JaCarta Management System 4LX

Руководство администратора. Часть 3

Установка и настройка сервера аутентификации (JAS)

Версия продукта	4LX
Версия документа	1.00
Статус	Публичный
Дата	29 декабря 2023 г.
Листов	139

2023

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

Оглавление

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) для среды функционирования Linux.

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 и условных обозначений приведены в таблице 1.

Табл. 1 — Элементы оформления

Выделение	Используется для выделения наименований полей, кнопок, секций, вкладок экранных форм
`file.exe`	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. 6	Используется для выделения перекрестных ссылок
	Важная информация
	Ссылка, примечание, заметка
	Совет
	Рекомендация

1.4 Обозначения и сокращения

Табл. 2— Обозначения и сокращения

AD	Active Directory – служба каталогов Microsoft
AD FS	Active Directory Federation Services – служба федерации Active Directory
ALO, СДР ALO	**Aladdin LiveOffice** – средство обеспечения безопасной дистанционной работы (СДР) компании Аладдин. В качестве электронного ключа (USB-носителя) использует устройство Aladdin LiveToken (далее для простоты – **СДР ALO**)
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
JMS	То же, что «JaCarta Management System 4LX»
JWA **(JMS Web Agent)**	Программное обеспечение, обеспечивающее взаимодействие web-клиента JMS с ЭК/ЗНИ/СДР из среды web-браузера.
JWA Tray **(JMS Web Agent Tray)**	Программа, позволяющая выполнять базовые операции с ЭК/ЗНИ/СДР пользователя в фоновом режиме или через простое графическое меню. Запущенное приложение отображается значком в области уведомлений рабочего стола
Messaging-токен	Аутентификатор, позволяющий проводить аутентификацию путем 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
PIN-код администратора	Секретная последовательность, известная только администратору, которую необходимо предъявить для аутентификации администратора в приложении электронного ключа
PIN-код подписи **(PIN-код ЭП)**	Секретная последовательность, известная только пользователю, которую необходимо предъявить для выполнения операции электронной подписи
PIN-код пользователя	Секретная последовательность, известная только пользователю, которую необходимо предъявить для аутентификации пользователя в приложении электронного ключа
PUSH-токен	Разновидность **Программного OTP-токена**, реализованная в мобильном приложении Aladdin 2FA (A2FA) компании Аладдин, обеспечивающая аутентификацию пользователя с использование дополнительного фактора OTP без необходимости введения одноразового пароля пользователем
REST	Метод сетевого взаимодействия приложений, при котором вызов представляет собой обычный HTTP-запрос
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
USB	Universal Serial Bus, универсальная последовательная шина
web-клиент JMS	Web-приложение Клиент JMS. Комплекс программ, состоящий из компонента JMS Web Agent из комплекта поставки ПО JMS и web-клиента, функционирующего в среде web-браузера
Аутентификатор (аутентификатор с поддержкой OTP)	Средство аутентификации пользователя; информационный объект, являющийся единицей учета на сервере JAS. В JAS принимаются к учету следующие виды аутентификаторов: • OTP-токен • PUSH-токен • Messaging-токен • U2F-аутентификатор
БД	База данных
ЗНИ	Защищенный носитель информации – электронный ключ JaCarta SF/ГОСТ, обеспечивающий гарантированную защиту информации, хранимую во внутренних разделах электронного ключа (скрытые разделы RW и CD-ROM)
КД	Ключевой документ – в терминологии JMS это ключевая информация (КИ), записанная на электронный ключ (ключевой носитель – СКЗИ) и хранящаяся на нем
КИ	Ключевая информация – в терминах JMS это сертификат открытого ключа и соответствующий данному сертификату закрытый ключ (Номер КИ – это серийный номер сертификата открытого ключа)
Клиентский агент	То же, что приложение **Клиент JMS**. Приложение с графическим пользовательским интерфейсом, предназначенное управления электронными ключами на рабочих станциях конечных пользователей.
Консольный агент	Приложение, предназначенное для конфигурирования сервера JAS. Устанавливается вместе с компонентом JAS
НД	Нормативный документ – в терминах JMS означает вид документов (актов), формируемых при операциях с СКЗИ в соответствии с требованиями регулятора
ПО	Программное обеспечение
ПО Консоль управления JMS	Приложение административной консоли JMS, позволяет осуществлять операции, связанные с управлением жизненным циклом OTP-, PUSH- и U2F-аутентификаторов
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
СДР	Средство дистанционной работы пользователей с вычислительными и информационными ресурсами автоматизированной (информационной) системы

СКЗИ	Средство криптографической защиты информации
ФКН	Функциональный ключевой носитель
ФСБ	Федеральная служба безопасности Российской Федерации
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЭК	Электронный ключ – электронное устройство, используемое как средство аутентификации, и/или защищенного хранения информации, и/или USB-носитель СДР

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 УСТАНАВЛИВАТЬ 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 УСТАНАВЛИВАЯ 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 УСТАНАВЛИВАЙТЕ 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 индивидуальное, 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 нелицензионным 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 подразумевающихся 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, НЕСМОТРЯ 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 утерянные сбережения, вызванные использованием или связанные 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 УСТАНАВЛИВАТЬ 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]).

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.

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

- RFC 4226 (или **HOTP**) – генерация одноразового пароля, основанная на HMAC;
- RFC 6238 (или **TOTP**) – усовершенствованный алгоритм HOTP 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

Параметр	Значение
Операционная система	• Astra Linux SE 1.6 Smolensk • Astra Linux SE 1.7 • Astra Linux CE 2.12 Orel • РЕД ОС 7.2, 7.3 • ОС Альт 8 СП
Сервер СУБД	• Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 • Microsoft SQL Server 2014 • Microsoft SQL Server 2012 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 • PostgreSQL версии 9.6.10 и выше

Параметр	Значение
	• Jatoba 1.9.1-3 и выше
Дополнительное ПО	FreeIPA 4.5.x
Аппаратная платформа	Процессор: 2-ядерный 2,0 ГГц и выше
Оперативная память (не менее)	4 Гбайт
Свободное место на жестком диске (не менее)	20 Гбайт
Сетевой адаптер	100 Мб/с

*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.

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	
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	• Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012	• Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012
Дополнительное ПО	Microsoft .NET Framework 4.6.2 и выше	
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 Системные требования для установки JAS-плагина для Microsoft RDG

Табл. 5 – Системные требования для установки JAS-плагина для Microsoft RDG

Параметр	Значение
Операционная система	• Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012
Дополнительное ПО	Microsoft .NET Framework 4.6.2 и выше
Аппаратная платформа	Процессор: 2-ядерный 2,0 ГГц и выше
Оперативная память (не менее) в дополнение к требованиям операционной системы	500 МБ
Свободное место на жестком диске (не менее)	100 Мбайт
Сетевой адаптер	100 Мб/с

3.4 Системные требования для установки JAS-плагина для JOL

Табл. 6 – Системные требования для установки JAS-плагина для JOL

Параметр	Значение
Операционная система	• Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 (32/64-битные платформы) • Microsoft Windows 10 (32/64-битные платформы) • Microsoft Windows 8.1 (32/64-битные платформы)
Дополнительное ПО	Microsoft .NET Framework 4.6.2 и выше
Аппаратная платформа	Процессор: 2-ядерный 2,0 ГГц и выше
Оперативная память (не менее) в дополнение к требованиям операционной системы	500 МБ
Свободное место на жестком диске (не менее)	15 Мбайт
Сетевой адаптер	100 Мб/с

3.5 Системные требования для установки JAS-плагина для FreeRADIUS

Табл. 7 – Системные требования для установки JAS-плагина для FreeRADIUS

Параметр	Значение
Операционная система	• Astra Linux SE 1.6 Smolensk • Astra Linux SE 1.7 • Astra Linux CE 2.12 Orel • РЕД ОС 7.2, 7.3 • ОС Альт 8 СП
Аппаратная платформа	Процессор: 2-ядерный 2,0 ГГц и выше
Оперативная память (не менее) в дополнение к требованиям операционной системы	1 ГБ
Свободное место на жестком диске (не менее)	10 ГБ
Сетевой адаптер	100 Мб/с

3.6 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. 8 ниже).

Табл. 8 – Пакеты установки JAS

ОС	Файл	Описание
Astra Linux	**aladdin-jas-engine_4.1.0.XXXX_x64.deb**	Пакет установки серверного компонента JAS, включает в себя сервер бизнес-логики JAS и его консольный агент (только для 64-битных систем)
РЕД ОС	**aladdin-jas-engine_4.1.0.XXXX_x64.rpm**	
ОС Альт	**aladdin-jas-engine_4.1.0.XXXX_alt_x64.rpm**	

Табл. 9 – Пакеты установки JAS-плагинов для платформы Windows

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.NPSPlugin_X.X.X.XXX_x64.msi	Пакет установки JAS-плагина для службы AD FS (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)

Табл. 10 – Пакеты установки JAS-плагинов

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.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.

Все параметры лицензии на использование сервера JAS (период использования, разрешенное число аутентификаторов и пр.) устанавливаются в файле лицензии базового компонента – системы JMS.

6. Сетевые программные интерфейсы JAS

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 консольным агентом сервера JAS.

Подробнее о настройке данных интерфейсов см. в разделе «Настройка сетевых программных интерфейсов сервера JAS», с. 21.

7. Установка и первоначальная настройка сервера JAS

7.1 Начальные условия для развертывания JAS

Для развертывания продукта должны быть выполнены следующие начальные условия.

1. В сетевой доступности для сервера JAS должна быть установлена служба управления учетными записями (сервер ресурсной системы, например AD, FreeIPA и т.п.).
2. На компьютере, на котором предполагается устанавливать сервер JAS, должен быть установлен клиентский компонент соответствующей ресурсной системы (AD, FreeIPA и т.п.). Сервер JAS следует зарегистрировать в том же домене ресурсной системы, что и связанный сервер JMS. При установке рекомендуется использовать руководство поставщика сервиса https://wiki.astralinux.ru/display/doc/FreeIPA+Astra+Linux.
3. В сетевой доступности для сервера JAS должен быть установлен сервер СУБД, на котором функционирует БД связанного сервера JMS. При установке могут быть полезны рекомендации поставщика СУБД, например https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362076.

7.2 Установка и первоначальная настройка сервера и консольного агента JAS

Примечание. Все команды в данном разделе выполняются в контексте пользователя root.

7.2.1 Подготовительные действия

Для подготовки к развертыванию сервера JAS и консольного агента JAS выполните следующие действия.

1. Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки JAS, следующие файлы:
   - дистрибутив JAS согласно Табл. 8, с. 17;
   - jas_init.ini.
2. В папке с дистрибутивом JAS создайте файл первоначальной конфигурации сервера JAS jas_init.ini по следующему образцу:

```
[service]
execPath=/opt/jas-engine/Aladdin.JAS.Engine
administrationServiceUrls=http://*:8220
controlServiceUrls=http://*:8219
authenticationServiceUrls=http://*:8221
autoStart=true
culture=ru

[database]
type=PostgreSQL
serverAddress=192.168.10.11
serverPort=5432
databaseName=Test_FreeIPA_JMS_4.1_14
databaseLogin=postgres
databasePassword=123456qweRTY
encryptionPassword=123456qweRTY
```

Назначение остальных параметров файла конфигурации приведено в разделе «Приложение 1. Параметры файла первоначальной конфигурации сервера JAS», с. 107.

7.2.2 Установка сервера JAS

1. Установите на текущем хосте сервер JAS с помощью соответствующей команды.

1.1. Для ОС Astra Linux или ОС Альт:

```
sudo apt-get install <путь_к_файлу_deb/rpm-пакета согласно Табл. 8, с. 17>
```

1.2. Для РЕД ОС:

```
sudo dnf install <путь_к_файлу_rpm_пакета согласно Табл. 8, с. 17>
```

7.2.3 Начальное конфигурирование сервера JAS

1. Выполните начальное конфигурирование сервера JAS с помощью следующей команды консольного агента:

```
sudo Aladdin.JAS.Agent.Terminal server initialize -p <путь к ini-файлу
jas_init.ini>
```

Подключение к БД JMS выполняется автоматически, если была найдена БД с именем, указанным в файле первичной конфигурации JAS.

Примечание. Полное описание команд консольного агента см. в разделе «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal», с. 109.

По окончании конфигурирования в консоли должна отобразиться строка «Инициализация сервера JAS выполнена успешно».

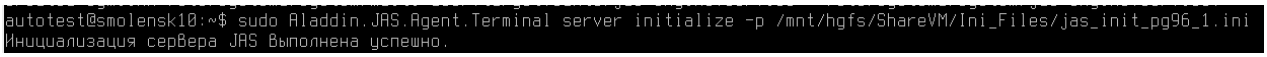


Рис. 1 – Сообщение в консоли об успешной начальной настройке сервера JAS

2. Проверьте статус службы сервера JAS следующей командой.

```
systemctl status jas-engine
```

Состояние должно быть «active (running)»:

Рис. 2 – Отображение статуса службы сервера JAS

3. Проверьте статус сервера бизнес-логики JAS с помощью следующей команды консольного агента

```
Aladdin.JAS.Agent.Terminal server status
```

В случае корректной работы сервера бизнес-логики должна отобразиться строка «Текущее состояние сервера: Работает».

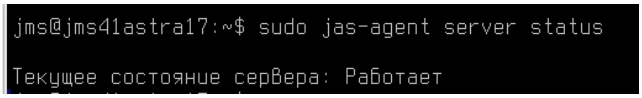


Рис. 3 – Отображение статуса сервера бизнес-логики JAS

7.2.4 Настройка сетевых программных интерфейсов сервера JAS

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

1. На хосте, на котором установлен компонент Сервер JAS, откройте с помощью текстового редактора файл конфигурации /etc/aladdin/jas-engine/AppSettings.json.
2. 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 указанными ниже настройками);
   - **AuthenticationService** – интерфейс взаимодействия с OTP-клиентами (например, с JAS-плагином для NPS);
   - **ControlService** – интерфейс для взаимодействия сервера JAS с консольным агентом JAS – Aldddin.JAS.Agent.Terminal. Свои настройки консольный агент JAS также считывает из общего конфигурационного файла AppSettings.json;

   руководствуясь Табл. 11.

Табл. 11 — Параметры сетевых программных интерфейсов

Параметр	Описание

SecurityType
 	
(Параметр недоступен для программного интерфейса **AuthenticationService**)
	Параметр указывается в секциях **AdministrationServiceWebApi** и/или **ControlServiceWebApi** конфигурационного файла.
	
	Тип аутентификации пользователя при подключении по соответствующему сетевому программному интерфейсу.
	
	Допустимы следующие значения:
	• **None** – аутентификация отключена, доступ к сетевому интерфейсу осуществляется анонимно (значение по умолчанию);
	• **Basic** – базовая http-аутентификация (пароль и логин передаются в запросе на аутентификацию на указанном интерфейсе);
	
	По умолчанию параметр отсутствует, что соответствует значению **None**.
	
	В случае если необходимо включить аутентификацию, в соответствующей секции необходимо добавить параметры **SecurityType**, **UserName** и **Password.** В параметрах **UserName** и **Password** указываются ожидаемые данные для аутентификации на сетевом интерфейсе.
	
	Например:
	`{`
	`"Name": "AdministrationServiceWebApi",`
	`"Settings": {`
	`"KeepAliveTimeout": "00:02:00",`
	`"MinRequestBodyBytesPerSecond": "240",`
	`…`
	`"SecurityType": "Basic",`
	`"Username": "user",`
	`"Password": "pass"`
	`}`

ControlServiceWebApiAddresses	Адрес интерфейса **ControlService** для взаимодействия с консольным агентом JAS Значение параметра по умолчанию: "ControlServiceWebApiAddresses": "http://localhost:8219" **Примечание.** В случае установки защищенного соединения для программного интерфейса по протоколу SSL/TLS вместо протокола http следует указывать протокол https. Кроме того, в секцию настроек интерфейса следует добавить параметр **Thumbprint**, см. ниже. Подробнее порядок настройки интерфейса на работу через SSL описан в разделе «Настройка SSL/TLS для интерфейса ControlService», с. 100

Параметр	Описание
AdministrationServiceWebApiAddresses	Адрес интерфейса **AdministrationService** для взаимодействия с сервером JMS (сервер JMS выполняет подключение к серверу JAS для управления им) Значение параметра по умолчанию: "AdministrationServiceWebApiAddresses": "http://*:8220", **Примечание.** В случае установки защищенного соединения для программного интерфейса по протоколу SSL/TLS в параметре вместо протокола http указывается https. Кроме того, в секцию настроек интерфейса следует добавить параметр **Thumbprint**, см. ниже. Данные настройки выполняются автоматически посредством команды ssl enable консольного агента JAS, подробное описание см. в разделе «Настройка SSL-подключения сервера JMS к серверу JAS (AdministrationService API)», с. 98
AuthenticationServiceWebApiAddresses	Адрес интерфейса **AuthenticationService** для взаимодействия с OTP-клиентами (например, модулем OTP для NPS) Значение параметра по умолчанию: "AuthenticationServiceWebApiAddresses": "http://*:8221" **Примечание.** В случае установки защищенного соединения для программного интерфейса по протоколу SSL/TLS в параметре вместо протокола http указывается https. Кроме того, в секцию настроек интерфейса следует добавить параметр **Thumbprint**, см. ниже. Данные настройки выполняются автоматически посредством команды ssl enable консольного агента JAS, подробное описание см. в разделе «Настройка SSL/TLS на интерфейсе AuthenticationService», с. 99
Thumbprint	Значение отпечатка SSL-сертификата сервера JAS в соответствующих секциях конфигурационного файла (**ControlServiceWebApi**, **AdministrationServiceWebApi** и **AuthenticationServiceWebApi**). При настройке интерфейса **ControlServiceWebApiAddresses** данный параметр необходимо добавить в секцию **ControlServiceWebApi** вручную при установке защищенного соединения по протоколам SSL/TLS с соответствующим программным интерфейсом. Подробнее см. раздел «Настройка SSL/TLS для интерфейса ControlService», с. 100 Например: `{ "Name": "ControlServiceWebApi", "Settings": { "KeepAliveTimeout": "00:02:00", "MinRequestBodyBytesPerSecond": "240", … "Thumbprint": "2CE4D90BF553B28C45E20B828F955582E9D6CCAE" }`

3. Для вступления настроек в силу перезапустите службу сервера JAS:

```
sudo systemctl restart jas-engine
```

7.2.5 Подключение сервера JMS к серверу JAS для обеспечения управления

Для того чтобы сервер JAS мог нормально функционировать после его установки и настройки его интерфейсов, необходимо выполнить подключение к нему сервера JMS. Данное подключение выполняется на хосте сервера JMS командой *jas configure* консольного агента Aladdin.JAS.Agent.Terminal (подробнее см. Часть 1 Руководства администратора [2], раздел «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal»), например:

```
Aladdin.EAP.Agent.Terminal jas configure -u http://localhost:8220 -s Basic -l
DOMAIN\jas -p zxasqw12!@
```

В параметрах команды следует указывать значения в соответствии с ранее выполненными на сервере JAS настройками для интерфейса **AdministrationService** (см. раздел «Настройка сетевых программных интерфейсов сервера JAS», с. 21).

Порядок настройки подключения JMS к серверу JAS по защищённому соединению (SSL) описан в разделе «Настройка SSL-подключения сервера JMS к серверу JAS (AdministrationService API)», с. 98.

8. Порядок настройки транспорта для работы с Messaging-токенами

Чтобы настроить транспорт для работы с Messaging-токенами (параметры передачи служебной информации и самих OTP-паролей по SMS) выполните следующие действия.

1. Выгрузите конфигурационный json-файл нужного типа профиля с помощью команды *sms savedefault* консольного агента JAS, например:

   ```
   Aladdin.JAS.Agent.Terminal sms savedefault -t offline -p
   /mnt/hgfs/ShareVM/offline_default.json
   ```

   Подробное описание команды *sms savedefault* и остальных команд консольного агента JAS см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.JAS.Agent.Terminal», с. 109.
2. Отредактируйте сохраненный файл, установив нужную вам конфигурацию, руководствуясь разделом «Приложение 3. Справочник конфигурационных файлов JAS», с. 115, и выполните его регистрацию, например:

   ```
   sudo Aladdin.JAS.Agent.Terminal sms register -p
   /mnt/hgfs/ShareVM/jas_http_config_1.json
   ```
3. Получите список зарегистрированных профилей с помощью команды sms list, например:

   ```
   sudo Aladdin.JAS.Agent.Terminal sms list
   ```
4. Найдите в полученном списке профиль, зарегистрированный на шаге 2. Установите его индекс (номер) и активируйте его (установите в качестве активного профиля) командой *sms setactive*, например:

   ```
   sudo Aladdin.JAS.Agent.Terminal sms setactive --index 2
   ```

   Примечание. В случае если профиль является единственным в списке, он является активным (установка активного профиля не требуется).

9. Другие настройки JAS

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

9.1 Настройка параметров ведения журнала событий в JAS

Сервер JAS позволяет записывать в журнал событий сообщения следующих уровней:

- **OFF** – ведение журнала событий отключено;
- **FATAL** – неустранимая 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. 12 представлены параметры ведения журнала событий для сервера бизнес-логики JAS и серверного агента (ПО Сервер JAS).

Табл. 12 – Настройка параметров ведения основных журналов событий

Компонент JAS	Расположение файла конфигурации	Сведения о настройке ведения журнала событий
Сервер бизнес-логики JAS (*jas-engine*)	Файл конфигурации журналирования **opt\jas-engine\Aladdin.JAS.Engine.log4net**	1. Откройте файл конфигурации с помощью текстового редактора. 2. Отредактируйте значение элемента **<level value>** для элемента **<root>**. Используйте значения, приведённые в начале настоящего раздела.  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**).
Консольный агент (jas-agent)	Файл конфигурации журналирования **opt\jas-engine\jas-agent\Aladdin.JAS.Agent.Terminal.log4net**	

Сохраните изменения и закройте файл конфигурации.

Также существует возможность настроить параметры ведения журнала событий для других компонентов JAS:

- JAS-плагин для NPS, см. раздел «Настройка JAS-плагина для NPS», с. 41;
- JAS-плагин для AD FS см. раздел «Настройка JAS-плагина для AD FS», с. 65;
- JAS-плагин для MS RDG, см. раздел «Настройка JAS-плагина для MS RDG», с. 78;
- JOL, см. раздел «Настройки JOL и порядок их применения», с. 87.

9.2 Настройки журналирования событий аутентификации JAS

Для настройки журналирования событий аутентификации (могут фиксироваться в журнале в БД JMS и посредством Syslog) следует выполнить следующие действия.

1. Выгрузите текущий файл конфигурации журналирования (JournalingManager.json) командой *server config show* консольного агента JAS, например:

```
Aladdin.JAS.Agent.Terminal server config show --path /tmp/jas_config
```

Примечание. Подробнее см. описание команды *server config show* в разделе «Приложение 2. Справочник команд консольного агента Aladdin.JAS.Agent.Terminal», с. 109.

2. Отредактируйте значения параметров настроек *SQLAuthEventLogLevel* и *SyslogAuthEventLogLevel* в соответствии с разделом «Приложение 3. Справочник конфигурационных файлов JAS» -> SyslogManager.json, с. 127.

3. Загрузите отредактированный файл конфигурации журналирования в систему командой *server config upload* консольного агента JAS, например:

```
Aladdin.JAS.Agent.Terminal server config upload -j
/tmp/jas_config/JournalingManager.json
```

4. Для вступления настроек в силу перезапустите сервис JAS

```
systemctl restart jas-engine
```

9.3 Управление конфигурационными файлами сервера JAS

Консольный агент JAS предоставляет ряд команд для выгрузки (с целью редактирования) и последующей загрузки в систему конфигурационных файлов JAS, в частности:

- **BusinessLogic.json** – настройки аутентификации, настройки U2F, настройки TFL;
- **CertificateValidator.json** – настройки сертификатов для U2F;
- **JournalingManager.json** – настройки журналирования аутентификации (подробнее см. «Настройки журналирования событий аутентификации JAS», выше);
- **NotificationManager.json** – настройки профилей Messaging-транспорта (только выгрузка, о настройке профилей Messaging-транспорта подробнее см. «Порядок настройки транспорта для работы с Messaging-токенами», с. 24);
- **SyslogManager.json** – настройки Syslog.

Примечание. Состав и толкование параметров данных файлов приведено в разделе «Приложение 3. Справочник конфигурационных файлов JAS», с. 115.

Управление конфигурационными файлами осуществляется командами *server config show* и *server config upload* консольного агента JAS (подробнее см. раздел «Приложение 2. Справочник команд консольного агента Aladdin.JAS.Agent.Terminal», с. 109).

10. Лицензия на сервер 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. Для просмотра информации о текущих зарегистрированных лицензиях продукта можно воспользоваться соответствующей командой консольного агента JAS

```
Aladdin.JAS.Agent.Terminal licenses list
```

Подробнее см. в разделе «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal», с. 109.

Полное управление лицензиями JMS/JAS доступно в аналогичной команде консольного агента AladdinJAS.Agent.Terminal, см. Часть 1 Руководства администратора [2] , раздел «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal»

Без установки лицензии сервер JAS не может быть запущен (запуск приведет к соответствующей ошибке).

11. Обновление JAS

Для обновления JAS следует:

- остановить службу JAS;
- удалить текущую установку командой управления дистрибутивами;
- установить обновленную версию JAS;
- выполнить проверку работоспособности обновленной версии.

Команда для остановки службы JAS:

```
systemctl stop jas-engine
```

Команда для удаления инсталляции JAS:

```
apt remove jas-engine
```

Установка и проверка статуса функционирования новой версии JAS *aladdin-jas-engine_4.1.x.xxxx* выполняется как и при первичной установке (см. раздел 7.2.2, с. 20). При обновлении сервера не потребуется повторно создавать и настраивать файл первоначальной конфигурации *jas_init.ini*, поскольку текущий системный конфигурационный файл сервера JAS при обновлении продукта берется в качестве исходного при конфигурировании новой версии продукта.

Обновление JAS, являющегося компонентом системы JMS, следует выполнять в согласовании с обновлением остальных компонентов JMS (подробнее см. руководство по установке и настройке JMS [2], раздел «Порядок обновления компонентов JMS»).

12. Установка и настройка JAS-плагина для NPS

12.1 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.

12.1.1 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.

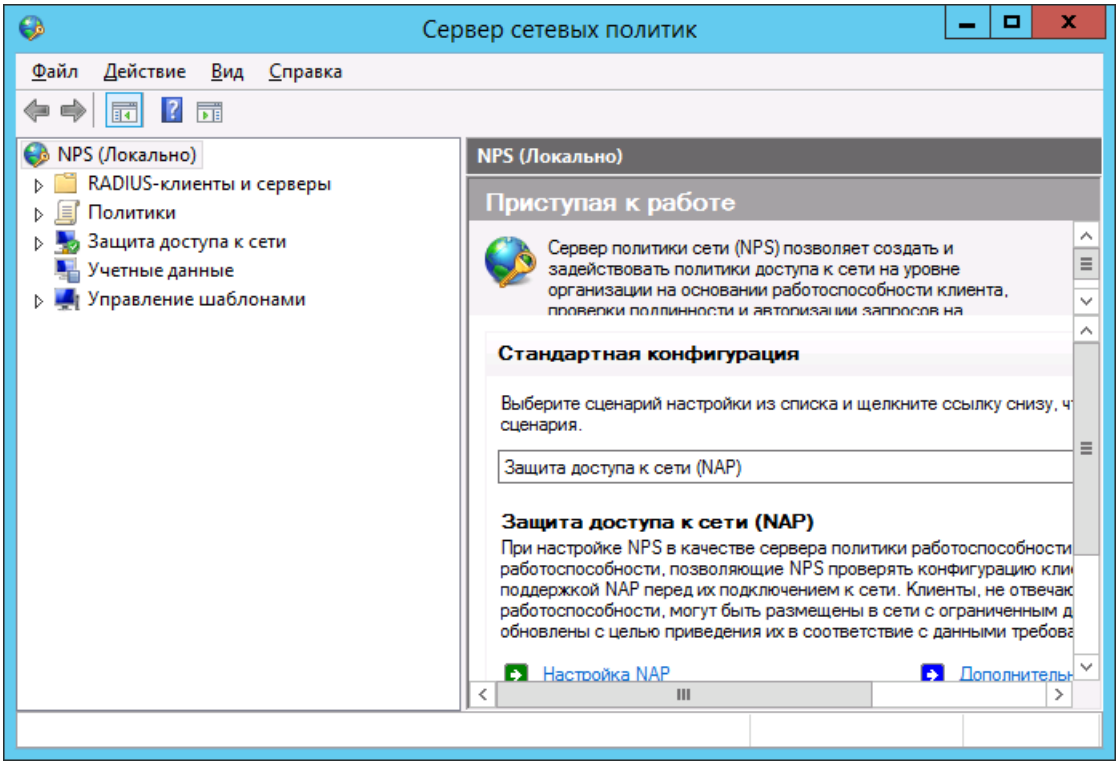


Рис. 4 – Оснастка сервера политики сети

2. Перейдите в раздел **Политики > Политики запросов на подключение** (см. рис. 5 ниже).

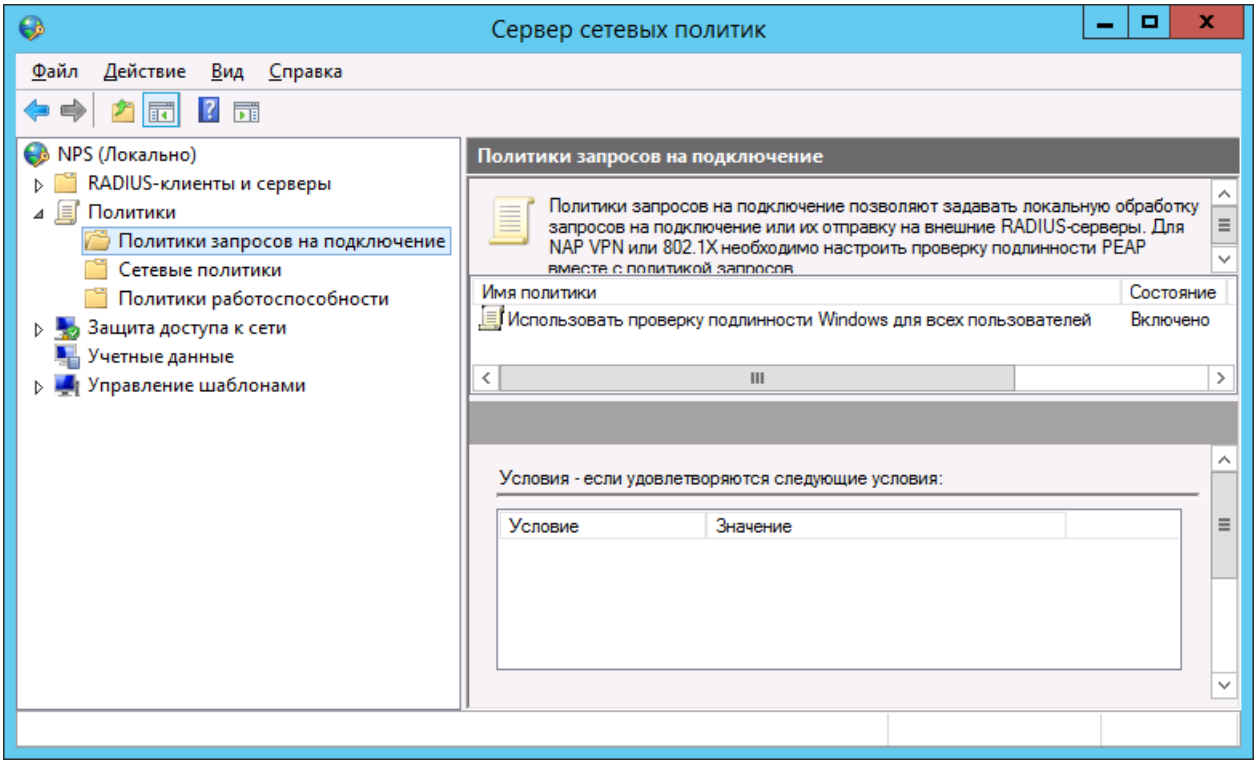


Рис. 5 – Политики запросов на подключение

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. 6 ниже.

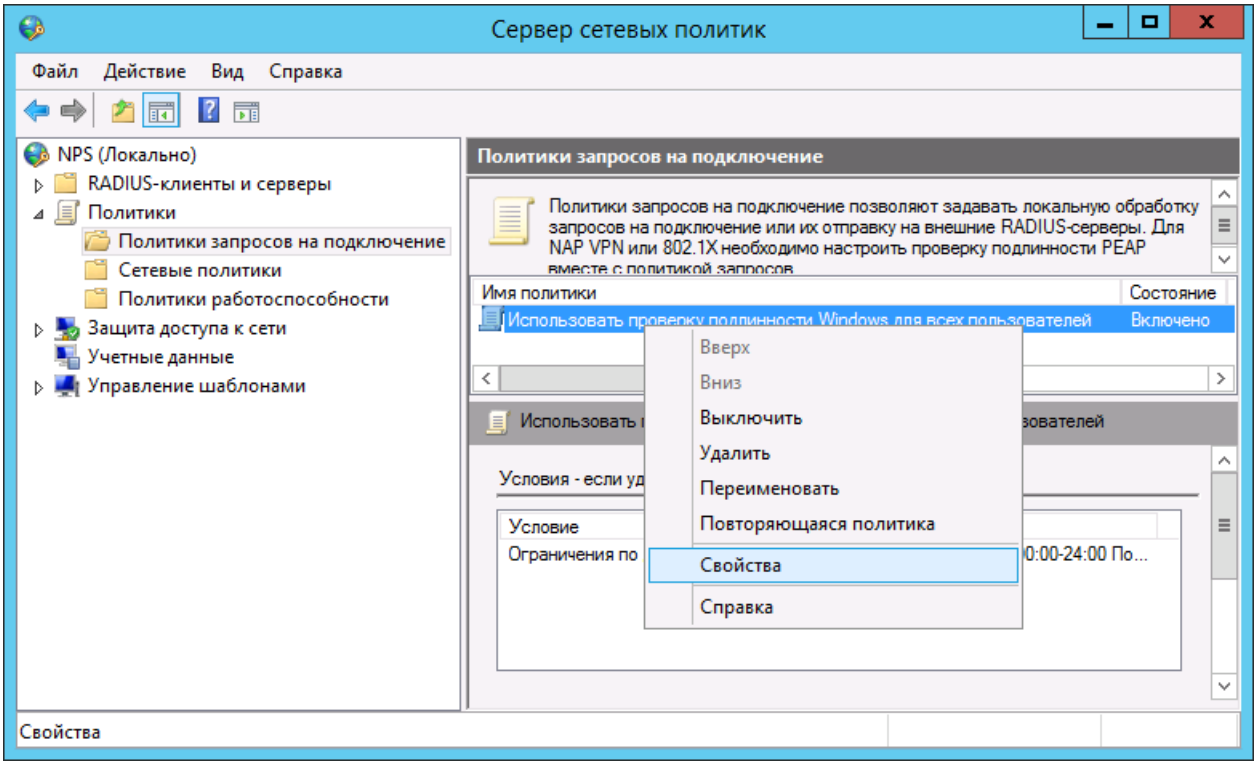


Рис. 6 – Отображение свойств политики запросов на подключение

Отобразится следующее окно.

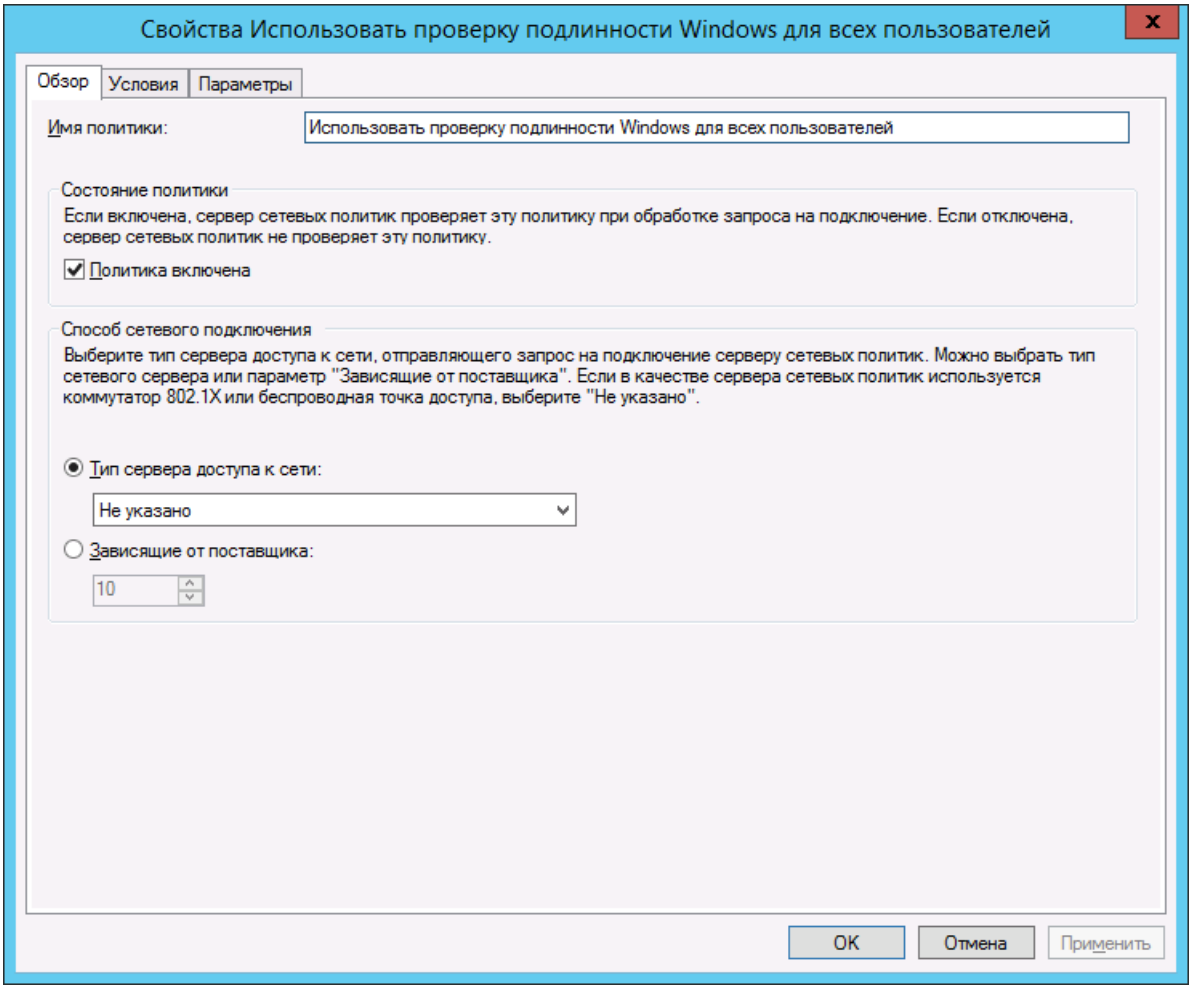


*Рис. 7 – Вкладка **Общие***

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

Окно примет следующий вид.

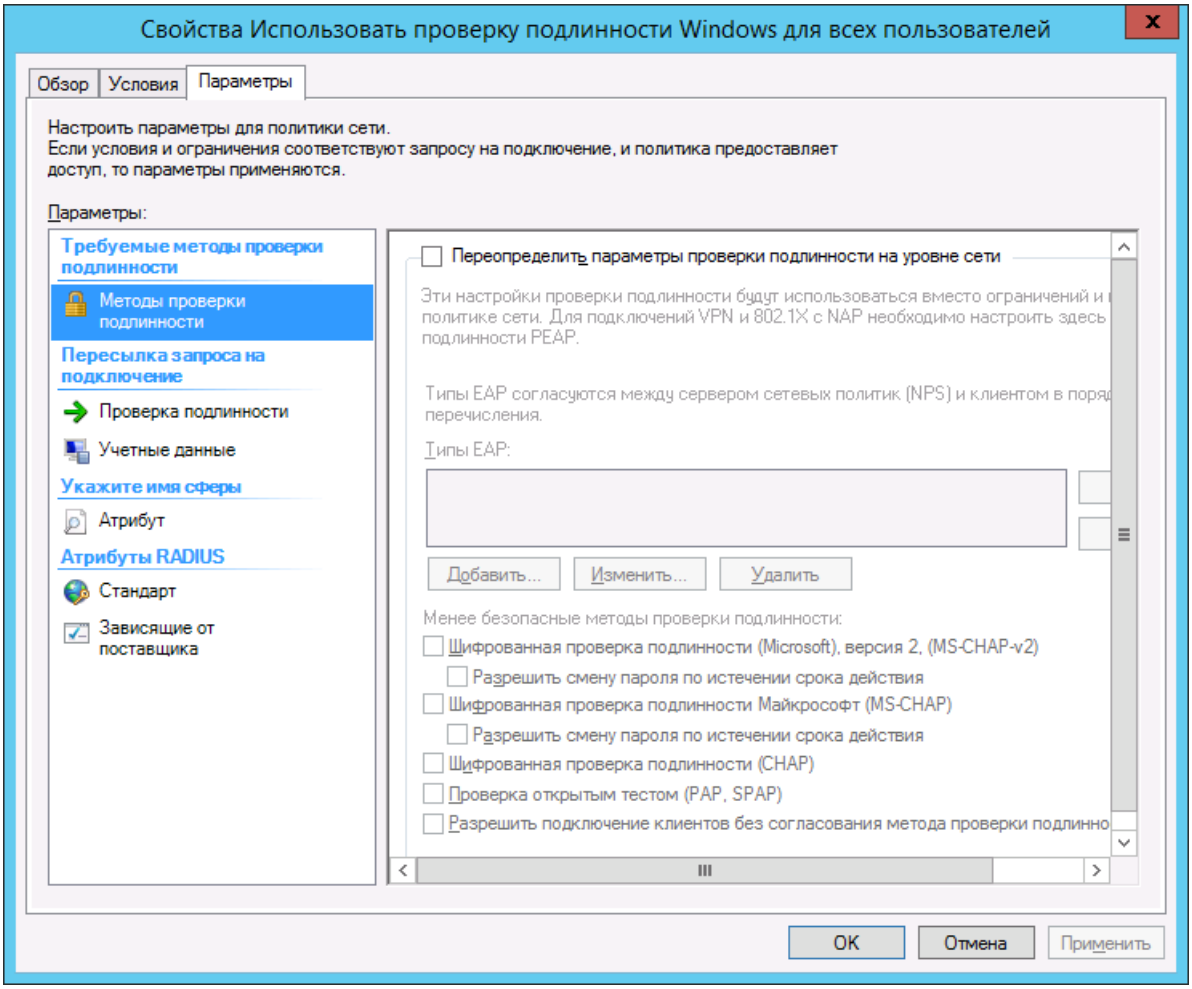


*Рис. 8 – Вкладка **Параметры***

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 **OK**.

Отобразится сообщение с предложением отобразить справку.

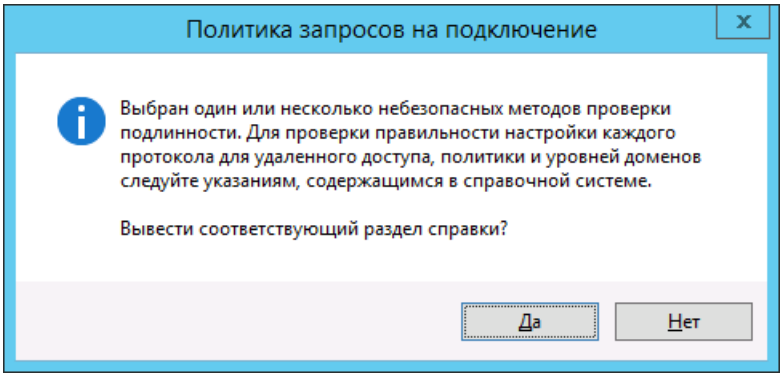


Рис. 9 – Сообщение с предложением отобразить справку

9. Нажмите **Нет**.

12.1.2 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. 10 ниже).

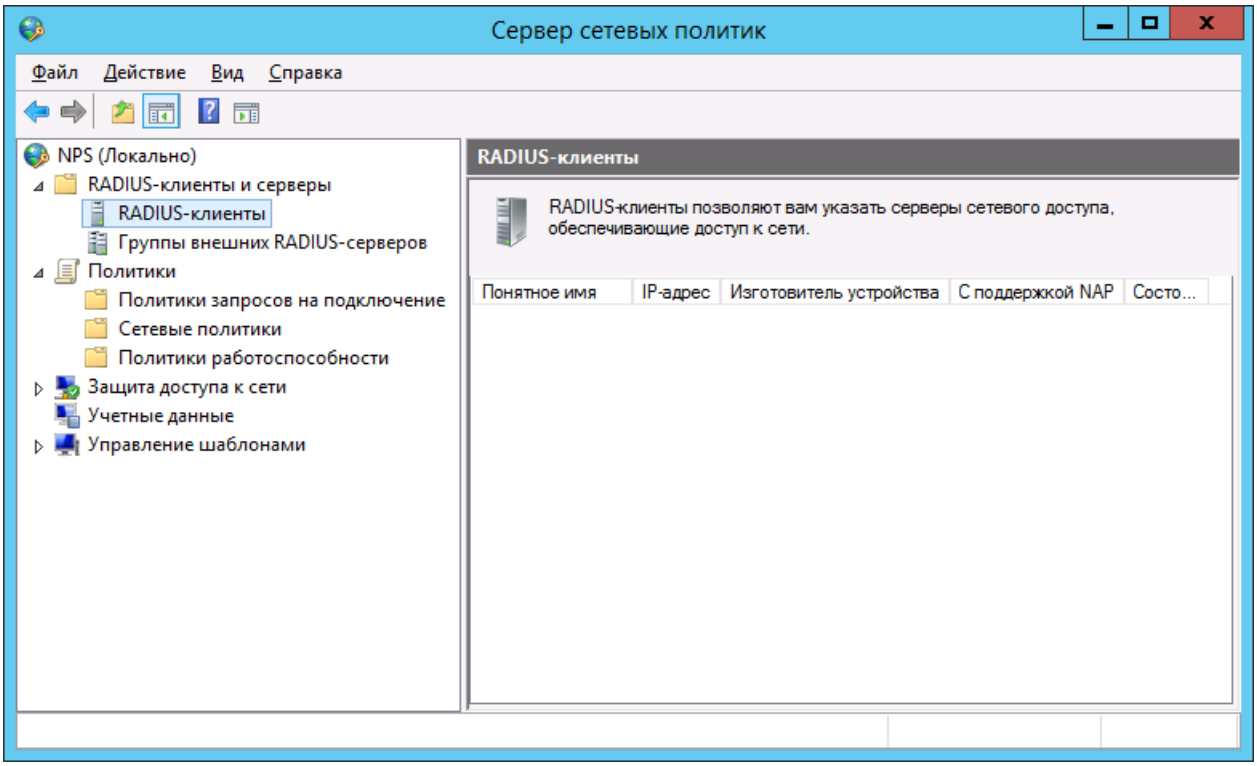


Рис. 10 - RADIUS-клиенты и серверы

2. Нажмите правой кнопкой мыши на пункте **RADIUS-клиенты** и выберите **Новый документ** (см. рис. 11 ниже).

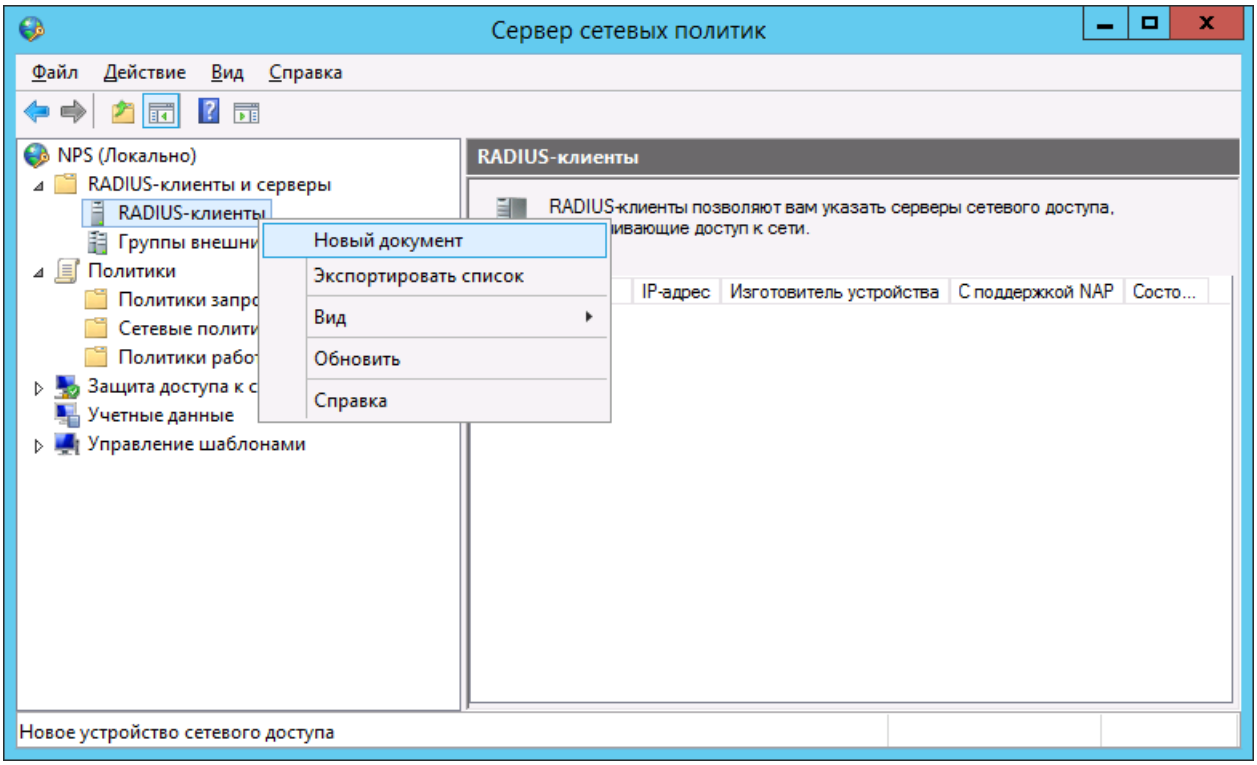


Рис. 11 - Создание RADIUS-клиента

Отобразится следующее окно.

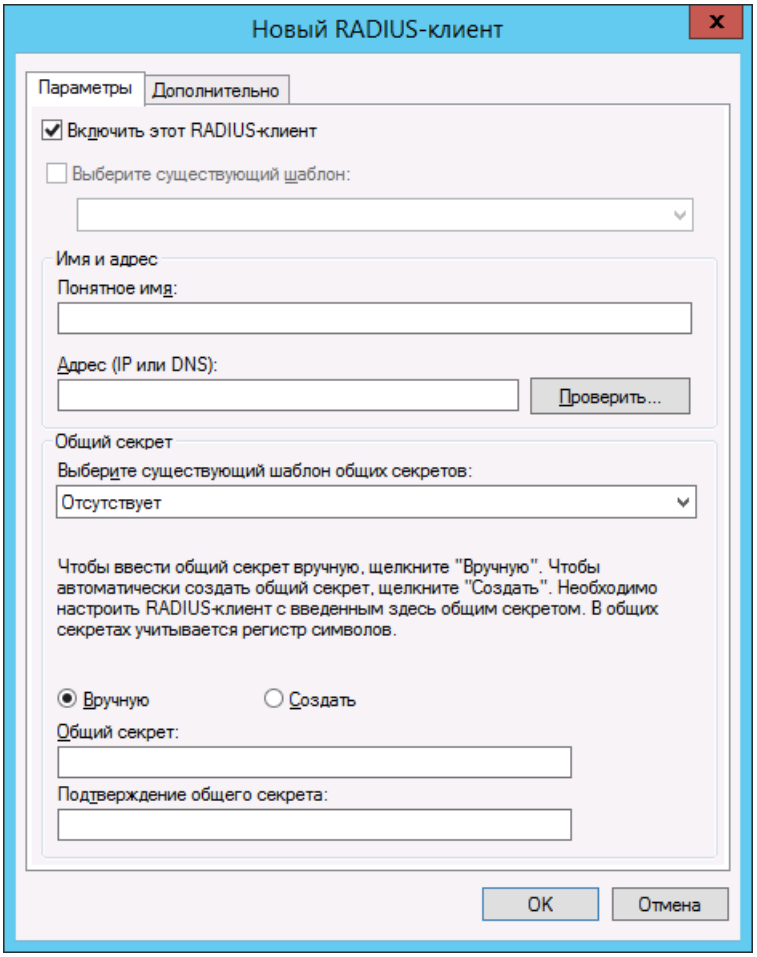


Рис. 12 – Окно настроек RADIUS-клиента

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 введённого адреса, нажмите кнопку **Проверить**.

Отобразится следующее окно.

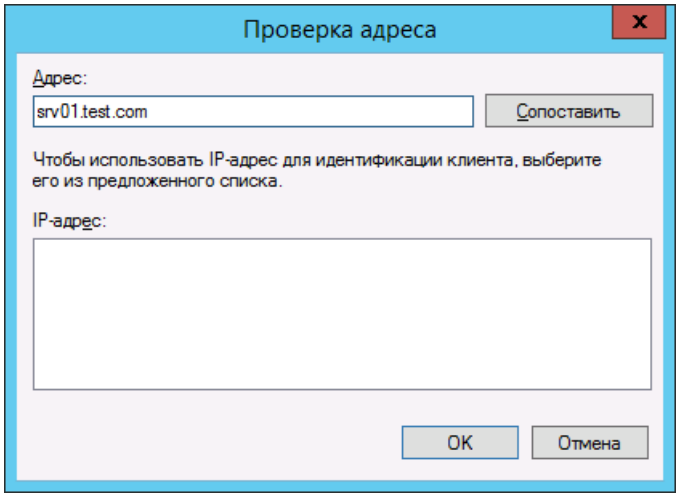


Рис. 13 – Проверка адреса

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

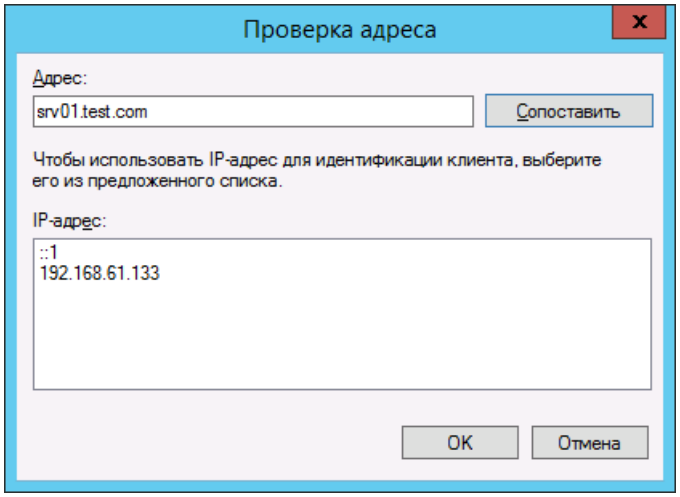


Рис. 14 – Проверка адреса успешна

8. Нажмите **OK**.

Окно настройки RADIUS-клиента будет выглядеть следующим образом.

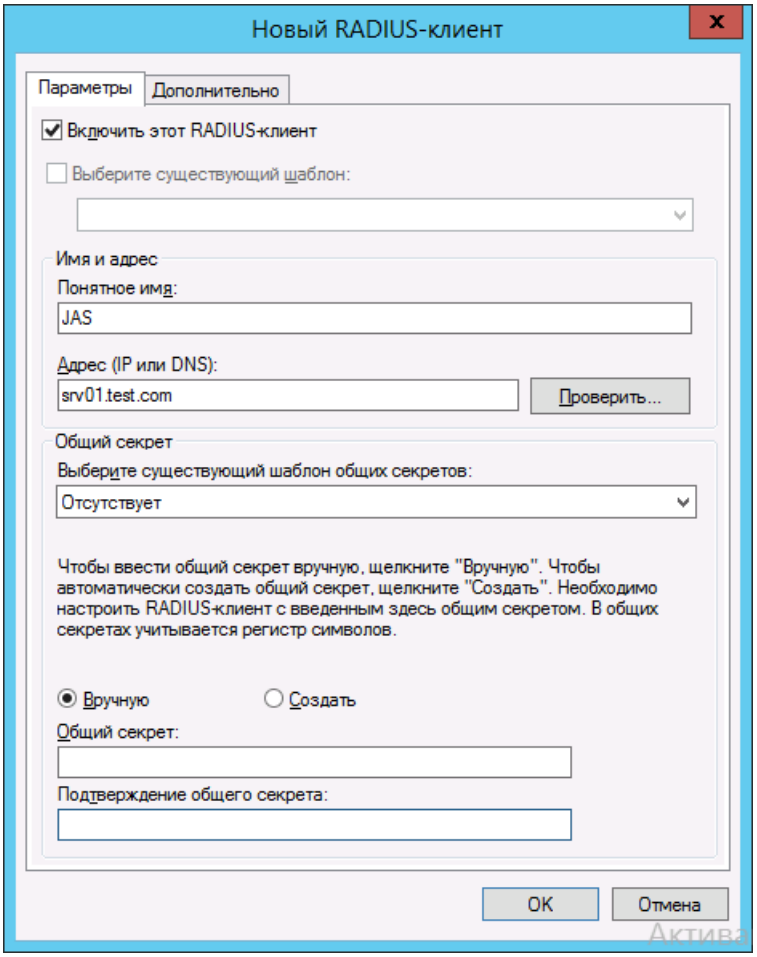


Рис. 15 – Окно настройки RADIUS-клиента

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 **OK**.

Созданный RADIUS-клиент отобразится в оснастке сервера политики сети.

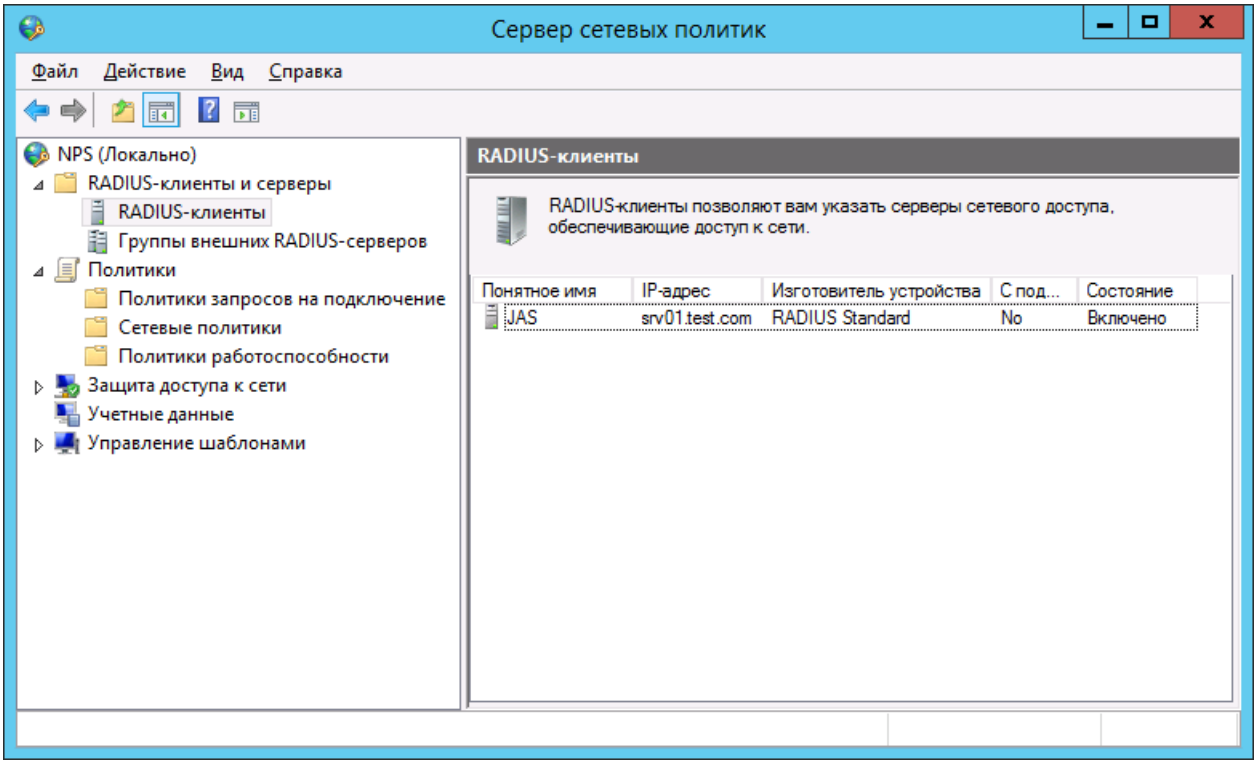


Рис. 16 – RADIUS-клиент создан

12.2 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.

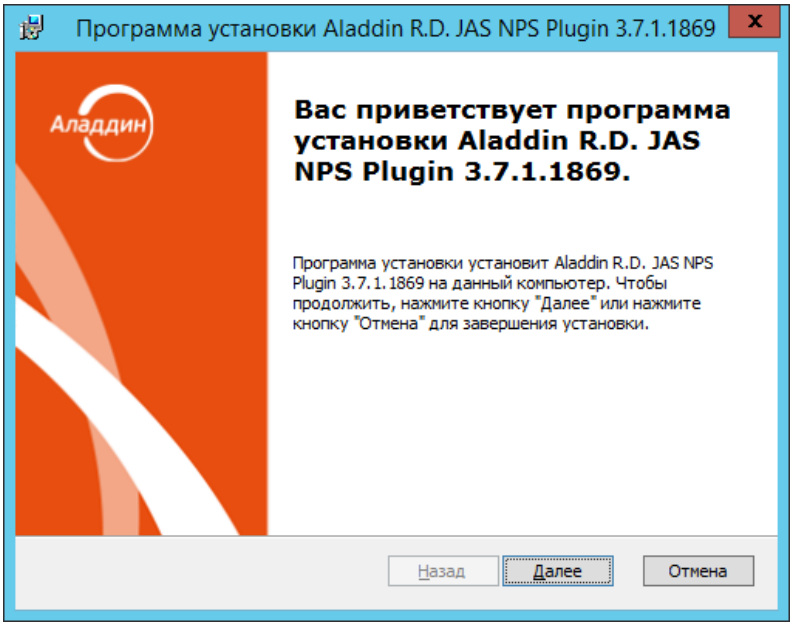


Рис. 17 – Окно приветствия мастера установки JAS-плагина для NPS

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

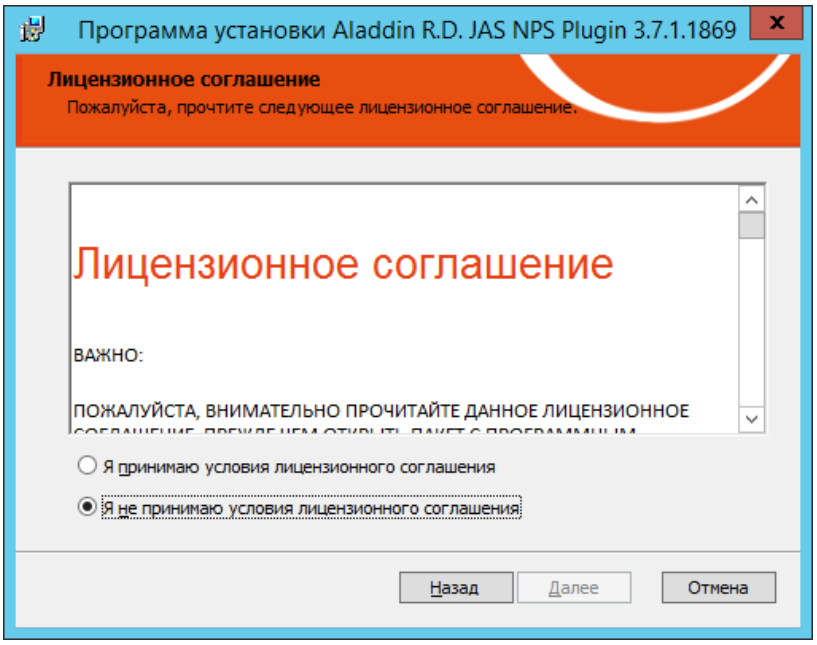


Рис. 18 – Окно лицензионного соглашения

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

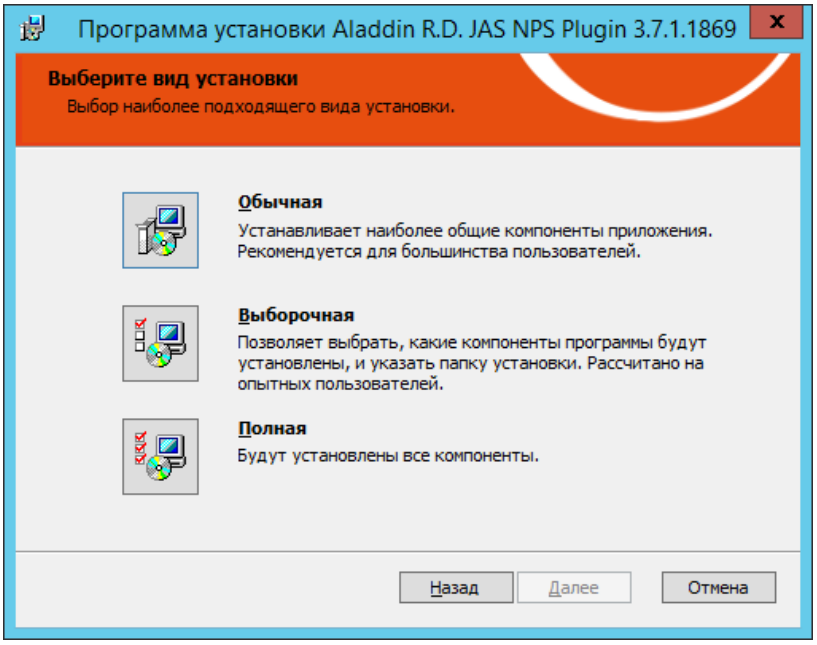


Рис. 19 - Окно выбора варианта установки

4. Выберите **Полная**.

Отобразится следующее окно.

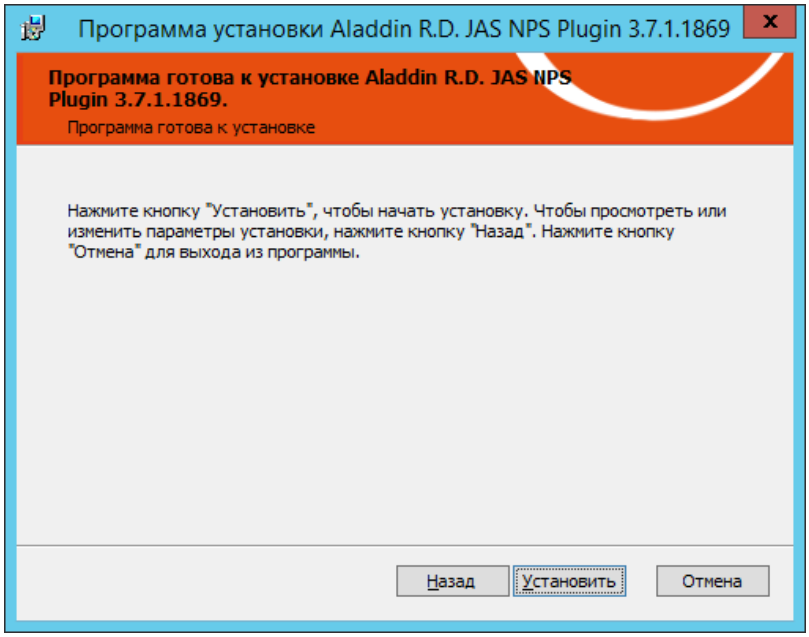


Рис. 20 – Подготовка к установке

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

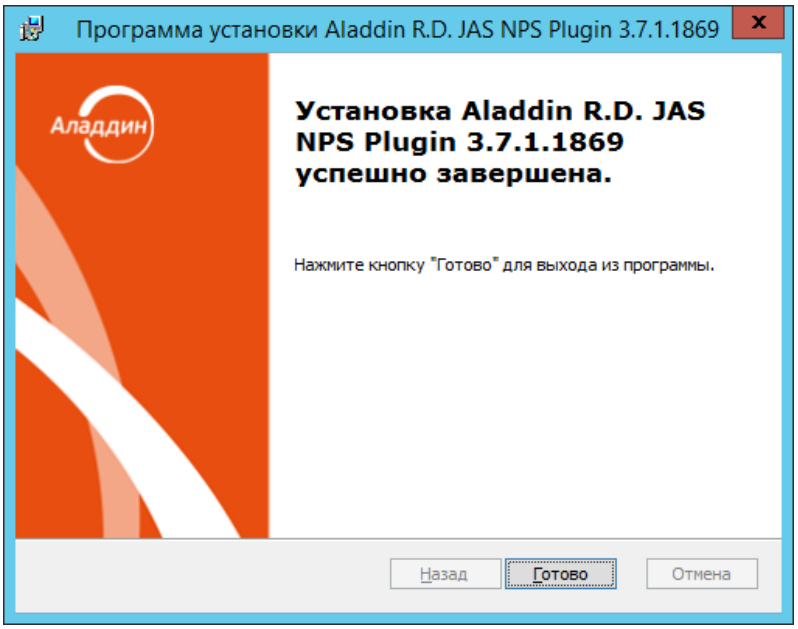


Рис. 21 – Окно завершения установки

6. Нажмите **Готово**.

Отобразится следующее сообщение.

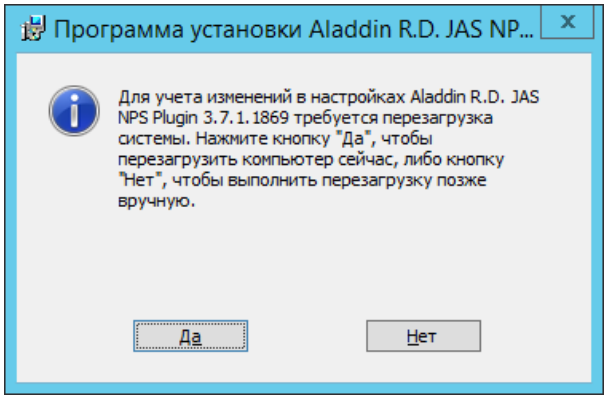


Рис. 22 – Предупреждение о необходимости перезагрузки

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

12.3 Настройка JAS-плагина для NPS

После установки JAS-плагина для NPS автоматически откроется окно так называемого «конфигуратора» **Настройка JAS-плагина для NPS** (Рис. 23, с. 42).

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

12.3.1 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.

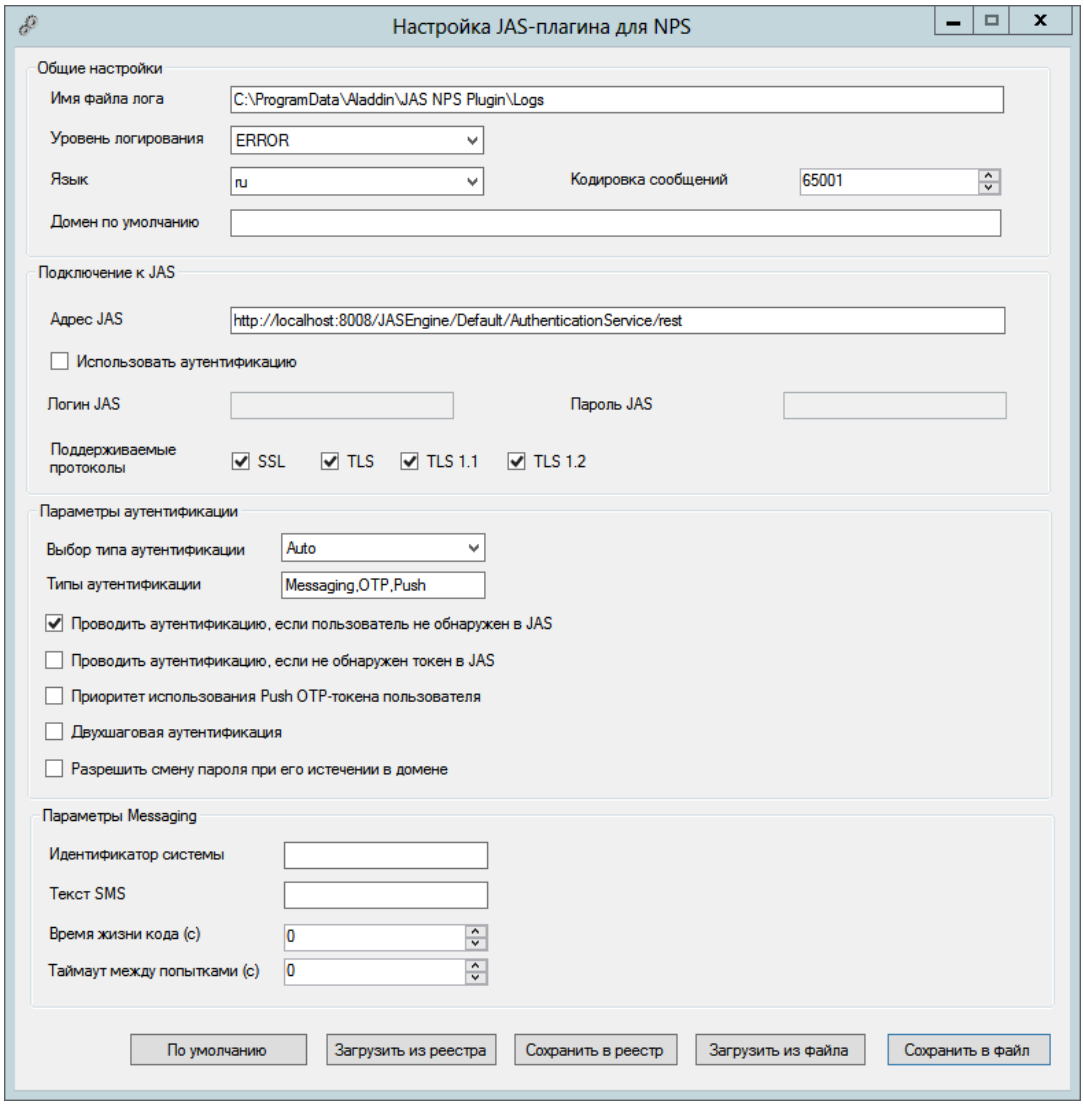


Рис. 23 – Окно Настройка JAS-плагина для NPS

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. 24)

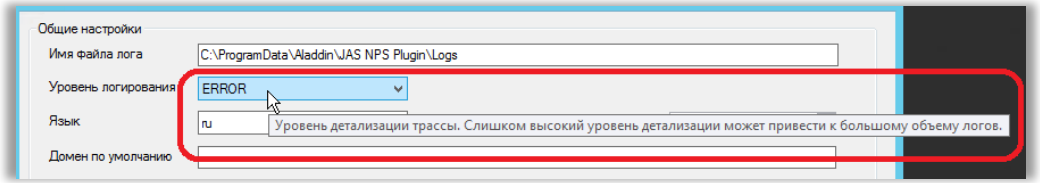


Рис. 24 – Использование всплывающей подсказки в полях формы

10. Выполните настройку, руководствуясь Табл. 13.

Табл. 13 - Настройка JAS-плагина для NPS

Поле конфигуратора	Имя параметра в реестре	Описание
<Секция> **Общие настройки**		
Имя файла лога	**LogFilePath**	Путь, по которому будет сохраняться файл журнала
Уровень логирования	**LogLevel**	Уровень ведения журнала событий. • **OFF** –ведение журнала событий отключено; • **FATAL** – неустранимая ошибка; • **ERROR** – ошибка (значение по умолчанию); • **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**
Язык	**Culture**	Язык пользовательского интерфейса JAS-плагина. Допустимые значения: • **en** (английский язык); • **ru** (русский язык). Значение по умолчанию: **ru** **Примечание.** Параметр определяет, на каком языке имя плагина в должно отражаться в консоли настроек NPS, а также язык сообщений в журналах JAS-плагина для NPS (за локализацию сообщений в браузере пользователя отвечают настройки языка веб-страниц браузера).
Кодировка сообщеинй	**ReplyMessageCodePage**	**Важно!** Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **ChallengeResponseRadiusAuth** = True, выше) 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: • **65001** – кодировка UTF8; • **1251** – Windows-1251; Значение по умолчанию: **65001** **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.

Поле конфигуратора	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>**:8221/api/v4.1** где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com;
Использовать аутентификацию	<без параметра в реестре>	Флаг следует оставить неустановленным (в текущей версии данная настройка не используется).
Логин JAS	**JASUsername**	Не заполняется (в текущей версии данная настройка не используется)
Пароль JAS	**JASPassword**	Не заполняется (в текущей версии данная настройка не используется)
Поддерживаемые протоколы	**SecurityProtocols**	Список поддерживаемых протоколов шифрования для обмена данных между сетевыми узлами. Представляются списком через запятую (например: `Ssl3, Tls, Tls11, Tls12`). Допустимые значения: • Ssl3; • Tls; • Tls11; • Tls12. По умолчанию указываются все допустимые типы протоколов
<Секция> **Параметры аутентификации**		
Выбор типа аутентификации	**AuthTypeSelection**	Режим выбора типа аутентификации. **Важно!** Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **ChallengeResponseRadiusAuth** = True, выше) Допустимые значения: • **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). Значение по умолчанию: **Auto**
Типы аутентификации	**AuthTypes**	Поддерживаемые типы аутентификации и их приоритет.

Поле конфигуратора	Имя параметра в реестре	Описание
		Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **ChallengeResponseRadiusAuth** = True, выше) Возможные методы аутентификации: • **Messaging** – аутентификация по Messaging-токену; • **OTP**—аутентификация по OTP-токенам; • **Push** Методы указываются через запятую в порядке снижения приоритета. Значение по умолчанию: **Messaging, OTP, Push**
Проводить аутентификацию, если пользователь не обнаружен в JAS	**UserNotFound Action**	Действия JAS-плагина, если пользователь, который пытается аутентифицироваться, не зарегистрирован в JAS. Доступные значения: • **Pass** (Пропускать запрос); • **Reject** (Отклонять запрос). Значение по умолчанию: **Pass** (Пропускать запрос).
Проводить аутентификацию, если не обнаружен токен в JAS	**TokensNotFoundAction**	Действия JAS-плагина, 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: • **Pass** (Пропускать запрос); • **Reject** (Отклонять запрос). Значение по умолчанию: **Reject** (Отклонять запрос).
Приоритет использования Push OTP-токена пользователя	**PushTokenAction**	Настройка режима аутентификации по Push-токену OTP. Допустимые значения: • **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 Messging-токенов, использующих режим PAP). Значение по умолчанию: **Reject** (Отклонять запрос).
Двухшаговая аутентификация	**ChallengeResponseRadiusAuth**	Режим работы JAS-плагина для NPS. Допустимые значения: • **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). Значение по умолчанию: **False**

Поле конфигуратора	Имя параметра в реестре	Описание

Разрешить смену пароля при его истечении в домене	**AllowChangeExpiredPassword**	Настройка возможности смены пароля пользователя через NPS-плагин при его истечении в домене.
		
		Допустимые значения:
		• **False** – смена пароля запрещена;
		• **True** – смена пароля разрешена;
		
		Значение по умолчанию: **False**
		
		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:
		`c:\Program Files\Aladdin\JaCarta Authentication Server\Aladdin.JAS.Engine.exe.config`
		Значение параметра задается в секундах.
		`<add key="ChangeDomainPasswordTimeout" value="300"/>`
		Также есть возможность ограничить максимальное количество попыток смена пароля при помощи параметра:
		`<add key="MaxPasswordInputAttempts" value="5"/>`

<Секция> **Параметры messaging**		
Идентификатор системы	**MessagingSystemId**	Идентификатор внешней системы, в которой будут искаться пользователи при аутентификации по Messaging. **Важно!** Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **ChallengeResponseRadiusAuth** = True, выше) **Примечание.** Идентификатор должен совпадать с идентификатором в поле **Внешняя система** на вкладке **Параметры выпуска** соответствующего профиля выпуска Messaging-токенов (см. руководство по функциями управления JMS [3]. раздел «Настройка профиля выпуска Messaging-токенов») Допустимые значения: символьная строка Значение по умолчанию: пустая строка.
Текст SMS	**MessagingAdditionalInfo**	Текст, который будет отправляться в SMS пользователю вместе с кодом аутентификации для Messaging. Например «Код аутентификации для входа в систему XYZ » **Важно!** Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **ChallengeResponseRadiusAuth** = True, выше) Допустимые значения: символьная строка Значение по умолчанию: пустая строка.

Поле конфигуратора	Имя параметра в реестре	Описание
Время жизни кода (с)	**MessagingTtl**	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. По умолчанию – пустая строка (не задано) **Важно!** Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **ChallengeResponseRadiusAuth** = True, выше) **Примечание.** Значение **Время жизни OTP** указывается на вкладке **Параметры выпуска** соответствующего профиля выпуска Messaging-токенов (см. руководство по функциями управления JMS [3]. раздел «Настройка профиля выпуска Messaging-токенов») Допустимые значения: целое число Значение по умолчанию: пустая строка.
Таймаут между попытками (мс)	**MessagingRetryDelay**	Таймаут между попытками аутентификации посредством Messaging-токена (в миллисекундах), например 5000. 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. 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 функциями управления JMS [3]). Значение по умолчанию: пустая строка (не задано)

Поле конфигуратора	Имя параметра в реестре	Описание
<настройка отсутствует в графическом конфигураторе, осуществляется только в реестре>	**DefaultUserDomain**	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. **Примечания:** 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) • **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. Значение по умолчанию: пустая строка
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 конфигуратора 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. 26.
Сохранить в файл		Отображаемые в форме параметры можно сохранить в reg-файл для последующего восстановления настроек
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. 25.

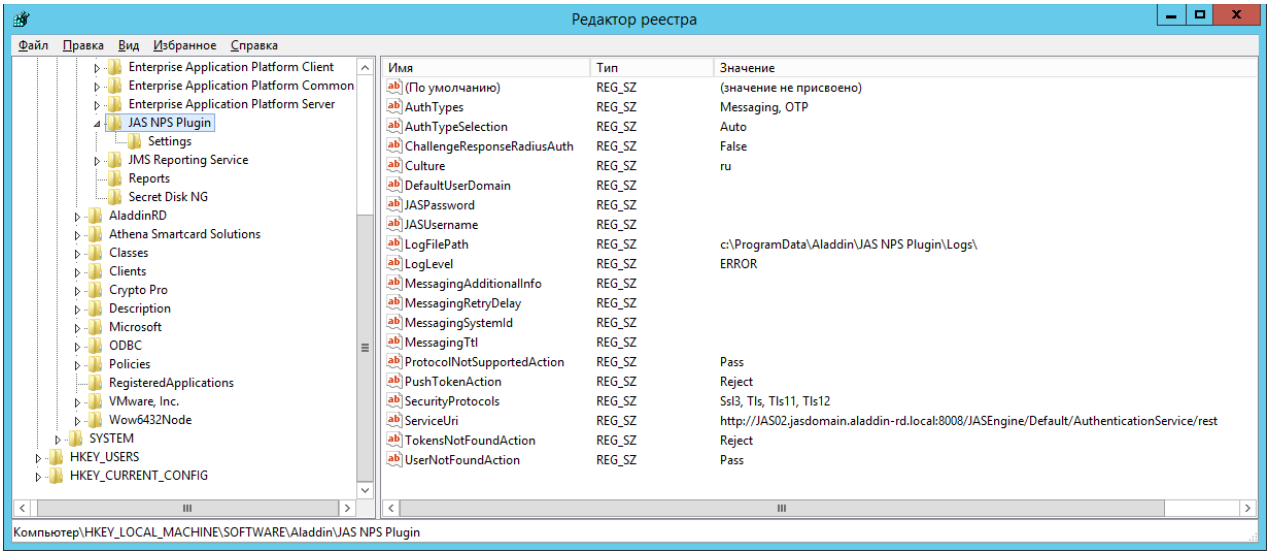


Рис. 25 – Настройки JAS-плагина для NPS

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. 26.

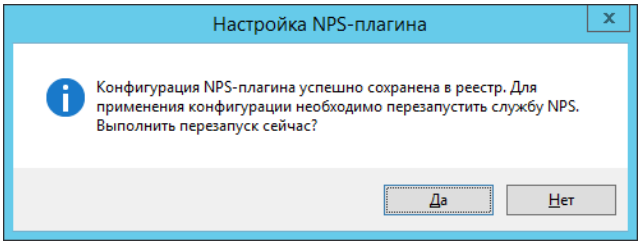


Рис. 26 – Диалог перезапуска службы NPS

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.

12.3.2 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. 13, с. 43), как показано на Рис. 27.

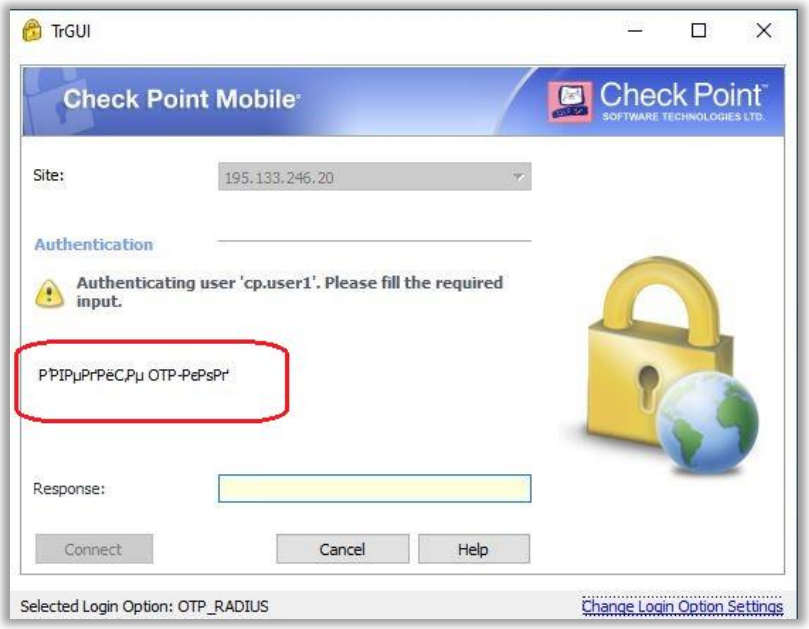


Рис. 27 – Пример некорректного отображения кириллической строки запроса на информацию (ReplyMessage)

В процессе проработки интеграции JAS со сторонним продуктом следует провести исследование на предмет выбора необходимой кодировки (параметр **ReplyMessageCodePage** Табл. 13, с. 43), 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.

12.4 Проверка работы JAS-плагина для NPS

12.4.1 Одношаговая процедура ввода второго фактора аутентификации

Одношаговая процедура подразумевает проверку только дополнительного фактора аутентификации пользователя. В рассматриваемом примере это ввод одноразового пароля (OTP) с помощью заблаговременно выпущенного в JMS OTP-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. 13, с. 43).

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 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]).

2. 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]).
3. На RADIUS-клиенте запустите утилиту **NTRadPing**.
   Окно утилиты будет выглядеть следующим образом.

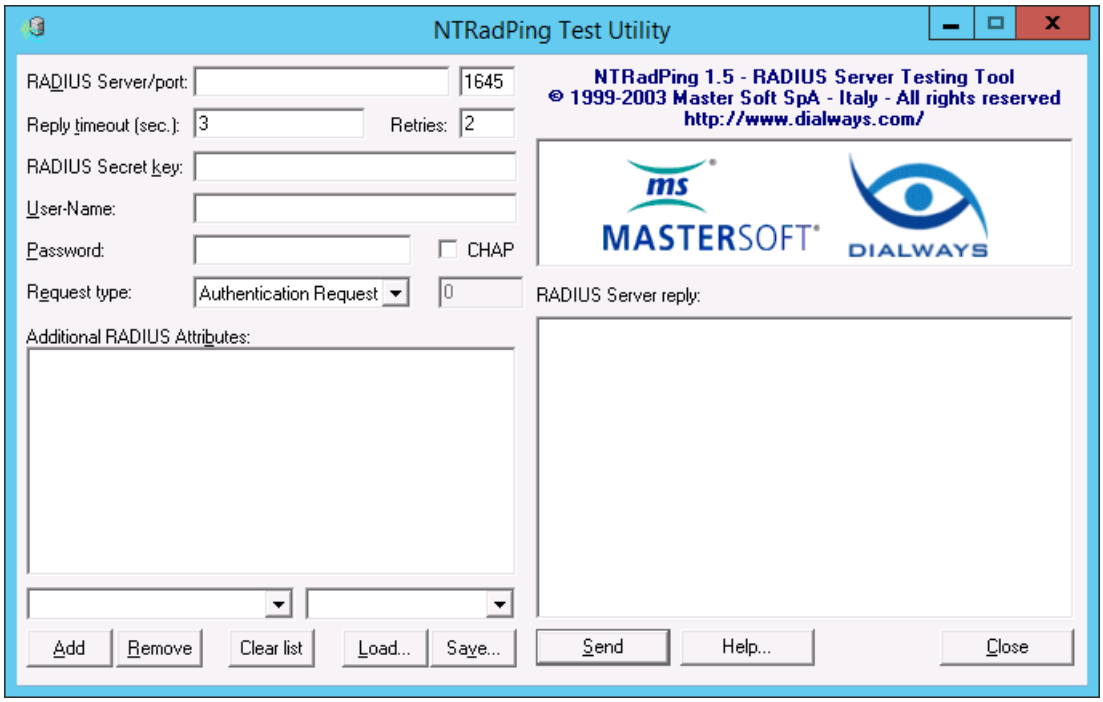


*Рис. 28 – Окно утилиты **NTRadPing***

4. Выполните настройку соединения, руководствуясь табл. 14 ниже.

Табл. 14 – Настройка соединения с RADIUS-сервером

Настройка	Описание
RADIUS Server/port (RADIUS-сервер/порт)	1. В левом поле укажите IP-адрес RADIUS-сервера. 2. В правом поле укажите порт, по которому будет происходить соединение или оставьте значение по умолчанию (**1645**)
Reply timeout (Время ожидания ответа)	Задайте время ожидание 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. 33)
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 указанно пользователя 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)

5. 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.

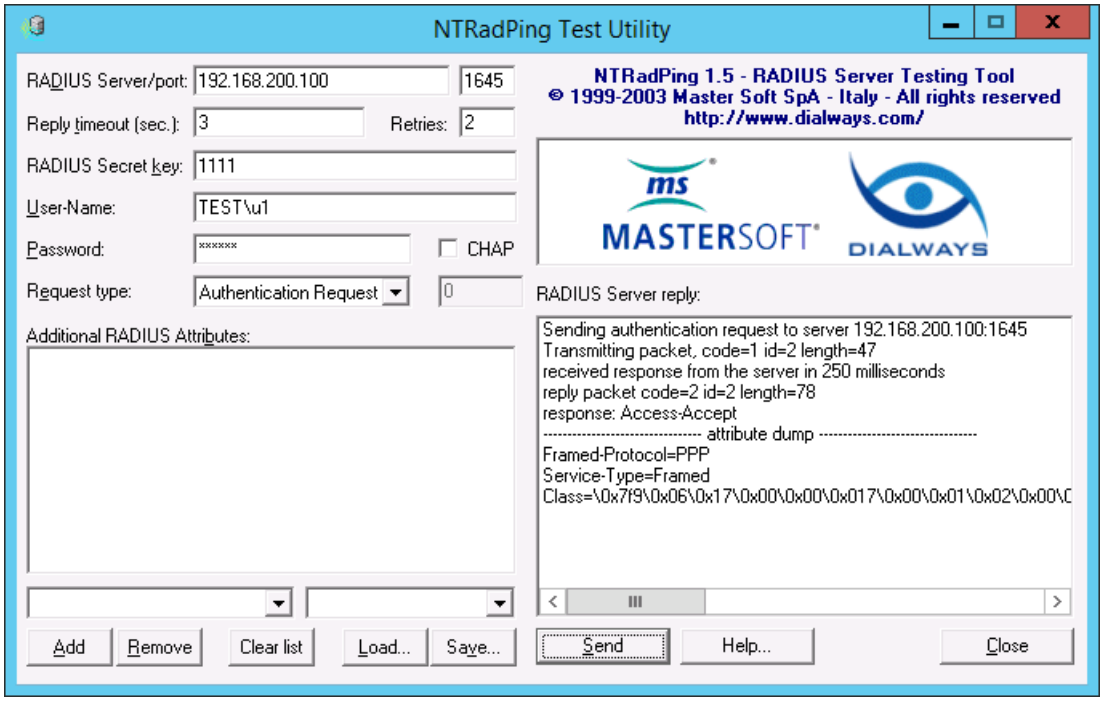


Рис. 29 – Ответ RADIUS-сервера

6. 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. раздел «Настройка сетевых программных интерфейсов сервера JAS», с. 21) и настройки JAS-плагина для NPS (см. «Настройка JAS-плагина для NPS», с. 41).

12.4.2 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. 13, с. 43).

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. 50).

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

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

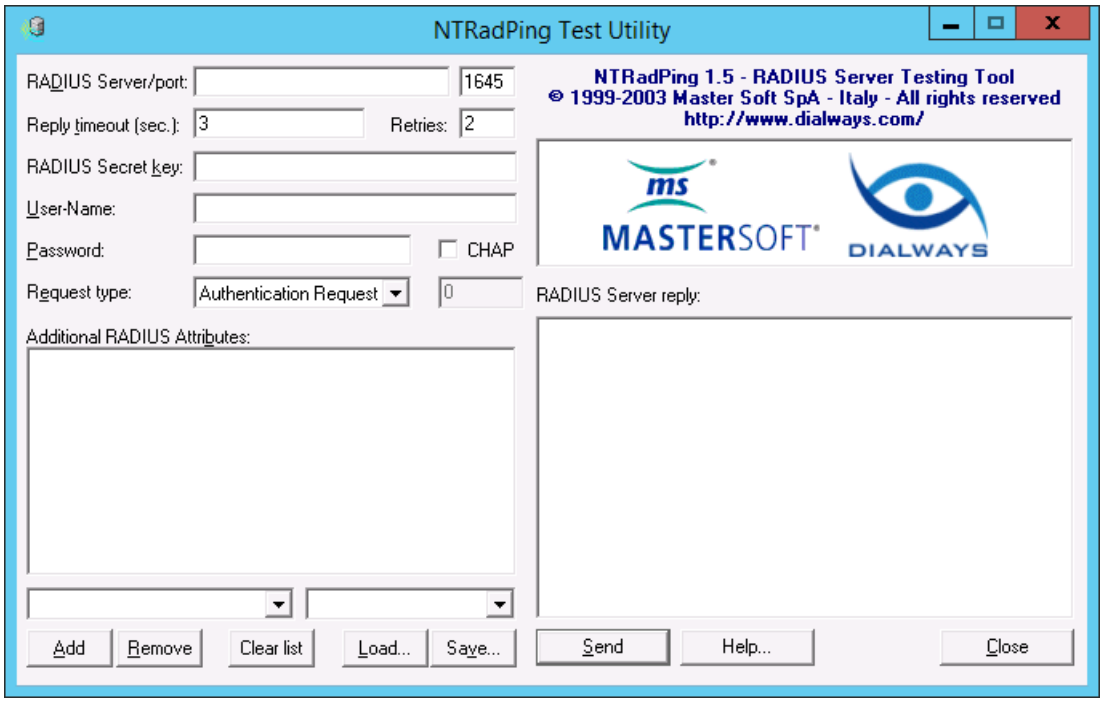


*Рис. 30 – Начальный вид окна утилиты **NTRadPing***

8. Выполните настройку соединения, руководствуясь табл. 14 (с. 51), 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).
9. Нажмите **Send**.

В окне программы отобразится информация следующего вида.

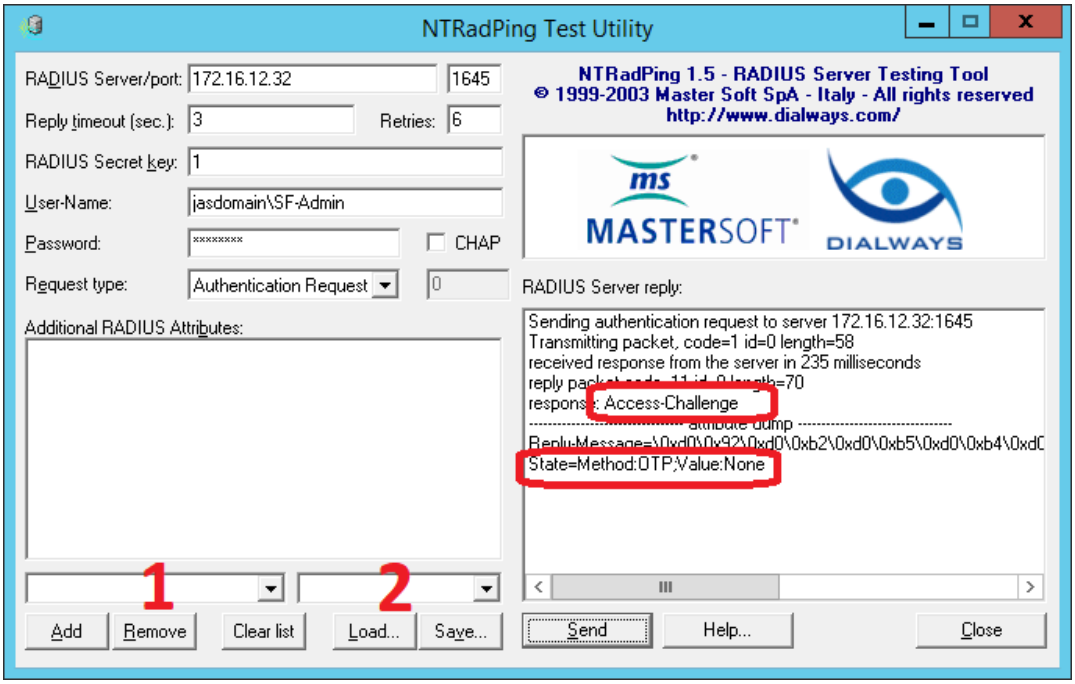


Рис. 31 – Ответ RADIUS-сервера

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

10. Для ввода второго фактора аутентификации (OTP) выполните следующие действия.

10.1. В поле настройки атрибута запроса (Рис. 31, поле, обозначенное цифрой «1») введите *State*.
10.2. В поле настройки значения атрибута запроса (Рис. 31, поле, обозначенное цифрой «2») введите значение из указанной выше подсказки (*Method:OTP;Value:None*)
10.3. Нажмите **Add**

В окне программы отобразится информация следующего вида.

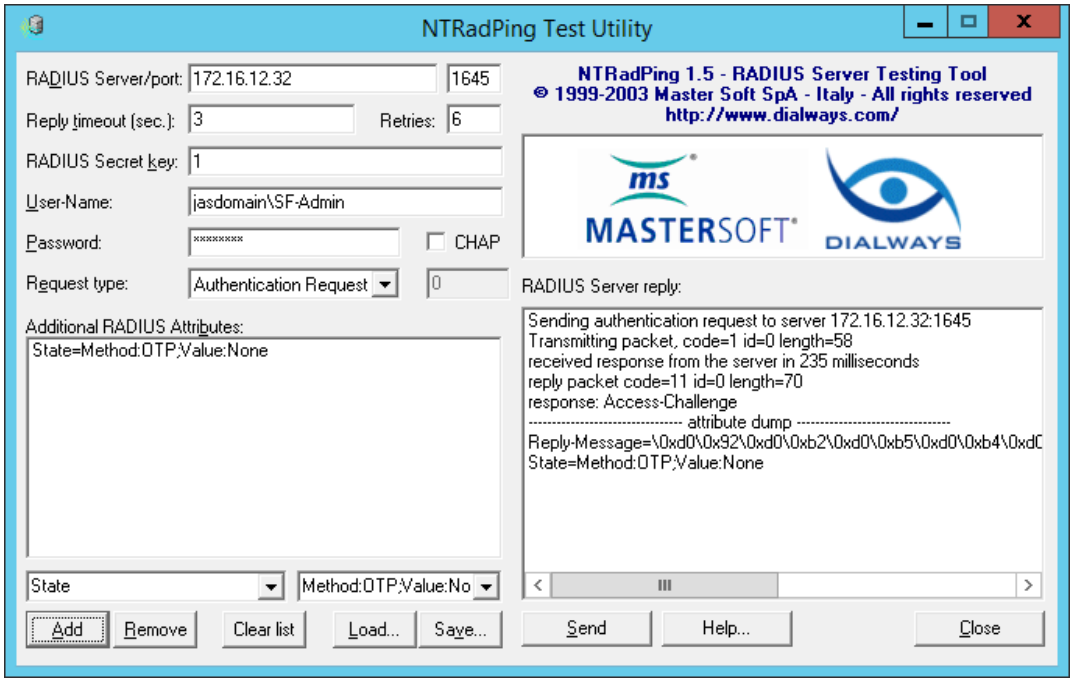


Рис. 32 – Отображение дополнительных атрибутов запроса к RADIUS-серверу (Additional RADIUS Attributes)

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

11. 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)

12. Нажмите **Send**.

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

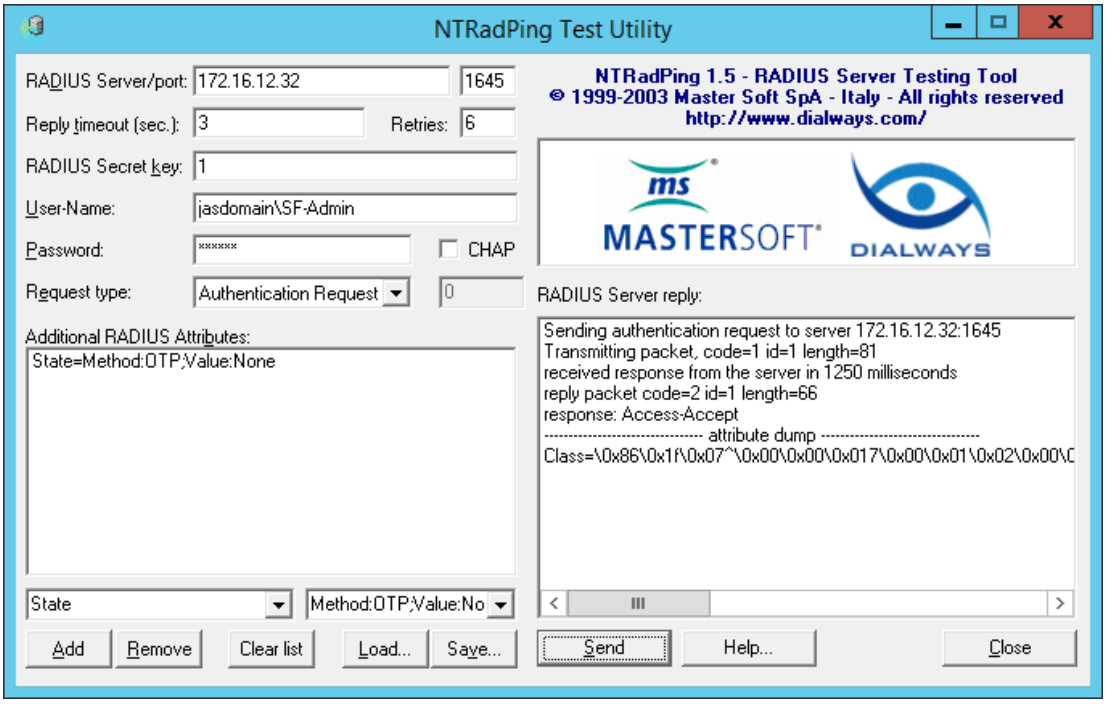


Рис. 33 – Ответ RADIUS-сервера

13. 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. раздел «Настройка сетевых программных интерфейсов сервера JAS», с. 21), настройки JAS-плагина для NPS (см. «Настройка JAS-плагина для NPS», с. 41) или проверьте корректность одноразового пароля в поле **Password**.

12.4.3 Двухшаговая процедура аутентификации с выбором типа второго фактора

Данная процедура проверки работы JAS-плагина 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. 13, с. 43).

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**.

14. Выполните настройку соединения, руководствуясь табл. 14 (с. 51), 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).
15. Нажмите **Send**.
    В окне программы отобразится информация следующего вида.

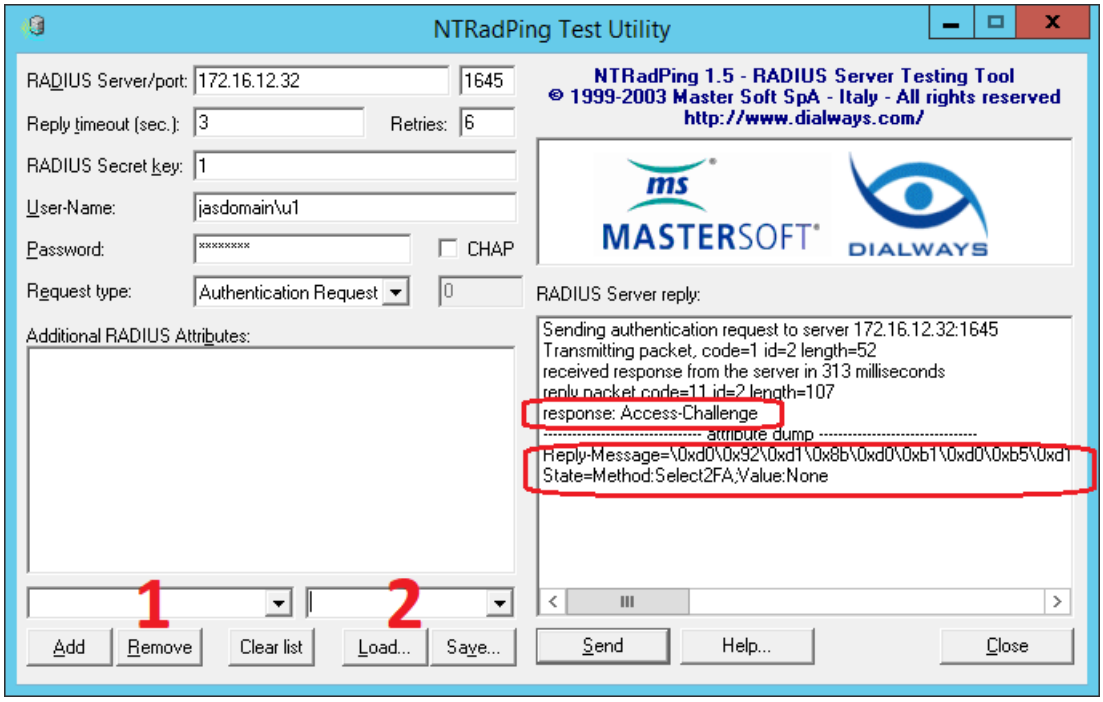


Рис. 34 – Ответ RADIUS-сервера

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

- для типа второго фактора аутентификации (Reply Message). В некоторых случаях (как в примере на Рис. 34), чтобы просмотреть числовые идентификаторы метода (например 1-OTP; 2-SMS) следует прокрутить содержимое поля **RADIUS Server reply** вправо (Рис. 35, 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. 13, с. 43).

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

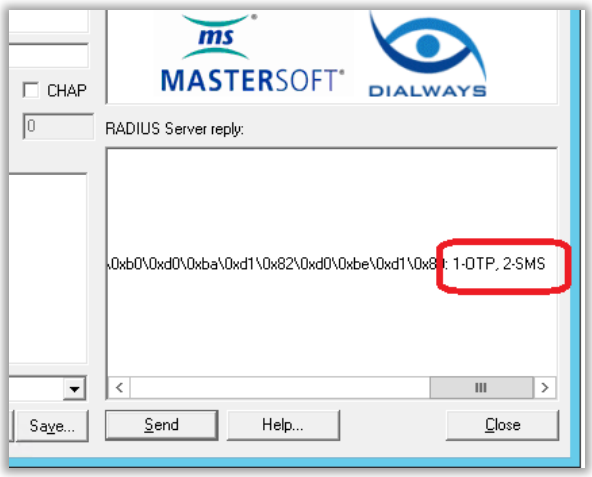


Рис. 35 – Прокрутка поля до конца, чтобы получить идентификатор метода

16. Для выбора типа второго фактора аутентификации (OTP, Messaging или Push) выполните следующие действия.

16.1. 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).

16.2. Нажмите **Send.**

В окне программы отобразится информация следующего вида.

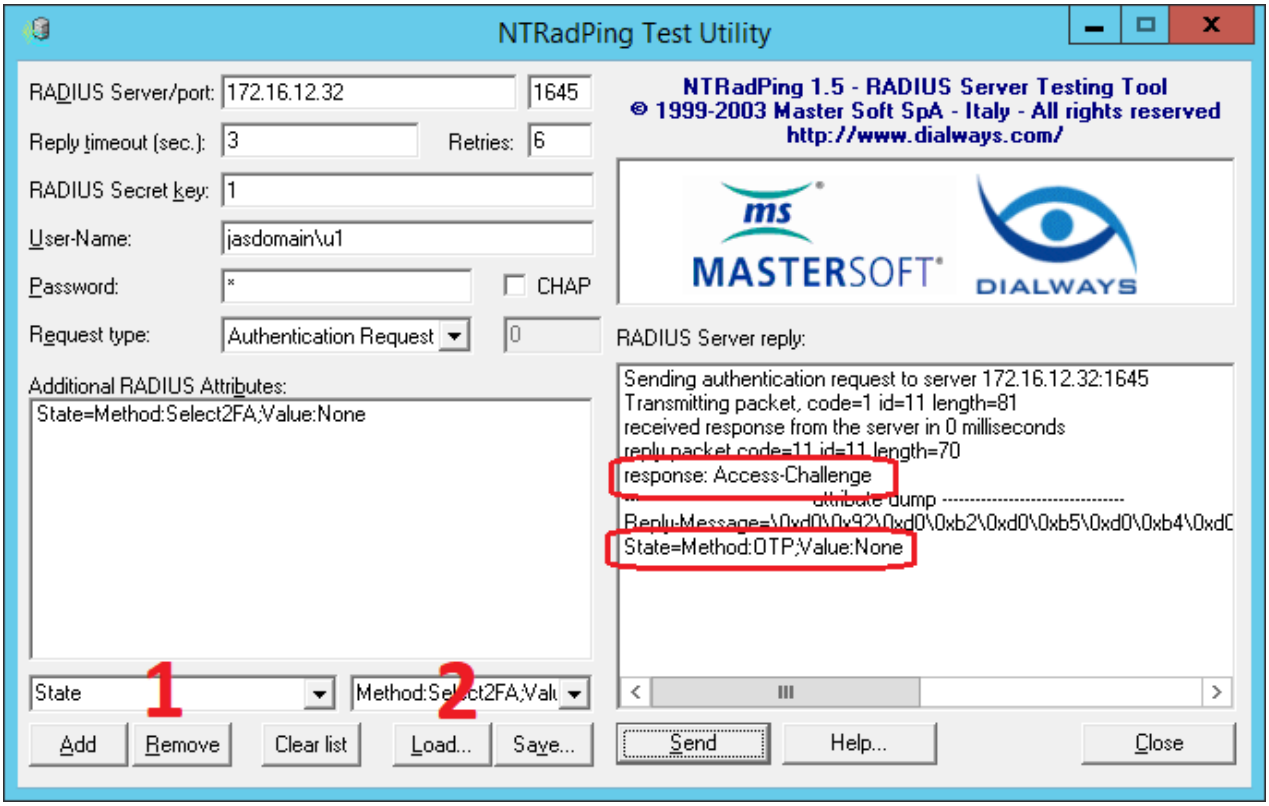


Рис. 36 – Ответ RADIUS-сервера

Примечание. В случае выбора идентификатора для метода Push указанное на Рис. 36 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 **atrribute dump** отобразится подсказка для имени метода для запроса второго фактора аутентификации (в данном случае *State=Method:OTP;Value:None*)

17. Для ввода второго фактора аутентификации (OTP) выполните следующие действия.

17.1. В поле настройки атрибута запроса (Рис. 36, поле, обозначенное цифрой «1») введите *State*.
17.2. В поле настройки значения атрибута запроса (Рис. 36, поле, обозначенное цифрой «2») введите значение из указанной выше подсказки (*Method:OTP;Value:None*)
17.3. Нажмите **Add**

В окне программы отобразится информация следующего вида.

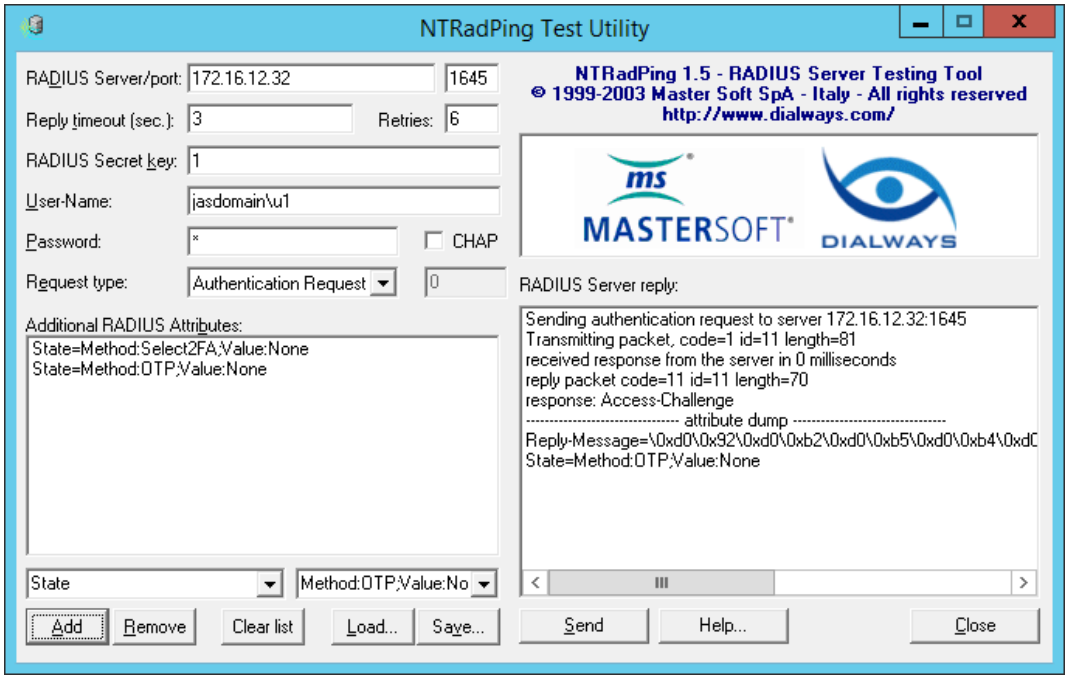


Рис. 37 – Отображение дополнительных атрибутов запроса к RADIUS-серверу (Additional RADIUS Attributes)

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

18. 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)

19. Нажмите **Send**.

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

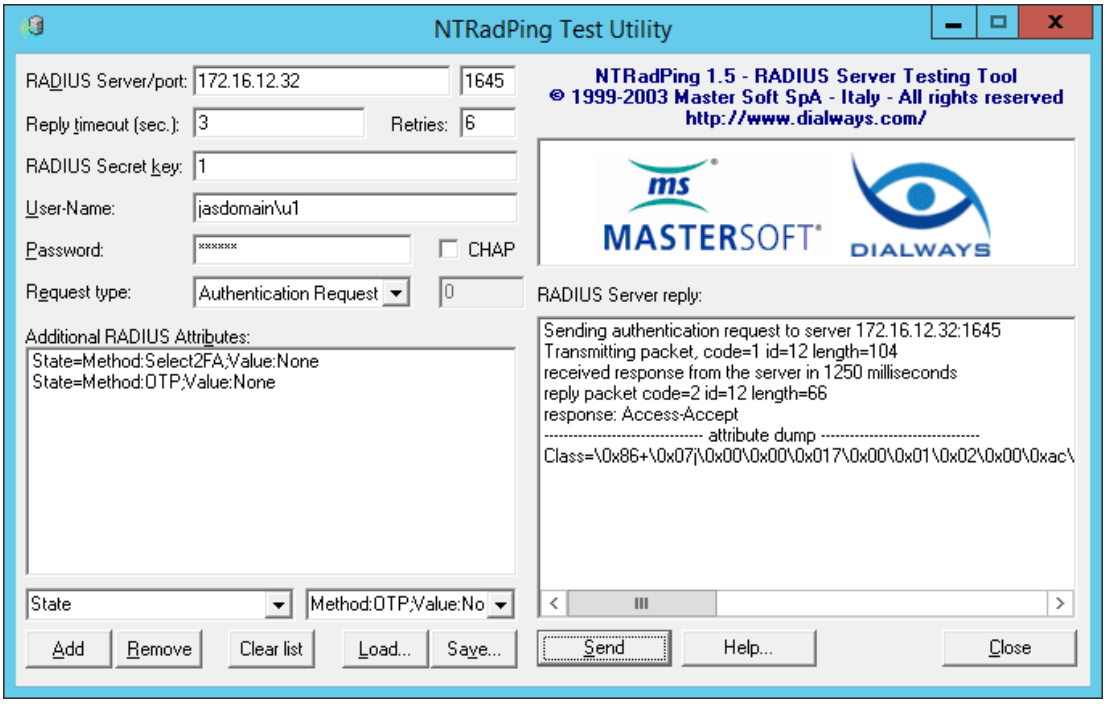


Рис. 38 – Ответ RADIUS-сервера

20. 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. раздел «Настройка сетевых программных интерфейсов сервера JAS», с. 21) настройки JAS-плагина для NPS (см. «Настройка JAS-плагина для NPS», с. 41) или проверьте корректность одноразового пароля в поле **Password**.

13. Установка и настройка JAS-плагина для AD FS

13.1 Подготовка к установке JAS-плагина для AD FS

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

13.2 Установка JAS-плагина для AD FS

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

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

Отобразится следующее окно.

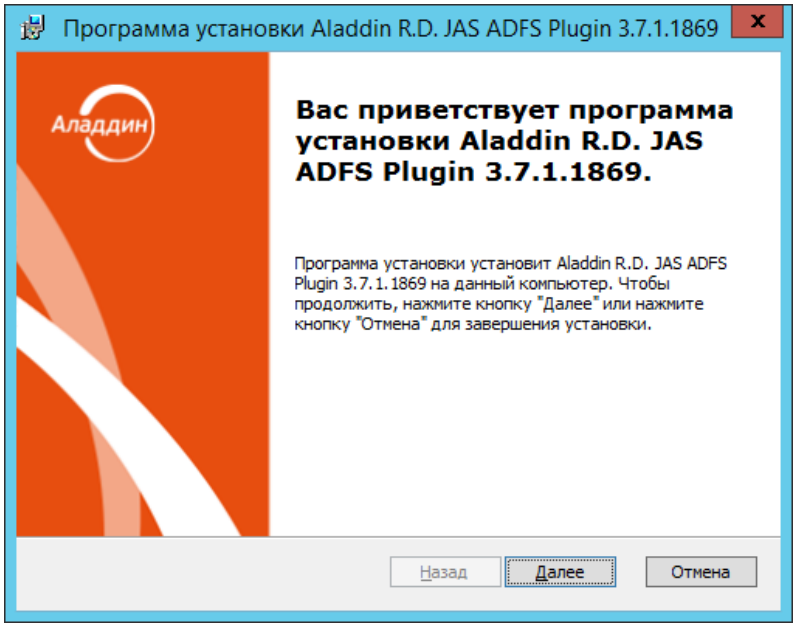


Рис. 39 – Окно приветствия мастера установки JAS-плагина для AD FS

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

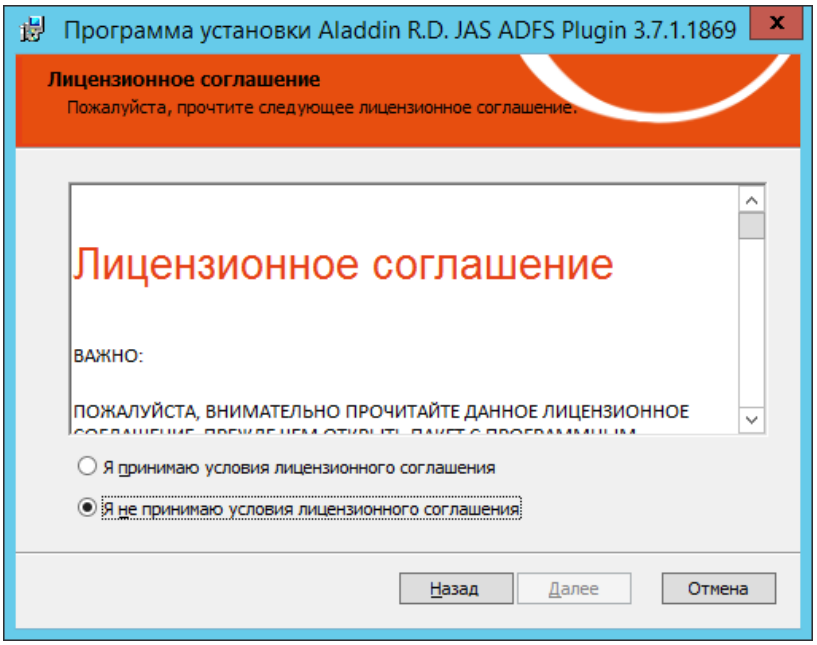


Рис. 40 – Окно лицензионного соглашения

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

Отобразится следующее окно.

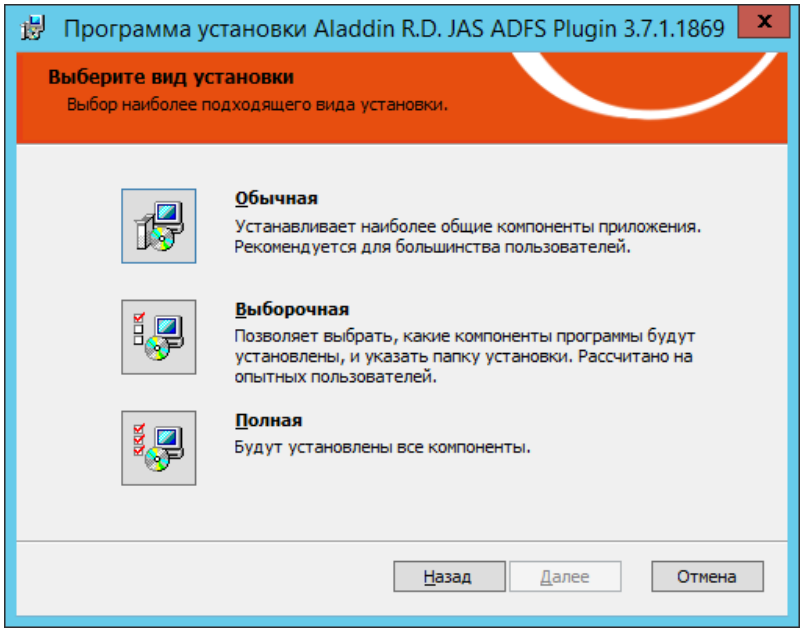


Рис. 41 - Окно выбора варианта установки

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

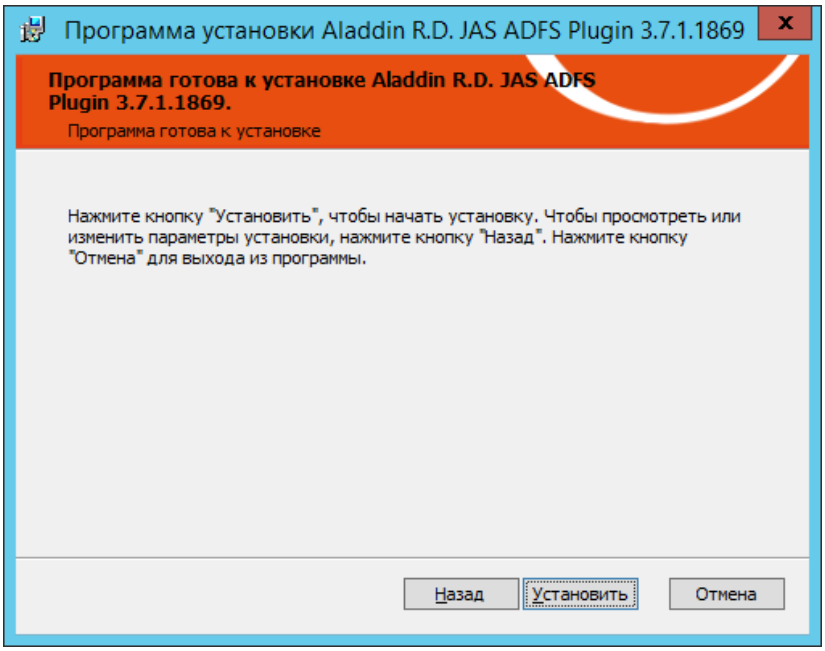


Рис. 42 – Подготовка к установке

5. Нажмите **Установить**.

По завершении установки отобразится следующее окно.

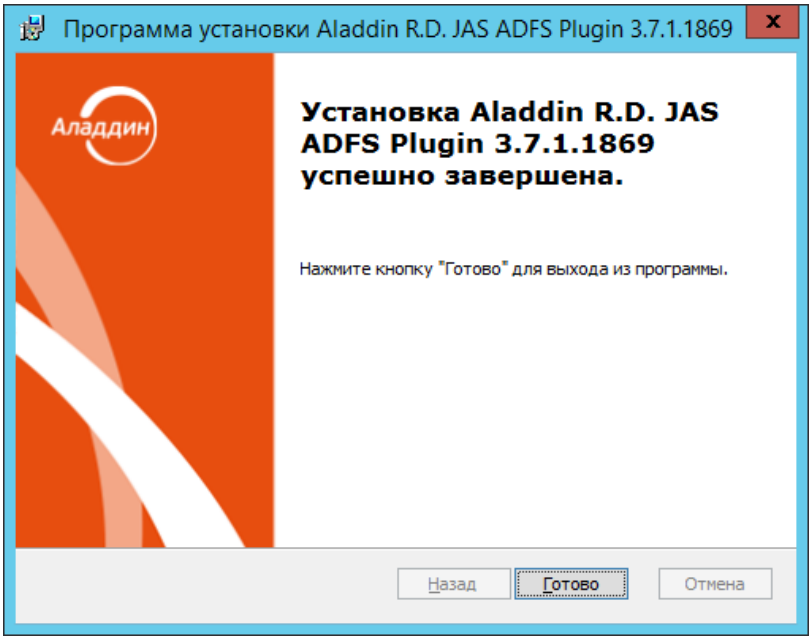


Рис. 43 – Окно завершения установки

6. Нажмите **Готово.**

JAS-плагин для ADFS установлен.

Сразу после установки плагина будет автоматически запущен так называемый «конфигуратор» **Настройка AFDS-плагина** (см. «Настройка JAS-плагина для AD FS», с. 65).

После установки JAS-плагин становится доступен для подключения в настройках службы AD FS (Рис. 45).

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. 44**)**.

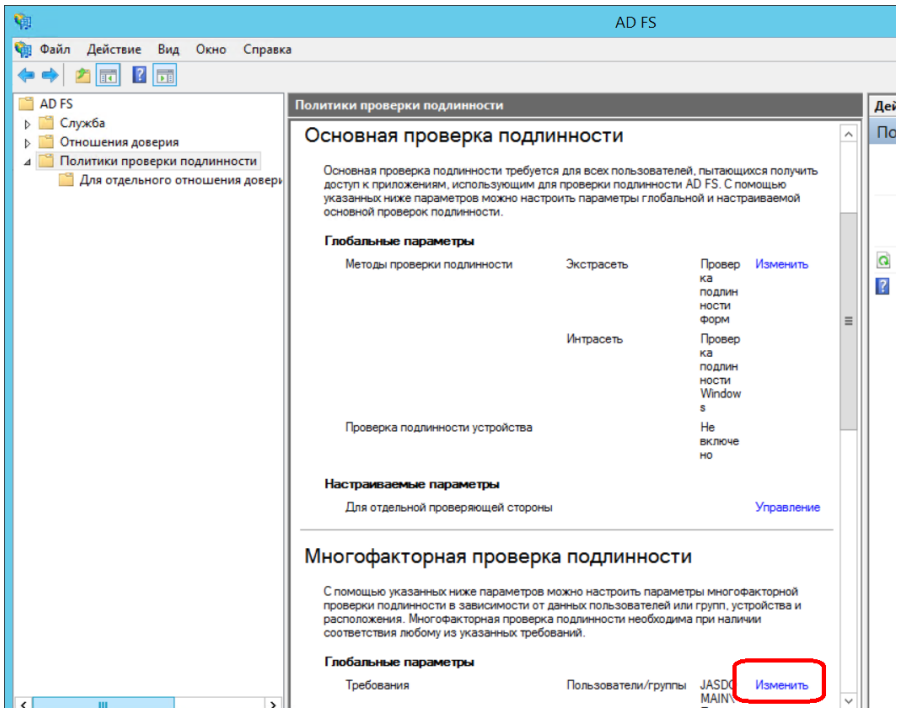


Рис. 44 – Вызов окна изменения параметров многофакторной аутентификации посредством AD FS

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

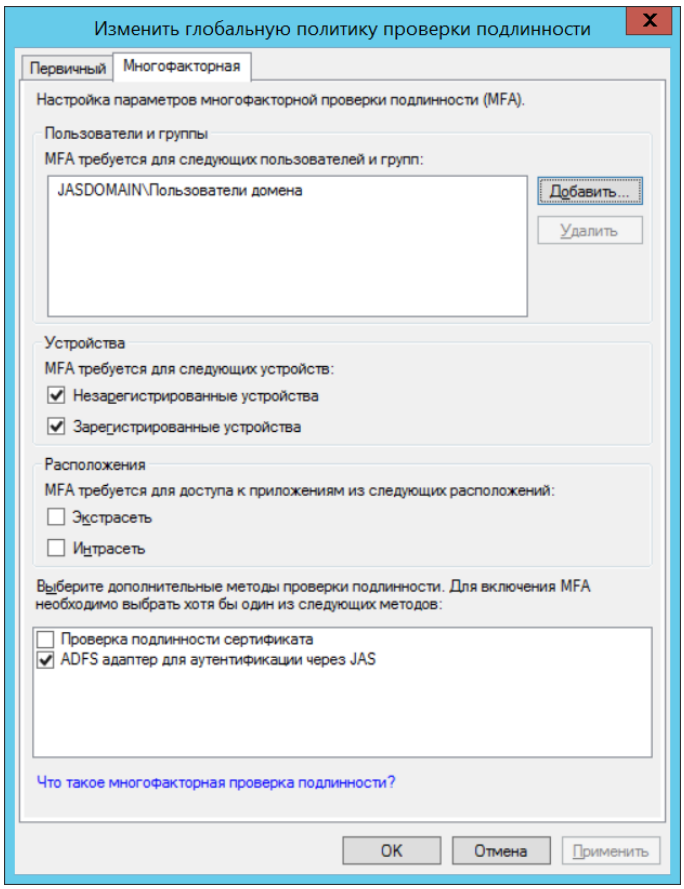


Рис. 45 – Проверка корректности установки JAS-плагина для AD FS

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.

13.3 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. 46, с. 66).

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

13.3.1 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.

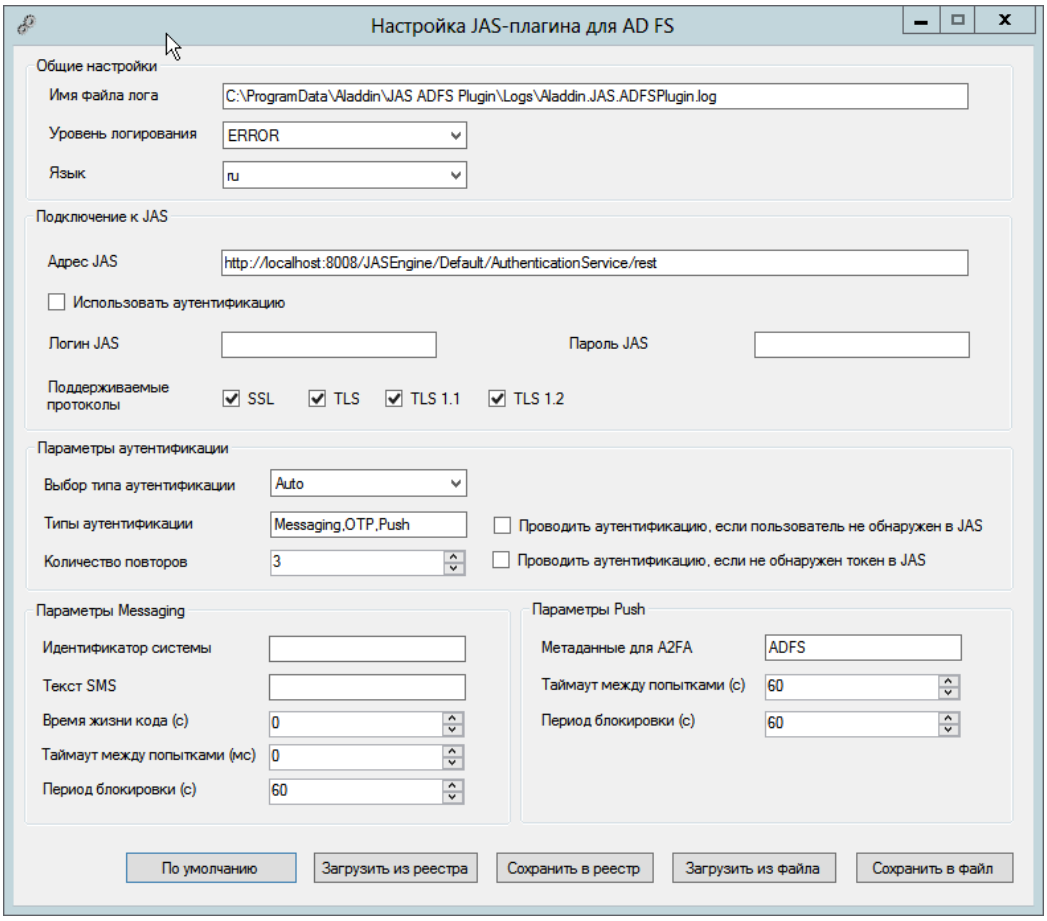


Рис. 46 – Окно Настройка JAS-плагина для AD FS

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. 47)

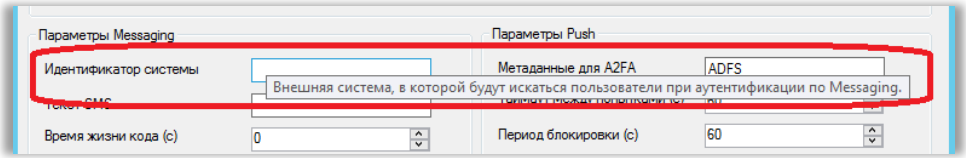


Рис. 47 – Использование всплывающей подсказки в полях формы

2. Выполните настройку, руководствуясь Табл. 15.

Табл. 15 - Настройка JAS-плагина для AD FS

Поле конфигуратора	Имя параметра в реестре	Описание
<Секция> **Общие настройки**		
Имя файла лога	**LogFilePath**	Путь, по которому будет сохраняться файл журнала
Уровень логирования	**LogLevel**	Уровень ведения журнала событий. • **OFF** –ведение журнала событий отключено; • **FATAL** – неустранимая ошибка; • **ERROR** – ошибка (значение по умолчанию); • **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**
Язык	**Culture**	Язык пользовательского интерфейса JAS-плагина для AD FS. Допустимые значения: • **en** (английский язык); • **ru** (русский язык). Значение по умолчанию: **ru** **Примечание.** Параметр определяет, на каком языке имя плагина в должно отражаться 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).
<Секция> **Подключение к JAS**		
Адрес JAS	**ServiceUri**	Адрес сервера JAS в следующем формате: **http://**<FQDN-имя сервера>**:8221/api/v4.1** где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com;
Использовать аутентификацию	**WithSecurity**	Флаг следует оставить неустановленным (в текущей версии данная настройка не используется).
Логин JAS	**JASUsername**	Не заполняется (в текущей версии данная настройка не используется)
Пароль JAS	**JASPassword**	Не заполняется (в текущей версии данная настройка не используется)

Поле конфигуратора	Имя параметра в реестре	Описание
Поддерживаемые протоколы	**SecurityProtocols**	Список поддерживаемых протоколов шифрования для обмена данных между сетевыми узлами. Представляются списком через запятую (например: `Ssl3, Tls, Tls11, Tls12`). Допустимые значения: • Ssl3; • Tls; • Tls11; • Tls12. По умолчанию указываются все допустимые типы протоколов
		<Секция> **Параметры аутентификации**
Выбор типа аутентификации	**AuthTypeSelection**	Режим выбора типа аутентификации, если их задано более одного (см. параметр **AuthTypes**, выше). Допустимые значения: **Auto** — автоматический; **Manual** — ручной 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**). Значение по умолчанию: **Auto**.
Типы аутентификации	**AuthTypes**	Поддерживаемые типы аутентификации и их приоритет. Текстовое поле. Подробнее логика использования параметра **AuthTypes** описана в Табл. 16, с. 73. Допустимые значения: **Messaging** – аутентификация в JAS осуществляется посредством Messaging-токенов; **OTP** – аутентификация в JAS осуществляется посредством OTP-токенов; **Push** – аутентификация в JAS осуществляется посредством Push-токенов. Допускается одновременное указание обоих типов (указываются через запятую); приоритет типа аутентификации устанавливается порядком его следования (у первого – выше). Значение по умолчанию: "**Messaging, OTP, Push**" **Примечание.** 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 конфигуратора	Имя параметра в реестре	Описание
Количество повторов	**RetriesCount**	Кол-во доступных пользователю *дополнительных* попыток аутентификации (т.е. ввода одноразового пароля) посредством OTP-токена. (Настройка не действует в отношении Messaging-токенов) Значение по умолчанию: **3** **Важно!** 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 путем конфигурирования сервера JAS, параметр **MaxAuthFailCount** (Максимальное количество неудачных попыток аутентификации) секции **OtpTokenConfigPreferenses** (подробнее смотри раздел «Приложение 3. Справочник конфигурационных файлов JAS», с. 115)
Проводить аутентификацию, если пользователь не обнаружен в JAS	**UserNotFoundAction**	Действия JAS-плагина, если пользователь, который пытается аутентифицироваться, не зарегистрирован в JAS. Подробнее логика обращения к параметру **UserNotFoundAction** описана в Табл. 16, с. 73. Допустимые значения: • **Accept** (флаг установлен) – автоматическая успешная аутентификация (решение об успешной аутентификации принимается вне сервера JAS); • **Reject** (флаг не установлен) – отклонять запрос. Значение по умолчанию: **Reject**
Проводить аутентификацию, если не обнаружен токен в JAS	**TokensNotFoundAction**	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. 16, с. 73. Допустимые значения: • **Accept** (флаг установлен) – автоматическая успешная аутентификация (решение об успешной аутентификации принимается вне сервера JAS); • **Reject** (флаг не установлен) – отклонять запрос. Значение по умолчанию: **Reject**
		<Секция> **Параметры messaging**
Идентификатор системы	**MessagingSystemId**	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 функциями управления JMS [3]. Значение по умолчанию: пустая строка
Текст SMS	**MessagingAdditionalInfo**	Текст, который будет отправляться в SMS пользователю вместе с одноразовым паролем. Значение по умолчанию: пустая строка

Поле конфигуратора	Имя параметра в реестре	Описание
Время жизни кода (с)	**MessagingTtl**	Время жизни для одноразового пароля (в секундах, напр. 180), в течение которого ответ пользователя будет актуальным. 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 функциями управления JMS [3]). Значение по умолчанию: пустая строка (не задано)
Таймаут между попытками (мс)	**MessagingRetryDelay**	Таймаут между попытками аутентификации посредством Messaging-токена (в миллисекундах), например 5000. 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. 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 функциями управления JMS [3]). Значение по умолчанию: пустая строка (не задано)
Период блокировки (с)	**MessagingNewSmsTimeout**	Задержка (в секундах) доступности кнопки для отправки нового одноразового пароля (OTP). Параметр имеет действие только в рамках пользовательского интерфейса (не передается на сервер JAS и не регулирует его работу). Если значение больше нуля – кнопка отправки нового OTP будет доступна по истечению указанного времени. Если значение равно нулю – кнопка будет доступна всегда. Если значение меньше нуля – кнопка никогда не будет показываться. **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. Значение по умолчанию: **60**
		<Секция> **Параметры Push**
Метаданные для A2FA	**PushMetadata**	Дополнительная информация (метаданные), которые будут отображаться на экране мобильного приложения Aladdin 2FA при отправке Push-запроса на аутентификацию. Строковый тип. Значение по умолчанию: **ADFS**

Поле конфигуратора	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 конфигураторе, 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 конфигуратора 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. 49.
Сохранить в файл		Отображаемые в форме параметры можно сохранить в reg-файл для последующего восстановления настроек
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 ADFS Plugin],** Рис. 48.

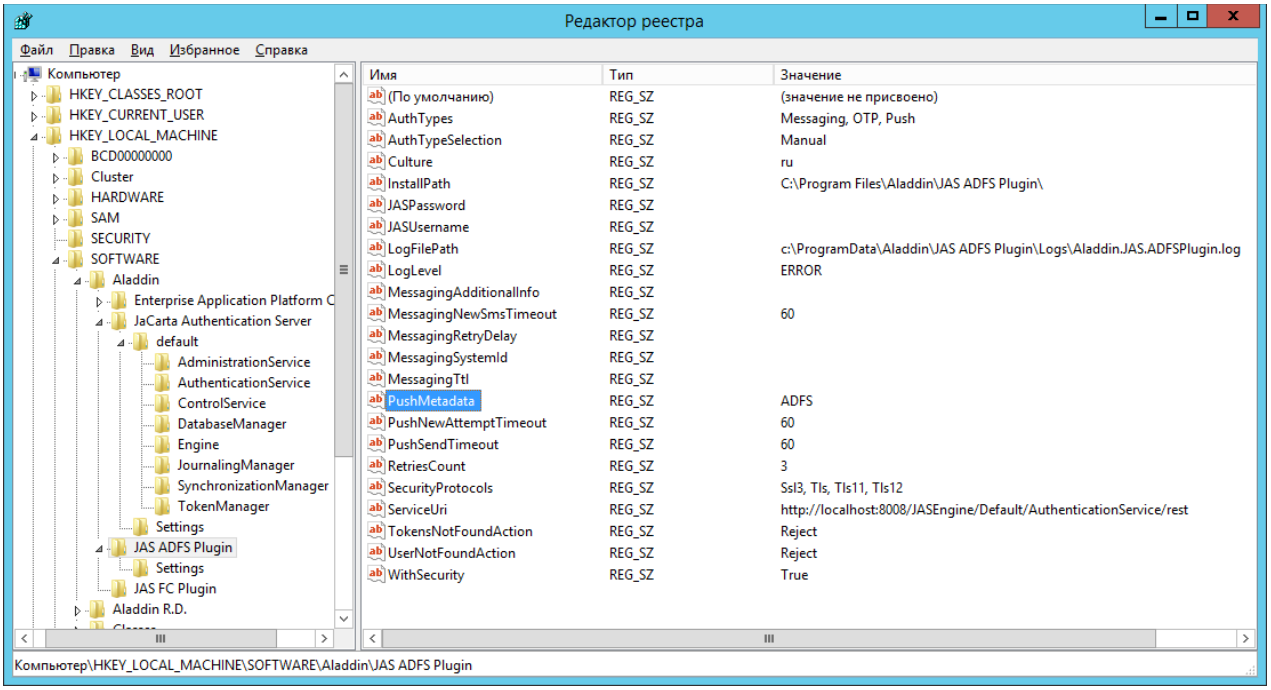


Рис. 48 – Настройки JAS-плагина для AD FS в реестре

3. 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]**
4. По нажатии 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. 49.

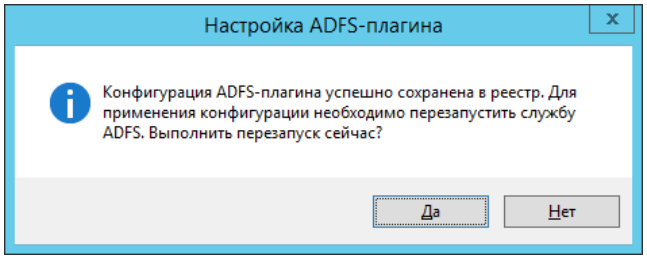


Рис. 49 – Настройки JAS-плагина для AD FS в реестре

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. 16 – 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)**			
OTP-токен	Messaging-токен	***AuthTypes:*** OTP, Messaging	***AuthTypes:*** Messaging, OTP	***AuthTypes:*** OTP	***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 OTP	Аутентификация по OTP	Аутентификация по OTP	UserNotFoundAction
Действует	Заблокирован	Аутентификация по OTP	Аутентификация по OTP	Аутентификация по OTP	TokensNotFoundAction
Действует	Действует	Аутентификация по OTP	Аутентификация по Messaging	Аутентификация по OTP	Аутентификация по Messaging

Примечания к Табл. 16:

1. Состояние *Заблокирован* подразумевает блокировку всех токенов соответствующего типа (например, OTP), а состояние *Действует* подразумевает наличие хотя бы одного незаблокированного токена соответствующего типа (например, OTP).
2. Информация, приведенная в Табл. 16 имеет иллюстративный характер для комбинации из двух значений параметра AuthTypes (а именно OTP 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. 16);
   - Если метод PUSH имеет наивысший приоритет но Push-токен у пользователя отсутствует, то право аутентификации переходит к следующему по приоритету методу (см. Табл. 16);
   - 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 отрабатывает опция TokensNotFoundAction;
     - Если PUSH-токен отсутствует, то отрабатывает опция UserNotFoundAction.

13.4 Проверка работы JAS-плагина для AD FS

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

1. Убедитесь в том, что JAS-плагин для AD FS 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 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/

Откроется веб-страница следующего вида:

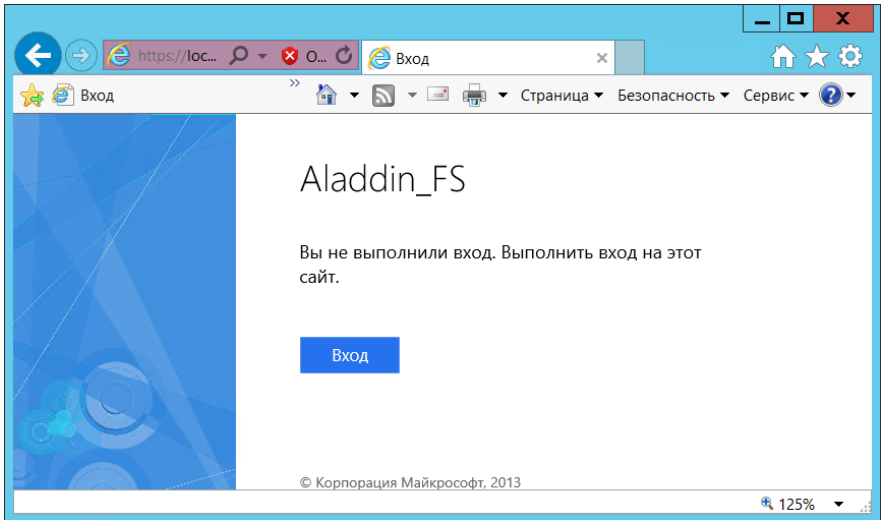


Рис. 50 – Стартовая проверочная страница службы федерации AD

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. 51).

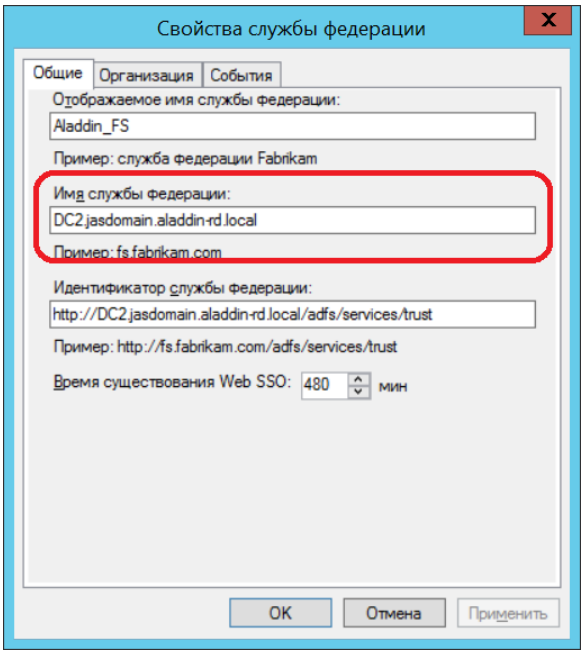


Рис. 51 – Просмотр имени Службы федерации Active Directory

5. Нажмите **Вход**. Отобразится страница, как на Рис. 52 (для случая настройки реестра *AuthTypeSelection=Auto*, см. Табл. 15, с. 67) или как на Рис. 53 (для случая настройки реестра *AuthTypeSelection=Manual*).

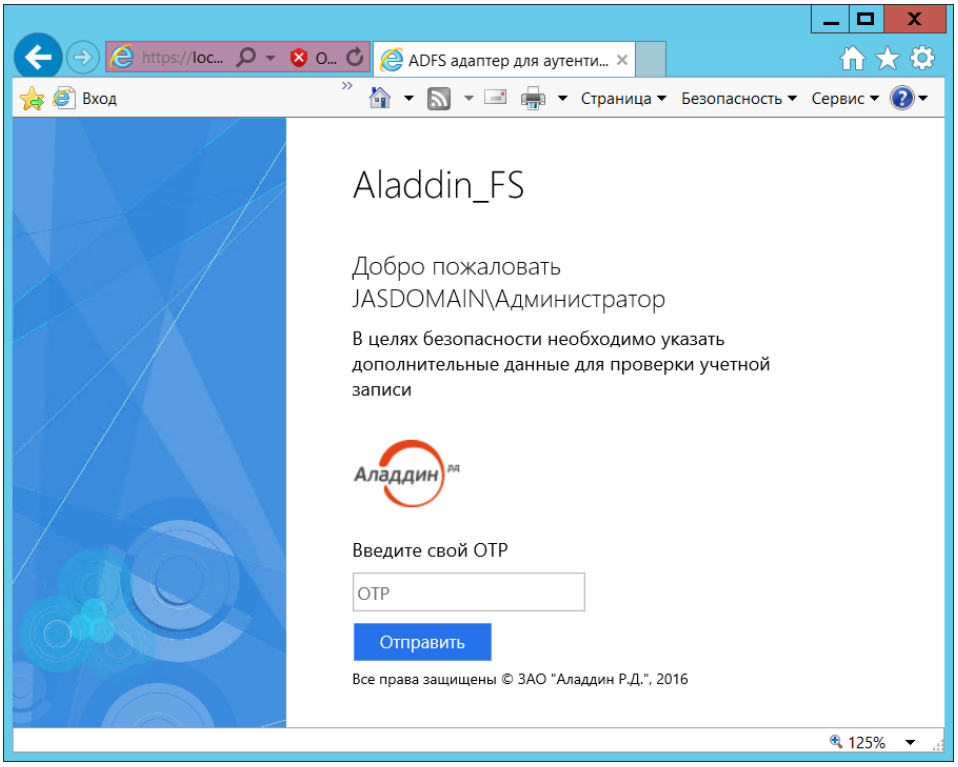


Рис. 52 – Веб-страница AD FS, использующей OTP-аутентификацию посредством JAS-плагина

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

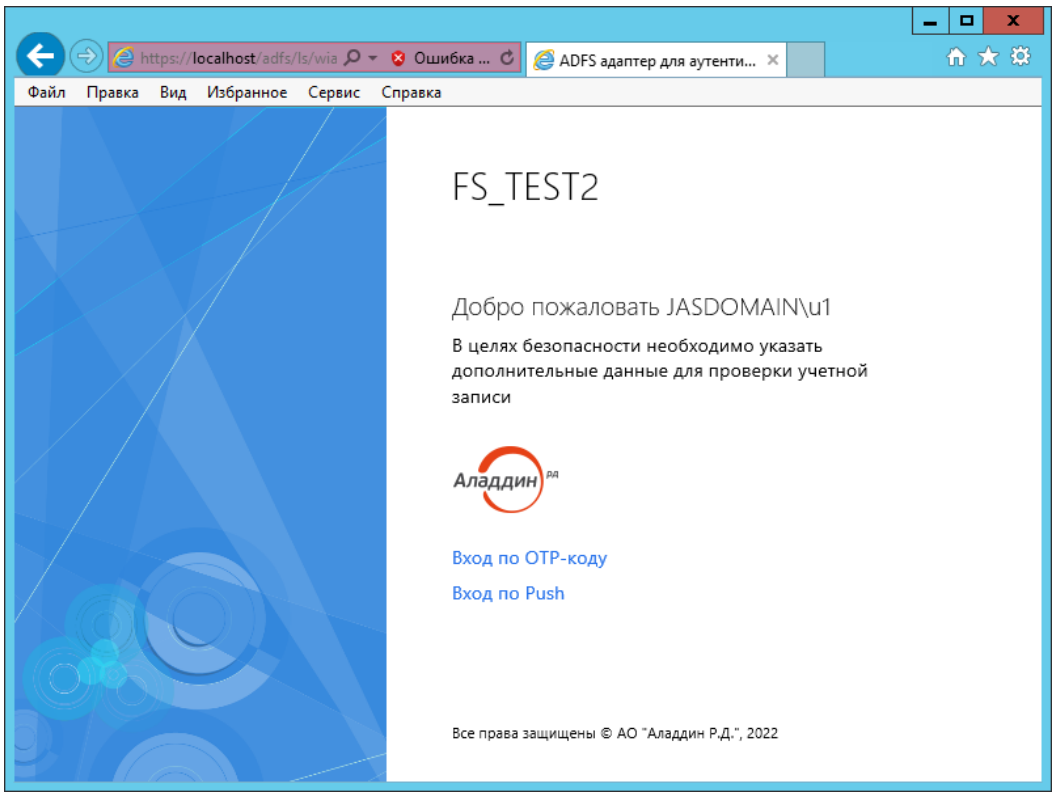


Рис. 53 – Веб-страница AD FS, с примером множественного ручного выбора типа аутентификации

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

14. 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).

14.1 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.

14.2 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.

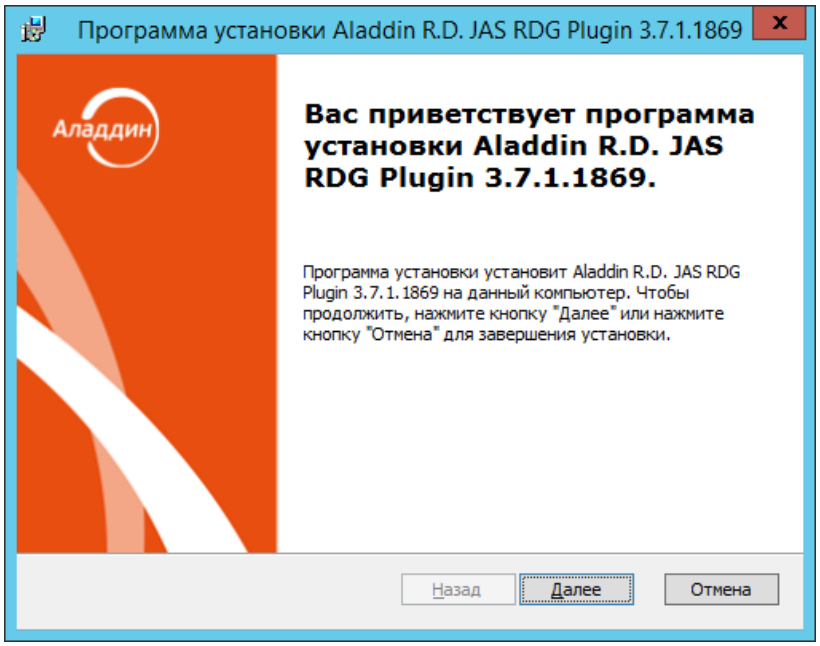


Рис. 54 – Окно приветствия мастера установки JAS-плагина для MS RDG

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.

4. По завершении установки отобразится следующее окно.

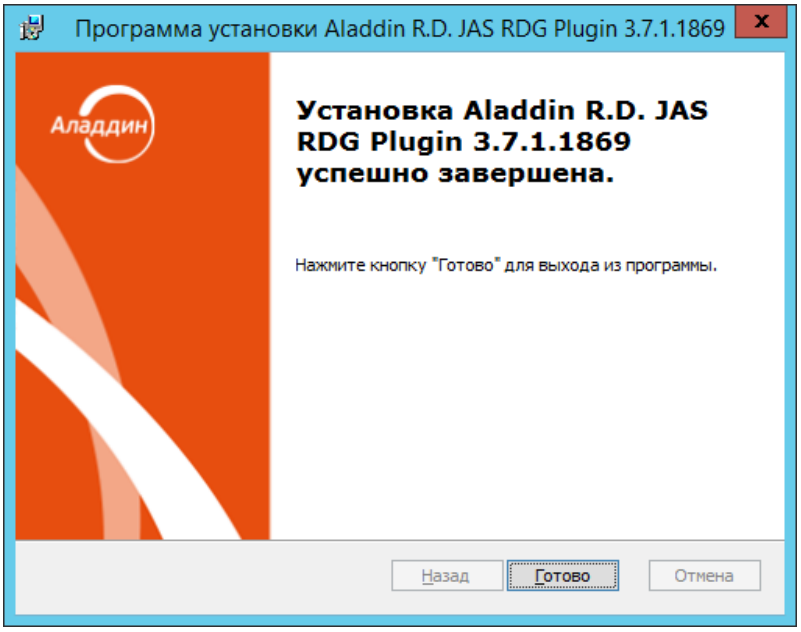


Рис. 55 – Окно завершения установки

5. Нажмите **Готово**.
   Отобразится следующее сообщение.

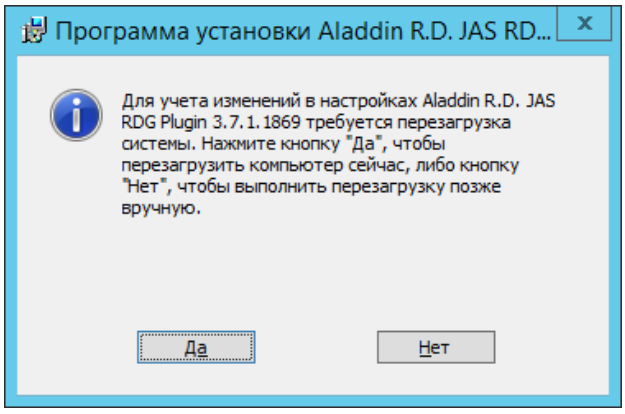


Рис. 56 – Предупреждение о необходимости перезагрузки

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

14.3 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. 57, с. 79).

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

14.3.1 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.

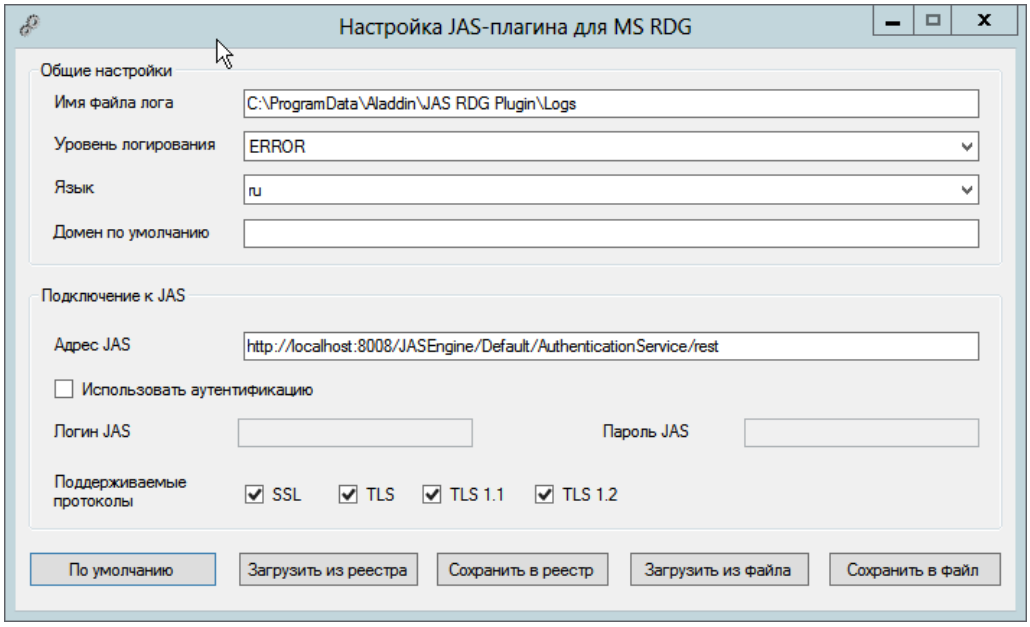


Рис. 57 – Окно Настройка JAS плагина для MS RDG

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. 58)

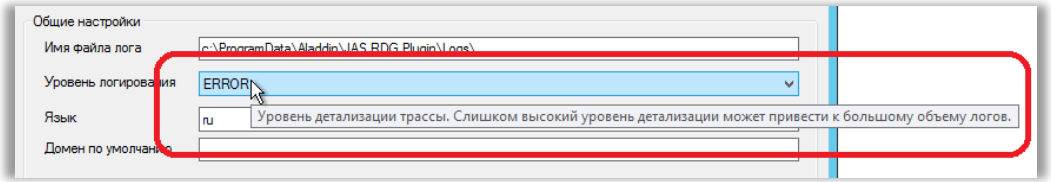


Рис. 58 – Использование всплывающей подсказки в полях формы

2. Выполните настройку, руководствуясь Табл. 17.

Табл. 17 - 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 конфигуратора	Имя параметра в реестре	Описание
Уровень логирования	**LogLevel**	Уровень ведения журнала событий. • **OFF** –ведение журнала событий отключено; • **FATAL** – неустранимая ошибка; • **ERROR** – ошибка (значение по умолчанию); • **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**
Язык	**Culture**	Язык пользовательского интерфейса JAS-плагина. Допустимые значения: • **en** (английский язык); • **ru** (русский язык). Значение по умолчанию: **ru** **Примечание.** В текущей версии параметр не используется. Во всех интерфейсах JAS-плагина для MS RDG используется только русский язык.
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>**:8221/api/v4.1** где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com;
Использовать аутентификацию	<без параметра в реестре>	Флаг следует оставить неустановленным (в текущей версии данная настройка не используется).
Логин JAS	**JASUsername**	Не заполняется (в текущей версии данная настройка не используется)
Пароль JAS	**JASPassword**	Не заполняется (в текущей версии данная настройка не используется)

Поле конфигуратора	Имя параметра в реестре	Описание
Поддерживаемые протоколы	**SecurityProtocols**	Список поддерживаемых протоколов шифрования для обмена данных между сетевыми узлами. Представляются списком через запятую (например: `Ssl3, Tls, Tls11, Tls12`). Допустимые значения: • 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 конфигуратора 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. 60.
Сохранить в файл		Отображаемые в форме параметры можно сохранить в reg-файл для последующего восстановления настроек
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 RDG Plugin],** Рис. 59.

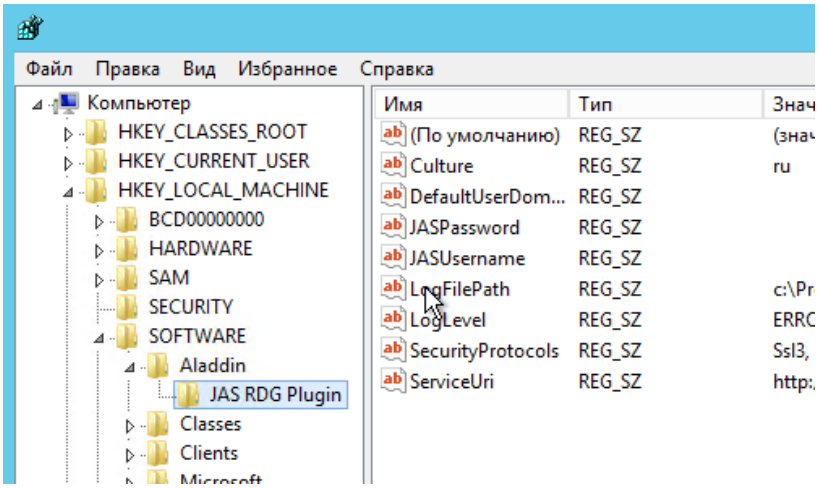


Рис. 59 – Настройки JAS-плагина для MS RDG

3. 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. 60.

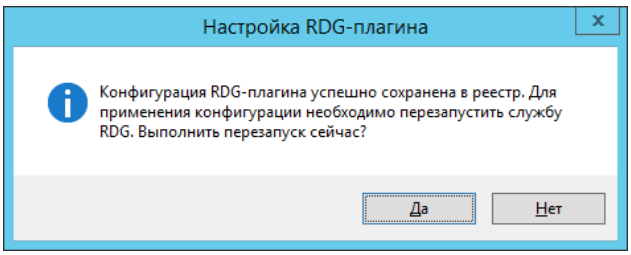


Рис. 60 – Диалог перезапуска службы MS RDG

4. 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]**
5. После внесения изменений в реестр перезагрузите компьютер.
6. 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).

7. 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 web-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.

14.4 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:

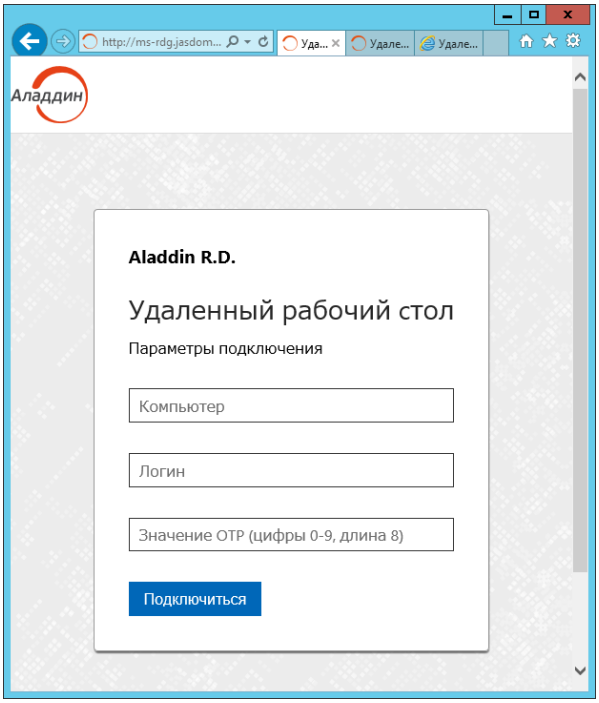


Рис. 61 – Web-страницу плагина для аутентификации на шлюзе RDG

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. 78) 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. 62):

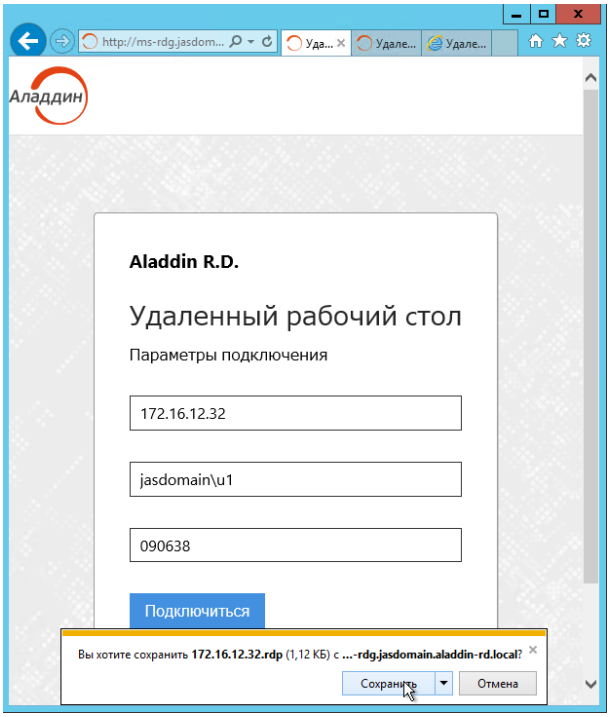


Рис. 62 – Сохранение rdp-фала на диск

7. Запустите сохраненный rdp-файл на выполнение (Рис. 63):

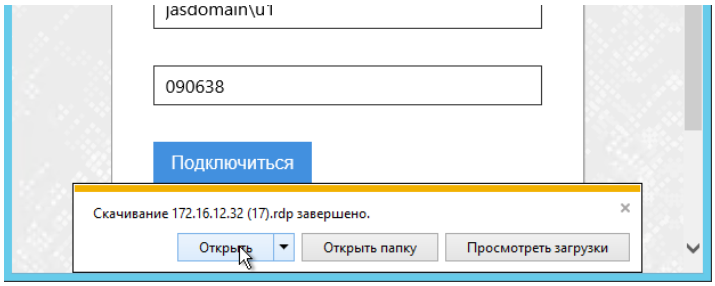


Рис. 63 – Запуск rdp-фала на выполнение

8. Дождитесь запуска процедуры подключения к удаленному рабочему столу (Рис. 64):

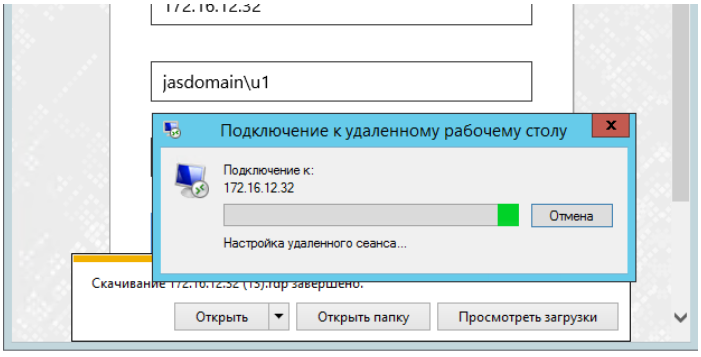


Рис. 64 – Подключение к удаленному рабочему столу

9. Введите пароль в окне подключения к удаленному рабочему столу (Рис. 65):

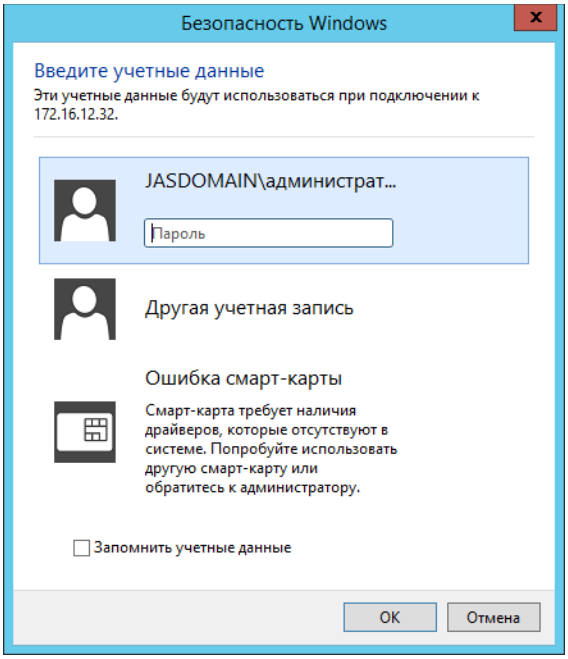


Рис. 65 – Окно ввода пароля для подключения к удаленному рабочему столу

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

14.4.1 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. 61, с. 83) web-браузер отображается ошибка следующего вида.

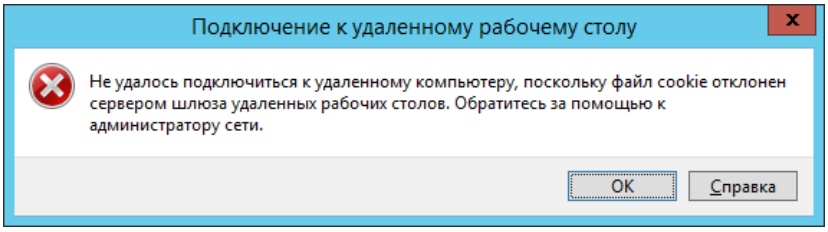


Рис. 66 – Типовое окно ошибки при вводе неверного OTP-пароля

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

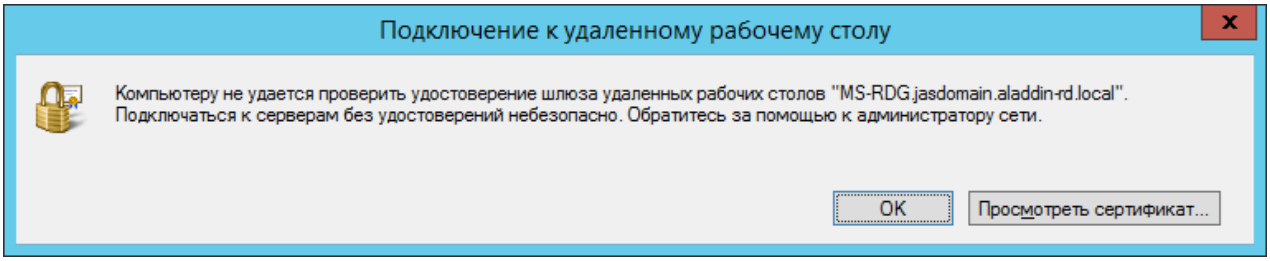


Рис. 67 – Типовое сообщение при ошибке настройки взаимодействия с Шлюзом удаленных рабочих столов

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.

15. 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. 68).

Рис. 68 – Запрос учетных данных для двухфакторной аутентификации JAS OTP Logon

15.1 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.

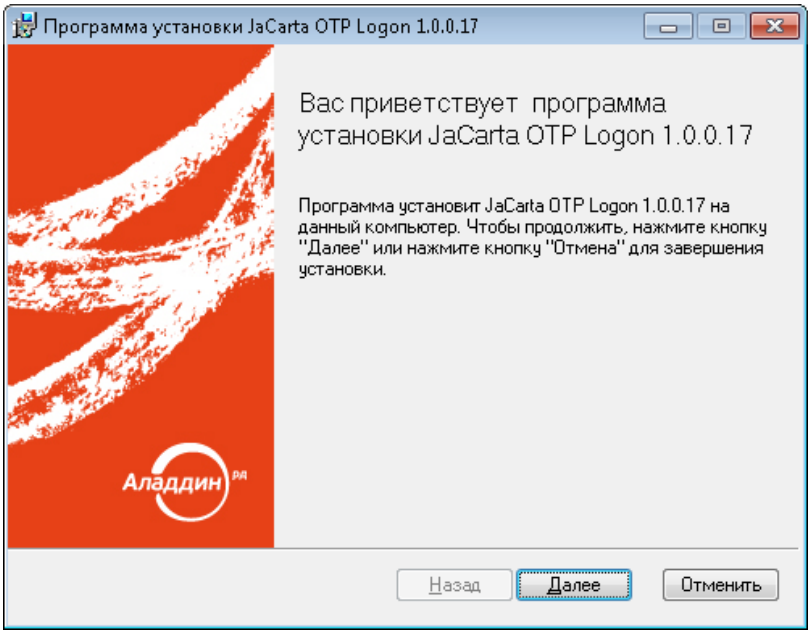


Рис. 69 – Экран приветствия мастера установки JaCarta OTP Logon

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. раздел «Настройка сетевых программных интерфейсов сервера JAS», 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.»

15.2 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. 18, с. 89; требуется настройка централизованного хранилища групповых политик, см. раздел «Групповая политика JOL», с. 92);
- настройки JOL из локальной групповой политики (см. раздел «Локальная групповая политика JOL», с. 93).
- настройки JOL в реестре (см. Табл. 18; могут быть переопределены вручную);
- настройки по умолчанию (прошиты в исходном коде продукта).

Приоритет в определении конфигурации JOL имеют настройки доменной групповой политики, GPO (Рис. 70, 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. 18, с. 89). 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. 18).

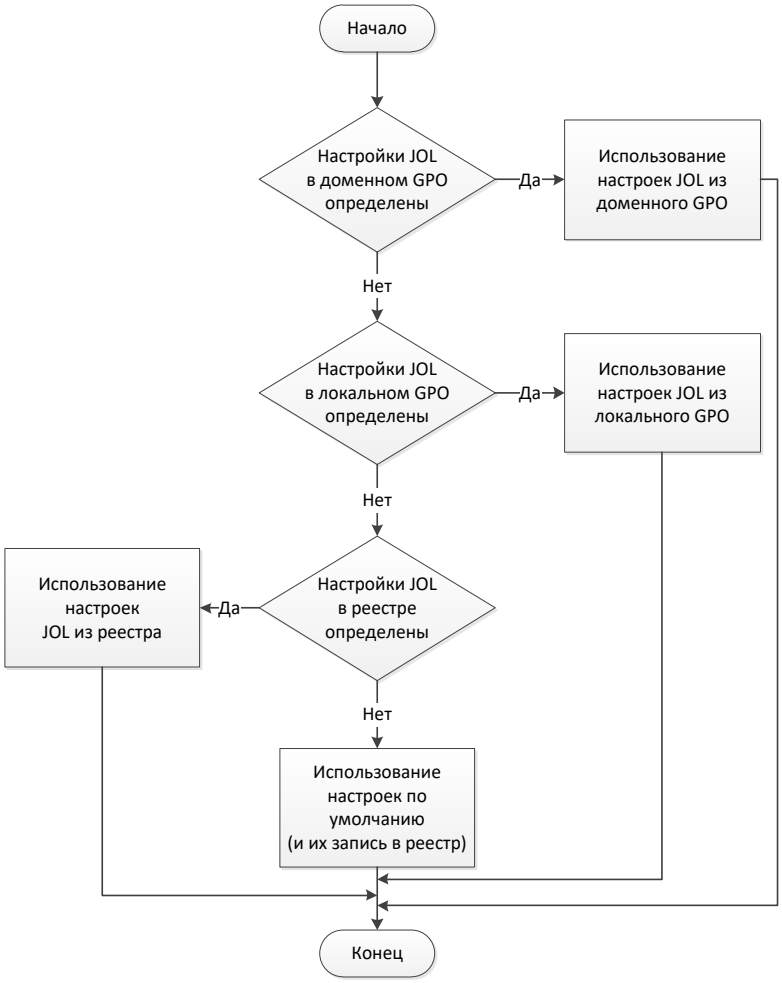


Рис. 70 – Порядок применения настроек JOL

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. 18, 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. 18 – Параметры конфигурации JOL

Название пункта настройки JOL в GPO	Параметр настройки JOL в реестре	Описание
Настройки фильтрации поставщиков учетных данных	**LogonProvidersFilter**	Параметр, определяющий доступные пользователю поставщики учетных данных (Credential Provider) при входе в Windows. Доступные значения: • **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. Значение по умолчанию: **0** (Пользователю доступны все поставщики учетных данных, включая JOL)
Отображать поставщики учетных данных по списку их GUID	**LogonProvidersList**	Список GUID-идентификаторов поставщиков учетных данных, доступных пользователю для входа в Windows. Указываются через запятую. (Параметр активен только при значении LogonProvidersFilter=3); GUIDы следует перечислить в формате: {XXXX-XXXXX-XXXXX-XXXXX}, {YYYY-YYYYY-YYYYY-YYYYY} Значения по умолчанию не предусмотрено.
Адрес сервиса аутентификации JAS	**ServiceUri**	Адрес сервера JAS в следующем формате: **http://**<FQDN-имя сервера>**:8221/api/v4.1** где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com;
Действия JOL при использовании заблокированных OTP-токенов	**TokensNotFoundAction**	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: • **Pass** (Пропускать запрос) • **Reject** (Отклонять запрос) Значение по умолчанию: **Reject**
Действия JOL по запросу от незарегистрированных пользователей	**UserNotFoundAction**	Действия JOL, если пользователь, который пытается аутентифицироваться, не зарегистрирован в JAS. Доступные значения: • **Pass** (Пропускать запрос) • **Reject** (Отклонять запрос) Значение по умолчанию: **Reject**

Название пункта настройки JOL в GPO	Параметр настройки JOL в реестре	Описание
Автоматически добавлять Windows-пароль пользователя в поле OTP-пароль	**ConcatenatePassword**	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: • **Enable** (Включить) • **Disable** (Отключить) Значение по умолчанию: **Disable**
Добавлять имя внедоменной рабочей станции	**AddWsPrefix**	Включить/отключить автоматическое добавление к имени пользователя имени внедоменной рабочей станции (например WKS234\user). Доступные значения: • **Enable** (Включить) • **Disable** (Отключить) Значение по умолчанию: **Disable** **Важно!** В текущей версии JMS параметр может иметь только значение **Disable** (использование JOL для аутентификации на внедоменных станциях недоступно)
Язык интерфейса JAS OTP Logon	**Culture**	Управление языком пользовательского интерфейса. Доступные значения: • **RU** (Русский) • **EN** (Английский) Значение по умолчанию: **RU**
Путь к файлам журнала (лог-файлам)	**LogFilePath**	Путь, по которому буден сохраняться файл журнала. Значение по умолчанию: **C:\ProgramData\AladdinRD\JAS OTP Logon\Logs**
Уровень детализации ведения журнала	**LogLevel**	Уровень ведения журнала событий (логов). • **OFF** – ведение журнала событий отключено; • **FATAL** – отображать неустранимые ошибки; • **ERROR** – ошибки; • **WARN** – предупреждения; • **INFO** – информация; • **DEBUG** – отладка; • **ALL** – показывать все события. Каждый последующий уровень включает все предыдущие (кроме OFF), например, если выставлено значение INFO, то будут записываться сообщения уровней: INFO, WARN, ERROR, FATAL Значение по умолчанию: **ERROR**

Название пункта настройки JOL в GPO	Параметр настройки JOL в реестре	Описание
Настройка проверки действительности сертификата сервера	**SSLVerifyPeer**	Включение/отключение проверки на клиентском компьютере действительности сертификата сервера при настроенном SSL-соединении. Доступные значения: • **0** (Отключить) • **1** (Включить) Значение по умолчанию: **1**
Настройка проверки CN сертификата сервера	**SSLVerifyHost**	Включение/отключение проверки на клиентском компьютере имени субъекта (CN) сертификата (сервера) с именем, указанным в параметре **ServiceUri** (выше, в таблице). Доступные значения: • **0** (Отключить) • **2** (Включить) Значение по умолчанию: **2**
Использовать JOL для локальной сессии	**UseJolInLocalSessions**	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). В случае если настройка выключена (значение **0**), 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. Настройка не распространяется на RDP-подключения. Доступные значения: • **0** (Отключить) • **1** (Включить) Значение по умолчанию: **1**
Использовать JOL для удаленной сессии	**UseJolInRemoteSessions**	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. В случае если настройка выключена (значение **0**), значение параметра **LogonProvidersFilter**=2 («входить только через JOL», см. выше) игнорируется, и вход по RDP будет осуществлен через стандартный поставщик учётных данных. Настройка не распространяется при подключении к локальному компьютеру. Доступные значения: • **0** (Отключить) • **1** (Включить) Значение по умолчанию: **1**

Название пункта настройки JOL в GPO	Параметр настройки JOL в реестре	Описание
<Параметр отсутствует в GPO, настройка доступна только локально в реестре компьютера с JOL>	**SSLVersionTLS**	Параметр устанавливает максимальную версию TLS для работы компонента JOL. Допустимые значения: • **0** - Использовать TLS версии 1.0; • **1** - Использовать TLS версии 1.1; • **2** - Использовать TLS версии 1.2; • **3** - Использовать TLS версии 1.3 Значение по умолчанию: **2**

15.3 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. 137).

2. Настройте групповую политику на *контроллере домена* с помощью **Редактора управления групповыми политиками** (Рис. 71) руководствуясь Табл. 18, с. 89, или интерактивными подсказками редактора политик**.**

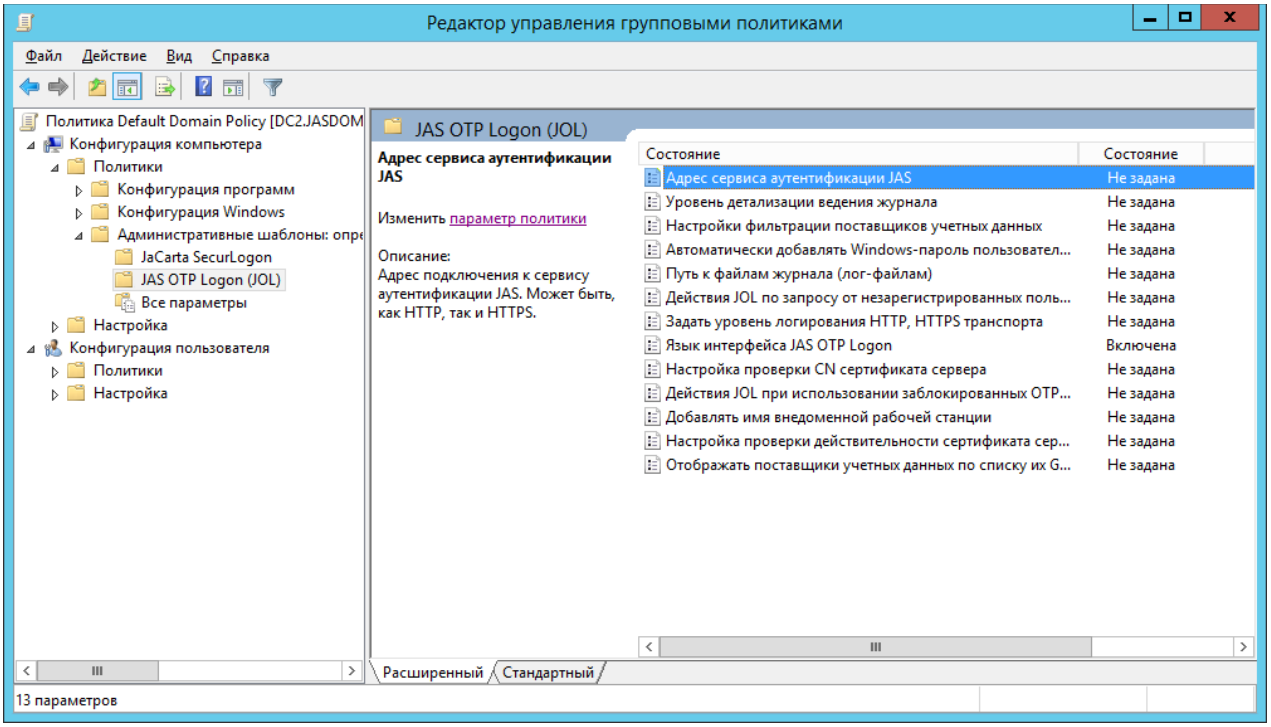


*Рис. 71 – Настройка групповой политики **JAS OTP Logon (JOL)***

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.).

15.4 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 стации.

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. 18, с. 89).

15.5 Порядок аутентификации в Windows с помощью JOL

Для аутентификации в Windows с помощью JOL выполните следующие действия.

1. На экране входа в систему (Рис. 72) 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. 72 – Стандартный экран входа в систему (ОС Windows)

4. Среди отображенных поставщиков учетных данных (Рис. 73) выберите **Разблокировка по OTP**.

Рис. 73 – Выбор JOL как поставщика учетных данных

5. На экране входа по OTP (Рис. 74) 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. 74 – 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:

  - «OTP» (см. описание параметра **Режим аутентификации** в профилях выпуска OTP-токенов в руководстве по функциям управления JMS [3]);
  - «Доменный пароль + OTP», но при этом в групповой политике включена настройка «**Автоматически добавлять Windows-пароль пользователя в поле OTP-пароль**» (см. Табл. 18, с. 89, значение `Enable`; настройка через реестр описана там же);
- PIN-код OTP и пароль OTP (без пробела), если для данного токена режим аутентификации имеет значение:
  - «OTP PIN-код + OTP» (см. описание параметра **Режим аутентификации** в профилях выпуска OTP-токенов в руководстве по функциям управления JMS [3]);
  - «Доменный пароль + OTP PIN-код + OTP», но при этом в групповой политике включена настройка «**Автоматически добавлять Windows-пароль пользователя в поле OTP-пароль**» (см. Табл. 18, с. 89, значение `Enable`; настройка через реестр описана там же);
- все необходимые значения, в соответствии с режимом аутентификации («OTP», «OTP PIN-код + OTP», «Доменный пароль + OTP»или «Доменный пароль + OTP PIN-код + OTP»; для трех последних – параметры вводятся без пробела), если в групповой политике выключена настройка «**Автоматически добавлять Windows-пароль пользователя в поле OTP-пароль**» (см. Табл. 18, с. 89, значение `Disable`; настройка через реестр описана там же).

6. Для аутентификации нажмите *ввод*.

16. 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 TLS 1.0, TLS 1.1 и TLS 1.2.. Техническая возможность использования того или иного протокола и его автоматический выбор будет зависеть от следующих параметров (Табл. 19, ниже).

Табл. 19 – 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. 96
Операционная система Linux	«Настройка SSL/TLS в операционной системе Linux», с. 96
Сервер JAS (поддержка версии протокола)	«Установка версий защищённого протокола на стороне сервера JAS», с. 97
Сервер JAS (настройка SSL/TLS на API-интерфейсах)	«Настройка SSL-подключения на API-интерфейсах сервера JAS», с. 97 В частности разделы: • «Настройка SSL-подключения сервера JMS к серверу JAS (AdministrationService API)» • «Настройка SSL/TLS на интерфейсе AuthenticationService»

JAS-плагины NPS и AD FS	«Настройка SSL/TLS на стороне клиентов», с. 100
Компонент JOL	«Настройка SSL/TLS на стороне компонента JOL», с. 101

Таким образом, для обеспечения поддержки этих протоколов необходимо выполнить ряд настроек как на стороне сервера JAS, так и на другой стороне соединения (Рис. 75).

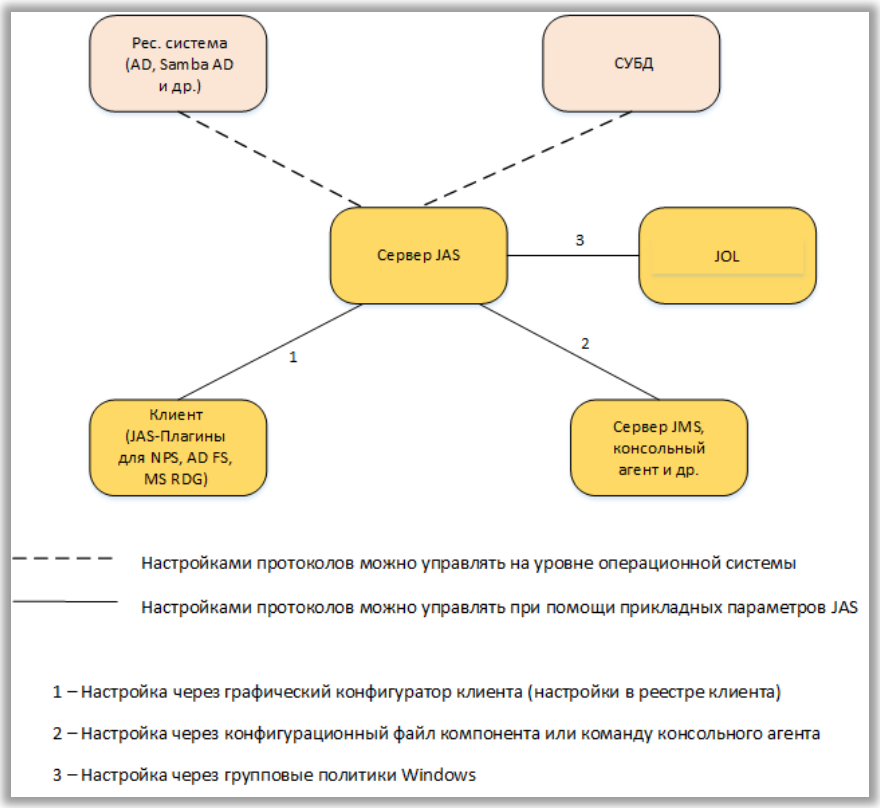


Рис. 75 – Схема настроек SSL/TLS на сторонах – участниках защищенного соединения

16.1 Настройка SSL/TLS в операционной системе Windows

Операционная система Windows на клиентах JAS (JAS-плагины NPS, AD FS, MS RDG, JOL), а также на почтовом сервере (если он работает под управлением ОС Windows) должна поддерживать требуемый протокол SSL/TLS. Настройки поддержки протоколов на уровне ОС задаются в разделе реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\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.

16.2 Настройка SSL/TLS в операционной системе Linux

Операционная система Linux на соответствующих компонентах системы (сервер JAS, JMS, почтовый сервер, сервер СУБД) должна поддерживать требуемый протокол SSL/TLS.

Проверку текущего набора поддерживаемых протоколов можно выполнить соответствующей командой OpenSSL в используемой версии Linux, например:

```
openssl ciphers -v | awk '{print $2}' | sort | uniq
```

Пример выдачи такой команды:

```
root@jms4lastral7:~# openssl ciphers -v | awk '{print $2}' | sort | uniq
SSLv3
TLSv1
TLSv1.2
TLSv1.3
```

Рис. 76 – Пример выдачи при проверке поддерживаемых протоколов SSL/TLS в ОС Linux

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

16.3 Установка версий защищённого протокола на стороне сервера JAS

Для настройки протоколов защиты транспортного уровня исходящих соединений сервера JAS на его хосте откройте на редактирование конфигурационный файл `/etc/aladdin/jas-engine/AppSettings.json` и в секции "Name": "Engine" проверьте значение параметра "SecurityProtocols", например:

```
{
      "Name": "Engine",
      "Settings": {
        "ID": "{02707361-31a2-42d0-b664-2dc5e8d41023}",
        "SecurityProtocols": "Tls, Tls11, Tls12"
         ...
      }

{
```

В данном параметр указывается список поддерживаемых протоколов шифрования для обмена данных между сетевыми узлами. Значения перечисляются через запятую (например: "`Ssl3, Tls, Tls11, Tls12`"). Допустимые значения:

- Ssl3;
- Tls;
- Tls11;
- Tls12.

Значение по умолчанию: "Tls, Tls11, Tls12"

При необходимости выполните редактирование значения параметра и перезагрузите процесс сервера JAS командой:

```
systemctl restart jas-engine
```

16.4 Настройка SSL-подключения на API-интерфейсах сервера JAS

Для обеспечения поддержки защищенных протоколов SSL/TLS необходимо выполнить ряд настроек в API-интерфейсах сервера JAS (Рис. 77).

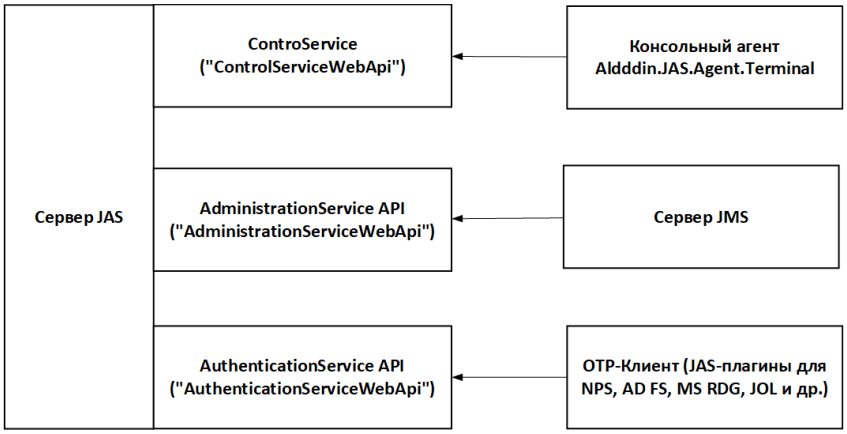


Рис. 77 – Схема настройки SSL на API-интерфейсах компонентов JAS/MS

Перед настройкой SSL в JAS необходимо выпустить SSL-сертификат сервера JAS. В случае если для подключения по SSL/TLS со стороны сервера JMS (интерфейс AdministrationService API) и клиентов (интерфейс AuthenticationService API) планируется использовать разные сертификаты, нужно выпустить два сертификата.

16.4.1 Настройка SSL-подключения сервера JMS к серверу JAS (AdministrationService API)

Подключения сервера JMS к JAS по SSL выполняется в два этапа. Сначала использование защищённого протокола необходимо включить на интерфейсе AdministrationService API сервера JAS, а затем установленные параметры подключения (новый адрес интерфейса) нужно указать в настройках сервера JMS. Для настройки выполните следующие шаги.

1. Для включения SSL на интерфейсе AdministrationService API сервера JAS следует использовать команду *ssl enable* консольного агента AladdinJAS.Agent.Terminal. Например:

```
sudo Aladdin.JAS.Agent.Terminal ssl enable --path
/home/user/Desktop/jas1.jms4.local.pfx --password P@ssw0rd! --api admin
```

В результате успешной настройки конфигурации на консоли отобразится:

```
user@jas1:/etc/aladdin/jas-engine$ sudo Aladdin.JAS.Agent.Terminal ssl enable --path /home/user/Desktop/jas1.jms4.local.pfx --password P@ssw0rd! --api admin
Настройка SSL Выполнена успешно.
Остановка сервера...
Запуск JAS-сервиса...
JAS-сервис запущен.
Текущее состояние сервера: Запускается
user@jas1:/etc/aladdin/jas-engine$
```

Рис. 78 – Выдача команды настройки SSL на API-интерфейсах сервера JAS

В приведенном примере используется ssl-сертификат сервера JAS. Команда предусматривает также возможность использовать уже ранее установленный в системе сертификат.

Примечания:

1. Если для интерфейсов AdministrationService и AuthenticationService необходимо использовать один и тот же SSL-сертификат сервера JAS, то в команде ssl enable можно использовать ключ "--api all", защищённые протокол будет включен на обоих интерфейсах с одним и тем же сертификатом.
2. Подробное описание команды ssl enable ее см. в разделе «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal», с. 109.

Для проверки текущей настройки SSL на интерфейсах сервера JAS используйте команду консольного агента *ssl show*, например:

```
sudo Aladdin.JAS.Agent.Terminal ssl show
```

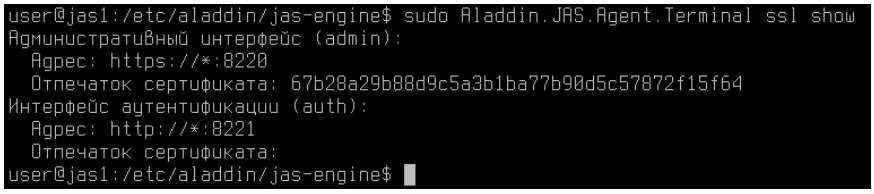


Рис. 79 – Пример выдачи команды ssl show

2. На сервере JMS выполните команду *jas configure* консольного агента JMS *Aladdin.EAP.Agent.Terminal*, указав https-адрес *Adminstration API* сервера JAS, настроенного на шаге 1, например:

```
Aladdin.EAP.Agent.Terminal jas configure -u https://<fqdn_Сервера_JAS>:8220 -s <тип аутентификации> -l <логин_пользователя_JAS> -p <логин_пользователя_JAS>
```

где:

<fqdn_Сервера_JAS> — Полное доменное имя сервера JAS, указанное в его SSL-сертификате;

<тип_аутентификации> —значение параметр SecurityType, установленного в для программного интерфейса AdminstrationService (подробнее см. Табл. 11, с. 22)

<логин_пользователя_JAS> —логин пользователя, под которым осуществляется аутентификация на сервере JAS

<пароль_пользователя_JAS> —пароль пользователя, под которым осуществляется аутентификация на сервере JAS

Подробное описание команды *jas configure* консольного агента JMS см. в Части 1 Руководства администратора [2] , раздел «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal»

16.4.2 Настройка SSL/TLS на интерфейсе AuthenticationService

Для включения защищённого протокола на интерфейсе AuthenticationService API сервера JAS выполните команду *ssl enable* консольного агента Aladdin.JAS.Agent.Terminal, как это было описано в разделе «Настройка SSL-подключения сервера JMS к серверу JAS (AdministrationService API)», но с ключом "--api auth", например:

```
Aladdin.JAS.Agent.Terminal ssl enable --path /opt/41/f_pfx/ssl.pfx --password P@ssw0rd --api auth
```

Примечание. Подробное описание команды ssl enable ее см. в разделе «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal», с. 109.

После включения защищенного протокола на интерфейсе аутентификации для корректной работы системы необходимо внести изменения также на клиентских компьютерах, подробнее см. разделы «Настройка SSL/TLS на стороне клиентов», с. 100 и «Настройка SSL/TLS на стороне компонента JOL», с. 101.

16.4.3 Настройка SSL/TLS для интерфейса ControlService

Для настройки защищённого подключения к JAS по интерфейсу ControlService (например для управления сервером через консольный агент) на хосте сервера JAS откройте на редактирование конфигурационный файл `/etc/aladdin/jas-engine/AppSettings.json` и внесите следующие изменения.

1. В секции "Name": "ControlServiceWebApi" в параметре "ControlServiceWebApiAddresses" замените http на https, например:

```
{
      "Name": "ControlServiceWebApi",
      "Settings": {
...
        "ControlServiceWebApiAddresses": "https://*:8219",
```

Примечание. Подробное описание параметров сетевых интерфейсов сервера JAS и их настройки приведено в разделе «Настройка сетевых программных интерфейсов сервера JAS», Табл. 11, с. 22.

2. В той же секции добавьте параметр "Thumbprint" со значением отпечатка SSL-сертификата хоста с сервером JAS, предварительно установленного на данном хосте (допускается использование сертификата, установленного, как описано в разделах «Настройка SSL-подключения сервера JMS к серверу JAS (AdministrationService API)») или «Настройка SSL/TLS на интерфейсе AuthenticationService», например:

```
{
      "Name": "AdministrationServiceWebApi",
      "Settings": {
...
      "Thumbprint": "2CE4D90BF553B28C45E20B828F955582E9D6CCAE"
```

3. Для вступления в силу внесенных изменений перезагрузите процесс сервера JAS:

```
systemctl restart jas-engine
```

16.5 Настройка SSL/TLS на стороне клиентов

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

1. В случае если клиенты JAS не имеют доступа к выпустившему 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]**

Примечание. Операции настройки можно выполнить в конфигураторе NPS (см. раздел «Работа с конфигуратором JAS-плагина для NPS», с. 41)

2.1.1. Отредактируйте строковый параметр **ServiceUri** (в конфигураторе – **Адрес JAS**) – после редактирования этот параметр должен иметь то же значение, что было настроено на сервере JAS для службы AuthenticationService (см. раздел «Настройка SSL/TLS на интерфейсе AuthenticationService», с. 99).

Для настройки набора поддерживаемых протоколов SSL/TLS отредактируйте параметр **SecurityProtocol=Ssl3, Tls, Tls11, Tls12** (в конфигураторе – **Поддерживаемые протоколы**).

Разрешается указывать один или несколько протоколов.
По умолчанию разрешены все протоколы.

2.2. В случае JAS-плагинов для AD FS и MS RDG в соответствующих разделах реестра (или посредством соответствующих графических конфигураторов, см. разделы «Работа с конфигуратором JAS-плагина для AD FS» с. 65 и «Работа с конфигуратором JAS-плагина для MS RDG», с. 79) выполните те же настройки, что были выполнены на шагах 2.1.1—0 для JAS-плагина для NPS.

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

16.6 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 стации вне домена ресурсной системы, в которой функционирует сервер JAS, или если участники SSL-соединения не имеют доступа к выпустившему 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. 87).
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. 87).
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. 96).

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

16.7 Настройка SSL/TLS в JAS для связи с ресурсной системой

Поскольку сервер JAS использует настройки подключения к ресурсным системам, взятые из JMS, используя общую с JMS базу данных, специальных настроек в конфигурации JAS не требуется.

Однако если сервер JAS размещен на отдельном хосте, и при этом данный компьютер не введен в домен Samba AD или AD, то необходимо сделать доверенным на этой машине SSL-сертификат ресурсной системы (т.е. установить корневой сертификат ресурсной системы). Для этого необходимо выполнить шаги по добавлению корневого сертификата в качестве доверенного, описанные в Части 1 Руководства администратора [2], в разделе «Настройка SSL для доступа к ресурсной системе», но уже в отношении сервера JAS.

16.8 Настройка SSL/TLS для работы с PostgreSQL

16.9 Настройка двустороннего SSL-соединения с SMPP-сервером

Если в случае выбора SMPP-протокола при настройке Messaging-транспорта (см. «Порядок настройки транспорта для работы с Messaging-токенами», с. 24) необходимо настроить двустороннее SSL-соединение, где в качестве клиентской стороны по отношению к SMPP-серверу

будет выступать сервер JAS, то в качестве "клиентского" сертификата следует выбрать предварительно установленный на хосте сертификат сервера JAS.

Условия данного SSL-соединения определяются соответствующими параметрами профиля SMPP-транспорта: **SslProtocols** и **SslThumbprint**, подробнее см. «Табл. 24 – Настройка smpp-транспорта сообщений», с. 120.

Настройка осуществляется путем выгрузки и редактирования профиля smpp-транспорта, так как это описано в разделе «Порядок настройки транспорта для работы с Messaging-токенами».

17. Развертывание отказоустойчивого кластера JAS

В настоящем разделе приведены шаги по настройке отказоустойчивого кластера серверов JAS, включающего в себя два узла.

Развертывание кластера приводится на примере следующей инфраструктуры:

1. Windows AD (ОС Windows server 2019)
2. PostgreSQL 14 (ОС Astra 1.6)
3. JMS Server (ОС Astra 1.7 или более поздняя версия)
4. Два сервера с ОС Astra 1.7, на которых будут развернуты узлы кластера JAS Server.

Подразумевается, что JMS Server установлен и настроен согласно Части 1 Руководства администратора [2].

В примере приводится развертывание кластера JAS в виртуальной среде.

17.1 Подготовка к установке кластера

1. Разверните виртуальную машину (ВМ) с ОС Астра 1.7 (создание ВМ первого узла.)
2. Выполните клонирование ВМ Астра 1.7 (создание ВМ для второго узла.)
3. Измените адрес склонированной ВМ. (Режим работы с подсетью 172.16.13.0/24.)
4. Выполните переименование обеих ВМ и внесите изменения в файлы **/etc/hosts** на них (в частности, удалив из них строку, содержащую *localhost*), руководствуясь разделами «Настройки на первом узле», с. 102 и «Настройки на втором узле», с. 102.

17.1.1 Настройки на первом узле

Предполагается, что у ВМ при создании было установлено имя *astra17*, если нет, выполните команду:

```
hostnamectl set-hostname astra17
```

Выполните последовательность команд для настройки окончательного имени и файла *hosts*:

```
hostnamectl set-hostname $(hostname)-1
sudo sed -i '$a 172.16.13.55 \t astra17-1' /etc/hosts
sudo sed -i '$a 172.16.13.56 \t astra17-2' /etc/hosts
sudo sed -i '/^127\.0\.1\.1/d' /etc/hosts
```

17.1.2 Настройки на втором узле

Предполагается, что у ВМ при создании было установлено имя *astra17*, если нет, выполните команду:

```
hostnamectl set-hostname astra17
```

Выполните последовательность команд для настройки окончательного имени и файла *hosts*:

```
hostnamectl set-hostname $(hostname)-2
sudo sed -i '$a 172.16.13.55 \t astra17-1' /etc/hosts
sudo sed -i '$a 172.16.13.56 \t astra17-2' /etc/hosts
sudo sed -i '/^127\.0\.1\.1/d' /etc/hosts
```

17.1.3 Настройки на обоих узлах

1. На обоих узлах выполните следующие команды:

```
sudo apt install pacemaker pcs astra-resource-agents
sudo passwd hacluster
sudo pcs cluster destroy
```

2. Выполните установку сервера JAS без инициализации (т.е. до выполнения команды *Aladdin.JAS.Agent.Terminal server initialize*), руководствуясь разделом «Установка и первоначальная настройка сервера JAS», с. 19 на обоих узлах.
3. Выполните инициализацию сервера JAS (см. раздел «Начальное конфигурирование сервера JAS», с. 20) на первом узле.
4. Скопируйте конфигурационный файл **/etc/aladdin/jas-engine/AppSettings.json** с первого узла на второй узел.
5. Проверьте, что на каждой ВМ процесс JAS запускается и переходит в состояние «работает».
6. Перезагрузите оба узла.

17.2 Настройки кластера

Команды, описанные ниже, выполняются на одном из узлов кластера (любом).

1. Выполните аутентификацию всех узлов кластера:

```
sudo pcs host auth astra17-1 astra17-2 -u hacluster -p 123456qweRTY
```

2. Задайте название кластера и список его участников:

```
sudo pcs cluster setup astracluster astra17-1 astra17-2 –force
```

где `astracluaster` -- имя кластера.

3. Запустите экземпляры кластера и добавьте их в автостарт:

```
sudo pcs cluster enable --all
sudo pcs cluster start --all
```

4. Отключите механизм stonith:

```
sudo pcs property set stonith-enabled=false
```

5. Отключите механизм кворума:

```
pcs property set no-quorum-policy=ignore
```

6. Проверьте статус сервиса и кластера:

```
sudo pcs status
sudo pcs cluster status
```

В консольной выдаче команды не должно быть ошибок.

17.3 Настройка ресурсов кластера

1. Создайте «мигрирующий» IP-адрес для доступа к ресурсам:

```
sudo pcs resource create ClusterIP ocf:heartbeat:IPaddr2 ip=172.16.13.220
cidr_netmask=32 op monitor interval=15s
```


Примечание. Выполненная настройка действует следующим образом. Еесли узел отключается, то IP-адрес мигрирует на рабочий узел кластера вместе с сервисом. Сохраняется доступность по одному и тому же IP-адресу вне зависимости от узла, на котором работает ресурс.

2. Создайте ресурс JAS сервиса:

```
sudo pcs resource create JAS service:jas-engine  op monitor interval=20
```


Примечание. Выполненная настройка действует следующим образом. Если узел стал недоступен, то осуществляется переход к следующему доступному узлу и на нем поднимаются все ресурсы..

3. Задайте связь между ресурсами:

```
pcs constraint colocation add ClusterIP with JAS score=INFINITY
```


Примечание. Выполненная настройка действует следующим образом. Кластер ищет узел, на котором расположить сервис JAS, а затем подтягивает сервис виртуального IP-адреса ClusterIP. Параметр score=INFINITY устанавливает условие, что они должны быть всегда вместе на одном узле.

4. Задайте последовательность запуска сервисов (сначала установка ресурса IP-адреса, затем – ресурса JAS):

```
pcs constraint order ClusterIP then JAS
```

5. Добавьте свойство **resource-stickiness** («липкости») ресурса к узлу, чтобы ресурс не перемещался стохастически между узлами:

```
pcs resource defaults resource-stickiness=100
```


Примечание. Поясним необходимость установки *resource-stickiness*. Без такой установки возможен, в частности, такой сценарий: произошел отказ 1-го узла, ресурс мигрирует на узел 2. Узел 1 восстановился, ресурс мигрировал обратно. После установки же «липкости» ресурс останется там, куда мигрировал после исходного отказа.

6. Добавьте количество сбоев перед миграцией на другой узел. По умолчанию сервис будет перезапускаться постоянно на одном и том же узле:

```
pcs resource defaults migration-threshold=10
```

Базовая настройка завершена. Результат настройки можно описать следующими положениями:

- обеспечена единая точка доступа к ресурсу (ClusterIP);
- гарантирован запуск одного экземпляра сервиса, работающего на одном из узлов;
- обеспечена автоматическая миграция сервиса при возникновении неполадок с сервисом (например, сервис JAS не может запуститься) или в случае физической недоступности узла (по причине программного или аппаратного отказа сервера).

17.4 Дополнительные команды по работе с кластером

pcs resource refresh – сбросить ошибки сервисов на узле кластера. Если использовать с параметром **–full** то сбросит ошибки на всех узлах.

pcs status – возвратить информацию о состоянии узлов кластера и его ресурсов.

pcs constraint – вывести список зависимостей между ресурсами, между узлами, между ресурсами и узлами.

17.5 Настройка SSL на интерфейсах JAS в кластерной конфигурации

Для настройки на API-интерфейсах JAS работы по защищённым протоколам выполните следующие действия.

1. Для «мигрирующего» IP-адреса кластера (см. раздел «Настройка ресурсов кластера», с. 104) добавьте в DNS имя так называемой «кластерной роли» (например например *jas-cluster.jms4.local*).

Примечание. При работе в домене AD данную операцию (создание DNS-имени для IP-адреса) можно выполнить из оснастки *Диспетчер DNS*.

2. На DNS-имя *кластерной роли* выпустите SSL-сертификат со следующими параметрами:
   - Subject Name – DNS-имя *кластерной роли* (в нашем примере *jas-cluster.jms4.local*)
   - Сертификат должен предоставлять возможность экспорта закрытого ключа.

Примечания:

- Для выпуска сертификата в MSCA можно воспользоваться инструкциями из справочника по выпуску сертификатов в MSCA [6], с. 137
- В случае отсутствия УЦ в сети допускается выпуск самоподписанного сертификата с помощь утилиты openssl

3. Экспортируйте сертификат в формате .pfx (при экспорте для шифрования пароля рекомендуется использовать алгоритм AES256-SHA256).
4. Выполните установку полученного SSL-сертификата *кластерной роли* на API-интерфейсах *AdminictrationService* и *AuthenticationService* (см. подробнее в разделах «Настройка SSL-подключения сервера JMS к серверу JAS (AdministrationService API)», с. 98 и «Настройка SSL/TLS на интерфейсе AuthenticationService» с. 99) на все узлы кластера.

Примечания:

1. Если для API-интерфейсов AdminictrationService и AuthenticationService необходимо использовать разные SSL-сертификаты по двум разным DNS-адресам (например для доступа внутри DMZ и из-за её пределов) для *кластерной роли* следует зарегистрировать отдельные DNS-имена (на мигрирующий IP-адрес), выпустить на каждое из них соответствующий SSL-сертификат и установить на соответствующие API-интерфейсы JAS.
2. Настройку подключения JMS к серверу JAS (команда Aladdin.EAP.Agent.Terminal jas configure) достаточно выполнить один раз, указав при этом в параметрах подключения адрес *кластерной роли* и аутентификационные данные пользователя, зарегистрированного на всех узлах кластера (убедитесь, что на всех узлах кластера JAS установлены одинаковые параметры аутентификации SecurityType, UserName и Password на интерфейсе AdminictrationService, подробнее см. Табл. 11, с. 22)) Например:

```
Aladdin.EAP.Agent.Terminal jas configure -u https://<fqdn_кластерной_роли_JAS>:8220
-s <тип аутентификации> -l <логин_пользователя_JAS> -p <логин_пользователя_JAS>
```

где:

<fqdn_кластерной_роли_JAS> -- полное доменное имя *кластерной роли*, указанное в её SSL-сертификате (в нашем примере *jas-cluster.jms4.local*);

<тип_аутентификации> -- значение параметра SecurityType, установленного в для программного интерфейса AdminstrationService на всех узлах кластера (подробнее см. Табл. 11, с. 22);

<логин_пользователя_JAS> -- логин пользователя, под которым осуществляется аутентификация на всех узла кластера JAS;

<пароль_пользователя_JAS> -- пароль пользователя, под которым осуществляется аутентификация на всех узлах кластера JAS.

Подробное описание команды *jas configure* консольного агента JMS см. в Части 1 Руководства администратора [2] , раздел «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal»

5. Для проверки корректности подключения сервера JMS к серверу JAS на стороне сервера JAS выполните команду *jas show* консольного агента JMS *Aladdin.EAP.Agent.Terminal*, например:

```
Aladdin.EAP.Agent.Terminal jas show
```

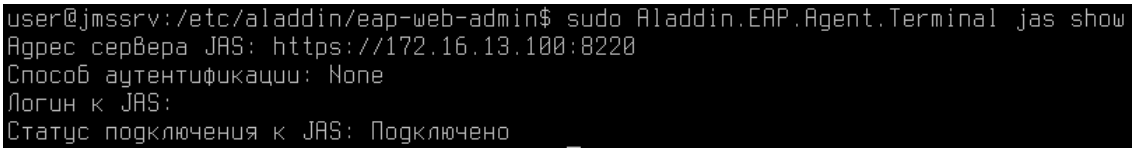


Рис. 80 – Пример выдачи команды jasl show

Приложение 1. Параметры файла первоначальной конфигурации сервера JAS

Секция service

Настройки сервиса JAS.

Секция является обязательной при инициализации с созданием БД и при инициализации с использованием существующей БД.

Имя настройки	Обязательность наличия	Описание
execPath	Да	Путь до исполняемого файла сервера JAS.
administrationServiceUrls	Да	Адреса Admin WebAPI: административного API (см. «Сетевые программные интерфейсы JAS», с. 18). Можно задать несколько адресов через «;». Для возможности использования API извне, один из адресов должен содержать внешний URL, либо с IP сервера, либо с его доменным именем. Например, «http://localhost:8120;http://192.168.2.202:8120», если машина с сервером JMS имеет IP 192.168.2.202. Значение по умолчанию: http://*:8120
controlServiceUrls	Да	Адреса Control WebAPI, используемого агентом сервера (см. «Сетевые программные интерфейсы JAS», с. 18). Можно задать несколько адресов через «;». Значение по умолчанию: http://localhost:8119
authenticationServiceUrls	Да	Адреса для Auth WebAPI: общей точки аутентификации для других API (см. «Сетевые программные интерфейсы JAS», с. 18). Можно задать несколько адресов через «;». Значение по умолчанию: http://*:8121
autoStart	Нет	Автостарт сервиса JAS Доступные значения: - true (по умолчанию) - false
culture	Нет	Язык сервера JAS (если язык не задан, сервер разворачивается с культурой по умолчанию – ru)

Секция database

Настройки подключения к базе данных JMS.

Секция является обязательной при инициализации сервера JAS.

В секции database должна быть указана БД, используемая сервером JMS.

Имя настройки	Обязательность наличия	Описание

type	Да	Тип СУБД. На данный момент поддерживается только одно значение: PostgreSQL
serverAddress	Да	Адрес сервера БД JMS
serverPort	Да	Порт сервера БД JMS
databaseName	Да	Имя БД JMS, к которой необходимо подключиться
databaseLogin	Да	Имя пользователя, которое будет использоваться сервером JAS для доступа используемой БД JMS
databasePassword	Да	Пароль пользователя
encryptionPassword	Да	Пароль шифрования данных JAS

Приложение 2. Справочник команд консольного агента Aladdin.JAS.Agent.Terminal

Синтаксис команды:

```
Aladdin.JAS.Agent.Terminal <команда> [[<параметр>] [<ключ>] [<аргумент>]] ...
[[<параметр>] [<ключ>] [<аргумент>]]
```

Для получения справки из консоли следует ввести следующую команду:

```
Aladdin.JAS.Agent.Terminal --help
```

Ключ --help работает на всех уровнях вложенности команд консольного агента (т.е. его можно использовать также после *команды* или *параметра*), например

```
Aladdin.JAS.Agent.Terminal server initialize --help
```

Полный перечень *команд, параметров* и *ключей* консольного агента приведен ниже.

Команда

licenses (просмотр лицензий JAS/JMS)

Параметр	Описание

list	Выводит информацию о текущих зарегистрированных лицензиях.
	Пример команды:
	`Aladdin.JAS.Agent.Terminal licenses list`
	Пример вывода:
	`PS D:\ITA\Aladdin\eapcore\JAS\OUTPUT\Bin\Debug\AnyCPU> ./Aladdin.JAS.Agent.Terminal.exe licenses list`
	`Id: 4`
	`Comment:`
	`Purpose:`
	`ProductId: 0x0811`
	`ProductName: Enterprise Application Platform`
	`GrantedName: IT Assist`
	`IssuedDate: 01.05.2022 10:15:18`
	`IssuedName:`
	`State: Valid`
	`ValidFrom: 01.03.2022 03:00:00`
	`ValidTo: 11.06.2032 03:00:00`
	`IsValid: True`
	`Version: 1.0.0.0`
	`VersionTo: 1.0.0.0`
	`LicenseKey: 5b6e809b-d073-4e6e-9238-cb81966968d0`
	`Features: 32`
	` NodeCount : 10`
	` UserCount : 10000`
	` GraceUserCount : 10`
	` TokenCount : 10000`
	` GraceTokenCount : 10`
	` TokenUserCount : 10000`
	` GraceTokenUserCount : 10`
	` ExternalTokenModels : 10000`
	` CryptoDevice : true`
	Примечание. Полное управление лицензиями JMS/JAS доступно в аналогичной команде консольного агента AladdinJAS.Agent.Terminal, см. Часть 1 Руководства администратора [2], раздел «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal»

Команда

server (управление сервером JMS)

Параметр	Описание

status	Вывод текущего статуса сервера. (Не требует ключей.)
	Пример вывода:
	`PS C:\Program Files\JaCarta Authentication System\Server Agent> ./Aladdin.JAS.Agent.Terminal.exe server status`
	`Текущее состояние сервера: Работает`

• **start**
• **stop**
• **pause**
• **continue**
	Управление статусом сервера. (Не требует ключей.)
	• **start** – запуск сервера
	• **stop** – остановка сервера
	• **pause** – приостановление работы сервера
	• **continue** – восстановить работу сервера после установки на паузу
	Пример команды:
	`Aladdin.JAS.Agent.Terminal server stop`
	Пример вывода:
	`PS C:\Program Files\JaCarta Authentication System\Server Agent> ./Aladdin.JAS.Agent.Terminal.exe server stop`
	`Успешно.`
	`Текущее состояние сервера: Остановлен`

initialize	Инициализирует сервер JMS: выполняет последовательную настройку всех параметров конфигурации сервера JMS, определенную в ini-файле конфигурации (передается в параметре ключа -p). Пример ini-файла см. в разделе «Подготовительные действия», с. 19. ⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo. **Ключи:** • **-p** (обязательный) – файл (.ini) конфигурации сервера JAS вместе с путём в файловой системе. • **-t** (опциональный) -- значение таймаута для операций запуска/остановки сервера в миллисекундах. **Пример команды:** `sudo Aladdin.JAS.Agent.Terminal server initialize -p /mnt/hgfs/SmolenskShared/jas_conf.ini -t 120000`
password	Выполняет установку мастер-пароля БД JAS. Инициализирует сервер JMS: выполняет последовательную настройку всех параметров конфигурации сервера JMS, определенную в ini-файле конфигурации (передается в параметре ключа -p). Пример ini-файла см. в разделе «Подготовительные действия», с. 19. ⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo. **Ключи:** • **--value** -- значение пароля. **Пример команды:** `sudo Aladdin.JAS.Agent.Terminal server password –value ‘ZXasqw12!@ZXasqw12!@’`

autostart	Используется для управления автостартом сервиса сервера JAS: `Aladdin.JAS.Agent.Terminal server autostart enable` - включает автостарт `Aladdin.JAS.Agent.Terminal server autostart disable` - отключает автостарт

config show	Выгружает текущие настройки сервера JAS по каждому из компонентов. На входе передается имя каталога, в который будет выгружена конфигурация. Если каталог не существует – он будет создан, если какой-то из файлов конфигурации уже существует на диске – он будет обновлен. Конфигурация выгружается в формате JSON
	Пример команды:
	`Aladdin.JAS.Agent.Terminal server config show --path /tmp/jas_config`
	Пример выдачи:
	`PS C:\Program Files\JaCarta Authentication System\Server Agent> ./Aladdin.JAS.Agent.Terminal.exe server config show --path c:\temp\jas_config`
	`Расширенная конфигурация сервера JAS выгружена в каталог 'c:\temp\jas_config'.`
	Настройки выгружаются в файлы:
	• **BusinessLogic.json**
	• **CertificateValidator.json**
	• **JournalingManager.json**
	• **NotificationManager.json**
	• **SyslogManager.json**

config upload	Активация расширенных настроек JAS из файла. За одно выполнение команды можно задать настройки одного или нескольких компонентов. **Ключи:** • **-b** — путь к загружаемому файлу настроек аутентификации, U2F, TFL; • **-c** — путь к загружаемому файлу настройки сертификатов для U2F; • **-j** — путь к загружаемому файлу настройки журналирования аутентификации; • **-n** — путь к загружаемому файлу настройки профилей Messaging-транспорта; **Примечание.** Ключ **-n** не рекомендуется использовать для настройки профилей Messaging-транспорта. Для конфигурирования Messaging-транспорта используйте команду sms, подробнее см. «Порядок настройки транспорта для работы с Messaging-токенами», с. 24); • **-s** — путь к загружаемому файлу настройки Syslog. **Пример команды:** `Aladdin.JAS.Agent.Terminal server config upload -b /tmp/jas_config/BusinessLogic.json -c /tmp/jas_config/CertificateValidator.json -j /tmp/jas_config/JournalingManager.json -n /tmp/jas_config/NotificationManager.json -s /tmp/jas_config/SyslogManager.json` Формат и назначение конфигурационных файлов приведены в разделе «Приложение 3. Справочник конфигурационных файлов JAS», с. 115.

Команда

sms

Параметр	Описание
savedefault	Команда по получению (выгрузке в виде файла) конфигураций по умолчанию для трёх типов messaging-транспорта (транспорта для отправки SMS-сообщений пользователям):

	• **Offline** -- сохранение сообщений в локальную папку для отладки сервиса; • **SMPP** – SMPP-транспорт (стандартный протокол взаимодействия с SMS-шлюзом); • **HTTP** – HTTP-транспорт для взаимодействия с SMS-шлюзом. **Ключи:** • **-t** — один из трех типов транспорта (**Offline**, **SMPP** и **HTTP**, значения могут быть указаны без учёта регистра); • **-p** — путь сохранения конфигурационного файла. **Пример команды:** `Aladdin.JAS.Agent.Terminal sms savedefault -t offline -p /mnt/hgfs/ShareVM/offline_default.json` Формат файла конфигураций см. в разделе «Приложение 3. Справочник конфигурационных файлов JAS», с. 115

register	Регистрирует указанный профиль для SMS-транспорта
	⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo.
	Ключи:
	• **-p** или **--path** (обязательный) – указывается файл конфигурации профиля транспорта.
	Пример команды:
	`sudo Aladdin.JAS.Agent.Terminal sms register -p /mnt/hgfs/ShareVM/jas_http_config_1.json`
	Пример выдачи:
	`autotest1@astra-172-12-22:~$ sudo jas-agent sms register -p /mnt/hgfs/ShareVM/jas_http_config_1.json`
	`Профиль 'Профиль HTTP транспорта 2' зарегистрирован.`

list	Отображает зарегистрированные профили SMS-транспорта. Каждый профиль отображается с присвоенным ему индексом (номером).
	Активный профиль выделяется знаком [*].
	⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo.
	Пример команды:
	`sudo Aladdin.JAS.Agent.Terminal sms list`
	Пример выдачи:
	`autotest1@astra-172-12-22:~$ sudo jas-agent sms list`
	`1.  [*] Имя: Профиль HTTP транспорта  Тип: Http`
	`2.  [ ] Имя: Профиль SMPP транспорта 8  Тип: Smpp`

setactive	Устанавливает активный профиль SMS-транспорта по указанному индексу (номеру). ⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo. **Ключи:** • **--index** (обязательный) – укажите индекс (номер) профиля, выбрав один из индексов, полученный с помощью команды **sms list** (см. выше). **Пример команды:**

	`sudo Aladdin.JAS.Agent.Terminal sms setactive --index 2`
	
	Пример выдачи:
	
	`autotest1@astra-172-12-22:~$ sudo jas-agent sms setactive --index 2`
	`Профиль 'Профиль SMPP транспорта 8' активирован.`

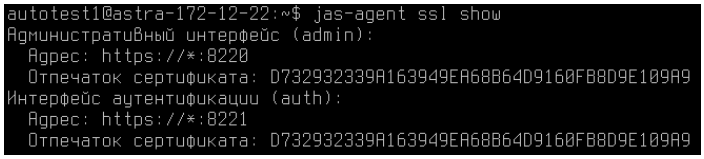
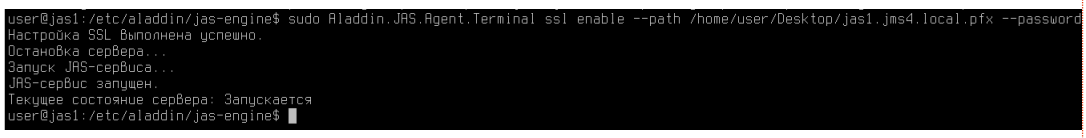
remove	Удаляет профиль SMS-транспорта по указанному имени профиля.
	
	⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo.
	
	Ключи:
	
	• **--name** (обязательный) – укажите имя профиля, как оно указано в выдаче команды **sms list** (см. выше).
	
	Пример команды:
	
	`sudo Aladdin.JAS.Agent.Terminal sms remove "Профиль Http-транспорта"`
	
	Пример выдачи:
	
	`autotest1@astra-172-12-22:~$ sudo jas-agent sms remove --name "Профиль HTTP транспорта"`
	`Профиль 'Профиль HTTP транспорта 6' удалён.`

test	Отправляет тестовое SMS-сообщение на указанный телефон по указанному имени профиля.
	
	⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo.
	
	Ключи:
	
	• **--phone** (обязательный) – укажите номер телефона, по которому следует отправить тестовое сообщение.
	• **--name** (обязательный) – укажите имя профиля, как оно указано в выдаче команды **sms list** (см. выше).
	
	Пример команды:
	
	`sudo Aladdin.JAS.Agent.Terminal sms test --phone 89101111111 --name "Профиль Smpp-транспорта"`
	
	Пример выдачи:
	
	`autotest1@astra-172-12-22:~$ sudo jas-agent sms test --phone 89101111111 --name "Профиль SMPP транспорта"`
	`Тестовое сообщение успешно отправлено.`

Команда

ssl (настройка SSL для API-интерфейсов *AdministrationService* и *AuthenticationService*)

Параметр	Описание
show	Отображает текущую конфигурацию SSL для интерфейсов AdministrationService и AuthenticationService. **Например:** `sudo Aladdin.JAS.Agent.Terminal ssl show`

	Пример выдачи: 
enable	Позволяет активировать SSL для интерфейсов AdministrationService и AuthenticationService. ⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo. **Ключи:** • **--path** – путь к файлу сертификата для SSL; • **--password** – пароль от указанного сертификата; • **--thumbprint** – отпечаток сертификата; • **--api** – тип API: административный – admin, аутентификация – auth, оба – all (по умолчанию) Для активации SSL требуется указать либо путь к файлу сертификата и пароль от контейнера сертификата, либо указать отпечаток уже зарегистрированного в хранилище сертификата. **Например:** `sudo Aladdin.JAS.Agent.Terminal ssl enable --path /home/user/Desktop/jas1.jms4.local.pfx --password P@ssw0rd! --api admin` **Пример выдачи:** 
disable	Позволяет отключить SSL для интерфейсов AdministrationService и AuthenticationService. ⚠ **Важно!** Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo. **Ключи:** • **--api** – тип API: административный – admin, аутентификация – auth, оба – all (по умолчанию)

Приложение 3. Справочник конфигурационных файлов JAS

CertificateValidator.json (Настройки сертификатов для U2F)

Примечание. Описание основных настроек U2F содержатся в разделах «Секция U2fSettings», с. 130 и «Секция TFLSettings», с. 131.

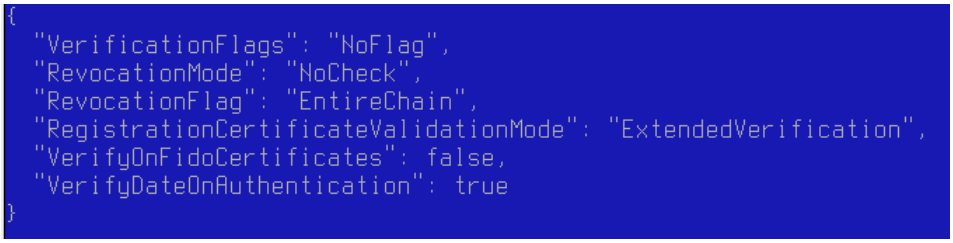


*Рис. 81 – Пример содержимого файла **CertificateValidator.json***

Табл. 20 – Настройки проверки аттестационных сертификатов U2F-устройств

Имя настройки	Описание
VerificationFlags	Выбор флагов детальной настройки проверки сертификатов (для ясности ниже приведен графический интерфейс настройки проверки сертификата из предыдущей версии продукта – JAS 3.7.1, см. Рис. 82, с. 117). Каждый флаг соответствует одному элементу набора атрибутов *System.Security.Cryptography.X509Certificates.X509VerificationFlags* платформы .NET компании Microsoft, см. Табл. 21, с. 117 (подробное описание атрибутов содержится в документации Microsoft, см. веб-ресурс [1], с. 137). **Примечание.** Для выполнения проверки аттестационного сертификата U2F-устройства корневые и дочерние сертификаты должны быть предварительно загружены в хранилище сертификатов При необходимости выбора нескольких флагов, их можно указать через знак конвейера «|». Доступные значения: • **AllFlags** – установить все флаги • **NoFlag** – сбросить все флаги • **IgnoreNotTimeValid** – Игнорировать истекшее время при проверке • **IgnoreCtlNotTimeValid** – Игнорировать списки CTL с истекшим временем • **IgnoreNotTimeNested** – Игнорировать временную вложенность сертификатов • **IgnoreInvalidBasicConstraints** – Игнорировать базовые ограничения проверки • **AllowUnknownCertificateAuthority** – Игнорировать неизвестные центры сертификации • **IgnoreWrongUsage** – Игнорировать недопустимый тип использования сертификата • **IgnoreInvalidName** – Игнорировать недопустимое имя при проверке

	• **IgnoreInvalidPolicy**— Игнорировать недопустимые политики при проверке • **IgnoreEndRevocationUnknown**— Игнорировать, что отзыв конечного сертификата неизвестен • **IgnoreCtlSignerRevocationUnknown**— Игнорировать, что отзыв подписчика сертификата неизвестен • **IgnoreCertificateAuthorityRevocationUnknown**— Игнорировать неизвестные отзывы центров сертификации • **IgnoreRootRevocationUnknown**— Игнорировать неизвестный отзыв корневого сертификата
RevocationMode	Проверка отзыва сертификатов. Параметр определяет обязательность и способ проверки сертификата на отзыв по спискам отзыва сертификатов. Параметр предлагает 3 варианта настройки: • **NoCheck** – Не проверять • **Online** – проверять сертификат в интерактивном режиме • **Offline** – проверять сертификат на основе загруженных списков отзывов сертификатов
RevocationFlag	Проверять на отзыв Параметр определяет необходимость и способ проверки на отзыв цепочки сертификатов. Предлагается 3 варианта настройки: • **EndCertificateOnly** – (Конечный сертификат) – выполняется проверка на отзыв только аттестационного сертификата U2F-устройства; • **EntireChain** – (Всю цепочку) – выполняется проверка на отзыв цепочки сертификатов; • **ExcludeRoot – (**Всю цепочку, кроме корневого) – выполняется проверка на отзыв всех сертификатов в цепочке, кроме корневого
RegistrationCertificateValidationMode	**Проверка сертификатов при регистрации** Настройка проверки аттестационных сертификатов U2F-устройства в процессе регистрации U2F-аутентификатора. Допустимые значения: • **Off –** (Отключена) – проверка аттестационного сертификата не выполняется • **DateOnly –** Проверять только срок действия сертификата • **ExtendedVerification –** (Расширенные параметры проверки) – производится проверка сертификата в соответствии с полями окна расширенной проверки (см. Рис. 82, с. 117).
VerifyOnCertificates	Флаг, устанавливающий необходимость проверять аттестационный сертификат с использованием списка загруженных доверенных сертификата альянса FIDO Допустимые значения: **true/false** **Примечания:** 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 в БД JMS. Управление доверенными FIDO-

	сертификатами осуществляется путем обращения к соответствующему API посредством протокола http согласно разделу «Приложение 4. Команды управления доверенными сертификатами альянса FIDO», с. 133. 3. Настройки параметров **VerificationFlags**, **RevocationMode** и **RevocationFlag** (описаны выше) не распространяются на проверку с помощью списка доверенных FIDO-сертификатов
VerifyDateOnAuthentication	**Проверка сертификатов при аутентификации** Настройка проверки аттестационных сертификатов U2F-устройства в процессе аутентификации с использование U2F-аутентификатора. Допустиымые значения: • **false** – (Отключена) – проверка аттестационного сертификата не выполняется • **true –** Проверять только срок действия сертификата

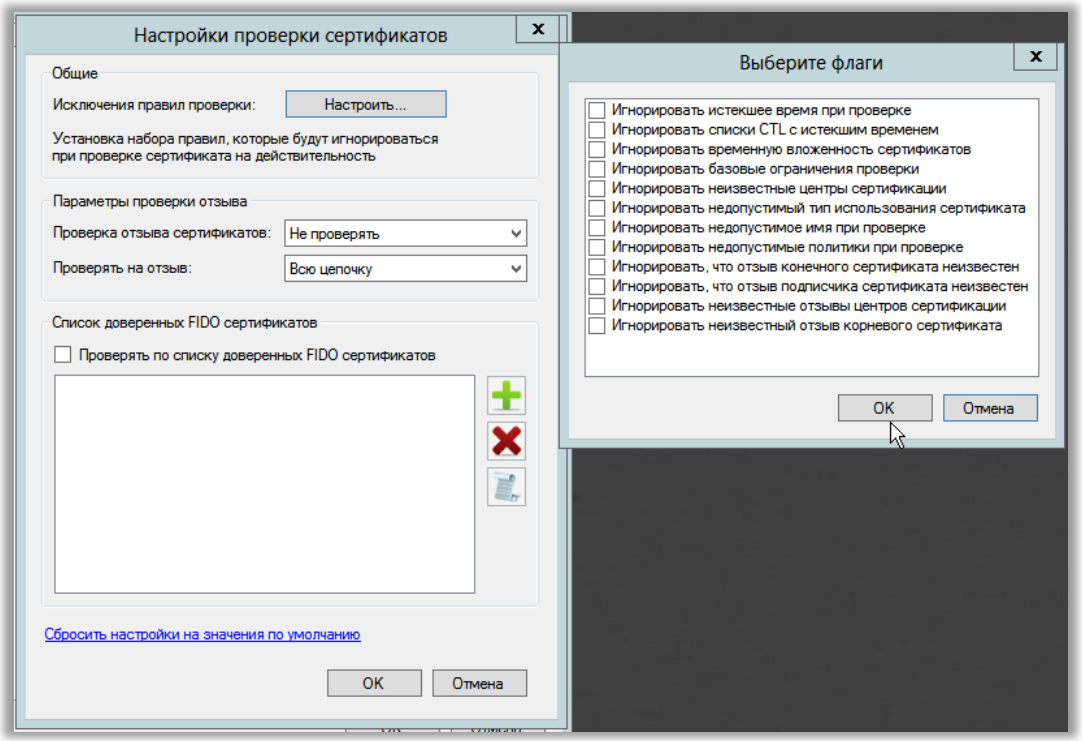


Рис. 82 – Интерфейс настройки проверки сертификата в предыдущей версии продукта JMS (графический интерфейс серверного агента JAS v3.7.1)

Табл. 21 – Настройки исключений проверок сертификата

Атрибут *X509VerificationFlags* платформы .NET	Флаг исключения проверки сертификата
IgnoreNotTimeValid	Игнорировать истекшее время при проверке
IgnoreCtlNotTimeValid	Игнорировать списки CTL с истекшим временем
IgnoreNotTimeNested	Игнорировать временную вложенность сертификатов
IgnoreInvalidBasicConstraints	Игнорировать базовые ограничения проверки
AllowUnknownCertificateAuthority	Игнорировать неизвестные центры сертификации
IgnoreWrongUsage	Игнорировать недопустимый тип использования сертификата
IgnoreInvalidName	Игнорировать недопустимое имя при проверке

IgnoreInvalidPolicy	Игнорировать недопустимые политики при проверке
IgnoreEndRevocationUnknown	Игнорировать, что отзыв конечного сертификата неизвестен
IgnoreCtlSignerRevocationUnknown	Игнорировать, что отзыв подписчика сертификата неизвестен
IgnoreCertificateAuthorityRevocationUnknown	Игнорировать неизвестные отзывы центров сертификации
IgnoreRootRevocationUnknown	Игнорировать неизвестный отзыв корневого сертификата

JournalingManager.json

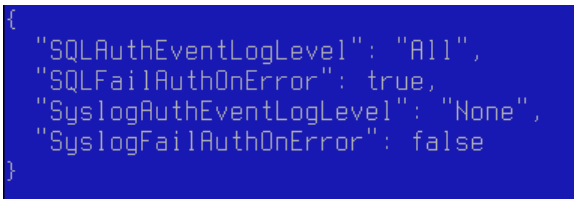


Рис. 83 – Пример содержимого файла JournalingManager.json

Табл. 22 – Настройки журналирования JAS

Имя настройки	Описание
SQLAuthEventLogLevel	Настройки записи событий аутентификации в журнал JMS (значения: None – отключено, ErrorOnly – только ошибки, All – полное логирование)
SQLFailAuthOnError	Аутентифицировать/не аутентифицировать при ошибке записи в журнал JMS (значения: true/false)
SyslogAuthEventLogLevel	Настройки записи событий аутентификации в журнал Syslog (значения: None – отключено, ErrorOnly – только ошибки, All – полное логирование)
SyslogFailAuthOnError	Аутентифицировать/не аутентифицировать при ошибке записи в журнал Syslog (значения: true/false)

NotificationManager.json

Так как настройки Offline-, SMPP- и HTTP-транспорта заметно различаются между собой, реализована отдельная команда для выгрузки шаблонов конфигурации профилей транспорта. Данные шаблоны являются частью файла NotificationManager.json.

Далее рассматриваются конфигурационные файлы профилей для каждого из доступных видов транспорта.

Параметры offline-транспорта:

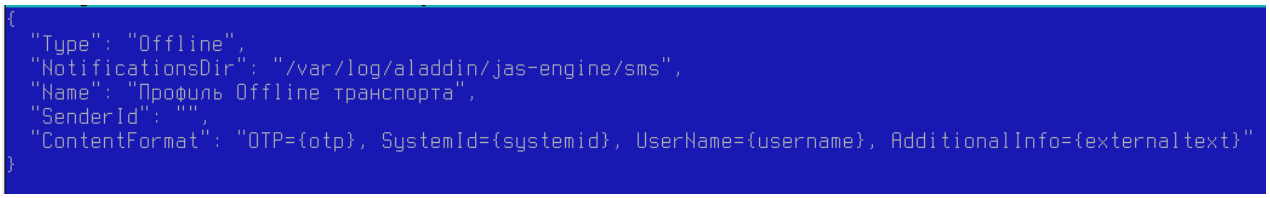


Рис. 84 – Пример содержимого профиля offline-транспорта

Табл. 23 – Настройка Offline-транспорта сообщений

Имя настройки	Описание
Type	Тип доставки сообщения. Значение: **"Offline"**

NotificationsDir	Имя папки директории для сохранения сообщений для Offline-профиля. Значение по умолчанию: **"/var/log/aladdin/jas-engine/sms"**
Name	Название профиля. Значение по умолчанию: **"Профиль Offline транспорта"**
SenderId	Отправитель. Следует указать имя отправителя. (Предназначено для отражения в сообщении пользователю). По умолчанию указано пустое значение.
ContentFormat	Формат сообщения. Формат строки сообщения, предназначенного для дальнейшей отправки пользователю. Содержит зарезервированные переменные, которые будут заменены при отправке данного сообщения: • **{otp}** – сгенерированный одноразовый пароль; • **{systemid}** – идентификатор внешней системы; • **{username}** – имя пользователя; • **{externaltext}** – строка, передаваемая внешней системой. Формат сообщения по умолчанию: `OTP={otp}, SystemId={systemid}, UserName={username}, AdditionalInfo={externaltext}` (Для ясности ниже приведен графический интерфейс предыдущей версии продукта – JAS 3.7.1, см. Рис. 85, ниже)

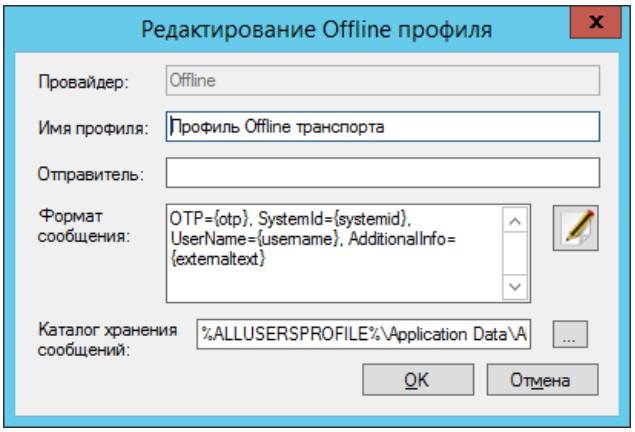
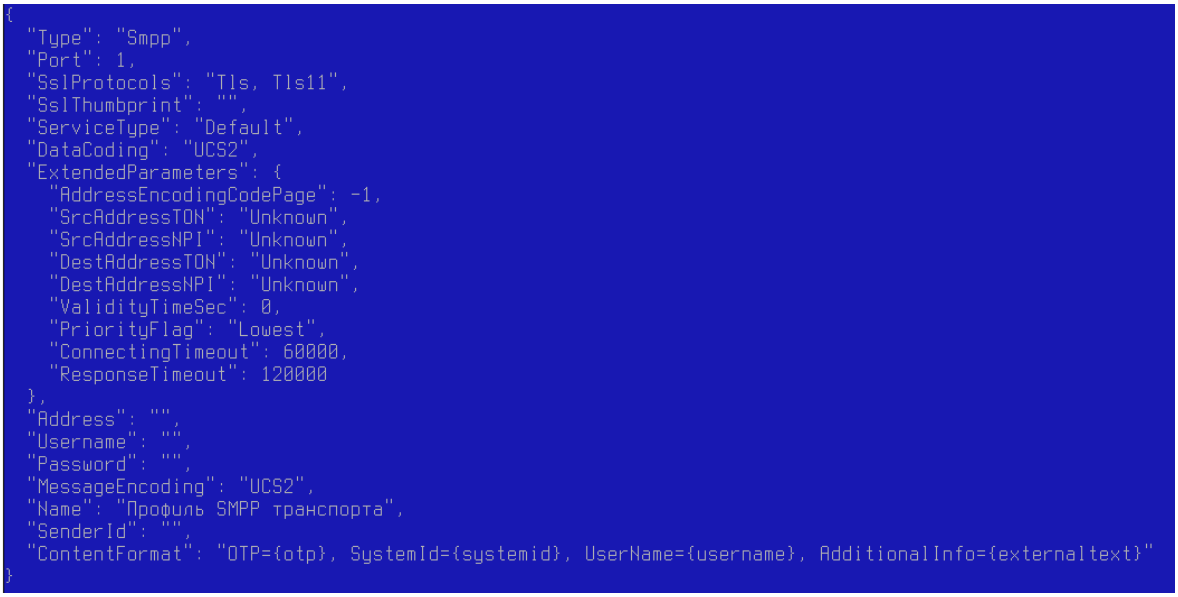


Рис. 85 – Интерфейс настройки Offline-профиля в предыдущей версии продукта JMS (графический интерфейс серверного агента JAS v3.7.

Параметры smpp-транспорта:



```
{
  "Type": "Smpp",
  "Port": 1,
  "SslProtocols": "Tls, Tls11",
  "SslThumbprint": "",
  "ServiceType": "Default",
  "DataCoding": "UCS2",
  "ExtendedParameters": {
    "AddressEncodingCodePage": -1,
    "SrcAddressTON": "Unknown",
    "SrcAddressNPI": "Unknown",
    "DestAddressTON": "Unknown",
    "DestAddressNPI": "Unknown",
    "ValidityTimeSec": 0,
    "PriorityFlag": "Lowest",
    "ConnectingTimeout": 60000,
    "ResponseTimeout": 120000
  },
  "Address": "",
  "Username": "",
  "Password": "",
  "MessageEncoding": "UCS2",
  "Name": "Профиль SMPP транспорта",
  "SenderId": "",
  "ContentFormat": "OTP={otp}, SystemId={systemid}, UserName={username}, AdditionalInfo={externaltext}"
}
```

Рис. 86 – Пример содержимого профиля smpp-транспорта

Табл. 24 – Настройка smpp-транспорта сообщений

Имя настройки	Описание
Type	Тип доставки сообщения. Значение: **Smpp**
Port	Порт подключения к серверу SMPP Значение по умолчанию: **1**
SslProtocols	Настройки SSL/TLS Выберите протоколы безопасного соединения, которые могут применяться для связи с сервером SMPP. Допустимые значения: • **Ssl30** – SSL 3.0 • **Tls** – TLS 1.0 • **Tls11** – TL 1.1 • **Tls12** – TLS 1.2 Допускается одновременный выбор нескольких протоколов, указываются через запятую. Значение по умолчанию: **Tls, Tls11** При поддержке протокола с серверной и клиентской стороны, будет выбран протокол наиболее поздней версии
SslThumbprint	Отпечаток «клиентского» (по отношению к SMPP-серверу) SSL-сертификата. Если необходимо установить двустороннюю аутентификацию по SSL/TLS, у данного параметра следует установить значение отпечатка SSL-сертификата сервера JAS, предварительно установленного на хосте сервера JAS. По умолчанию указано пустое значение.

ServiceType	**Тип сервиса отправки**
	
	Выберите тип сервиса отправки сообщений по SMPP.
	
	Допустимые значения:
	
	• **Default** – SMS (по умолчанию)
	• **Ussd** – USSD
	
	Примечания:
	
	1. При выборе значения **USSD**, необходимо убедиться в поддержке сервиса USSD со стороны шлюза.
	2. При выборе значения **USSD** на SMS-шлюз также передается код команды USSD, значение которой задается в конфигурационном файле **/opt/jas-engine/Aladdin.JAS.Engine.dll.config**:
	`<appSettings>`
	`...`
	`<add key="USSDParamValue" value=="3" />`
	`...`
	`<appSettings>`

DataCoding	Схема кодирования данных (например, UCS2)
AddressEncodingCodePage	Кодировка адресов отправителя и получателя (например, Default (GSM) или -1 (IBM Латиница))
SrcAddressTON	Тип номера отправителя
SrcAddressNPI	Номер плана индикации отправителя (NPI)
DestAddressTON	Тип номера получателя
DestAddressNPI	Номер плана индикации получателя
ValidityTimeSec	Срок доставки сообщения (в секундах). Время (в секундах), в течение которого сервер будет пытаться передать сообщение, если оно еще не передано
PriorityFlag	Приоритет доставки сообщения (например, Lowest – самый низкий)
ConnectingTimeout	Таймаут соединения. Время (в миллисекундах), в течение которого клиент будет пытаться установить соединение
ResponseTimeout	Таймаут ожидания ответа. Время (в миллисекундах) ожидания ответа от сервера на переданный пакет данных
Address	Адрес сервиса отправки сообщений (адрес подключения к серверу SMPP)
Username	Логин (в сервисе отправки сообщений). Имя пользователя для проверки подлинности отправителя (параметр SystemId протокола SMPP). Этот параметр является обязательным и должен иметь непустое значение
Password	Пароль (в сервисе отправки сообщений)
MessageEncoding	Кодировка сообщения (Значение по умолчанию: **UCS2**)
Name	Название профиля транспорта. Значение по умолчанию: **Профиль SMPP транспорта**
SenderId	Отправитель. Следует указать имя отправителя. (Предназначено для отражения в сообщении пользователю). По умолчанию указано пустое значение.
ContentFormat	Формат сообщения. Формат строки сообщения, предназначенного для дальнейшей отправки пользователю. Содержит зарезервированные переменные, которые будут заменены при отправке данного сообщения: • **{otp}** – сгенерированный одноразовый пароль; • **{systemid}** – идентификатор внешней системы;

	• **{username}** – имя пользователя; • **{externaltext}** – строка, передаваемая внешней системой. Формат сообщения по умолчанию: `OTP={otp}, SystemId={systemid}, UserName={username}, AdditionalInfo={externaltext}` (Для ясности ниже приведен графический интерфейс предыдущей версии продукта – JAS 3.7.1, см. Рис. 87, ниже)

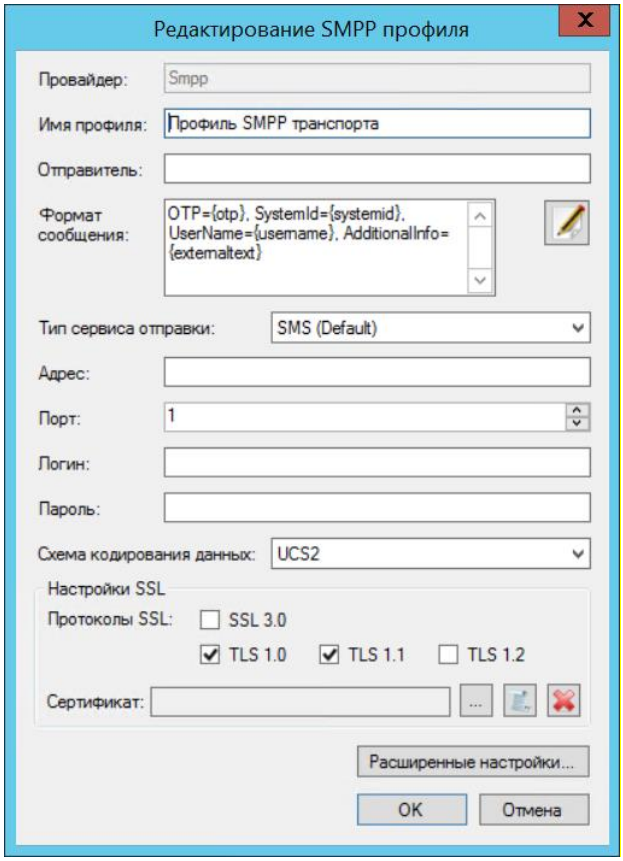


Рис. 87 – Интерфейс настройки SMPP-профиля в предыдущей версии продукта JMS (графический интерфейс серверного агента JAS v3.7)

Пример рабочего конфигурационного файла транспорта SMPP:

```
{
  "ActiveProfileName": "Профиль Smpp-транспорта",
  "Profiles": [
    {
      "$type": "Aladdin.JAS.Common.SmsProviderProfile.SmppSmsProviderProfile,
Aladdin.JAS.Common",
      "Type": "Smpp",
      "Port": 33333,
      "SslProtocols": "None",
      "SslThumbprint": "",
      "ServiceType": "Default",
      "DataCoding": "UCS2",
      "ExtendedParameters": {
        "AddressEncodingCodePage": -1,
        "SrcAddressTON": "Unknown",
```

```
        "SrcAddressNPI": "Unknown",
        "DestAddressTON": "Unknown",
        "DestAddressNPI": "Unknown",
        "ValidityTimeSec": 0,
        "PriorityFlag": "Lowest",
        "ConnectingTimeout": 60000,
        "ResponseTimeout": 120000
      },
      "Address": "192.168.10.13",
      "Username": "jas-sms",
      "Password": "71b5ec29-9998-4d40-97c1-582c68a6b228",
      "MessageEncoding": "UCS2",
      "Name": "Профиль Smpp-транспорта",
      "SenderId": "Sender",
      "ContentFormat": "OTP={otp}, SystemId={systemid}, UserName={username},
AdditionalInfo={externaltext}"
    }
  ],
  "MessageQueueSize": 10000,
  "StopTimeout": 1000,
  "Enabled": true,
  "RetryCount": 3
}
```

Параметры http-транспорта:

```
{
  "SecurityType": "None",
  "QueryParamsFormat": "",
  "MethodType": "GET",
  "ContentType": "",
  "AcceptType": "",
  "ResponseSuccessString": "",
  "ResponseSuccessHttpCode": 200,
  "UseMD5Password": false,
  "UseAuthorizationHeader": false,
  "Timeout": 60000,
  "ReadWriteTimeout": 120000,
  "Type": "Http",
  "Address": "",
  "Username": "",
  "Password": "",
  "MessageEncoding": "utf-8",
  "Name": "Профиль HTTP транспорта",
  "SenderId": "",
  "ContentFormat": "OTP={otp}, SystemId={systemid}, UserName={username}, AdditionalInfo={externaltext}"
}
```

Рис. 88 – Пример содержимого профиля http-транспорта

Табл. 25 – Настройка http-транспорта сообщений

Имя настройки	Описание
SecurityType	Тип аутентификации по HTTP-соединению Допустимые значения: • **None** – анонимная (по умолчанию) • **Basic**
QueryParamsFormat	Формат параметров URL-запроса.

	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: • **{username}** – имя пользователя; • **{password}** – пароль пользователя; • **{encoding}** – кодировка; • **{sender}** – идентификатор отправителя; • **{message}** – отправляемое сообщение; • **{phonelist}** – список телефонных номеров (разделены запятыми), на которые будет отправлено сообщение; • **{phone}** – телефонный номер, на который будет отправлено сообщение; Пример формата параметров запроса: `login={username}&psw={password}&charset={encoding}&phones={phonelist}&mes={message}&sender={sender}`
MethodType	Метод http запроса. Имя метода, используемого в HTTP-запросе, который отправляется на SMS-шлюз. Доступные значения: • **GET** • **POST**
ContentType	Тип содержимого (тип содержимого в теле HTTP-запроса). Доступные значения: • **text/plain** • **text/html** • **text/xml** • **application/xml** • **application/json** • **application/x-www-form-urlencoded** Этот параметр доступен только при запросах типа POST (см. поле **Тип запроса**).
AcceptType	Заголовок Accept. Доступные значения: • ***/*** • **text/plain** • **text/html** • **text/xml** • **application/xml** • **application/json** • **application/x-www-form-urlencoded**
ResponseSuccessString	Строка положительного ответа. Строка, вхождение которой в ответ от SMS-шлюза означает, что передача сообщения завершилась успешно
ResponseSuccessHttpCode	Http код положительного ответа (например, 200)
UseMD5Password	Хэш MD5 Признак использования хэша MD5 от пароля при передаче

	Допустимые значения: • **true** • **false**
UseAuthorizationHeader	Отправлять логин/пароль в заголовке Authorization. Допустимые значения: • **true** • **false**
Timeout	Таймаут соединения
ReadWriteTimeout	Таймаут ожидания ответа
Type	Тип доставки сообщения. Значение: **Hmpp**
Address	Адрес сервиса отправки сообщений. Адрес (URL-строка) для отправки HTTP-запросов на рассылку SMS-сообщения
Username	Логин (в сервисе отправки сообщений). Имя пользователя учетной записи коммерческого SMS-шлюза
Password	Пароль (в сервисе отправки сообщений)
MessageEncoding	Кодировка отправляемого сообщения. Допустимые значения: • **windows-1251** • **utf-8** • **koi8-r**
Name	Название профиля транспорта. Значение по умолчанию: **Профиль SMPP транспорта**
SenderId	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)
ContentFormat	Формат сообщения. Формат строки сообщения, отправляемого через SMS-шлюз. Содержит зарезервированные переменные, которые будут заменены при отправке данного сообщения: • **{otp}** – сгенерированный одноразовый пароль; • **{systemid}** – идентификатор внешней системы; • **{username}** – имя пользователя; • **{externaltext}** – строка, передаваемая внешней системой. Для редактирования формата нажмите  . Формат сообщения по умолчанию: OTP={otp}, SystemId={systemid}, UserName={username}, AdditionalInfo={externaltext} (Для ясности ниже приведен графический интерфейс предыдущей версии продукта – JAS 3.7.1, см. Рис. 89, с.126)

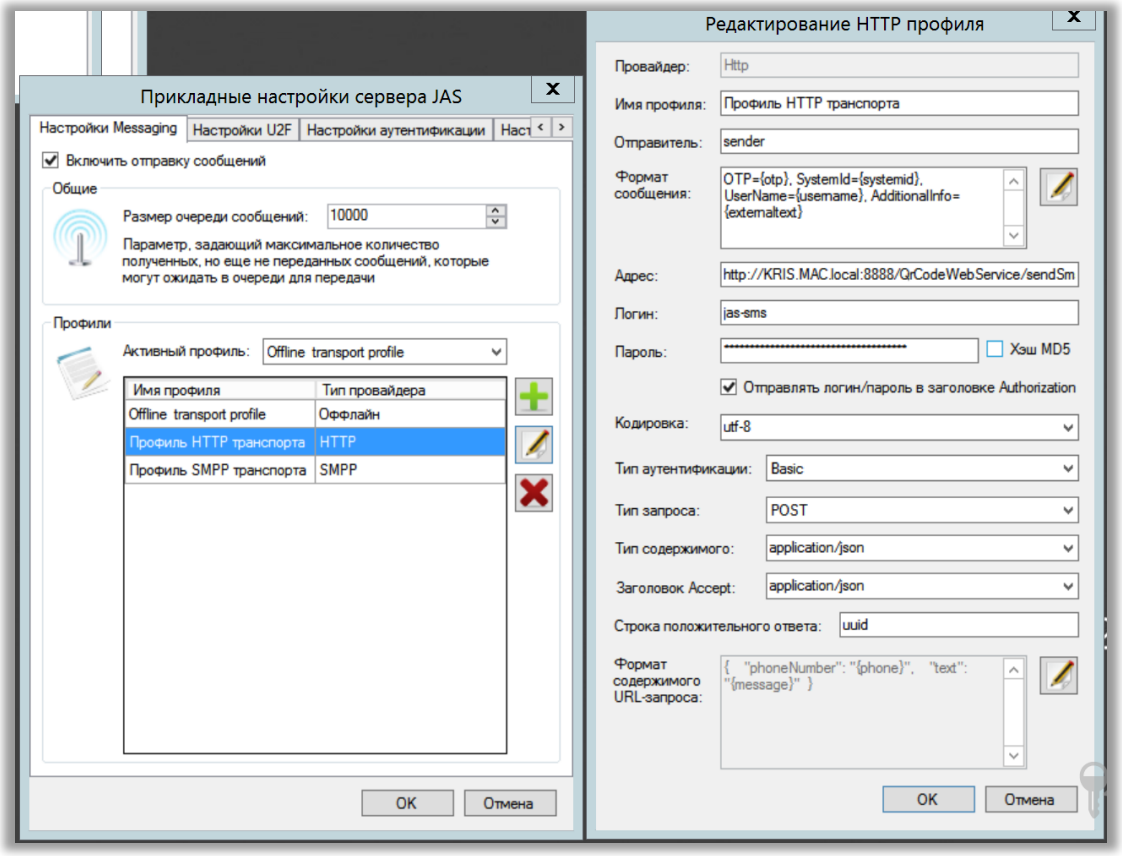


Рис. 89 – Интерфейс настройки Messaging-транспорта (в частности HTTP) в предыдущей версии продукта JMS (графический интерфейс серверного агента JAS v3.7.1)

Пример рабочего конфигурационного файла транспорта HTTP:

```
    {
  "ActiveProfileName": "Профиль Http-транспорта",
  "Profiles": [
    {
      "$type": "Aladdin.JAS.Common.SmsProviderProfile.HttpSmsProviderProfile,
Aladdin.JAS.Common",
      "SecurityType": "None",
      "QueryParamsFormat":
"phones={phonelist}&message={message}&login={username}&password={password}&custompar
ameters={customparameters}",
      "MethodType": "GET",
      "ContentType": "application/json",
      "AcceptType": "application/json",
      "ResponseSuccessString": "",
      "ResponseSuccessHttpCode": 200,
      "UseMD5Password": false,
      "UseAuthorizationHeader": false,
      "Timeout": 60000,
      "ReadWriteTimeout": 120000,
      "Type": "Http",
      "Address": "http://192.168.10.13:8099/TestHttpSmsService/sendsms",
      "Username": "jas-sms",
      "Password": "71b5ec29-9998-4d40-97c1-582c68a6b228",
      "MessageEncoding": "utf-8",
      "Name": "Профиль Http-транспорта",
      "SenderId": "Sender",
```

```
      "ContentFormat": "OTP={otp}, SystemId={systemid}, UserName={username},
AdditionalInfo={externaltext}"
    },
  ],
  "MessageQueueSize": 10000,
  "StopTimeout": 1000,
  "Enabled": true,
  "RetryCount": 3
}
```

SyslogManager.json

SyslogManager.json – настройка подключения к Syslog

```
{
  "Server": "127.0.0.1",
  "Port": 514,
  "RfcVersion": "Rfc5424",
  "UseEncryption": false,
  "Protocol": "Tcp",
  "AppName": "JAS",
  "MessageTransfer": "NonTransparentFraming"
}
```

*Рис. 90 – Пример содержимого файла **SyslogManager.json***

Табл. 26 – Настройки Syslog

Имя настройки	Описание
Server	Адрес сервера Syslog IP-адрес или полное доменное имя (FQDN) Syslog-сервера.
Port	Порт сервера Syslog (в зависимости от настроек сервера Syslog, по умолчанию 514)
RfcVersion	Версия RFC. Выберите спецификацию Syslog для работы с сервером. Допустимые значения: • **RFC 5424** (по умолчанию) • **RFC 3164**
UseEncryption	Использовать защищенное соединение. Установите флаг, если для связи с Syslog-сервером необходимо использовать защищенное (SSL/TLS) соединение. Допустимые значения: • **true** • **false** Настройка актуальна только при использовании протокола TCP.
Protocol	Протокол отправки сообщений syslog Выберите протокол транспортного уровня для работы с Syslog. Допустимые значения: • **TCP** (по умолчанию) • **UDP**
AppName	Наименование приложения Текстовый идентификатор приложения (используется в выходных данных Syslog для идентификации приложения)

	Значение по умолчанию: **JAS**
MessageTransfer	Метод фрейминга для syslog сообщений. Метод определения границ сообщения в случае, если одновременно посылается несколько сообщений Допустимые значения: • **OctetCounting** (по умолчанию) – в начале каждого Syslog-сообщения устанавливается его длина для определения границ сообщения; • **NonTransparentFraming** – сообщения могут разделяться следующими символами: ASCII LF, ASCII NUL или последовательностью символов CR и LF

Примечание. Для ясности ниже приведен графический интерфейс настройки Syslog предыдущей версии продукта – JAS 3.7.1, Рис. 91)

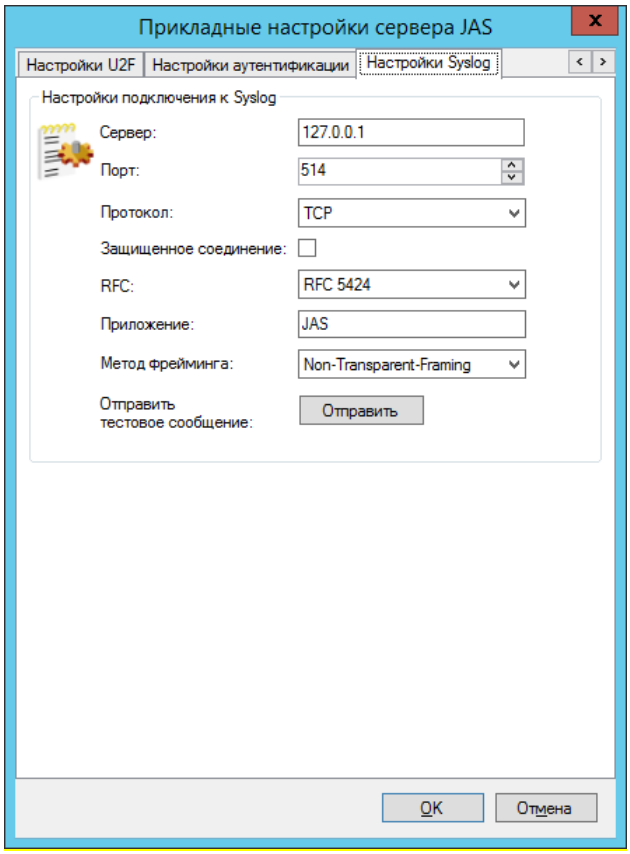


Рис. 91 – Интерфейс настройки Syslog в предыдущей версии продукта JMS (графический интерфейс серверного агента JAS v3.7.1)

BusinessLogic.json

BusinessLogic.json – настройка поведения бизнес-логики.

*Рис. 92 – Пример содержимого файла **BusinessLogic.json***

Секция OtpTokenConfigPreferenses

Табл. 27 – Настройки аутентификации

Имя настройки	Описание
MaxAuthFailCount	Максимальное количество неудачных попыток аутентификации (для OTP-токенов). Количество попыток аутентификации пользователя при вводе им неверного одноразового пароля, после которых все OTP-токены данного пользователя будут заблокированы. **Примечания:** 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. Значение по умолчанию – 100.

PushMaxAuthFailCount	Максимальное количество неудачных попыток аутентификации (для Push-токенов), число попыток до блокировки токена. Правила ограничения аналогичны правилам для параметра **MaxAuthFailCount** (выше). **Примечание.** Под "неудачными попытками аутентификации" в случае Push-токенов понимается потенциальная злонамеренная эмуляция Push-приложения с попытками перебора OTP-секрета. Значение по умолчанию – 100.
MessagingMaxAuthFailCount	Максимальное количество неудачных попыток аутентификации (для Messaging-токенов), число попыток до блокировки токена. Правила ограничения аналогичны правилам для параметра **MaxAuthFailCount** (выше), за исключением условия блокировки всех Messaging-токенов пользователя: блокировка выполняется только для того токена, по которому было превышено число попыток аутентификации. Значение по умолчанию – 100.

Примечание. Для ясности ниже приведен графический интерфейс настройки Syslog предыдущей версии продукта – JAS 3.7.1, Рис. 93)

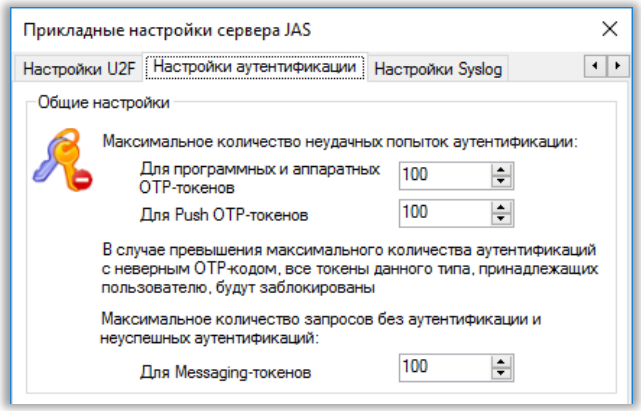


Рис. 93 – Интерфейс настройки аутентификации в предыдущей версии продукта JMS (графический интерфейс серверного агента JAS v3.7.1)

Секция U2fSettings

Табл. 28 – Настройки U2F

Имя настройки	Описание
U2fContextExpiredCheckPeriod	Таймаут аутентификации по контексту в миллисекундах. **Примечание.** Создание контекста (операционной среды сеанса аутентификации) является промежуточным шагом при аутентификации по U2F. При стандартных условиях эксплуатации параметр не требует изменения значения по умолчанию. Значение по умолчанию: 60000
RegistrationTimeoutMsec	Максимальное время регистрации (мс).

	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. Значение по умолчанию: 60000
AutenticationTimeoutMsec	Максимальное время аутентификации (мс). 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. Значение по умолчанию: 60000
MaxConcurrentAutentications	Максимальное количество одновременных аутентификаций по токену. (Максимальное количество одновременных аутентификаций по одному U2F-аутентификатору.) Значение по умолчанию: 100

Примечание. Для ясности ниже приведен графический интерфейс настройки Syslog предыдущей версии продукта – JAS 3.7.1, Рис. 94)

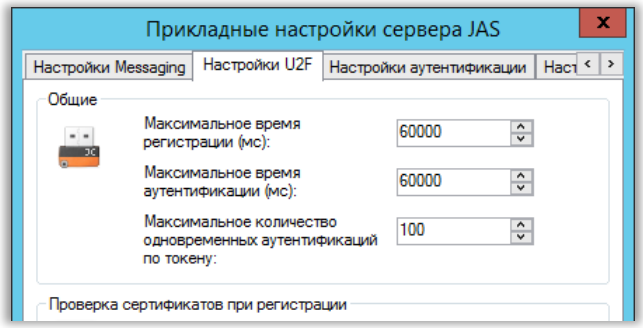


Рис. 94 – Интерфейс настройки U2F в предыдущей версии продукта JMS (графический интерфейс серверного агента JAS v3.7.1)

Секция TFLSettings

В данной секции настройки определяют "правила валидации" FacetId при аутентификации по U2F с использованием серверов TFL (Trusted Facet List). Подробнее см. соответствующую спецификацию U2F, https://fidoalliance.org/specs/fido-u2f-v1.0-ps-20141009/fido-appid-and-facets-ps-20141009.html, а также web-ресурс со спецификациями FIDO [2].

Табл. 29 – Настройки секции TFLSettings

Имя настройки	Описание
PublicSuffixesUrl	Url-адрес для загрузки публичных суффиксов доменных имен.

Имя настройки	Описание
EnableFacetValidation	Флаг включения проверки фасетов. Допустимые значения: • **true**-проверка включена (значение по умолчанию), • **false** – проверка отключена
EnableContentTypeValidation	Флаг включения проверки соответствия MIME-типа ответного сообщения от сервера TFL. Допустимые значения: • **true**-проверка включена (значение по умолчанию), • **false** – проверка отключена
PublicSuffixesDownloadTimeoutMsec	Таймаут ожидания загрузки публичных суффиксов (мс) Значение по умолчанию: **1500**
RegistrationTimeoutMsec	Таймаут ожидания ответа на HTTP-запрос (мс) Значение по умолчанию: **1000**

Приложение 4. Команды управления доверенными сертификатами альянса FIDO

В настоящем приложении описан порядок регистрации в БД JAS доверенных сертификатов альянса FIDO для обеспечения возможности работы с U2F-аутентификаторами, а также удаления, обновления и получения списка указанных сертификатов.

Управление сертификатами осуществляется путём обращения к соответствующему API продукта посредством вызова методов (POST, PUT, DELETE) протокола http.

Примечание. Для выполнения http-запросов можно использовать любую утилиту командной строки для работы с протоколом http, например кроссплатформенную утилиту CURL.

Регистрация сертификата

Регистрация FIDO-сертификата в БД JMS выполняется вызовом POST-метода следующего формата:

```
POST <адрес API>
{
    "ExternalId" : "<уникальный идентификатор сертификата>",
    "CertificateBody" : "<тело сертификата в кодировке  base64 >",
    "Thumbprint" : "<отпечаток сертификата>",
    "Enabled" : <флаг доступности сертификата для проверки true/false>
}
```

Например:

```
POST http://localhost:8219/api/v4.1/config/fidocert
{
    "ExternalId" : "bdc5c250-8251-46db-854f-283fc790c49e",
    "CertificateBody" :
"WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQbcrSVr0Bb9OWM2xXiyM8ogH1A4CvnpYqetSVwhtq3ssomgBM
cEpI1jXaonv5qk3sPrwJs9Ccu0Wv5R5DlbN+eMAoGCCqGSM49BAMCA0gAMEUCIQDSJkXRNnnc9Z0zKdSn4Ap
ENimxjtHG7M65ZifFImaviAIgFbWVz1ZU99PyqHdwiGVAcWY9NQnfQm/7sShktyIKwaE=",
    "Thumbprint" : "2CE4D90BF553B28C45E20B828F955582E9D6CCAE",
    "Enabled" : true
}
```

При успешном выполнении метода возвращается ответ следующего вида:

```
{
    "ExternalId": "bdc5c250-8251-46db-854f-283fc790c49e",
    "CertificateBody":
"WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQbcrSVr0Bb9OWM2xXiyM8ogH1A4CvnpYqetSVwhtq3ssomgBM
cEpI1jXaonv5qk3sPrwJs9Ccu0Wv5R5DlbN+eMAoGCCqGSM49BAMCA0gAMEUCIQDSJkXRNnnc9Z0zKdSn4Ap
ENimxjtHG7M65ZifFImaviAIgFbWVz1ZU99PyqHdwiGVAcWY9NQnfQm/7sShktyIKwaE=",
    "Thumbprint": "2CE4D90BF553B28C45E20B828F955582E9D6CCAE",
    "Enabled": true
}
```

Удаление сертификата

Удаление FIDO-сертификата из БД JMS выполняется вызовом DELETE-метода следующего формата:

```
DELETE <адрес API>
{
    "ExternalId" : "<уникальный идентификатор сертификата>"
}
```

Например:

```
DELETE http://localhost:8219/api/v4.1/config/fidocert
{
    "ExternalId" : "bdc5c250-8251-46db-854f-283fc790c49e"
}
```

При успешном выполнении метода возвращается ответ следующего вида:

```
true
```

Обновление сертификата

Чтобы заменить FIDO-сертификат в БД JMS, следует выполнить вызов PUT-метода следующего формата:

```
PUT <адрес API>
{
    "ExternalId" : "<уникальный идентификатор сертификата>",
    "CertificateBody" : "<тело сертификата в кодировке  base64 >",
    "Thumbprint" : "<отпечаток сертификата>",
    "Enabled" : <флаг доступности сертификата для проверки true/false>
}
{
    "ExternalId" : "<уникальный идентификатор сертификата>"
}
```

Например:

```
PUT http://localhost:8219/api/v4.1/config/fidocert
{
    "ExternalId" : "bdc5c250-8251-46db-854f-283fc790c49e",
    "CertificateBody" :
"WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQbcrSVr0Bb9OWM2xXiyM8ogH1A4CvnpYqetSVwhtq3ssomgBM
cEpI1jXaonv5qk3sPrwJs9Ccu0Wv5R5DlbN+eMAoGCCqGSM49BAMCA0gAMEUCIQDSJkXRNnnc9Z0zKdSn4Ap
ENimxjtHG7M65ZifFImaviAIgFbWVz1ZU99PyqHdwiGVAcWY9NQnfQm/7sShktyIKwaE=",
    "Thumbprint" : "2CE4D90BF553B28C45E20B828F955582E9D6CCAE",
    "Enabled" : false
}
```

При успешном выполнении метода возвращается ответ следующего вида:

```
true
```

Получение списка сертификатов

Чтобы получить список зарегистрированных в БД JMS FIDO-сертификатов, следует выполнить вызов POST-метода следующего формата:

```
POST <адрес API>
{
    "Start" : <порядковый номер сертификата, начиная с которого нужно
отобразить список; нумерация начинается с нуля>,
    "Size" : <максимальное число сертификатов для вывода>
}
```

Например:

```
POST http://localhost:8219/api/v4.1/config/fidocert/search

{
    "Start" : 0,
    "Size" : 100
```

```
}
```

При успешном выполнении метода возвращается список сертификатов следующего вида:

```
{
    "Entities": [
        {
            "ExternalId": "bdc5c250-8251-46db-854f-283fc790c49e",
            "CertificateBody":
"WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQbcrSVr0Bb9OWM2xXiyM8ogH1A4CvnpYqetSVwhtq3ssomgBM
cEpI1jXaonv5qk3sPrwJs9Ccu0Wv5R5DlbN+eMAoGCCqGSM49BAMCA0gAMEUCIQDSJkXRNnnc9Z0zKdSn4Ap
ENimxjtHG7M65ZifFImaviAIgFbWVz1ZU99PyqHdwiGVAcWY9NQnfQm/7sShktyIKwaE=",
            "Thumbprint": "2CE4D90BF553B28C45E20B828F955582E9D6CCAE",
            "Enabled": false
        }
    ],
    "TotalCount": 1
}
```

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 4LX. Руководство администратора. Часть 1. Установка и настройка [Текст]. — «Аладдин Р.Д.». — Файл JMS-4LX Руководство Администратор 1.docx

3 JaCarta Management System 4LX. Руководство администратора . Часть 2. Функции управления [Текст]. — «Аладдин Р.Д.». — Файл JMS-4LX Руководство Администратор 3.docx

4 JaCarta Management System 4LX. Руководство пользователя [Текст]. — «Аладдин Р.Д.». — Файл JMS-4LX Руководство Пользователь.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»

6 JaCarta Management System v3.7.1. Подготовка и выпуск сертификатов в MSCA для JMS [Текст]. — «Аладдин Р.Д.». — Файл JMS_x.x.x_Cert_Guide.docx

Полезные web-ресуры

1 Microsoft. Developer Network. Documentation. X509VerificationFlags Enumeration: 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

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.

Аладдин

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