



УТВЕРЖДЕН

RU.АЛДЕ.03.16.001-04 32 01-1-ЛУ

JaCarta Management System v3.7

Руководство администратора. Часть 3

Установка и настройка сервера аутентификации
(JAS)

RU.АЛДЕ.03.16.001-04 32 01-3

Версия продукта	3.7.1
Версия документа	1.00
Статус	Публичный
Дата	14 декабря 2022 г.
Листов	157

2023

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

Оглавление

1.	О документе	5
1.1	Назначение документа	5
1.2	На кого ориентирован данный документ	5
1.3	Соглашения по оформлению	5
1.4	Обозначения и сокращения	6
1.5	Авторские права, товарные знаки, ограничения	8
1.6	Лицензионное соглашение	9
2.	Введение	12
3.	Системные требования	12
3.1	Системные требования для установки серверного компонента JAS	12
3.2	Системные требования для установки модулей расширения для служб Windows	13
3.3	Поддерживаемые модели OTP-токенов	14
4.	Пакеты установки	14
5.	Лицензирование сервера аутентификации JAS	15
6.	Предварительные действия	15
7.	Установка и первичная настройка	16
7.1	Установка	16
7.2	Подключение JAS к базе данных JMS	19
7.3	Задание пароля шифрования	19
7.4	Настройка сетевых программных интерфейсов JAS Server	19
8.	Настройка в JAS протоколов SSL/TLS	23
8.1	Настройка SSL/TLS в операционной системе	24
8.2	Настройка SSL-соединения на стороне сервера JAS	24
8.3	Настройка SSL/TLS на стороне клиентов	24
8.4	Настройка SSL/TLS на стороне компонента JOL	25
8.5	Настройка SSL/TLS для работы с Microsoft SQL Server	26
9.	Другие настройки JAS	26
9.1	Настройка параметров ведения журнала событий	26
9.2	Изменение языка графического интерфейса	27
10.	Обновление JAS	27
11.	Сервер JAS	28
11.1	Меню быстрого доступа в области уведомлений	28
12.	Окно управления ПО Сервер JAS	28
12.1	Статус	30

12.2	Настройка	31
12.2.1	Мастер подключения к базе данных JMS	31
12.2.2	Настройки сервиса	38
12.2.3	Прикладные настройки сервера	40
12.3	Безопасность	58
12.3.1	Общий вид вкладки Безопасность	58
12.3.2	Настройки использования SSL/TLS	58
12.3.3	Настройки безопасности	62
12.4	Лицензии (проверка/просмотр лицензии на использование продукта JAS)	64
13.	Установка и настройка JAS-плагина для NPS	65
13.1	Подготовка сервера NPS	65
13.1.1	Настройка политики запросов на подключение	65
13.1.2	Настройка параметров RADIUS-клиента	70
13.2	Установка JAS-плагина для NPS	75
13.3	Настройка JAS-плагина для NPS	78
13.3.1	Работа с конфигуратором JAS-плагина для NPS	78
13.3.2	Выбор корректной кодировки диалогового запроса ReplyMessage при интеграции JAS со сторонними продуктами	87
13.4	Проверка работы JAS-плагина для NPS	88
13.4.1	Одношаговая процедура ввода второго фактора аутентификации	88
13.4.2	Двухшаговая процедура аутентификации	90
13.4.3	Двухшаговая процедура аутентификации с выбором типа второго фактора	94
14.	Установка и настройка JAS-плагина для AD FS	98
14.1	Подготовка к установке JAS-плагина для AD FS	98
14.2	Установка JAS-плагина для AD FS	98
14.3	Настройка JAS-плагина для AD FS	103
14.3.1	Работа с конфигуратором JAS-плагина для AD FS	103
14.4	Проверка работы JAS-плагина для AD FS	112
15.	Установка и настройка JAS-плагина для MS RDG	115
15.1	Подготовка к установке JAS-плагина для MS RDG	115
15.2	Установка JAS-плагина для MS RDG	116
15.3	Настройка JAS-плагина для MS RDG	117
15.3.1	Работа с конфигуратором JAS-плагина для MS RDG	118
15.4	Проверка работы JAS-плагина для MS RDG	122
15.4.1	Типовые сообщения об ошибках при аутентификации с помощью JAS-плагина для MS RDG	125
16.	Установка и настройка отказоустойчивого кластера JAS	126
16.1	Системные требования JAS-плагина для службы кластеров	126
16.2	Подготовка к установке JAS-плагина для службы кластеров	126
16.3	Установка JAS-плагина для службы кластеров	127

16.4	Настройка JAS-плагина для службы кластеров	130
16.5	Настройка отказоустойчивого кластера JAS	132
16.6	Проверка работы отказоустойчивого кластера JAS	134
17.	Двухфакторная аутентификация для входа в Windows (JOL)	134
17.1	Установка JOL	135
17.2	Настройки JOL и порядок их применения	136
17.3	Групповая политика JOL (административный шаблон GPO)	141
17.4	Локальная групповая политика JOL	142
17.5	Порядок аутентификации в Windows с помощью JOL	142
18.	Установка и настройка Сервиса Aladdin 2FA (A2FA)	144
18.1	Дистрибутив	144
18.2	Системные требования	144
18.3	Порядок установки Сервиса A2FA	144
18.4	Порядок подключения Сервиса A2FA к серверу JAS	145
18.5	Настройка выпуска OTP- и PUSH-токенов на базе платформы A2FA	145
18.6	Порядок работы с OTP- и PUSH-токенами в рамках платформы A2FA	145
19.	Технические сведения	145
19.1	Оптимизация производительности JAS	145
19.2	Рекомендации по развёртыванию JAS	146
19.2.1	Критерии выбора конфигурации с сервером RADIUS	146
19.2.2	Рекомендуемые варианты конфигурации	146
19.2.3	Требования к OTP-клиентам, использующим интерфейсы WCF или REST	147
19.3	Описание интерфейсов REST и WCF	149
19.3.1	REST	149
19.3.2	WCF	151
20.	Установка плагина «Крипто БД» на сервер JAS	152
	Контакты, техническая поддержка	154
	Список литературы	155
	Полезные web-ресурсы	155
	Регистрация изменений	156

1. О документе

1.1 Назначение документа

Настоящий документ является частью руководства администратора JMS и представляет собой описание операций по установке и настройке компонента JAS (сервер аутентификации JaCarta Authentication Server).





1.2 На кого ориентирован данный документ

Документ предназначен для администраторов корпоративных информационных систем, обеспечивающих интеграцию компонента JAS с информационной инфраструктурой организации.

1.3 Соглашения по оформлению

В данном документе для представления ссылок, терминов и наименований, примеров кода программ используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице 1.

Табл. 1 – Элементы оформления

Выделение	Используется для выделения наименований полей, кнопок, секций, вкладок экранных форм
<code>file.exe</code>	Используется для выделения имен файлов, каталогов, текстов программ
[1]	Ссылка на пункт в списке литературы (приведен в конце документа)
Гиперссылка	Используется для выделения внешних ссылок
Ссылка, с. 5	Используется для выделения перекрестных ссылок
	Важная информация
	Ссылка, примечание, заметка
	Совет
	Рекомендация

1.4 Обозначения и сокращения

Табл. 2– Обозначения и сокращения

Аутентификатор (аутентификатор с поддержкой OTP)	Средство аутентификации пользователя; информационный объект, являющийся единицей учета на сервере JAS. В JAS принимаются к учету следующие виды аутентификаторов: <ul style="list-style-type: none"> • OTP-токен • PUSH-токен • Messaging-токен • U2F-аутентификатор
БД	База данных
ПО	Программное обеспечение
ПО Сервер JAS	Также <i>серверный агент</i> , служит для оперативного управления (логический запуск/остановка/приостановка/перезапуск) бизнес-логики JAS, реализуемой серверной службой Aladdin JAS Engine Service – default
ПО Консоль управления JMS (JMS Admin)	Приложение административной консоли JMS, позволяет осуществлять операции, связанные с управлением жизненным циклом OTP-, PUSH- и U2F-аутентификаторов
AD	Active Directory – служба каталогов Microsoft
AD FS	Active Directory Federation Services – служба федерации Active Directory
FC	Microsoft Failover Cluster – компонент «отказоустойчивая кластеризация» (при установке в Windows разворачивает службу кластеров)
JAS	JaCarta Authentication Server
JAS-плагины	Модули расширения для служб Windows (NPS, AD FS, FC, MS RDG, Credential Provider – JOL), обеспечивающие интеграцию с сервером JAS
Messaging-токен	Аутентификатор, позволяющий проводить аутентификацию посредством отправки OTP посредством службы SMS оператора мобильной связи
NPS	Network Policy Server – служба политики сети и доступа Microsoft Windows
OTP	One-Time Password – одноразовый пароль
OTP-токен	Электронный ключ – аппаратная реализация средства аутентификации с поддержкой OTP. Один из видов аутентификаторов, поддерживаемых сервером JAS
Программный OTP-токен	Мобильное приложение, такое как Aladdin 2FA (A2FA) компании Аладдин (или аналогичные приложения других поставщиков), предназначенное для генерации одноразовых паролей для доступа пользователей к различным ресурсам. В среде JMS программные OTP-аутентификаторы (включая технологию PUSH) классифицируются как OTP-токены
PUSH-токен	Разновидность Программного OTP-токена , реализованная в мобильном приложении Aladdin 2FA (A2FA) компании Аладдин, обеспечивающая

аутентификацию пользователя с использованием дополнительного фактора OTP без необходимости введения одноразового пароля пользователем

REST	Метод сетевого взаимодействия приложений, при котором вызов представляет собой обычный HTTP-запрос
JAS Server	Серверный компонент JAS. Включает в себя сервер бизнес-логики JAS, реализованный в виде службы Windows, и серверный агент (ПО <i>Сервер JAS</i>)
U2F	Universal 2nd Factor – открытый стандарт протокола двухфакторной аутентификации. Разрабатывается альянсом FIDO (FIDO Alliance)
U2F-аутентификатор	Аутентификатор, представляющий собой регистрационную информацию, хранимую на сервере JAS используемую для аутентификации пользователя по протоколу U2F альянса FIDO
WCF	Программный фреймворк Microsoft, реализующий сетевое взаимодействие приложений с использованием различных протоколов

1.5 Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации.

Обладателем исключительных авторских и имущественных прав является АО «Аладдин Р. Д.».

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на АО «Аладдин Р. Д.» обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является АО «Аладдин Р. Д.».

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО «Аладдин Р. Д.» без предварительного уведомления.

АО «Аладдин Р. Д.» не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

АО «Аладдин Р. Д.» не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование

программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе АО «Аладдин Р. Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

АО «Аладдин Р. Д.» НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р. Д.» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

1.6 Лицензионное соглашение

ВАЖНО:

ПОЖАЛУЙСТА, ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ, ПРЕЖДЕ ЧЕМ ОТКРЫТЬ ПАКЕТ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ И/ИЛИ ИСПОЛЬЗОВАТЬ ЕГО СОДЕРЖИМОЕ И/ИЛИ ПРЕЖДЕ, ЧЕМ ЗАГРУЖАТЬ ИЛИ УСТАНОВЛИВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

ВСЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ НАСТОЯЩЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (включая без ограничений библиотеки, утилиты, файлы для скачивания с Web-сайта, CD-ROM, Руководства, описания и др. документацию), далее «ПО», «Продукт»), ПРЕДОСТАВЛЯЕМЫЕ КОМПАНИЕЙ АО «Аладдин Р.Д.» (или любым дочерним предприятием – каждое из них упоминаемое как «КОМПАНИЯ») ПОДЧИНЯЮТСЯ И БУДУТ ПОДЧИНЯТЬСЯ УСЛОВИЯМ, ОГОВОРЕННЫМ В ДАННОМ СОГЛАШЕНИИ. ОТКРЫВАЯ ПАКЕТ, СОДЕРЖАЩИЙ ПРОДУКТ И/ИЛИ ЗАГРУЖАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ как определено далее по тексту) И/ИЛИ УСТАНОВЛИВАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ВАШ КОМПЬЮТЕР И/ИЛИ ИСПОЛЬЗУЯ ДАННЫЙ ПРОДУКТ, ВЫ ПРИНИМАЕТЕ ДАННОЕ СОГЛАШЕНИЕ И СОГЛАШАЕТЕСЬ С ЕГО УСЛОВИЯМИ.

ЕСЛИ ВЫ НЕ СОГЛАСНЫ С ДАННЫМ СОГЛАШЕНИЕМ, НЕ ОТКРЫВАЙТЕ ЭТОТ ПАКЕТ И/ИЛИ НЕ ЗАГРУЖАЙТЕ И/ИЛИ НЕ УСТАНОВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НЕЗАМЕДЛИТЕЛЬНО (не позднее 7 дней с даты получения этого пакета) ВЕРНИТЕ ЭТОТ ПРОДУКТ В АЛАДДИН Р.Д., СОТРИТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВСЕ ЕГО ЧАСТИ В СВОЕМ КОМПЬЮТЕРЕ И НЕ ИСПОЛЬЗУЙТЕ ЕГО НИКОИМ ОБРАЗОМ.

Лицензионное соглашение на использование программного обеспечения. Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) - конечным пользователем (далее "Пользователь") и компанией АО «Аладдин Р.Д.» (далее «компания Аладдин Р.Д.», «Правообладатель») относительно предоставления неисключительного права на использование настоящего программного обеспечения - комплекса программ для ЭВМ, и документации (печатные материалы, носители и файлы с информацией), являющихся неотъемлемой частью ПО, включая все дальнейшие усовершенствования.

Лицензионный договор считается заключенным с момента начала использования Вами ПО любым способом или с момента, когда Вы примете все условия настоящего Лицензионного договора в процессе установки ПО. Лицензионный договор сохраняет свою силу в течение всего срока действия исключительного права на ПО, если только иное не оговорено в Лицензионном договоре или в отдельном письменном договоре между Вами и компанией Аладдин Р.Д. Срок действия Лицензионного договора также может зависеть от объема Вашей Лицензии, описанного в данном Лицензионном договоре.

Права на ПО охраняются действующими законодательством и международными соглашениями. Вы подтверждаете свое согласие с тем, что Лицензионный договор имеет такую же юридическую силу, как и любой другой письменный договор, заключенный Вами. В случае нарушения Лицензионного договора Вы можете быть привлечены в качестве ответчика.

1. Предмет Соглашения

1.1. Предметом настоящего Соглашения является передача Правообладателем конечному Пользователю неисключительного права на использование ПО. ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Все условия, оговоренные далее, относятся как к ПО в целом, так и ко всем его компонентам в отдельности. Данное соглашение не передает Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничего в данном Соглашении не подтверждает отказ компании Аладдин Р.Д. от прав на интеллектуальную собственность по какому бы то ни было законодательству.

1.2. Компания Аладдин Р.Д. сохраняет за собой все права, явным образом не предоставленные Вам настоящим Лицензионным договором. Настоящий Лицензионный договор не предоставляет Вам никаких прав на товарные знаки Компании Аладдин Р.Д.

1.3. В случае, если Вы являетесь физическим лицом, то территория, на которой допускается использование ПО, включает в себя весь мир. В случае, если Вы являетесь юридическим лицом (обособленным подразделением юридического лица), то территория на которой допускается приобретение ПО, ограничена страной регистрации юридического лица (обособленного подразделения юридического лица), если только иное не оговорено в отдельном письменном договоре между Вами и Компанией Аладдин Р.Д.

2. Имущественные права

- 2.1. Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как "Программное обеспечение"), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остается исключительной собственностью компании Аладдин Р.Д.
- 2.2. Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтвержденные или включенные в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нем, а также все права на ПО являются и будут являться собственностью исключительно компании Аладдин Р.Д.
- 2.3. Вам, конечному Пользователю, предоставляется неисключительное право на использование ПО в указанных в документации целях и при соблюдении приведенных ниже условий.

3. Условия использования

- 3.1. ПО может быть использовано только в строгом соответствии с документами, инструкциями и рекомендациями Правообладателя, относящимися к данному ПО.
- 3.2. ПО может предоставляться на нескольких носителях, в том числе с помощью сети интернет. Независимо от количества носителей, на которых Вы получили ПО, Вы имеете право использовать ПО только в объеме предоставленной Вам Лицензии.
- 3.3. После уплаты Вами соответствующего вознаграждения компания Аладдин Р.Д. настоящим предоставляет Вам, а Вы получаете индивидуально, неисключительное и ограниченное право на использование данного Программного обеспечения только в форме исполняемого кода, как описано в прилагаемой к Программному обеспечению документации и только в соответствии с условиями данного Соглашения:
 - ▶ Вы можете установить Программное обеспечение и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей документации компании Аладдин Р.Д.
 - ▶ Вы можете добавить/присоединить Программное обеспечение к программам Вашего компьютера с единственной целью, описанной в данном Соглашении.

Продукт должен использоваться и обслуживаться строго в соответствии с описаниями и инструкциями компании Аладдин Р.Д., приведенными в данном и других документах компании Аладдин Р.Д.

- 3.4. За исключением указанных выше разрешений, Вы обязуетесь:
 - 3.4.1. Не использовать и не выдавать сублицензии на данное Программное обеспечение и любую другую Продукцию компании Аладдин Р.Д., за исключением явных разрешений в данном Соглашении и в Руководстве по интеграции.
 - 3.4.2. Не продавать, не выдавать лицензий или сублицензий, не сдавать в аренду или в прокат, не передавать, не переводить на другие языки, не закладывать, не разделять Ваши права в рамках данного Соглашения с кем-либо или кому-либо еще.
 - 3.4.3. Не модифицировать (в том числе не вносить в ПО изменения в целях его функционирования на технических средствах Конечного пользователя), не демонтировать, не декомпилировать или дизассемблировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения.

- 3.4.4. Не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть.
- 3.4.5. Не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо еще использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.
- 3.4.6. Не пытаться обойти технические ограничения в Программе;
- 3.4.7. Не использовать Программу для оказания услуг на платной и бесплатной основе;
- 3.4.8. Не создавать условия для использования ПО лицами, не имеющими прав на использование ПО, в том числе работающими с Вами в одной многопользовательской системе или сети Интернет.
- 3.4.9. Вы не вправе удалять, изменять или делать малозаметными любые уведомления об авторских правах, правах на товарные знаки или патенты, которые указаны на/в ПО.
- 3.4.10. Вы обязуетесь соблюдать права третьих лиц, в том числе авторские права на объекты интеллектуальной собственности.
- 3.5. Компания Аладдин Р.Д. не несет обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов данного Программного обеспечения.
- Нелегальное использование, распространение и воспроизведение (копирование) программного обеспечения является нарушением действующего законодательства и преследуется по Закону.
- В случае нарушения настоящего Соглашения Правообладатель лишает Пользователя права на использование ПО. При этом Правообладатель полностью отказывается от своих гарантийных обязательств.

4. Ограниченная гарантия

Компания Аладдин Р.Д. гарантирует, что:

Данное Программное обеспечение с момента поставки его Вам в течение двенадцати (12) месяцев будет функционировать в полном соответствии с Руководством Пользователя (Администратора), при условии, что оно будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Правообладатель гарантирует соответствие компонентов ПО спецификациям, а также работоспособность ПО при выполнении Пользователем условий, оговоренных в документации на ПО. ПО поставляется "таким, какое оно есть". Правообладатель не гарантирует, что ПО соответствует вашим требованиям, и что все действия ПО будут выполняться безошибочно. Правообладатель не гарантирует корректную совместную работу ПО с программным обеспечением или оборудованием других производителей.

5. Отказ от гарантии

- 5.1. КОМПАНИЯ АЛАДДИН Р.Д. НЕ ГАРАНТИРУЕТ, ЧТО ЛЮБОЙ ИЗ ЕГО ПРОДУКТОВ БУДЕТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ЕГО РАБОТА БУДЕТ БЕСПЕРЕБОЙНОЙ ИЛИ БЕЗОШИБОЧНОЙ. В ОБЪЕМЕ, ПРЕДУСМОТРЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РФ, КОМПАНИЯ АЛАДДИН Р.Д. ОТКРЫТО ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ГАРАНТИЙ, НЕ ОГОВОРЕННЫХ ЗДЕСЬ, ОТ ВСЕХ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИЮ ТОВАРНОГО ВИДА И ПРИГОДНОСТИ ИСПОЛЬЗОВАНИЯ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ.
- НИ ОДИН ИЗ ДИЛЕРОВ, ДИСТРИБЬЮТОРОВ, ПРОДАВЦОВ, АГЕНТОВ ИЛИ СОТРУДНИКОВ КОМПАНИИ АЛАДДИН Р.Д. НЕ УПОЛНОМОЧЕН ПРОИЗВОДИТЬ МОДИФИКАЦИИ, РАСШИРЕНИЯ ИЛИ ДОПОЛНЕНИЯ К ДАННОЙ ГАРАНТИИ.
- 5.2. Если Вы произвели какие-либо модификации Программного обеспечения или любой из частей данного Продукта во время гарантийного периода, то гарантия, упомянутая выше, будет немедленно прекращена.
- 5.3. Гарантия недействительна, если Продукт используется на или в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в документации, или используется на компьютере с любым установленным нелегальным программным обеспечением.
- 5.4. ПО и обновления предоставляются такими, каковы они есть, и Компания Аладдин Р.Д. не предоставляет на них никаких гарантий.

Компания Аладдин Р.Д. не гарантирует и не может гарантировать работоспособность ПО и результаты, которые Вы можете получить, используя ПО.

- 5.5. За исключением гарантий и условий, которые не могут быть исключены или ограничены в соответствии с применимым законодательством, Компания Аладдин Р.Д. не предоставляет Вам никаких гарантий (в том числе явно выраженных или подразумеваемых в статутном или общем праве или обычаями делового оборота) ни на что, включая, без ограничения, гарантии о не нарушении прав третьих лиц, товарной пригодности, интегрируемости, удовлетворительного качества и годности к использованию ПО. Все риски, связанные с качеством работы и работоспособностью ПО, возлагаются на Вас.
- 5.6. Компания Аладдин Р.Д. не предоставляет никаких гарантий относительно программами для ЭВМ других производителей, которые могут предоставляться в составе ПО.

6. Исключение косвенных убытков

Стороны признают, что Продукт по сути своей сложный и не может быть полностью лишен ошибок. КОМПАНИЯ АЛАДДИН Р.Д. НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ, ПОБОЧНЫЕ ИЛИ ПОТЕНЦИАЛЬНЫЕ УБЫТКИ), ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЕННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ КАКОГО-ЛИБО ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОЙ КОМПОНЕНТЫ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АЛАДДИН Р.Д. ПИСЬМЕННО УВЕДОМЛЕН О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

7. Ограничение ответственности

В СЛУЧАЕ ЕСЛИ, НЕСМОТЯ НА УСЛОВИЯ ДАННОГО СОГЛАШЕНИЯ, КОМПАНИЯ АЛАДДИН Р.Д. ПРИЗНАНА ОТВЕТСТВЕННОЙ ЗА УБЫТКИ НА ОСНОВАНИИ КАКИХ-ЛИБО ДЕФЕКТОВ ИЛИ НЕСООТВЕТСТВИЯ ЕГО ПРОДУКТОВ, ПОЛНАЯ ОТВЕТСТВЕННОСТЬ ЗА КАЖДУЮ ЕДИНИЦУ ДЕФЕКТНЫХ ПРОДУКТОВ НЕ БУДЕТ ПРЕВЫШАТЬ СУММУ, ВЫПЛАЧЕННУЮ КОМПАНИИ АЛАДДИН Р.Д. ЗА ЭТИ ДЕФЕКТНЫЕ ПРОДУКТЫ.

Компания Аладдин Р.Д. ни при каких обстоятельствах не несет перед Вами никакой ответственности за убытки, вынужденные перерывы в деловой активности, потерю деловых либо иных данных или информации, претензии или расходы, реальный ущерб, а также упущенную выгоду и утраченные сбережения, вызванные использованием или связанными с использованием ПО, а также за убытки, вызванные возможными ошибками и опечатками в ПО и/или в документации, даже если Компании Аладдин Р.Д. стало известно о возможности таких убытков, потерь, претензий или расходов, равно как и за любые претензии со стороны третьих лиц. Вышеперечисленные ограничения и исключения действуют в той степени, насколько это разрешено применимым законодательством. Единственная ответственность Компании Аладдин Р.Д. по настоящему Лицензионному договору ограничивается суммой, которую Вы уплатили за ПО.

8. Прекращение действия

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- (i) Лицензия, предоставленная Вам данным Соглашением, прекращает свое действие, и Вы после ее прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;
- (ii) Вы незамедлительно вернете в компанию Аладдин Р.Д. все имущество, в котором используются права Аладдин Р.Д. на интеллектуальную собственность и все копии такового и/или сотрете/удалите любую информацию, содержащуюся в них в электронном виде. Разделы 1, 3, 6-11 будут продолжать действовать даже в случае прекращения действия настоящего Соглашения.

9. Срок действия Договора

- 9.1. Если иное не оговорено в настоящем Лицензионном договоре либо в отдельном письменном договоре между Вами и Компанией Аладдин Р.Д., настоящий Лицензионный договор действует в течение всего срока действия исключительного права на ПО.
- 9.2. В случае нарушения вами условий настоящего Соглашения или неспособности далее выполнять его условия вы обязуетесь уничтожить все копии ПО (включая архивные, файлы с информацией, носители, печатные материалы) или вернуть все относящиеся к ПО материалы организации, в которой вы приобрели ПО. После этого Соглашение прекращает свое действие.
- 9.3. Без ущерба для каких-либо других прав Компания Аладдин Р.Д. имеет право в одностороннем порядке расторгнуть настоящий Лицензионный договор при несоблюдении Вами его условий и ограничений. При прекращении действия настоящего Лицензионного договора Вы обязаны уничтожить все имеющиеся у Вас копии ПО (включая архивные, файлы с информацией, носители, печатные материалы), все компоненты ПО, а также удалить ПО и вернуть все относящиеся к ПО материалы организации, в которой вы приобрели ПО.
- 9.4. Вы можете расторгнуть настоящий Лицензионный договор удалив ПО и уничтожив все копии ПО, все компоненты ПО и сопровождающую его документацию. Такое расторжение не освобождает Вас от обязательств оплатить ПО.

10. Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законами Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Применение Конвенции Организации Объединенных Наций о Договорах международной купли-продажи товаров (the United Nations Convention of Contracts for the International Sale of Goods) однозначно исключается. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

11. Государственное регулирование и экспортный контроль

Приобретая и/или начиная использовать Продукт, Вы обязуетесь соблюдать все применимые международные и национальные законы, которые распространяются на продукты, подлежащие экспортному контролю. Настоящее ПО не должно экспортироваться или реэкспортироваться в нарушение экспортных ограничений, имеющихся в законодательстве страны, в которой приобретено или получено ПО. Вы также подтверждаете, что применимое законодательство не запрещает Вам приобретать или получать ПО.

12. Программное обеспечение третьих сторон

Если Продукт содержит в себе любое программное обеспечение, предоставленное какой-либо третьей стороной, такое программное обеспечение третьей стороны предоставляется "как есть" без какой-либо гарантии, и разделы 2, 3, 6, 8, 9-12 настоящего Соглашения применяются ко всем таким поставщикам программного обеспечения и к поставляемому ими программному обеспечению, как если бы это были Аладдин Р.Д. и Продукт соответственно.

13. Разное

- 13.1. Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только

посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

- 13.2. Все права на материалы, не содержащиеся в ПО, но доступные посредством использования ПО, принадлежат своим законным владельцам и охраняются действующим законодательством об авторском праве и международными соглашениями. Настоящий Лицензионный договор не предоставляет Вам никаких прав на использование такой интеллектуальной собственности.
- 13.3. ПО содержит коммерческую тайну и иную конфиденциальную информацию, принадлежащую Компании Аладдин Р.Д. и третьим лицам, которая охраняется действующим законодательством Российской Федерации, международными соглашениями и законодательством страны приобретения и/или использования ПО.
- 13.4. Вы соглашаетесь на добровольную передачу Компании Аладдин Р.Д. в процессе использования и регистрации ПО своих персональных данных и выражаете свое согласие на сбор, обработку, использование своих персональных данных в соответствии с применимым законодательством, на условиях обеспечения конфиденциальности. Предоставленные Вами персональные данные будут храниться и использоваться только внутри Компании Аладдин Р.Д. и ее дочерних компаний и не будут предоставлены третьим лицам, за исключением случаев, предусмотренных применимым законодательством.
- 13.5. В случае предъявления любых претензий или исков, связанных с использованием Вами ПО Вы обязуетесь сообщить Компании Аладдин Р.Д. о таких фактах в течение трех (3) дней с момента, когда Вам стало известно об их возникновении. Вы обязуетесь совершить необходимые действия для предоставления Компании Аладдин Р.Д. возможности участвовать в рассмотрении таких претензий или исков, а также предоставлять необходимую информацию для урегулирования соответствующих претензий и/или исков в течение семи (7) дней с даты получения запроса от Компании Аладдин Р.Д.
- 13.6. Вознаграждением по настоящему Лицензионному договору признается стоимость Лицензии на ПО, установленная Компанией Аладдин Р.Д. или Партнером Компании Аладдин Р.Д., которая, подлежит уплате в соответствии с определяемым Компанией Аладдин Р.Д. или Партнером Компании Аладдин Р.Д. порядком. Вознаграждение также может быть включено в стоимость приобретенного Вами оборудования или в стоимость полной версии ПО. В случае если Вы являетесь физическим лицом, настоящий Лицензионный договор может быть безвозмездным.
- 13.7. В случае если какая-либо часть настоящего Лицензионного договора будет признана утратившей юридическую силу (недействительной) и не подлежащей исполнению, остальные части Лицензионного договора сохраняют свою юридическую силу и подлежат исполнению.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

2. Введение

JaCarta Authentication Server (JAS) – программное обеспечение, предоставляющее сервис дополнительного фактора аутентификации (2FA – Two-Factor Authentication) за счет использования таких аутентификаторов, как аппаратные и программные OTP-токены (включая PUSH- и Messaging-токены), а также U2F-аутентификаторы. ПО JAS является составной частью ПО JMS (JaCarta Management System). Для получения доступа к функциональности JAS необходимо приобрести соответствующую лицензию (подробнее см. раздел «Версии поставки продукта и лицензионные опции» в руководстве по установке и настройке JMS [2]).

Сервер JAS включает в себя *сервер бизнес-логики JAS* в виде службы Windows и *серверный агент* – ПО Сервер JAS.

Все операции, связанные с управлением жизненным циклом OTP-, PUSH- и U2F-аутентификаторов, производятся из консоли управления JMS (см. руководство администратора по функциям управления JMS [3]).

В поставку JAS также включен следующий набор JAS-плагинов (модулей расширения служб Windows для интеграции с сервером JAS):

- для сервера политики сети (Network Policy Sever – NPS). Этот плагин позволяет использовать одноразовые пароли для аутентификации пользователей в приложениях, использующих протокол RADIUS;
- для службы федерации Active Directory (AD Federation Services – AD FS) из состава ОС Windows. Данный плагин обеспечивает интеграцию службы AD FS с сервером JAS;
- для службы кластеров (компонента ОС Windows «Отказоустойчивая кластеризация»; Failover Clustering – FC). Данный плагин позволяет развертывать отказоустойчивый кластер из двух экземпляров сервера JAS на основе службы кластеров Windows.

JAS обеспечивает поддержку двух спецификаций генерации одноразовых паролей (OTP):

- RFC 4226 (или **НОТР**) – генерация одноразового пароля, основанная на HMAC;
- RFC 6238 (или **ТОТР**) – усовершенствованный алгоритм НОТР с использованием меток времени.

В JAS реализована поддержка программных OTP-аутентификаторов, таких как мобильное приложение Aladdin 2FA компании Аладдин (или аналогичные приложения других поставщиков). Программный OTP-аутентификатор представляет собой мобильное приложение, предназначенное для генерации одноразовых паролей для доступа пользователей к различным ресурсам.

3. Системные требования

3.1 Системные требования для установки серверного компонента JAS

Табл. 3 – Системные требования для установки серверного компонента JAS

Компонент Требование	Серверный компонент JAS (JAS Server)
Процессор Оперативная память Сетевая карта	Начальный уровень производительности (до 40 аутентификаций/с по протоколу RADIUS, 200 аутентификаций/с по протоколам WCF/REST): <ul style="list-style-type: none"> • процессор: Intel Core i3-3xxx (2 физических ядра), частота от 3 ГГц; • оперативная память: минимум 2 Гбайт (рекомендуемый объем – 4 Гбайт); • сетевая карта: 100 Мб/с

Компонент Требование	Серверный компонент JAS (JAS Server)
	<p>Базовый уровень производительности (до 100 аутентификаций/с по протоколу RADIUS, 500 аутентификаций/с по протоколам WCF/REST):</p> <ul style="list-style-type: none"> • процессор: Intel Core i5-3xxx (4 физических ядра), частота от 3 ГГц; • оперативная память: минимум 2 Гбайт (рекомендуемый объем – 4 Гбайт); • сетевая карта: 100 Мб/с <p>Высокий уровень производительности (более 200 аутентификаций/с по протоколу RADIUS, более 1000 аутентификаций/с по протоколам WCF/REST):</p> <ul style="list-style-type: none"> • процессор: Intel Core i7-3xxx (4 физических ядра), частота от 3 ГГц; • оперативная память: минимум 2 Гбайт (рекомендуемый объем – 4 Гбайт); • сетевая карта: 100 Мб/с (рекомендуется 1Гб/с)
Место на диске	Не менее 20 Гбайт
Операционная система	<ul style="list-style-type: none"> • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019
База данных	<ul style="list-style-type: none"> • MS SQL Server 2008 (SP1); • MS SQL Server 2008 R2; • MS SQL Server 2012; • MS SQL Server 2014; • MS SQL Server 2016; • MS SQL Server 2017; • MS SQL Server 2019. <p>(Необходимый компонент - SQL Server Database Engine)</p> <p>Поддерживаемые редакции MS SQL Server: Express, Standard, Enterprise.</p>
Дополнительное ПО	Microsoft .NET Framework 4.5 (или 4.6.2, 4.7, 4.8)
Другие требования	Установка должна осуществляться от имени учётной записи с правами администратора
	На компьютерах, на которых установлены компоненты Сервер JAS и Сервер JMS время UTC должно совпадать

Значения объема оперативной памяти приведены из расчета поддержки до 1 млн аутентификаторов с поддержкой OTP, при условии, что под управлением ОС функционирует только Сервер JAS.



Сервер JAS не следует устанавливать на контроллер домена Active Directory, т.к. это может препятствовать автоматическому запуску серверных компонентов JAS.

3.2 Системные требования для установки модулей расширения для служб Windows

Табл. 4 – Системные требования для установки модулей расширения для служб Windows

Компонент Требование	JAS-плагин для NPS	JAS-плагин для AD FS
Процессор	Intel Dual-Core 2 ГГц и выше	

Компонент Требование	JAS-плагин для NPS	JAS-плагин для AD FS
Оперативная память*	Минимум: 1 Гбайт в дополнении к объему, установленному системными требованиями NPS	Минимум: 1 Гбайт в дополнении к объему, установленному системными требованиями AD FS
Место на диске	От 10 Гбайт	От 10 Гбайт
Операционная система	<ul style="list-style-type: none"> Windows Server 2008 SP2 (32/64-битные платформы); Windows Server 2008 R2 SP1; Windows Server 2012; Windows Server 2012 R2 	Windows Server 2012 R2
Дополнительное ПО	Microsoft .NET Framework 4.5	
Другие требования	Установка должна осуществляться от имени учётной записи с правами администратора	
Установленная роль сервера	Роль Службы политики сети и доступа (NPS)	Роль Службы федерации Active Directory (AD FS)

*Значения объема оперативной памяти приведены из расчета поддержки до 1 млн аутентификаторов с поддержкой OTP при условии, что под управлением ОС функционирует только указанный компонент JAS.

3.3 Поддерживаемые модели OTP-токенов

JAS поддерживает возможность работы со следующими моделями OTP-токенов:

- мобильное приложение Aladdin 2FA компании Аладдин (обеспечивает работу программных OTP- и PUSH-токенов);
- eToken PASS;
- eToken NG OTP;
- eToken NG OTP (Java);
- JC-WebPass;
- Google Authenticator;
- «Яндекс Ключ»;
- другие OTP-токены, реализующие спецификации RFC 4226 и 6238.

4. Пакеты установки

В поставку JAS входят следующие пакеты установки (см. табл. 5 ниже).

Табл. 5 – Пакеты установки JAS

Файл	Описание
Aladdin.JAS.Server-X.X.X.XXX-x64.msi	Пакет установки серверного компонента JAS, включает в себя сервер бизнес-логики JAS и серверный агент – ПО Сервер JAS (только для 64-битных систем)

Файл	Описание
Aladdin.JAS.NPSPlugin-X.X.X.XXX-x64.msi	Пакет установки JAS-плагина для сервера NPS (только для 64-битных систем)
Aladdin.JAS.ADFSPlugin-X.X.X.XXX-x64.msi	Пакет установки JAS-плагина для службы AD FS (только для 64-битных систем)
Aladdin.JAS.FCPlugin-X.X.X.XXX-x64.msi	Пакет установки JAS-плагина для службы кластеров (только для 64-битных систем)
Aladdin.JAS.RDGPlugin-X.X.X.XXX-x64.msi	Пакет установки JAS-плагина для службы шлюза удаленных рабочих столов (только для 64-битных систем)

5. Лицензирование сервера аутентификации JAS

Установка лицензии на использование сервера JAS происходит автоматически при подключении к серверу JMS (см. раздел «Мастер подключения к базе данных JMS », с. 31).

Все параметры лицензии на использование сервера JAS (период использования, разрешенное число аутентификаторов и пр.) устанавливаются в файле лицензии базового компонента – системы JMS (см. руководство по установке и настройке JMS [2], раздел «Окно управления сервером JMS (серверный агент)» -> «Лицензии»).

6. Предварительные действия

JAS предоставляет следующие сетевые программные интерфейсы для обеспечения взаимодействия своих компонентов:

- **AdministrationService** – через этот интерфейс с сервером JAS взаимодействует сервер JMS;
- **AuthenticationService** – через этот интерфейс с сервером JAS взаимодействуют OTP-клиенты (например, JAS-плагин для NPS);
- **ControlService** – интерфейс для взаимодействия с ПО Сервер JAS (серверным агентом).

Взаимодействие по этим интерфейсам может происходить анонимно (т.е. без проверки подлинности учётной записи, от имени которой действует тот или иной компонент) либо с использованием проверки подлинности (аутентификации пользователя) Windows. В последнем случае для каждого из интерфейсов необходимо указать группу, члены которой смогут действовать через соответствующие интерфейсы.



Подробные сведения о настройке параметров взаимодействия через сетевые программные интерфейсы представлены в пункте «Настройка сетевых программных интерфейсов JAS», с. 19.

Ниже приведён пример создания двух групп Active Directory для обеспечения взаимодействия через интерфейсы **AdministrationService** и **AuthenticationService** соответственно.

1. С помощью оснастки **Active Directory – пользователи и компьютеры** создайте две глобальные группы безопасности.
2. В настоящем документе для примера будут использоваться следующие названия групп:
 - **JAS Administrators** – для **AdministrationService** (интерфейс взаимодействия с сервером JMS);
 - **JAS Clients** - для **AuthenticationService** (интерфейс для OTP-клиентов).
3. Создайте пользователя, от чьего имени OTP-клиенты (например, JAS-плагин для NPS) будут подключаться к серверу JAS через интерфейс **AuthenticationService**. В настоящем документе для примера такой пользователь будет носить имя **NPS2JAS**.



Запомните пароль пользователя **NPS2JAS** – он понадобится вам при настройке параметров JAS-плагина для NPS.

4. В группу **JAS Administrators** добавьте пользователя, от имени которого должно осуществляться подключение сервера JMS к серверу JAS (процедура «Настройка подключения к JAS» описана в руководстве по настройке и установке JMS [2]).



Примечание. Если значение **JAS Administrators** не определено, то подключение сервера JMS к серверу JAS может быть осуществлено только от имени пользователя, который устанавливал сервер JAS.

5. В группу **JAS Clients** добавьте пользователя **NPS2JAS**.

7. Установка и первичная настройка

7.1 Установка

Чтобы установить серверный компонент JAS, выполните следующие действия.

1. Запустите файл установки **Aladdin.JAS.Server-X.X.X.XXX-x64.msi** (только для 64-битных систем).
Отобразится следующее окно.

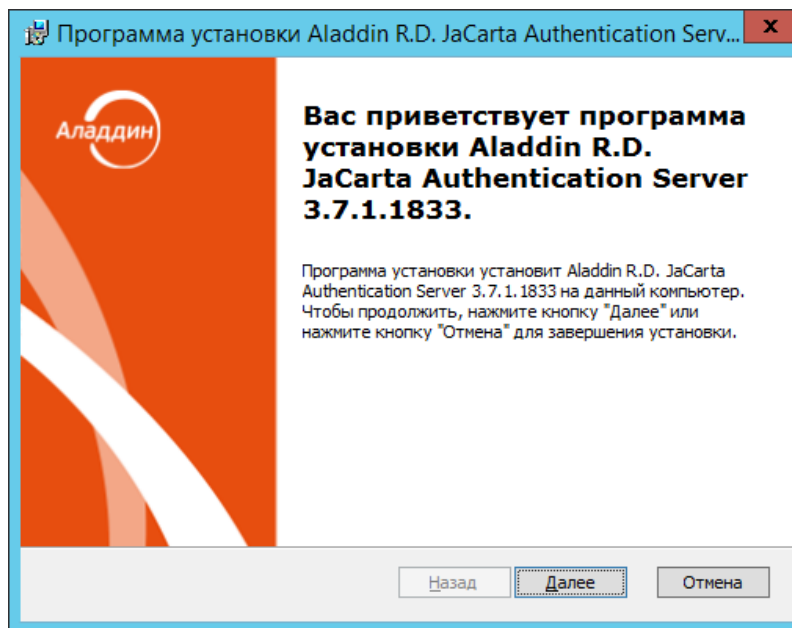


Рис. 1 – Экран приветствия мастера установки Сервер JAS

- Нажмите **Далее**.
Отобразится следующее окно.

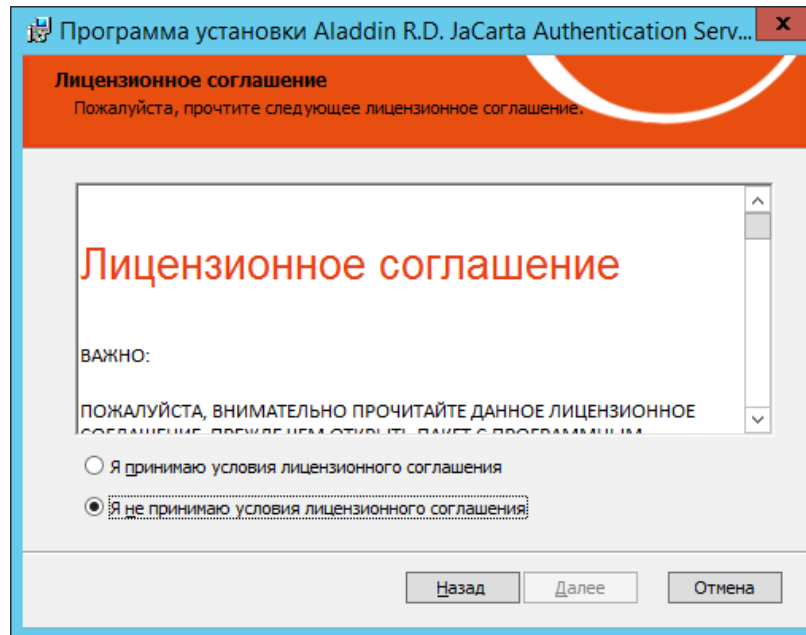


Рис. 2 – Подтверждение лицензионного соглашения

- Чтобы продолжить, выберите пункт **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.
Отобразится следующее окно.

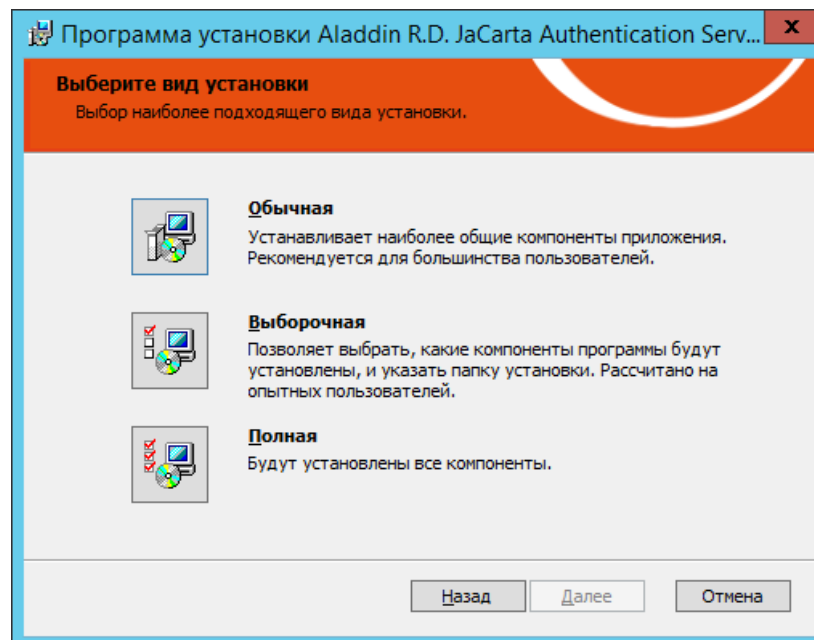


Рис. 3 – Выбор варианта установки

4. Выберите **Полная**.
Отобразится следующее окно.

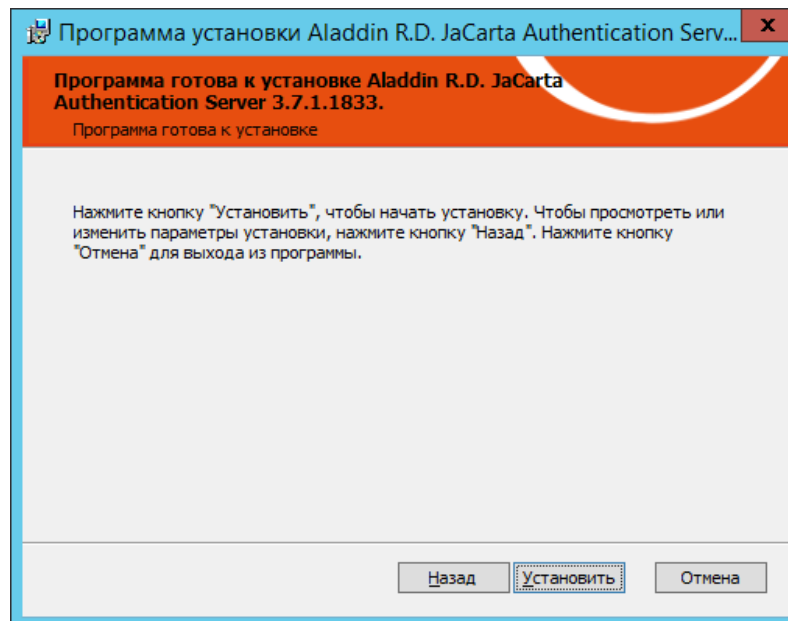


Рис. 4 – Готовность к установке

5. Нажмите **Установить**.
По завершении установки отобразится следующее окно.

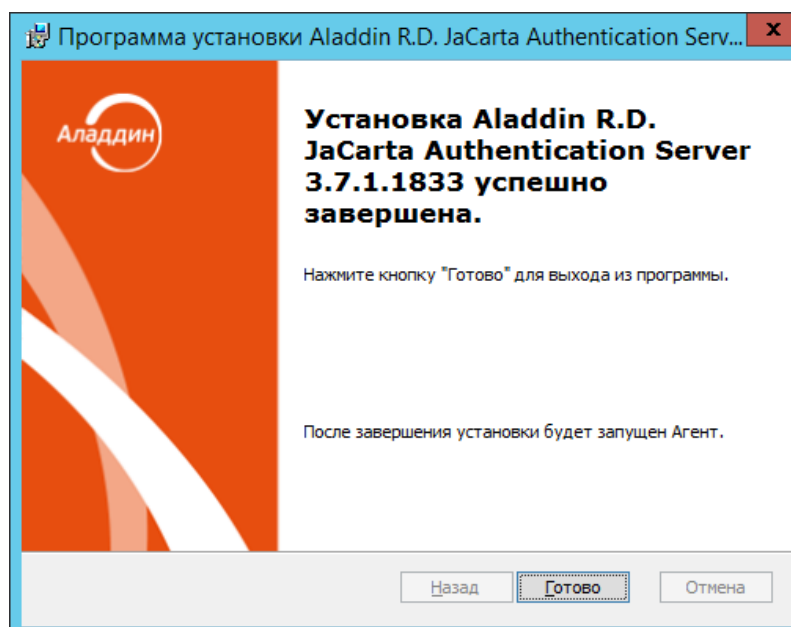


Рис. 5 – Установка завершена

6. Нажмите **Готово** для завершения процедуры.

7. Проверьте, выполняется ли служба **Aladdin JAS Engine Service – default**, и если служба не выполняется, запустите её (см. рис. 6 below).

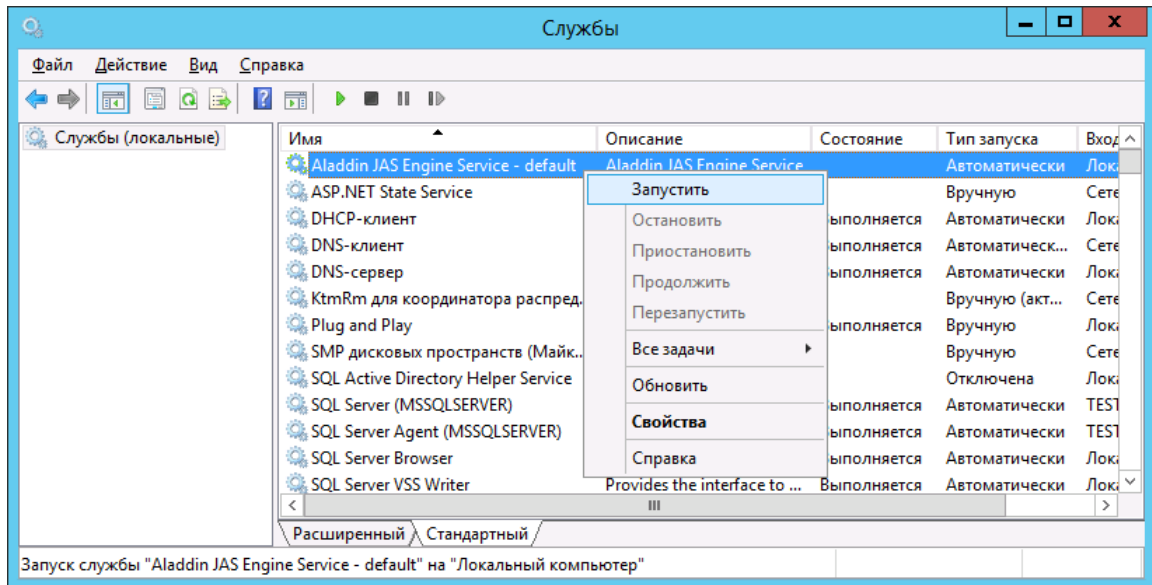


Рис. 6 – Запуск службы **Aladdin JAS Engine Service – default**

7.2 Подключение JAS к базе данных JMS

Выполните процедуру, описанную в разделе «Мастер подключения к базе данных JMS», с. 31.

7.3 Задание пароля шифрования

Выполните процедуру, описанную в разделе «Настройки безопасности», с. 62).

7.4 Настройка сетевых программных интерфейсов JAS Server

Чтобы настроить параметры взаимодействия компонентов JAS с сервером JAS через сетевые программные интерфейсы, выполните следующие действия.

1. На компьютере, на котором установлен компонент Сервер JAS, откройте редактор реестра.
2. Перейдите в следующий раздел:
[HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JaCarta Authentication Server\default].

Окно реестра будет выглядеть следующим образом.

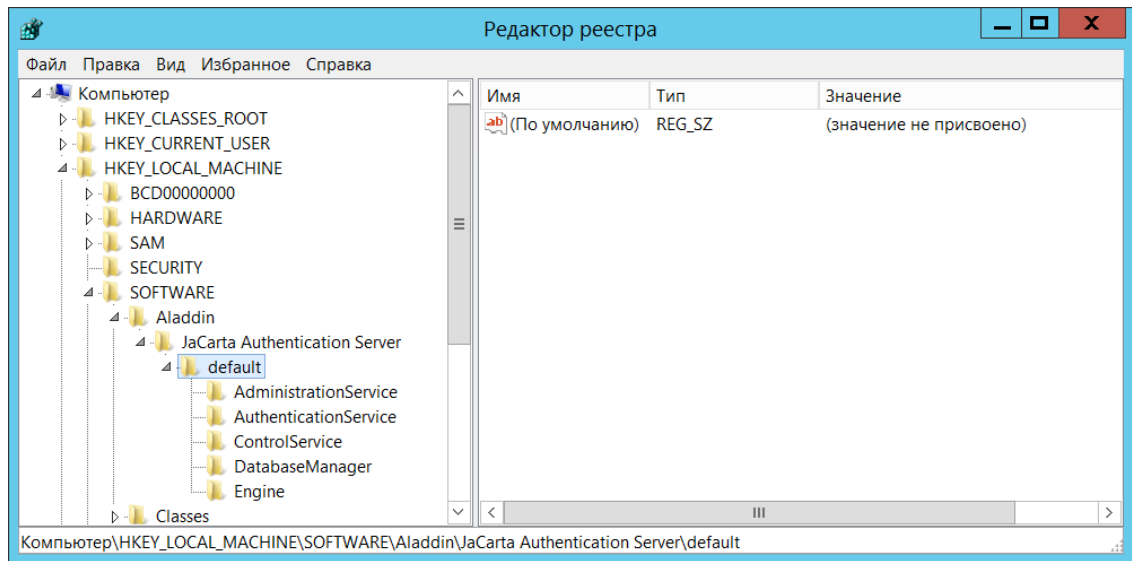




Рис. 7 – Окно редактора реестра







3. Выполните настройку сетевого программного интерфейса:

- **AdministrationService** – интерфейс для взаимодействия с сервером JMS (сервер JMS выполняет подключение к серверу JAS для управления им в соответствии с настройками, указанными в этом разделе реестра);
- **AuthenticationService** – интерфейс взаимодействия с OTP-клиентами (например, модулем OTP для NPS);
- **ControlService** – интерфейс для взаимодействия с ПО Сервер JAS (серверным агентом JAS);

руководствуясь Табл. 6

Табл. 6 – Параметры сетевых программных интерфейсов

Параметр	Описание
SecurityType	<p>Тип аутентификации пользователя при подключении по соответствующему сетевому программному интерфейсу.</p> <p>Допустимы следующие значения:</p> <ul style="list-style-type: none"> • None – аутентификация отключена, доступ к сетевому интерфейсу осуществляется анонимно; • Windows (значение по умолчанию) – используется стандартная аутентификация Windows. (выбор протокола: NTLM или Kerberos – выполняется автоматически); • Basic – базовая http-аутентификация (пароль и логин передаются в теле запроса); • NTLM – используется аутентификация Windows по протоколу NTLM. <p> Важно! При использовании базовой http-аутентификации, а также протокола NTLM (т.е. при значениях Basic и NTLM) соответствующие сетевые программные интерфейсы недоступны для публикации (параметр Address) по протоколу net.tcp (возможно использование только протокола http).</p> <p> Примечания:</p> <ol style="list-style-type: none"> 1. В случае если сервер JAS используется совместно с компонентом JOL (см. «Двухфакторная аутентификация для входа в Windows (JOL)», с. 134), аутентификация должна быть отключена (значение None). 2. В случае если аутентификация отключена (None), задавать значения для настроек AuthorizeAsGroupMember и AuthorizationGroupStore необязательно, т.к. в этом случае они ни на что не влияют. 3. В настоящем документе рассматривается вариант, в котором проверка подлинности Windows включена.
AuthorizeAsGroupMember	<p>В случае включения аутентификации (см. параметр SecurityType) для авторизации на доступ к соответствующему сервису в параметре AuthorizeAsGroupMember следует указать группу, члены которой будут авторизованы для взаимодействия через настраиваемый интерфейс. Только члены указанной группы будут иметь доступ к интерфейсу.</p> <p>Чтобы отключить авторизацию (независимо от выбранного типа аутентификации), оставьте параметр пустым.</p> <p>В настоящем документе в зависимости от интерфейса используется следующая группа:</p> <ul style="list-style-type: none"> • интерфейс AdministrationService - группа JAS Administrators; • интерфейс AuthenticationService – группа JAS Clients. <p>Подробнее см. «Предварительные действия», с. 15.</p>

Параметр	Описание
AuthorizationGroupStore	<p>Позволяет задать хранилище, в котором находится группа, указанная в настройке AuthorizeAsGroupMember. (Если настройка отсутствует, создайте соответствующий строковый параметр и присвойте ему нужное значение.) Доступны следующие значения:</p> <ul style="list-style-type: none"> • Domain (Домен) – группа Active Directory; • Machine (Локальный компьютер) – локальная группа. <p> В настоящем документе рассматривается вариант, в котором используется группа Active Directory</p>
Address	<p>Адрес публикации сетевого программного интерфейса по протоколам http (SOAP) или net.tcp. Представляет собой строку URL, например:</p> <ul style="list-style-type: none"> • <code>http://<FQDN-имя сервера>:8010/JASEngine/Default/AdministrationService</code> • <code>net.tcp://<FQDN-имя сервера>:8009/JASEngine/Default/AuthenticationService</code> <p>Или</p> <ul style="list-style-type: none"> • <code>net.tcp://<FQDN-имя сервера>:8009/...</code> <p>где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, <code>srv01.test.com</code>; либо, в случае кластерной конфигурации JAS, полное доменное имя (FQDN) <i>кластерной роли</i>, созданной на этапе настройки отказоустойчивого кластера (см. «Настройка отказоустойчивого кластера JAS», с. 132).</p> <p> Важно! Параметр доступен только для интерфейсов AdministrationService и AuthenticationService</p> <p> Примечание. В случае установки защищенного соединения для интерфейса AdministrationService по протоколу SSL/TLS вместо протокола http следует указывать протокол https, а также указать полное DNS- имя сервера, подробнее см. раздел «Настройка в JAS протоколов SSL/TLS», 23.</p>
RestAddress	<p>Адрес публикации соответствующего сетевого программного интерфейса по протоколу http (REST). Представляет собой строку URL, например:</p> <p><code>http://<FQDN-имя сервера>:8010/JASEngine/Default/AuthenticationService/rest</code></p> <p>где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, <code>srv01.test.com</code>; либо, в случае кластерной конфигурации JAS, полное доменное имя (FQDN) <i>кластерной роли</i>, созданной на этапе настройки отказоустойчивого кластера (см. «Настройка отказоустойчивого кластера JAS», с. 132).</p> <p> Важно! Параметр доступен только для интерфейсов AuthenticationService</p> <p> Примечание. В случае установки защищенного соединения для интерфейса AuthenticationService по протоколу SSL/TLS вместо протокола http следует указывать протокол https, а также указать полное DNS- имя сервера, подробнее см. раздел «Настройка в JAS протоколов SSL/TLS», 23.</p>
Thumbprint	<p>Данный параметр необходимо добавить вручную при установке защищенного соединения по протоколам SSL/TLS, подробнее см. раздел «Настройка в JAS протоколов SSL/TLS», 23.</p> <p> Важно! Параметр доступен только для интерфейсов AdministrationService и AuthenticationService</p>

4. Для вступления настроек в силу перезапустите службу **Aladdin JAS Engine Service – default** (рис. 8).

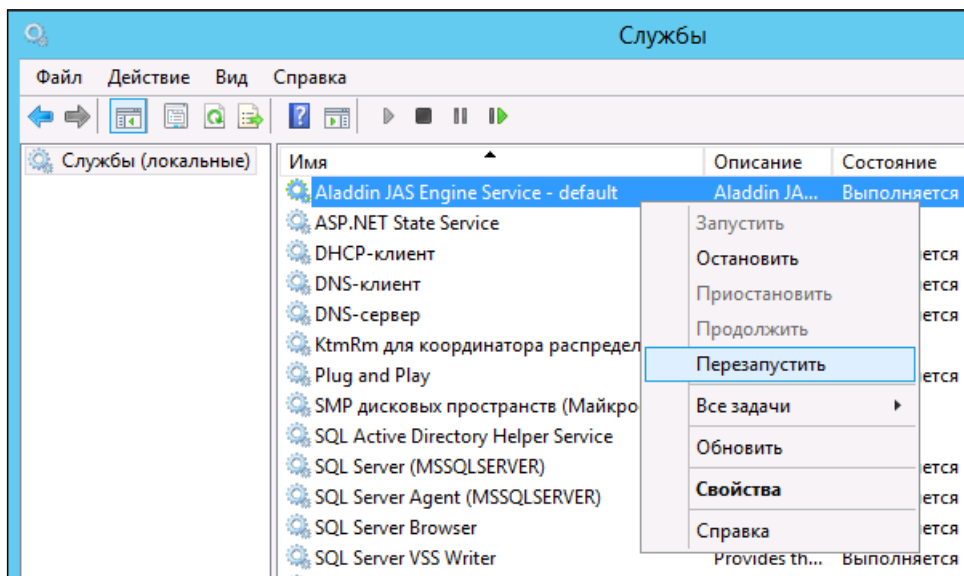


Рис. 8 – Перезапуск серверной службы

8. Настройка в JAS протоколов SSL/TLS

В JAS реализована поддержка следующих версий протоколов защиты транспортного уровня:

- SSL 3.0;
- TLS 1.0;
- TLS 1.1;
- TLS 1.2.

По умолчанию в JAS включена поддержка всех указанных версий протоколов. Техническая возможность использования того или иного протокола и его автоматический выбор будет зависеть от следующих параметров (Табл. 7, ниже).

Табл. 7 – Объекты настройки для обеспечения защищенного соединения компонентов JAS по SSL/TLS

Объект настройки	Раздел настоящего документа
Операционная система Windows	«Настройка SSL/TLS в операционной системе», с. 24
Сервер JAS	«Настройка SSL-соединения на стороне сервера JAS», с. 24
JAS-плагины NPS и AD FS	«Настройка SSL/TLS на стороне клиентов», с. 24
Компонент JOL	«Настройка SSL/TLS на стороне компонента JOL», с. 25

Таким образом, для обеспечения поддержки этих протоколов необходимо выполнить ряд настроек как на стороне сервера JAS, так и на другой стороне соединения (Рис. 9).

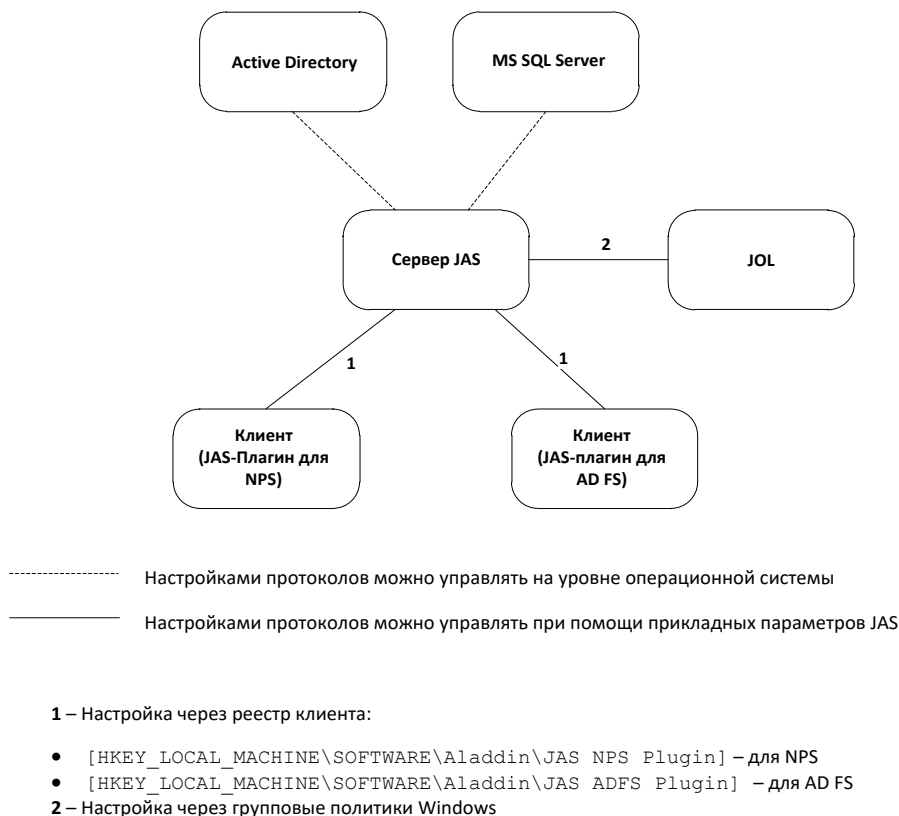


Рис. 9 – Схема настроек SSL/TLS на сторонах – участниках защищенного соединения

8.1 Настройка SSL/TLS в операционной системе

Операционная система Windows на целевой машине (сервере или клиенте JAS, почтовом сервере, сервере СУБД и т.д.) должна поддерживать требуемый протокол SSL/TLS. Настройки протоколов задаются в разделе реестра

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SC
 HANNEL\Protocols**

Для настройки протоколов SSL/TLS в операционной системе обратитесь к ее документации.



После редактирования реестра с целью настройки SSL/TLS необходимо перезагрузить операционную систему.

8.2 Настройка SSL-соединения на стороне сервера JAS

Настройки SSL-соединения на стороне сервера JAS выполняются на вкладке **Безопасность** приложения Сервер JAS (серверный агент) в секции **Настройки использования SSL/TLS** (подробнее см. раздел «Настройки использования SSL/TLS», с. 58).

В случае кластерной конфигурации JAS указанные в данном разделе настройки следует выполнить на каждом из узлов кластера.

8.3 Настройка SSL/TLS на стороне клиентов

Для настройки протоколов SSL/TLS на стороне клиентов (JAS-плагинов для NPS и AD FS) выполните следующие действия.

1. В случае если клиент JAS установлен вне домена Active Directory, в котором функционирует сервер, или если участники SSL-соединения не имеют доступа к выпущившему сертификат

- удостоверяющему центру, импортируйте сертификат SSL в раздел **Доверенные корневые центры сертификации** хранилища клиентского компьютера.
2. Выполните настройку протоколов SSL/TLS на компьютере клиента.
 - 2.1. В случае JAS-плагина для NPS в разделе реестра [**HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JAS NPS Plugin**]
 - 2.1.1. Отредактируйте строковый параметр **ServiceUri** – после редактирования этот параметр должен иметь то же значение, что было настроено на сервере JAS для службы AuthenticationService (см. раздел «Настройка SSL-соединения на стороне сервера JAS», above), а именно:
https:// <FQDN-имя сервера>:8008/JASEngine/Default/AuthenticationService/rest
где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com; либо, в случае кластерной конфигурации JAS, полное доменное имя (FQDN) *кластерной роли*, созданной на этапе настройки отказоустойчивого кластера (см. «Настройка отказоустойчивого кластера JAS», с. 132).
 - 2.1.2. Для настройки набора поддерживаемых протоколов SSL/TLS отредактируйте параметр **SecurityProtocol=Ssl3, Tls, Tls11, Tls12**

Разрешается указывать один или несколько протоколов.
По умолчанию разрешены все протоколы.
 - 2.2. В случае JAS-плагина для AD FS в разделе реестра [**HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JAS ADFS Plugin**] выполните те же настройки, что были выполнены на шагах 2.1.1–2.1.2.



Важно! После редактирования реестра, связанного с настройкой SSL/TLS, следует перезапустить службу клиента (сервиса NPS или AD FS соответственно).

8.4 Настройка SSL/TLS на стороне компонента JOL

Для настройки протоколов SSL/TLS на стороне компонента JOL выполните следующие действия.

1. В случае если компонент JOL установлен на рабочей станции вне домена Active Directory, в котором функционирует сервер JAS, или если участники SSL-соединения не имеют доступа к выпущившему сертификат удостоверяющему центру, импортируйте сертификат SSL в раздел **Доверенные корневые центры сертификации** хранилища рабочей станции с установленным компонентом JOL.
2. В настройках JOL в адресе сервиса аутентификации JAS (параметр **ServiceUri**) замените протокол «http» на «https» (порядок выполнения настроек компонента JOL на рабочих станциях приведен в разделе «Настройки JOL и порядок их применения», с. 136).
3. При необходимости ограничить максимальную используемую версию TLS, вызванной особенностями конфигурации сетевой инфраструктуры, в реестровом параметре **SSLVersionTLS** на компьютере с JOL установите необходимую версию TLS (подробнее см. раздел «Настройки JOL и порядок их применения», с. 136).
4. В случае если в операционной системе на компьютере, где установлен JOL, необходимо согласовать с JOL список поддерживаемых протоколов SSL/TLS, выполните соответствующие настройки средствами ОС Windows (см. раздел «Настройка SSL/TLS в операционной системе», с. 24).



Примечание. Настройки платформы .Net Framework, в частности в отношении поддерживаемых протоколов SSL/TLS, на защищенное подключение JOL к серверу JAS не влияют.


8.5 Настройка SSL/TLS для работы с Microsoft SQL Server

При использовании шифрованного подключения к базе данных из JAS также может потребоваться дополнительная настройка протоколов защиты транспортного уровня на стороне сервера SQL.

Данная настройка описана в руководстве по установке и настройке сервера JMS [2], разделы «Настройка SSL/TLS для работы с Microsoft SQL Server», «Подготовка сервера MS SQL для работы по SSL/TLS» .

9. Другие настройки JAS


В настоящем разделе приведены настройки, связанные с изменением конфигурационных файлов компонентов JAS. Редактирование конфигурационных файлов может осуществляться с помощью любого текстового редактора, например, с помощью программы **Блокнот**.

 При этом всякий раз текстовый редактор должен быть открыт от имени администратора – в противном случае система не позволит сохранить сделанные изменения.

9.1 Настройка параметров ведения журнала событий

Сервер JAS позволяет записывать в журнал событий сообщения следующих уровней:


- **OFF** – ведение журнала событий отключено;
- **FATAL** – неустраняемая ошибка;
- **ERROR** – ошибка;
- **WARN** – предупреждение;
- **INFO** – информация;
- **DEBUG** – отладка;
- **ALL** – показывать все события.

 Каждый последующий уровень включает все предыдущие (кроме **OFF**). Например, если выставлено значение **INFO**, то будут отображаться сообщения уровней: **INFO, WARN, ERROR, FATAL**.

В табл. 8 представлены параметры ведения журнала событий для сервера бизнес-логики JAS и серверного агента (ПО Сервер JAS).

Табл. 8 – Настройка параметров ведения основных журналов событий

Компонент JAS	Расположение файла конфигурации	Сведения о настройке ведения журнала событий
Сервер бизнес-логики JAS	<p>Файл конфигурации Aladdin.JAS.Engine.exe.config находится в каталоге установки JAS Server. Путь к файлу по умолчанию:</p> <p>C:\Program Files\Aladdin\JaCarta Authentication Server\</p>	<ol style="list-style-type: none"> 1. Откройте файл конфигурации с помощью текстового редактора. 2. Отредактируйте значение элемента <level value> для элемента <root>. Используйте значения, приведённые в начале настоящего раздела.

Компонент JAS	Расположение файла конфигурации	Сведения о настройке ведения журнала событий
Серверный агент (ПО Сервер JAS)	<p>Файл конфигурации Aladdin.JAS.Agent.exe.config находится в каталоге установки JAS Server. Путь к файлу по умолчанию:</p> <p>C:\Program Files\Aladdin\JaCarta Authentication Server\</p>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <pre><root> <level value="DEBUG" /></pre> </div> <p> В настройках файла конфигурации сервера JAS под элементом <root> также располагаются элементы, позволяющие задать индивидуальные настройки ведения журнала событий для различных служб и интерфейсов JAS. Чтобы изменить уровень ведения журнала событий, в элементе <level value=...>, соответствующем нужной службе или интерфейсу, также укажите нужное значение (от OFF до ALL).</p>

Сохраните изменения и закройте файл конфигурации.





Также существует возможность настроить параметры ведения журнала событий JAS-плагина для NPS. Процедура отличается от приведённой выше и приведена в подразделе «Настройка JAS-плагина для NPS», с. 78.

9.2 Изменение языка графического интерфейса

Интерфейс JAS может отображаться на двух языках:

- русский (по умолчанию);
- английский.

Чтобы изменить отображаемый язык интерфейса, выполните следующие действия.

1. С помощью текстового редактора последовательно откройте файлы конфигурации:
 - ▶ **<каталог установки JAS Server>\Aladdin.JAS.Engine.exe.config;**
 - ▶ **<каталог установки JAS Server>\Aladdin.JAS.Agent.exe.config;**
 - ▶ **<каталог установки JAS Server>\Aladdin.JAS.DbWizard.exe.config;**
2. Найдите строку **<add key="Culture" value="ru" />**.
3. Замените значение элемента в соответствии со сведениями, представленными ниже:
 - **<add key="Culture" value="ru" />** - русский язык интерфейса;
 - **<add key="Culture" value="en" />** - английский язык интерфейса.
4. Сохраните сделанные изменения и закройте файлы конфигурации.
5. перезапустите службу *Aladdin JAS Engine Service – default*;
6. в области уведомлений нажмите правой кнопкой мыши на значке   и выберите выход;
7. В меню **Пуск** выберите **JaCarta Authentication Server > Сервер JAS**.

Язык интерфейса изменён.

10. Обновление JAS



Для обновления JAS на новую версию сначала удалите все установленные компоненты JAS, после чего выполните установку новых версий компонентов JAS и их настройку.

Для обновления БД JAS (после установки обновленной версии JAS) следует заново выполнить подключение к БД JMS (см. раздел «Мастер подключения к базе данных JMS», с. 31). После того как закончится выполнение мастера подключения, обновление БД JAS выполнится автоматически.

11. Сервер JAS

ПО Сервер JAS, или *серверный агент*, служит для оперативного управления (логический запуск/остановка/приостановка/перезапуск) бизнес-логикой JAS, реализуемой серверной службой **Aladdin JAS Engine Service – default**, и базовой настройки параметров функционирования JAS.

11.1 Меню быстрого доступа в области уведомлений

Сервер JAS отображается в виде значка  () в области уведомлений. Чтобы отобразить меню быстрого доступа, Нажмите правой кнопкой мыши на этом значке. Меню выглядит следующим образом.

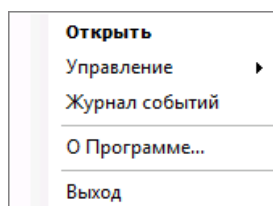







Рис. 10 – Меню быстрого доступа в области уведомлений

Меню содержит следующие пункты (см. табл. 9 ниже).

Табл. 9 – Меню в области уведомлений

Пункт	Описание
Открыть	Открывает окно управления сервером JAS – подробнее см. «Окно управления ПО Сервер JAS» ниже
Управление	<p>Позволяет изменить статус сервера, доступны следующие пункты:</p> <ul style="list-style-type: none"> • Старт – запуск сервера JAS; • Стоп – остановка сервера JAS; • Пауза – приостановка работы сервера JAS; • Продолжить – возобновление работы сервера JAS после приостановки; • Рестарт – перезапуск сервера JAS. <p>Изменение статуса сервера также возможно выполнить из окна управления сервером JAS (подробнее см. «Окно управления ПО Сервер JAS» ниже).</p> <p> После внесения изменений в реестр необходимо перезапустить серверную службу Aladdin JAS Engine Service – default из оснастки Windows Службы. При перезапуске сервера с помощью настоящего меню (пункт Рестарт) новые параметры не будут применены</p>
Журнал событий	Отображает журнал событий, связанных с использованием JAS (о настройке параметров ведения журнала событий см. «Настройка параметров ведения журнала событий», с. 26).
О Программе	Отображает сведения о JAS
Выход	Скрывает значок  () из области уведомлений

12. Окно управления ПО Сервер JAS

Чтобы открыть окно управления JAS, нажмите правой кнопкой мыши на значке  () в области уведомлений и выберите **Открыть**.

Окно будет выглядеть следующим образом.

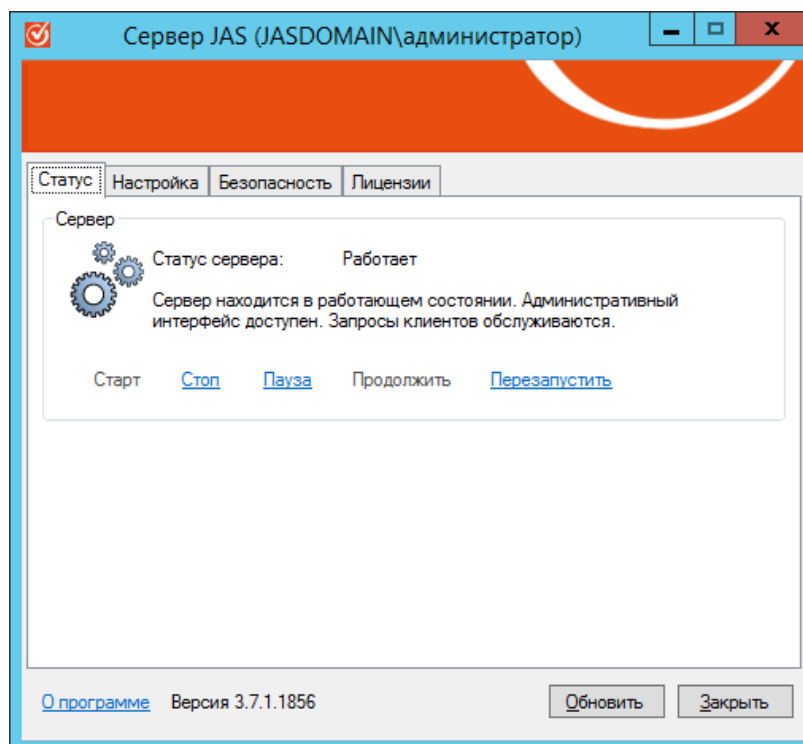


Рис. 11 – Окно управления сервером JAS

В зависимости от выбранной вкладки окно предоставляет доступ к следующим настройкам (табл. 10 ниже).

Табл. 10 – Окно управления сервером JAS

Вкладка	Ссылка	Описание
Статус		Отображает статус сервера JAS, а также позволяет останавливать и перезапускать сервер JAS (подробнее см. «Статус», с. 30).
Настройка		Позволяет выполнить первоначальную настройку конфигурации... Подробнее см. «Настройка», с. 31.
Безопасность		Позволяет выполнить настройки параметров безопасности функционирования сервера JAS. Подробнее см. раздел «Безопасность», с. 58
Лицензии		На вкладке Лицензии отображается лицензия, на основе которой эксплуатируется сервер JAS, подробнее см. «Лицензии (проверка/просмотр лицензии на использование продукта JAS)», с. 64

12.1 Статус

Вкладка **Статус** окна управления сервером JAS выглядит следующим образом (см. рис. 12).

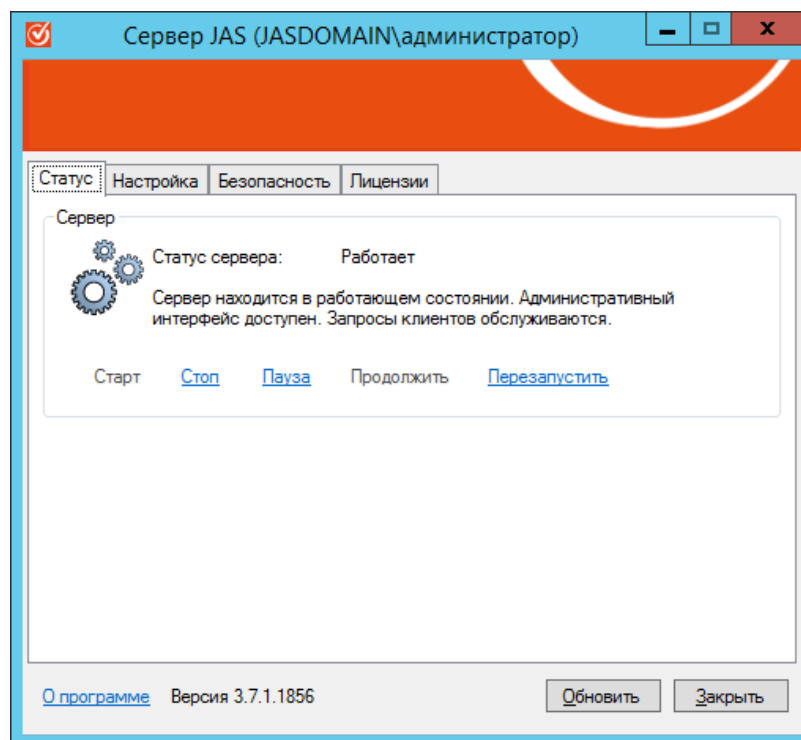


Рис. 12 – Вкладка **Статус**

Вкладка **Статус** содержит следующие элементы (см. табл. 11).

Табл. 11 – Вкладка **Статус**

Элемент	Описание
Статус сервера	Отображает состояние сервера JAS на текущий момент.
Старт	Запускает сервер JAS (впервые или после остановки).
Пауза	Приостанавливает работу сервера JAS.
Стоп	Останавливает работу сервера JAS.
Продолжить	Возобновляет работу сервера JAS (после приостановки).
Перезапустить	Перезапускает сервер JAS. Важно! После внесения изменений в реестр необходимо перезапустить серверную службу Aladdin JAS Engine Service – default из оснастки Windows Службы . При перезапуске сервера с помощью настоящего меню (пункт Рестарт) новые параметры не будут применены

Для обновления отображаемых сведений щелкните на кнопке **Обновить**.

12.2 Настройка

Вкладка **Настройка** выглядит следующим образом.

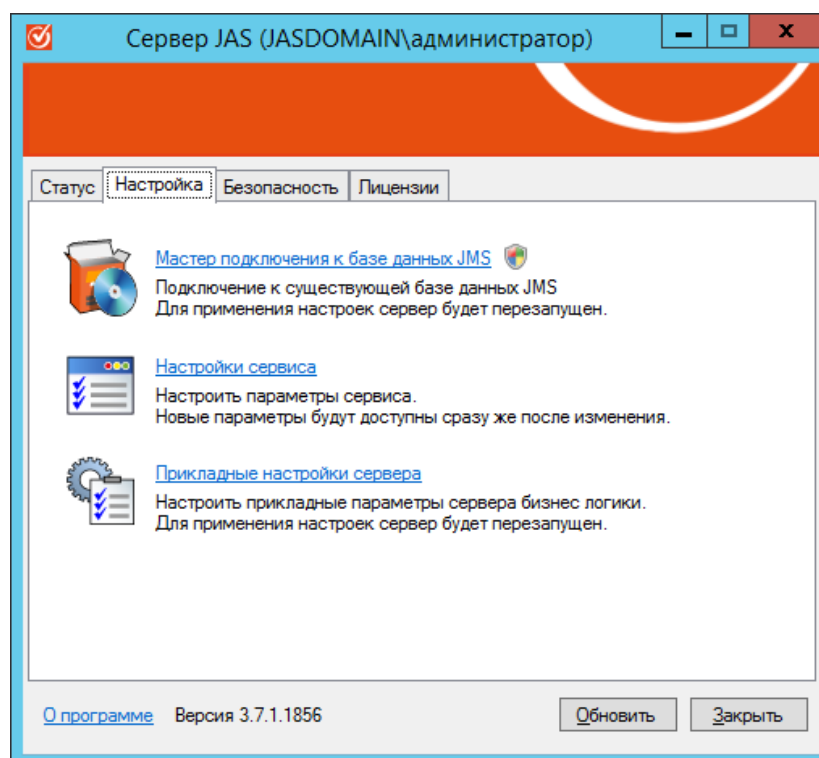


Рис. 13 – Вкладка Настройка

Вкладка содержит следующие элементы (см. табл. 12).

Табл. 12 – Элементы вкладки Настройка



Элемент интерфейса	Описание
Ссылка Мастер подключения к базе данных JMS	Запускает процедуру подключения JAS к базе данных JMS (см. «Мастер подключения к базе данных JMS», с. 31)
Ссылка Настройки сервиса	Позволяет настроить параметры работы серверной службы JAS (подробнее см. «Настройки сервиса» ниже)
Ссылка Прикладные настройки сервера	Позволяет задать значения параметров, включая настройки по умолчанию, для различных типов аутентификаторов (подробнее см. «Прикладные настройки сервера», с. 40)

12.2.1 Мастер подключения к базе данных JMS

В данном разделе описывается процедура подключения JAS к базе данных JMS.

Важно! Перед выполнением настроек, указанных в данном разделе следует выполнить операции по установке и настройке компонента JMS Server, в процессе которых будет создана база данных JMS. Компонент JAS в своей работе использует тот же SQL-сервер, что и компонент JMS Server. Процедура установки компонента JMS Server приведена в документе «Руководство администратора. Часть 1» [2].

Чтобы настроить подключение к базе данных, выполните следующие действия.

1. Нажмите правой кнопкой мыши на значке  (или ) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Настройка**.
Окно примет следующий вид.

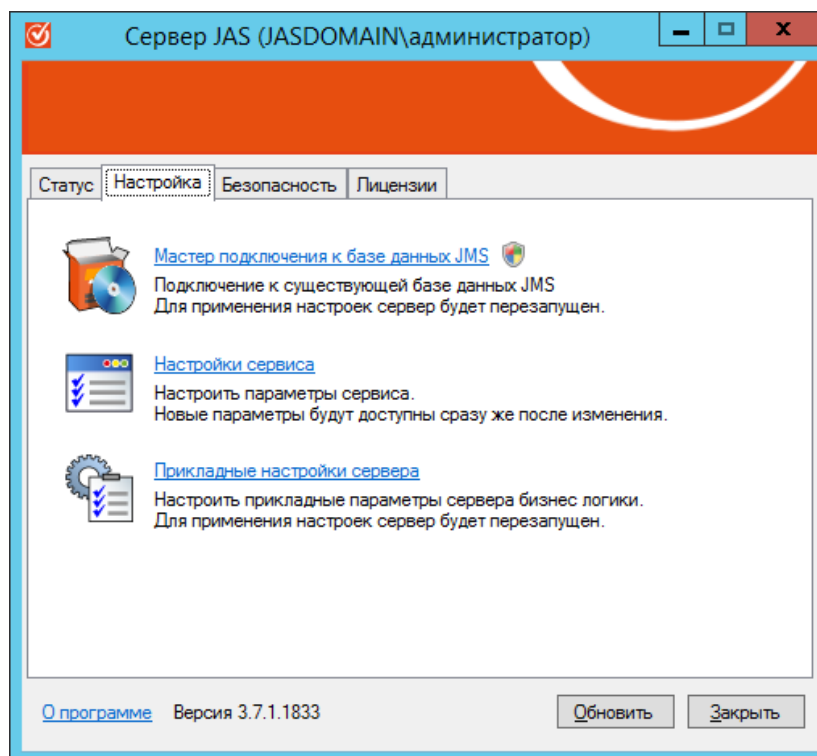


Рис. 14 – Вкладка Настройка

3. Нажмите на ссылке **Мастер подключения к базе данных JMS**.
Отобразится следующее окно.

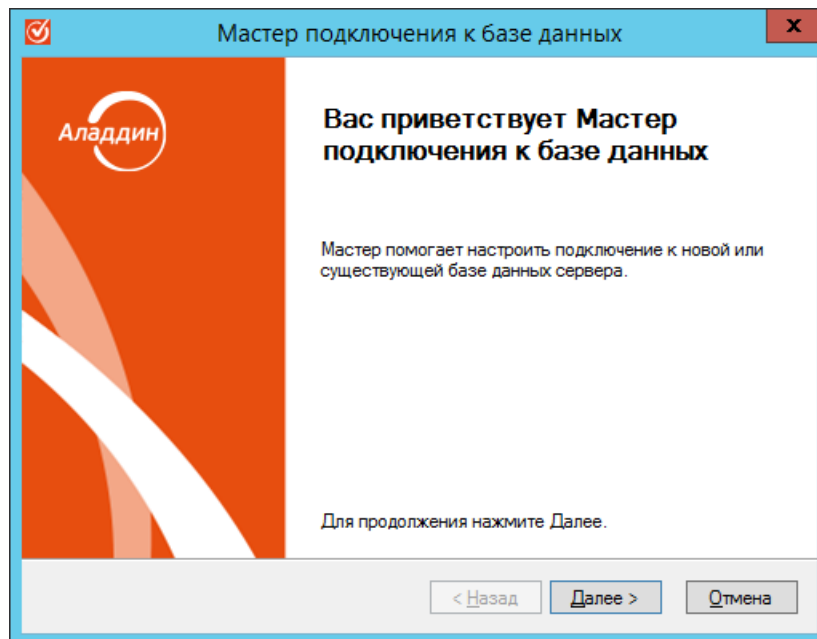


Рис. 15 – Окно приветствия мастера подключения к базе данных

4. Нажмите **Далее**.
Отобразится следующее окно.

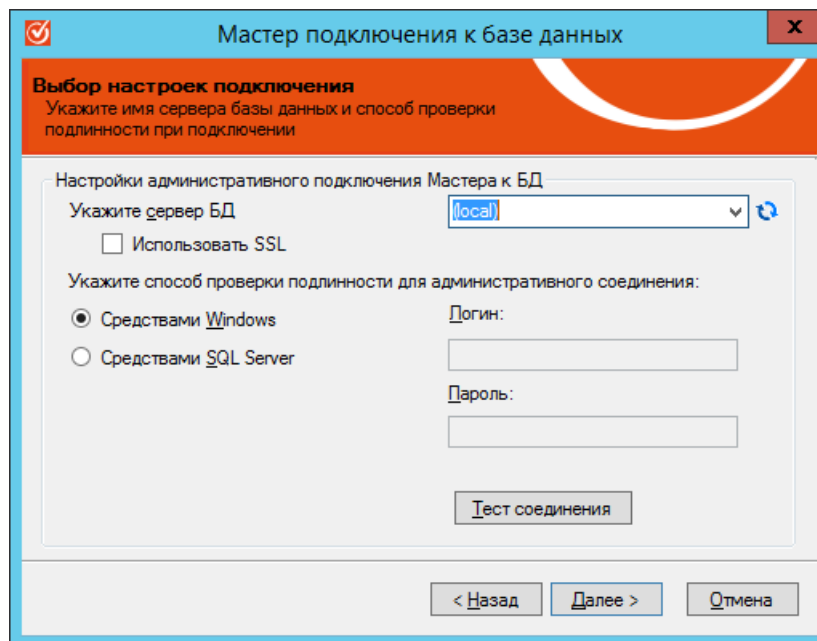


Рис. 16 – Выбор настроек подключения

5. Выполните следующие настройки:

в списке **Укажите сервер БД** выберите сервер базы данных, ранее использовавшийся для установки БД JMS, см «Руководство администратора. Часть 1» [2]; если имя сервера отсутствует в списке, укажите его вручную;
если у вас настроен доступ к серверу базы данных по SSL, установите флажок **Использовать SSL**;

выберите способ проверки подлинности для соединения с базой данных:

- ▶ **Средствами Windows** – проверка будет осуществляться средствами проверки подлинности Windows;
- ▶ **Средствами SQL Server** – в этом случае в полях **Логин** и **Пароль** введите соответственно имя пользователя и пароль учётной записи, которая имеет права на управления базой данных.



В настоящем документе для примера будет использоваться вариант **Средства Windows**.

6. Нажмите **Тест соединения**.
При успешном соединении отобразится следующее сообщение.

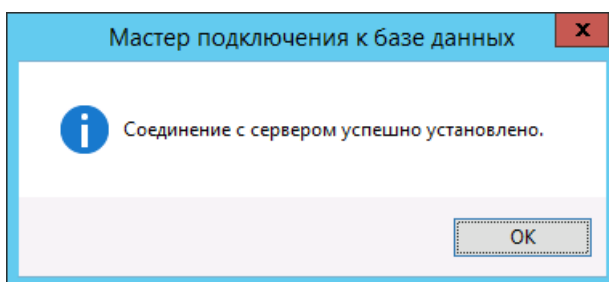


Рис. 17 – Сообщение об успешной проверке соединения

7. Нажмите **OK**.
8. В окне выбора настроек подключения нажмите **Далее**.
Отобразится следующее окно.

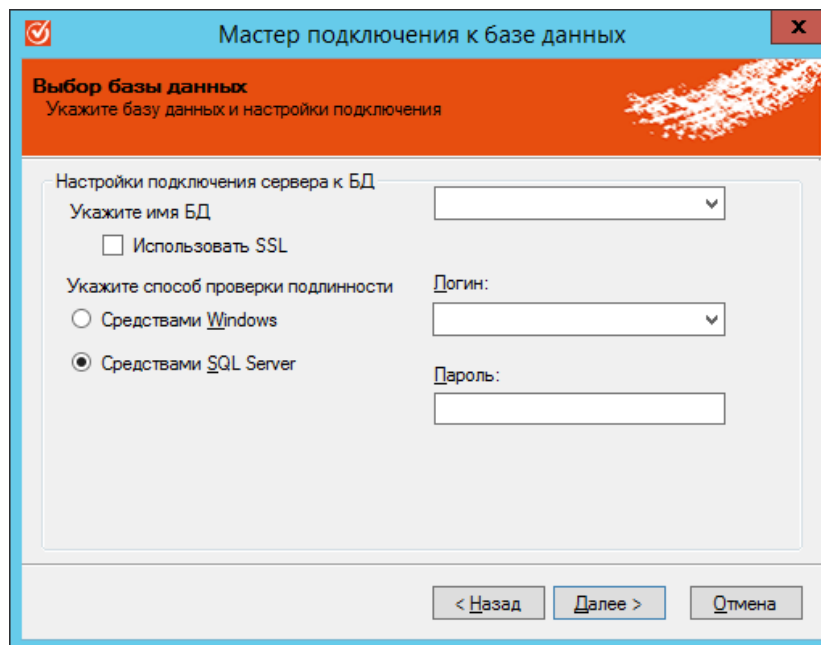



Рис. 18 – Выбор базы данных


9. Выполните следующие настройки:

в поле **Укажите имя БД** выберите имя базы данных JMS, к которой вы подключаетесь;
если у вас настроено SSL-соединение с базой данных, установите флажок **Использовать SSL**;

выберите один из двух способов проверки подлинности:

- ▶ **Средствами Windows** – в этом случае для аутентификации пользователя будет использоваться проверка подлинности Windows;
- ▶ **Средствами SQL Server** – если вы выбрали этот пункт, то в списке Логин выберите имя учётной записи, в поле Пароль введите пароль для неё.

 Если проверка подлинности производится средствами SQL-сервера, выбранная учётная запись должна обладать полномочиями, достаточными для управления сервером SQL. Если на момент настройки подключения к базе данных эта учётная запись не обладает такими полномочиями, их необходимо установить вручную.

 В настоящем руководстве для примера будет использоваться проверка аутентификации средствами Windows.

10. Нажмите **Далее**.
Отобразится следующее окно.

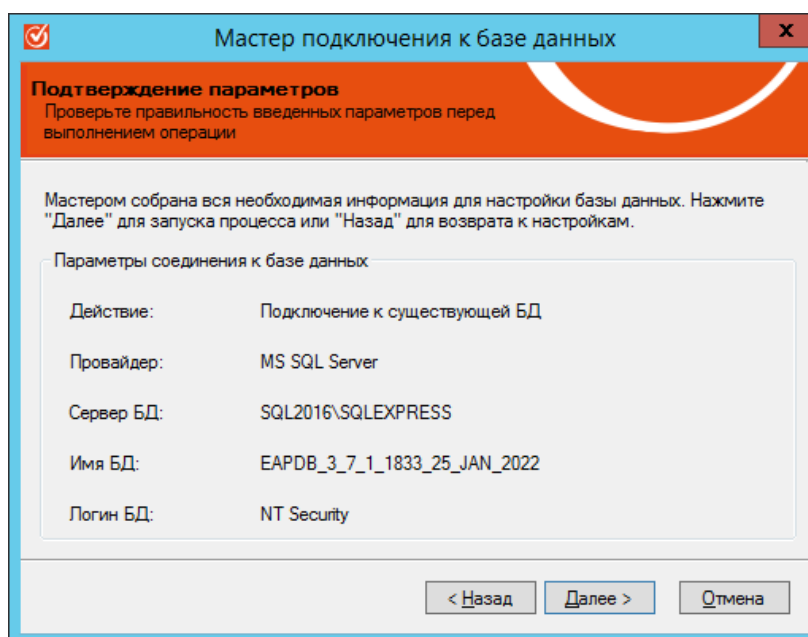


Рис. 19 – Подтверждение параметров

11. Нажмите **Далее**.

В случае если JAS подключается к ранее использовавшейся БД JMS, требующей обновления, то будут выполнены следующие несколько шагов обновления БД JAS. В противном случае переходите к завершающему шагу процедуры. Отобразится следующее окно.

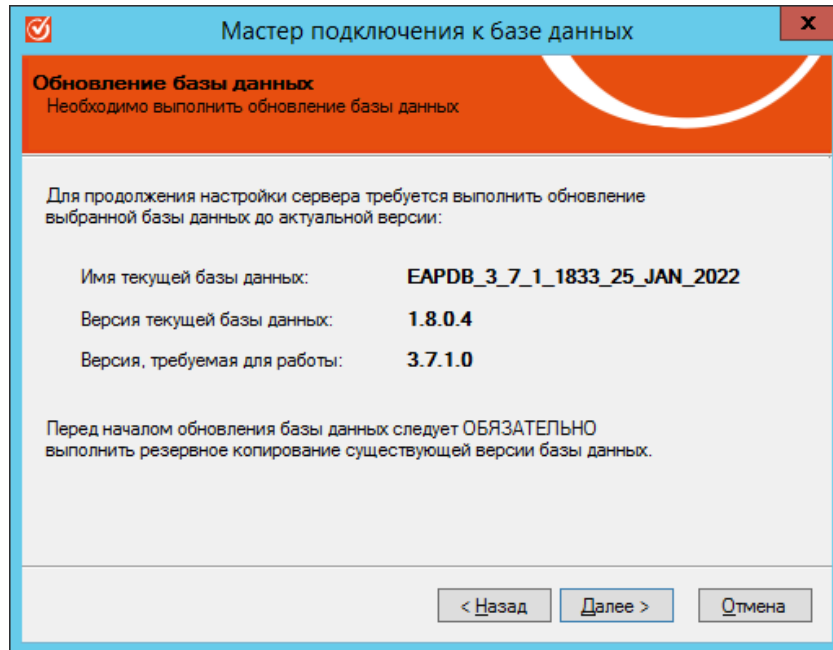



Рис. 20 – Окно уведомления о необходимости обновить БД JAS

12. Нажмите **Далее**.

 Перед началом обновления базы данных настоятельно рекомендуется выполнить резервное копирование существующей версии базы данных. Также, по возможности, следует завершить все ранее начатые операции, связанные с обращением к мастер-ключу БД.

Отобразится следующее окно.

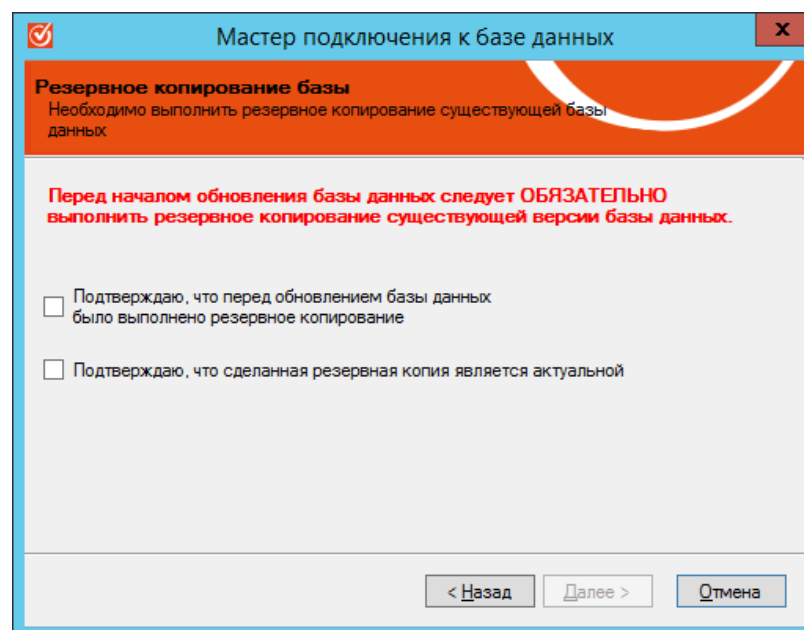


Рис. 21 – Начало процедуры обновления базы данных

13. Установите флаги подтверждения, после чего нажмите **Далее**.
14. Дождитесь завершения операции обновления базы данных. В зависимости от объема данных этот процесс может занять несколько минут.
По завершении обновления отобразится окно с детализацией обновления.

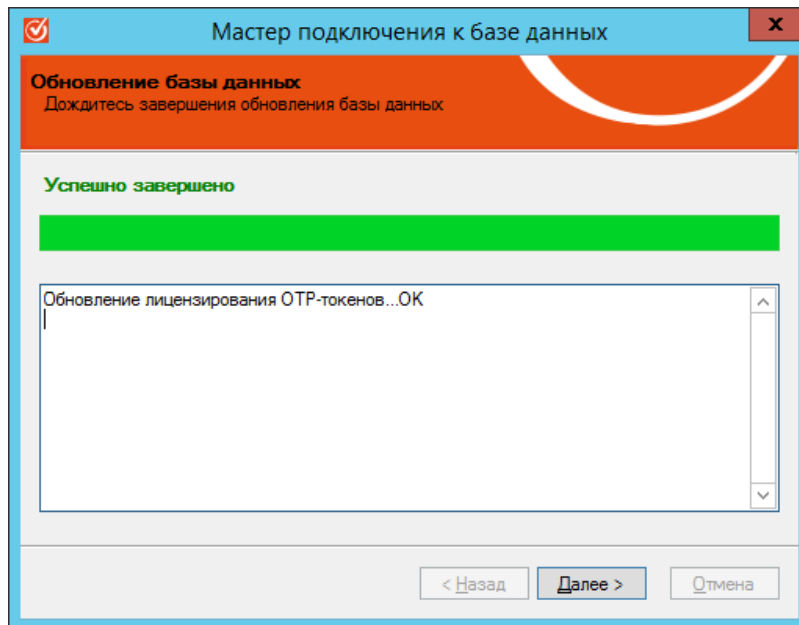


Рис. 22 – Детализация обновления БД

15. Нажмите **Далее**.
По завершении обновления отобразится следующее окно.

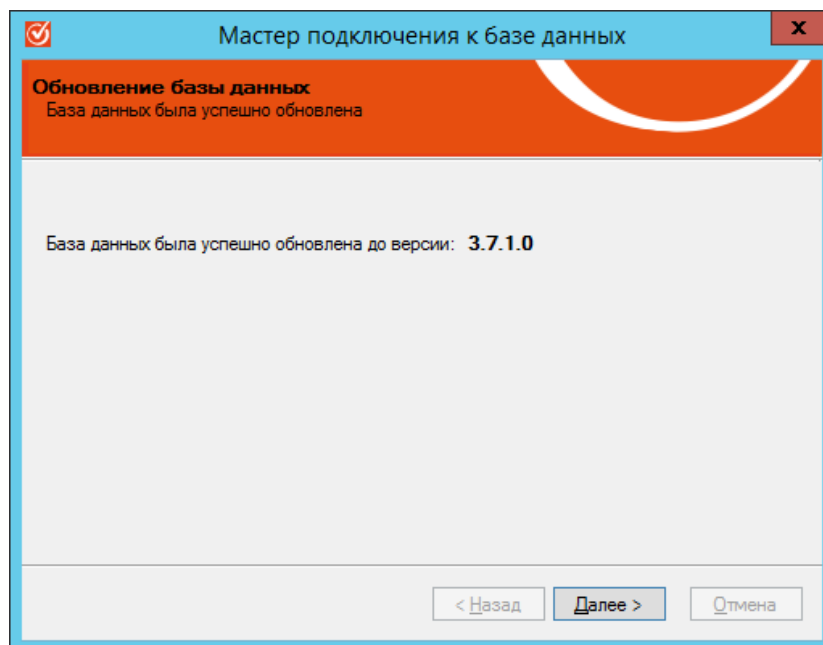


Рис. 23 – Завершение процедуры обновления базы данных

16. Нажмите **Далее**.

Отобразится следующее окно.

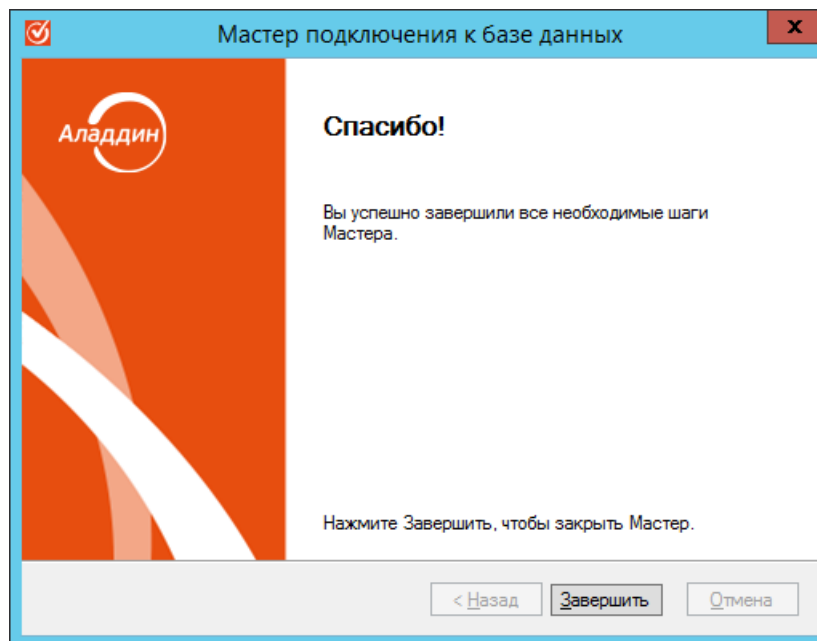


Рис. 24 – Завершение подключения к базе данных

17. Нажмите **Завершить**.

 **Важно!**

1. После настройки не забудьте запустить сервер бизнес-логики JAS (вкладка **Статус**, ссылка **Старт**, см. раздел «Окно управления ПО Сервер JAS», с. 28).
2. Выполненной процедуры недостаточно для завершения полной интеграции сервера JAS с сервером JMS. Для завершения такой интеграции следует выполнить ряд шагов в серверном агенте JMS (приложении Сервер JMS) в разделе **Настройки JAS**. Подробнее см. раздел «Настройки JAS» документа «JaCarta Management System v3.7. Руководство администратора. Часть 1. Установка и настройка» [2], с. 155.

12.2.2 Настройки сервиса

В настоящем разделе описана настройка правил управления сервером бизнес-логики JAS, в частности, в зависимости от состояния службы JAS.

Чтобы настроить параметры работы серверной службы JAS, выполните следующие действия.

1. Откройте окно управления сервером JAS и перейдите на вкладку **Настройки**.
2. Нажмите **Настройки сервиса**.

Отобразится следующее окно.

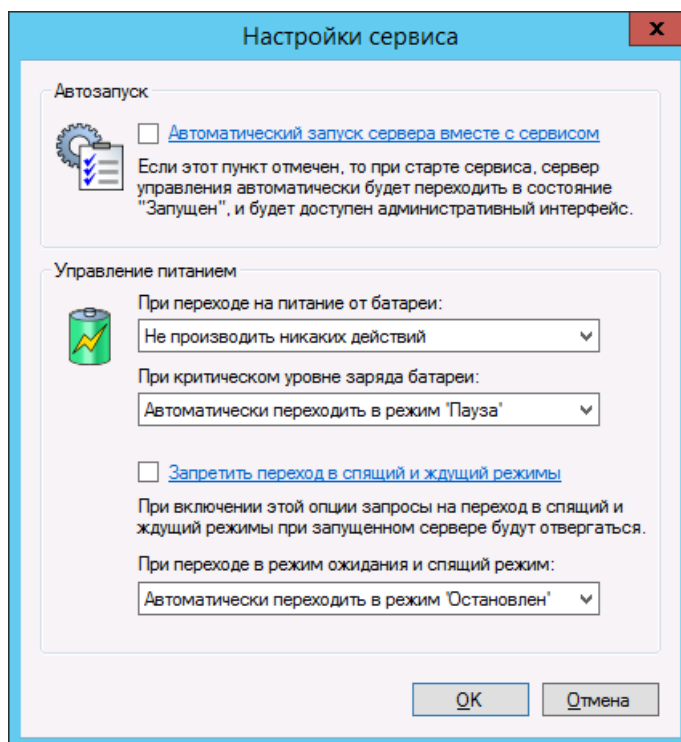


Рис. 25 – Параметры настройки серверной службы JAS

3. Выполните настройку, руководствуясь табл. 13 ниже.

Табл. 13 – Настройка серверной службы

Секция	Настройка	Описание
Автозапуск	Автоматический запуск сервера вместе с сервисом	Если флажок установлен, при запуске службы автоматически будет запускаться сервер управления JAS
Управление питанием	При переходе на питание от батареи	<p>Позволяет настроить параметры работы серверной службы при переходе на питание от батареи. Список содержит следующие пункты:</p> <ul style="list-style-type: none"> • Не производить никаких действий; • Автоматически переходить в режим 'Пауза'; • Автоматически переходить в режим 'Остановлен'
	При критическом уровне заряда батареи	<p>Позволяет настроить параметры работы серверной службы при критическом уровне заряда батареи. Список содержит следующие пункты:</p> <ul style="list-style-type: none"> • Не производить никаких действий; • Автоматически переходить в режим 'Пауза'; • Автоматически переходить в режим 'Остановлен'
	Запретить переход в спящий и ждущий режим	Если флажок установлен, запросы на переход в спящий и ждущий режимы при запущенном сервере будут отвергаться

Секция	Настройка	Описание
	При переходе в режим ожидания и спящий режим	<p>Список активен, только если снят флажок Запретить переход в спящий и ждущий режим. Список содержит следующие пункты:</p> <ul style="list-style-type: none"> • Не производить никаких действий; • Автоматически переходить в режим 'Пауза'; • Автоматически переходить в режим 'Остановлен'

4. Нажмите **ОК**, чтобы сохранить изменения.
- 5.

12.2.3 Прикладные настройки сервера

Чтобы изменить прикладные настройки сервера, выполните следующие действия.



Настройки, регулирующие параметры функционирования токенов, будут действовать на все токены, выпускаемые из Консоли управления JMS.

1. Откройте окно управления сервером JAS и перейдите на вкладку **Настройка**.

12.2.3.1 Настройки Messaging-транспорта



Примечание. Messaging-транспорт обеспечивает доставку одноразовых паролей как в случае использования Messaging-токенов, так и для механизма аутентификации пользователей в личном кабинете JWM посредством SMS-оповещения.

2. Нажмите на ссылке **Прикладные настройки сервера**. Выберите вкладку **Настройки Messaging**. Отобразится следующее окно.

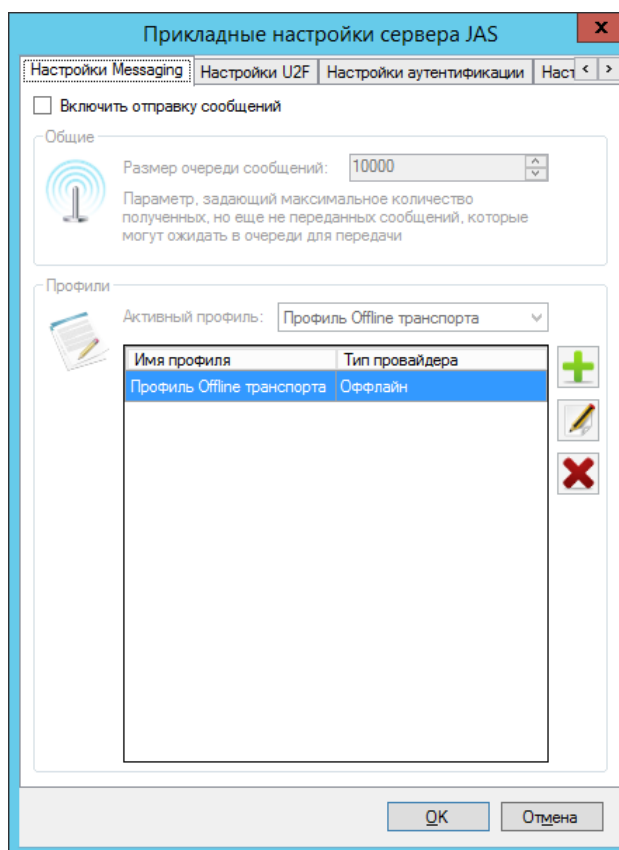



Рис. 26 – Окно настройки Messaging-транспорта

3. Выполните настройки Messaging-транспорта, руководствуясь Табл. 14.

Табл. 14 – Настройка Messaging-транспорта сообщений

Настройка	Описание
Включить отправку сообщений	<p>Установите флаг для включения транспорта сообщений, т.е. для отправки:</p> <ol style="list-style-type: none"> уведомлений и одноразовых паролей пользователям посредством Messaging-токенов. SMS-оповещений для механизма аутентификации пользователей в личном кабинете JWM. <p>По умолчанию транспорт сообщений выключен</p>
Размер очереди сообщений	<p>При необходимости измените размер очереди сообщений.</p> <p>Очередь сообщений представляет собой последовательность сообщений на сервере JAS, ожидающих отправки в SMS-центр. При переполнении очереди сообщений новые запросы на аутентификацию будут отклоняться с ошибкой.</p> <p>Значение по умолчанию: 10000</p>
Секция Профили	<p>Настройте и установите профиль транспорта сообщений (поле Активный профиль). В один момент времени может быть активен только один профиль. (порядок настройки профилей описан начиная с шага 4, ниже).</p> <p>По умолчанию активен Профиль Offline транспорта, который записывает SMS-сообщение в файл, никуда не отправляя</p> <p>Для реальной отправки сообщений добавьте и настройте профили HTTP- и SMPP-транспорта.</p> <p> Примечание. При использовании HTTP- или SMPP-транспорта доставка сообщений к SMS-центрам мобильных операторов производится посредством SMS-шлюзов (в том числе коммерческих). Для работы через такой шлюз необходимо предварительно завести на нём учетную запись, выполнив в ней все необходимые настройки.</p>

4. Для добавления в список нового профиля профиля Offline-транспорта нажмите кнопку  (Рис. 26, с. 40) и выберите **Профиль провайдера Offline**. Отобразится следующее окно.

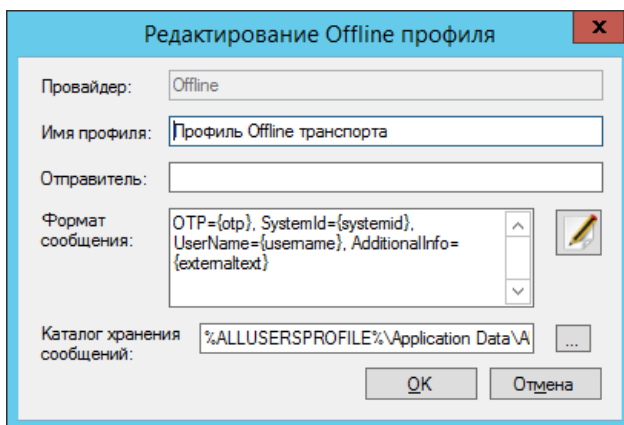



Рис. 27 – Настройки профиля Offline-транспорта

5. Выполните настройку профиля, руководствуясь Табл. 15.

Табл. 15 – Настройка Offline-транспорта сообщений

Настройка	Описание
Провайдер	Тип доставки сообщения – Offline (сохранение сообщений в локальную папку для отладки сервиса). Неизменяемое поле
Имя профиля	Имя профиля, которое будет отображаться в списке профилей
Отправитель	Введите имя отправителя. (Предназначено для отражения в сообщении пользователю)
Формат сообщения	<p>Формат строки сообщения, предназначенного для дальнейшей отправки пользователю. Содержит зарезервированные переменные, которые будут заменены при отправке данного сообщения:</p> <ul style="list-style-type: none"> • {otp} – сгенерированный одноразовый пароль; • {systemid} – идентификатор внешней системы; • {username} – имя пользователя; • {externaltext} – строка, передаваемая внешней системой. <p>Для редактирования формата нажмите  .</p> <p>Формат сообщения по умолчанию: OTP={otp}, SystemId={systemid}, UserName={username}, AdditionalInfo={externaltext}</p>
Каталог хранения сообщений	<p>Введите имя папки для сохранения сообщений при выборе данного Offline-профиля в качестве активного. Папка по умолчанию:</p> <p>C:\ProgramData\Aladdin\JaCarta Authentication Server\Notifications</p>

6. Нажмите **ОК**, чтобы сохранить изменения.
7. Для добавления в список профиля HTTP-транспорта нажмите кнопку  (Рис. 26, с. 40) и выберите **Профиль провайдера Http**.
Отобразится следующее окно.

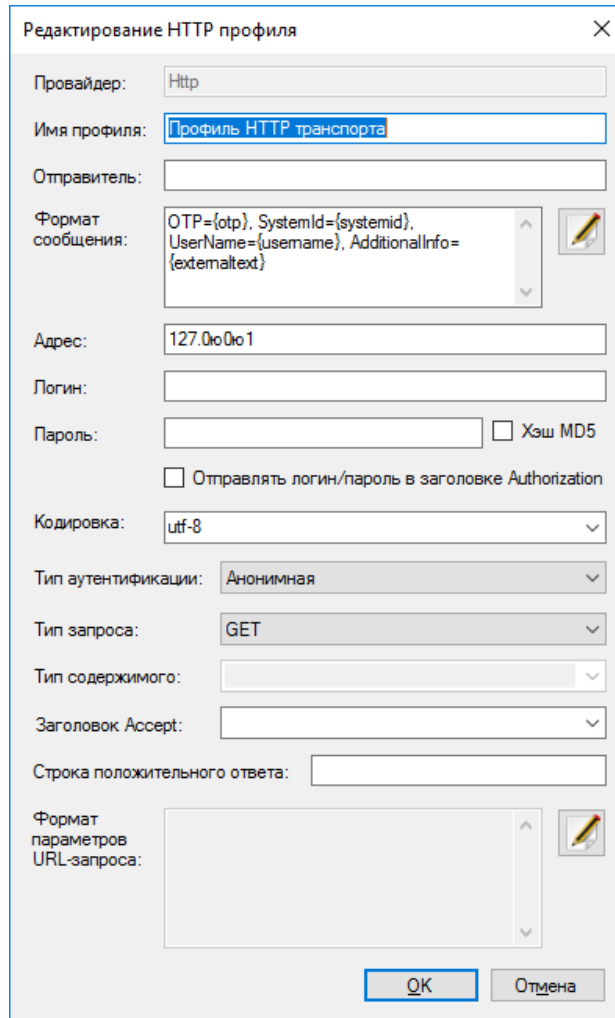



Рис. 28 – Настройки профиля HTTP-транспорта


8. Выполните настройку профиля, руководствуясь Табл. 16.

Табл. 16 – Настройка HTTP-транспорта сообщений

Настройка	Описание
Провайдер	Тип доставки сообщения – Http (доставка сообщений по протоколу HTTP). Неизменяемое поле
Имя профиля	Имя профиля, которое будет отображаться в списке профилей

Настройка	Описание
Отправитель	Идентификатор отправителя – имя, которое будет указано в качестве отправителя сообщения. В общем случае это имя регистрируется у операторов связи (должно соответствовать имени отправителя в настройках учетной записи пользователя коммерческого SMS-шлюза)
Формат сообщения	<p>Формат строки сообщения, отправляемого через SMS-шлюз. Содержит зарезервированные переменные, которые будут заменены при отправке данного сообщения:</p> <ul style="list-style-type: none"> • {otp} – сгенерированный одноразовый пароль; • {systemid} – идентификатор внешней системы; • {username} – имя пользователя; • {externaltext} – строка, передаваемая внешней системой. <p>Для редактирования формата нажмите  .</p> <p>Формат сообщения по умолчанию:</p> <pre>OTP={otp}, SystemId={systemid}, UserName={username}, AdditionalInfo={externaltext}</pre>
Адрес	Адрес (URL-строка) для отправки HTTP-запросов на рассылку SMS-сообщения
Логин	Имя пользователя учетной записи коммерческого SMS-шлюза
Пароль	Пароль пользователя
Отправлять логин/пароль в заголовке Authorization	Флаг
Хэш MD5	Признак использования хэша MD5 от пароля при передаче
Кодировка	<p>Кодировка отправляемого сообщения.</p> <p>Доступные значения:</p> <ul style="list-style-type: none"> • windows-1251 • utf-8 • koi8-r
Тип аутентификации	<p>Тип аутентификации по HTTP-соединению</p> <p>Доступные значения:</p> <ul style="list-style-type: none"> • Анонимная • Basic
Тип запроса	<p>Имя метода, используемого в HTTP-запросе, который отправляется на SMS-шлюз.</p> <p>Доступные значения:</p> <ul style="list-style-type: none"> • GET • POST

Настройка	Описание
Тип содержимого	<p>Тип содержимого в теле HTTP-запроса.</p> <p>Доступные значения:</p> <ul style="list-style-type: none"> • text/plain • text/html • text/xml • application/xml • application/json • application/x-www-form-urlencoded <p>Этот параметр доступен только при запросах типа POST (см. поле Тип запроса).</p>
Заголовок Асепт	<p>Доступные значения:</p> <ul style="list-style-type: none"> • */* • text/plain • text/html • text/xml • application/xml • application/json • application/x-www-form-urlencoded
Строка положительного ответа	<p>Строка, вхождение которой в ответ от SMS-шлюза означает, что передача сообщения завершилась успешно</p>
Формат параметров URL-запроса	<p>Строка, задающая формат передаваемых параметров к SMS-шлюзу. Для HTTP-запроса типа GET это формат фрагмента URI-строки, для запроса типа POST – это содержимое тела запроса. Строка содержит зарезервированные переменные, которые будут заменены при отправке сообщения:</p> <ul style="list-style-type: none"> • {username} – имя пользователя; • {password} – пароль пользователя; • {encoding} – кодировка; • {sender} – идентификатор отправителя; • {message} – отправляемое сообщение; • {phonenumber} – список телефонных номеров (разделены запятыми), на которые будет отправлено сообщение; • {phone} – телефонный номер, на который будет отправлено сообщение; <p>Пример формата параметров запроса: <code>login={username}&psw={password}&charset={encoding}&phones={phonenumber}&mes={message}&sender={sender}</code></p>

9. Для добавления в список профиля SMPP-транспорта нажмите кнопку  (Рис. 26, с. 40) и выберите **Профиль провайдера Smpp**.

Отобразится следующее окно.

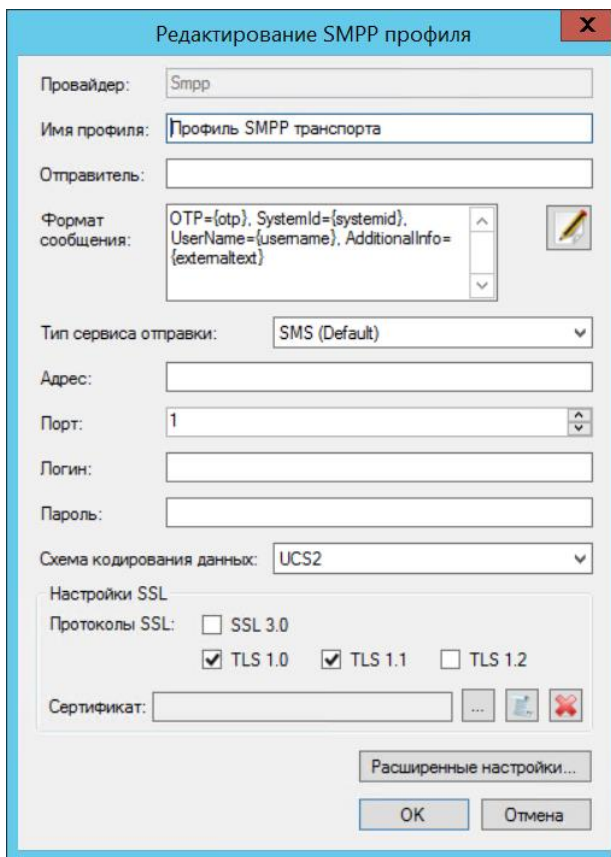






Рис. 29 – Настройки профиля SMPP-транспорта

10. Выполните настройку профиля, руководствуясь Табл. 17.

Табл. 17 – Настройка SMPP-транспорта сообщений

Настройка	Описание
Провайдер	Тип доставки сообщения – SMPP (доставка сообщений по протоколу SMPP). Неизменяемое поле
Имя профиля	Имя профиля, которое будет отображаться в списке профилей
Отправитель	Идентификатор отправителя – имя, которое будет указано в качестве отправителя сообщения. В общем случае это имя регистрируется у операторов связи (в настройках учетной записи пользователя SMS-шлюза)

Настройка	Описание
<p>Формат сообщения</p>	<p>Формат строки сообщения, отправляемого через SMS-шлюз. Содержит зарезервированные переменные, которые будут заменены при отправке данного сообщения:</p> <ul style="list-style-type: none"> • {otp} – сгенерированный одноразовый пароль; • {systemid} – идентификатор внешней системы; • {username} – имя пользователя; • {externaltext} – строка, передаваемая внешней системой. <p> Для редактирования формата нажмите  .</p> <p>Формат сообщения по умолчанию:</p> <pre>OTP={otp}, SystemId={systemid}, UserName={username}, AdditionalInfo={externaltext}</pre>
<p>Тип сервиса отправки</p>	<p>Выберите тип сервиса отправки сообщений по SMPP.</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • SMS (по умолчанию) • USSD <p> Примечания:</p> <ol style="list-style-type: none"> 1. При выборе значения USSD, необходимо убедиться в поддержке сервиса USSD со стороны шлюза. 2. При выборе значение USSD на SMS-шлюз также передается код команды USSD, значение которой задается в конфигурационном файле <каталог установки JAS Server>\Aladdin.JAS.Engine.exe.config: <pre><appSettings> ... <add key="USSDParamValue" value=="3" /> ...</pre>
<p>Адрес</p>	<p>Адрес подключения к серверу SMPP</p>
<p>Порт</p>	<p>Порт подключения к серверу SMPP</p>
<p>Логин</p>	<p>Имя пользователя для проверки подлинности отправителя (параметр SystemId протокола SMPP).</p> <p>Это поле является обязательным и должно иметь непустое значение</p>
<p>Пароль</p>	<p>Пароль пользователя</p>
<p>Схема кодирования данных</p>	<p>Выберите тип кодировку передаваемых сообщений</p>
<p>Настройки SSL</p>	<p>Выберите протоколы безопасного соединения, которые могут применяться для связи с сервером SMPP. Допускается одновременный выбор следующих протоколов:</p> <ul style="list-style-type: none"> • SSL 3.0 • TLS 1.0 • TLS 1.1 • TLS 1.2 <p>При поддержке протокола с серверной и клиентской стороны, будет выбран протокол наиболее поздней версии</p>

Настройка	Описание
Сертификат	Если необходимо установить двустороннюю аутентификацию по SSL/TLS, выберите клиентский сертификат
Расширенные настройки	Кнопка вызова интерфейса расширенных настроек протокола SMPP.  Примечание. Параметры расширенных настроек SMPP имеют предустановленные значения по умолчанию, изменять которые без необходимости не рекомендуется

11. При необходимости выполнить расширенные настройки SMPP нажмите **Расширенные настройки**.
Отобразится следующее окно.

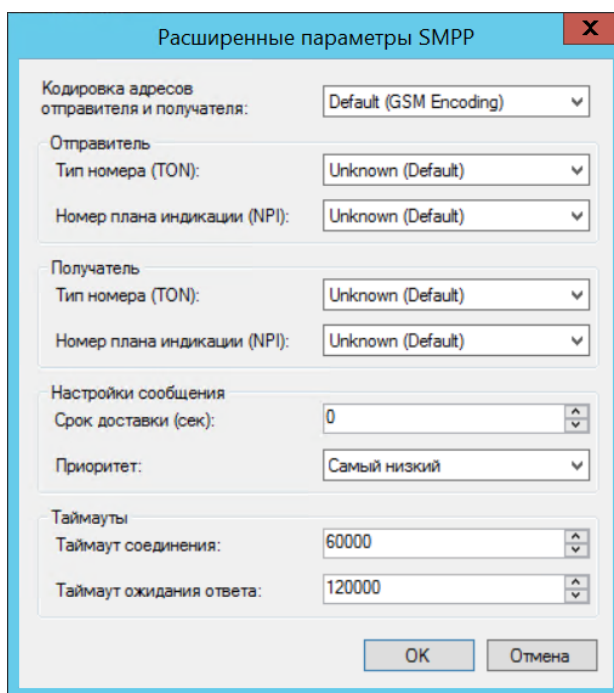


Рис. 30 – Расширенные настройки профиля SMPP-транспорта

12. Выполните настройку профиля, руководствуясь Табл. 18.



Табл. 18 – Расширенные настройки SMPP-транспорта сообщений

Настройка	Описание
Кодировка адресов отправителя и получателя	Задаёт кодировку строки адреса получателя и приемника сообщений
Тип номера (TON) (отправителя)	Задаёт тип номера отправителя
Номер плана индикации (NPI) (отправителя)	Задаёт номер плана индикации отправителя

Настройка	Описание
Тип номера (TON) (получателя)	Задаёт тип номера получателя
Номер плана индикации (NPI) (получателя)	Задаёт номер плана индикации получателя
Срок доставки (сек) (настройки сообщения)	Время (в секундах), в течение которого сервер будет пытаться передать сообщение, если оно еще не передано
Приоритет (настройки сообщения)	Приоритет передаваемого сообщения. Доступные значения: <ul style="list-style-type: none"> • Самый низкий • Низкий • Высокий • Самый высокий
Таймаут соединения	Время (в миллисекундах), в течение которого клиент будет пытаться установить соединение
Таймаут ожидания ответа	Время (в миллисекундах) ожидания ответа от сервера на переданный пакет данных

13. Нажмите **OK** дважды, чтобы сохранить изменения.

14. Для удаления или редактирования профиля транспорта сообщений выберите его из списка

(Рис. 26, с. 40) и нажмите соответственно кнопку  или  .

12.2.3.2 Настройки U2F

15. Выберите вкладку **Настройки U2F** (Рис. 31).

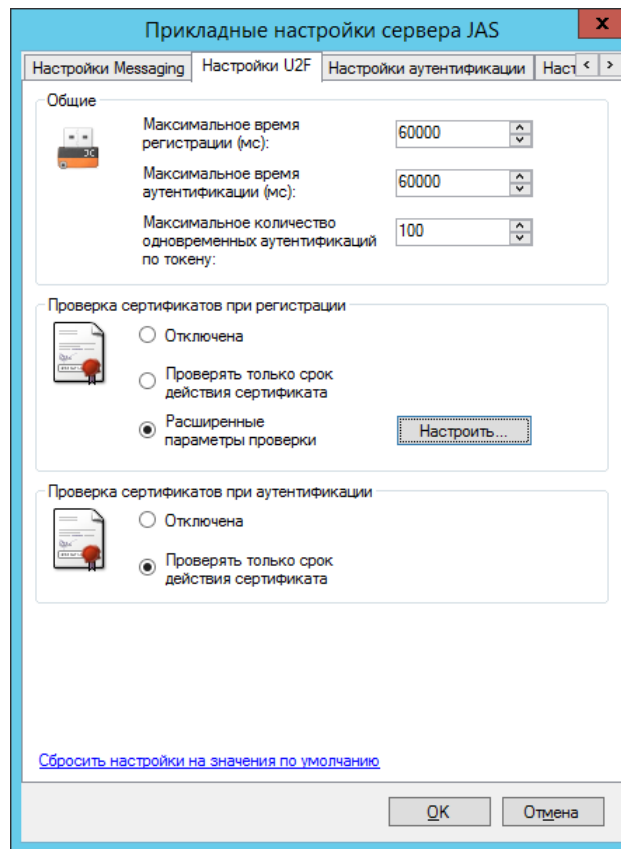


Рис. 31 – Настройки U2F

16. Выполните настройку, руководствуясь Табл. 19.

Табл. 19 – Настройки U2F

Настройка	Описание
Максимальное время регистрации (мс)	<p>Максимальное время (в миллисекундах), в течение которого начатая процедура регистрации может быть завершена успешно. Если в течение данного времени начатая процедура регистрации не завершилась, то она считается устаревшей и заканчивается с ошибкой (регистрация не выполняется). Сообщение об ошибке записывается в журналы BusinessLogic.log, Engine.log.</p> <p>Значение по умолчанию: 60000</p>
Максимальное время аутентификации (мс)	<p>Максимальное время (в миллисекундах), в течение которого начатая процедура аутентификации может быть завершена успешно. Если в течение данного времени начатая процедура аутентификации не завершилась, то она считается устаревшей и заканчивается с ошибкой (аутентификация не выполняется). Сообщение об ошибке записывается в журналы BusinessLogic.log, Engine.log.</p> <p>Значение по умолчанию: 60000</p>

Настройка	Описание
Максимальное количество одновременных аутентификаций по токenu	Максимальное количество одновременных аутентификаций по данному U2F-аутентификатору. Значение по умолчанию: 100
Проверка сертификатов при регистрации	Настройка проверки аттестационных сертификатов U2F-устройства в процессе регистрации U2F-аутентификатора. Предоставляет три варианта: <ul style="list-style-type: none"> • Отключена – проверка аттестационного сертификата не выполняется • Проверять только срок действия сертификата • Расширенные параметры проверки – производится проверка сертификата в соответствии с полями окна расширенной проверки (Рис. 32). Окно расширенной проверки вызывается нажатием кнопки Настроить...
Проверка сертификатов при аутентификации	Настройка проверки аттестационных сертификатов U2F-устройства в процессе аутентификации с использованием U2F-аутентификатора. Предоставляет два варианта: <ul style="list-style-type: none"> • Отключена – проверка аттестационного сертификата не выполняется • Проверять только срок действия сертификата

17. В случае необходимости выполните расширенную настройку проверки аттестационных сертификатов U2F-устройства для процедуры регистрации U2F-аутентификатора. Для этого следует нажать кнопку **Настроить...** на панели **Проверка сертификата при регистрации** (Рис. 31). Откроется следующее окно:

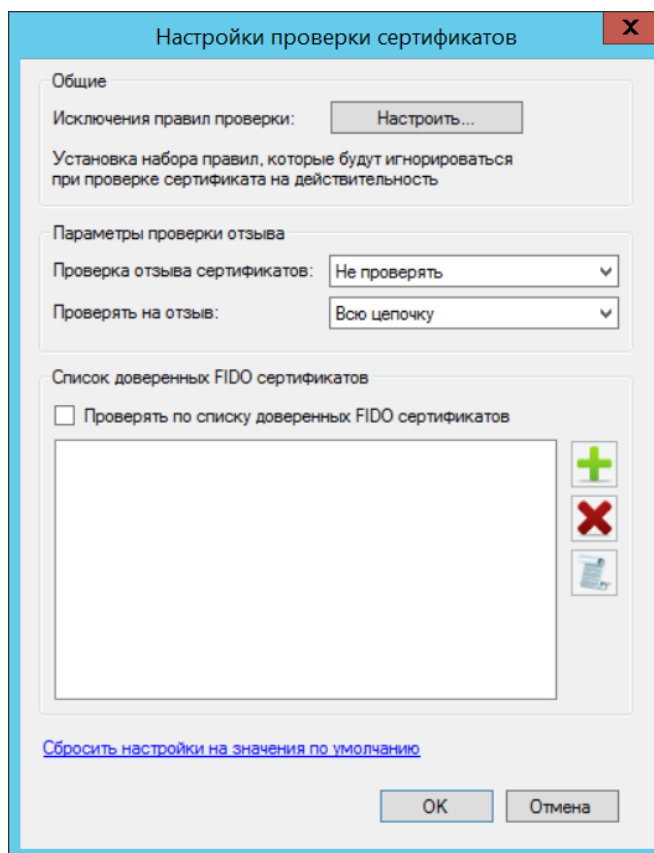


Рис. 32 – Окно настройки расширенной проверки аттестационного сертификата

18. Выполните настройку, руководствуясь Табл. 20.

Табл. 20 – Настройки проверки аттестационных сертификатов U2F-устройств






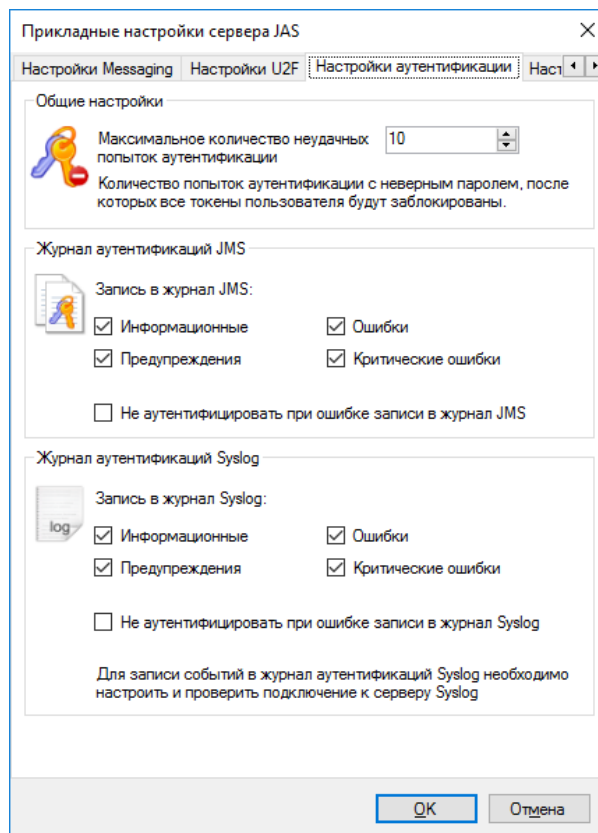
Настройка	Описание
Исключения правил проверки	<p>При нажатии на кнопку Настроить..., располагающейся в данном поле, раскроется окно Выберите флаги со списком флагов для отключения правил проверки на действительность сертификатов X.509.</p> <p>Каждый флаг соответствует одному элементу набора атрибутов <i>System.Security.Cryptography.X509Certificates.X509VerificationFlags</i> платформы .NET компании Microsoft, см. Табл. 21 (подробное описание атрибутов содержится в документации Microsoft, см. веб-ресурс [1], с. 155).</p> <p> Для выполнения проверки аттестационного сертификата U2F-устройства корневые и дочерние сертификаты должны быть предварительно загружены в Windows в хранилище сертификатов пользователя, от имени учетной записи которого осуществляется запуск сервера JAS</p>
Проверка отзыва сертификатов	<p>Поле определяет обязательность и способ проверки сертификата на отзыв по спискам отзыва сертификатов. Поле предлагает 3 варианта настройки:</p> <ul style="list-style-type: none"> • Не проверять • Онлайн – проверять сертификат в интерактивном режиме • Оффлайн – проверять сертификат на основе загруженных списков отзывов сертификатов
Проверять на отзыв	<p>Поле определяет необходимость и способ проверки на отзыв цепочки сертификатов. Предлагается 3 варианта настройки:</p> <ul style="list-style-type: none"> • Конечный сертификат – выполняется проверка на отзыв только аттестационного сертификата U2F-устройства; • Всю цепочку – выполняется проверка на отзыв цепочки сертификатов; • Всю цепочку, кроме корневого – выполняется проверка на отзыв всех сертификатов в цепочке, кроме корневого
Проверять по списку доверенных FIDO сертификатов	<p>Флаг, устанавливающий необходимость проверять аттестационный сертификат с использованием списка загруженных доверенных сертификата альянса FIDO</p> <p> Примечания:</p> <ol style="list-style-type: none"> 1. Проверка с использованием списка доверенных FIDO-сертификатов заключается в проверке наличия аттестационного сертификата U2F-устройства в этом списке. 2. Доверенные FIDO-сертификаты должны быть предварительно загружены. У сертификатов, используемых для проверки, должен быть установлен флажок слева. 3. Настройки проверки сертификатов на панелях Общие и Параметры проверки отзыва (Рис. 32) не распространяются на проверку с помощью списка доверенных FIDO-сертификатов
Список доверенных FIDO сертификатов	<p>Поле содержит список доверенных сертификатов альянса FIDO. Справа от списка расположены кнопки управления:</p> <ul style="list-style-type: none"> •  – кнопка добавления доверенного сертификата FIDO в список; •  – кнопка удаления сертификата; •  – кнопка просмотра загруженного сертификата. <p>Каждый загруженный сертификат можно включить/исключить из списка, устанавливая/сбрасывая флажок слева от строки с сертификатом</p>

Табл. 21 – Настройки исключений проверок сертификата

Флаг исключения проверки сертификата	Атрибут X509VerificationFlags платформы .NET
Игнорировать истекшее время при проверке	IgnoreNotTimeValid
Игнорировать списки CTL с истекшим временем	IgnoreCtlNotTimeValid
Игнорировать временную вложенность сертификатов	IgnoreNotTimeNested
Игнорировать базовые ограничения проверки	IgnoreInvalidBasicConstraints
Игнорировать неизвестные центры сертификации	AllowUnknownCertificateAuthority
Игнорировать недопустимый тип использования сертификата	IgnoreWrongUsage
Игнорировать недопустимое имя при проверке	IgnoreInvalidName
Игнорировать недопустимые политики при проверке	IgnoreInvalidPolicy
Игнорировать, что отзыв конечного сертификата неизвестен	IgnoreEndRevocationUnknown
Игнорировать, что отзыв подписчика сертификата неизвестен	IgnoreCtlSignerRevocationUnknown
Игнорировать неизвестные отзывы центров сертификации	IgnoreCertificateAuthorityRevocationUnknown
Игнорировать неизвестный отзыв корневого сертификата	IgnoreRootRevocationUnknown






12.2.3.3 Настройки аутентификации


19. Выберите вкладку **Настройки аутентификации** (Рис. 33).

Рис. 33 – Вкладка **Настройка аутентификации**


20. Выполните настройку, руководствуясь Табл. 22.

Табл. 22 – Настройки аутентификации

Настройка	Описание
<Секция> Общие настройки	
Максимальное количество неудачных попыток аутентификации	<p>Количество попыток аутентификации пользователя при вводе им неверного одноразового пароля, после которых все OTP-токены данного пользователя будут заблокированы.</p> <p> Примечания:</p> <ol style="list-style-type: none"> 1. Значение параметра является централизованным для JMS и действует на все OTP-токены независимо от момента их выпуска. 2. Для каждого OTP-токена пользователя ведется отдельный счетчик оставшихся попыток аутентификации, значение которых одновременно уменьшается на единицу при каждой попытке аутентификации данным пользователем с неверным одноразовым паролем. В случае если у одного из OTP-токенов, принадлежащих пользователю, обнуляется число попыток аутентификации, то блокируются (т.е. приобретают статус Отключен с причиной блокировки Попытка перебора) все остальные OTP-токены, принадлежащие данному пользователю. Для разблокировки OTP-токенов следует выполнить операцию включения отдельно для каждого из токенов пользователя (см. раздел «Включение и отключение OTP-токена» в руководстве по функциям управления JMS, [3]). 3. В случае если значение параметра будет уменьшено администратором JMS в процессе эксплуатации ранее выпущенных токенов, и при этом счетчик попыток у какого-либо токена, принадлежащих пользователю, превысит новое значение параметра, блокировка всех токенов данного пользователя произойдет при следующей неудачной попытке аутентификации данным пользователем с помощью OTP-токена. <p>Значение по умолчанию – 100.</p>
<Секция> Журнал аутентификаций JMS	
Запись в журнал JMS	<p>Выполните настройку записи событий в Журнал аутентификации JMS (подробнее см. руководство по функциям управления JMS [3]).</p> <p>Флаги настройки:</p> <ul style="list-style-type: none"> • Информационные – запись в журнал сообщений об успешной аутентификации (значок ) • Предупреждения – запись в журнал предупреждений (значок ) • Ошибки – запись в журнал сообщений об ошибках аутентификации (значок ) • Критические ошибки – запись в журнал сообщений о критически важных событиях (значок ) <p>По умолчанию все флаги установлены.</p>
Не аутентифицировать при сбое записи в журнал JMS	<p>Установленный флаг обеспечивает блокировку аутентификации пользователей с использованием OTP-токенов (всех типов) и U2F-аутентификаторов при сбоях записи в журнал аутентификации JMS</p> <p>По умолчанию флаг не установлен.</p>

Настройка	Описание
<Секция> Журнал аутентификаций Syslog	
Запись в журнал Syslog	<p>Выполните настройку записи событий в журнал аутентификации Syslog (подробнее см. руководство по функциям управления JMS [3]).</p> <p>Флаги настройки:</p> <ul style="list-style-type: none"> • Информационные – запись в журнал сообщений об успешной аутентификации; • Предупреждения – запись в журнал предупреждений; • Ошибки – запись в журнал сообщений об ошибках аутентификации; • Критические ошибки – запись в журнал сообщений о критически важных событиях; <p>По умолчанию все флаги установлены.</p> <p> Примечание. Настройки параметров подключения к серверу Syslog выполняются на вкладке Настройки Syslog (см. «Настройки Syslog», below).</p>
Не аутентифицировать при сбое записи в журнал Syslog	<p>Установленный флаг обеспечивает блокировку аутентификации пользователей с использованием OTP-токенов (всех типов) и U2F-аутентификаторов при сбоях записи в журнал аутентификации Syslog.</p> <p>По умолчанию флаг не установлен.</p>

12.2.3.4 Настройки Syslog

 **Примечание.** Включение/отключение записи событий аутентификации на сервер Syslog осуществляется на вкладке **Настройки аутентификации** (см. «Настройки аутентификации», с. 53).

21. Выберите вкладку **Настройки Syslog** (Рис. 34).

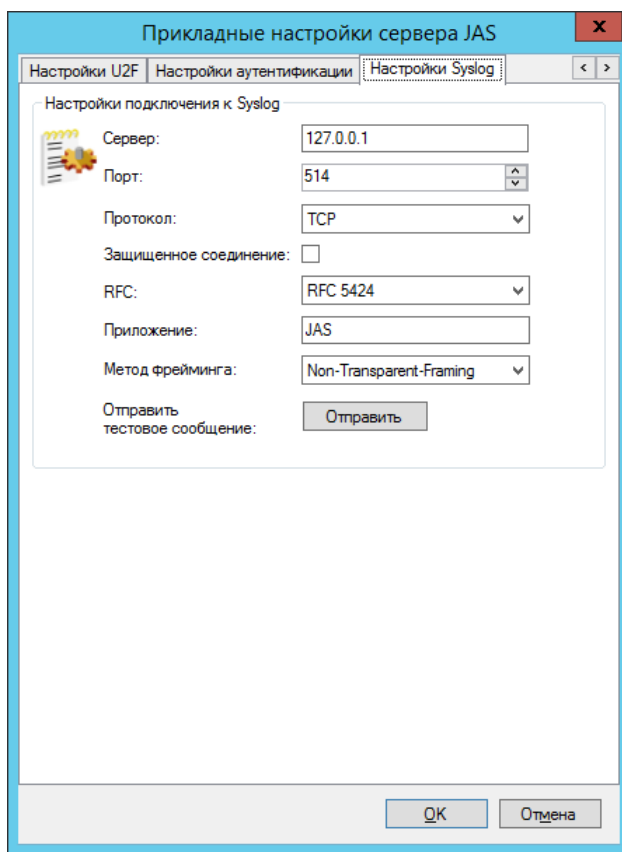



Рис. 34 – Вкладка Настройка Syslog

22. Выполните настройку, руководствуясь Табл. 23.

Табл. 23 – Настройки журнала аутентификаций

Настройка	Описание
Сервер	Укажите IP-адрес или полное доменное имя (FQDN) Syslog-сервера.
Порт	Выберите порт подключения к почтовому Syslog-серверу.
Протокол	Выберите протокол транспортного уровня для работы с Syslog. Возможные варианты: <ul style="list-style-type: none"> • TCP (по умолчанию) • UDP
Защищенное соединение	Установите флаг, если для связи с Syslog-сервером необходимо использовать защищенное (SSL/TLS) соединение. Опция доступна только при использовании протокола TCP.
RFC	Выберите спецификацию Syslog для работы с сервером. Возможные варианты: <ul style="list-style-type: none"> • RFC 5424 (по умолчанию) • RFC 3164

Настройка	Описание
	 Примечание. Рекомендуется использовать RFC5424, т.к. стандарт RF3164 подразумевает, что сообщение может содержать только печатные символы из таблицы ASCII с кодами в диапазоне от 32 до 126. При выборе RFC3164 невозможна передача кириллицы
Приложение	<p>Текстовый идентификатор приложения (используется в выходных данных Syslog для идентификации приложения)</p> <p>Нередактируемое значение: JAS</p>
Метод фрейминга	<p>Метод определения границ сообщения в случае, если одновременно посылаются несколько сообщений</p> <p>Возможные варианты:</p> <ul style="list-style-type: none"> • Octet Counting (по умолчанию) – в начале каждого Syslog-сообщения устанавливается его длина для определения границ сообщения; • Not-Transparent-Framing – сообщения могут разделяться следующими символами: ASCII LF, ASCII NUL или последовательностью символов CR и LF
Отправить тестовое сообщение	<p>Нажмите кнопку с целью проверки корректности введенных данных в полях данного окна. При верных данных на сервер будет отправлено тестовое сообщение.</p>

23. По завершении настройки нажмите **ОК** два раза.

12.3 Безопасность

12.3.1 Общий вид вкладки Безопасность

Вкладка **Безопасность** выглядит следующим образом.

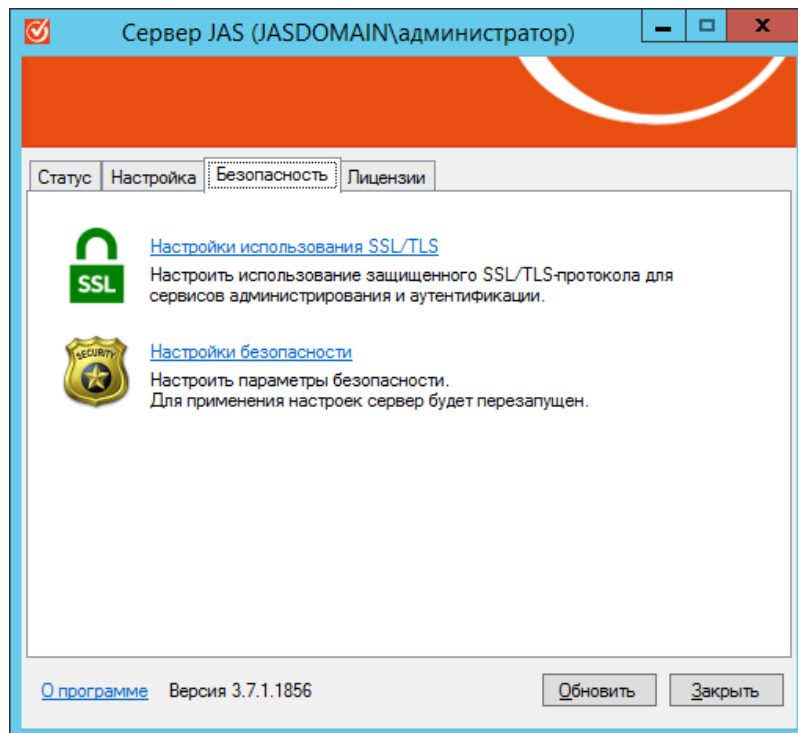


Рис. 35 – Вкладка Безопасность

Вкладка содержит следующие элементы (см. Табл. 24).

Табл. 24 – Элементы вкладки Безопасность

Элемент интерфейса	Описание
Ссылка Настройки протокола SSL/TLS	Управляет сертификатами SSL для программных интерфейсов JAS и позволяет установить/запретить использование протоколов SSL/TLS при исходящих соединениях – подробнее см. «Настройки использования SSL/TLS», с. 58.
Ссылка Настройки безопасности	Позволяет задать пароль шифрования для защиты базы данных JAS (подробнее см. «Настройки безопасности», с. 62)

12.3.2 Настройки использования SSL/TLS

Перед настройкой SSL в JAS необходимо выпустить сертификат сервера JAS (сертификат SSL может быть выпущен, например, с помощью Центра сертификации Microsoft по шаблону Компьютер). В случае если для подключения по SSL/TLS со стороны сервера JMS и клиентов планируется использовать разные сертификаты, нужно выпустить два сертификата.

Убедитесь, что в хранилище сертификатов на сервере JAS установлены необходимые сертификаты. Для этого выполните следующие действия.

1. Откройте окно хранилища сертификатов компьютера на сервере JAS.

2. В отобразившемся окне выберите **Сертификаты (локальный компьютер) -> Личное -> Сертификаты.**

Выпущенные сертификаты для поддержки SSL-соединения с сервером JAS (см. руководство по установке и настройке JMS [2], раздел «Выпуск сертификата в хранилище сертификатов компьютера») отобразится в списке сертификатов компьютера (Рис. 36).

Важно! В случае запуска службы сервера JAS от имени служебной учетной записи (а не системной Local System) SSL-сертификаты сервера (или SSL-сертификат кластерной роли, в случае кластера) следует поместить в личное хранилище пользователя, от имени которого будет запускаться служба сервера.

Примечания:

1. Для обеспечения возможности SSL-соединения сервера JAS с сервером JMS и клиентами (JAS-плагины NPS и AD FS) можно использовать как один сертификат, так и два разных сертификата, см. Табл. 25. В настоящем руководстве используется единый сертификат для обоих интерфейсов.
2. При настройке кластерной конфигурации JAS следует использовать сертификат, выпущенный для *кластерной роли*, созданной на этапе настройки отказоустойчивого кластера (см. «Настройка отказоустойчивого кластера JAS», с. 132).

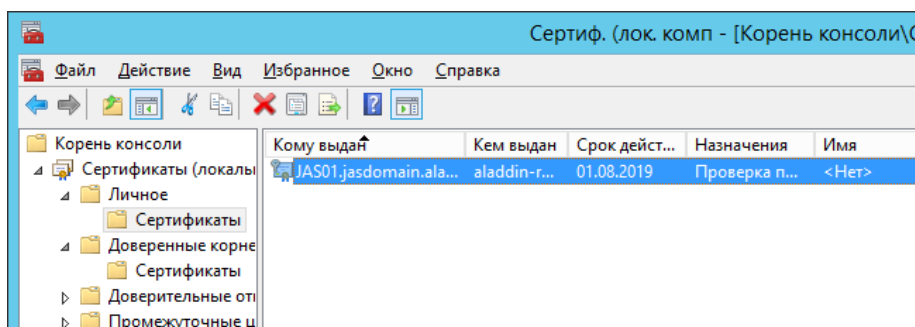


Рис. 36 – Проверка наличия SSL-сертификата в хранилище «Личное» локального компьютера

Чтобы настроить протоколы SSL/TLS выполните следующие действия.

1. В окне управления сервером JAS перейдите на вкладку **Безопасность** и нажмите **Настройки использования SSL/TLS.**

Отобразится окно следующего вида.

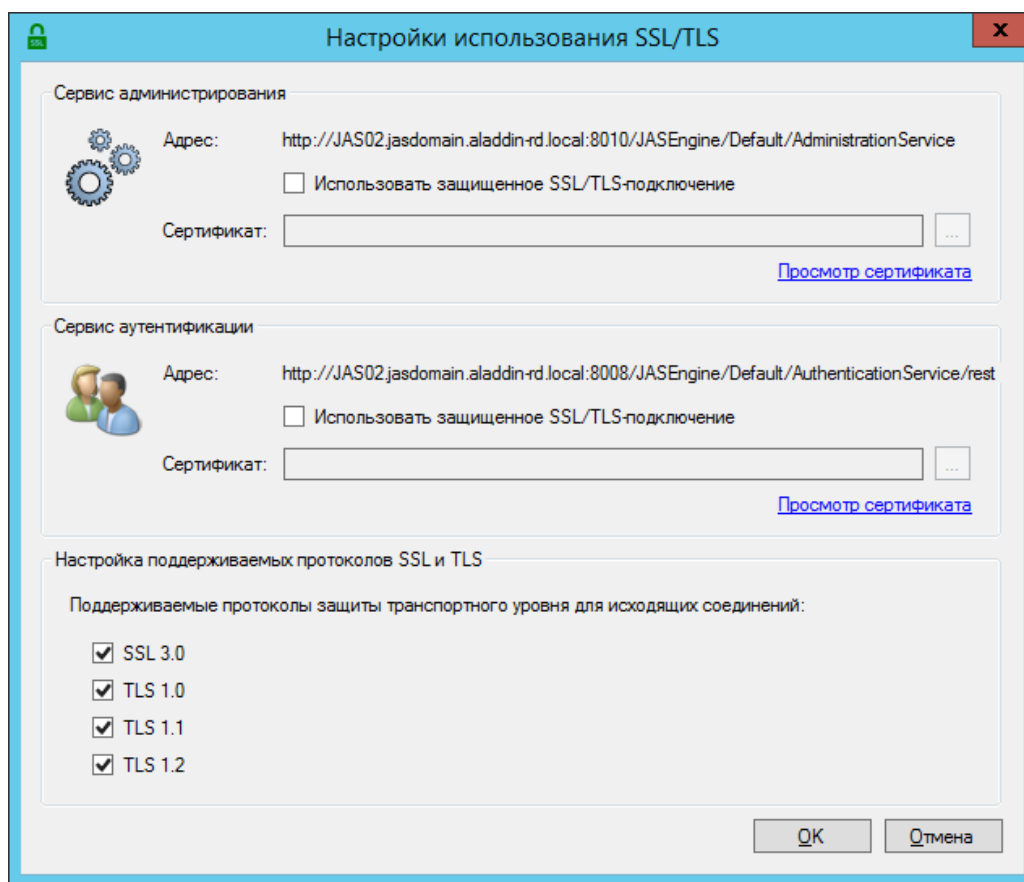







Рис. 37 – Настройки протокола SSL/TLS

2. Выполните настройки, руководствуясь Табл. 25.

Табл. 25 – Настройки использования SSL/TLS



Элемент интерфейса	Описание
<Секция> Сервис администрирования	
(API-интерфейс <i>AdministrationService</i> сервера JAS для взаимодействия с сервером JMS)	
Адрес	Адрес интерфейса сервиса администрирования (считывается из реестра)
Использовать защищенное SSL/TLS-подключение	Установите флаг, если соединение должно осуществляться по протоколу SSL/TLS
Сертификат	Нажмите кнопку  и выберите сертификат, который должен использоваться в протоколах SSL/TLS со стороны сервера JAS (Поле доступно для редактирования только при установленном флаге Использовать защищенное SSL/TLS-подключение)
Ссылка Просмотр сертификата	Нажмите для просмотра свойств установленного сертификата
<Секция> Сервис аутентификации	

Элемент интерфейса	Описание
	(API-интерфейс <i>AuthenticationService</i> сервера JAS для взаимодействия с взаимодействуют OTP-клиентами (например, с JAS-плагином для NPS);)
Адрес	Адрес сервиса аутентификации (считывается из реестра)
Использовать защищенное SSL-соединение	Установите флаг, если соединение должно осуществляться по протоколу SSL/TLS
Сертификат	Нажмите кнопку  и выберите сертификат, который должен использоваться в протоколах SSL/TLS со стороны сервера JAS (Поле доступно для редактирования только при установленном флаге Использовать защищенное SSL/TLS-подключение)
Ссылка Просмотр сертификата	Нажмите для просмотра свойств установленного сертификата
<Секция> Настройка поддерживаемых протоколов SSL и TLS	
Поддерживаемые протоколы защиты транспортного уровня для исходящих соединений	<p>Данная настройка предназначена для определения списка поддерживаемых протоколов защиты транспортного уровня и распространяется только на исходящие соединения (отправка почтовых уведомлений, соединение с внешними системами и др.). По умолчанию в компоненте JAS Server включены все предусмотренные в нем протоколы защиты транспортного уровня.</p> <p> Важно! Данная настройка не распространяется на подключения к СУБД MS SQL Server.</p> <p>При необходимости установите/сбросьте флаги протоколов, которые должны / не должны использоваться при исходящих соединениях с внешними системами. Доступные опции:</p> <ul style="list-style-type: none"> • SSL 3.0 • TLS 1.0 • TLS 1.1 • TLS 1.2 <p> Примечание. Настройка может быть востребована отдельными организациями, использующими JAS, в которых установлен организационный запрет на применение определенных (например устаревших) протоколов защиты данных.</p> <p> Важно! Настройка протоколов должна быть выполнена так, чтобы был разрешен хотя бы один из протоколов, установленных в связанном с JAS сервере JMS, т.е. на вкладке Безопасность серверного агента JMS. (см. руководство по установке и настройке JMS [2], раздел «Настройки протокола SSL/TLS»). Кроме того, должны быть установлены те протоколы, по которым будет осуществляться взаимодействие с клиентами JAS (NPS и ADFS, см. параметр SecurityProtocols в настройках соответствующих компонентов).</p>

3. Нажмите **ОК**, чтобы сохранить настройки.
4. При включении SSL-соединений будет произведена автоматическая перезагрузка службы сервера JAS.

12.3.3 Настройки безопасности

Для работы сервера JAS необходимо задать пароль шифрования, который будет использоваться для защиты данных в базе данных JAS. Чтобы сделать это, выполните следующие действия.

1. Нажмите правой кнопкой мыши на значке  (или ) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Безопасность**.
Окно примет следующий вид.

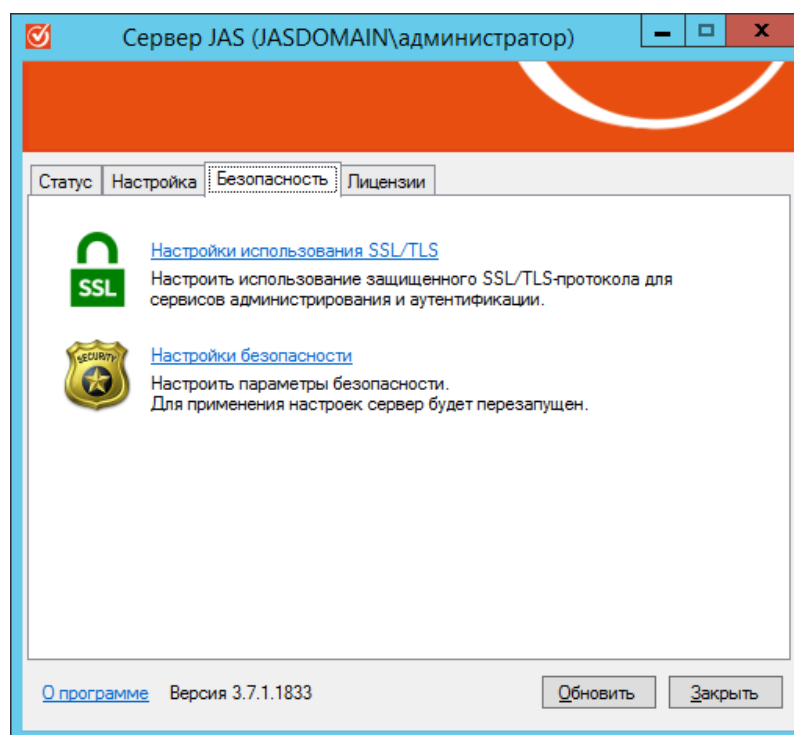


Рис. 38 – Вкладка Настройка

3. Нажмите **Настройка безопасности**.

Отобразится следующее окно.

Настройка безопасности

Настройка пароля шифрования

Пароль шифрования используется для защиты данных в БД. Он единожды задается при первоначальной настройке, и его дальнейшие изменения не подразумеваются.

Пароль не задан. Необходимо ввести новый пароль.

Пароль en

Пароль должен содержать не менее 2 символа(ов) нижнего регистра.

Подтверждение

OK Отмена

Рис. 39 – Задание пароля шифрования

4. В полях **Пароль** и **Подтверждение** задайте пароль шифрования и введите подтверждение соответственно. Пароль должен соответствовать следующим критериям:
- содержать как минимум 2 символа алфавита в верхнем регистре;
 - содержать как минимум 2 символа алфавита в нижнем регистре;
 - содержать как минимум 2 цифры;
 - содержать как минимум 2 символа, не входящих в алфавитно-цифровой набор;
 - должен быть не короче 20 символов.

После ввода пароля окно примет следующий вид.

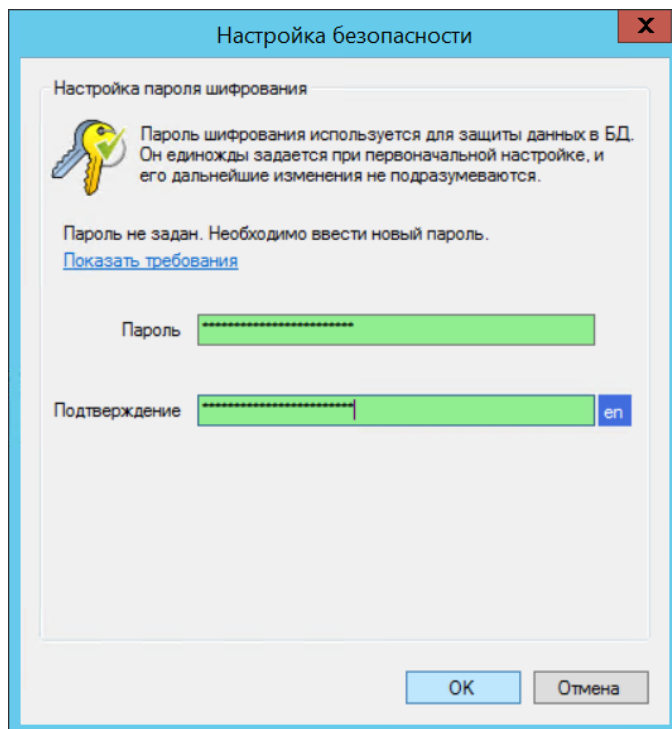


Рис. 40 – Пароль шифрования соответствует критериям безопасности

5. Нажмите **OK** для завершения процедуры.

12.4 Лицензии (проверка/просмотр лицензии на использование продукта JAS)

Лицензия на сервер JAS приобретается в составе «родительского» экземпляра сервера JMS (к которому подключается сервер JAS) и устанавливается в том же экземпляре сервера JMS (в приложении Сервер JMS, подробнее см. руководство по установке и настройке JMS [2], раздел «Лицензии (установка лицензии на JMS/JAS)»). Из серверного агента JAS (приложения Сервер JAS, Рис. 41, ниже) возможно только проверить наличие лицензии. Для этого откройте вкладку **Лицензии**. Корректно установленная лицензия подсвечивается зеленым цветом.

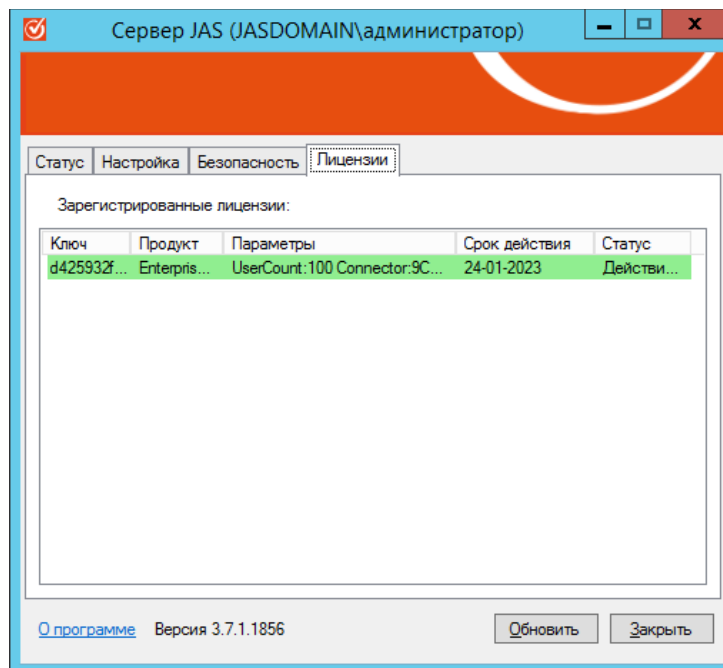


Рис. 41 – Вкладка **Лицензии** с корректно установленной лицензией



Без установки лицензии сервер JAS не может быть запущен (при нажатии на **Старт** на вкладке **Статус**, Рис. 12, с. 30, будет выведено соответствующее сообщение об ошибке).

13. Установка и настройка JAS-плагина для NPS

13.1 Подготовка сервера NPS

В настоящем подразделе приведены настройки сервера NPS, которые позволят проверить функциональность JAS-плагина для NPS из состава JAS. Вариант настроек приведён в качестве примера, в общем случае интеграции JAS с NPS настройки могут отличаться от приведенных в настоящем разделе.

13.1.1 Настройка политики запросов на подключение

Чтобы настроить политику запросов на подключение, выполните следующие действия.

1. Запустите оснастку сервера политики сети.

Окно оснастки будет выглядеть следующим образом.

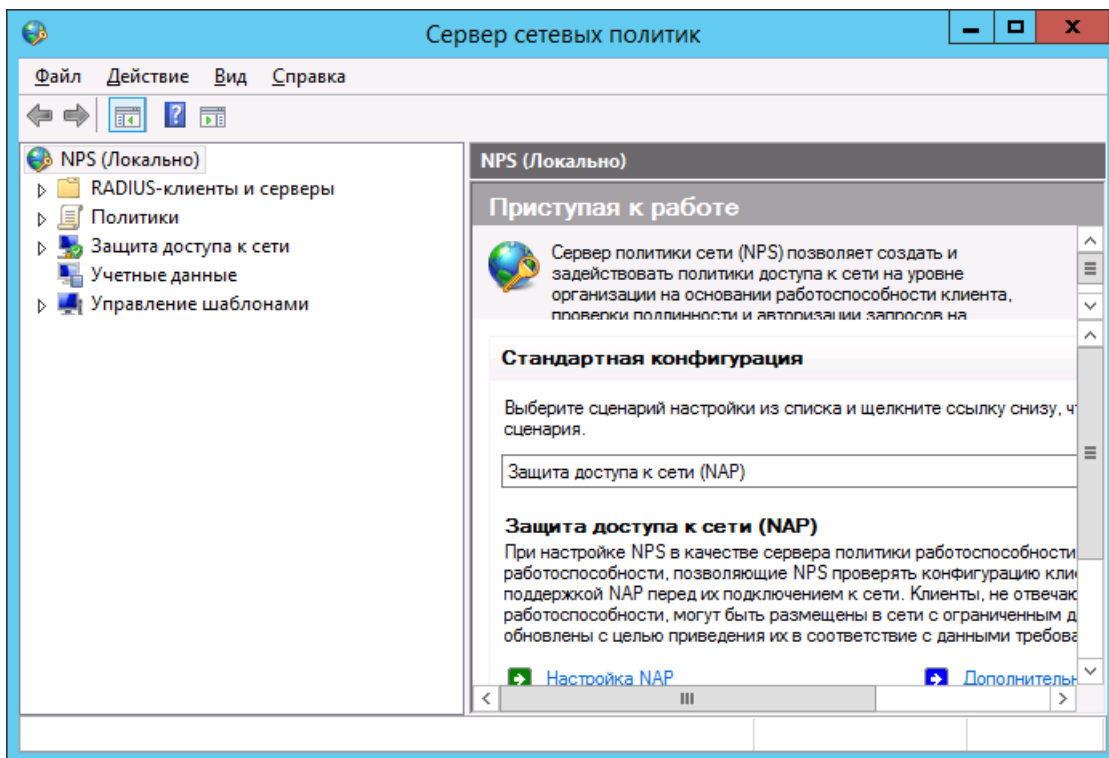


Рис. 42 – Оснастка сервера политики сети

2. Перейдите в раздел **Политики > Политики запросов на подключение** (см. рис. 43 ниже).

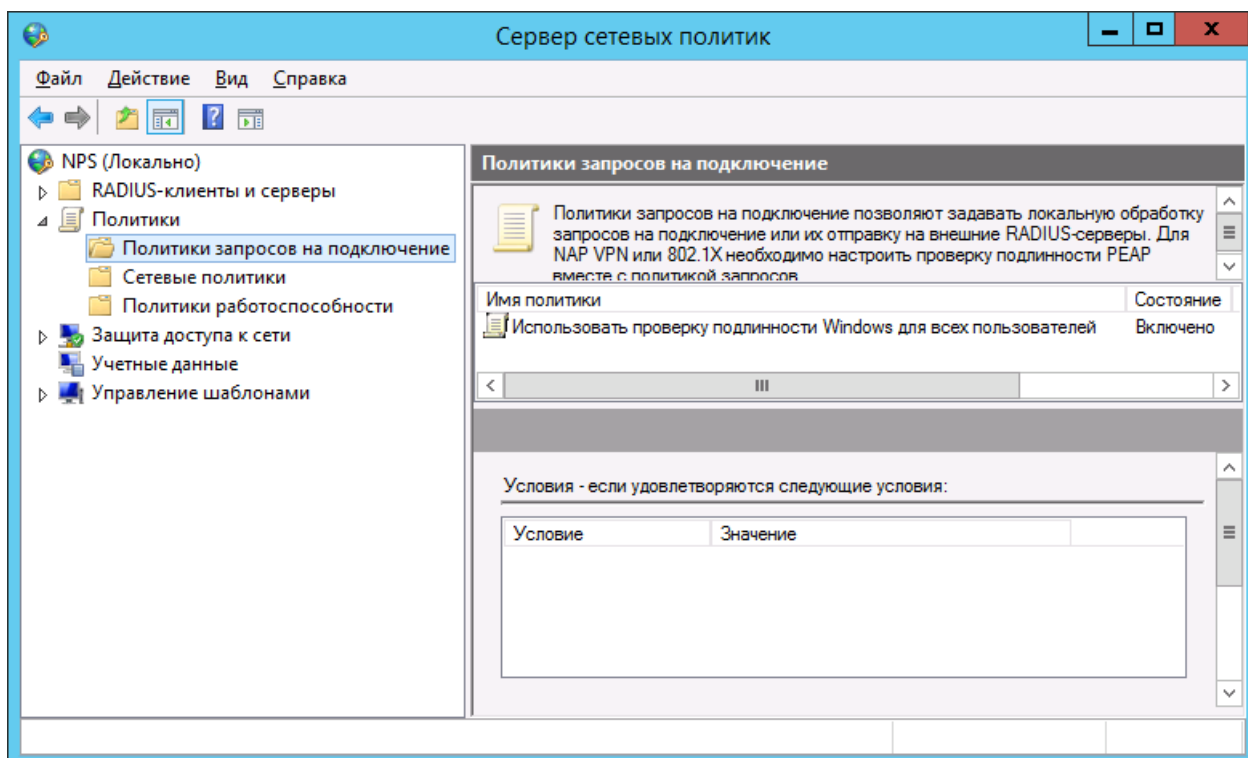


Рис. 43 – Политики запросов на подключение

3. В правой части окна нажмите правой кнопкой мыши на пункте **Использовать проверку подлинности Windows для всех пользователей** и выберите **Свойства**, как показано на рис. 44 ниже.

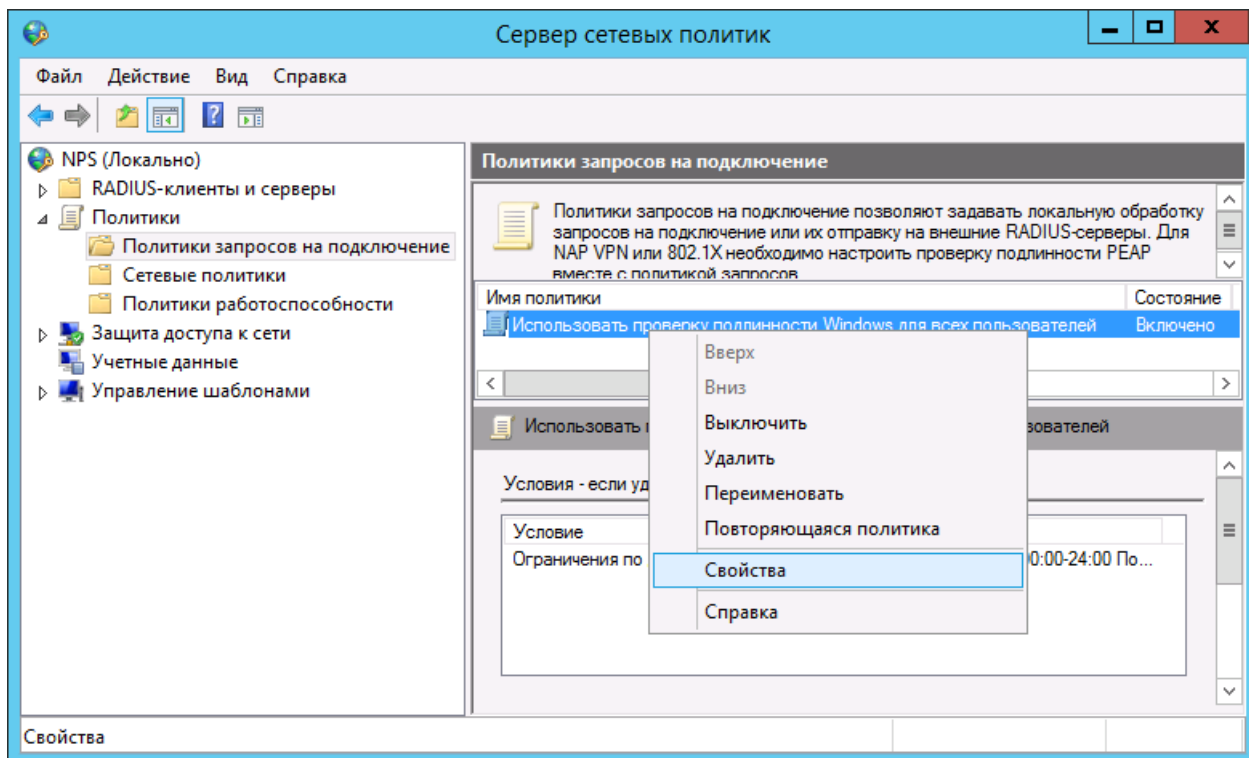


Рис. 44 – Отображение свойств политики запросов на подключение

Отобразится следующее окно.

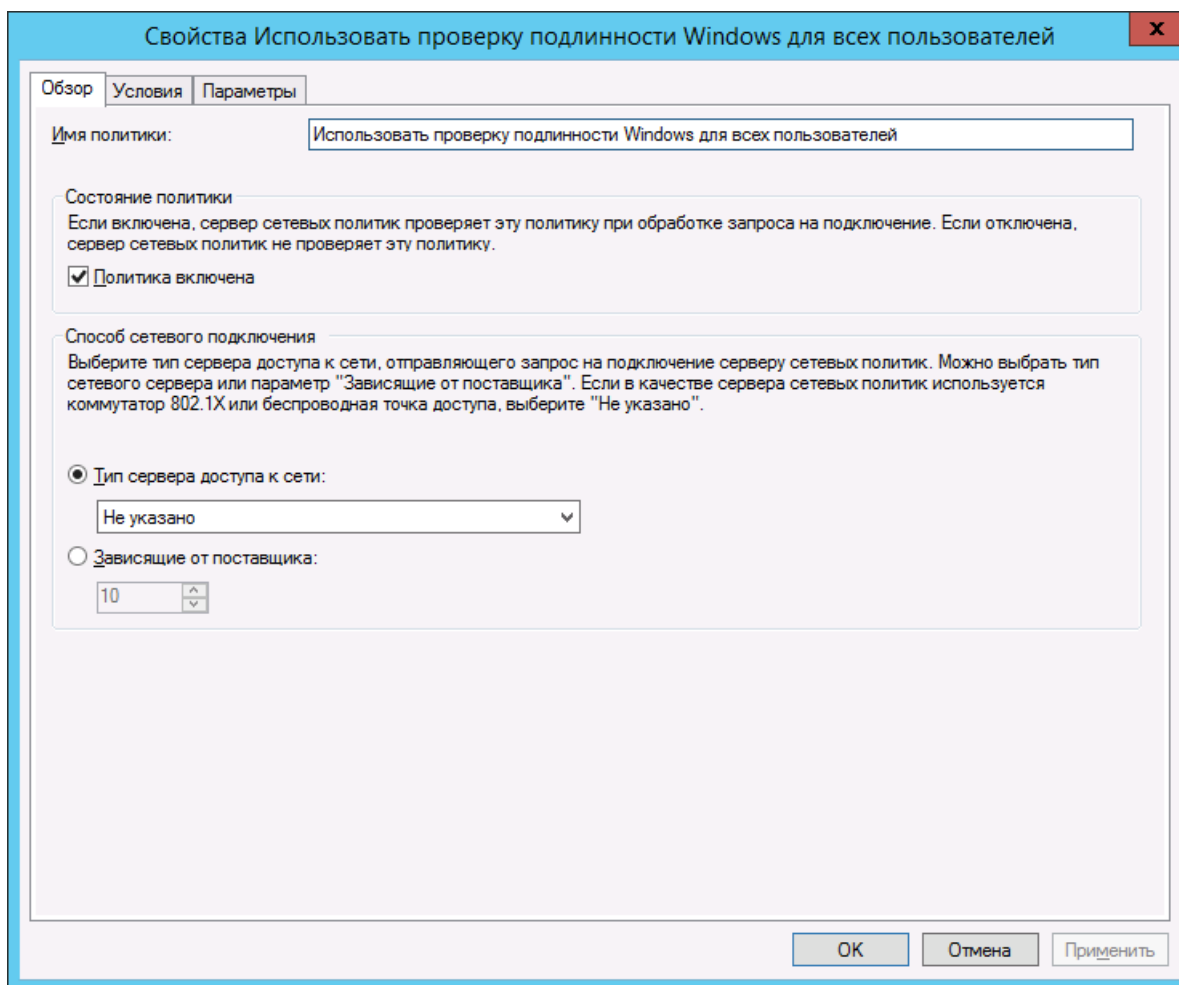


Рис. 45 – Вкладка **Общие**

4. Убедитесь в том, что флажок **Политика включена** установлен.
5. Перейдите на вкладку **Параметры**.

Окно примет следующий вид.

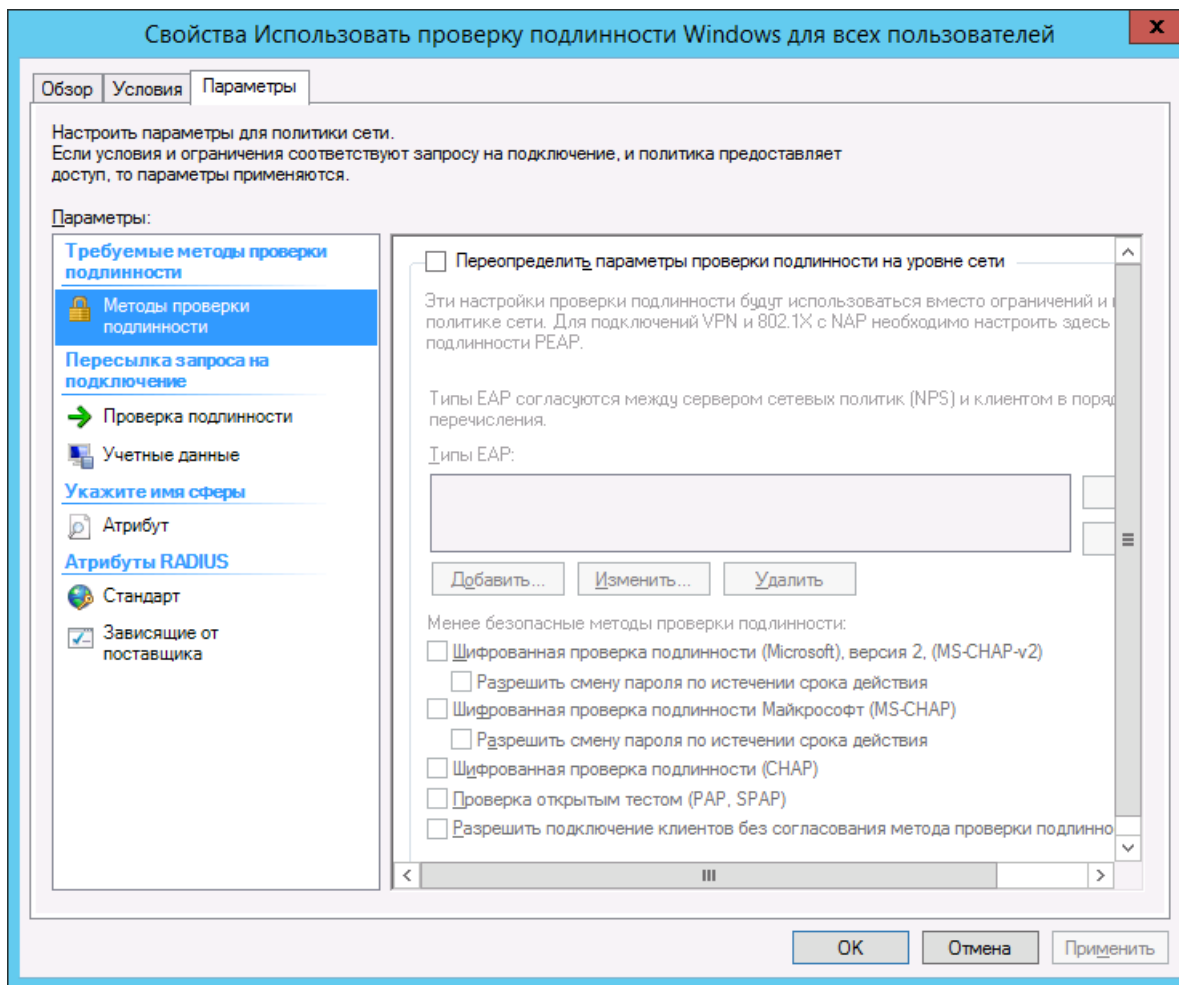


Рис. 46 – Вкладка **Параметры**

6. В левой части окна выберите пункт **Методы проверки подлинности**.
7. Выполните следующие настройки:
 - 7.1. установите флажок **Переопределить параметры проверки подлинности на уровне сети**;
 - 7.2. установите флажок **Проверка подлинности открытым тестом (PAP, SPAP)**.
8. Нажмите **ОК**.

Отобразится сообщение с предложением отобразить справку.

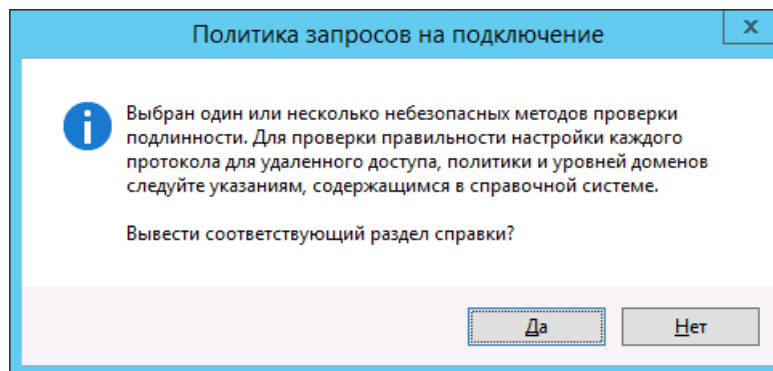


Рис. 47 – Сообщение с предложением отобразить справку

9. Нажмите **Нет**.

13.1.2 Настройка параметров RADIUS-клиента

Чтобы настроить параметры RADIUS-клиента, выполните следующие действия.

1. В оснастке сервера перейдите в раздел **RADIUS-клиенты и серверы** (см. рис. 48 ниже).

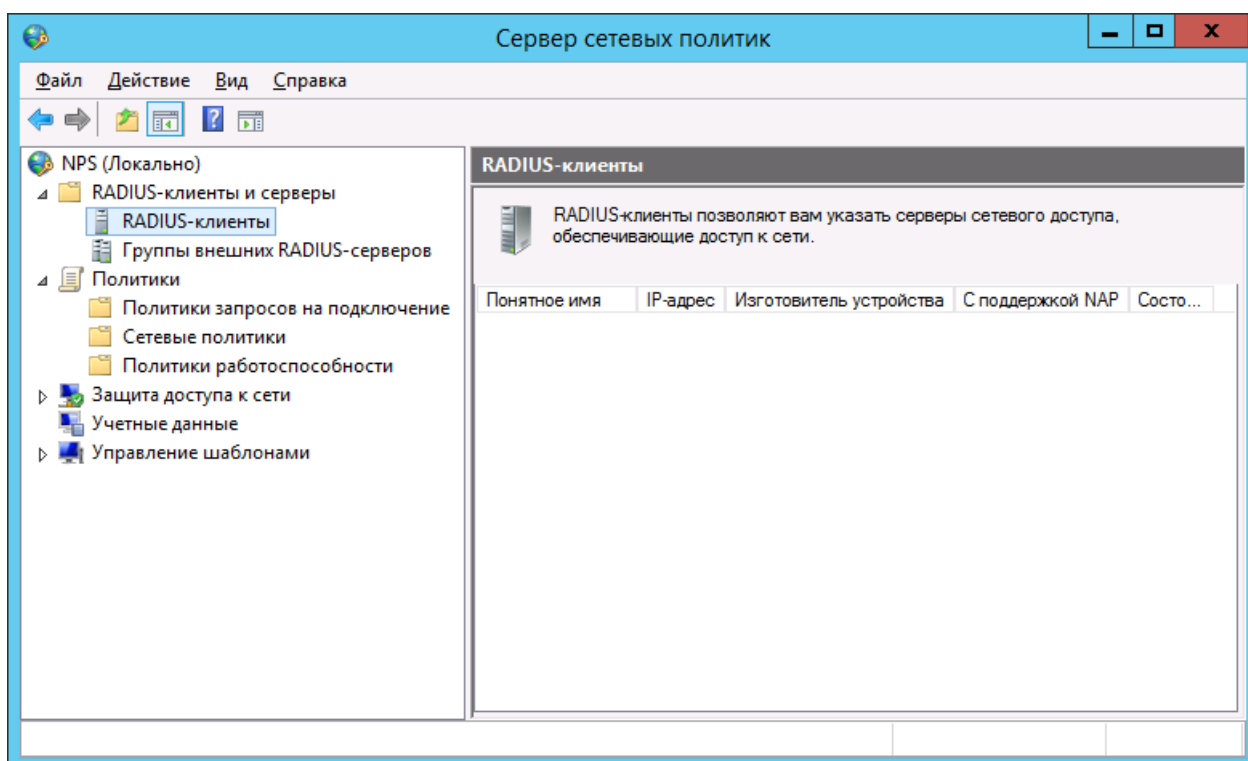


Рис. 48 - RADIUS-клиенты и серверы

2. Нажмите правой кнопкой мыши на пункте **RADIUS-клиенты** и выберите **Новый документ** (см. рис. 49 ниже).

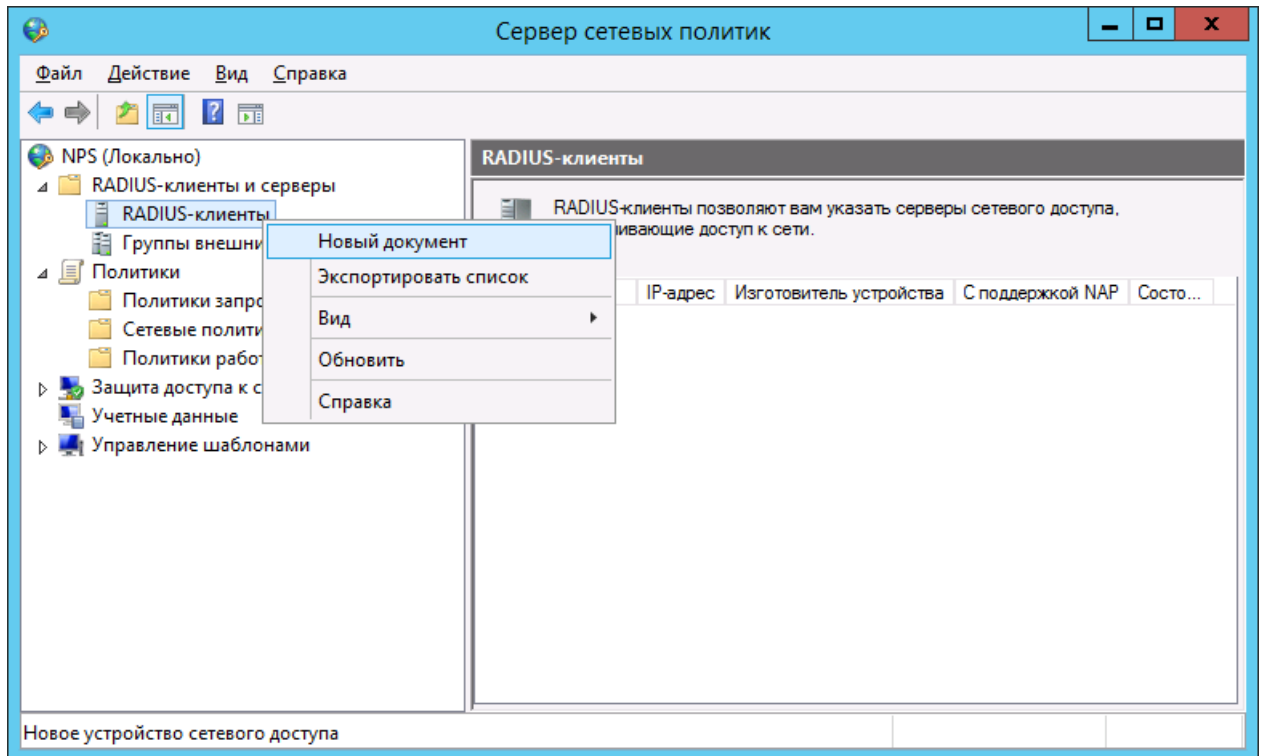


Рис. 49 - Создание RADIUS-клиента

Отобразится следующее окно.

Новый RADIUS-клиент

Параметры **Дополнительно**

Включить этот RADIUS-клиент

Выберите существующий шаблон:

Имя и адрес

Понятное имя:

Адрес (IP или DNS):

Общий секрет

Выберите существующий шаблон общих секретов:

Отсутствует

Чтобы ввести общий секрет вручную, щелкните "Вручную". Чтобы автоматически создать общий секрет, щелкните "Создать". Необходимо настроить RADIUS-клиент с введенным здесь общим секретом. В общих секретах учитывается регистр символов.

Вручную Создать

Общий секрет:

Подтверждение общего секрета:

Рис. 50 – Окно настроек RADIUS-клиента

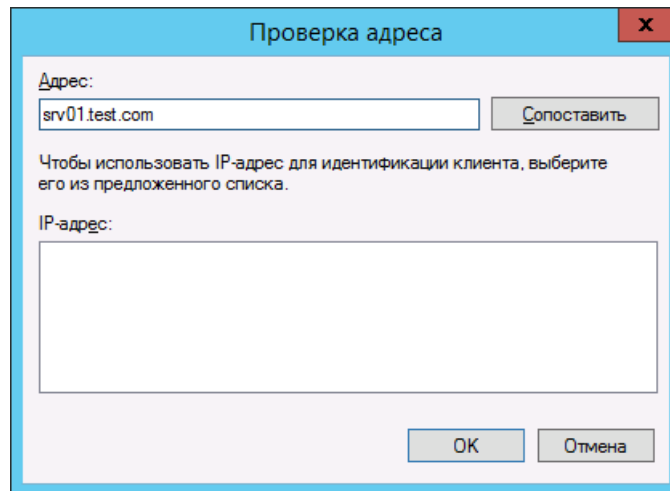
3. Убедитесь в том, что флажок **Включить этот RADIUS-клиент** установлен.
4. В поле **Понятное имя** введите имя RADIUS-клиента (это может быть любое значение).
5. В поле **Адрес (IP или DNS)** введите IP-адрес или NetBIOS-имя сервера RADIUS-клиента.



Примечание. Под RADIUS-клиентом подразумевается конечный прикладной сервис (например сервис Citrix, или, как в примере для настоящего руководства, – программа NtRadPing), с которого осуществляются запросы к серверу NPS, а не сервер JAS. Хотя в частном случае в качестве хоста для RADIUS-клиента может использоваться и компьютер, на котором установлен сервер JAS.

6. Чтобы открыть окно проверки введенного адреса, нажмите кнопку **Проверить**.

Отобразится следующее окно.



Проверка адреса

Адрес:
srv01.test.com

Сопоставить

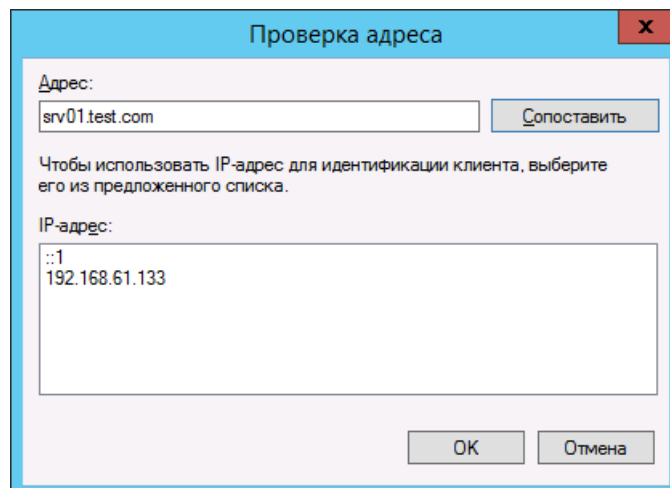
Чтобы использовать IP-адрес для идентификации клиента, выберите его из предложенного списка.

IP-адрес:

OK Отмена

Рис. 51 – Проверка адреса

7. Чтобы сопоставить DNS-имя с IP-адресом RADIUS-клиента, нажмите кнопку **Сопоставить**. При успешном сопоставлении IP-адрес отобразится в соответствующем поле.



Проверка адреса

Адрес:
srv01.test.com

Сопоставить

Чтобы использовать IP-адрес для идентификации клиента, выберите его из предложенного списка.

IP-адрес:
::1
192.168.61.133

OK Отмена

Рис. 52 – Проверка адреса успешна

8. Нажмите **OK**.

Окно настройки RADIUS-клиента будет выглядеть следующим образом.

Рис. 53 – Окно настройки RADIUS-клиента

9. В секции **Общий секрет** выполните следующие действия:

- 9.1. выберите пункт **Вручную**;
- 9.2. в полях **Общий секрет** и **Подтверждение общего секрета** введите секретное значение и его подтверждение соответственно.



Важно!

1. Это общее значение для NPS-сервера и RADIUS-клиента. Сохраните его в надёжном месте.
2. Строка общего секрета не должна начинаться с цифры или специального символа, что связано с особенностями работы криптоалгоритмов сервера NPS компании Microsoft (наличие цифры или спецсимвола в начале строки приводит к ошибкам при расшифровке секрета на стороне NPS и последующей ошибке аутентификации). Общий секрет может начинаться только со строчной или прописной буквы латинского алфавита.
3. В случае смены общего секрета в процессе настроек сервиса следует перезагрузить компьютер, на котором функционирует служба (сервер) NPS, в противном случае возможна некорректная работа сервиса (связано с особенностью реализации продукта Microsoft).

10. Нажмите **ОК**.

Созданный RADIUS-клиент отобразится в оснастке сервера политики сети.

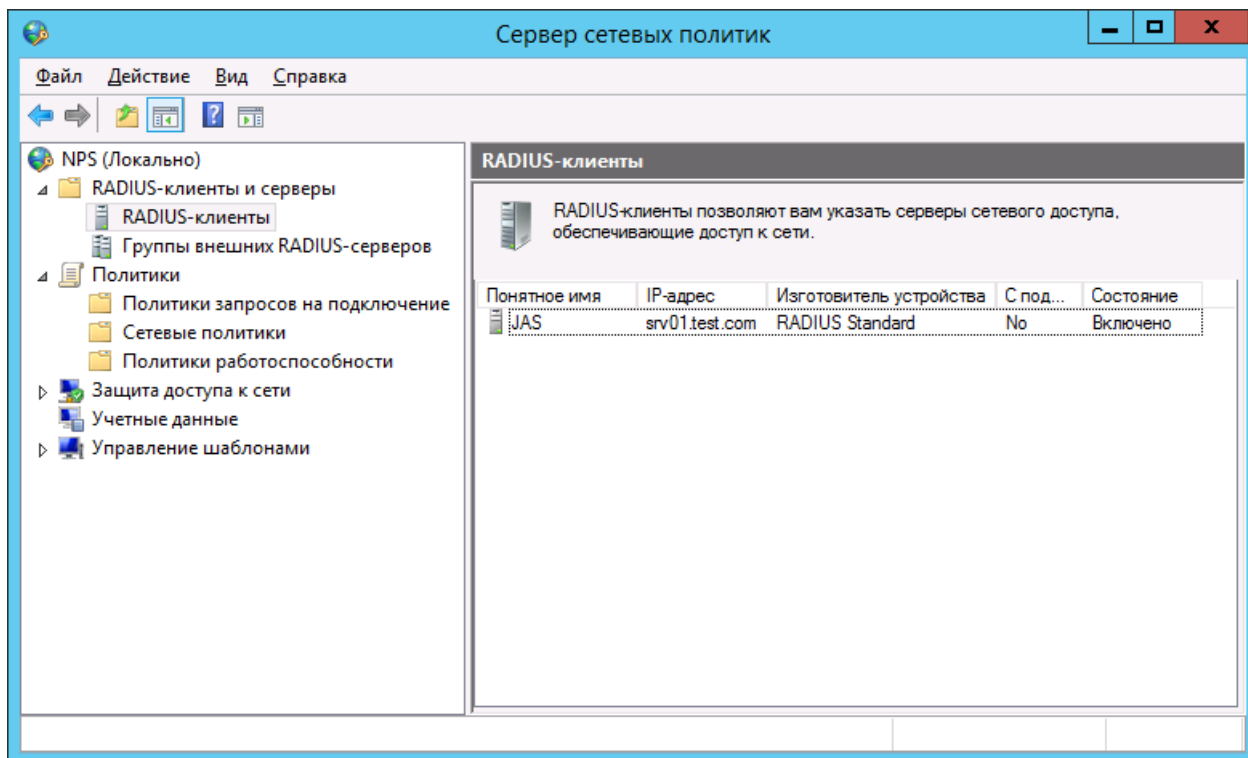


Рис. 54 – RADIUS-клиент создан

13.2 Установка JAS-плагина для NPS

Чтобы установить JAS-плагина для NPS, выполните следующие действия.

1. Запустите файл установки: **Aladdin.JAS.NPSPlugin-X.X.X.XXX-x64.msi** (только для 64-битных систем).
Отобразится следующее окно.

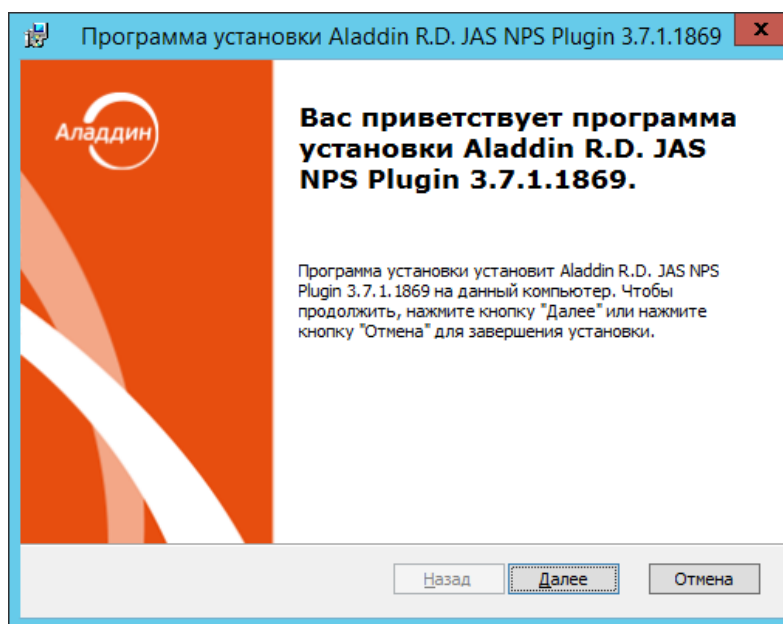


Рис. 55 – Окно приветствия мастера установки JAS-плагина для NPS

- Нажмите **Далее**.
Отобразится следующее окно.

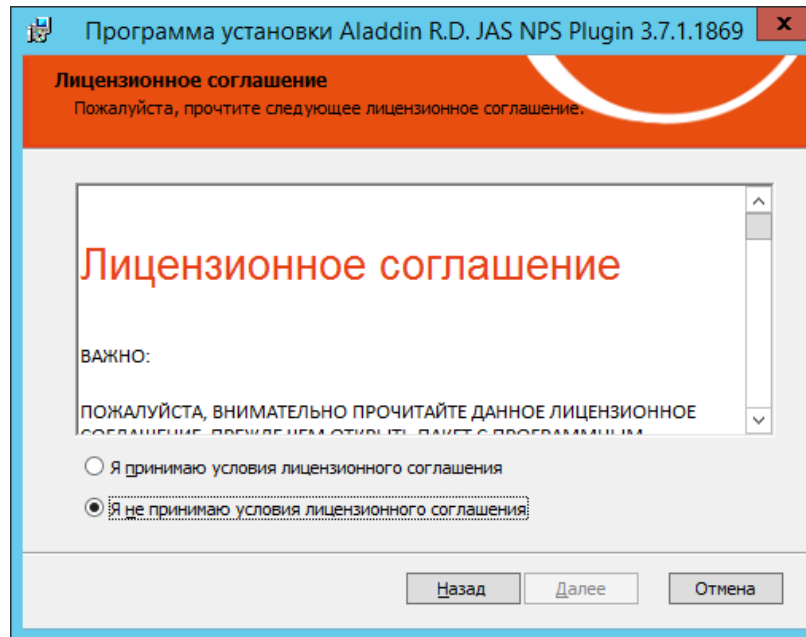


Рис. 56 – Окно лицензионного соглашения

- Выберите **Я принимаю условия лицензионного соглашения**, после чего нажмите **Далее**.
Отобразится следующее окно.

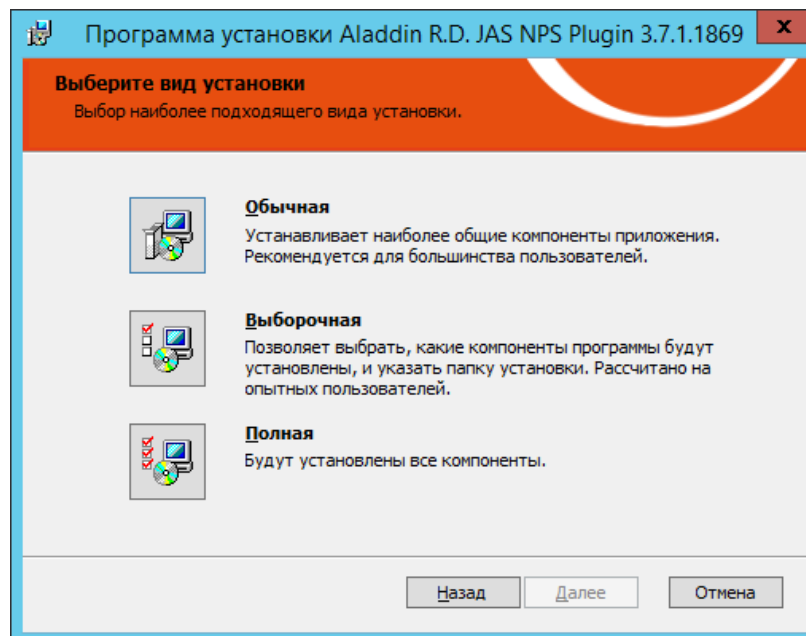


Рис. 57 - Окно выбора варианта установки

- Выберите **Полная**.

Отобразится следующее окно.

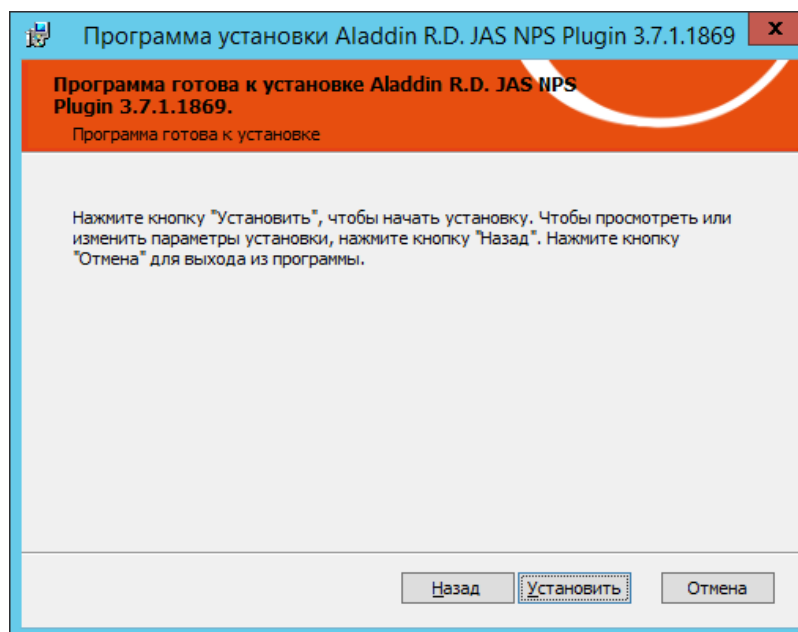


Рис. 58 – Подготовка к установке

5. Нажмите **Установить**.
По завершении установки отобразится следующее окно.

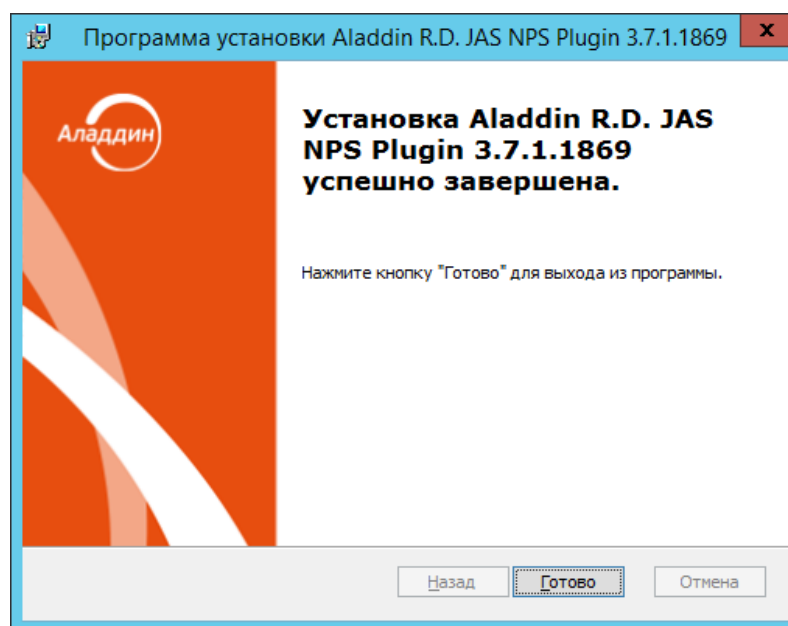


Рис. 59 – Окно завершения установки

6. Нажмите **Готово**.

Отобразится следующее сообщение.

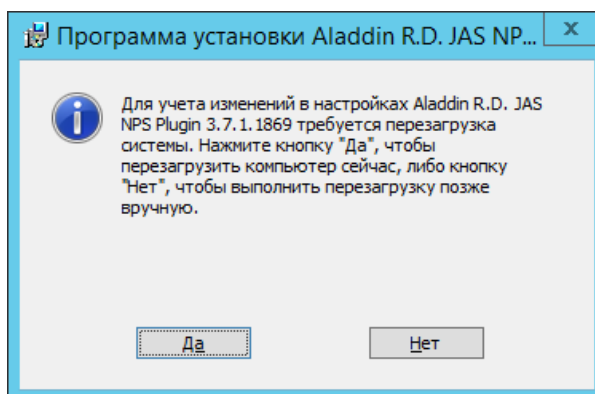


Рис. 60 – Предупреждение о необходимости перезагрузки

7. Нажмите **Нет**.
8. Дождитесь автоматической загрузки графического конфигуратора JAS-плагина для NPS и переходите к его настройкам (см. ниже).

13.3 Настройка JAS-плагина для NPS

После установки JAS-плагина для NPS автоматически откроется окно так называемого «конфигуратора» **Настройка JAS-плагина для NPS** (Рис. 61, с. 79).

Если вы закрыли окно конфигуратора, то можете запустить его вручную, см. «Работа с конфигуратором JAS-плагина для NPS», below.

13.3.1 Работа с конфигуратором JAS-плагина для NPS

Ниже описана процедура работы с конфигуратором **Настройка JAS-плагина для NPS**.

9. В меню **Пуск** выберите **JaCarta Authentication Server -> Настройка JAS-плагина для NPS**.
Отобразится следующее окно.

Настройка JAS-плагина для NPS

Общие настройки

Имя файла лога: C:\ProgramData\Aladdin\JAS NPS Plugin\Logs

Уровень логирования: ERROR

Язык: ru Кодировка сообщений: 65001

Домен по умолчанию:

Подключение к JAS

Адрес JAS: http://localhost:8008/JASEngine/Default/AuthenticationService/rest

Использовать аутентификацию

Логин JAS: Пароль JAS:

Поддерживаемые протоколы: SSL TLS TLS 1.1 TLS 1.2

Параметры аутентификации

Выбор типа аутентификации: Auto

Типы аутентификации: Messaging.OTP.Push

Проводить аутентификацию, если пользователь не обнаружен в JAS

Проводить аутентификацию, если не обнаружен токен в JAS

Приоритет использования Push OTP-токена пользователя

Двухшаговая аутентификация

Разрешить смену пароля при его истечении в домене

Параметры Messaging

Идентификатор системы:

Текст SMS:


Время жизни кода (с): 0

Таймаут между попытками (с): 0

По умолчанию Загрузить из реестра Сохранить в реестр Загрузить из файла Сохранить в файл

Рис. 61 – Окно Настройка JAS-плагина для NPS

При загрузке конфигурактор считывает текущее содержание настроек плагина из реестра.

 **Примечание.** При редактировании полей формы можно воспользоваться всплывающей подсказкой при наведении курсора мыши на поле ввода (Рис. 62)

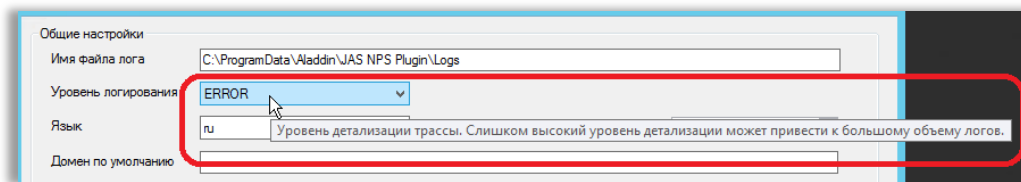







Рис. 62 – Использование всплывающей подсказки в полях формы

10. Выполните настройку, руководствуясь Табл. 26.



Табл. 26 - Настройка JAS-плагины для NPS


Поле конфигулятора	Имя параметра в реестре	Описание
<Секция> Общие настройки		
Имя файла лога	LogFilePath	Путь, по которому будет сохраняться файл журнала
Уровень логирования	LogLevel	<p>Уровень ведения журнала событий.</p> <ul style="list-style-type: none"> • OFF – ведение журнала событий отключено; • FATAL – неустраняемая ошибка; • ERROR – ошибка (значение по умолчанию); • WARN – предупреждение; • INFO – информация; • DEBUG – отладка; • ALL – показывать все события. <p> Каждый последующий уровень включает все предыдущие (кроме OFF), например, если выставлено значение INFO, то будут отображаться сообщения уровней: INFO, WARN, ERROR, FATAL</p>
Язык	Culture	<p>Язык пользовательского интерфейса JAS-плагины. Допустимые значения:</p> <ul style="list-style-type: none"> • en (английский язык); • ru (русский язык). <p>Значение по умолчанию: ru</p> <p> Примечание. Параметр определяет, на каком языке имя плагина в должно отражаться в консоли настроек NPS, а также язык сообщений в журналах JAS-плагины для NPS (за локализацию сообщений в браузере пользователя отвечают настройки языка веб-страниц браузера).</p>
Кодировка сообщений	ReplyMessageCodePage	<p>Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг ChallengeResponseRadiusAuth = True, выше)</p> <p>Кодировка текстовых сообщений (ReplyMessage), используемых в пользовательском диалоге при двухшаговой процедуре аутентификации в NPS-плагине для JAS. В качестве обозначения кодировок допускается использовать только из цифровые обозначения, например:</p> <ul style="list-style-type: none"> • 65001 – кодировка UTF8; • 1251 – Windows-1251; <p>Значение по умолчанию: 65001</p> <p> Примечание. Тип кодировки влияет на отображение строки запроса на информацию в диалоговых окнах интегрируемых продуктов. Подробнее см. в разделе «Выбор корректной кодировки диалогового запроса ReplyMessage при интеграции JAS со сторонними продуктами», ниже.</p>


Поле конфигурирования	Имя параметра в реестре	Описание
Домен по умолчанию	DefaultUserDomain	Значение по умолчанию имени домена пользователя. Данное значение добавляется к имени пользователя при аутентификации в web-форме JAS-плагина, если в плагин было передано имя пользователя без домена. Значение по умолчанию: пустая строка
<Секция> Подключение к JAS		
Адрес JAS	ServiceUri	Адрес сервера JAS в следующем формате: http://<FQDN-имя сервера>:8008/JASEngine/Default/AuthenticationService/rest. где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com; либо, в случае кластерной конфигурации JAS, полное доменное имя (FQDN) <i>кластерной роли</i> , созданной на этапе настройки отказоустойчивого кластера (см. «Настройка отказоустойчивого кластера JAS», с. 132).
Использовать аутентификацию	<без параметра в реестре>	Установите флаг, если для подключения к интерфейсу OTP-клиентов на сервере JAS следует использовать Windows-аутентификацию. Для этого в полях Логин JAS и Пароль JAS (ниже) следует указать аутентификационные данные учётной записи, от имени которой будет осуществляться подключение. В случае если флаг не установлен, подключение к интерфейсу OTP-клиентов на сервере JAS будет осуществляться анонимно, т.е. без аутентификации.
Логин JAS	JASUsername	Имя пользователя, входящего в группу с правом подключения по интерфейсу для OTP-клиентов. В настоящем документе для примера используется пользователь NPS2JAS , входящий в группу JAS Clients (см. «Предварительные действия», с. 15, и «Настройка сетевых программных интерфейсов JAS», с. 19).  Имя пользователя следует задавать без указания домена, например NPS2JAS (а не NPS2JAS@test.com или TEST\NPS2JAS).
Пароль JAS	JASPassword	Пароль пользователя, указанного в настройке JASUsername (выше).  Важно! После задания параметра JASPassword при запуске плагина указанная строка будет зашифрована и записана в параметр JASEncryptedPassword , а параметр JASPassword будет удален. Расшифровка параметра возможна только при работе плагина под той же учетной записью, под которой производилось зашифрование. В случае необходимости смены учетной записи для запуска плагина или в случае смены пароля пользователя JAS необходимо задать в параметрах строку JASPassword . После перезапуска плагина произойдет зашифрование нового пароля, и старый пароль будет заменен

Поле конфигулятора	Имя параметра в реестре	Описание
Поддерживаемые протоколы	SecurityProtocols	<p>Список поддерживаемых протоколов шифрования для обмена данных между сетевыми узлами. Представляются списком через запятую (например: Ssl3, Tls, Tls11, Tls12). Допустимые значения:</p> <ul style="list-style-type: none"> • Ssl3; • Tls; • Tls11; • Tls12. <p>По умолчанию указываются все допустимые типы протоколов</p>
<Секция> Параметры аутентификации		
Выбор типа аутентификации	AuthTypeSelection	<p>Режим выбора типа аутентификации.</p> <p>Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг ChallengeResponseRadiusAuth = True, выше)</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • Auto – автоматический выбор (в соответствии с приоритетами, определенными в параметре AuthTypes, см. выше); • Manual – ручной выбор (выбор типа аутентификации производится пользователем в реализованном пользовательском интерфейсе). <p>Значение по умолчанию: Auto</p>
Типы аутентификации	AuthTypes	<p>Поддерживаемые типы аутентификации и их приоритет.</p> <p>Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг ChallengeResponseRadiusAuth = True, выше)</p> <p>Возможные методы аутентификации:</p> <ul style="list-style-type: none"> • Messaging – аутентификация по Messaging-токену; • OTP – аутентификация по OTP-токенам; • Push <p>Методы указываются через запятую в порядке снижения приоритета.</p> <p>Значение по умолчанию: Messaging, OTP, Push</p>
Проводить аутентификацию, если пользователь не обнаружен в JAS	UserNotFoundAction	<p>Действия JAS-плагина, если пользователь, который пытается аутентифицироваться, не зарегистрирован в JAS. Доступные значения:</p> <ul style="list-style-type: none"> • Pass (Пропускать запрос); • Reject (Отклонять запрос). <p>Значение по умолчанию: Pass (Пропускать запрос).</p>

Поле конфигулятора	Имя параметра в реестре	Описание
Проводить аутентификацию, если не обнаружен токен в JAS	TokensNotFoundAction	<p>Действия JAS-плагины, если у пользователя, обратившегося с запросом на аутентификацию, в JAS зарегистрированы OTP-токены (хотя бы один), но ни один из них не активен (все отключены/заблокированы). Допустимые значения:</p> <ul style="list-style-type: none"> • Pass (Пропускать запрос); • Reject (Отклонять запрос). <p>Значение по умолчанию: Reject (Отклонять запрос).</p>
Приоритет использования Push OTP-токена пользователя	PushTokenAction	<p>Настройка режима аутентификации по Push-токену OTP.</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • Pass – Разрешение Push-токену OTP работать по протоколу PAP. Поскольку у метода PUSH имеется приоритет перед остальными методами аутентификации (обычными OTP-токенами и Messaging-токенами), то при установленном флаге Pass при аутентификации пользователя будет использоваться только Push-токен OTP (у Push-токена OTP приоритет перед другими выпущенными для пользователя токенами) • Reject – Push -токену OTP запрещено работать по протоколу PAP. Push -токен OTP используется только для режимов аутентификации CHAP и MSCHAP. (По факту, это включение приоритета аутентификации пользователя с помощью обычных OTP- и Messaging-токенов, использующих режим PAP). <p>Значение по умолчанию: Reject (Отклонять запрос).</p>
Двухшаговая аутентификация	ChallengeResponseRadiusAuth	<p>Режим работы JAS-плагины для NPS. Допустимые значения:</p> <ul style="list-style-type: none"> • True – двухшаговый режим аутентификации (перед вводом дополнительного параметра аутентификации, например OTP, на первом шаге процедуры вводится значение доменного пароля пользователя); • False -- одношаговый режим аутентификации (значение дополнительного параметра аутентификации, например OTP, вводится за один шаг). <p>Значение по умолчанию: False</p>

Поле конфигулятора	Имя параметра в реестре	Описание
Разрешить смену пароля при его истечении в домене	AllowChangeExpiredPassword	<p>Настройка возможности смены пароля пользователя через NPS-плагин при его истечении в домене.</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • False – смена пароля запрещена; • True – смена пароля разрешена; <p>Значение по умолчанию: False</p> <p> Примечание. Если опция смены пароля пользователя через NPS-плагин разрешена, то максимальная продолжительность сессии сброса пароля – от момента ввода текущего пароля до подтверждения нового пароля – по умолчанию составляет 300 секунд. При необходимости параметр настраивается в серверном конфигурационном файле JAS:</p> <pre>c:\Program Files\Aladdin\JaCarta Authentication Server\Aladdin.JAS.Engine.exe.config</pre> <p>Значение параметра задается в секундах.</p> <pre><add key="ChangeDomainPasswordTimeout" value="300"/></pre> <p>Также есть возможность ограничить максимальное количество попыток смена пароля при помощи параметра:</p> <pre><add key="MaxPasswordInputAttempts" value="5"/></pre>
<Секция> Параметры messaging		
Идентификатор системы	MessagingSystemId	<p>Идентификатор внешней системы, в которой будут искаться пользователи при аутентификации по Messaging.</p> <p>Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг ChallengeResponseRadiusAuth = True, выше)</p> <p> Примечание. Идентификатор должен совпадать с идентификатором в поле Внешняя система на вкладке Параметры выпуска соответствующего профиля выпуска Messaging-токенов (см. руководство по функциям управления JMS [3], раздел «Настройка профиля выпуска Messaging-токенов»)</p> <p>Допустимые значения: символьная строка</p> <p>Значение по умолчанию: пустая строка.</p>
Текст SMS	MessagingAdditionalInfo	<p>Текст, который будет отправляться в SMS пользователю вместе с кодом аутентификации для Messaging. Например «Код аутентификации для входа в систему XYZ »</p> <p>Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг ChallengeResponseRadiusAuth = True, выше)</p> <p>Допустимые значения: символьная строка</p> <p>Значение по умолчанию: пустая строка.</p>

Поле конфигурирующего	Имя параметра в реестре	Описание
Время жизни кода (с)	MessagingTtl	<p>Время жизни одноразового пароля из SMS-сообщения (в секундах), т.е. время, в течение которого ответ пользователя будет принят. Если не задан – сервер аутентификации будет использовать значение параметра Время жизни OTP, заданное в профиле выпуска Messaging-токена.</p> <p>По умолчанию – пустая строка (не задано)</p> <p>Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг ChallengeResponseRadiusAuth = True, выше)</p> <p> Примечание. Значение Время жизни OTP указывается на вкладке Параметры выпуска соответствующего профиля выпуска Messaging-токенов (см. руководство по функциям управления JMS [3]. раздел «Настройка профиля выпуска Messaging-токенов»)</p> <p>Допустимые значения: целое число</p> <p>Значение по умолчанию: пустая строка.</p>
Таймаут между попытками (мс)	MessagingRetryDelay	<p>Таймаут между попытками аутентификации посредством Messaging-токена (в миллисекундах), например 5000.</p> <p>Параметр применяется непосредственно к серверу JAS, который на его основе принимает решение о возможности приёма попытки аутентификации. При попытке аутентификации, произошедшей до истечения указанного таймаута, возникает ошибка аутентификации.</p> <p>Если параметр не задан (пустая строка), то сервер JAS в процессе аутентификации будет использовать либо собственное значение по умолчанию (5000 мс), либо значение, заданное в свойствах Messaging-токена (см. параметр Задержка генерации OTP (мс) в свойствах Messaging-токена или профиля выпуска Messaging-токенов; см. руководство по функциям управления JMS [3]).</p> <p>Значение по умолчанию: пустая строка (не задано)</p>

Поле конфигулятора	Имя параметра в реестре	Описание
<настройка отсутствует в графическом конфигуляторе, осуществляется только в реестре>	DefaultUserDomain	<p>Значение по умолчанию имени домена пользователя. Данное значение добавляется к имени пользователя при аутентификации, например, в web-интерфейсе, если пользователь указал свое имя без домена.</p> <p> Примечания:</p> <ol style="list-style-type: none"> 1. Параметр применим к разным ресурсным системам, в частности к доменным именам Active Directory (AD), RemoteAD и JDS. 2. В случае если пользователь при аутентификации указал свое полное имя (включая домен) в любом формате (FQDN, NetBIOS, UPN см. ниже примеры), то значение, указанное в параметре DefaultUserDomain плагином игнорируется. Примеры форматов указания полного имени пользователя (с именем домена) <ul style="list-style-type: none"> • FQDN: jasdomain.aladdin-rd.local\user • NetBIOS: jasdomain\user • UPN: user@jasdomain.aladdin-rd.local 3. В случае указания пустого значения DefaultUserDomain (по умолчанию) в JAS включается интеллектуальный механизм восстановления недостающего имени (по принципу регистрации OTP-аутентификаторов пользователя в том или ином домене). В случае если пользователь имеет OTP-аутентификаторы в разных доменах, выдается соответствующее сообщение об ошибке с рекомендацией указать полное имя явным образом. <p>Значение по умолчанию: пустая строка</p>
Кнопки управления		
По умолчанию		Привести значения в форме к значениям по умолчанию (например, для последующего редактирования или сохранения в реестр)
Загрузить из реестра		Загрузить в форму значения из реестра. (При запуске конфигулятора значения из реестра автоматически загружаются в поля формы.)
Сохранить в реестр		Сохранение текущих значений из формы в реестр. В момент нажатия на кнопку пользователю предлагается перезапуск службы NPS, Рис. 64.
Сохранить в файл		Отображаемые в форме параметры можно сохранить в reg-файл для последующего восстановления настроек или их распространения на узлы кластера (в случае кластерной конфигурации JAS)
Загрузить из файла		Конфигуратор позволяет загрузить в форму параметры плагина из reg-файла, ранее сохраненного с помощью кнопки Сохранить в файл



Примечание. Указанные в таблице параметры реестра (графа **Имя параметра в реестре**) располагаются в разделе реестра [HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JAS NPS Plugin], Рис. 63.

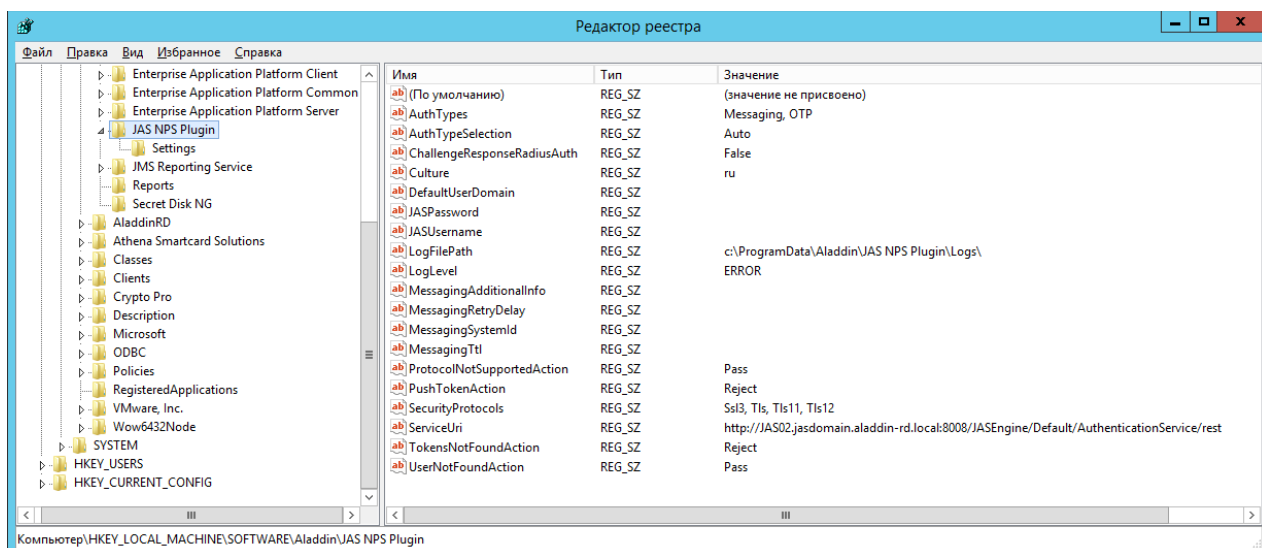


Рис. 63 – Настройки JAS-плагина для NPS

11. По нажатии на кнопку **Сохранить в реестр** отредактированные значения полей будут сохранены в реестр, при этом пользователю будет предложено выполнить автоматическую перезагрузку службы NPS с тем, чтобы новые значения настроек вступили в силу, Рис. 64.

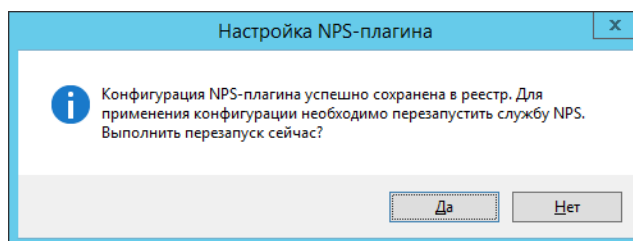


Рис. 64 – Диалог перезапуска службы NPS

В некоторых случаях для вступления настроек в силу требуется перезапуск самого компьютера, где установлена служба NPS с JAS-плагином.

После сохранения настроек JAS-плагин для NPS готов к работе.

13.3.2 Выбор корректной кодировки диалогового запроса ReplyMessage при интеграции JAS со сторонними продуктами

При интеграции JAS (с использованием JAS-плагина для NPS) со сторонними продуктами, предоставляющими возможность расширения сценария аутентификации за счет использования второго фактора, могут возникать сложности с отображением названий полей на русском языке (т.е при значении параметра реестра **Culture**=ru, см. Табл. 26, с. 80), как показано на Рис. 65.

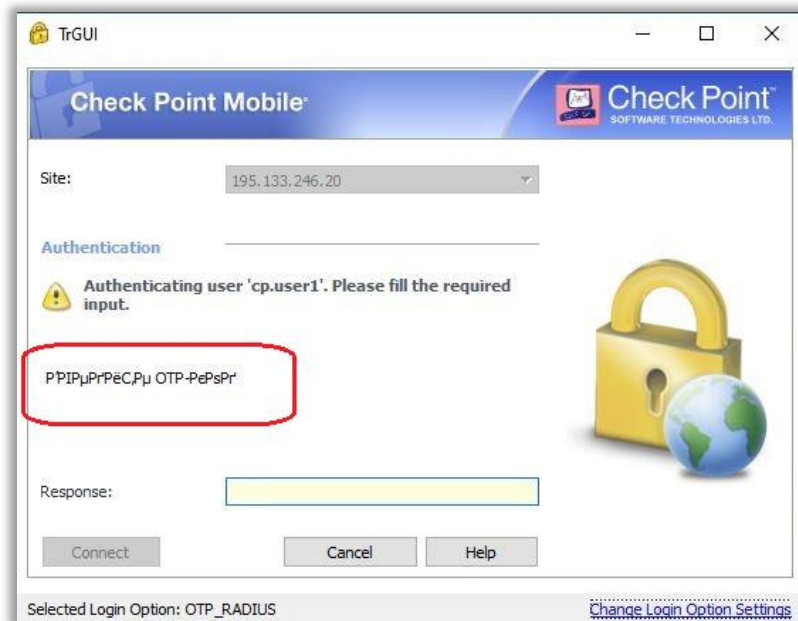


Рис. 65 – Пример некорректного отображения кириллической строки запроса на информацию (ReplyMessage)

В процессе проработки интеграции JAS со сторонним продуктом следует провести исследование на предмет выбора необходимой кодировки (параметр Табл. 26, с. 80), обеспечивающей корректное отображение диалоговой строки.

Например, для корректного отображения кириллического запроса (ReplyMessage) при интеграции JAS со шлюзом Check Point Gateway, а именно в клиенте CheckPoint Mobile, в параметре **ReplyMessageCodePage** следует использовать кодировку 1251, а при интеграции с VPN-продуктом Cisco AnyConnect следует использовать кодировку 65001.

13.4 Проверка работы JAS-плагина для NPS

13.4.1 Одношаговая процедура ввода второго фактора аутентификации

Одношаговая процедура подразумевает проверку только дополнительного фактора аутентификации пользователя. В рассматриваемом примере это ввод одноразового пароля (ОТР) с помощью заблаговременно выпущенного в JMS ОТР-токена.

JAS-плагин для NPS по умолчанию (т.е. сразу после установки) настроен на одношаговую процедуру. Данный тип аутентификации (один шаг) устанавливается значением параметра реестра ChallengeResponseRadiusAuth=false (см. Табл. 26, с. 80).

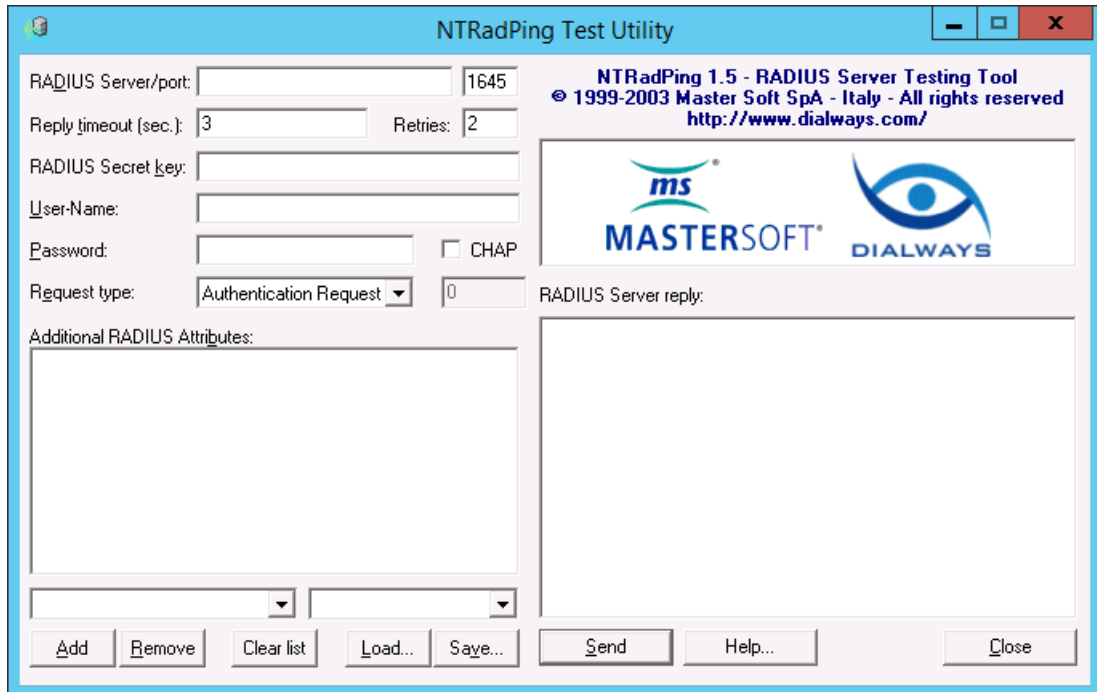
Чтобы проверить работу JAS-плагина для NPS в режиме одношаговой процедуры, выполните следующие действия.



В настоящем документе описана процедура проверки с использованием свободно распространяемой утилиты **NTRadPing.exe**.

1. Используя консоль управления JMS выпустите аппаратный или программный ОТР-токен (см. разделы «Выпуск аппаратных ОТР-токенов» и «Выпуск программных ОТР-токенов (мобильное приложение Aladdin 2FA)» в руководстве администратора по функциям управления JMS [3]).

- В случае OTP-токена с алгоритмом HOTP выполните его синхронизацию (см. раздел «Синхронизация значений OTP (только для токенов HOTP)» в руководстве администратора по функциям управления JMS [3]).
- На RADIUS-клиенте запустите утилиту **NTRadPing**.
Окно утилиты будет выглядеть следующим образом.

Рис. 66 – Окно утилиты *NTRadPing*

- Выполните настройку соединения, руководствуясь табл. 27 ниже.

Табл. 27 – Настройка соединения с RADIUS-сервером

Настройка	Описание
RADIUS Server/port (RADIUS-сервер/порт)	<ol style="list-style-type: none"> В левом поле укажите IP-адрес RADIUS-сервера. В правом поле укажите порт, по которому будет происходить соединение или оставьте значение по умолчанию (1645)
Reply timeout (Время ожидания ответа)	Задайте время ожидания ответа RADIUS-сервера в секундах
Retries (Число попыток)	Укажите число автоматических попыток соединения
RADIUS Secret key (Значение общего секрета)	Укажите значение секрета для RADIUS-сервера (см. «Настройка параметров RADIUS-клиента», с. 70)
User-Name (Имя пользователя)	Укажите имя пользователя с действующим OTP-токеном, от имени которого будет происходить попытка аутентификации. Имя пользователя должно быть указано в следующем формате: <NetBIOS-имя домена>\<имя пользователя> , например, TEST\u1

Настройка	Описание
Password (Пароль)	Введите сгенерированное значение одноразового пароля (OTP). В зависимости от параметров аутентификации указано пользователем может потребоваться также ввести PIN-код для OTP или пароль Windows. В настоящем документе рассматривается базовый вариант, в котором для аутентификации пользователь должен ввести только значение OTP
Request type (Тип запроса)	Убедитесь, что в списке выбран пункт Authentication Request (Запрос на аутентификацию)

- Нажмите кнопку **Send** (Отправить) внизу интерфейса.
Если JAS-плагин для NPS настроен верно и если в окне утилиты были введены конкретные данные, в секции **RADIUS Server reply** (Ответ RADIUS-сервера) отобразятся следующие сведения.

The screenshot shows the NTRadPing Test Utility interface. On the left, there are input fields for RADIUS Server/port (192.168.200.100:1645), Reply timeout (3s), Retries (2), RADIUS Secret key (1111), User-Name (TEST\u1), Password (masked), and Request type (Authentication Request). A 'Send' button is highlighted. On the right, the 'RADIUS Server reply' section shows the following output:

```

Sending authentication request to server 192.168.200.100:1645
Transmitting packet, code=1 id=2 length=47
received response from the server in 250 milliseconds
reply packet code=2 id=2 length=78
response: Access-Accept
..... attribute dump .....
Framed-Protocol=PPP
Service-Type=Framed
Class=\0x7f9\0x06\0x17\0x00\0x00\0x017\0x00\0x01\0x02\0x00\C

```

Рис. 67 – Ответ RADIUS-сервера

- Убедитесь в том, что в строке response (ответ) содержится значение **Access-Accept** (Доступ-Принят) – в этом случае аутентификация успешна. В противном случае проверьте настройки интерфейса для OTP-клиентов (см. «Настройка сетевых программных интерфейсов JAS», с. 19) и настройки JAS-плагины для NPS (см. «Настройка JAS-плагины для NPS», с. 78).

13.4.2 Двухшаговая процедура аутентификации

Двухшаговая процедура аутентификации включает в себя проверку доменного пароля и второго фактора аутентификации

Рассматриваемая в данном примере процедура реализуется для пользователей, у которых установлен только один тип токенов для генерации одноразового пароля (либо OTP-, либо Messaging-, либо PUSH-токены). Пример с использованием одновременно нескольких типов токенов (и OTP-, и Messaging-, и PUSH-токенов) приведен в разделе «Двухшаговая процедура аутентификации с выбором типа второго фактора», ниже.

В рассматриваемом примере в качестве второго фактора вводится одноразовый пароль, полученный с помощью выпущенного в JMS OTP-токена.

Для инициации двухшаговой процедуры с ручным выбором второго фактора, реализуемой JAS-плагином для NPS, в его настройках в реестре следует установить следующие значения параметров:

- ChallengeResponseRadiusAuth=true;
- AuthTypeSelection=Auto;
- AuthTypes=OTP.

(Подробнее см. Табл. 26, с. 80).



Примечание. После изменения параметров реестра для их вступления в силу следует перезапустить компьютер.

Подготовка к процедуре проверки в данном примере аналогична подготовительным шагам (шаги 1–2) предыдущего примера (см. раздел «Одношаговая процедура ввода второго фактора аутентификации», с. 88).

Чтобы проверить работу JAS-плагины для NPS в режиме двухшаговой процедуры аутентификации, выполните следующие действия.

1. На RADIUS-клиенте запустите утилиту **NTRadPing**.
Окно утилиты будет выглядеть следующим образом.

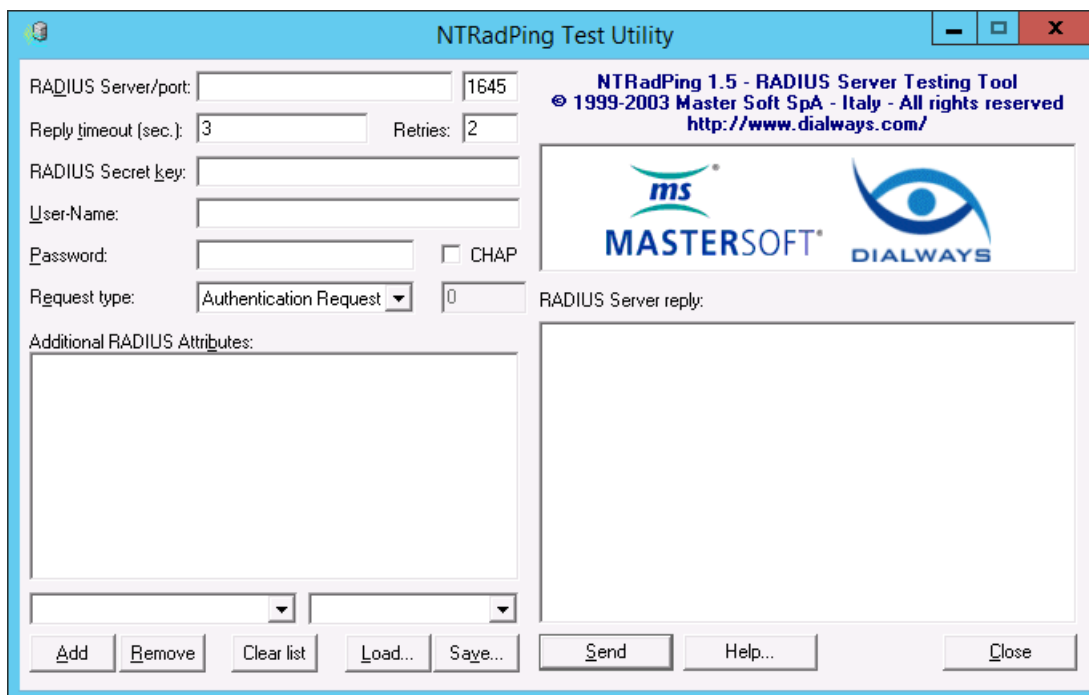


Рис. 68 – Начальный вид окна утилиты **NTRadPing**

2. Выполните настройку соединения, руководствуясь табл. 27 (с. 89), с единственным отличием: в поле **Password** вместо OTP-пароля введите доменный (AD) пароль пользователя, указанного в поле **User Name**. (Это первый шаг – ввод первого фактора аутентификации).
3. Нажмите **Send**.

В окне программы отобразится информация следующего вида.

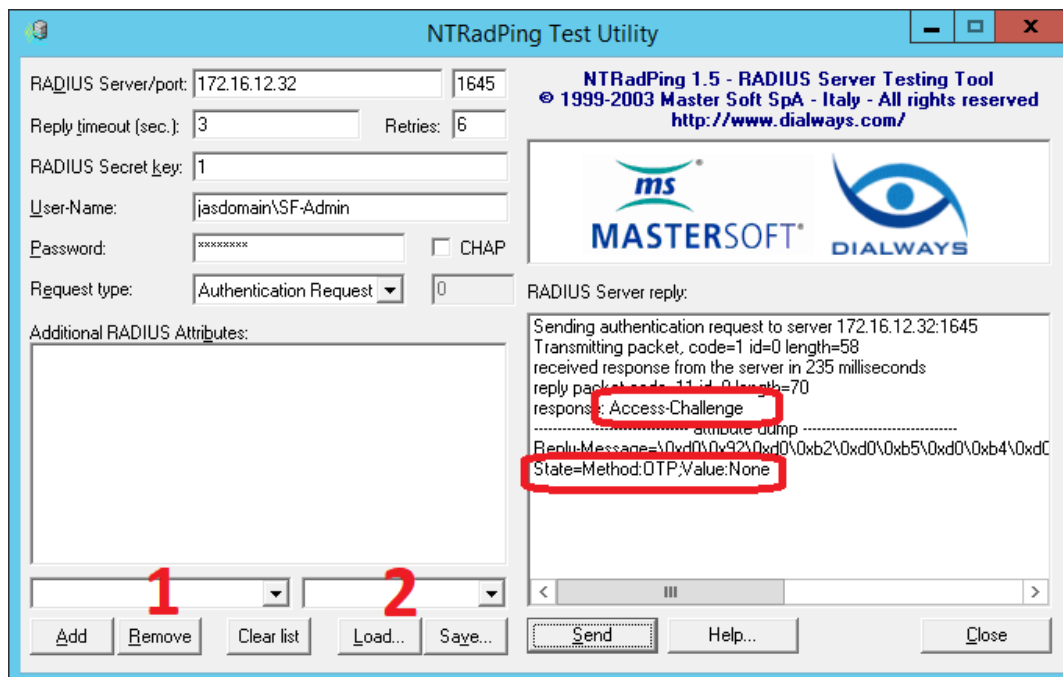


Рис. 69 – Ответ RADIUS-сервера

В поле **RADIUS Server reply** отобразится ответ типа *Access Challenge* (запрос второго фактора аутентификации). В секции **attribute dump** отобразится подсказка для имени метода для запроса второго фактора аутентификации (в данном случае *State=Method:OTP;Value:None*)

4. Для ввода второго фактора аутентификации (OTP) выполните следующие действия.
 - 4.1. В поле настройки атрибута запроса (Рис. 69, поле, обозначенное цифрой «1») введите *State*.
 - 4.2. В поле настройки значения атрибута запроса (Рис. 69, поле, обозначенное цифрой «2») введите значение из указанной выше подсказки (*Method:OTP;Value:None*)
 - 4.3. Нажмите **Add**

В окне программы отобразится информация следующего вида.

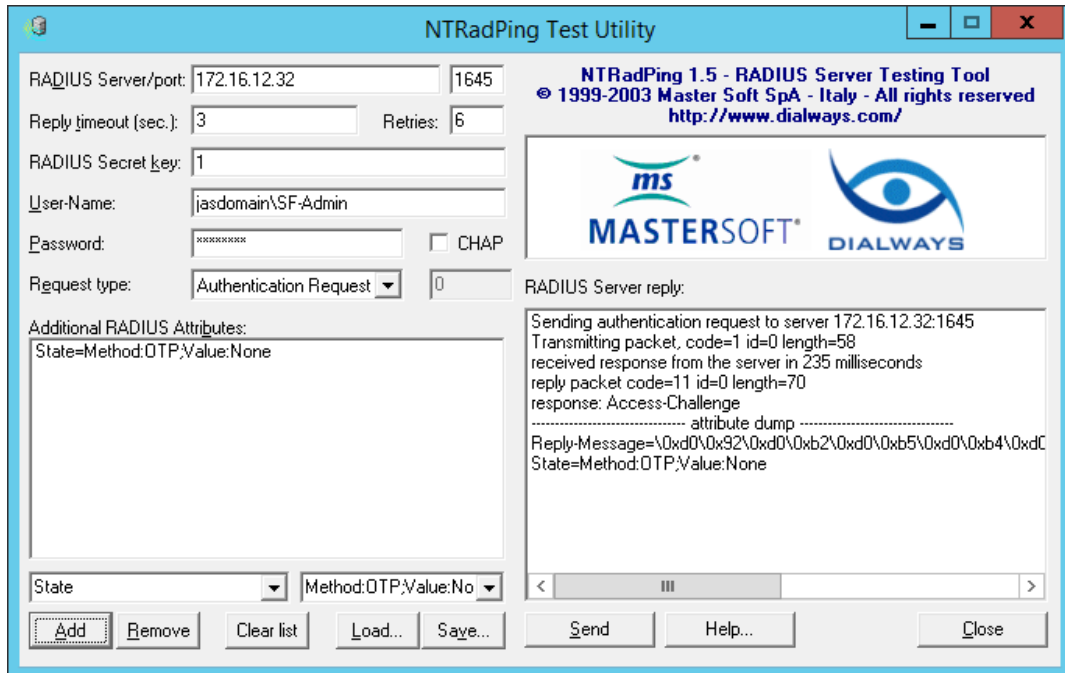


Рис. 70 – Отображение дополнительных атрибутов запроса к RADIUS-серверу (Additional RADIUS Attributes)

Значение дополнительного атрибута запроса отобразится в поле **Additional RADIUS Attributes**.

5. В поле **Password** введите сгенерированное в OTP-токене значение одноразового пароля



Примечание. В данном примере подразумевается, что в настройках OTP-токена выбран режим «только OTP», без необходимости добавления PIN-кода или доменного пароля)

6. Нажмите **Send**.

В поле **RADIUS Server reply** отобразятся следующие сведения.

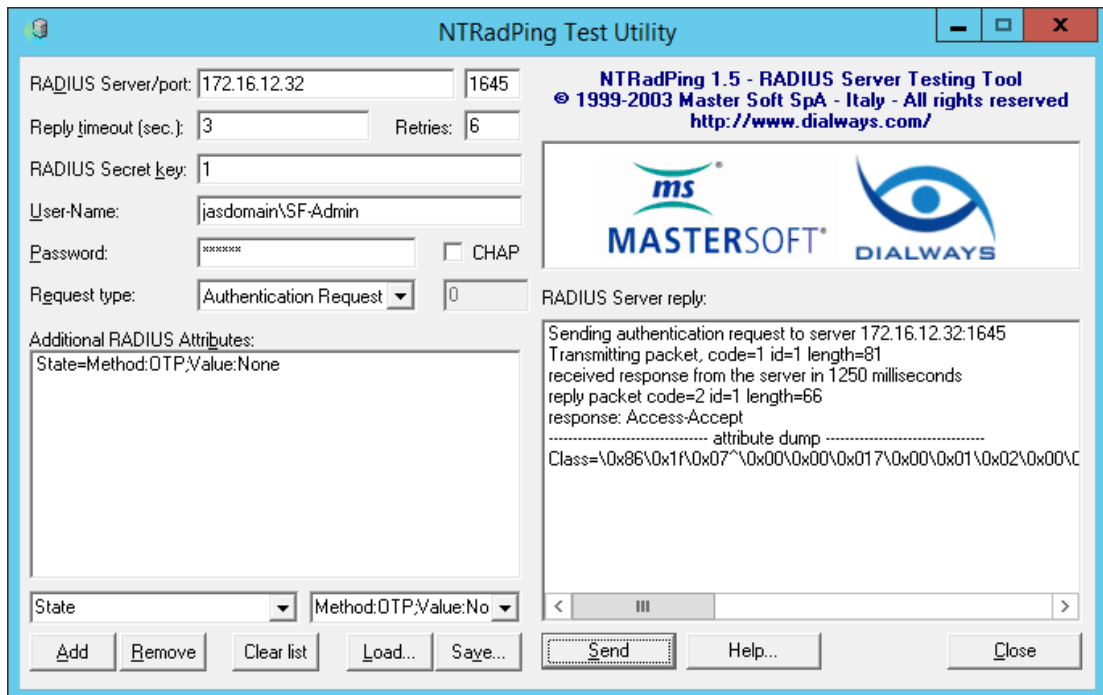


Рис. 71 – Ответ RADIUS-сервера

- Убедитесь в том, что в строке *response* (ответ) содержится значение *Access-Accept* – в этом случае аутентификация успешна. В противном случае проверьте настройки интерфейса для OTP-клиентов (см. «Настройка сетевых программных интерфейсов JAS», с. 19), настройки JAS-плагинов для NPS (см. «Настройка JAS-плагинов для NPS», с. 78) или проверьте корректность одноразового пароля в поле **Password**.

13.4.3 Двухшаговая процедура аутентификации с выбором типа второго фактора

Данная процедура проверки работы JAS-плагинов аналогична предыдущей, но подразумевает наличие у пользователя одновременно двух типов OTP-аутентификаторов (OTP-, Messaging- и PUSH-токенов) с возможностью выбора типа аутентификатора.

Для инициации двухшаговой процедуры с ручным выбором второго фактора (на примере двух типов токенов – OPT- и Messaging-), реализуемой JAS-плагином для NPS, в его настройках в реестре следует установить следующие значения параметров:

- ChallengeResponseRadiusAuth=true;
- AuthTypeSelection=Manual;
- AuthTypes=OTP, Messaging;
- MessagingSystemId= <значение, указанное в соответствующем профиле выпуска Messaging-токена>

(Подробнее см. Табл. 26, с. 80).



Примечание. После изменения параметров реестра для их вступления в силу следует перезапустить компьютер.

Для подготовки к процедуре выпустите для пользователя Messaging-токен и как минимум один OTP-токен.

Чтобы проверить работу JAS-плагина для NPS в режиме двухшаговой процедуры аутентификации с выбором типа второго фактора, выполните следующие действия.

- На RADIUS-клиенте запустите утилиту **NTRadPing**.
1. Выполните настройку соединения, руководствуясь табл. 27 (с. 89), с единственным отличием: в поле **Password** вместо OTP-пароля введите доменный (AD) пароль пользователя, указанного в поле **User Name**. (Это первый шаг – ввод первого фактора аутентификации).
 2. Нажмите **Send**.
В окне программы отобразится информация следующего вида.

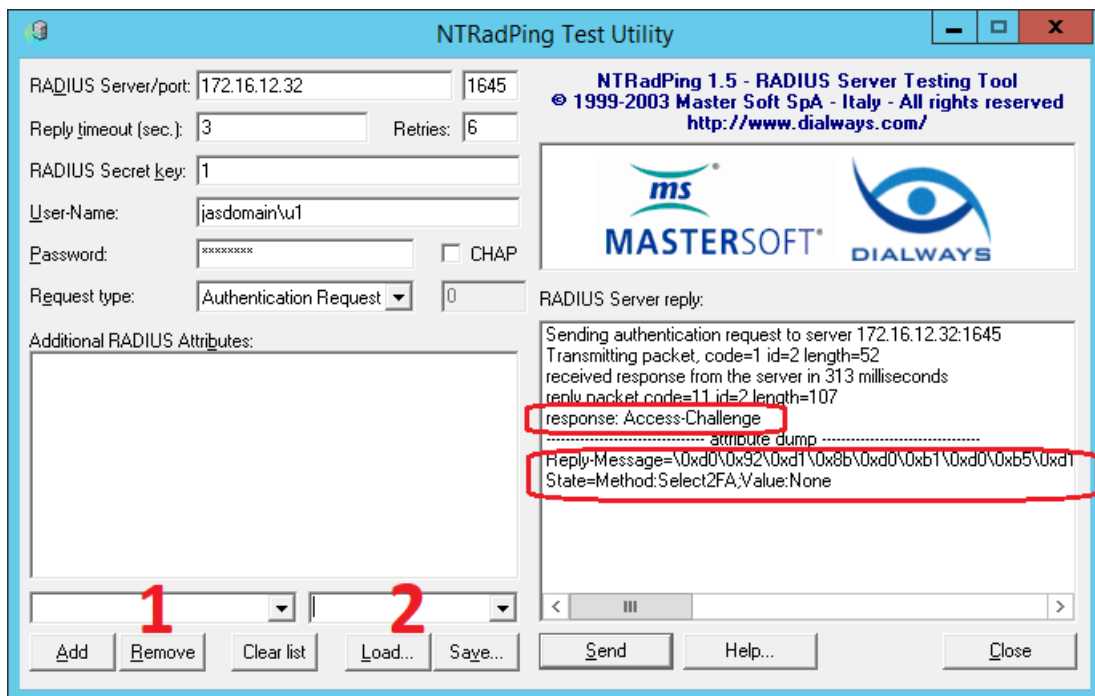


Рис. 72 – Ответ RADIUS-сервера

В поле **RADIUS Server reply** отобразится ответ типа *Access Challenge* (запрос второго фактора аутентификации). В секции **attribute dump** отобразятся подсказки:

- для типа второго фактора аутентификации (Reply Message). В некоторых случаях (как в примере на Рис. 72), чтобы просмотреть числовые идентификаторы метода (например 1-OTP; 2-SMS) следует прокрутить содержимое поля **RADIUS Server reply** вправо (Рис. 73, ниже)



Примечание. Для метода Push может быть указан дополнительный идентификатор (отсутствует в данном примере). Нумерация соответствует порядку следования типов аутентификации в параметре AuthTypes в реестре (см. Табл. 26, с. 80).

- для имени метода для запроса типа второго фактора аутентификации (в данном случае *State=Method:Select2FA;Value:None*)

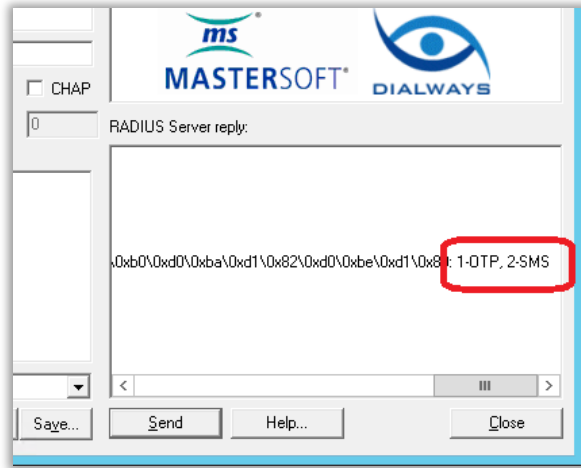


Рис. 73 – Прокрутка поля до конца, чтобы получить идентификатор метода

3. Для выбора типа второго фактора аутентификации (OTP, Messaging или Push) выполните следующие действия.
 - 3.1. В поле **Password** укажите идентификатор второго фактора аутентификации согласно подсказке (например для OTP следует ввести 1; для SMS следует ввести 2, и т.д.). В данном примере вводится «1» (идентификатор для OTP).
 - 3.2. Нажмите **Send**.

В окне программы отобразится информация следующего вида.

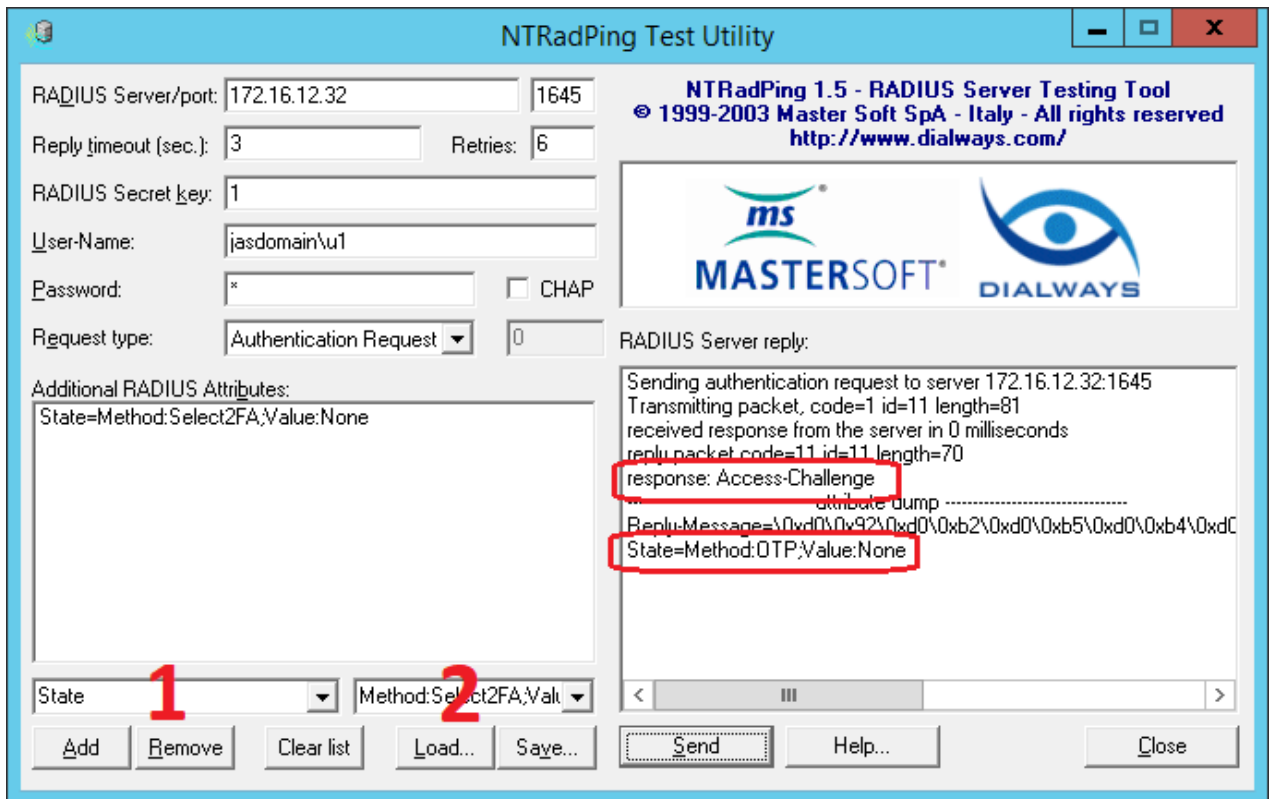


Рис. 74 – Ответ RADIUS-сервера



Примечание. В случае выбора идентификатора для метода Push указанное на Рис. 74 информация не отобразится. Ожидаемым действием пользователя будет нажатие на кнопку подтверждения аутентификации в мобильном приложении на смартфоне.

В поле **RADIUS Server reply** отобразится ответ типа *Access Challenge* (запрос второго фактора аутентификации). В секции **attribute dump** отобразится подсказка для имени метода для запроса второго фактора аутентификации (в данном случае *State=Method:OTP;Value:None*)

4. Для ввода второго фактора аутентификации (OTP) выполните следующие действия.
 - 4.1. В поле настройки атрибута запроса (Рис. 74, поле, обозначенное цифрой «1») введите *State*.
 - 4.2. В поле настройки значения атрибута запроса (Рис. 74, поле, обозначенное цифрой «2») введите значение из указанной выше подсказки (*Method:OTP;Value:None*)
 - 4.3. Нажмите **Add**

В окне программы отобразится информация следующего вида.

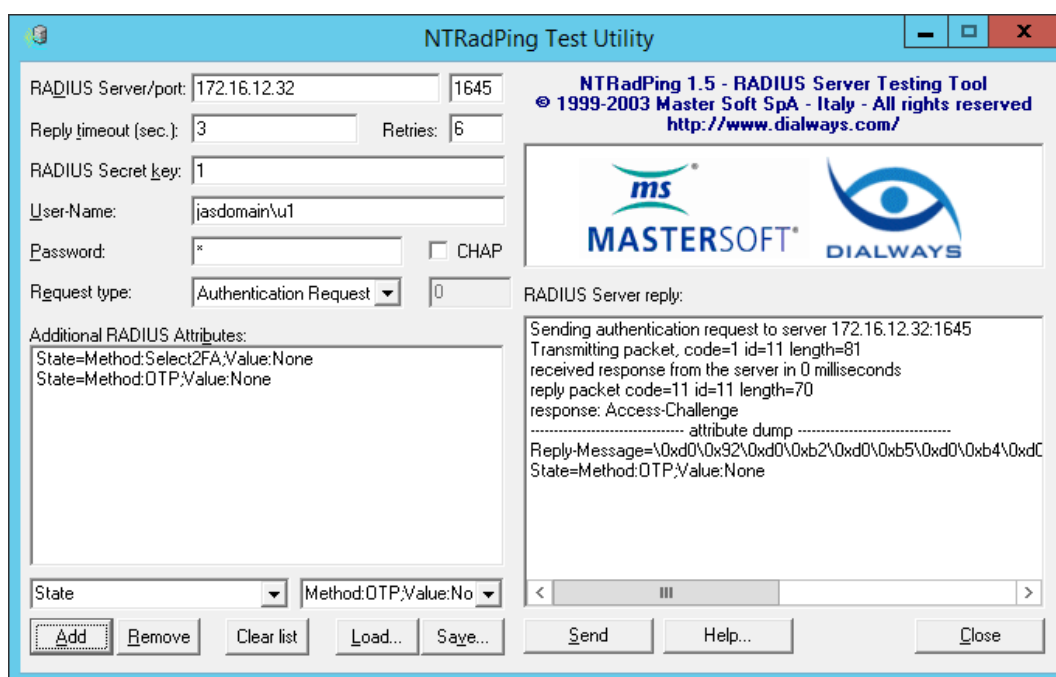


Рис. 75 – Отображение дополнительных атрибутов запроса к RADIUS-серверу (Additional RADIUS Attributes)

Значение введенного атрибута запроса отобразится второй строкой в поле **Additional RADIUS Attributes**.

5. В поле **Password** введите сгенерированное в OTP-токене значение одноразового пароля



Примечание. В данном примере подразумевается, что в настройках OTP-токена выбран режим «только OTP», без необходимости добавления PIN-кода или доменного пароля)

6. Нажмите **Send**.

В поле **RADIUS Server reply** отобразятся следующие сведения.

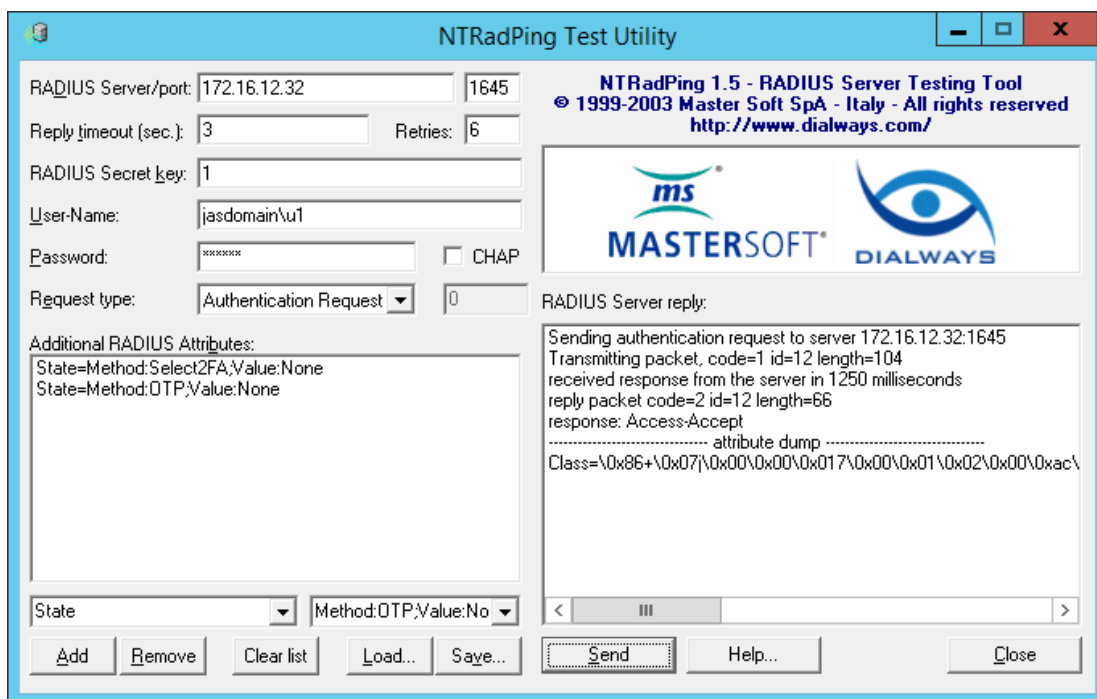


Рис. 76 – Ответ RADIUS-сервера

- Убедитесь в том, что в строке *response* (ответ) содержится значение *Access-Accept* – в этом случае аутентификация успешна. В противном случае проверьте настройки интерфейса для OTP-клиентов (см. «Настройка сетевых программных интерфейсов JAS», с. 19), настройки JAS-плагинов для NPS (см. «Настройка JAS-плагинов для NPS», с. 78) или проверьте корректность одноразового пароля в поле **Password**.

14. Установка и настройка JAS-плагинов для AD FS

14.1 Подготовка к установке JAS-плагинов для AD FS

Перед установкой JAS-плагинов установите роль *Службы федерации Active Directory* (имя службы Active Directory Federation Service – AD FS) в соответствии с документацией Microsoft Windows Server.

14.2 Установка JAS-плагинов для AD FS

Чтобы установить JAS-плагин (модуль расширения) для AD FS, на сервере с установленной ролью *Службы федерации Active Directory* выполните следующие действия.

- Запустите файл установки: **Aladdin.JAS.ADFSPlugin-X.X.X.XXX-x64.msi** (только для 64-битных систем).

Отобразится следующее окно.

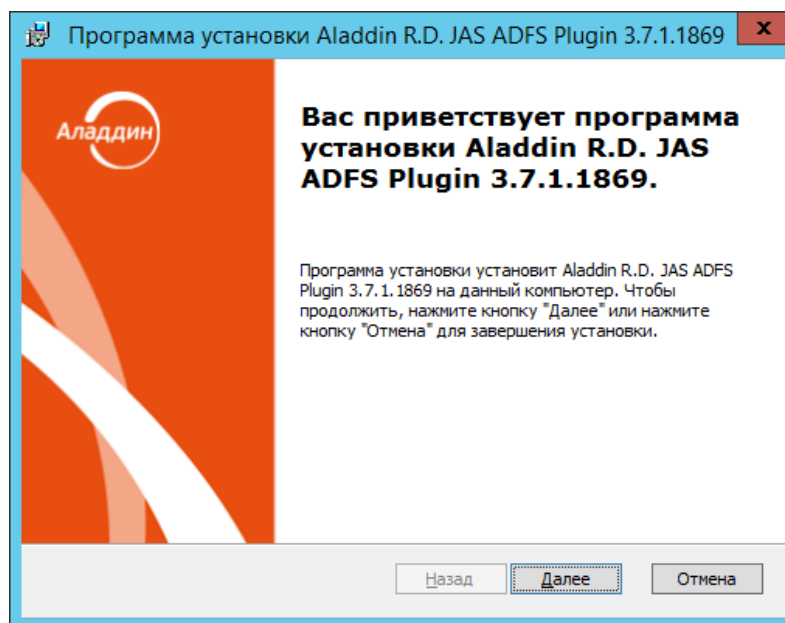


Рис. 77 – Окно приветствия мастера установки JAS-плагина для AD FS

2. Нажмите **Далее**.
Отобразится следующее окно.

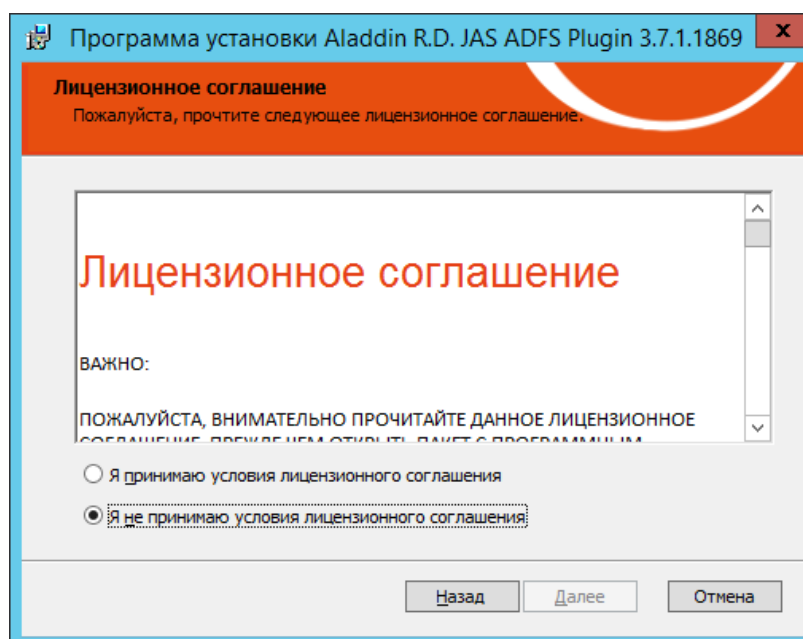


Рис. 78 – Окно лицензионного соглашения

3. Выберите **Я принимаю условия лицензионного соглашения**, после чего нажмите **Далее**.

Отобразится следующее окно.

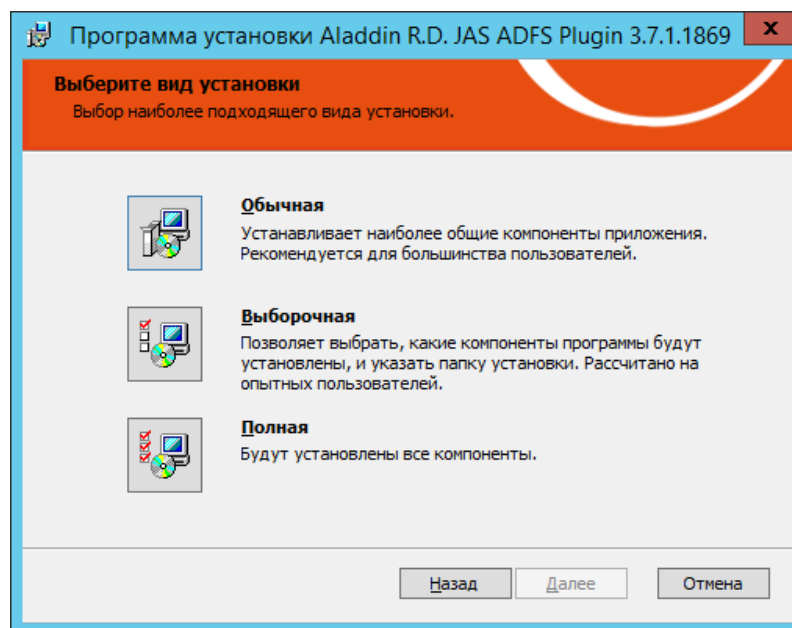


Рис. 79 - Окно выбора варианта установки

4. Выберите **Полная**.
Отобразится следующее окно.

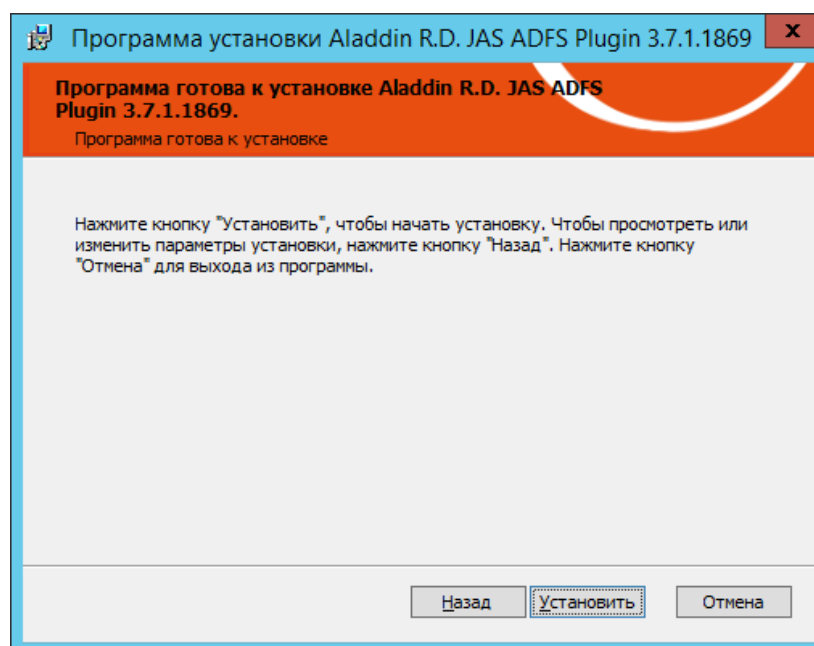


Рис. 80 – Подготовка к установке

5. Нажмите **Установить**.

По завершении установки отобразится следующее окно.

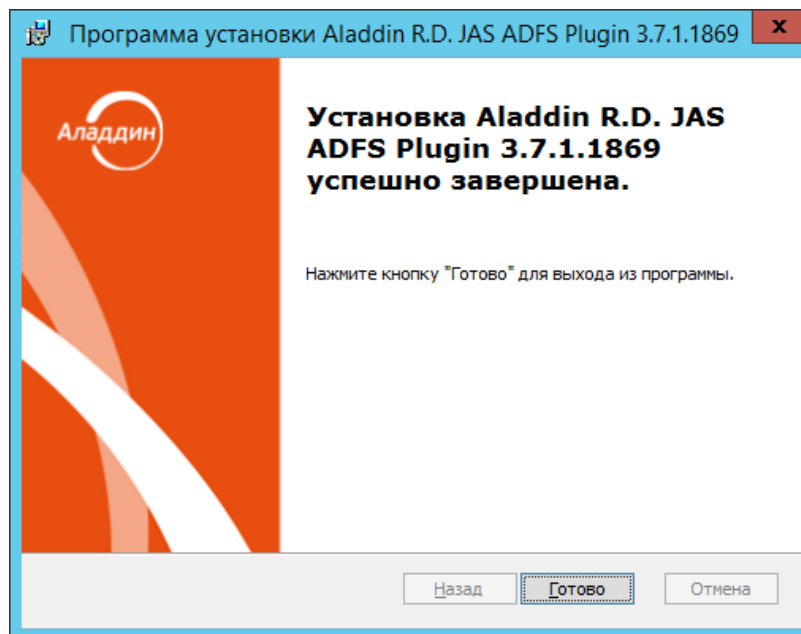


Рис. 81 – Окно завершения установки

6. Нажмите **Готово**.

JAS-плагин для ADFS установлен.

Сразу после установки плагина будет автоматически запущен так называемый «конфигуратор» **Настройка ADFS-плагина** (см. «Настройка JAS-плагина для AD FS», с. 103).

После установки JAS-плагин становится доступен для подключения в настройках службы AD FS (Рис. 83).

Для проверки корректности установки JAS-плагина для AD FS откройте оснастку MMC **Управление AD FS**. Раскройте путь **AD FS -> Политики проверки подлинности**. На панели справа в разделе

Многофакторная проверка подлинности напротив пункта **Глобальные параметры** нажмите **Изменить** (Рис. 82).

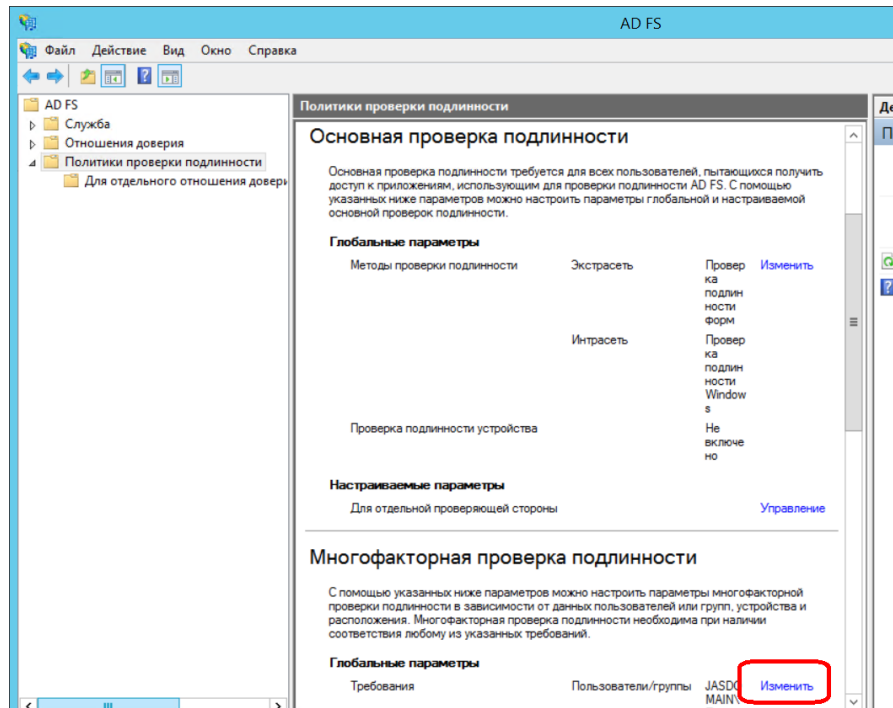


Рис. 82 – Вызов окна изменения параметров многофакторной аутентификации посредством AD FS

В открывшемся окне откройте на вкладку **Многофакторная**:

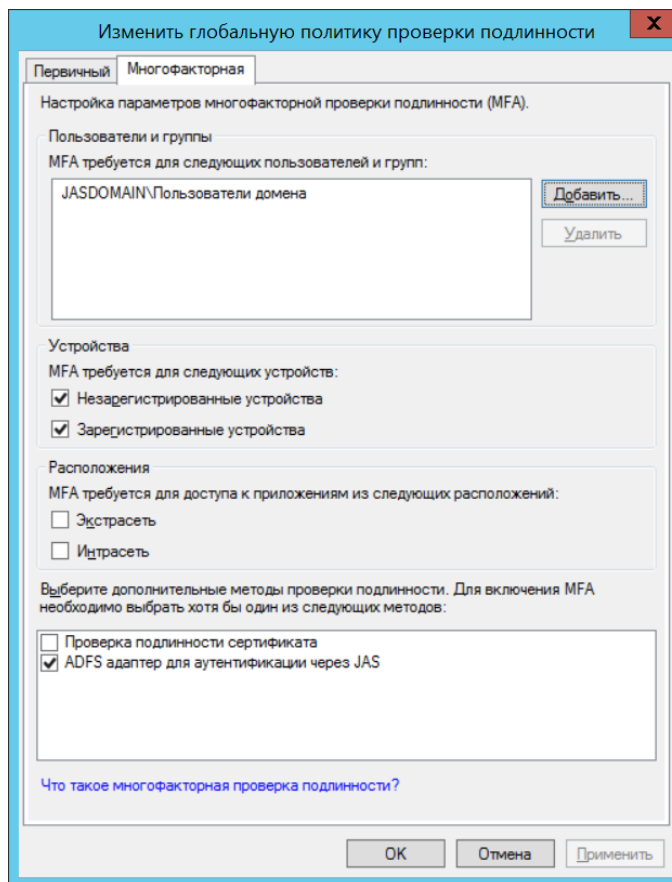


Рис. 83 – Проверка корректности установки JAS-плагина для AD FS

Убедитесь в наличии логического поля **ADFS адаптер для аутентификации через JAS** (его присутствие свидетельствует о корректной установке JAS-плагина для AD FS).

Убедитесь, что флажок **ADFS адаптер для аутентификации через JAS** установлен.

Убедитесь, что сделаны остальные необходимые настройки многофакторной аутентификации посредством AD FS в соответствии с документацией Microsoft Windows Server.

14.3 Настройка JAS-плагина для AD FS

После установки JAS-плагина AD FS автоматически откроется окно так называемого «конфигуратора» **Настройка JAS-плагина для AD FS** (Рис. 84, с. 104).

Если вы закрыли окно конфигуратора, то можете запустить его вручную, см. «Работа с конфигуратором JAS-плагина для AD FS», ниже.

14.3.1 Работа с конфигуратором JAS-плагина для AD FS

Ниже описана процедура работы с конфигуратором **Настройка JAS-плагина для AD FS**.

1. В меню **Пуск** выберите **JaCarta Authentication Server -> Настройка JAS-плагина для AD FS**. Отобразится следующее окно.

Рис. 84 – Окно Настройка JAS-плагина для AD FS

При загрузке конфигуратор считывает текущее содержание настроек плагина из реестра.








Примечание. При редактировании полей формы можно воспользоваться всплывающей подсказкой при наведении курсора мыши на поле ввода (Рис. 85)


Рис. 85 – Использование всплывающей подсказки в полях формы


2. Выполните настройку, руководствуясь Табл. 28.

Табл. 28 - Настройка JAS-плагина для AD FS

Поле конфигулятора	Имя параметра в реестре	Описание
<Секция> Общие настройки		
Имя файла лога	LogFilePath	Путь, по которому будет сохраняться файл журнала
Уровень логирования	LogLevel	<p>Уровень ведения журнала событий.</p> <ul style="list-style-type: none"> • OFF – ведение журнала событий отключено; • FATAL – неустраняемая ошибка; • ERROR – ошибка (значение по умолчанию); • WARN – предупреждение; • INFO – информация; • DEBUG – отладка; • ALL – показывать все события. <p> Каждый последующий уровень включает все предыдущие (кроме OFF), например, если выставлено значение INFO, то будут отображаться сообщения уровней: INFO, WARN, ERROR, FATAL</p>
Язык	Culture	<p>Язык пользовательского интерфейса JAS-плагина для AD FS. Допустимые значения:</p> <ul style="list-style-type: none"> • en (английский язык); • ru (русский язык). <p>Значение по умолчанию: ru</p> <p> Примечание. Параметр определяет, на каком языке имя плагина в консоли настроек ADFS, а также язык сообщений в журналах JAS-плагина для ADFS (за локализацию сообщений в браузере пользователя отвечают настройки языка веб-страниц браузера).</p>
<Секция> Подключение к JAS		
Адрес JAS	ServiceUri	<p>Адрес сервера JAS в следующем формате:</p> <p>http://<FQDN-имя сервера>:8008/JAS/Engine/Default/AuthenticationService/rest.</p> <p>где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com; либо, в случае кластерной конфигурации JAS, полное доменное имя (FQDN) <i>кластерной роли</i>, созданной на этапе настройки отказоустойчивого кластера (см. «Настройка отказоустойчивого кластера JAS», с. 132).</p>

Поле конфигурирующего	Имя параметра в реестре	Описание
Использовать аутентификацию	WithSecurity	<p>Установите флаг, если для подключения к интерфейсу OTP-клиентов на сервере JAS следует использовать аутентификацию.</p> <p>В случае если при установленном флаге в полях Логин JAS и Пароль JAS (см. ниже) указаны значения, то аутентификация будет осуществляться от имени учетной записи, указанной в данных аутентификационных параметрах.</p> <p>В случае если при установленном флаге в полях Логин JAS и Пароль JAS ничего не указано, то для подключения к интерфейсу OTP-клиентов на сервере JAS будет использоваться учётная запись локальной системы.</p> <p>Допустимы следующие значения параметра WithSecurity:</p> <ul style="list-style-type: none"> • True – проверка подлинности Windows включена. Значение соответствует включённому флагу Использовать аутентификацию. В случае если в полях Логин JAS и Пароль JAS (см. ниже) указаны значения, то аутентификация будет осуществляться от имени учетной записи, указанной в данных аутентификационных параметрах. В случае если в полях Логин JAS и Пароль JAS ничего не указано, то для подключения к интерфейсу OTP-клиентов на сервере JAS будет использоваться учётная запись локальной системы; • False – проверка подлинности Windows отключена (значение по умолчанию). Значение соответствует отключённому флагу Использовать аутентификацию. <p>Если отключить флаг Использовать аутентификацию, взаимодействие через интерфейс OTP-клиентов на сервере JAS будет происходить анонимно – в этом случае задавать значения для настроек AuthorizeAsGroupMember и AuthorizationGroupStore (см. раздел «Настройка сетевых программных интерфейсов JAS», с. 19) необязательно, т.к. в этом случае они ни на что не влияют.</p> <p> В настоящем документе рассматривается сценарий, в котором проверка подлинности Windows включена</p>
Логин JAS	JASUsername	<p>Имя пользователя, входящего в группу с правом подключения по интерфейсу для OTP-клиентов. В настоящем документе для примера используется пользователь NPS2JAS, входящий в группу JAS Clients (см. «Предварительные действия», с. 15, и «Настройка сетевых программных интерфейсов JAS», с. 19).</p> <p> Имя пользователя следует задавать без указания домена, например NPS2JAS (а не NPS2JAS@test.com или TEST\NPS2JAS).</p> <p>Если в настоящей настройке не указывать никакого значения, для доступа к интерфейсу OTP-клиентов будет использоваться текущая учётная запись, от имени которой запущена служба AD FS</p>
Пароль JAS	JASPassword	<p>Пароль пользователя, указанного в настройке JASUsername (выше).</p> <p> Важно! После задания параметра JASPassword при запуске плагина указанная строка будет зашифрована и записана в параметр JASEncryptedPassword, а параметр JASPassword будет удален. Расшифровка параметра возможна только при работе плагина под той же учетной записью, под которой производилось зашифрование. В случае необходимости смены учетной записи для запуска плагина или в случае смены пароля пользователя JAS необходимо задать в параметрах строку JASPassword. После перезапуска плагина произойдет зашифрование нового пароля, и старый пароль будет заменен</p>

Поле конфигулятора	Имя параметра в реестре	Описание
Поддерживаемые протоколы	SecurityProtocols	<p>Список поддерживаемых протоколов шифрования для обмена данных между сетевыми узлами. Представляются списком через запятую (например: Ssl3, Tls, Tls11, Tls12). Допустимые значения:</p> <ul style="list-style-type: none"> • Ssl3; • Tls; • Tls11; • Tls12. <p>По умолчанию указываются все допустимые типы протоколов</p>
<Секция> Параметры аутентификации		
Выбор типа аутентификации	AuthTypeSelection	<p>Режим выбора типа аутентификации, если их задано более одного (см. параметр AuthTypes, выше). Допустимые значения:</p> <p>Auto – автоматический; Manual – ручной</p> <p>Ручной режим позволяет пользователю перед началом аутентификации самому выбрать подходящий тип аутентификации (в виде меню/списка; в текущей версии JAS это опции «Вход по OTP-коду», «Вход по коду из SMS» и «Вход по Push»). При автоматическом режиме выбор осуществляется согласно приоритету (подробнее см. в описании параметра AuthTypes).</p> <p>Значение по умолчанию: Auto.</p>
Типы аутентификации	AuthTypes	<p>Поддерживаемые типы аутентификации и их приоритет. Текстовое поле. Подробнее логика использования параметра AuthTypes описана в Табл. 29, с. 112.</p> <p>Допустимые значения:</p> <p>Messaging – аутентификация в JAS осуществляется посредством Messaging-токенов; OTP – аутентификация в JAS осуществляется посредством OTP-токенов; Push – аутентификация в JAS осуществляется посредством Push-токенов.</p> <p>Допускается одновременное указание обоих типов (указываются через запятую); приоритет типа аутентификации устанавливается порядком его следования (у первого – выше).</p> <p>Значение по умолчанию: "Messaging, OTP, Push"</p> <p> Примечание.</p> <ol style="list-style-type: none"> 1. Аутентификация доступна для указанного типа аутентификации, если на сервере существует хотя бы один незаблокированный токен соответствующего типа (OTP или Messaging), принадлежащий текущему пользователю. Если аутентификация не доступна для первого из указанных поддерживаемых типов аутентификации, то проверяется доступность аутентификации для следующего поддерживаемого типа аутентификации. 2. В случае неудачного завершения аутентификации по одному из доступных типов (например при исчерпании числа попыток ввода пароля), процесс аутентификации завершается (второй тип аутентификации не задействуется).

Поле конфигулятора	Имя параметра в реестре	Описание
Количество повторов	RetriesCount	<p>Кол-во доступных пользователю <i>дополнительных</i> попыток аутентификации (т.е. ввода одноразового пароля) посредством OTP-токена. (Настройка не действует в отношении Messaging-токенов)</p> <p>Значение по умолчанию: 3</p> <p> Важно!</p> <ol style="list-style-type: none"> 1. При обновлении JAS-плагина для AD FS с версии 1.6 до версии 1.7 в случае если значение параметра RetriesCount было больше или равно 1, данное значение следует уменьшить на 1 (в версии JAS 1.6 данный параметр обозначал общее число попыток аутентификации). 2. Настройка представляет собой условное ограничение (действует только в рамках текущего сеанса работы пользователя с web-формой при вводе одноразового пароля). Реальное ограничение числа попыток ввода пользователем одноразового пароля, превышение которого приводит к блокировке всех OTP-токенов пользователя, производится в серверном агенте JAS с помощью настройки Максимальное количество неудачных попыток аутентификации (см. Табл. 22, с. 54).
Проводить аутентификацию, если пользователь не обнаружен в JAS	UserNotFoundAction	<p>Действия JAS-плагина, если пользователь, который пытается аутентифицироваться, не зарегистрирован в JAS. Подробнее логика обращения к параметру UserNotFoundAction описана в Табл. 29, с. 112.</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • Accept (флаг установлен) – автоматическая успешная аутентификация (решение об успешной аутентификации принимается вне сервера JAS); • Reject (флаг не установлен) – отклонять запрос. <p>Значение по умолчанию: Reject</p>
Проводить аутентификацию, если не обнаружен токен в JAS	TokensNotFou ndAction	<p>Действия JAS-плагина, если у пользователя, обратившегося с запросом на аутентификацию, в JAS зарегистрированы OTP- и/или Messaging-токены, но все они заблокированы (отключены). Подробнее логика обращения к параметру TokenNotFoundAction описана в Табл. 29, с. 112.</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • Accept (флаг установлен) – автоматическая успешная аутентификация (решение об успешной аутентификации принимается вне сервера JAS); • Reject (флаг не установлен) – отклонять запрос. <p>Значение по умолчанию: Reject</p>
<Секция> Параметры messaging		
Идентификатор системы	MessagingSyst emId	<p>Идентификатор внешней системы, используется для поиска на сервере JAS Messaging-токена, принадлежащего данному пользователю (при выпуске токена определяется параметром Идентификатор системы в профиле выпуска Messaging-токенов, см. руководство по функциям управления JMS [3]).</p> <p>Значение по умолчанию: пустая строка</p>
Текст SMS	MessagingAddi tionalInfo	<p>Текст, который будет отправляться в SMS пользователю вместе с одноразовым паролем.</p> <p>Значение по умолчанию: пустая строка</p>

Поле конфигулятора	Имя параметра в реестре	Описание
Время жизни кода (с)	MessagingTtl	<p>Время жизни для одноразового пароля (в секундах, напр. 180), в течение которого ответ пользователя будет актуальным.</p> <p>Если параметр не задан (пустая строка), то сервер JAS в процессе аутентификации будет использовать значение, заданное в свойствах Messaging-токена (см. параметр Время жизни OTP (с), в свойствах Messaging-токена или профиля выпуска Messaging-токенов; руководство по функциям управления JMS [3]).</p> <p>Значение по умолчанию: пустая строка (не задано)</p>
Таймаут между попытками (мс)	MessagingRetryDelay	<p>Таймаут между попытками аутентификации посредством Messaging-токена (в миллисекундах), например 5000.</p> <p>Параметр применяется к работе непосредственно сервера JAS, который на его основе принимает решение о возможности приёма попытки аутентификации. При попытке аутентификации, произошедшей до истечения указанного таймаута, возникает ошибка аутентификации.</p> <p>Если параметр не задан (пустая строка), то сервер JAS в процессе аутентификации будет использовать либо собственное значение по умолчанию (5000 мс), либо значение, заданное в свойствах Messaging-токена (см. параметр Задержка генерации OTP (мс) в свойствах Messaging-токена или профиля выпуска Messaging-токенов; см. руководство по функциям управления JMS [3]).</p> <p>Значение по умолчанию: пустая строка (не задано)</p>
Период блокировки (с)	MessagingNewSmsTimeout	<p>Задержка (в секундах) доступности кнопки для отправки нового одноразового пароля (OTP).</p> <p>Параметр имеет действие только в рамках пользовательского интерфейса (не передается на сервер JAS и не регулирует его работу).</p> <p>Если значение больше нуля – кнопка отправки нового OTP будет доступна по истечению указанного времени.</p> <p>Если значение равно нулю – кнопка будет доступна всегда.</p> <p>Если значение меньше нуля – кнопка никогда не будет показываться.</p> <p> Примечание. Значение параметра должно быть согласовано со значением параметра Таймаут между попытками (мс) (MessagingRetryDelay), чтобы отправленное из пользовательского интерфейса значение OTP-секрета могло быть принято сервером JAS для принятия решения об аутентификации.</p> <p>Значение по умолчанию: 60</p>
<Секция> Параметры Push		
Метаданные для A2FA	PushMetadata	<p>Дополнительная информация (метаданные), которые будут отображаться на экране мобильного приложения Aladdin 2FA при отправке Push-запроса на аутентификацию. Строковый тип.</p> <p>Значение по умолчанию: ADFS</p>

Поле конфигулятора	Имя параметра в реестре	Описание
Таймаут между попытками (с)	PushNewAttemptTimeout	Интервал времени (в секундах) между повторами попыток отправки Push-запроса на мобильное устройство. В случае нарушения таймаута выводится ошибка следующего вида: «Частота доставки Push может быть ограничена - не чаще чем один раз в %PushNewAttemptTimeout% с.» Строковый тип. Допускается вносить только числовые значения или пустую строку. Значение по умолчанию: 60
Период блокировки (с)	PushSendTimeout	Максимальный таймаут (в секундах) ожидания подтверждения Push-запроса пользователем (нажатия пользователем на кнопку подтверждения или отказа). В случае если от пользователя за указанный период подтверждение или отказа от аутентификации не поступает, то возникает ошибка аутентификации. Строковый тип. Допускается вносить только числовые значения или пустую строку. Значение по умолчанию: 60
<настройка отсутствует в графическом конфигуляторе, осуществляется только в реестре>	InstallPath	Путь к установленному JAS-плагину для AD FS. (Требуется службе AD FS для загрузки пользовательских html-страниц) Значение по умолчанию: C:\Program Files\Aladdin\JAS ADFS Plugin\
Кнопки управления		
По умолчанию		Привести значения в форме к значениям по умолчанию (например, для последующего редактирования или сохранения в реестр)
Загрузить из реестра		Загрузить в форму значения из реестра. (При запуске конфигулятора значения из реестра автоматически загружаются в поля формы.)
Сохранить в реестр		Сохранение текущих значений из формы в реестр. В момент нажатия на кнопку пользователю предлагается перезапуск службы ADFS, Рис. 87.
Сохранить в файл		Отображаемые в форме параметры можно сохранить в рег-файл для последующего восстановления настроек или их распространения на узлы кластера (в случае кластерной конфигурации JAS)
Загрузить из файла		Конфигуратор позволяет загрузить в форму параметры плагина из рег-файла, ранее сохраненного с помощью кнопки Сохранить в файл



Примечание. Указанные в таблице параметры реестра (графа **Имя параметра в реестре**) располагаются в разделе реестра [HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JAS ADFS Plugin], Рис. 86.

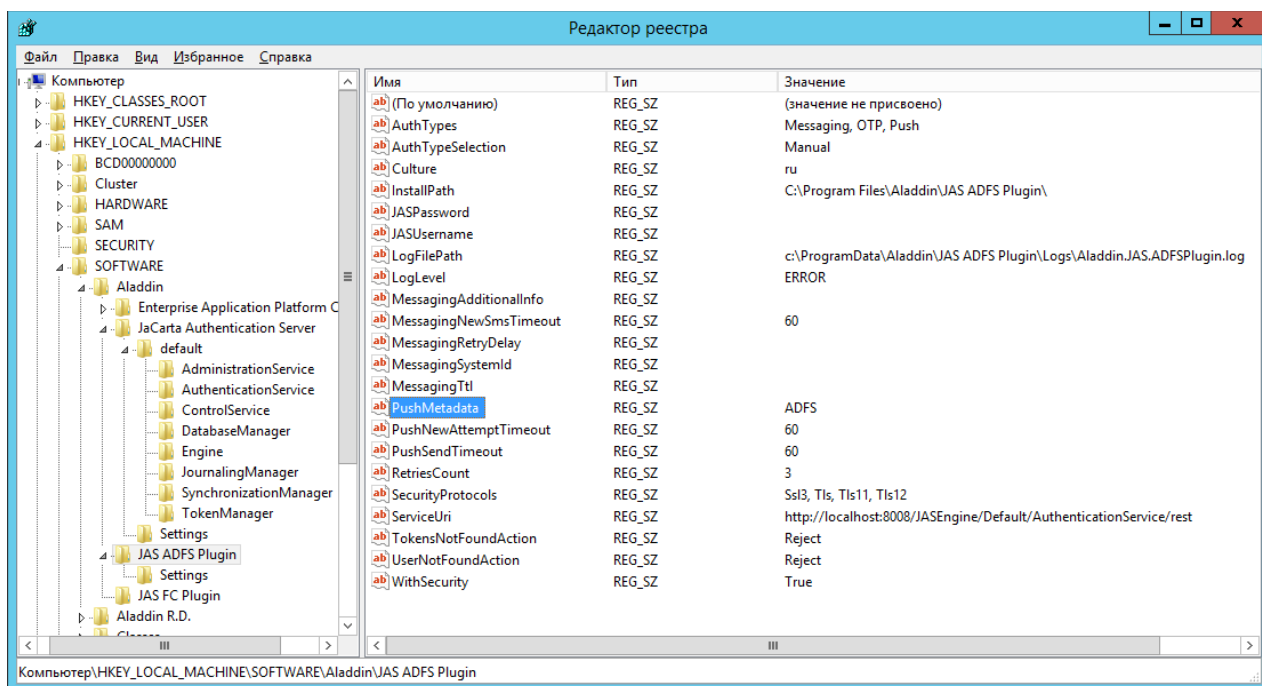


Рис. 86 – Настройки JAS-плагина для AD FS в реестре

- Если служба AD FS запускается от имени выделенной учетной записи (например от учетной записи пользователя), то необходимо предоставить данной учетной записи полные права (разрешение Full Control) на раздел реестра [HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JAS ADFS Plugin]
- По нажатию на кнопку **Сохранить в реестр** отредактированные значения полей будут сохранены в реестр, при этом пользователю будет предложено выполнить автоматическую перезагрузку службы AD FS с тем, чтобы новые значения настроек вступили в силу, Рис. 87.

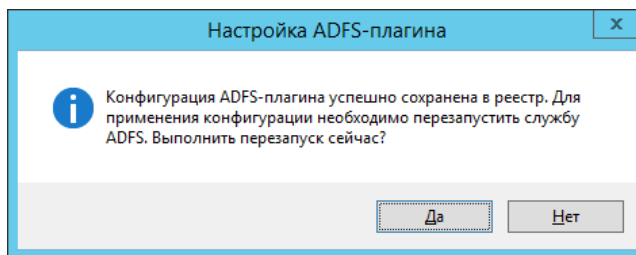


Рис. 87 – Настройки JAS-плагина для AD FS в реестре



Примечание. Для перезагрузки службы можно также использовать последовательность команд:

```
net stop adfssrv
net start adfssrv
```

В некоторых случаях для вступления настроек в силу требуется перезапуск самого компьютера, где установлена служба AD FS с JAS-плагином.

После сохранения настроек JAS-плагин для AD FS готов к работе.

Табл. 29 – Иллюстрация логики работы JAS-плагина для AD FS в зависимости от состояния токенов конкретного пользователя

Состояние токена		Действие JAS-плагина в зависимости от установленного типа аутентификации (значения параметра AuthTypes)			
ОТР-токен	Messaging-токен	AuthTypes: ОТР, Messaging	AuthTypes: Messaging, ОТР	AuthTypes: ОТР	AuthTypes: Messaging
Отсутствует	Отсутствует	UserNotFoundAction	UserNotFoundAction	UserNotFoundAction	UserNotFoundAction
Отсутствует	Заблокирован	TokensNotFoundAction	TokensNotFoundAction	UserNotFoundAction	TokensNotFoundAction
Отсутствует	Действует	Аутентификация по Messaging	Аутентификация по Messaging	UserNotFoundAction	Аутентификация по Messaging
Заблокирован	Отсутствует	TokensNotFoundAction	TokensNotFoundAction	TokensNotFoundAction	UserNotFoundAction
Заблокирован	Заблокирован	TokensNotFoundAction	TokensNotFoundAction	TokensNotFoundAction	TokensNotFoundAction
Заблокирован	Действует	Аутентификация по Messaging	Аутентификация по Messaging	TokensNotFoundAction	Аутентификация по Messaging
Действует	Отсутствует	Аутентификация по ОТР	Аутентификация по ОТР	Аутентификация по ОТР	UserNotFoundAction
Действует	Заблокирован	Аутентификация по ОТР	Аутентификация по ОТР	Аутентификация по ОТР	TokensNotFoundAction
Действует	Действует	Аутентификация по ОТР	Аутентификация по Messaging	Аутентификация по ОТР	Аутентификация по Messaging



Примечания к Табл. 29:

- Состояние *Заблокирован* подразумевает блокировку всех токенов соответствующего типа (например, ОТР), а состояние *Действует* подразумевает наличие хотя бы одного незаблокированного токена соответствующего типа (например, ОТР).
- Информация, приведенная в Табл. 29 имеет иллюстративный характер для комбинации из двух значений параметра AuthTypes (а именно ОТР и Messaging). Если в список значений будет добавлено также значение Push, то описание логики принятия решений будет дополнена следующим:
 - Если метод PUSH имеет наивысший приоритет и Push-токен не заблокирован, то произойдет аутентификация по нему.
 - Если метод PUSH имеет наивысший приоритет и Push-токен заблокирован, то право аутентификации переходит к следующему по приоритету методу (см. Табл. 29);
 - Если метод PUSH имеет наивысший приоритет но Push-токен у пользователя отсутствует, то право аутентификации переходит к следующему по приоритету методу (см. Табл. 29);
 - Если метод PUSH является единственным в списке или остался последним доступным среди методов аутентификации, то:
 - Если PUSH-токен в наличии у пользователя -- осуществляется аутентификация по PUSH-токену;
 - Если PUSH-токен заблокирован, то обрабатывает опция TokensNotFoundAction;
 - Если PUSH-токен отсутствует, то обрабатывает опция UserNotFoundAction.

14.4 Проверка работы JAS-плагина для AD FS

Для проверки работы JAS-плагина для AD FS выполните следующие действия:

- Убедитесь в том, что JAS-плагин для AD FS установлен и настроен в соответствии с предыдущими разделами.
- Используя консоль управления JMS выпустите аппаратный или программный ОТР-токен (см. разделы «Выпуск аппаратных ОТР-токенов» и «Выпуск программных ОТР-токенов»)

- (мобильное приложение Aladdin 2FA)» в руководстве администратора по функциям управления JMS [3]).
7. В случае OTP-токена с алгоритмом HOTP выполните его синхронизацию (см. раздел «Синхронизация значений OTP (только для токенов HOTP)» в руководстве администратора по функциям управления JMS [3]).
 8. В браузере Internet Explorer перейдите по ссылке https://<имя_Службы_федерации>/adfs/ls/idpinitiatedsignon (в случае если браузер запущен на сервере, хостирующем AD FS, можно использовать следующую ссылку: <https://localhost/adfs/ls/idpinitiatedsignon>).



Примечание. В версии ОС Microsoft Windows Server 2016 по умолчанию отключена тестовая веб-страница AD FS. Для включения этой возможности на сервере, хостирующем AD FS, следует выполнить следующую PowerShell-команду:

```
Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
```

Подробнее о решении проблемы см. по ссылке: <https://blogs.technet.microsoft.com/rmilne/2017/06/20/how-to-enable-idpinitiatedsignon-page-in-ad-fs-2016/>

Открется веб-страница следующего вида:

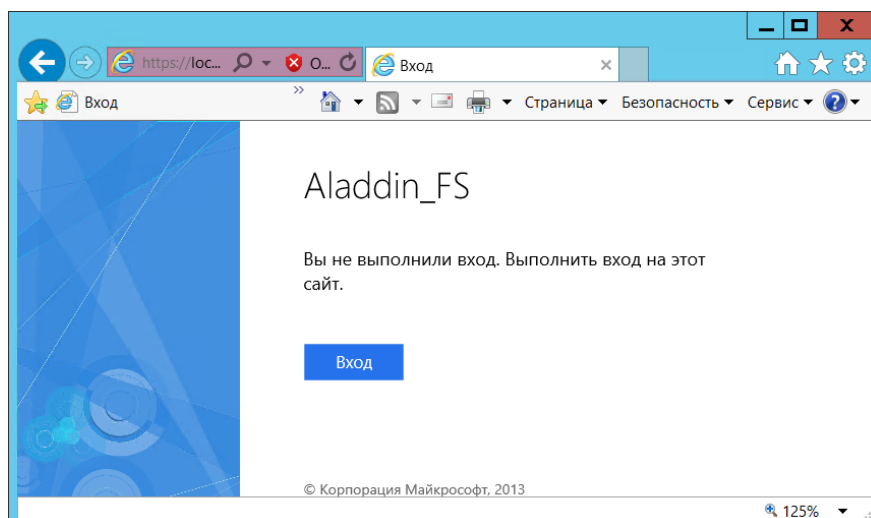


Рис. 88 – Стартовая проверочная страница службы федерации AD

где **Aladdin_FS** – отображаемое имя службы федерации, заданное при ее установке.



Примечание. В общем случае строку <имя_Службы_федерации> можно посмотреть в свойствах AD FS, в оснастке MMC **Управление AD FS**, см. Рис. 89).

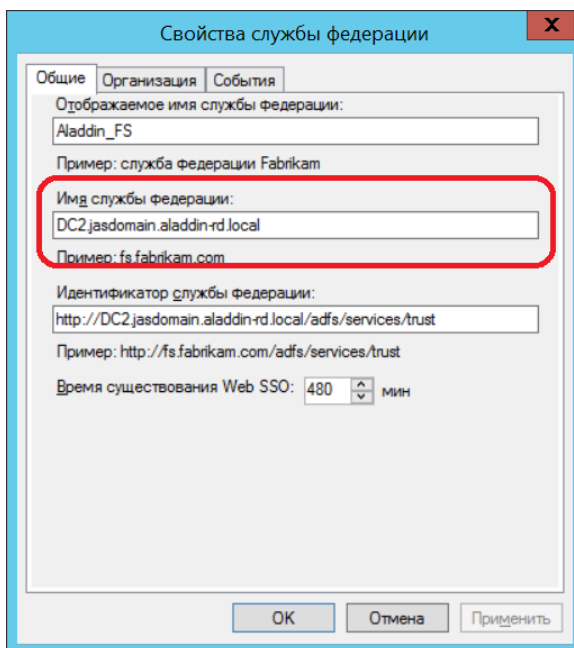


Рис. 89 – Просмотр имени Службы федерации Active Directory

9. Нажмите **Вход**. Отобразится страница, как на Рис. 90 (для случая настройки реестра *AuthTypeSelection=Auto*, см. Табл. 28, с. 105) или как на Рис. 91 (для случая настройки реестра *AuthTypeSelection=Manual*).

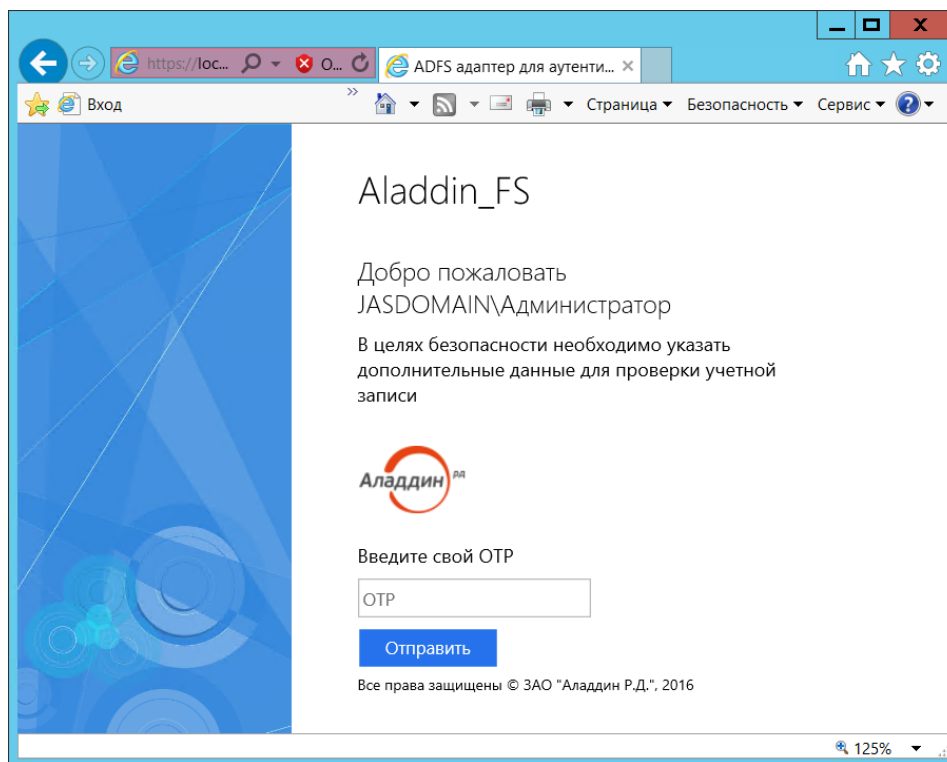


Рис. 90 – Веб-страница AD FS, использующей OTP-аутентификацию посредством JAS-плагина

где **JASDOMAIN\Администратор** – имя пользователя, под учетной записью которого был выполнен данный HTTP-запрос.

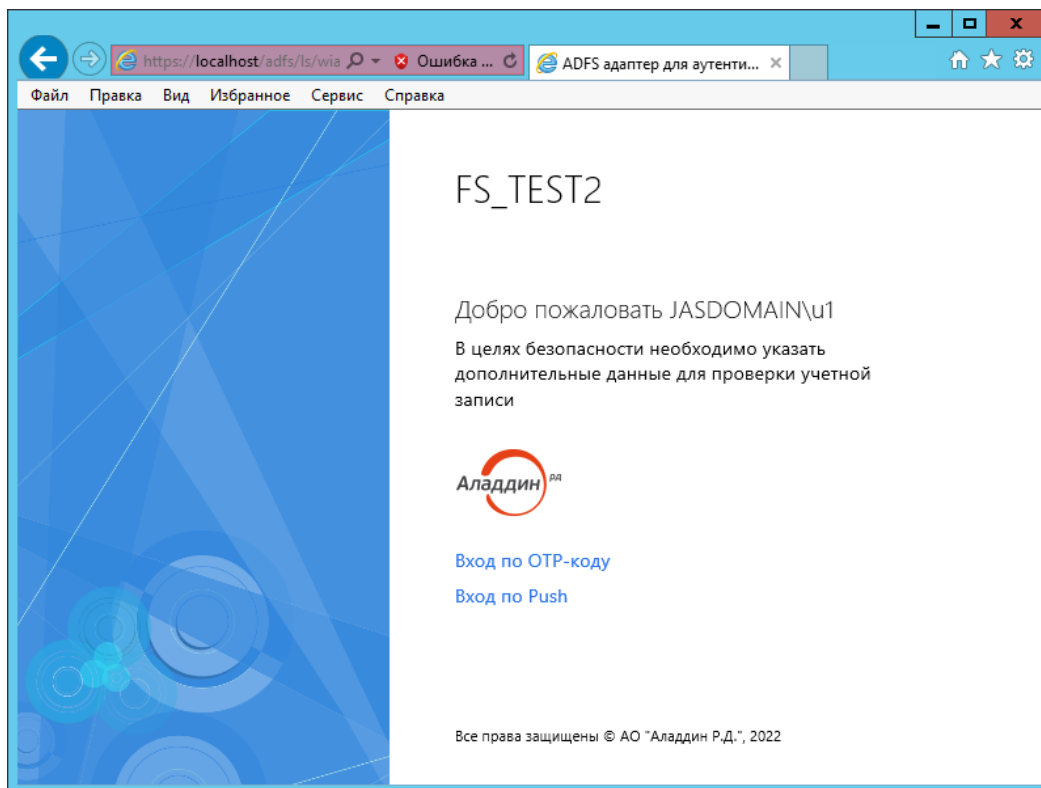



Рис. 91 – Веб-страница AD FS, с примером множественного ручного выбора типа аутентификации

В случае если в браузере отражены данные веб-страницы, служба федерации Active Directory и JAS-плагин для AD FS настроены правильно.

15. Установка и настройка JAS-плагина для MS RDG

JAS-плагин (модуль расширения) для MS RDG позволяет пользователям выполнять аутентификацию на шлюзе Microsoft RDG с применением усиленной аутентификации на основе OTP для дальнейшего подключения к удаленному рабочему столу. Подключение происходит в автоматизированном режиме из Web-браузера с динамической генерацией RDP-файла для каждого инициируемого пользователем сеанса работы с удаленным рабочим столом.

 **Важно!** Аутентификация на шлюзе MS RDG применением JAS-плагина возможна только при использовании программных и аппаратных OTP-токенов (Messaging-токены и U2F-аутентификаторы не поддерживаются).

15.1 Подготовка к установке JAS-плагина для MS RDG

Перед установкой JAS-плагина установите службу роли *Шлюза удаленных рабочих столов* (имя службы – «Шлюз удаленных рабочих столов», Remote Desktop Gateway) в соответствии с документацией Microsoft Windows Server.

15.2 Установка JAS-плагина для MS RDG

Чтобы установить JAS-плагин для MS RDG, на сервере с установленной ролью *Шлюза удаленных рабочих столов* выполните следующие действия.

1. Запустите файл установки: **Aladdin.JAS.RDGPlugin-X.X.X.XXX-x64.msi** (только для 64-битных систем).
Отобразится следующее окно.

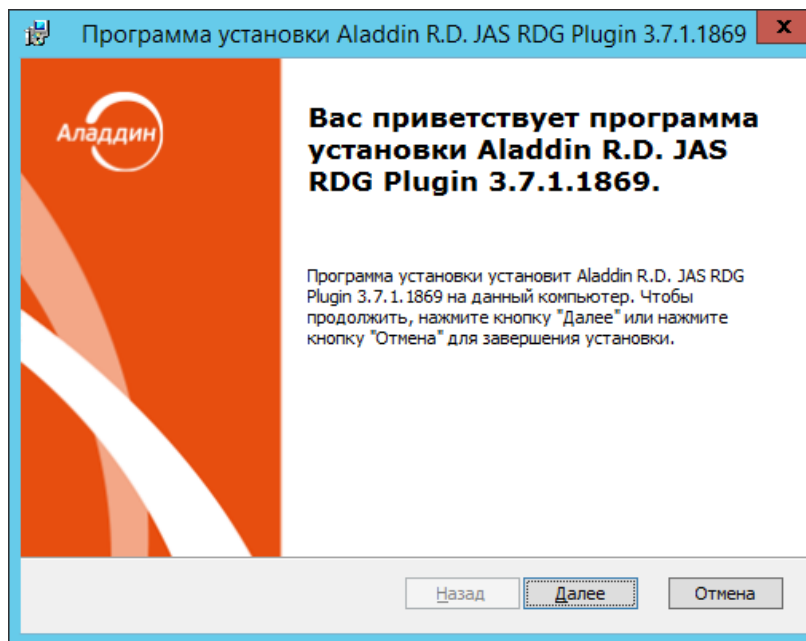


Рис. 92 – Окно приветствия мастера установки JAS-плагина для MS RDG

2. Нажмите **Далее**. В окне лицензионного соглашения выберите **Я принимаю условия лицензионного соглашения**, после чего нажмите **Далее**.
3. В окне выбора вида установки выберите **Полная** и следуйте указаниям мастера до окончания установки плагина.

- По завершении установки отобразится следующее окно.

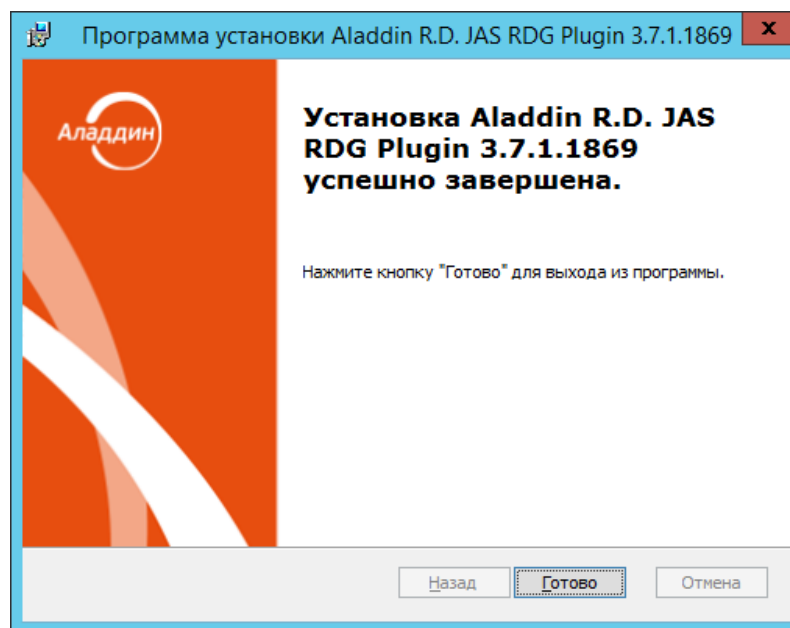


Рис. 93 – Окно завершения установки

- Нажмите **Готово**.
Отобразится следующее сообщение.

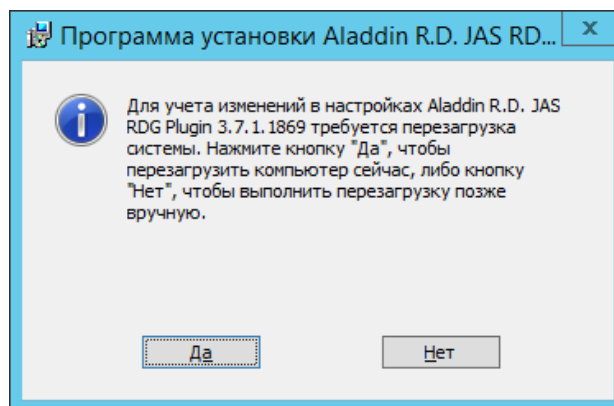


Рис. 94 – Предупреждение о необходимости перезагрузки

- Нажмите **Нет**.
- Дождитесь автоматической загрузки графического конфигуратора JAS-плагина для MS RDG и переходите к его настройкам (см. ниже)

15.3 Настройка JAS-плагина для MS RDG

После установки JAS-плагина для MS RDG автоматически откроется окно так называемого «конфигуратора» **Настройка JAS-плагина для MS RDG** (Рис. 95, с. 118).

Если вы закрыли окно конфигуратора, то можете запустить его вручную, см. «Работа с конфигуратором JAS-плагина для MS RDG», ниже.

15.3.1 Работа с конфигуратором JAS-плагина для MS RDG

Ниже описана процедура работы с конфигуратором **Настройка JAS-плагина для MS RDG**.

1. В меню **Пуск** выберите **JaCarta Authentication Server -> Настройка JAS-плагина для MS RDG**. Отобразится следующее окно.

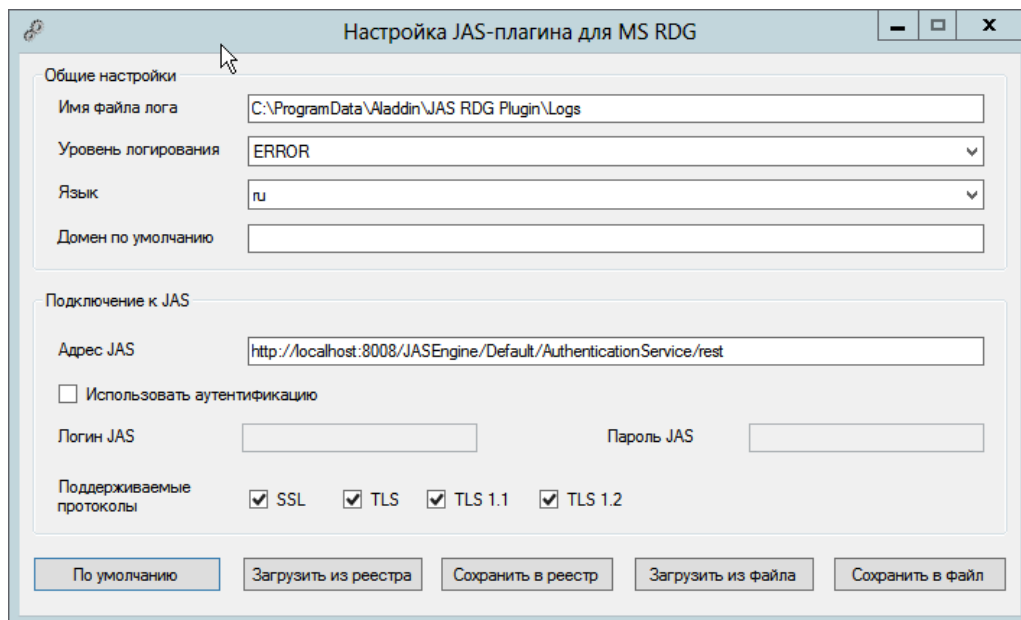


Рис. 95 – Окно Настройка JAS плагина для MS RDG

При загрузке конфигуратор считывает текущее содержание настроек плагина из реестра.

Примечание. При редактировании полей формы можно воспользоваться всплывающей подсказкой при наведении курсора мыши на поле ввода (Рис. 96)

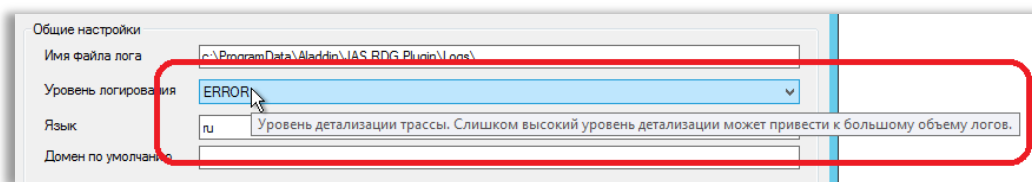






Рис. 96 – Использование всплывающей подсказки в полях формы

2. Выполните настройку, руководствуясь Табл. 30.

Табл. 30 - Настройка JAS-плагина для MS RDG

Поле конфигуратора	Имя параметра в реестре	Описание
<Секция> Общие настройки		
Имя файла лога	LogFilePath	Путь, по которому будет сохраняться файл журнала

Поле конфигурируемого параметра	Имя параметра в реестре	Описание
Уровень логирования	LogLevel	<p>Уровень ведения журнала событий.</p> <ul style="list-style-type: none"> • OFF – ведение журнала событий отключено; • FATAL – неустраняемая ошибка; • ERROR – ошибка (значение по умолчанию); • WARN – предупреждение; • INFO – информация; • DEBUG – отладка; • ALL – показывать все события. <p> Каждый последующий уровень включает все предыдущие (кроме OFF), например, если выставлено значение INFO, то будут отображаться сообщения уровней: INFO, WARN, ERROR, FATAL</p>
Язык	Culture	<p>Язык пользовательского интерфейса JAS-плагина. Допустимые значения:</p> <ul style="list-style-type: none"> • en (английский язык); • ru (русский язык). <p>Значение по умолчанию: ru</p> <p> Примечание. В текущей версии параметр не используется. Во всех интерфейсах JAS-плагина для MS RDG используется только русский язык.</p>
Домен по умолчанию	DefaultUserDomain	<p>Значение по умолчанию имени домена пользователя. Данное значение добавляется к имени пользователя при аутентификации в web-форме JAS-плагина, если в плагин было передано имя пользователя без домена.</p> <p>Значение по умолчанию: пустая строка</p>
<Секция> Подключение к JAS		
Адрес JAS	ServiceUri	<p>Адрес сервера JAS в следующем формате:</p> <p>http://<FQDN-имя сервера>:8008/JAS/Engine/Default/AuthenticationService/rest.</p> <p>где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com; либо, в случае кластерной конфигурации JAS, полное доменное имя (FQDN) <i>кластерной роли</i>, созданной на этапе настройки отказоустойчивого кластера (см. «Настройка отказоустойчивого кластера JAS», с. 132).</p>
Использовать аутентификацию	<без параметра в реестре>	<p>Установите флаг, если для подключения к интерфейсу OTP-клиентов на сервере JAS следует использовать Windows-аутентификацию. Для этого в полях Логин JAS и Пароль JAS (ниже) следует указать аутентификационные данные учётной записи, от имени которой будет осуществляться подключение.</p> <p>В случае если флаг не установлен, подключение к интерфейсу OTP-клиентов на сервере JAS будет осуществляться анонимно, т.е. без аутентификации.</p>

Поле конфигулятора	Имя параметра в реестре	Описание
Логин JAS	JASUsername	Имя пользователя, входящего в группу с правом подключения по интерфейсу JAS для OTP-клиентов (в данном случае OTP-клиентом является плагин для MS RDG). В настоящем документе для примера используется пользователь NPS2JAS , входящий в группу JAS Clients (см. «Предварительные действия», с. 15, и «Настройка сетевых программных интерфейсов JAS» на с. 19).  Имя пользователя следует задавать без указания домена, например NPS2JAS (а не NPS2JAS@test.com или TEST\NPS2JAS).
Пароль JAS	JASPassword	Пароль пользователя, указанного в настройке JASUsername (выше).  Важно! После задания параметра JASPassword при запуске плагина указанная строка будет зашифрована и записана в параметр JASEncryptedPassword , а параметр JASPassword будет удален. Расшифровка параметра возможна только при работе плагина под той же учетной записью, под которой производилось зашифрование. В случае необходимости смены учетной записи для запуска плагина или в случае смены пароля пользователя JAS необходимо задать в параметрах строку JASPassword . После перезапуска плагина произойдет зашифрование нового пароля, и старый пароль будет заменен
Поддерживаемые протоколы	SecurityProtocols	Список поддерживаемых протоколов шифрования для обмена данных между сетевыми узлами. Представляются списком через запятую (например: Ssl3, Tls, Tls11, Tls12). Допустимые значения: <ul style="list-style-type: none"> • Ssl3; • Tls; • Tls11; • Tls12. По умолчанию указываются все допустимые типы протоколов
Кнопки управления		
По умолчанию		Привести значения в форме к значениям по умолчанию (например, для последующего редактирования или сохранения в реестр)
Загрузить из реестра		Загрузить в форму значения из реестра. (При запуске конфигулятора значения из реестра автоматически загружаются в поля формы.)
Сохранить в реестр		Сохранение текущих значений из формы в реестр. В момент нажатия на кнопку пользователю предлагается перезапуск службы NPS, Рис. 98.
Сохранить в файл		Отображаемые в форме параметры можно сохранить в рег-файл для последующего восстановления настроек или их распространения на узлы кластера (в случае кластерной конфигурации JAS)
Загрузить из файла		Конфигуратор позволяет загрузить в форму параметры плагина из рег-файла, ранее сохраненного с помощью кнопки Сохранить в файл



Примечание. Указанные в таблице параметры реестра (графа **Имя параметра в реестре**) располагаются в разделе реестра [HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JAS RDG Plugin], Рис. 97.

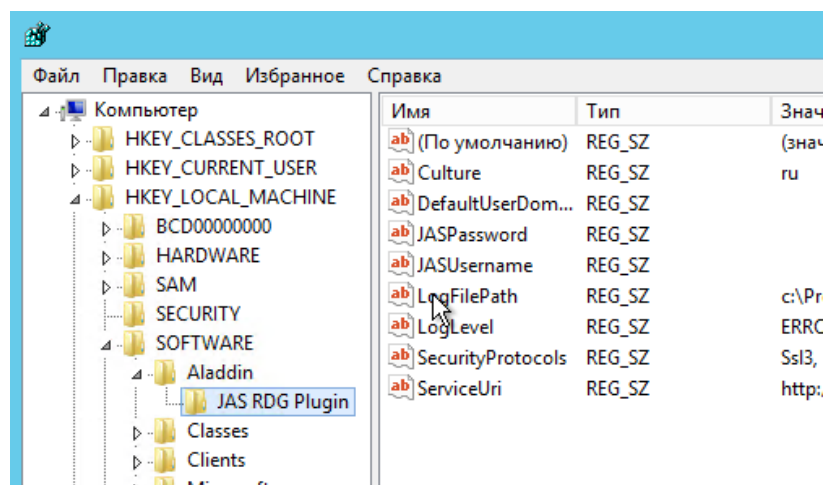


Рис. 97 – Настройки JAS-плагина для MS RDG

- По нажатии на кнопку **Сохранить в реестр** отредактированные значения полей будут сохранены в реестр, при этом пользователю будет предложено выполнить автоматическую перезагрузку службы MS RDG с тем, чтобы новые значения настроек вступили в силу, Рис. 98.

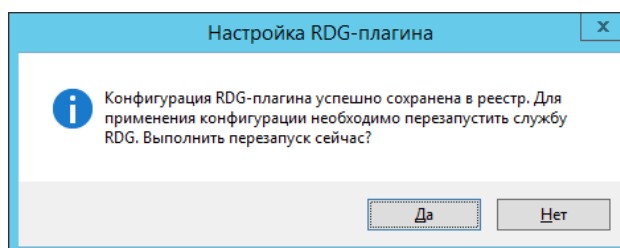



Рис. 98 – Диалог перезапуска службы MS RDG

- В редакторе реестра предоставьте права полного доступа учетной записи, от имени которой запускается служба *Шлюза удаленных рабочих столов* записи (по умолчанию это учетная запись `NETWORK_SERVICE`), к разделу реестра [HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JAS RDG Plugin]
- После внесения изменений в реестр перезагрузите компьютер.
- После перезагрузки компьютера убедитесь в том, что JAS-плагин для MS RDG загрузился корректно (в файле журнала – по умолчанию `C:\ProgramData\Aladdin\JAS RDG Plugin\Logs\Aladdin.JAS.RDGPlugin.log` – не должно быть записей об ошибках загрузки).
- Настройте доступ к папке `C:\Program Files\Aladdin\JAS RDG Plugin\RDGPluginWeb` через веб-сервер (IIS или любой другой, предоставляющий доступ к статическому контенту). Убедитесь, что веб-страницы плагина для аутентификации на шлюзе RDG на соответствующих языках открываются в браузере по адресам:
 - `https://<DNS-имя сервера RDG>/RDGPluginWeb/en/index.html`
 - `https://<DNS-имя сервера RDG>/RDGPluginWeb/ru/index.html`
 где <DNS-имя сервера RDG> -- имя сервера с развернутой службой *шлюза удаленных рабочих столов*, например `rdg.test`.

8. Настройте шаблон RDP-подключения в файле `C:\Program Files\Aladdin\JAS RDG Plugin\RDGPluginWeb\scripts\rdpTemplate.js`. В соответствии с имеющимися в нём комментариями.

 **Важно!** Для обеспечения корректной работы плагина в файле шаблона необходимо указать адрес RDG-шлюза. Для этого в строке

```
...  
'gatewayhostname:s:rdg.idsol.inc', // Имя узла шлюза удаленных  
рабочих столов  
...
```

вместо `rdg.idsol.inc` укажите DNS-имя сервера с развернутой службой *шлюза удаленных рабочих столов*, например `rdg.test`.

После выполнения настроек JAS-плагин для MS RDG готов к работе.

15.4 Проверка работы JAS-плагина для MS RDG

Для проверки работы JAS-плагина для MS RDG выполните следующие действия:

1. Убедитесь в том, что JAS-плагин для MS RDG установлен и настроен в соответствии с предыдущими разделами.
2. Используя консоль управления JMS выпустите аппаратный или программный OTP-токен (см. разделы «Выпуск аппаратных OTP-токенов» и «Выпуск программных OTP-токенов (мобильное приложение Aladdin 2FA)» в руководстве администратора по функциям управления JMS [3]).
3. В случае OTP-токена с алгоритмом HOTP выполните его синхронизацию (см. раздел «Синхронизация значений OTP (только для токенов HOTP)» в руководстве администратора по функциям управления JMS [3]).
4. В web-браузере откройте страницу плагина для аутентификации на шлюзе RDG на выбранном языке, например:
`https://<DNS-имя сервера RDG>/RDGPluginWeb/ru/index.html`,
где <DNS-имя сервера RDG> – имя сервера с развернутой службой шлюза удаленных рабочих столов.

Откроется веб-страница следующего вида:

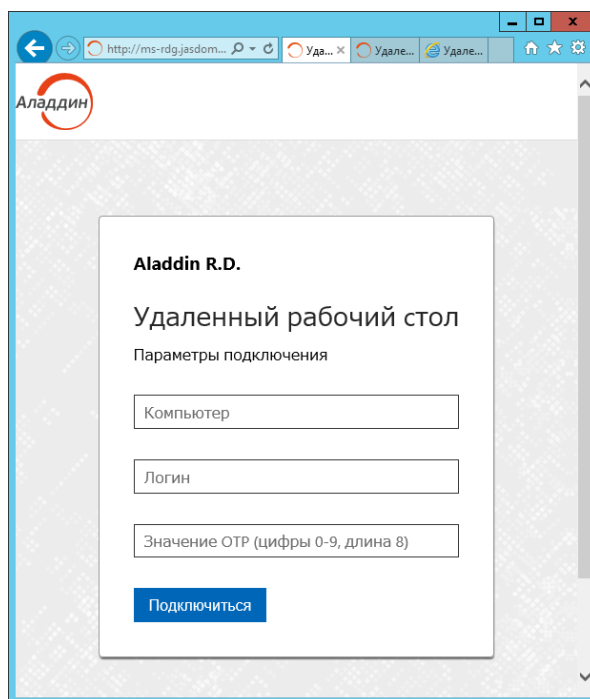


Рис. 99 – Web-страницу плагина для аутентификации на шлюзе RDG

5. Выполните следующие действия:

- 5.1. в поле **Компьютер** введите DNS-имя или IP-адрес компьютера, к которому осуществляется подключение;
- 5.2. в поле **Логин** укажите логин пользователя с указанием домена (например test\User) или без указания домена, если в параметре **DefaultUserDomain** реестра (см. «Настройка JAS-плагина для MS RDG», с. 117) указан домен по умолчанию;
- 5.3. в поле **Значение OTP ...** введите OTP-пароль из OTP-токена соответствующего пользователя;
- 5.4. нажмите **Подключиться**.

6. Сохраните (в случае запроса браузера) сформированный rdp-файл (Рис. 100):

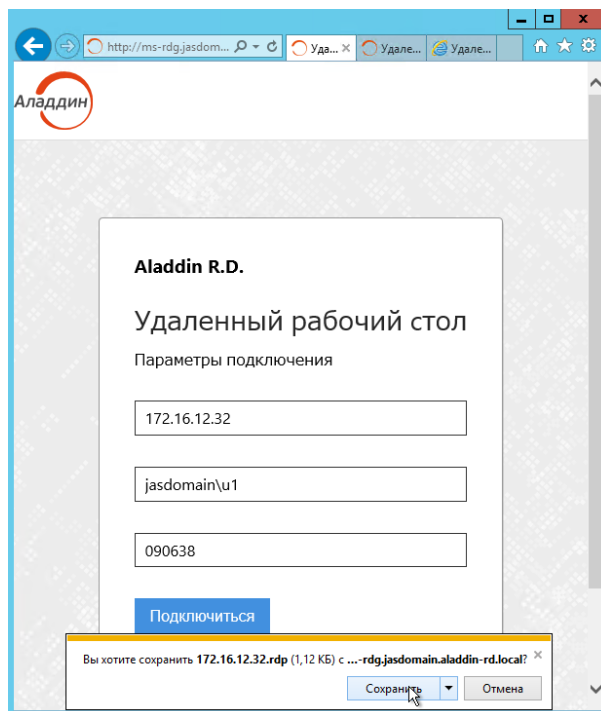


Рис. 100 – Сохранение rdp-фала на диск

7. Запустите сохраненный rdp-файл на выполнение (Рис. 101):

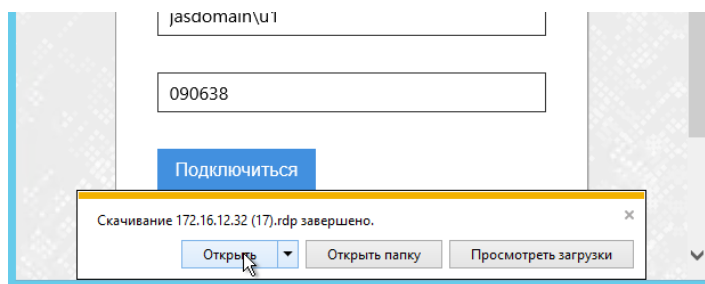


Рис. 101 – Запуск rdp-фала на выполнение

8. Дождитесь запуска процедуры подключения к удаленному рабочему столу (Рис. 102):

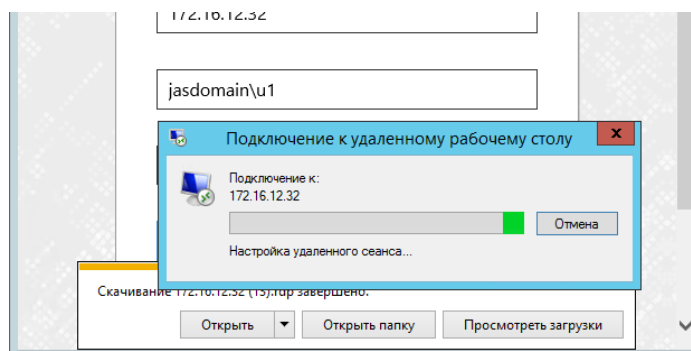


Рис. 102 – Подключение к удаленному рабочему столу

9. Введите пароль в окне подключения к удаленному рабочему столу (Рис. 103):

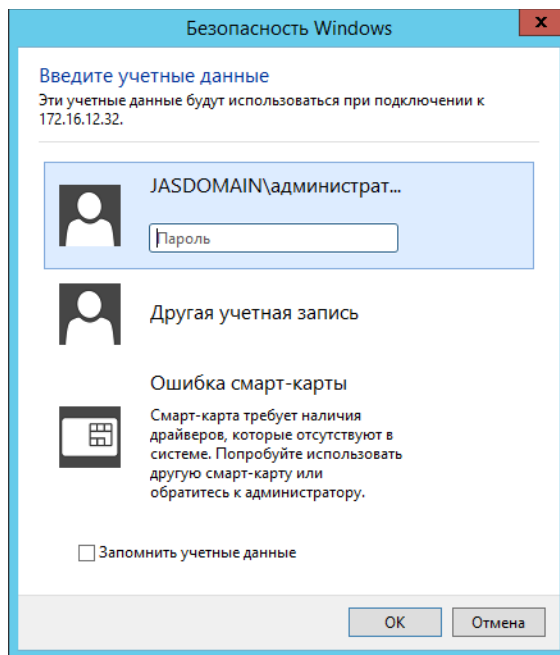


Рис. 103 – Окно ввода пароля для подключения к удаленному рабочему столу

В случае успешного открытия сеанса удаленного доступа, служба *Шлюза удаленных рабочих столов* и JAS-плагин для MS RDG настроены правильно.

15.4.1 Типовые сообщения об ошибках при аутентификации с помощью JAS-плагина для MS RDG

При вводе неверного OTP-пароля в форме аутентификации на шлюзе RDG (Рис. 99, с. 123) web-браузер отображается ошибка следующего вида.

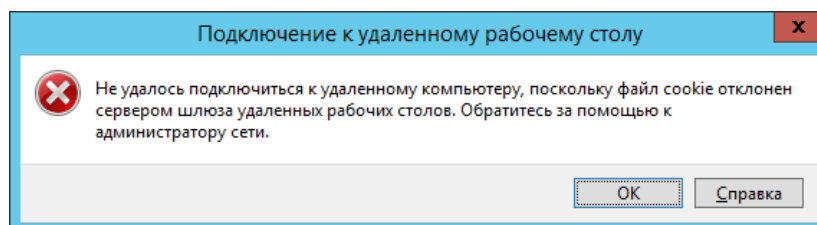


Рис. 104 – Типовое окно ошибки при вводе неверного OTP-пароля

В случае ошибок в настройке взаимодействия клиента с *шлюзом удаленных рабочих столов* может отображаться сообщение следующего вида.

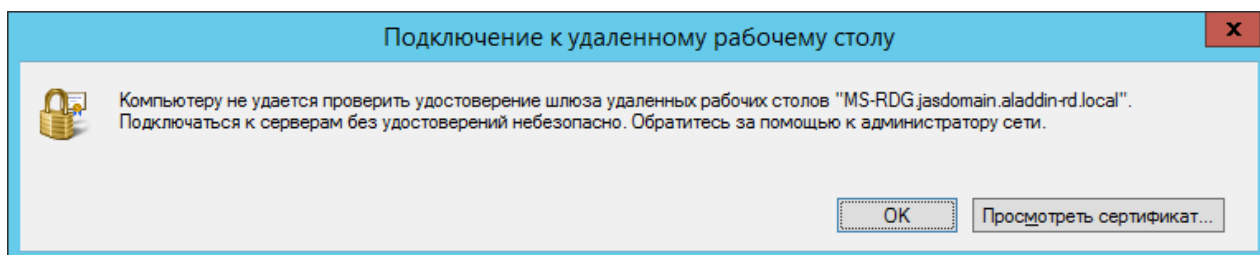


Рис. 105 – Типовое сообщение при ошибке настройки взаимодействия с Шлюзом удаленных рабочих столов

Одним из вариантов решения данной проблемы является установка сертификата шлюза удаленных рабочих машин на клиентский компьютер (с которого осуществляется удаленный доступ) в разделе *Доверенные корневые центры сертификации* хранилища компьютера.

16. Установка и настройка отказоустойчивого кластера JAS

Для организации отказоустойчивого кластера JAS используется компонент *Отказоустойчивая кластеризация* из состава ОС Windows Server, а также JAS-плагин из комплекта поставки JAS (см. раздел «Пакеты установки», с. 14) для *Службы кластеров*, развертываемой на каждом узле кластера в результате установки компонента *Отказоустойчивая кластеризация*.

16.1 Системные требования JAS-плагина для службы кластеров

Табл. 31 – Системные требования JAS-плагина для службы кластеров

Компонент	Требование
Процессор	Intel Dual-Core 2 ГГц и выше
Оперативная память	Минимум: 1 Гбайт в дополнении к объему, установленному системными требованиями FC
Место на диске	От 10 Гбайт
Операционная система	Windows Server 2012 R2
Дополнительное ПО	Microsoft .NET Framework 4.5
Другое	Установка должна осуществляться от имени учётной записи с правами администратора

Значения объема оперативной памяти приведены из расчета поддержки до 1 млн аутентификаторов (OTP-токенов и др.) при условии, что под управлением ОС функционирует только указанный JAS-плагин.

16.2 Подготовка к установке JAS-плагина для службы кластеров

Перед установкой JAS-плагина для службы кластеров на каждом узле кластера должны быть установлены:

- серверный компонент JAS (JAS Server);
- компонент *Отказоустойчивая кластеризация* из комплекта ОС Microsoft Windows Server. (После установки данного компонента на сервере – узле кластера – будет автоматически установлена *Служба кластеров*).

На каждом узле устанавливаемого кластера выполните следующие настройки:

1. Настройте *Сервер JAS* на работу с одной и той же базой данных (см. раздел «Мастер подключения к базе данных JMS», с. 31)
2. Настройте службу Aladdin JAS Engine Service (Рис. 106) так, чтобы при ее сбоях не выполнялось никаких действий, поскольку запуском и остановкой будет управлять *Служба кластеров*.

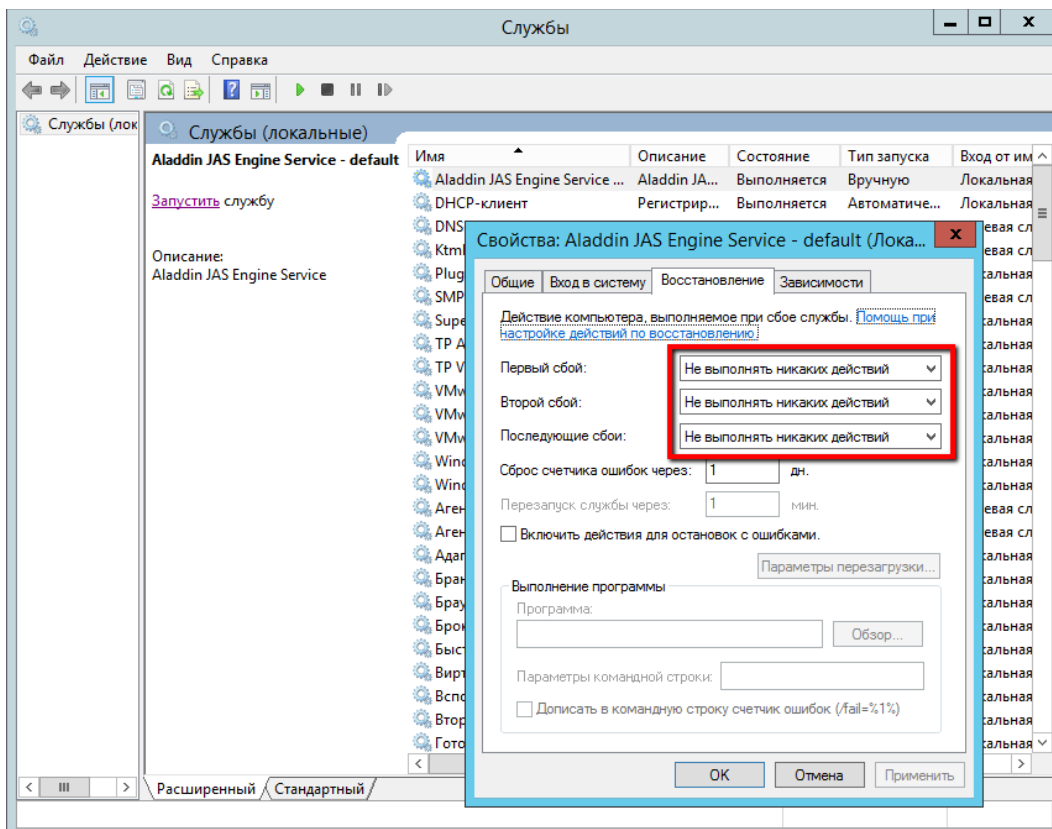


Рис. 106 – Настройка службы Aladdin JAS Engine Service

16.3 Установка JAS-плагина для службы кластеров

Чтобы установить JAS-плагин для службы кластеров, выполните следующие действия:

1. Запустите файл установки: **Aladdin.JAS.FCPlugin-X.X.X.XXX-x64.msi** (только для 64-битных систем).
Отобразится следующее окно.

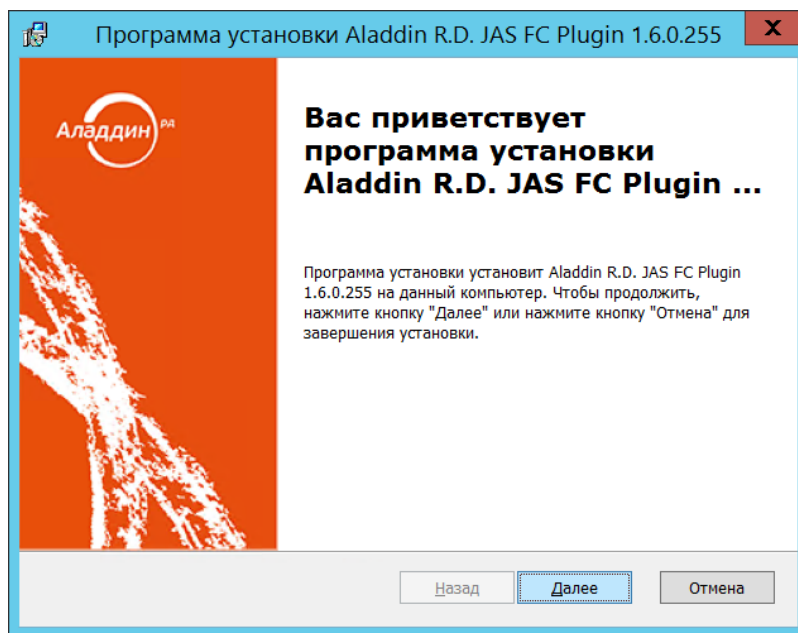


Рис. 107 – Окно приветствия мастера установки JAS-плагина для отказоустойчивого кластера

- Нажмите **Далее**.
Отобразится следующее окно.

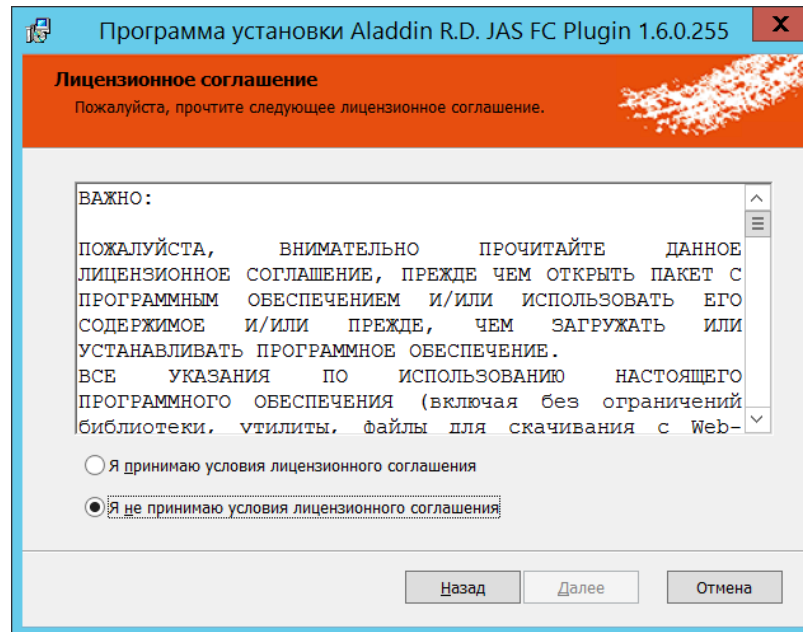


Рис. 108 – Окно лицензионного соглашения

- Выберите **Я принимаю условия лицензионного соглашения**, после чего нажмите **Далее**.
Отобразится следующее окно.

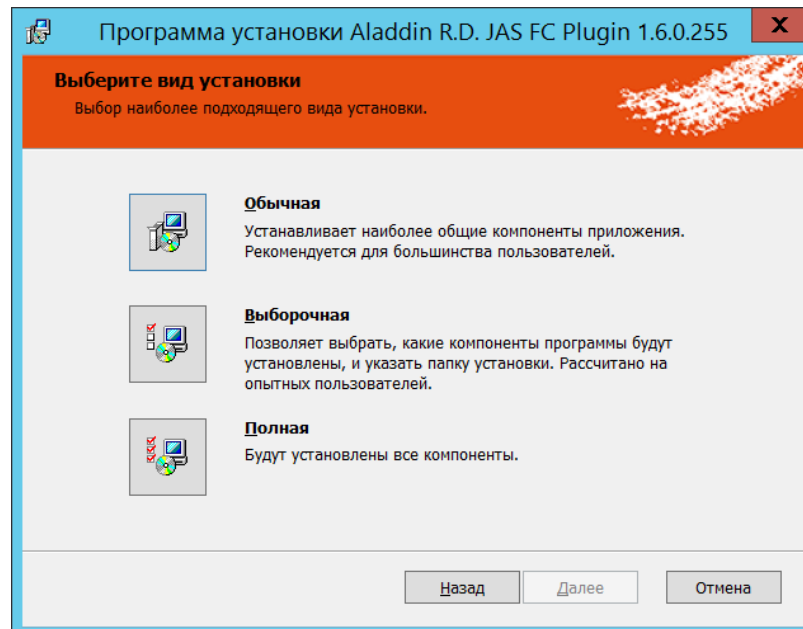


Рис. 109 - Окно выбора варианта установки

- Выберите **Полная**.

Отобразится следующее окно.

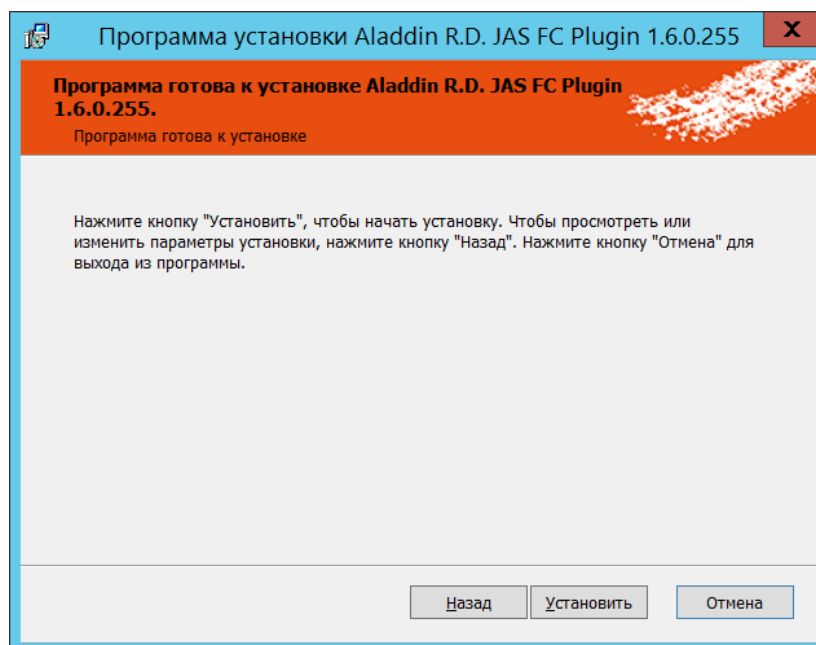


Рис. 110 – Подготовка к установке

6. Нажмите **Установить**.
По завершении установки отобразится следующее окно.

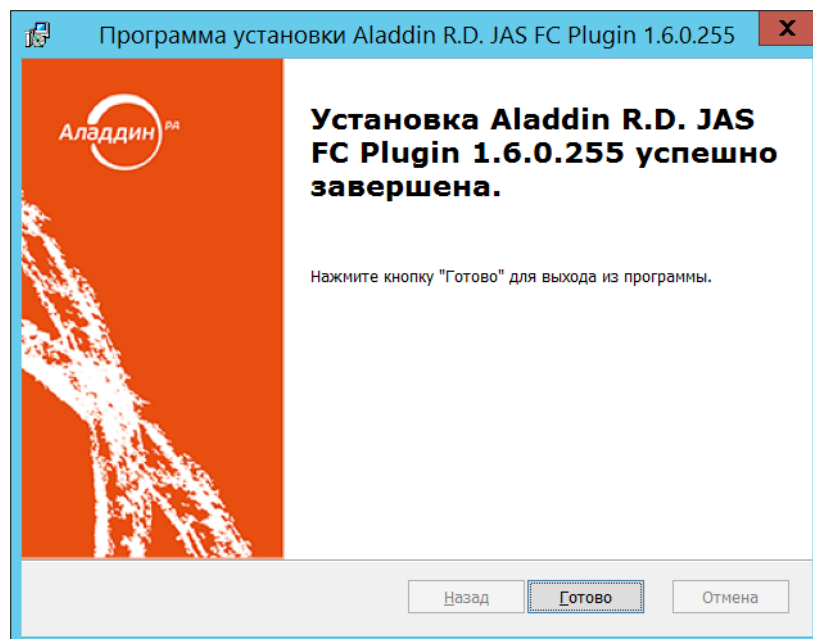


Рис. 111 – Окно завершения установки

7. Нажмите **Готово** и переходите к настройкам JAS-плагина для службы кластеров (ниже).

16.4 Настройка JAS-плагина для службы кластеров

Чтобы настроить JAS-плагин для службы кластеров, выполните следующие действия.

1. Откройте редактор реестра – для этого из командной строки выполните команду **regedit**.
2. Перейдите в следующий раздел реестра:

[HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JAS FC Plugin].

Раздел будет выглядеть следующим образом.

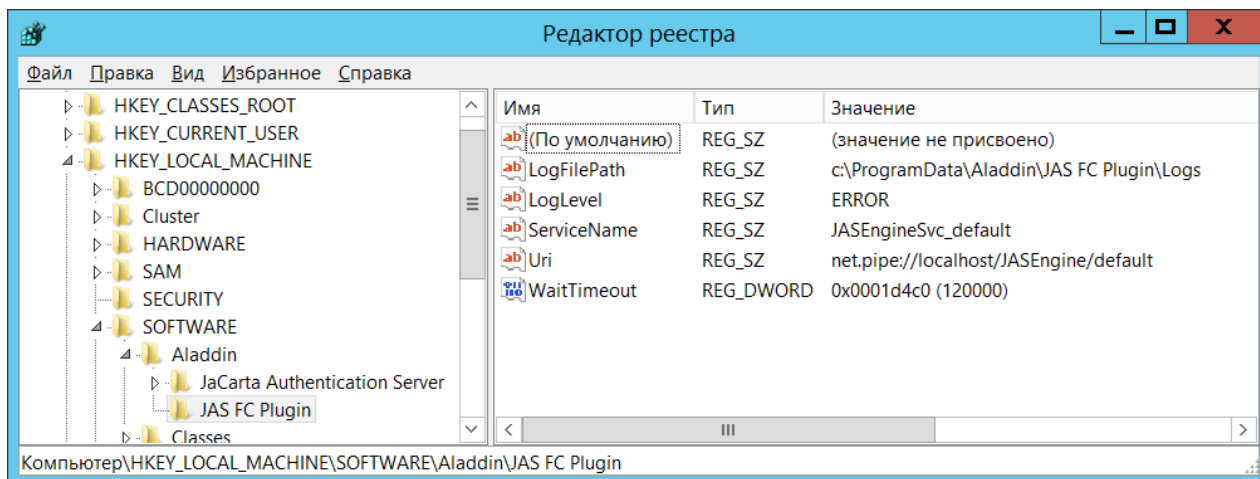



Рис. 112 – Настройки JAS-плагина для службы кластеров

3. Выполните настройку, руководствуясь Табл. 32 ниже.

Табл. 32 - Настройка JAS-плагина для службы кластеров

Настройка	Описание
Uri	<p>Адрес программного интерфейса на узле кластера для «прослушивания» запросов от JAS-плагина для службы кластеров и других клиентов:</p> <pre>net.pipe://localhost/JASEngine/default</pre> <p>Для корректной работы кластера следует использовать данное значение, установленное по умолчанию.</p>
LogFilePath	Путь, по которому будет сохраняться файл журнала
LogLevel	<p>Уровень ведения журнала событий.</p> <ul style="list-style-type: none"> • OFF – ведение журнала событий отключено; • FATAL – неустранимая ошибка; • ERROR – ошибка (значение по умолчанию); • WARN – предупреждение; • INFO – информация; • DEBUG – отладка; • ALL – показывать все события. <p> Каждый последующий уровень включает все предыдущие (кроме OFF), например, если выставлено значение INFO, то будут отображаться сообщения уровней: INFO, WARN, ERROR, FATAL</p>

Настройка	Описание
ServiceName	Имя службы JAS. В текущей версии продукта служба JAS (Aladdin JAS Engine Service) имеет имя: JASEngineSvc_default
WaitTimeout	<p>Время ожидания логического запуска Сервера JAS.</p> <p>Данная настройка связана со значительной задержкой логического запуска Сервера JAS при большом числе обслуживаемых аутентификаторов (например 1 миллиона).</p> <p>В случае если логического запуска сервера за время таймаута не происходит, в журнал JAS-плагина для службы кластеров (см. настройку LogFilePath) добавляется запись с описанием ошибки и в силу вступают настройки автоматического перезапуска ресурса службы кластеров, Рис. 113, ниже.</p> <p>Значение по умолчанию: 180000 (3 мин)</p> <p>Важно! Время, задаваемое параметром Время ожидания, определяемым в настройке политики перезагрузки ресурса в службе кластеров (см. вкладку Политика свойств ресурса Aladdin JAS Server, Рис. 113), не может быть меньшим значения, заданного параметром WaitTimeout настройки JAS-плагина для службы кластеров</p>

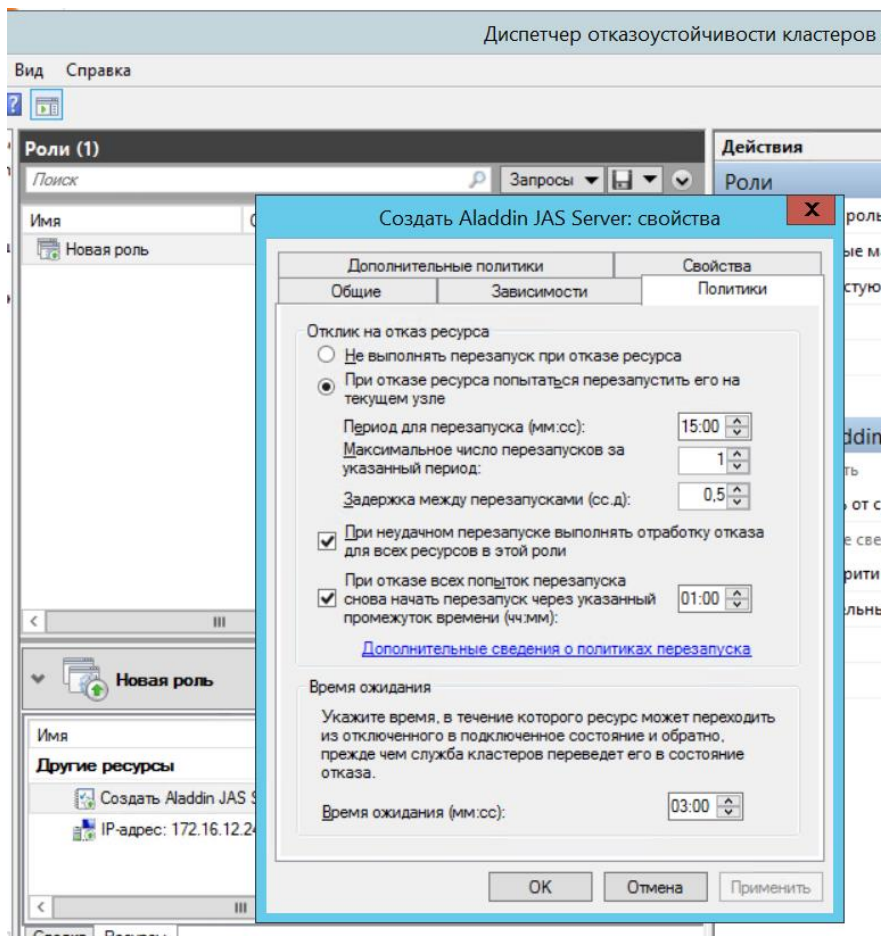


Рис. 113 – Настройка политики перезагрузки ресурса Aladdin JAS Server службы кластеров

4. После внесения изменений в реестр перезагрузите *Службу кластеров*, чтобы настройки вступили в силу.

16.5 Настройка отказоустойчивого кластера JAS

Для настройки отказоустойчивого кластера JAS выполните следующие действия.

1. В соответствии с документацией Microsoft Windows Server создайте отказоустойчивый кластер, добавив в него необходимое число предварительно созданных узлов (в настоящем документе рассматривается пример настройки кластера с двумя узлами). В процессе установке кластеру присваивается собственный IP-адрес и DNS-имя.
2. В *Диспетчере отказоустойчивости кластеров* для созданного кластера создайте пустую кластерную роль.

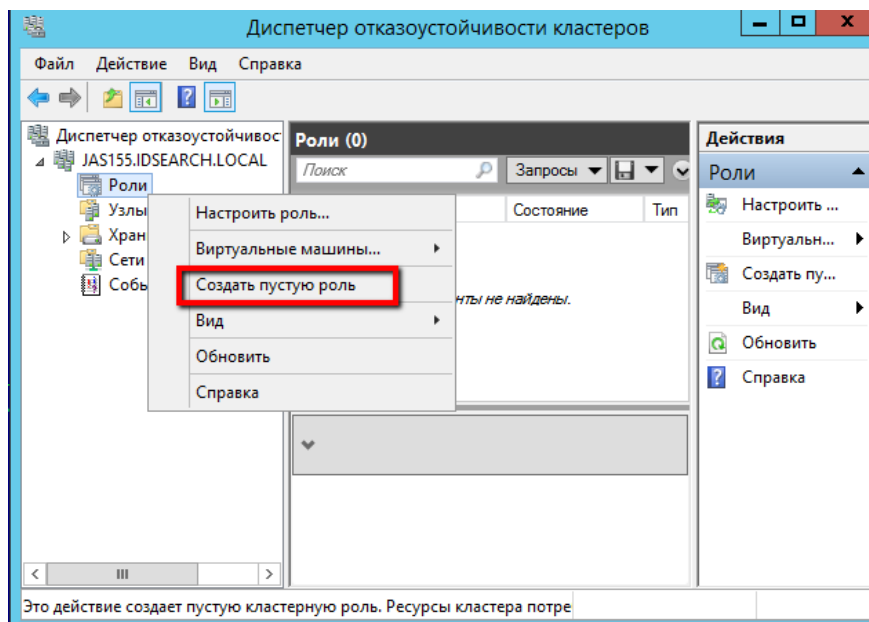


Рис. 114 – Добавление пустой роли кластеру серверов

3. В созданную *кластерную роль* добавьте ресурс **Aladdin JAS Server**.

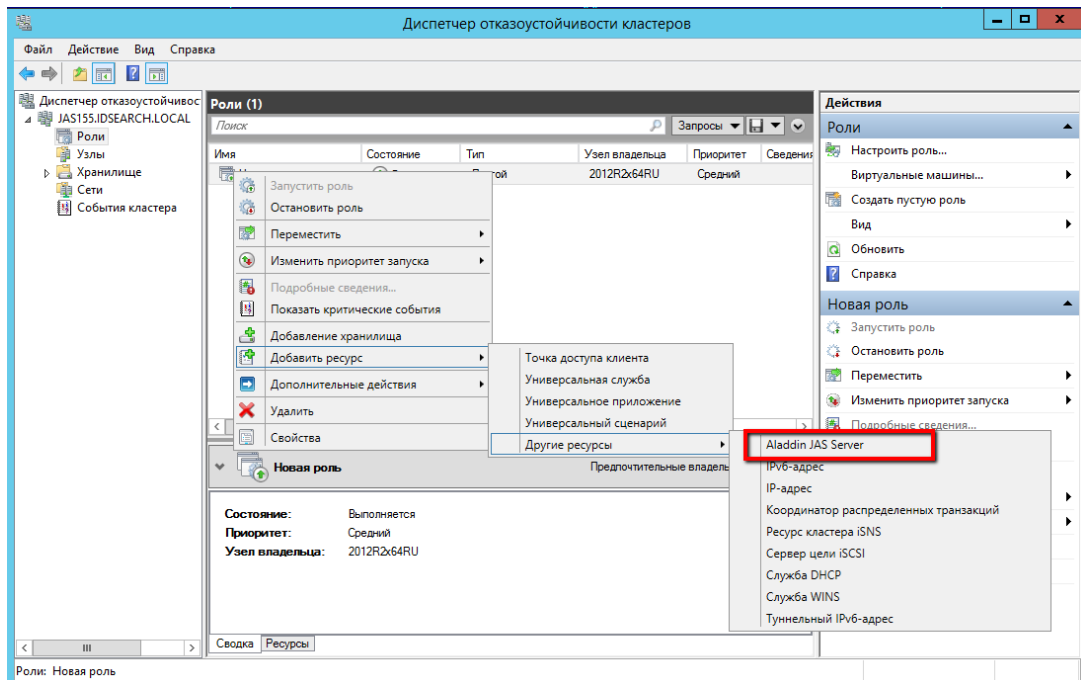


Рис. 115 – Добавление в пустую роль ресурса – Aladdin JAS Server



Примечание. В случае отсутствия Aladdin JAS Server в списке доступных ресурсов необходимо закрыть и повторно открыть Диспетчер отказоустойчивости кластеров.

4. В созданную *кластерную роль* добавьте еще один ресурс – **IP-адрес**. Выполните настройку IP-адреса для данной роли. На данном адресе отказоустойчивый кластер JAS будет принимать клиентские запросы. (В частности, данный адрес следует в дальнейшем использовать в настройках JAS-плагинов NPS и AD FS в случае их установки).



Обратите внимание, что IP-адрес *кластерной роли* должен отличаться IP-адреса кластера.



Примечание 1. В случае если для подключения к сетевым интерфейсам (*AdministrationServices* и *AuthenticationServices*) планируется использовать протоколы SSL/TLS, то для IP-адреса роли кластера следует создать DNS-имя из оснастки Диспетчер DNS. Полученное FQDN-имя следует использовать при получении соответствующего SSL-сертификата.



Примечание 2. В случае отсутствия Aladdin JAS Server в списке доступных ресурсов необходимо закрыть и повторно открыть Диспетчер отказоустойчивости кластеров.

5. Для завершения настройки отказоустойчивого кластера в соответствии с документацией Microsoft Windows Server выполните настройку параметров кворума кластера.

После добавления *кластерной роли* необходимо убедиться, что данная роль успешно запустилась (находится в состоянии **Выполняется**), и на одном из узлов кластера успешно запустился Сервер JAS.

16.6 Проверка работы отказоустойчивого кластера JAS

Процедура проверки работы отказоустойчивого кластера JAS приводится на примере кластера из двух узлов (*JAS01* и *JAS02*). Для проверки работы кластера выполните следующие действия.

1. Выполните предварительные условия проверки:
 - 1.1. Убедитесь, что кластер установлен и настроен в соответствии с предыдущими разделами.
 - 1.2. Убедитесь, что текущим сервером узла кластера является один из серверов JAS (например *JAS01*).

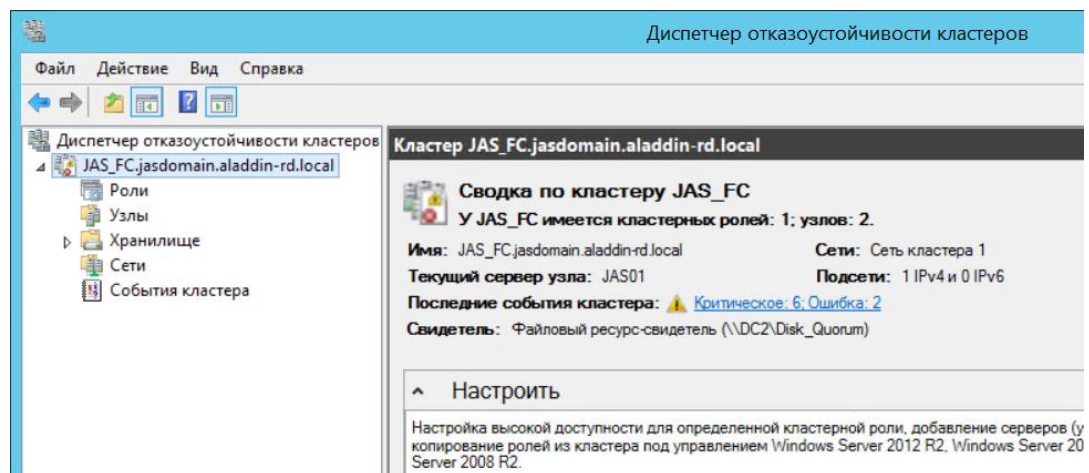


Рис. 116 – Индикация работающего узла (*JAS01*) отказоустойчивого кластера

- 1.3. Убедитесь, что на втором узле кластера (*JAS02*) служба **Aladdin JAS Engine Service – default** остановлена. (Если нет, выполните ее остановку принудительно).
2. Сделайте узел *JAS01* физически недоступным. (Например, отключите питание или сетевой интерфейс).
3. Убедитесь, что через некоторое время (при большом числе поддерживаемых аутентификаторов может составлять несколько минут) служба **Aladdin JAS Engine Service – default** на втором узле кластера (*JAS02*) сервера автоматически запустилась, после чего автоматически запустился Сервер JAS (*Статус сервера: Работает*).

Данное поведение отказоустойчивого кластера подтверждает, что резервный узел автоматически включается для поддержания работоспособности сервиса.

17. Двухфакторная аутентификация для входа в Windows (JOL)

JAS может быть использован для обеспечения двухфакторной аутентификации при входе в ОС Microsoft Windows за счет установки на клиентских машинах ПО JAS OTP Logon (JOL). В результате установки дистрибутива JOL на клиентском компьютере будет добавлен дополнительный поставщик учетных данных (Credential Provider), требующий для аутентификации пользователя ввода обычного и OTP- паролей (Рис. 117).

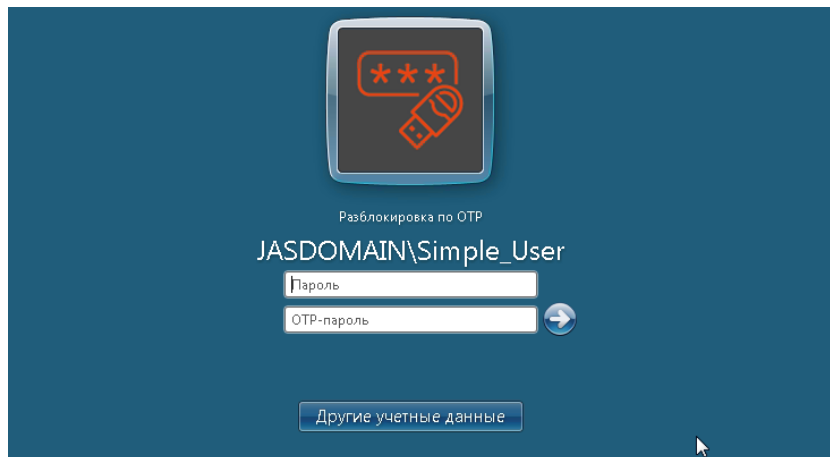


Рис. 117 – Запрос учетных данных для двухфакторной аутентификации JAS OTP Logon

17.1 Установка JOL

Чтобы установить на клиентской машине компонент JAS OTP Logon (JOL), выполните следующие действия.

1. В зависимости от разрядности операционной системы запустите соответствующий файл.
 - 32-бит: OTPLogon_X.X.X.XX_win-x86_XX-XX.msi;
 - 64-бит: OTPLogon_X.X.X.XX_win-x64_XX-XX.msi.

Отобразится следующее окно.

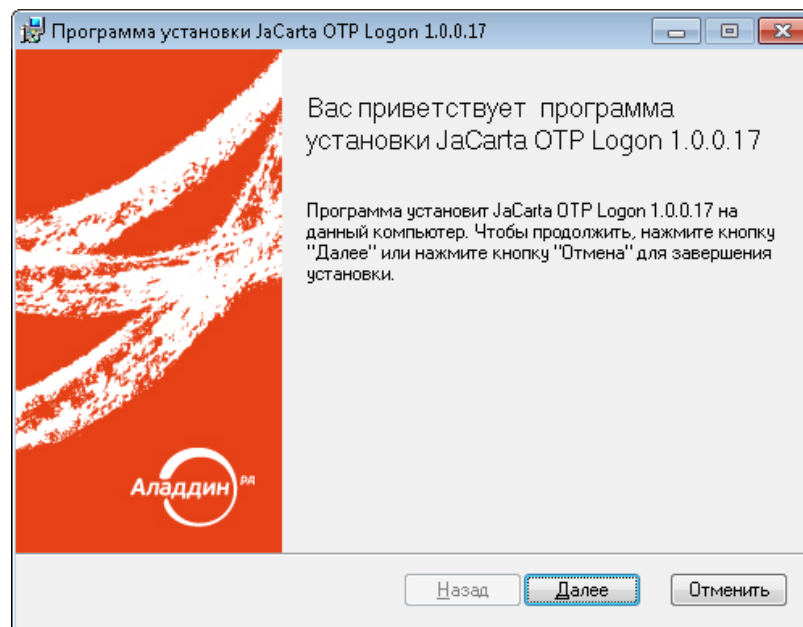


Рис. 118 – Экран приветствия мастера установки JaCarta OTP Logon

2. Нажмите **Далее** и следуйте указаниям мастера установки до окончания процедуры инсталляции.



Важно! Для корректной работы JOL на рабочих станциях параметр **SecurityType** в настройках сервера JAS должен иметь значение **None** (см. Табл. 6, с. 21). Включение

аутентификации на сетевом интерфейсе JAS (любое значение параметра SecurityType, отличное от **None**) приведет к появлению ошибки со следующим текстом: «Произошла ошибка аутентификации. Сервер аутентификации недоступен или работает неправильно. Обратитесь к администратору.»

17.2 Настройки JOL и порядок их применения

Настройки JOL могут устанавливаться из четырех источников

- настройки JOL из GPO – групповой политики **JAS OTP Logon (JOL)** (см. Табл. 33, с. 138; требуется настройка централизованного хранилища групповых политик, см. раздел «Групповая политика JOL», с. 141);
- настройки JOL из локальной групповой политики (см. раздел «Локальная групповая политика JOL», с. 142).
- настройки JOL в реестре (см. Табл. 33; могут быть переопределены вручную);
- настройки по умолчанию (прошиты в исходном коде продукта).

Приоритет в определении конфигурации JOL имеют настройки доменной групповой политики, GPO (Рис. 119, ниже). При отключении доменной групповой политики (или отдельных ее настроек) происходит обращение к локальному объекту GPO (или к отдельным его настройкам). В случае если доменная и локальная групповые политики не заданы, или в них не заданы отдельные параметры, то в силу вступают настройки (или отдельные параметры), определенные в реестре на клиентском компьютере, в разделе [**HKEY_LOCAL_MACHINE\SOFTWARE\AladdinRD\JAS OTP Logon**] , (параметры описаны в Табл. 33, с. 138). Если значения параметров в реестре не будут определены принудительно (вручную), то они установятся автоматически при первом запуске программы в соответствии значениями по умолчанию (см. там же, Табл. 33).

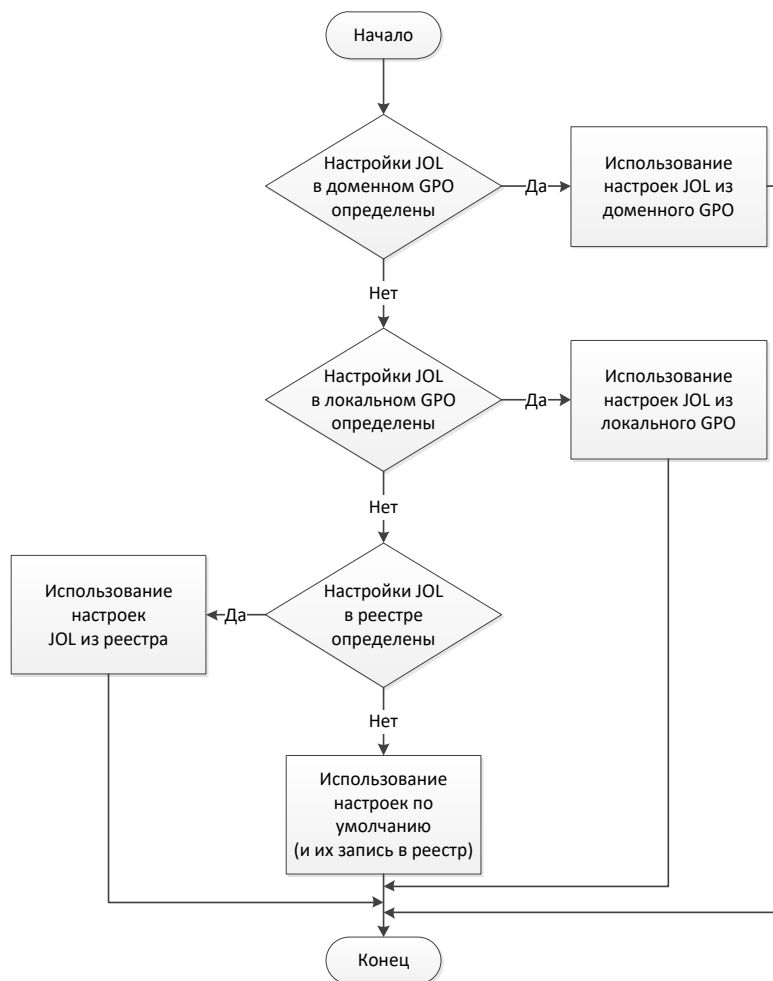




Рис. 119 – Порядок применения настроек JOL


В случае если групповые политики не заданы (или отключены), настройки JOL на конкретном клиентском компьютере могут быть изменены вручную, путем редактирования параметров в реестре (Табл. 33, ниже).



Примечание. Ручное редактирование параметров JOL в реестре должно производиться только в разделе [HKEY_LOCAL_MACHINE\SOFTWARE\AladdinRD\JAS OTP Logon]. Редактировать одноименные параметры реестра в разделе, отвечающем за групповые политики, не следует.

Табл. 33 – Параметры конфигурации JOL

Название пункта настройки JOL в GPO	Параметр настройки JOL в реестре	Описание
Настройки фильтрации поставщиков учетных данных	LogonProvidersFilter	<p>Параметр, определяющий доступные пользователю поставщики учетных данных (Credential Provider) при входе в Windows. Доступные значения:</p> <ul style="list-style-type: none"> • 0 – пользователю доступны все поставщики учетных данных (включая JOL); • 1 – пользователю доступны только JOL и вход по смарт-карте; • 2 – пользователю доступен только JOL; • 3 – пользователю доступны только поставщики учетных данных, GUID-идентификаторы которых перечислены в параметре LogonProvidersList, ниже. <p>Значение по умолчанию: 0 (Пользователю доступны все поставщики учетных данных, включая JOL)</p>
Отображать поставщики учетных данных по списку их GUID	LogonProvidersList	<p>Список GUID-идентификаторов поставщиков учетных данных, доступных пользователю для входа в Windows. Указываются через запятую. (Параметр активен только при значении LogonProvidersFilter=3);</p> <p>GUIDы следует перечислить в формате: {XXXX-XXXX-XXXX-XXXX}, {YYYY-YYYY-YYYY-YYYY}</p> <p>Значения по умолчанию не предусмотрено.</p>
Адрес сервиса аутентификации JAS	ServiceUri	<p>Адрес подключения к сервису аутентификации JAS в формате:</p> <p><code>http://<FQDN-имя сервера JAS>:8008/JASEngine/Default/AuthenticationService/rest/Authenticate</code></p> <p>где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com; либо, в случае кластерной конфигурации JAS, полное доменное имя (FQDN) <i>кластерной роли</i>, созданной на этапе настройки отказоустойчивого кластера (см. «Настройка отказоустойчивого кластера JAS», с. 132).</p> <p>Значение по умолчанию: http://localhost:8008/JASEngine/Default/AuthenticationService/rest/Authenticate</p> <p> Примечание. Для подключения JOL к серверу JAS по защищенному каналу с использованием протоколов SSL/TLS установленный по умолчанию протокол HTTP в адресе ServiceUri следует заменить на HTTPS. Подробнее о настройке SSL для JOL см. в разделе «Настройка SSL/TLS на стороне компонента JOL», с. 25</p> <p> Важно! Для корректной работы сервиса JOL при подключении к серверу JAS по SSL-соединению в адресе ServiceUri необходимо указать именно FQDN-имя сервера JAS (не IP-адрес), указанное в сертификате для SSL.</p>
Действия JOL при использовании заблокированных OTP-токенов	TokensNotFou ndAction	<p>Действия JOL, если у пользователя, обратившегося с запросом на аутентификацию, в JAS зарегистрированы OTP-токены (хотя бы один), но ни один из них не активен (все отключены/заблокированы). Допустимые значения:</p> <ul style="list-style-type: none"> • Pass (Пропускать запрос) • Reject (Отклонять запрос) <p>Значение по умолчанию: Reject</p>

Название пункта настройки JOL в GPO	Параметр настройки JOL в реестре	Описание
Действия JOL по запросу от незарегистрированных пользователей	UserNotFoundAction	<p>Действия JOL, если пользователь, который пытается аутентифицироваться, не зарегистрирован в JAS. Доступные значения:</p> <ul style="list-style-type: none"> • Pass (Пропускать запрос) • Reject (Отклонять запрос) <p>Значение по умолчанию: Reject</p>
Автоматически добавлять Windows-пароль пользователя в поле OTP-пароль	ConcatenatePassword	<p>Включить/отключить автоматическое добавление введенного пользователем пароля Windows в поле OTP (при установке для OTP-токена режима аутентификации «Доменный пароль+OTP» или «Доменный пароль + OTP PIN-код + OTP» (см. описание параметра Режим аутентификации в профилях выпуска OTP-токенов в руководстве по функциям управления JMS [3]). Доступные значения:</p> <ul style="list-style-type: none"> • Enable (Включить) • Disable (Отключить) <p>Значение по умолчанию: Disable</p>
Добавлять имя внедоменной рабочей станции	AddWsPrefix	<p>Включить/отключить автоматическое добавление к имени пользователя имени внедоменной рабочей станции (например WKS234\user). Доступные значения:</p> <ul style="list-style-type: none"> • Enable (Включить) • Disable (Отключить) <p>Значение по умолчанию: Disable</p> <p> Важно! В текущей версии JMS параметр может иметь только значение Disable (использование JOL для аутентификации на внедоменных станциях недоступно)</p>
Язык интерфейса JAS OTP Logon	Culture	<p>Управление языком пользовательского интерфейса. Доступные значения:</p> <ul style="list-style-type: none"> • RU (Русский) • EN (Английский) <p>Значение по умолчанию: RU</p>
Путь к файлам журнала (лог-файлам)	LogFilePath	<p>Путь, по которому будет сохраняться файл журнала.</p> <p>Значение по умолчанию: C:\ProgramData\AladdinRD\JAS OTP Logon\Logs\</p>

Название пункта настройки JOL в GPO	Параметр настройки JOL в реестре	Описание
Уровень детализации ведения журнала	LogLevel	<p>Уровень ведения журнала событий (логов).</p> <ul style="list-style-type: none"> • OFF – ведение журнала событий отключено; • FATAL – отображать неустраняемые ошибки; • ERROR – ошибки; • WARN – предупреждения; • INFO – информация; • DEBUG – отладка; • ALL – показывать все события. <p>Каждый последующий уровень включает все предыдущие (кроме OFF), например, если выставлено значение INFO, то будут записываться сообщения уровней: INFO, WARN, ERROR, FATAL</p> <p>Значение по умолчанию: ERROR</p>
Настройка проверки действительности сертификата сервера	SSLVerifyPeer	<p>Включение/отключение проверки на клиентском компьютере действительности сертификата сервера при настроенном SSL-соединении. Доступные значения:</p> <ul style="list-style-type: none"> • 0 (Отключить) • 1 (Включить) <p>Значение по умолчанию: 1</p>
Настройка проверки CN сертификата сервера	SSLVerifyHost	<p>Включение/отключение проверки на клиентском компьютере имени субъекта (CN) сертификата (сервера) с именем, указанным в параметре ServiceUri (выше, в таблице). Доступные значения:</p> <ul style="list-style-type: none"> • 0 (Отключить) • 2 (Включить) <p>Значение по умолчанию: 2</p>
Использовать JOL для локальной сессии	UseJolInLocalSessions	<p>Настройка определяет, следует ли использовать JOL-провайдер (Credential Provider, поставщик учётных данных) для локального сеанса пользователя, т.е. будет ли запрашиваться OTP-пароль, если вход в Windows осуществляется локально (не через RDP).</p> <p>В случае если настройка выключена (значение false), значение параметра LogonProvidersFilter=2 («входить только через JOL», см. выше) игнорируется, и вход на локальном компьютере (не через RDP) будет осуществлен через стандартный поставщик учётных данных.</p> <p>Настройка не распространяется на RDP-подключения.</p> <p>Доступные значения:</p> <ul style="list-style-type: none"> • false (Отключить) • true (Включить) <p>Значение по умолчанию: true</p>

Название пункта настройки JOL в GPO	Параметр настройки JOL в реестре	Описание
Использовать JOL для удаленной сессии	UseJolInRemoteSessions	<p>Настройка определяет, следует ли использовать JOL-провайдер (Credential Provider, поставщик учётных данных) при удалённом подключении к компьютеру, т.е. будет ли запрашиваться OTP-пароль, если вход в Windows осуществляется по RDP.</p> <p>В случае если настройка выключена (значение false), значение параметра LogonProvidersFilter=2 («входить только через JOL», см. выше) игнорируется, и вход по RDP будет осуществлен через стандартный поставщик учётных данных.</p> <p>Настройка не распространяется при подключении к локальному компьютеру.</p> <p>Доступные значения:</p> <ul style="list-style-type: none"> • false (Отключить) • true (Включить) <p>Значение по умолчанию: true</p>
<Параметр отсутствует в GPO, настройка доступна только локально в реестре компьютера с JOL>	SSLVersionTLS	<p>Параметр устанавливает максимальную версию TLS для работы компонента JOL. Допустимые значения:</p> <ul style="list-style-type: none"> • 0 - Использовать TLS версии 1.0; • 1 - Использовать TLS версии 1.1; • 2 - Использовать TLS версии 1.2; • 3 - Использовать TLS версии 1.3 <p>Значение по умолчанию: 2</p>

17.3 Групповая политика JOL (административный шаблон GPO)

Управление JOL на рабочих станциях домена Active Directory (AD) можно производить с помощью механизма групповой политики Windows.

Для создания групповой политики **JAS OTP Logon (JOL)** в выбранном домене AD выполните следующие действия.

1. В центральное хранилище административных шаблонов на *контроллере домена* добавьте поставляемый в комплекте с JAS административный шаблон определения групповой политики, включающий в себя ADMX- и ADML-файлы:
 - *JASOTPLogon.admx*;
 - *ru-RU\JASOTPLogon.adml* (для русской локализации);
 - *en-US\JASOTPLogon.adml* (для английской локализации).

Порядок создания центрального хранилища для административных шаблонов и добавления в него административных шаблонов групповых политик описан в соответствующей документации компании Microsoft (см. веб-ссылки [3], с. 155).

2. Настройте групповую политику на *контроллере домена* с помощью **Редактора управления групповыми политиками** (Рис. 120) руководствуясь Табл. 33, с. 138, или интерактивными подсказками редактора политик.

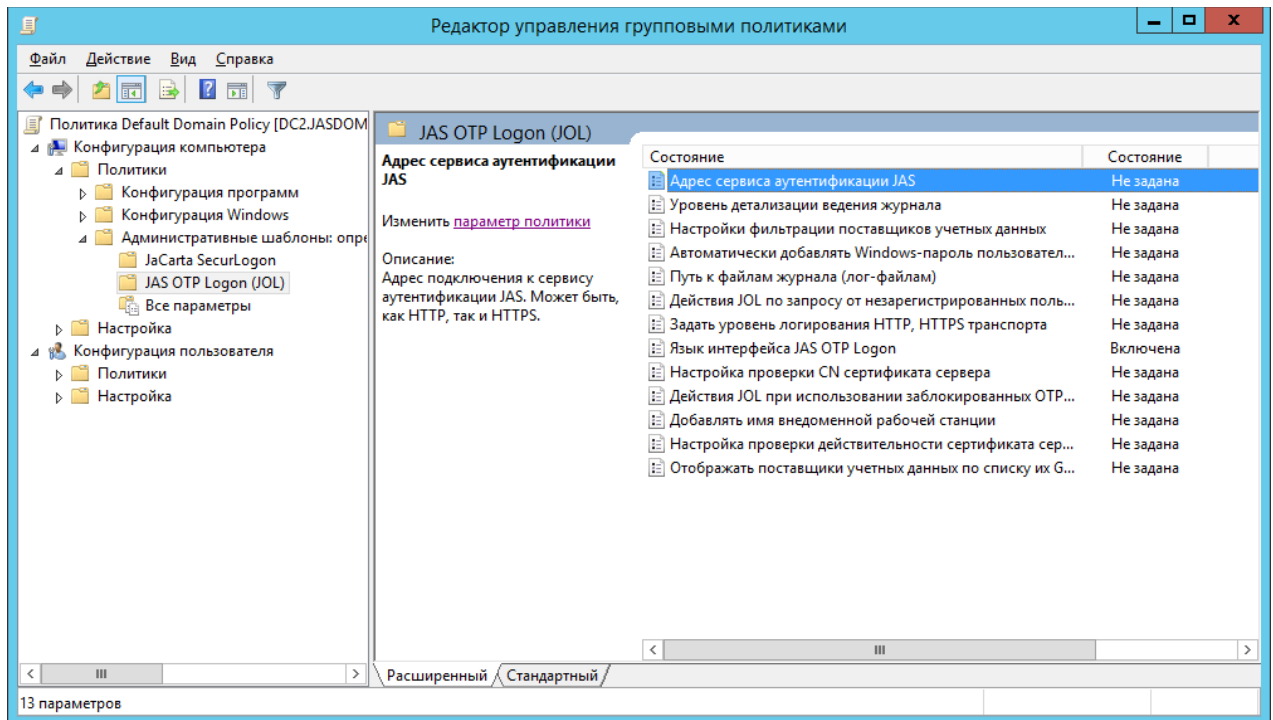


Рис. 120 – Настройка групповой политики JAS OTP Logon (JOL)

3. Дождитесь обновления групповой политики на рабочих станциях (задержка обусловлена настройками операционной среды), или выполните принудительное обновление групповой политики на соответствующей рабочей станции из командной строки (команда `gpupdate /force`).



Примечание. По умолчанию шаблон добавляется в групповую политику Default Domain Policy, распространяющую свое действие на компьютеры всего домена. Для ограничения (в применении к отдельным доменным компьютерам) или диверсификации действия шаблона групповой политики JOL используйте стандартные механизмы управления групповыми политиками и Active Directory (например, создание отдельных политик для подразделений OU; запрет на использование политики на отдельных компьютерах через настройки ее свойств – вкладка **Безопасность**; и др.).

17.4 Локальная групповая политика JOL

Шаблон, определяющий локальную групповую политику JOL, устанавливается в локальное хранилище административных шаблонов (каталог `C:\Windows\PolicyDefinitions`) автоматически в процессе инсталляции JOL на рабочей станции.

Локальная групповая политика обеспечивает дополнительную гибкость в настройках JOL и может быть использована при необходимости с помощью стандартных средств управления Windows. Набор параметров совпадает с административным шаблоном доменной групповой политики JOL (см. Табл. 33, с. 138).

17.5 Порядок аутентификации в Windows с помощью JOL

Для аутентификации в Windows с помощью JOL выполните следующие действия.

1. На экране входа в систему (Рис. 121) для выбора поставщика учетных данных JOL нажмите **Другие учетные записи**. (В случае если все поставщики учетных данных, кроме JOL, отключены, перейдите к шагу 5).



Рис. 121 – Стандартный экран входа в систему (ОС Windows)

4. Среди отображенных поставщиков учетных данных (Рис. 122) выберите **Разблокировка по OTP**.

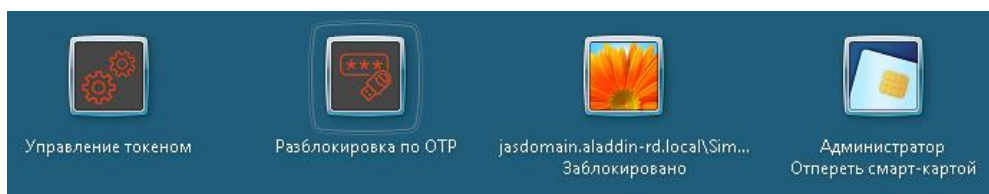



Рис. 122 – Выбор JOL как поставщика учетных данных

5. На экране входа по OTP (Рис. 123) в поле **Пароль** введите пароль Windows (в случае внедоменной рабочей станции – пароль локального пользователя, в случае доменного компьютера – пароль доменного пользователя).

 **Примечание.** В текущей версии JMS аутентификация с помощью JOL на внедоменных станциях недоступна

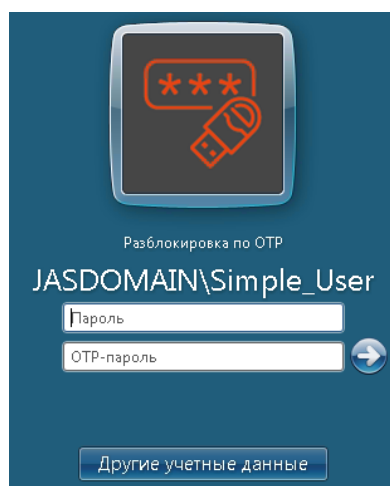


Рис. 123 – Ввод данных в окне JOL

В поле **OTP-пароль** в зависимости от настроек JOL введите следующее значение:

- пароль OTP, полученный из OTP-токена пользователя, если для данного токена режим аутентификации имеет значение:

- «ОТР» (см. описание параметра **Режим аутентификации** в профилях выпуска ОТР-токенов в руководстве по функциям управления JMS [3]);
- «Доменный пароль + ОТР», но при этом в групповой политике включена настройка **«Автоматически добавлять Windows-пароль пользователя в поле ОТР-пароль»** (см. Табл. 33, с. 138, значение `Enable`; настройка через реестр описана там же);
- PIN-код ОТР и пароль ОТР (без пробела), если для данного токена режим аутентификации имеет значение:
 - «ОТР PIN-код + ОТР» (см. описание параметра **Режим аутентификации** в профилях выпуска ОТР-токенов в руководстве по функциям управления JMS [3]);
 - «Доменный пароль + ОТР PIN-код + ОТР», но при этом в групповой политике включена настройка **«Автоматически добавлять Windows-пароль пользователя в поле ОТР-пароль»** (см. Табл. 33, с. 138, значение `Enable`; настройка через реестр описана там же);
- все необходимые значения, в соответствии с режимом аутентификации («ОТР», «ОТР PIN-код + ОТР», «Доменный пароль + ОТР»или «Доменный пароль + ОТР PIN-код + ОТР»; для трех последних – параметры вводятся без пробела), если в групповой политике выключена настройка **«Автоматически добавлять Windows-пароль пользователя в поле ОТР-пароль»** (см. Табл. 33, с. 138, значение `Disable`; настройка через реестр описана там же).

6. Для аутентификации нажмите *ввод*.

18. Установка и настройка Сервиса Aladdin 2FA (A2FA)

Aladdin 2FA (A2FA) – программная платформа производства компании Аладдин, предназначенная для двухфакторной аутентификации, состоящая из *мобильного приложения A2FA* и *Сервиса A2FA* (серверного приложения Aladdin 2FA Service).

В настоящем разделе рассматривается установка второго компонента – *Сервиса A2FA*.

18.1 Дистрибутив

Описание дистрибутива Сервиса Aladdin 2FA приведено в руководстве по A2FA [5] в разделе «Описание пакетов установки».

18.2 Системные требования

Системные требования Сервиса Aladdin 2FA приведены в документе RU.АЛДЕ.02.13.001-04 30 01-1 «Программное обеспечение JaCarta Management System v3.7. Формуляр», в разделе «Требования к среде функционирования компонента „Сервис Aladdin 2FA“».



Примечание. Рекомендации по выбору операционной платформы и дополнительного ПО приведены также в руководстве по A2FA [5] в разделе «Системные требования».

18.3 Порядок установки Сервиса A2FA

Для установки Сервиса A2FA выполните шаги, описанные в руководстве по A2FA [5] в разделе «Установка».

18.4 Порядок подключения Сервиса A2FA к серверу JAS

Для подключения к серверу JAS выполните настройки, описанные в руководстве по установке и настройке JMS [2], в разделе «Настройки подключения к JAS» в части настроек секции «Веб-сервис безопасной передачи OTP-секрета»

18.5 Настройка выпуска OTP- и PUSH-токенов на базе платформы A2FA

Порядок выполнения всех настроек, связанных с обеспечением возможности выпуска пользователями OTP- и PUSH-токенов, используемых в рамках платформы A2FA, описан в руководстве по функциям управления JMS [3], в разделе «Порядок настройки самостоятельного выпуска пользователями OTP-аутентификатора».

18.6 Порядок работы с OTP- и PUSH-токенами в рамках платформы A2FA

Порядок выпуска, активации и осуществление других функций управления пользователями в отношении OTP- и PUSH-токенов, поддерживаемых платформой A2FA, описан в руководстве пользователя JMS [4].

19. Технические сведения

19.1 Оптимизация производительности JAS

При наличии требований к повышенной производительности вы можете прибегнуть к следующим способам оптимизации работы JAS (см. табл. 34 ниже).

Табл. 34 – Способы оптимизации

Способ	Описание
Изменение уровня ведения журнала событий	<p>Снижение уровня детализации при ведении журнала событий ведёт к повышению производительности JAS. Таким образом, вы можете, например, вести журнал событий на уровне не выше ERROR (ошибка). Подробнее о том, как это сделать, см. следующие разделы настоящего руководства:</p> <ul style="list-style-type: none"> • сервер JAS: «Настройка параметров ведения журнала событий», с. 26; • JAS-плагин для NPS: «Настройка JAS-плагины для NPS», с. 78; • JAS-плагин для AD FS: «Настройка JAS-плагины для AD FS», с. 103; • JAS-плагин для службы кластеров: «Настройка JAS-плагины для службы кластеров», с. 130
Использование IP-адреса вместо DNS-имени в настройках подключения	<p>Чтобы устранить потерю производительности за счет разрешения имен на DNS-сервере, в настройках подключения компонентов JAS вы можете указывать IP-адреса вместо DNS-имен. Подробнее о том, как это сделать, см. следующие разделы настоящего руководства:</p> <ul style="list-style-type: none"> • JAS-плагин для NPS: «Настройка JAS-плагины для NPS», с. 78; • JAS-плагин для AD FS: «Настройка JAS-плагины для AD FS», с. 103; • JAS-плагин для службы кластеров: «Настройка JAS-плагины для службы кластеров», с. 130

19.2 Рекомендации по развёртыванию JAS

19.2.1 Критерии выбора конфигурации с сервером RADIUS

В табл. 35 ниже представлены основные критерии выбора варианта установки JAS с сервером RADIUS.

Табл. 35 – Критерии выбора конфигурации с сервером RADIUS

Критерий	Соответствие критерию	
	Нет	Да
Используется ли RADIUS для аутентификации пользователей приложения	Конфигурация без RADIUS (может быть достигнута максимальная производительность)	Конфигурация с RADIUS (упрощенная процедура внедрения, но производительность потенциально ниже, чем без RADIUS)
Повышенные требования к производительности аутентификации	Менее 200 аутентификаций в секунду – можно использовать любую конфигурацию.	Более 200 аутентификаций в секунду: <ul style="list-style-type: none"> • если можно обойтись без RADIUS, следует использовать интерфейсы WCF или REST; • если нельзя обойтись без RADIUS, следует использовать конфигурацию с несколькими серверами RADIUS
ОТР-клиент (приложение, в котором аутентифицируются пользователи) написан с использованием технологии .NET Framework	Можно использовать любую конфигурацию	Рекомендуется использовать интерфейс WCF (конфигурация без RADIUS) при выборе между REST и WCF
Предъявляются ли требования к ведению учета входов пользователей в систему	Можно использовать любую конфигурацию	Следует использовать функциональность учёта (Accounting), включенную в RADIUS-сервер

19.2.2 Рекомендуемые варианты конфигурации

В зависимости от наличия необходимости использования сервера RADIUS или ее отсутствия рассмотрим рекомендуемые конфигурации JAS (табл. 36).

Табл. 36 – Варианты конфигурации JAS

Вариант конфигурации	Наличие RADIUS-сервера	
	Без сервера RADIUS	С сервером RADIUS
Устанавливаемые компоненты	<ul style="list-style-type: none"> • MS SQL; • JAS Server; • JAS Admin 	<ul style="list-style-type: none"> • MS SQL; • JAS Server; • JAS Admin; • Сервер политики сети (NPS); • JAS-плагин для NPS из состава JAS

Вариант конфигурации \ Наличие RADIUS-сервера	Без сервера RADIUS	С сервером RADIUS
	При этом сервер, на котором установлен компонент JAS Server, может как являться членом домена, так и не являться им	
Возможность установки компонентов на один сервер	Все компоненты могут быть установлены на один сервер	Все компоненты могут быть установлены на один сервер. При этом не рекомендуется устанавливать компонент JAS Server на контроллер домена
Дополнительные меры для улучшения производительности	Не актуально	Существует возможность распределить нагрузку между несколькими серверами, например: <ul style="list-style-type: none"> • Сервер №1: RADIUS-сервер в режиме RADIUS-прокси (этот сервер необязательно должен быть сервером политики сети (NPS-сервером), также на него не устанавливается JAS-плагин для NPS) – перенаправляет запросы на аутентификацию на несколько RADIUS-серверов; • Сервер №2: сервер политики сети (NPS) + JAS-плагин для NPS; • Сервер №3: аналогичен Серверу №2 (также можно создать больше серверов политики сети); • Сервер №4: MS SQL + JAS Server + JAS Admin
Доступные для внешних приложений интерфейсы взаимодействия с JAS	<ul style="list-style-type: none"> • REST; • WCF 	<ul style="list-style-type: none"> • REST; • WCF; • RADIUS

19.2.3 Требования к OTP-клиентам, использующим интерфейсы WCF или REST

В табл. 37 ниже представлены требования к OTP-клиентам JAS. OTP-клиент – приложение, в котором аутентифицируются пользователи. В настоящем подразделе рассматриваются следующие разновидности OTP-клиентов:

- WCF-клиент (приложение, работающее через интерфейс WCF);
- REST-клиент (приложение, работающее через интерфейс REST).

Табл. 37 – Требования к OTP-клиентам JAS

Требование \ Тип OTP-клиента	WCF	REST
Требование к реализации	WCF-клиентом JAS (по протоколам HTTP или net.tcp) может быть только .NET-приложение для Windows	REST-клиентом JAS в общем случае может быть любое приложение любой операционной системы, которое способно послать запрос HTTP POST на сервер JAS. Чтобы успешно установить соединение с сервером, клиент также должен знать URL сервера JAS, имя пользователя и пароль. (Подробнее см. «Настройка сетевых программных интерфейсов JAS», с. 19.)
Аутентификация OTP-клиента	Для аутентификации запросов, поступающих на сервер JAS, используется встроенная проверка подлинности Windows (протоколы NTLM и Kerberos). Имя пользователя и пароль, под которыми аутентифицируется OTP-клиент, могут принадлежать:	

Тип OTP-клиента Требование	WCF	REST
	<ul style="list-style-type: none"> любому локальному пользователю Windows на компьютере, где установлен компонент JAS Server; любому доменному пользователю, если компьютер, на котором установлен компонент JAS Server, входит в домен Windows. <p> Подробнее см. «Настройка сетевых программных интерфейсов JAS», с. 19</p>	
Авторизация OTP-клиента	<p>В качестве авторизации используется проверка аутентифицированного пользователя на членство в группе JAS Clients (или любой другой, указанной в параметрах реестра AuthorizeAsGroupMember – подробнее см. «Настройка сетевых программных интерфейсов JAS», с. 19). Количество этих пользователей не ограничено, проверяется только членство в группе. Так что в общем случае пользователей может быть столько, сколько разрешит операционная система</p>	

Также, если вы используете вариант развёртывания с RADIUS-сервером и планируете аутентифицировать пользователей, которые не зарегистрированы в домене, отредактируйте параметры политики запросов на подключение описанным ниже способом. (В противном случае RADIUS-сервер будет отвергать все запросы пользователей на аутентификацию.)

1. Запустите оснастку сервера политики сети.
2. В правой части окна выберите **NPS > Политики > Политики запросов на подключение**.
Окно примет следующий вид.

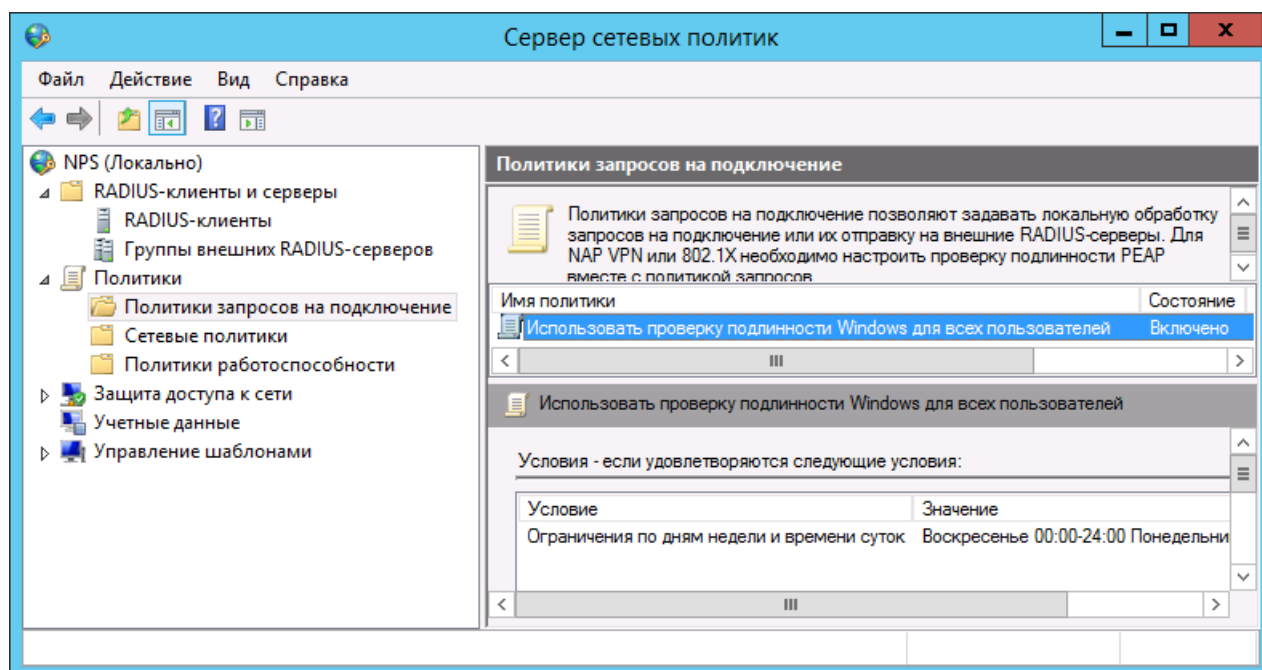
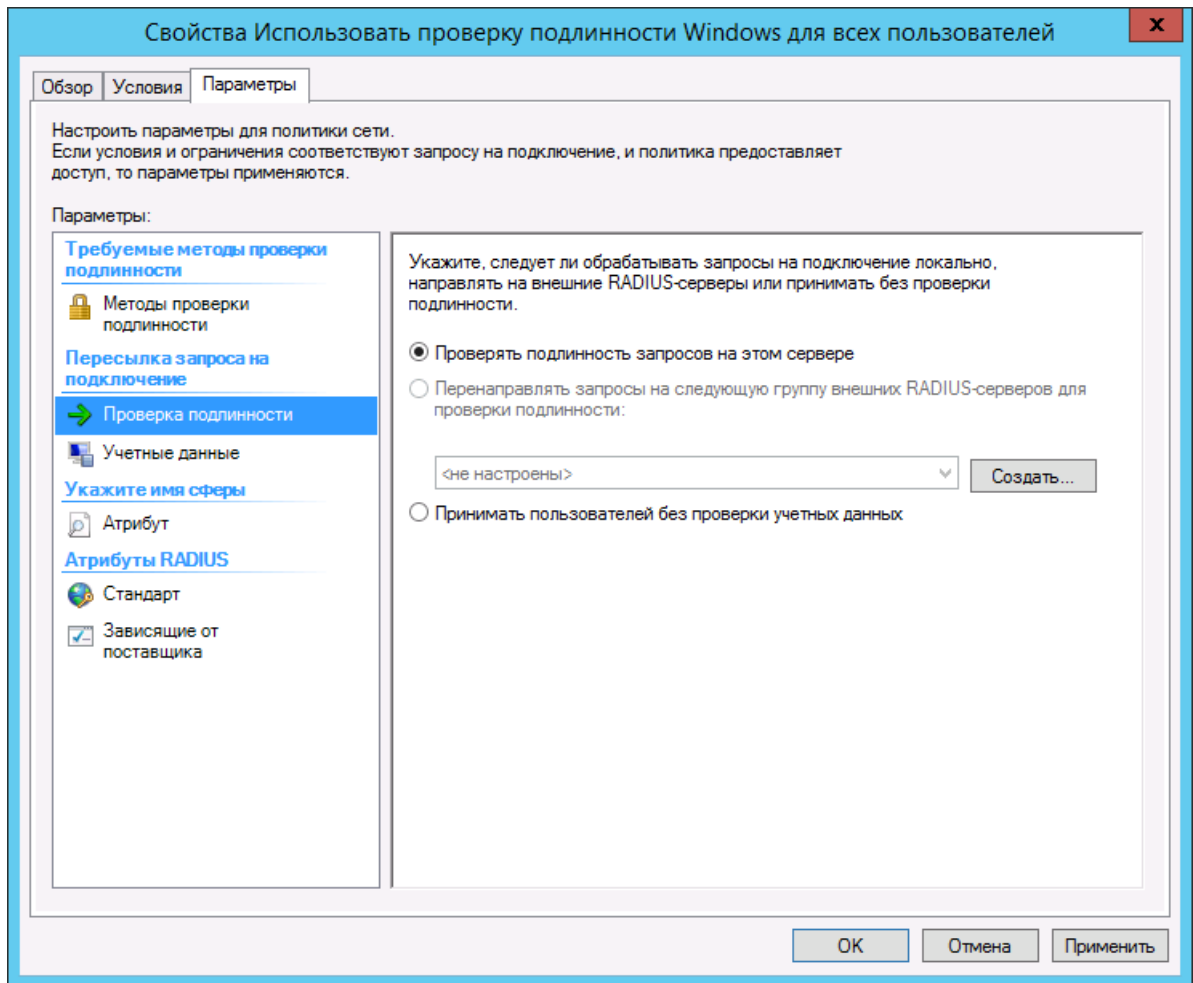


Рис. 124 – Политики запросов на подключение

3. В центральной части окна сделайте двойной щелчок на используемой политике.
4. В отобразившемся окне выберите вкладку **Параметры**.
5. В левой части окна выберите пункт **Проверка подлинности**.

Окно примет следующий вид.



6. В правой части окна выберите пункт **Принимать пользователей без проверки учётных данных**.
7. Нажмите **ОК**, чтобы сохранить изменения.

19.3 Описание интерфейсов REST и WCF

Интерфейс для OTP-аутентификации JAS поддерживает одновременно две точки доступа по типам транспорта "REST" и " WCF":

- точка доступа REST поддерживает протокол HTTP;
- точка доступа WCF поддерживает протоколы HTTP/SOAP и net.tcp (Binary).

19.3.1 REST

19.3.1.1 Общие сведения

Точка доступа REST доступна по следующему адресу:

http://<имя_хоста>:8008/JASEngine/Default/AuthenticationService/rest.

Это адрес по умолчанию, его можно изменить в настройках интерфейса взаимодействия с OTP-клиентами в реестре: **HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JaCarta Authentication Server\default\AuthenticationService\RestAddress.**



Подробнее см. «Настройка сетевых программных интерфейсов JAS», с. 19.

Обращение к JAS осуществляется посредством запросов HTTP POST, при этом используется протокол аутентификации Negotiate (NTLM и Kerberos).

19.3.1.2 Запросы клиента

Чтобы послать запрос на аутентификацию с использованием OTP, необходимо составить и отправить на сервер JAS сообщение HTTP POST следующего вида (см. табл. 38 ниже).

Табл. 38 – Запрос клиента

URL	http://<имя_хоста>:8008/JASengine/Default/AuthenticationService/rest/Authenticate
Тип содержимого	application/json
Формат запроса	<pre>{ "Username": "STRING", "Password": "STRING" }</pre> <p>Где Username – имя пользователя JAS в формате <Net-BIOS-имя домена>\<Имя пользователя>, а Password – значение OTP (совмещённый, если JAS настроен соответствующим образом, с PIN-кодом для OTP и/или паролем к профилю Windows)</p>

19.3.1.3 Ответ сервера

На клиентский запрос от сервера приходит HTTP-ответ. Возможные следующие HTTP-коды:

- **404** – служба недоступна по URL;
- **401** – ошибка аутентификации (неверный протокол или неверные учётные данные);
- **400** – неправильно сформирован запрос (неверный формат);
- **200** – успех – в этом случае ответ будет включать прикладное содержимое.

Ответ имеет следующий формат.

```
{
  "Result": INT,
  "ErrorId": "STRING",
  "Error": "STRING"
}
```

В табл. 39 ниже представлены возможные значения переменных.

Табл. 39 – Возможные значения переменных в ответе

Result	<p>Результат аутентификации, возможны следующие варианты:</p> <ul style="list-style-type: none"> • 1 – пользователь прошел OTP аутентификацию; • 0 – пользователь не прошел OTP аутентификацию; • -1 – произошла ошибка
ErrorId	<p>В случае ошибки (Result = -1) это поле содержит её строковый идентификатор:</p> <ul style="list-style-type: none"> • E_JAS_SERVER_NOT_RUNNING – сервер JAS не запущен; • E_JAS_AUTHORIZATION_IN_GROUP_ERROR – ошибка авторизации по членству в группе; • E_USER_NOT_SPECIFIED – в качестве имени пользователя передана пустая строка; • E_USER_NOT_FOUND – пользователь не найден; • E_TOKENS_NOT_FOUND – у пользователя нет ни одного токена с поддержкой OTP; • E_AUTHENTICATION_ERROR – общая ошибка OTP аутентификации.

Error

В случае ошибки (**Result = -1**) настоящее поле содержит текст этой ошибки.

19.3.1.4 Дополнительно

При использовании REST существует возможность получить страницу помощи с описанием перечня доступных методов, а также формата каждого метода и используемых типов данных с примерами. Для этого необходимо в настройках интерфейса взаимодействия с OTP-клиентами активировать публикацию метаданных. Чтобы сделать это, в разделе реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JaCarta Authentication Server\default\AuthenticationService

создайте строковый параметр **Metadata** и задайте для него значение **True** (Истина).

Увидеть страницу помощи можно будет по следующему адресу

http://<имя_хоста>:8008/JASEngine/Default/AuthenticationService/rest/help. Эта страница носит информационный характер и не подразумевает использование для интеграции, как, например, описание в формате WSDL.

19.3.2 WCF

19.3.2.1 Общие сведения

Точка доступа WCF доступна по адресу

http://<имя_хоста>:8008/JASEngine/Default/AuthenticationService. Адрес можно изменить в настройках интерфейса взаимодействия с OTP-клиентами в разделе реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JaCarta Authentication Server\default\AuthenticationService\Address.



Подробнее см. «Настройка сетевых программных интерфейсов JAS», с. 19.

Также в адресе можно изменить протокол. Поддерживаются HTTP или net.tcp. Здесь рассмотрен только протокол HTTP, т.к. он поддерживает стандартный протокол SOAP, предоставляющий более широкие возможности для интеграции.

19.3.2.2 WSDL

Одним из вариантов интеграции со службой аутентификации по протоколу HTTP/SOAP является использование описания в формате WSDL. Чтобы его получить, необходимо в настройках интерфейса взаимодействия с OTP-клиентами активировать публикацию метаданных. Для этого в разделе реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\JaCarta Authentication Server\default\AuthenticationService

создайте строковый параметр **Metadata** и задайте для него значение **True** (Истина).

После этого описание WSDL будет доступно по следующим адресам:

- **http://<имя_хоста>:8008/JASEngine/Default/AuthenticationService?wsdl;**
- **http:// <имя_хоста>:8008/JASEngine/Default/AuthenticationService?singleWsdl.**

20. Установка плагина «Крипто БД» на сервер JAS

На компьютер с установленным и настроенным компонентом JAS (в случае кластера – на все компьютеры с узлами кластера JAS) следует установить соответствующий плагин СКЗИ «Крипто БД».

Для этого выполните следующие действия.

1. Запустите на выполнение файл инсталлятора *Aladdin.JAS.CryptoDB.Server.Plugin.msi*. Отобразится следующее окно.

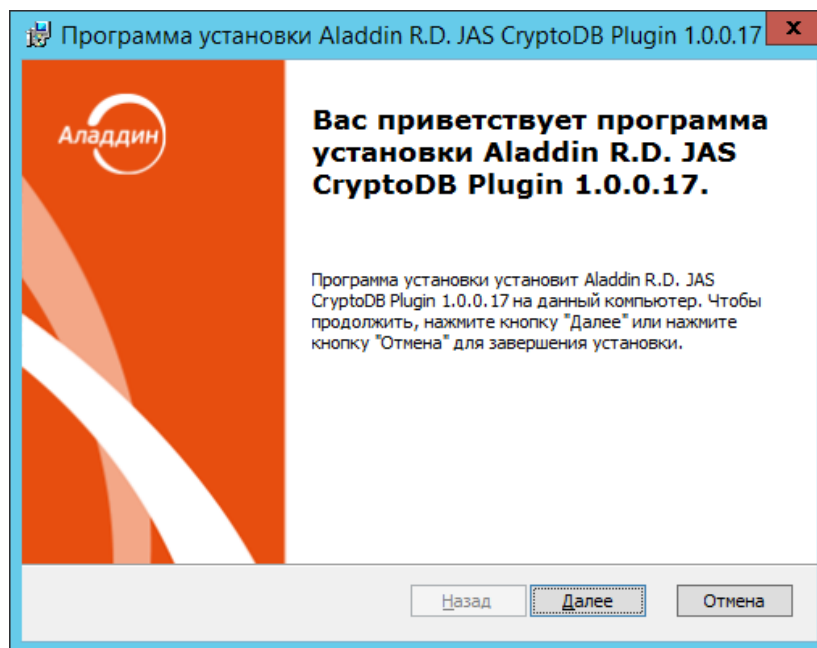


Рис. 125 – Окно приветствия мастера установки плагина СКЗИ «Крипто БД» для сервера JAS

2. Нажмите **Далее**. Отобразится окно лицензионного соглашения. Выберите **Я принимаю условия лицензионного соглашения**, нажмите **Далее** и следуйте указаниям мастера до полной установки плагина.

По завершении установки отобразится следующее окно.

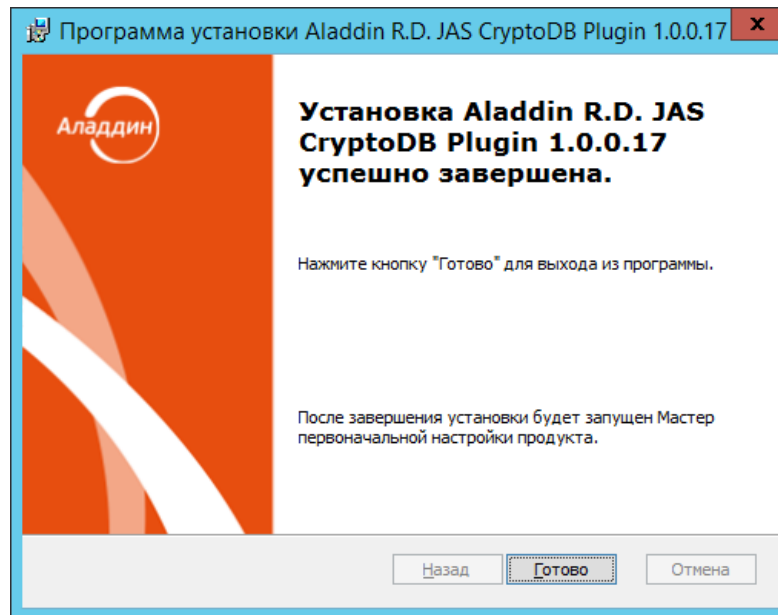


Рис. 126 – Окно завершения процедуры установки

По окончании установки на сервере JAS будет установлен плагин СКЗИ «Крипто БД» для JAS.

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания «Аладдин Р. Д.».

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40.

Факс: +7 (495) 646-08-82.

E-mail: aladdin@aladdin.ru (общий).

Web: www.aladdin.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт:

www.aladdin.ru/support/index.php

Список литературы

- 1 Universal 2nd Factor (U2F) Overview. FIDO Alliance Implementation Draft 15 September 2016 [Текст]. – FIDO Alliance, 2016. – 12 с.
- 2 JaCarta Management System v3.7. Руководство администратора. Часть 1. Установка и настройка [Текст]. – «Аладдин Р.Д.». – Файл JMS_x.x_AdminGuide_(Part1)_Installation_RU.docx
- 3 JaCarta Management System v3.7. Руководство администратора . Часть 2. Функции управления [Текст]. – «Аладдин Р.Д.». – Файл JMS_x.x_AdminGuide_(Part2)_Management_RU.docx
- 4 JaCarta Management System. Руководство пользователя [Текст]. – «Аладдин Р.Д.». – Файл JMS_x.x_UserGuide_RU.docx
- 5 Aladdin 2FA Service. Руководство администратора под Windows. Настройка взаимодействия Aladdin 2FA Service и JMS [Текст]. – «Аладдин Р.Д.». – Файл «Aladdin 2FA Service. Руководство администратора под Windows.pdf»

Полезные web-ресурсы

- 1 Microsoft. Developer Network. Documentation. X509VerificationFlags Enumeration:
[https://msdn.microsoft.com/en-us/library/system.security.cryptography.x509certificates.x509verificationflags\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.security.cryptography.x509certificates.x509verificationflags(v=vs.110).aspx)
- 2 FIDO Alliance. Download Specifications. <https://fidoalliance.org/download/>
- 3 Как создать центральное хранилище для административных шаблонов групповой политики в Windows и управлять им.
<https://support.microsoft.com/ru-ru/help/3087759/how-to-create-and-manage-the-central-store-for-group-policy-administra>

Регистрация изменений

Версия	Изменения
1.00	Исходная версия документа для JMS версии 3.7.1.

Коротко о компании

Компания «Аладдин Р. Д.» основана в апреле 1995 года и является российским разработчиком (вендором) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

Основные направления

- Обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация).
- Электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI.
- Защита персональных данных, данных на дисках компьютеров, серверов, баз данных.
- Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

Лицензии

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа.
- Система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты.
- Система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании соответствует требованиям
ГОСТ Р ИСО 9001-2015 (ISO 9001:2015). Сертификат СМК № РОСС RU.ФК14.К00011 от 20.07.18

© АО «Аладдин Р. Д.», 1995 – 2023. Все права защищены
Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web: www.aladdin.ru