium отсутствуют эталоны ваших отпечатков пальцев, нажмите CTRL+ALT+DEL для ввода имени и пароля вашей учетной записи. После входа в операционную систему создайте в БД BioLink IDenium эталон отпечатка вашего пальца

д) Отсутствует подключение к серверу BioLink IDenium

Проверьте, доступен ли сервер BioLink IDenium с APM пользователя. Также уточните, корректно ли функционирует сервер BioLink IDenium.

д) Обратитесь к системному администратору

В случае повторения ошибки обратитесь к системному администратору.

«Для данного пользователя вход в Windows с использованием отпечатков пальцев запрещен политиками IDenium»

Причина: Политики BioLink IDenium запрещают вам использовать отпечатки пальцев для входа в операционную систему. За дополнительной информацией обратитесь к

системному администратору.

«Для данного пользователя вход в Windows с использованием имени и пароля запрещен политиками IDenium»

Причина: Политики BioLink IDenium запрещают вам использовать имя пользователя и пароль для входа в операционную систему. За дополнительной информацией обратитесь к системному администратору.

5 Управление биометрическими идентификаторами и паролями

В этой главе собрана информация об операциях, которые пользователь может выполнять со своими идентификаторами (паролями и эталонами отпечатков пальцев) с помощью IDenium Windows Logon

5.1 Учетные данные пользователя

После установки IDenium к стандартным учетным данным (имя и пароль) пользователя домена добавляются биометрические идентификаторы. При этом все пользователи домена становятся также и пользователями IDenium.

Таким образом, учетные данные пользователя состоят из:

- **Эталонов отпечатков пальцев пользователя**

Отпечатки пальцев является основными идентификаторами пользователя в системе. Эталоны отпечатков пальцев могут создаваться либо при создании учетной записи пользователя системным администратором, либо самим пользователем на своем рабочем месте. Существует возможность создать для каждого пользователя до 10 эталонов отпечатков пальцев.

Информацию о создании, изменении и удалении эталонов отпечатков пальцев, можно найти в разделе Как ввести в систему отпечатки пальцев

- **Имени и пароля пользователя**

Имя и пароль пользователя используются в стандартных процедурах входа для идентификации и проверки подлинности прав пользователя путем сравнения введенной информации с данными из учетной записи пользователя в системе или сети, к которой пытается обратиться пользователь. Windows Logon позволяет заменить стандартную процедуру входа по паролю идентификацией пользователя по отпечатку пальца.

После установки IDenium Windows Logon на Вашей рабочей станции настоятельно рекомендуется использовать биометрические идентификаторы для входа в систему и доступа к защищенным ресурсам.

- **Цифровых сертификатов**

Цифровые сертификаты могут быть записаны на смарт-карту, которая и будет использоваться для идентификации пользователя в системе (точнее для идентификации будет использоваться цифровой сертификат).

Программный комплекс BioLink IDenium поддерживает вход в систему с помощью смарт-карт, позволяя заменить процедуру ввода ПИН-кода на предъявление биометрических идентификаторов.

5.2 Как ввести в систему отпечатки пальцев

Внимание! Только владелец отпечатков пальцев может ввести в систему свои отпечатки пальцев. Аналогично только владелец отпечатков пальцев может изменить, добавить или удалить какой-либо эталон отпечатка пальца. Несмотря на то, что администратор может изменять шаблоны отпечатков пальцев пользователя (используя свой компьютер), настоятельно рекомендуется, чтобы пользователь самостоятельно управлял эталонами своих отпечатков пальцев.

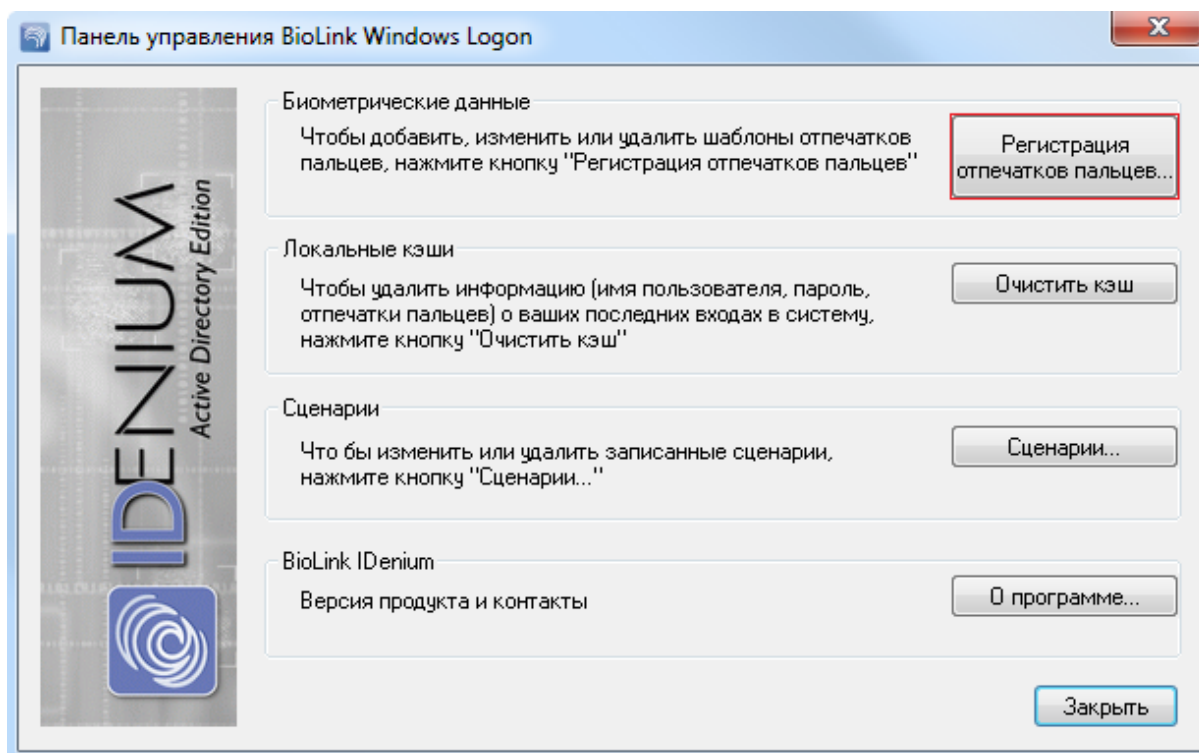
Существует возможность ввести до 10 отпечатков пальцев (т.е. все пальцы на руках). Другими словами, вы можете создать до 10 эталонов отпечатков пальцев в системе. Вы также можете удалять ранее введенные отпечатки и создавать вместо них новые.

Редактирование эталонов отпечатков пальцев пользователя может потребоваться в следующих случаях:

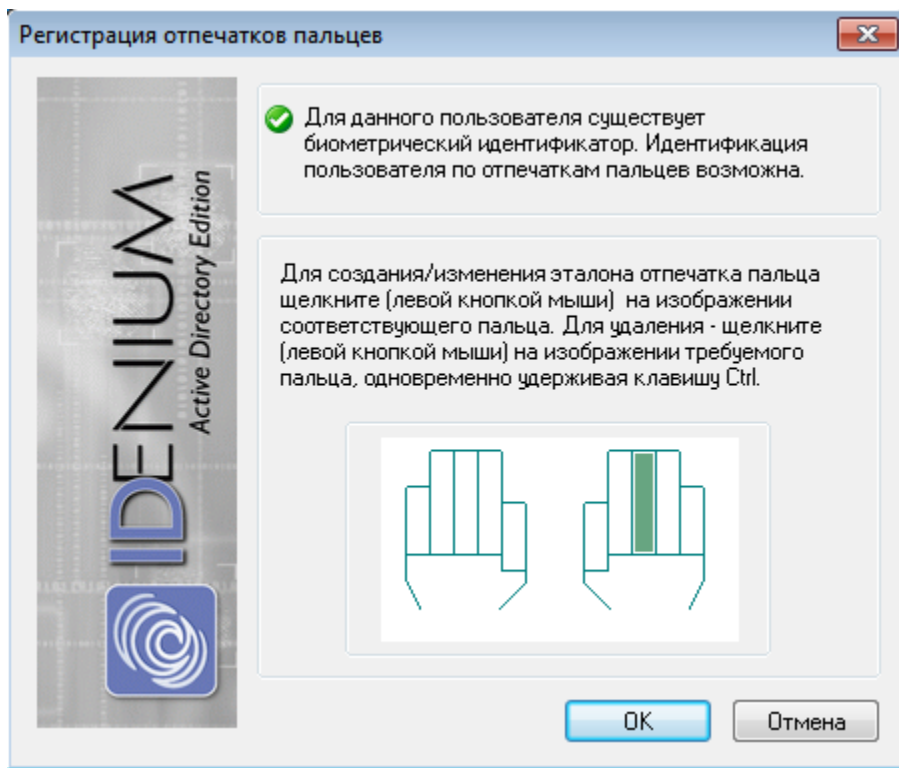
- Палец (ы), зарегистрированный (е) в системе временно поврежден (ы);
- Пользователь хочет использовать другой палец для входа в систему;
- Пользователь хочет добавить или удалить какой-либо эталон отпечатков пальцев.

Чтобы ввести в систему отпечатки пальца, выполните следующие действия:

1. Запустите **Панель управления BioLink Windows Logon**. Для этого нажмите **Пуск - Программы - BioLink IDenium Windows Logon - Панель управления BioLink Windows Logon**.



2. Далее нажмите кнопку **Регистрация отпечатков пальцев**, чтобы открыть диалоговое окно **Регистрация отпечатков пальцев**.



3. В диалоговом окне **Ввод отпечатков пальцев** щелкните (левой кнопкой мыши) по отпечатку, для которого требуется создать или изменить эталон отпечатка пальца. Если вы хотите удалить эталон, щелкните по требуемому пальцу, удерживая клавишу CTRL на клавиатуре.

4. Откроется форма **Обучение**

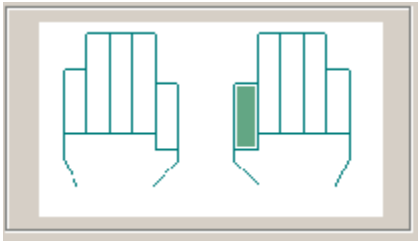


Следуя приглашениям программы в окне **Обучение**, приложите палец к окну биометрического сканера (например, это может быть BioLink U-Match в.3.5). В процессе обучения необходимо несколько раз приложить палец к окну сканера, следуя приглашениям программы. После успешного создания эталона отпечатка пальца окно закроется автоматически.

Для отмены процесса обучения надо нажать кнопку **Отмена** до завершения сканирования.

Примечание. Обратите внимание, что для корректного обучения необходимо каждый раз немного изменять положение пальца при сканировании. Каждый раз при сканировании палец нужно приподнимать и вновь прикладывать с небольшим смещением и поворотом. Если в окне обучения приглашение убрать палец с экрана сканера отображается даже тогда, когда палец не приложен к сканеру, почистите окно сканера с помощью специальных средств.

5. В диалоговом окне **Ввод отпечатков пальцев** палец, для которого существует эталон отпечатка пальца, будет отмечен зеленым цветом. Чтобы удалить эталон отпечаток пальца, необходимо щелкнуть левой кнопкой мыши, удерживая клавишу CTRL на клавиатуре.



6. Вы можете ввести в систему отпечатки всех 10 пальцев. Чтобы создать эталон отпечатка для другого пальца, повторите пункты 3 и 4 настоящего действия.
7. В форме **Ввод отпечатков пальцев** нажмите **ОК**, чтобы сохранить изменения. Если вы не хотите сохранять сделанные изменения, нажмите кнопку **Отмена**.

5.3 Очистка кэша

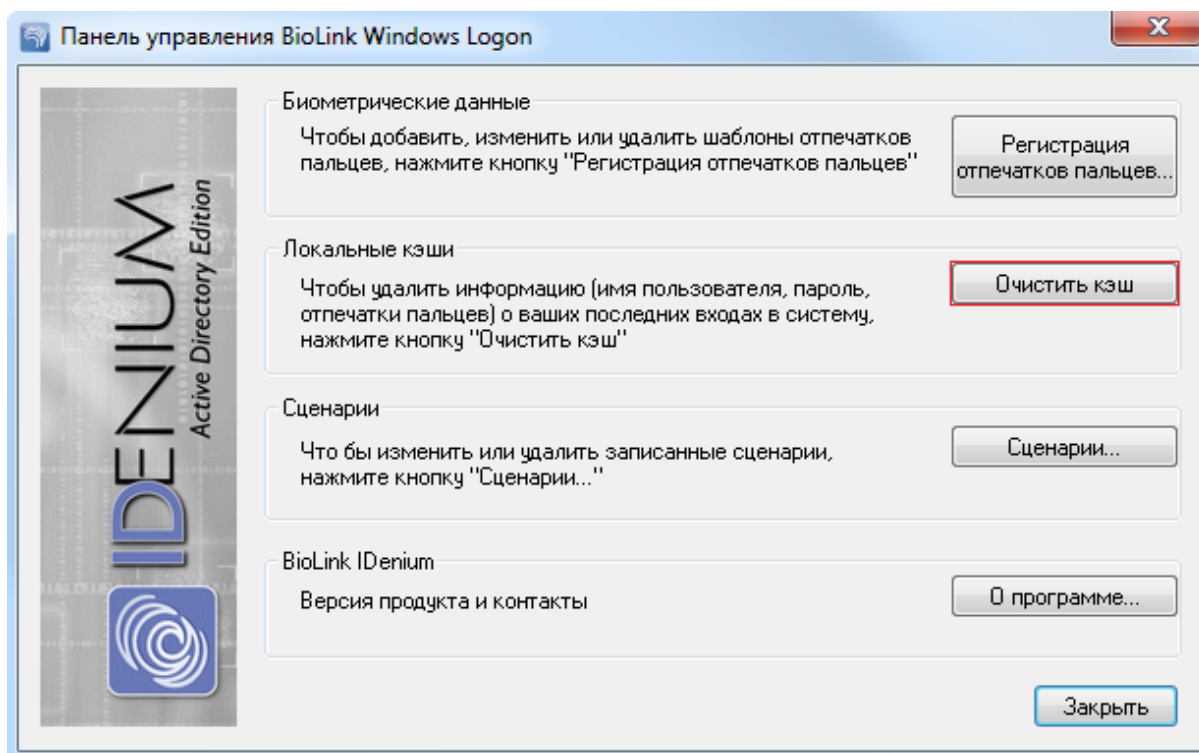
Кэширование конфиденциальной информации пользователей позволяет пользователям продолжать работу с защищенными ресурсами в случае недоступности сервера BioLink IDenium. В локальном кэше на жестком диске APM пользователя хранятся в закодированном виде пользовательские идентификаторы (имя пользователя, пароли, отпечатки пальцев), которые использовались при аутентификации во время входа в операционную систему, а также другая конфиденциальная пользовательская информация. Когда сервер BioLink IDenium становится недоступным, информация, хранящаяся в кэше локального APM пользователя, используется для предоставления доступа к защищенным ресурсам.

В общем случае, включение кэширования может привести к снижению общего уровня безопасности системы из-за того, что данные на APM пользователя потенциально подвержены большим рискам, чем информация, хранящаяся на выделенном сервере. Но в случае очистки кэша и недоступности сервера BioLink IDenium, выполнение операций, требующих аутентификации пользователя, будет невозможно.

Обратите также внимание, что при очистке кэша, удаляются данные только того пользователя, кто инициировал эту операцию. Идентификаторы других пользователей APM пользователя (имеющих другие учетные записи) останутся нетронутыми.

Чтобы очистить кэш, выполните следующие действия:

1. Запустите **Панель управления BioLink Windows Logon**. Для этого нажмите **Пуск - Программы - BioLink IDenium Windows Logon - Панель управления BioLink Windows Logon**.



2. Нажмите кнопку **Очистить кэш**.

3. Подтвердите удаление всей вашей информации из кэша, нажав кнопку **Да** в появившемся окне **Внимание**.

Внимание! Операция удаления ваших идентификаторов из локального кэша необратима и не может быть отменена. Если сервер BioLink IDenium не доступен, вход в систему, доступ к защищенным ресурсам или снятие блокировки компьютера могут оказаться невозможными.

Нажмите кнопку **Нет**, если вы не хотите очищать кэш.

Если на предыдущем шаге вы нажали кнопку **Да**, вся ваша информация, находящаяся в кэше, будет удалена.

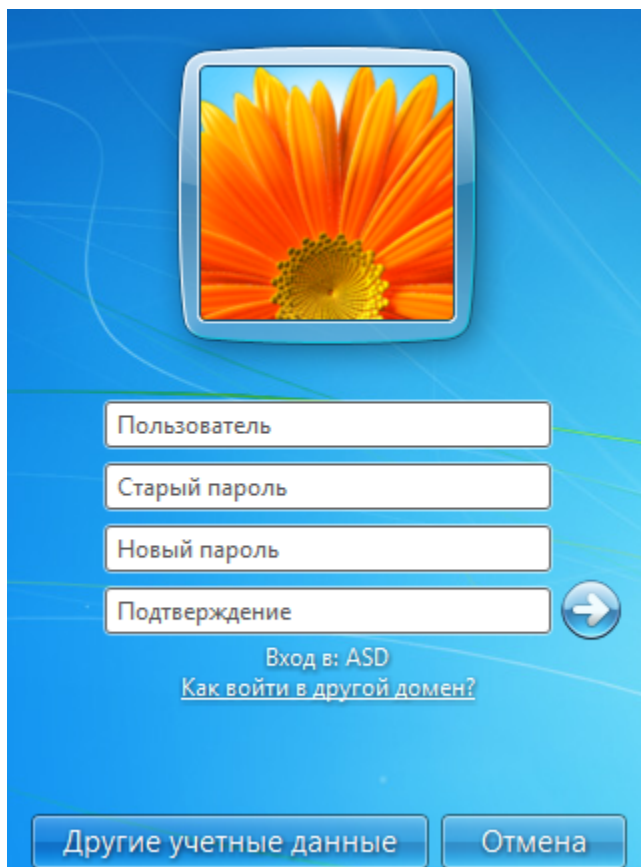
Замечание! Ваши пользовательские идентификаторы будут снова записаны в кэш при следующем входе в систему.

5.4 Изменение пароля пользователя

Пользователь может в любой момент изменить пароль своей расширенной учетной записи. Администратор системы также имеет привилегию изменять пароль любого пользователя.

Чтобы изменить пароль пользователя, выполните следующие действия:

1. Нажмите CTRL+ALT+DEL, чтобы вызвать окно **Блокировки Windows**.
2. Нажмите кнопку **Сменить пароль**.
3. В окне **Блокировки Windows** выполнить следующее:
 - Проверить правильность заполнения поля **Пользователь**. Должно быть указано имя домена/имя пользователя;
 - В поле **Старый пароль** ввести старый пароль пользователя;
 - В поле **Новый пароль** ввести новый пароль пользователя;
 - В поле **Подтверждение** ввести повторно новый пароль пользователя.



Пользователь

Старый пароль

Новый пароль

Подтверждение

Вход в: ASD
[Как войти в другой домен?](#)

Другие учетные данные

Отмена

4. Нажмите на стрелку ввода.

Внимание! Администратор локальной сети может запретить пользователям изменять свой пароль. В таком случае изменить пароль пользователя может только администратор.

6 Работа со сценариями IDenium Password Vault

Модуль BioLink IDenium Password Vault предназначен для замены доступа к различным приложениям по имени и паролю пользователя на биометрическую идентификацию.

Механизм работы BioLink IDenium Password Vault состоит в следующем:

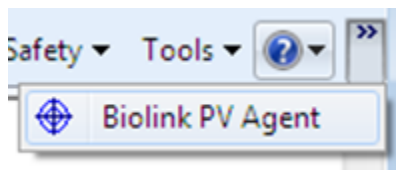
- для каждого диалогового окна, требующего авторизацию пользователя, можно создать специальные сценарии, позволяющие запомнить введенные имя и пароль пользователя;
- если пользователю необходимо авторизоваться в окне, для которого уже существует сценарий, то вместо ввода имени пользователя и пароля ему необходимо предъявить свои биометрические идентификаторы или предоставлен выбор выполняемого сценария, если на окно их было записано несколько;
- в случае, если предъявленные биометрические идентификаторы совпадают с хранящимися в БД Active Directory, будет выполнен сценарий, который автоматически подставит имя пользователя и пароль в соответствующие поля.

6.1 Запись сценариев BioLink IDenium Password Vault

Чтобы записать сценарий Password Vault для сайта, необходимо:

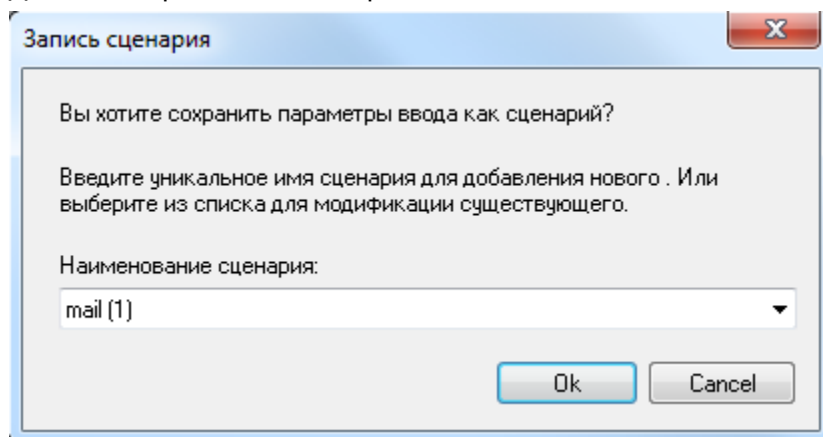
1. Открыть сайт, требующий учетные данные пользователя для входа
2. Заполнить форму входа на сайт
3.
 - a. Нажать кнопку входа на форме или
 - b. Нажать кнопку записи скрипта на панели браузера

Кнопка записи сценария в Internet Explorer



4. После этого откроется окно, предлагающее сохранить введенную информацию. При необходимости Вы можете изменить имя, под которым будет сохранен данный сценарий. Для подтверждения необходимо нажать кнопку ОК.

Диалог сохранения сценария



Чтобы записать сценарий BioLink IDenium Password Vault для приложения, выполните следующие действия:

1. запустите приложение, требующее авторизации пользователя.
2. дождитесь появления диалогового окна, приглашающего вас ввести имя пользователя и пароль.

3. начните запись сценария. Для этого:

- нажмите комбинацию клавиш ALT+CTRL+F10,

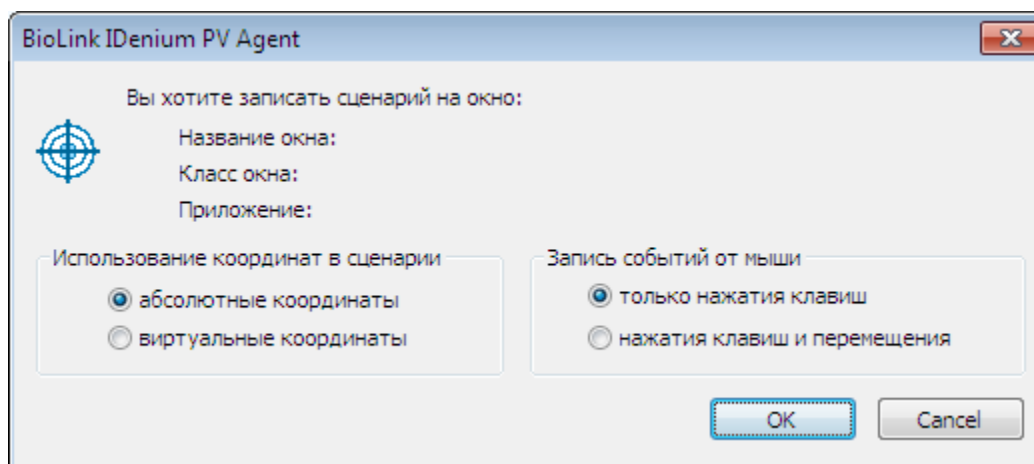
или

- щелкните правой кнопкой мыши значок модуля BioLink IDenium Password Vault Agent в области уведомлений и в появившемся контекстном меню выберите пункт «Начать запись сценария»,

1. в окне «**BioLink IDenium PV Agent**» настройте свойства создаваемого сценария. Вы можете настроить следующие свойства:

- выбрать, как будут вычисляться местоположение диалогового окна, для которого будет записан сценарий (абсолютные – пиксель, точка отсчета левый верхний угол экрана, виртуальные (относительные координаты, зависит от разрешения экрана)).
- определить, будут ли при записи сценария записываться не только щелчки мыши, но и перемещения мыши.

Окно «BioLink IDenium PV Agent»

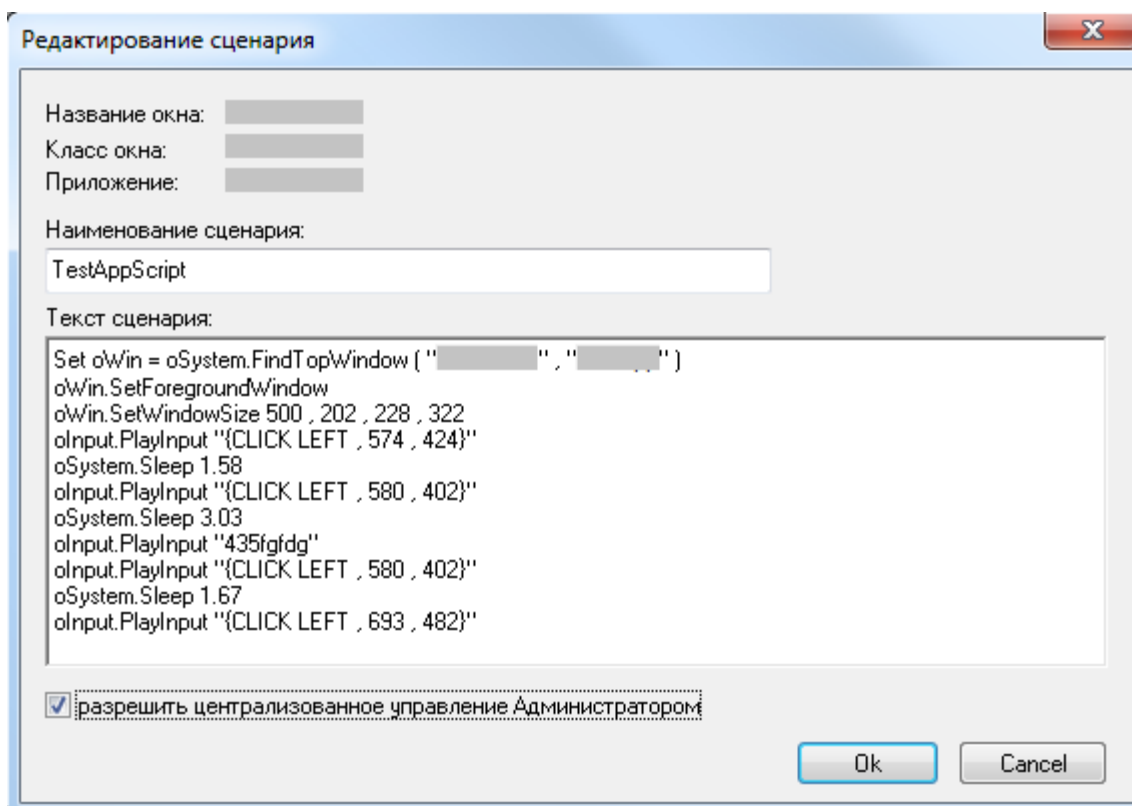


1. щелкните диалоговое окно, требующее авторизации пользователя. Обратите внимание, что в окне «**BioLink IDenium PV Agent**» изменились значения полей «**Название окна**», «**Класс окна**», «**Приложение**». Данные поля позволяют однозначно идентифицировать приложение и диалоговое окно, требующие авторизации пользователя,

2. в окне «BioLink IDenium PV Agent» нажмите кнопку ОК. Начнется запись сценария для выбранного диалогового окна,

3. в диалоговом окне, требующем авторизацию, введите ваше имя пользователя и пароль,
4. завершите запись сценария. Для этого:
 - нажмите комбинацию клавиш ALT+CTRL+F11,или
 - щелкните правой кнопкой мыши значок модуля BioLink IDenium Password Vault Agent в области уведомлений и в появившемся контекстном меню выберите пункт «**Завершить запись сценария**»,
1. сразу после окончания записи вы можете отредактировать сценарий, изменив название сценария и текст сценария в окне «**редактирования сценария**»,

Окно «редактирование сценария»



2. если вы хотите разрешить централизованное управление вашим сценарием, то отметьте соответствующее поле,
3. по окончании редактирования нажмите кнопку **ОК**. Запись сценария завершена.

Поддерживаемые переменные:

##DOMAIN## - передача имени домена

##USER## - передача доменного имени авторизованного пользователя

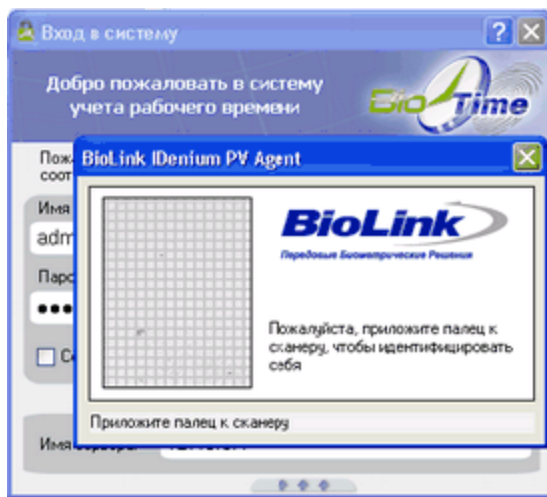
##PASSWORD## - передача доменного пароля авторизованного пользователя

6.2 Выполнение сценариев Password Vault

Чтобы выполнить ранее записанный сценарий, выполните следующие действия:

1. запустите приложение, требующее авторизации пользователя,
2. дождитесь появления диалогового окна, приглашающего вас ввести имя пользователя и пароль,
3. следуя приглашениям в окне «BioLink IDenium PV Agent» приложите палец к сканеру отпечатков пальцев,

Окно «BioLink IDenium PV Agent»



4. в случае успешной идентификации имя пользователя и пароль, введенные вами при записи этого сценария автоматически подставятся в соответствующие поля, ваша личность будет подтверждена, и вы сможете продолжить работу с приложением.

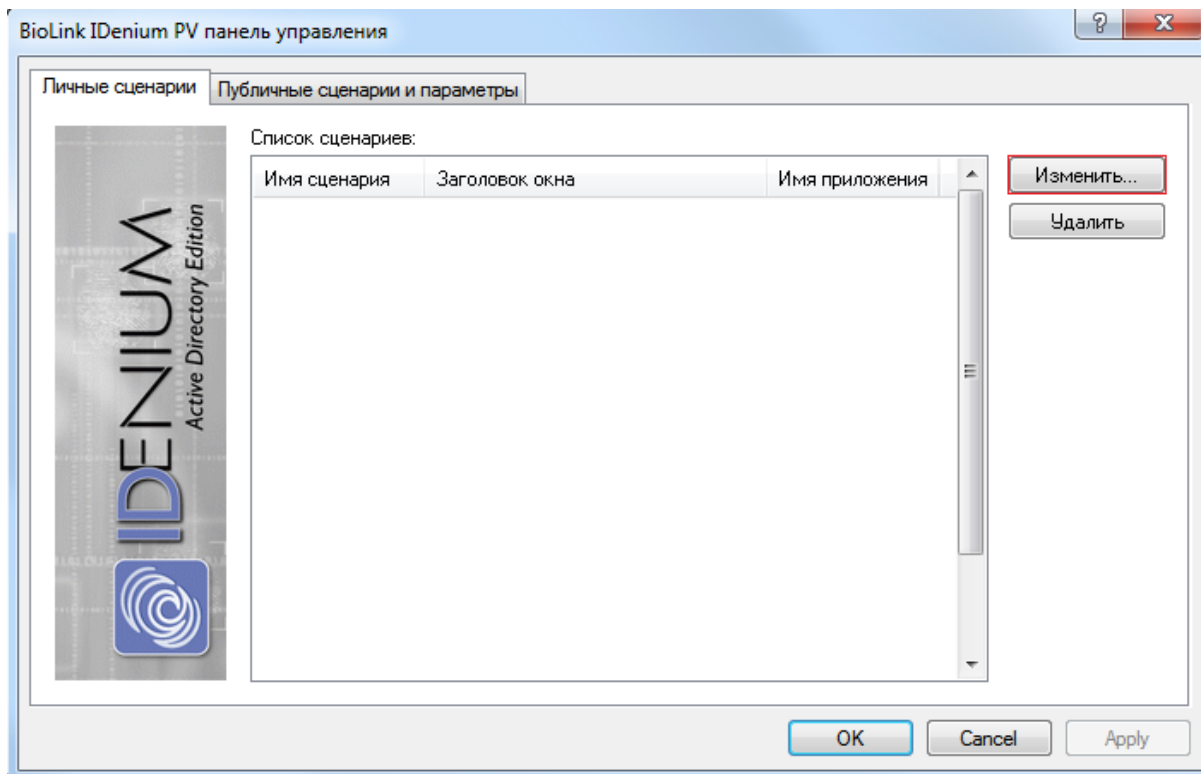
6.3 Изменение сценариев BioLink IDenium Password Vault

Сценарии Password Vault для сайтов не могут быть изменены непосредственно. Для этого следует использовать следующий способ:

1. Откройте требуемый сайт
2. Закройте появившееся окно сканирования отпечатка пальца
3. Заполните поля формы входа сайта требуемыми новыми значениями и осуществите вход
4. Появится диалоговое окно, в котором можно подтвердить изменение сценария или сохранить новый вариант в качестве альтернативного

Чтобы изменить ранее записанный сценарий для приложения, выполните следующие действия:

1. запустите панель управления сценариями BioLink IDenium Password Vault. Для этого щелкните правой кнопкой мыши значок приложения BioLink IDenium Password Vault Agent в области уведомлений и в появившемся контекстном меню выберите пункт **«Управление сценариями»**,
 2. в диалоговом окне **«BioLink IDenium PV панель управления»** в списке **«Список сценариев»**, выберите сценарий, которые вы хотите изменить,
- Окно «BioLink IDenium PV панель управления»



3. нажмите кнопку «**Изменить**»,
4. внесите необходимые изменения. Вы можете изменить название сценария и текст сценария,
5. по окончании нажмите кнопку **OK**.

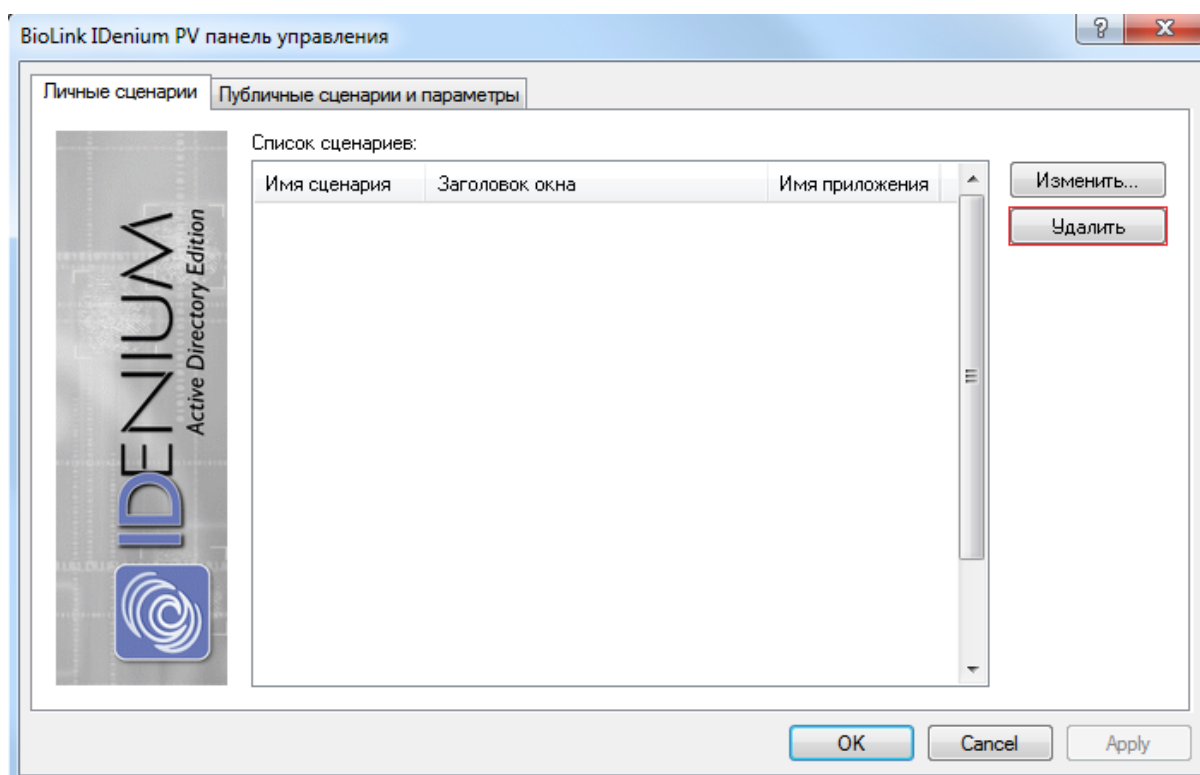
Примечание. Администратор BioLink IDenium может запретить вам вносить изменения в текст и название сценария. В таком случае вы не сможете изменить выбранный сценарий.

6.4 Удаление сценариев BioLink IDenium Password Vault

Чтобы удалить ранее записанный сценарий, выполните следующие действия:

1. запустите панель управления сценариями BioLink IDenium Password Vault. Для этого щелкните правой кнопкой мыши значок приложения BioLink IDenium Password Vault Agent в области уведомлений и в появившемся контекстном меню выберите пункт **«Управление сценариями»**,
2. в окне **«BioLink IDenium PV панель управления»** в списке **«Список сценариев»**, выберите сценарий, которые вы хотите удалить,

Окно «BioLink IDenium PV панель управления»



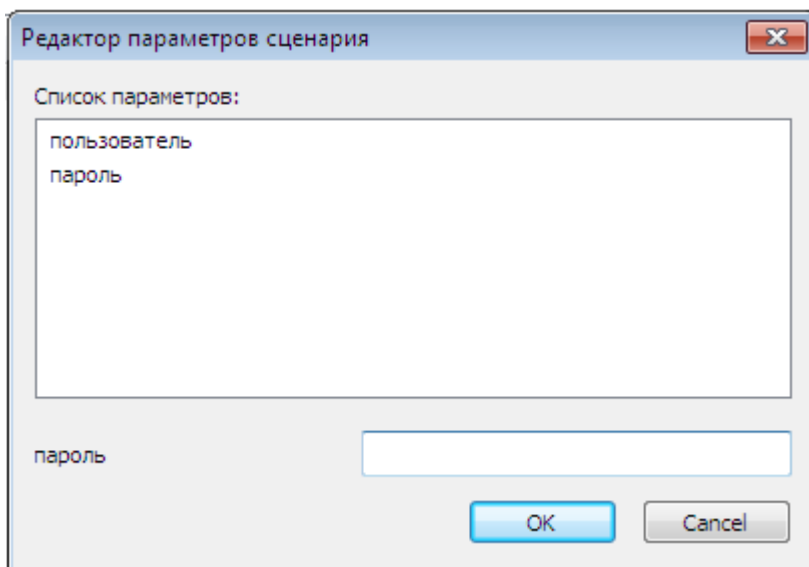
3. нажмите кнопку **«Удалить»**,
4. подтвердите удаление сценария,
5. по окончании нажмите кнопку **ОК**.

Примечание. Администратор BioLink IDenium может запретить вам удалять сценарии. В таком случае вы не сможете удалить выбранный сценарий.

6.5 Публичные сценарии и параметры BioLink IDenium Password Vault

Администратор может назначить пользователю сценарий, который содержит параметры необходимые к заполнению.

Если при запуске приложения и прохождении идентификации BioLink Password Vault, вы увидите окно схожее с окном представленным на скриншоте ниже, вам необходимо заполнить соответствующие поля.



Редактор параметров сценария

Список параметров:

- пользователь
- пароль

пароль

OK Cancel

Внимание!!! Форма для заполнения параметров при авторизации в приложении появляется единожды вне зависимости от того, правильно ли была введена информация. Повторное изменение параметров вы можете сделать при помощи приложения BioLink IDenium Password Vault Agent.

7 Сведения о программе

Для того чтобы узнать версию продукта и номер билда, необходимо в окне Панель управления Biolink Windows Logon нажать кнопку О программе.

