JaCarta SecurLogon

Руководство администратора

Аннотация

Настоящий документ содержит сведения по настройке и работе с JaCarta SecurLogon из состава Единого Клиента JaCarta.

Вопросы или пожелания по содержанию настоящего документа направляйте по адресу techwriters@aladdin-rd.ru.

Будем благодарны за конструктивные замечания и ответим на возникшие вопросы.

За технической поддержкой обращайтесь на веб-сайт ЗАО «Аладдин Р. Д.» по адресу http://www.aladdin-rd.ru/support/index.php.

Версия	1.0
Редакция от	31.10.2014
Листов	25

Телефон +7 (495) 223-00-01 • Факс +7 (495) 646-64-40 • aladdin@aladdin-rd.ru • www.aladdin-rd.ru

Содержание

1. Введение

1.1. Общие сведения

JaCarta SecurLogon позволяет повысить уровень безопасности при входе на локальный компьютер и в корпоративную сеть под управлением ОС Windows за счёт простого и быстрого перехода от авторизации по логину и паролю к двухфакторной аутентификации на основе электронного ключа. При этом отсутствует необходимость настройки Active Directory, внедрения PKI-инфраструктуры и создания собственного Удостоверяющего центра для выпуска сертификатов пользователей. При использовании JaCarta SecurLogon конечный пользователь не будет вводить с клавиатуры пароль Windows, что исключает возможность подсматривания или перехвата пароля злоумышленником.

1.2. Дополнительная документация

Для полного понимания настоящего документа рекомендуется ознакомиться с документом *Единый Клиент JaCarta – Руководство администратора*, содержащим сведения, касающиеся системных требований, установки и настройке с Единым клиентом JaCarta, а также сведения, касающиеся работы с электронными ключами.

2. Системные требования

Табл. 1

Системные требования SecurLogon

Операционные системы	○ Windows Vista ○ Windows 7 ○ Windows 8 ○ Windows 8.1 ○ Windows Server 2008 ○ Windows Server 2008 R2 ○ Windows 2012 ○ Windows 2012 R2
Поддерживаемые модели электронных ключей	**Электронные ключи JaCarta** ○ JaCarta PKI ○ JaCarta PKI/BIO ○ JaCarta PKI/Flash ○ JaCarta PKI/ГОСТ ○ JaCarta PKI/ГОСТ/Flash ○ JaCarta ГОСТ/Flash ○ JaCarta ГОСТ ○ JaCarta LT ○ JaCarta PKI/BIO/ГОСТ ○ JaCarta PKI. Обратная совместимость с продуктами компании Aladdin ○ JaCarta PKI/ГОСТ. Обратная совместимость с продуктами компании Aladdin **Электронные ключи eToken** ○ eToken PRO ○ eToken PRO (Java) ○ eToken NG-FLASH ○ eToken NG-FLASH (Java) ○ eToken NG-OTP ○ eToken NG-OTP (Java) ○ eToken ГОСТ

3. Установка лицензии SecurLogon

3.1. Установка лицензии на локальном компьютере

Добавить лицензию SecurLogon на локальном компьютере можно двумя способами:

- см. «Через меню настроек Единого Клиента JaCarta»;
- см. «В основном окне пользовательского интерфейса Единого Клиента JaCarta».

Чтобы добавить лицензию, вы пдолжны обладать правами администратора. Также, в случае добавления лицензии в основном окне пользовательского интерфейса Единого Клиента JaCarta необходимо подсоединить электронный ключ к компьютеру.

ЧЕРЕЗ МЕНЮ НАСТРОЕК ЕДИНОГО КЛИЕНТА JACARTA

1. Запустите Единый Клиент JaCarta.
2. В левой нижней части интерфейса нажмите **Настройки** и в отобразившемся окне выберите вкладку **SecurLogon**.
   Окно примет следующий вид.

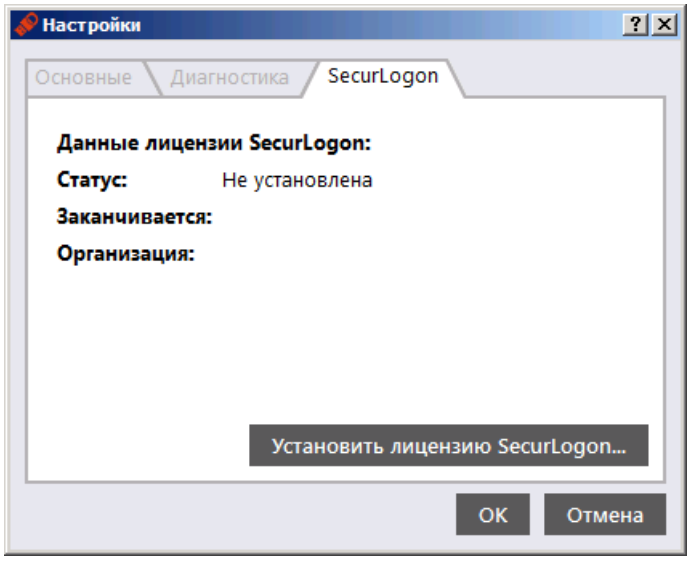

Рис. 1 – Вкладка SecurLogon окна настроек Единого Клиента JaCarta

3. Нажмите **Установить лицензию SecurLogon** и в отобразившемся окне укажите путь к файлу лицензии.

После добавления лицензии соответствующие данные отобразятся в окне настроек на вкладке **SecurLogon**.

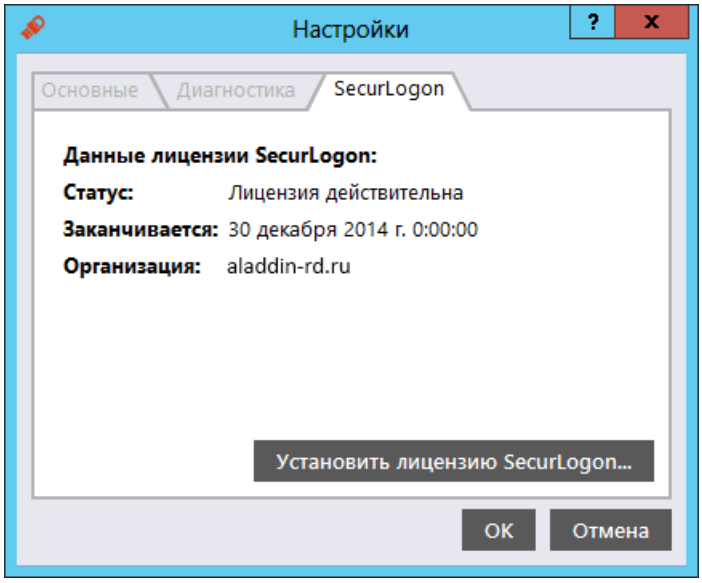

Рис. 2 – Информация об установленной лицензии

4. Нажмите **OK** для завершения процедуры.

В ОСНОВНОМ ОКНЕ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА ЕДИНОГО КЛИЕНТА JACARTA

1. Подсоедините к компьютеру электронный ключ, запустите Единый Клиент JaCarta и переключитесь в режим администратора.

2. В основной части интерфейса выберите вкладку **SecurLogon**.

Окно примет следующий вид.

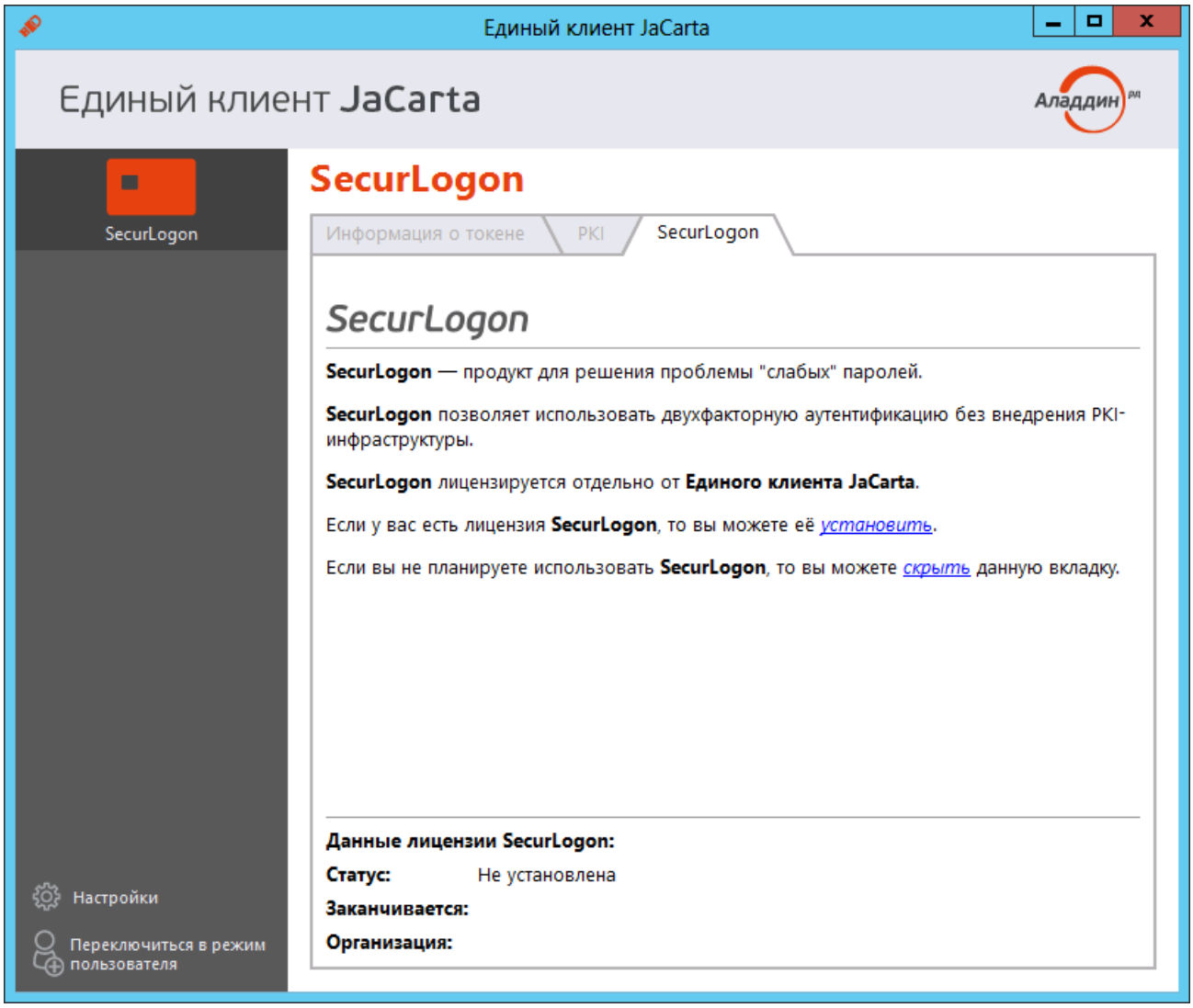

Рис. 3 – Вкладка **SecurLogon** в основном интерфейсе Единого Клиента JaCarta

3. Нажмите на ссылке **установить** в центральной части интерфейса и в отобразившемся окне укажите путь к файлу лицензии.

По успешном завершении операции вкладка примет следующий вид.

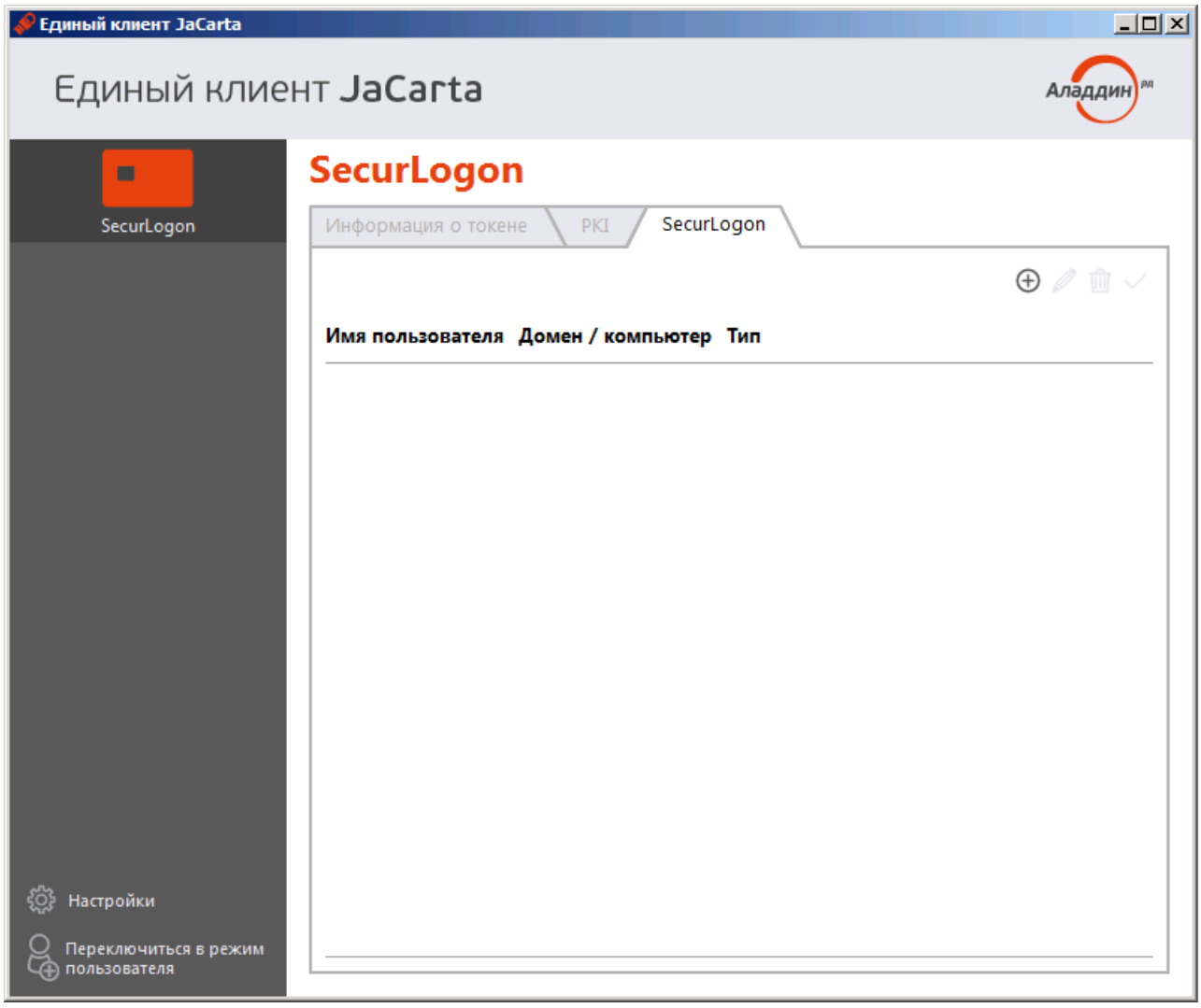

Рис. 4 – Лицензия успешно добавлена

4. Административный шаблон из состава SecurLogon

4.1. Доступ к настройкам административного шаблона

Чтобы отобразить настройки административного шаблона из состава SecurLogon, выполните следующие действия.

Эти действия можно выполнять как на контроллере домена, так и на компьютере, на которым установлены средства управлениям контроллером домена.

1. Из командной строки выполните команду **gpmc**.
Отобразится следующее окно.

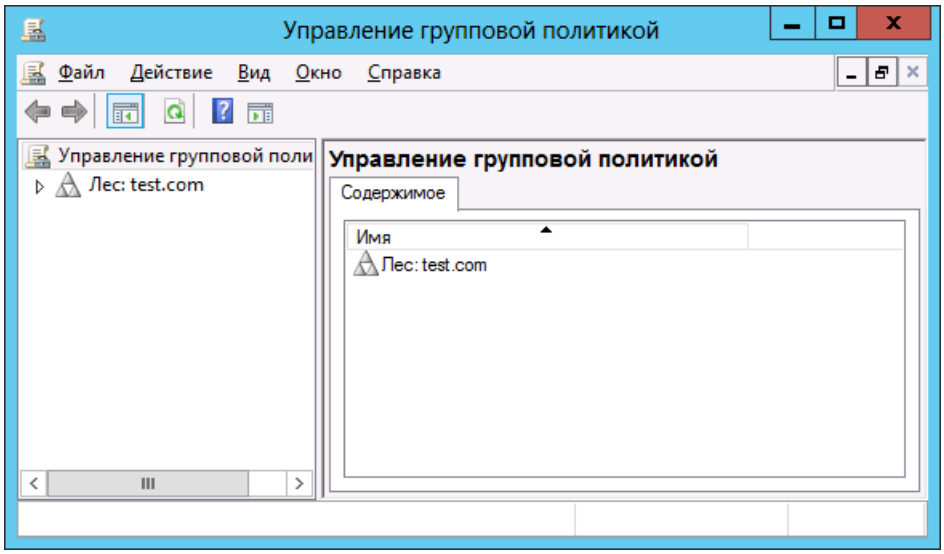

Рис. 5 – Окно управления групповой политикой.

2. Выберите **Лес > Домены > имя_домена**, нажмите правой кнопкой мыши на пункте **Default Domain Policy** (Политика домена по умолчанию) и выберите **Изменить** - как показано на изображении ниже.

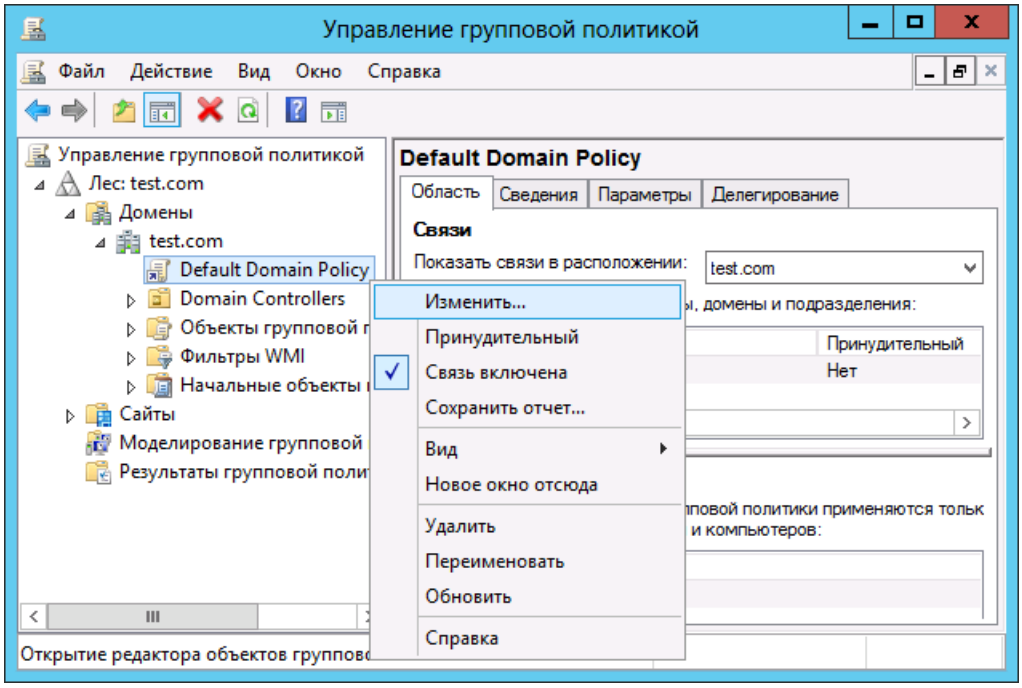

Рис. 6 – Изменение политики домена по умолчанию

Отобразится следующее окно.

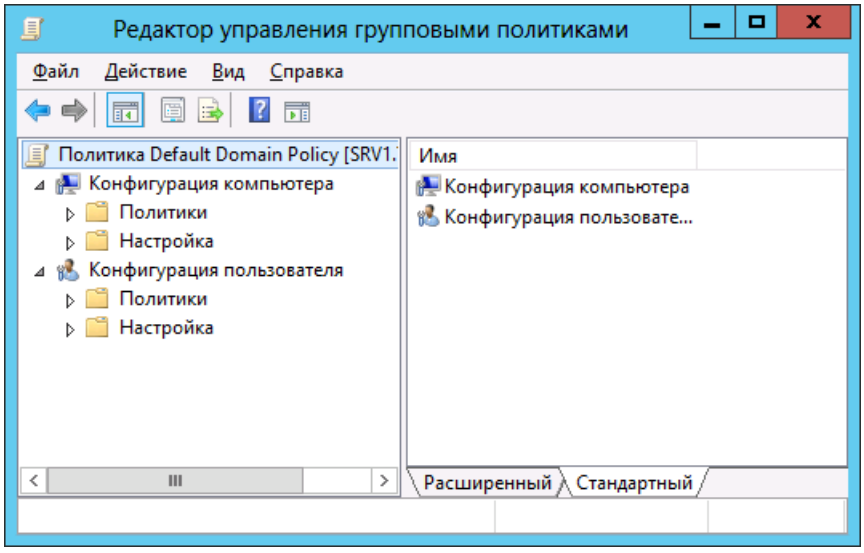

Рис. 7 – Окно редактора управления групповыми политиками

3. Выберите **Конфигурация компьютера > Политики > Административные шаблоны > JaCarta SecurLogon**.

Список политик управления отобразится в окне справа.

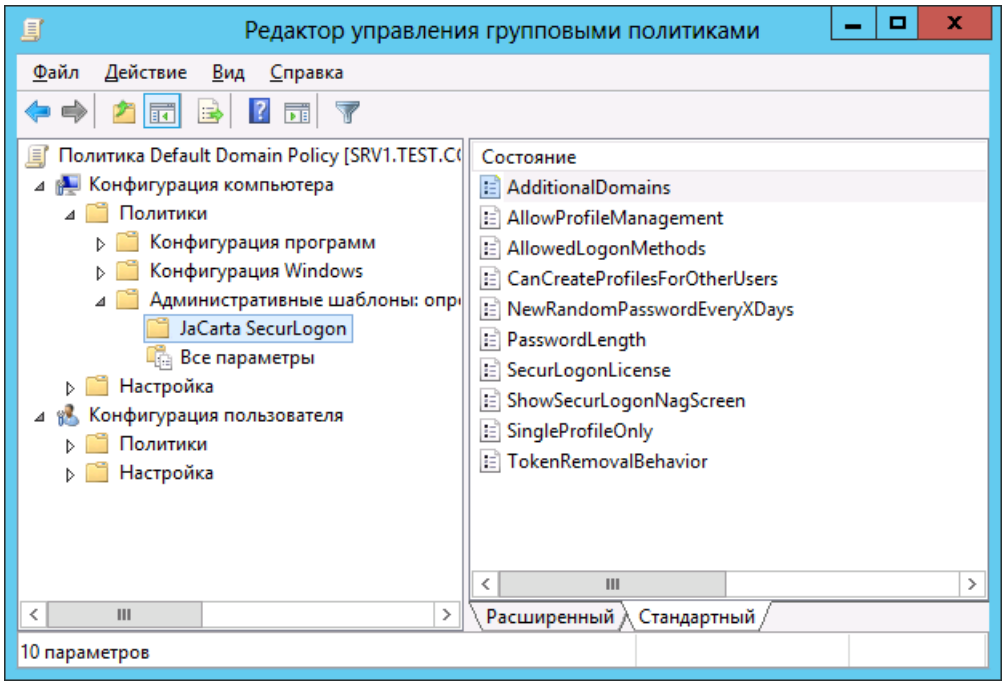

Рис. 8 – Политики управления SecurLogon

4. Выполните необходимую настройку, руководствуясь сведениями, приведёнными в подразделе «Настройки административного шаблона SecurLogon» ниже.

4.2. Настройки административного шаблона SecurLogon

Табл. 2

Политики управления SecurLogon

Название	Описание	Допустимые значения	Значение по умолчанию до распространения групповых политик[1]	Значение по умолчанию в шаблоне[2]
AdditionalDomains (Дополнительные домены)	Список дополнительных доменов, отображаемых при создании профиля или при входе с использованием профиля SecurLogon.	○ Имена доменов Windows, указанные через точку с запятой; ○ пустая строка.	Пустая строка	Пустая строка
AllowProfileManagement (Разрешить создание профилей пользователями)	Разрешает или запрещает пользователям создавать профили SecurLogon	○ **Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); ○ **Включено** – пользователи могут самостоятельно создавать профили; ○ **Отключено** – пользователи не могут самостоятельно создавать профили.	**Включено**	**Отключено**
AllowedLogonMethods (Разрешённые методы аутентификации)	Определяет перечень доступных методов аутентификации, которые доступны для входа в операционную систему.	○ **Не задано** – будет использоваться значение по умолчанию (последний столбец настоящей таблицы); ○ **Отключено** – будут использоваться стандартные механизмы Windows; ○ **Включено** – позволяет явно задать, какие методы входа можно будет использовать (при этом значение **1** означает, что метод разрешён, а **0** - запрещён): ○ Примечание: если все методы входа имеют одинаковые значения (как **0**, так и **1**), это означает, что все эти методы разрешены. • **DefaultPasswordLogon** – стандартный	Выбраны все методы	Выбраны все методы

[1] Эти значение применяются сразу после установки Единого Клиента JaCarta

[2] Применяются после распространения групповых политик, если в административный шаблон SecurLogon не было внесено никаких изменений

Название	Описание	Допустимые значения	Значение по умолчанию до распространения групповых политик[1]	Значение по умолчанию в шаблоне[2]
		вход в систему с использованием имени пользователя и пароля, вводимых с клавиатуры; • **DefaultSmartCardLogon** – вход с использованием сертификата, хранящегося в памяти электронного ключа; • **ManualPasswordLogon** – пароль для профиля SecurLogon вводится вручную; • **RandomPasswordLogon** – для профиля SecurLogon генерируется случайный пароль (см. «Создание профиля SecurLogon»). См. «Создание профиля SecurLogon».		
CanCreateProfilesForOtherUsers (Создание профилей для других пользователей)	Разрешает или запрещает пользователю создавать профили для других пользователей.	○ **Не задано** - будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); ○ **Включено** - пользователь может создавать профили для других пользователей; ○ **Отключено** - пользователь может создавать профили только для себя.	**Включено**	**Отключено**
NewRandomPasswordEveryXDays (Автоматически менять пароль каждые X дней)	Обновление случайного пароля для профиля SecurLogon каждые X дней. (Пользователь при этом должен запоминать только PIN-код электронного ключа.)	○ **Не задано** - будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); ○ **Включено** – при выборе этого пункта становится активным соответствующее поле, в котором нужно указать период (в днях), по истечении которого пароль для учётной записи Windows будет меняться; ○ **Отключено** – пароль учётной записи Windows не будет меняться автоматически.	**Отключено**	**Отключено**
PasswordLength (Длина случайного пароля учётной записи)	Задаёт длину случайного пароля для профиля SecurLogon.	○ **Не задано** - будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); ○ **Включено** – при выборе этого пункта становится активным соответствующее поле, в котором нужно указать длину случайного пароля (в символах), допустимые значения – от 14 до 63 символов; ○ **Отключено** – настройка не применяется.	**63**	**63**
SecurLogonLicense	Строка, содержащая лицензию	○ **Не задано** - будет использоваться значение по	**Пустая строка**	**Пустая строка**

Название	Описание	Допустимые значения	Значение по умолчанию до распространения групповых политик[1]	Значение по умолчанию в шаблоне[2]
(Лицензия SecurLogon)	SecurLogon.	умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); ○ **Включено** – при выборе этого пункта становится активным соответствующее поле, в которое необходимо полностью скопировать содержимое файла лицензии (для этого фай лицензии можно открыть в текстовом редакторе); ○ **Отключено** – лицензия не устанавливается (пустая строка);		
ShowSecurLogonNagScreen (Отображать вкладку **SecurLogon**, если лицензия не установлена)	Определяет отображать или не отображать вкладку **SecurLogon**, если лицензия не установлена.	○ **Не задано** - будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); ○ **Включено** – вкладка отображается; ○ **Отключено** – вкладка не отображается.	**Включено**	**Включено**
SingleProfileOnly (Один профиль на электронном ключе)	Разрешает или запрещает создание на одном электронном ключе нескольких профилей SecurLogon.	○ **Не задано** - будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); ○ **Включено** – пользователи могут создать только один профиль на электронном ключе; ○ **Отключено** – пользователи могут создавать несколько профилей на одном электронном ключе.	**Отключено**	**Отключено**
TokenRemovalBehavior (Поведение при отсоединении электронного ключа от компьютера)	Данная настройка определяет поведение системы в ситуации, в которой пользователь, осуществивший вход с помощью профиля SecurLogon, отсоединяет электронный ключ от компьютера.	○ **Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); ○ **Отключено** – никакие действия предприниматься не будут; ○ **Включено** – при выборе этого пункта становится активным соответствующий список, в котором можно выбрать вариант поведения системы: **Не выполнять никаких действий** – при отсоединении электронного ключа не предпринимается никаких действий; **Блокировать рабочую станцию** – при отсоединении электронного ключа происходит блокировка рабочего стола; • **Принудительный выход из системы** – при отсоединении электронного	**Не выполнять никаких действий**	**Не выполнять никаких действий**

Название	Описание	Допустимые значения	Значение по умолчанию до распространения групповых политик[1]	Значение по умолчанию в шаблоне[2]
		ключа производится принудительный выход из системы пользователя; • **Отключение при подключении через RDP** – при отсоединении электронного ключа происходит разрывания сеанса подключения через удалённый рабочий стол.		

5. Операции с профилями SecurLogon

5.1. Создание профиля SecurLogon

Чтобы создать профиль SecurLogon, выполните следующие действия.

1. Подсоедините электронный ключ, на котором вы хотите создать профиль SecurLogon, к компьютеру.
2. Запустите Единый Клиент JaCarta, переключитесь в режим администратора и перейдите на вкладку **SecurLogon**.
   Окно примет следующий вид.

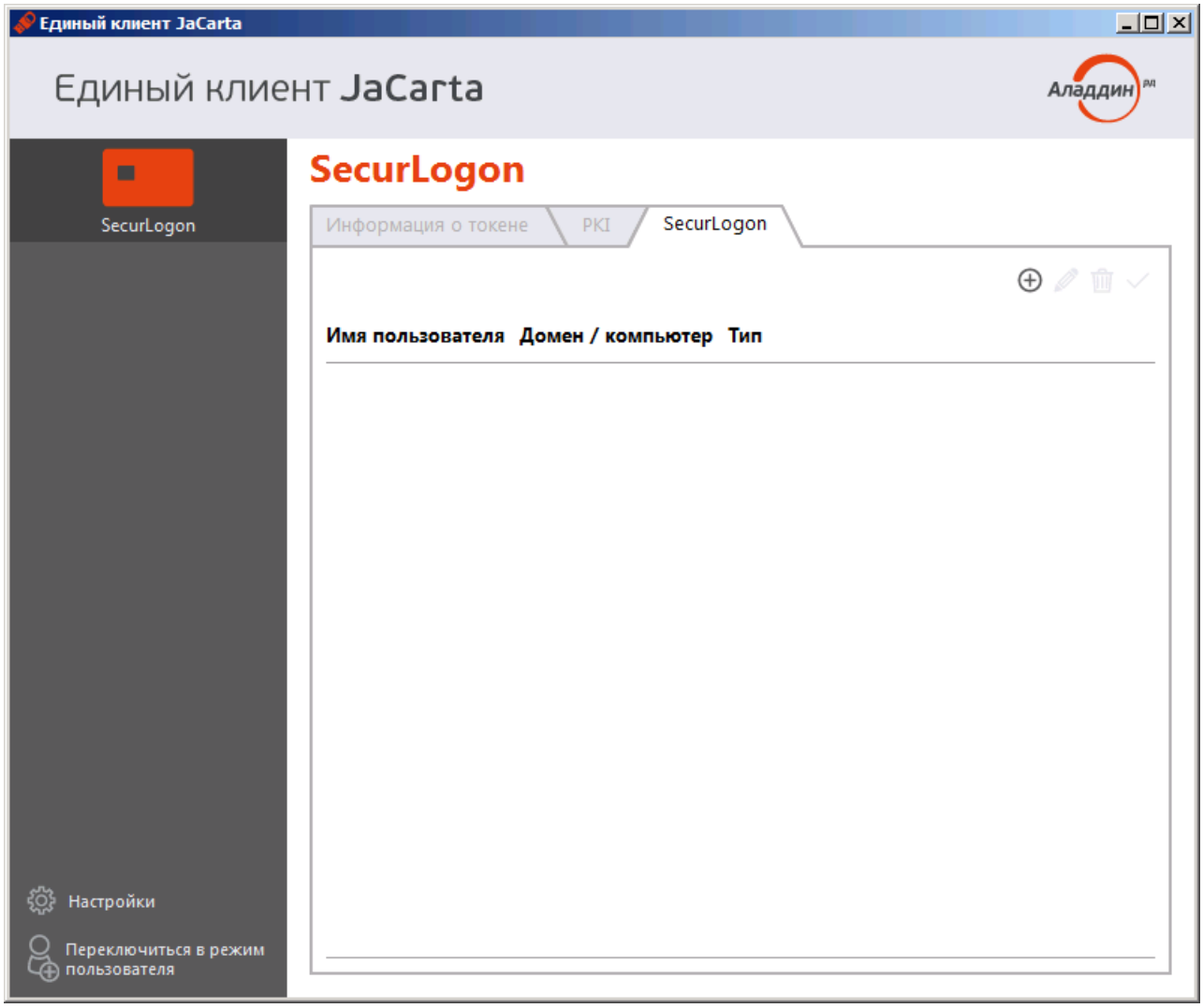

Рис. 9 – На подсоединённом ключе профили SecurLogon отсутствуют

3. Нажмите на значке ⊕ или нажмите правой кнопкой мыши в центральной части окна и в контекстном меню выберите **Создать**.
   Отобразится окно создания профиля SecurLogon.

Окна создания профиля SecurLogon различаются в зависимости от того, создаётся ли профиль для локальной учётной записи или для учётной записи в домене Windows (см. соответственно рис. 10 и рис. 11

ниже).

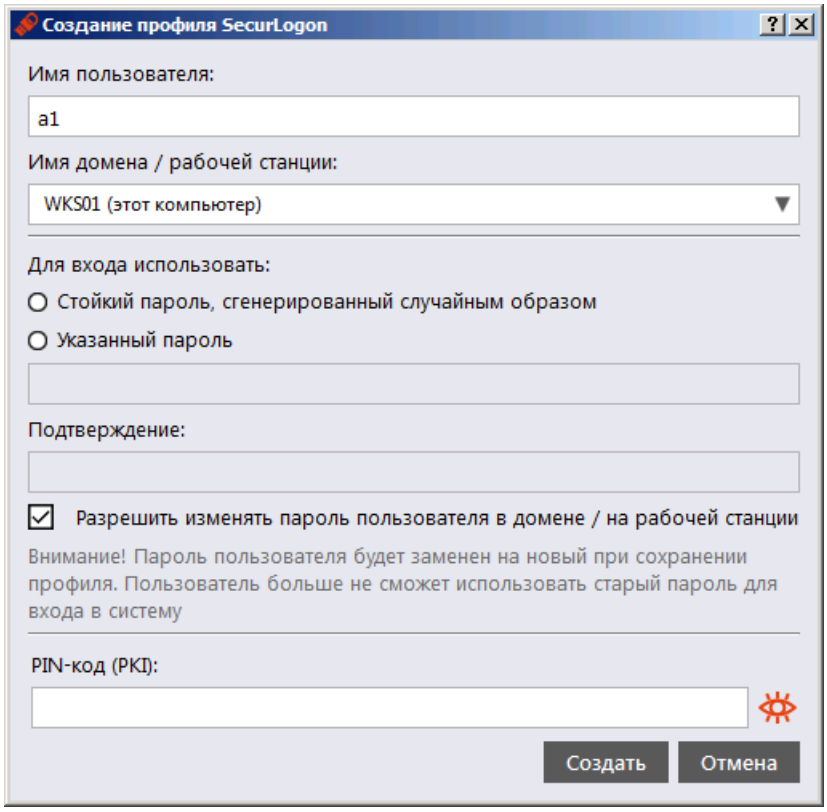

Рис. 10 - Создания профиля SecurLogon для локальной учётной записи

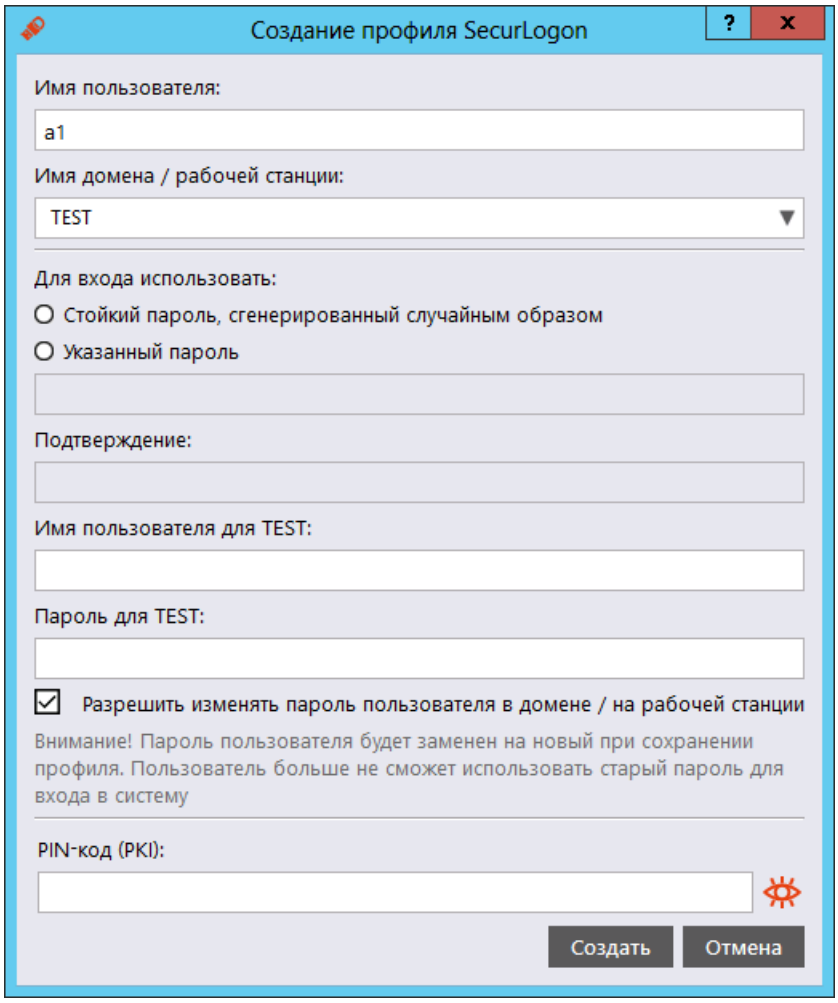

Рис. 11 – Создание профиля SecurLogon для учётной записи в домене Windows

4. Выполните настройку, руководствуясь табл. 3 ниже.

Табл. 3

Создание профиля SecurLogon

Настройка	Рабочая станция Домен
Имя пользователя	Имя пользователя, для которого будет создаваться профиль SecurLogon. Если профиль создаётся для учётной записи в домене Windows, то редактирование может быть недоступно в случае включённой настройкой **CanCreateProfilesForOtherUsers** (Создание профилей для других пользователей) отключена в административном шаблоне SecurLogon (см. «Настройки административного шаблона SecurLogon»).
Имя домена / рабочей станции	Позволяет выбрать имя домена или рабочей станции, на которой хранится учётная запись пользователя. Соответственно, если выбрано имя компьютера (рабочая станция), то профиль SecurLogon создаётся для локальной учётной записи. Если выбрано имя домена, профиль SecurLogon создаётся для учётной записи в домене Windows.
Для входа использовать	Выберите один из двух пунктов: ○ **Стойкий пароль, сгенерированный случайным образом** – пароль для учётной записи пользователя будет сгенерирован случайным образом; ○ **Указанный пароль** – пароль для учётной записи будет введён вручную; при выборе этого пункта становятся активными поле для ввода пароля и поле **Подтверждение**, в котором нужно указать подтверждение введённого пароля. Пользователь, который создаёт профиль SecurLogon (администратор SecurLogon), должен обладать достаточными правами для смены пароля пользователя, для которого создаётся профиль SecurLogon

Настройка	Рабочая станция	Домен
	(пользователь SecurLogon).	
Имя пользователя для домена	Не актуально.	Введите имя пользователя учётной записи администратора SecurLogon. Настройка активна, только если установлен флажок **Разрешить изменять пароль пользователя в домене / на рабочей станции** (подробнее см. описание соответствующей настройки).
Пароль для домена	Не актуально.	Введите пароль учётной записи администратора SecurLogon. Настройка активна, только если установлен флажок **Разрешить изменять пароль пользователя в домене / на рабочей станции** (подробнее см. описание соответствующей настройки).
Разрешить изменять пароль пользователя в домене / на рабочей станции	Данная настройка определяет, будет ли изменён пароль учётной записи пользователя, для которого создаётся профиль SecurLogon. Если флажок установлен, будет установлен пароль, заданный в настройке **Для входа использовать** (т.е. это может быть случайный пароль или пароль, введённый администратором при создании профиля). При этом администратор SecurLogon, который создаёт профиль SecurLogon, должен обладать достаточными полномочиями для смены пароля учётной записи пользователя SecurLogon. При создании профиля SecurLogon для учётной записи в домене Windows также необходимо заполнить следующие поля: **Имя пользователя для домена**; **Пароль для домена**. В этих полях необходимо указать имя пользователя и пароль учётной записи администратора SecurLogon, который впоследствии сможет изменять пароль пользователя SecurLogon.	
PIN-код	Введите текущий PIN-код электронного ключа.	

5. Нажмите **Создать**.

Созданный профиль отобразится на вкладке **SecurLogon** в интерфейсе Единого Клиента JaCarta.

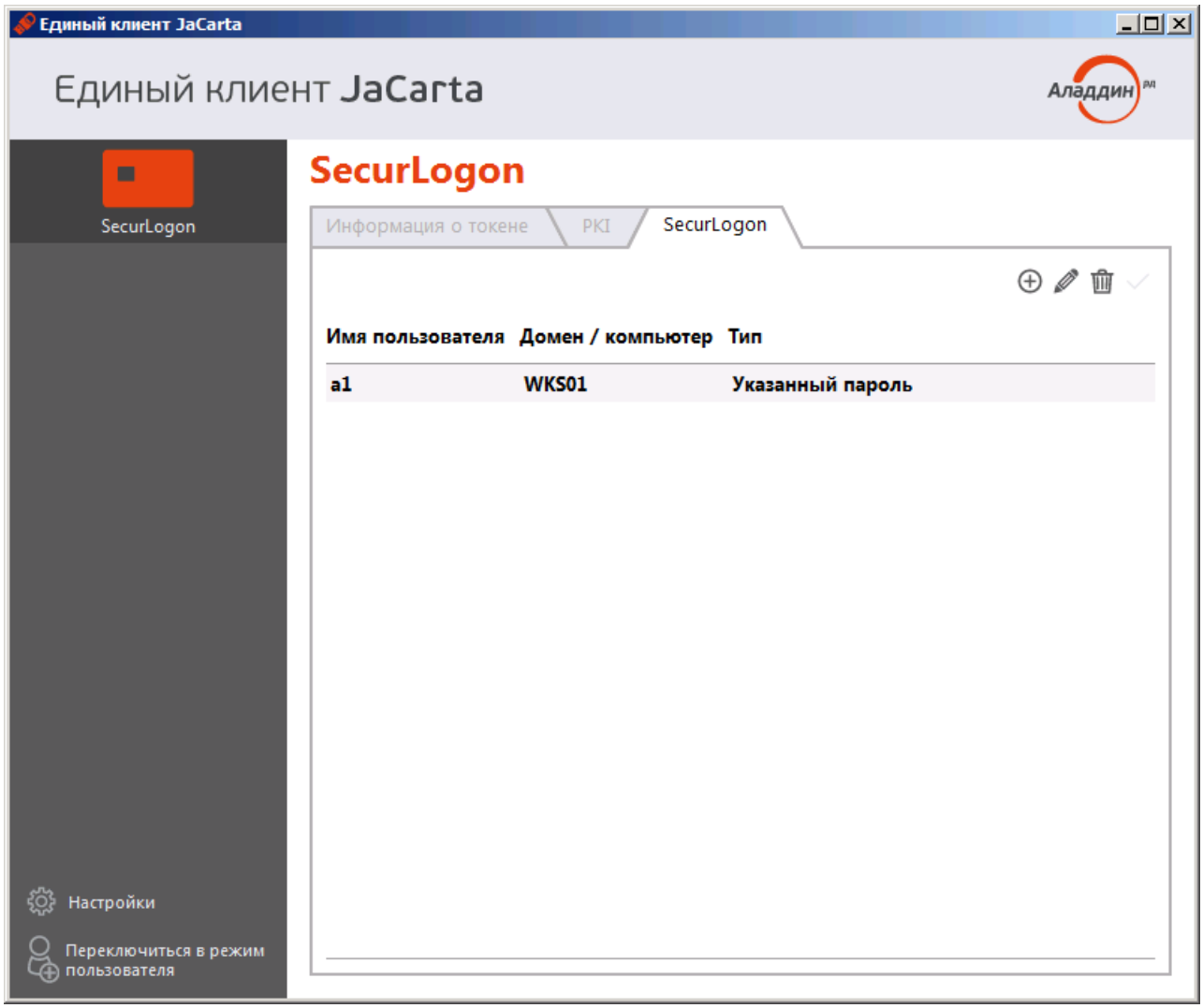

Рис. 12 – В памяти подсоединённого электронного ключа содержится профиль SecurLogon

5.2. Установка профиля по умолчанию

SecurLogon позволяет установить профиль по умолчанию – т.е. такой профиль будет отображаться первым при входе в систему. Чтобы установить профиль по умолчанию, выполните следующие действия.

1. Подсоедините электронный ключ, на котором вы хотите создать профиль SecurLogon, к компьютеру.
2. Запустите Единый Клиент JaCarta, переключитесь в режим администратора и перейдите на вкладку **SecurLogon**.
3. Левой кнопкой мыши выберите профиль, который вы хотите сделать профилем по умолчанию.
4. В основной части интерфейса нажмите на значке ✓ или нажмите правой кнопкой мыши на нужной учётной записи и из контекстного меню выберите **Установить по умолчанию**.

Отобразится следующее окно.

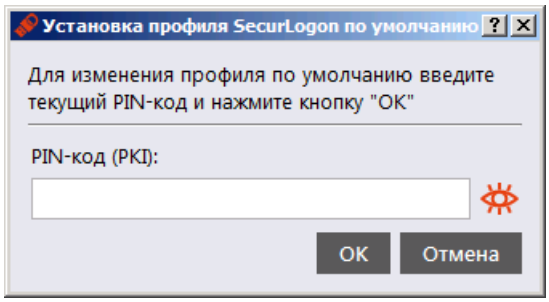

Рис. 13 – Установка профиля SecurLogon по умолчанию

5. Введите PIN-код электронного ключа и нажмите **OK**.

5.3. Редактирование существующего профиля SecurLogon

Чтобы отредактировать профиль SecurLogon, выполните следующие действия.

1. Подсоедините электронный ключ с записанным профилем SecurLogon к компьютеру.
2. Запустите Единый Клиент JaCarta, переключитесь в режим администратора и перейдите на вкладку **SecurLogon**.
3. Нажатием левой кнопки мыши в центральной части окна выберите профиль, который необходимо изменить.
4. В основной части интерфейса нажмите на значке ✎ или нажмите правой кнопкой мыши на нужном профиле и выберите **Редактировать**.

Отобразится окно редактирования профиля SecurLogon.

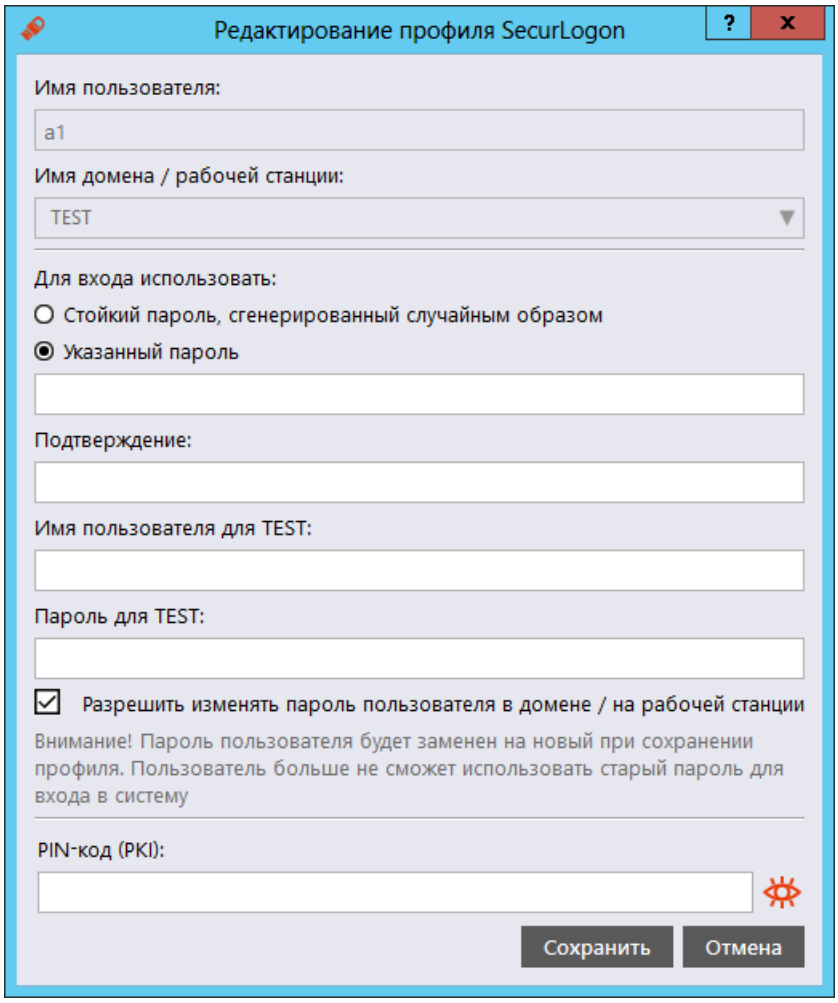

Рис. 14 – Окно редактирования профиля SecurLogon

5. Выполните необходимые настройки, аналогично созданию профиля SecurLogon (см. «Создание профиля SecurLogon»), после чего нажмите **Сохранить**.

5.4. Удаление профиля SecurLogon

Чтобы удалить профиль SecurLogon из памяти электронного ключа, выполните следующие действия.

1. Подсоедините электронный ключ с записанным профилем SecurLogon к компьютеру.
2. Запустите Единый Клиент JaCarta, переключитесь в режим администратора и перейдите на вкладку **SecurLogon**.
3. Нажатием левой кнопки мыши выберите профиль, который необходимо удалить.
4. В основной части интерфейса нажмите на значке 🗑 или нажмите правой кнопкой мыши на нужном профиле и выберите **Удалить**.
   Дальнейшая процедура различается в зависимости от типа пароля, установленного для профиля SecurLogon (вводимый вручную или случайный):

- см. пункт «Если пароль для профиля SecurLogon был задан вручную»;

- см. пункт «Если для профиля SecurLogon использовался случайный пароль»;

ЕСЛИ ПАРОЛЬ ДЛЯ ПРОФИЛЯ SECURLOGON БЫЛ ЗАДАН ВРУЧНУЮ

Отобразится следующее окно.

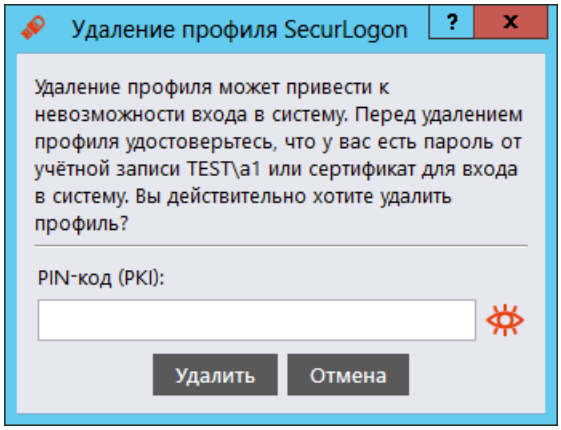

Рис. 15 – Подтверждение удаления профиля SecurLogon

В поле **PIN-код** введите текущий PIN-код электронного ключа, после чего нажмите **Удалить**.

ЕСЛИ ДЛЯ ПРОФИЛЯ SECURLOGON ИСПОЛЬЗОВАЛСЯ СЛУЧАЙНЫЙ ПАРОЛЬ

Отобразится следующее окно.

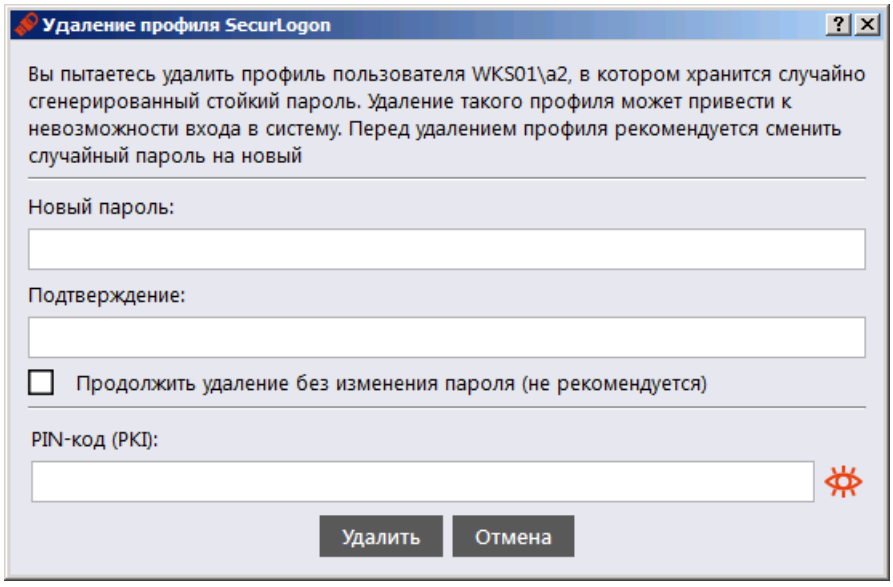

Рис. 16 – Форма удаления профиля SecurLogon со случайным паролем

Введите необходимые данные, руководствуясь табл. 4 ниже, после чего нажмите **Удалить**.

Табл. 4

Форма удаления профиля SecurLogon со случайным паролем

Настройка	Описание
Новый пароль	В соответствующих полях введите значение пароля учётной записи пользователя, который будет назначен после удаления профиля SecurLogon, и подтверждение соответственно. Эти поля скрыты, если установлен флажок Продолжить удаление без изменения пароля.
Подтверждение	
Продолжить удаление без изменения пароля	Установите э тот флажок, если хотите, чтобы для доступа к учётной записи пользователя сохранился случайный пароль, сгенерированный при создании профиля SecurLogon. Не рекомендуется включать эту настройку, т.к. в этом случае пароль для доступа к учётной записи пользователя останется неизвестным.
PIN-код	Введите PIN-код электронного ключа.

Лист регистрации изменений

Версия документа	Изменения
1.0	Исходная версия документа

Телефон: +7 (495) 223-00-01
Факс: +7 (495) 646-64-40
aladdin@aladdin-rd.ru
www.aladdin-rd.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (бессрочно), № 2874 от 18.05.12
Лицензия ФСБ России № 12632 Н от 20.12.12
Microsoft Silver OEM Hardware Partner, Oracle Gold Partner, Apple Developer
Сертификат соответствия СМК ГОСТ Р ИСО 9001-2011