УТВЕРЖДЕН
RU.АЛДЕ.03.16.001-05 32 01-1-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ JACARTA MANAGEMENT SYSTEM 4LX

Руководство администратора. Часть 4

Установка и настройка JAS RADIUS Server (JRS)

RU.АЛДЕ.03.16.001-05 32 01-4

Версия продукта	1.0
Версия документа	1.00
Статус	Публичный
Дата	7 марта 2025 г.
Листов	66

2025

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

Оглавление

1. О документе

1.1 Назначение документа

Настоящий документ является руководства администратора по JAS RADIUS Server (JRS) и представляет собой описание операций по установке и настройке данного программного продукта для среды функционирования Linux.

1.2 На кого ориентирован данный документ

Документ предназначен для администраторов корпоративных информационных систем, обеспечивающих интеграцию продукта JRS 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. 4	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
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	Программное обеспечение JaCarta Management System
Messaging-токен	Аутентификатор, позволяющий проводить аутентификацию посредством отправки OTP посредством службы SMS оператора мобильной связи
NPS	Network Policy Server – служба политики сети и доступа Microsoft Windows
OTP	One-Time Password – одноразовый пароль
OTP-токен	Электронный ключ – аппаратная реализация средства аутентификации с поддержкой OTP. Один из видов аутентификаторов, поддерживаемых сервером JAS
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
USB	Universal Serial Bus, универсальная последовательная шина
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
ПО	Программное обеспечение
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
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации

1.5 Авторские права, товарные знаки, ограничения

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

JAS RADIUS Server (JRS) представляет собой кроссплатформенный RADIUS-сервер с поддержкой двухфакторной аутентификации. Он также может выступать в качестве прокси-сервера, перенаправляя запросы в сторонние RADIUS серверы (например, NPS).

3. Системные требования

3.1 Системные требования JRS для платформы Windows

Табл. 3 – Системные требования JRS для платформы Windows

Параметр	Значение
Операционная система	• Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019
Аппаратная платформа	Процессор: 4-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

3.2 Системные требования JRS для платформы Linux

Табл. 4 – Системные требования JRS для платформы Linux

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: 4-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

4. Пакеты установки

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

Табл. 5 – Пакеты установки JAS

Файл	Описание
Aladdin.JasRadiusServer-1.0.0.xxx-x64.msi	Пакет установки JRS для среды Windows (только для 64-битных систем)
jas-radius-server_1.0.0.xxx_al_amd64.deb	deb-пакет установки JRS для среды для ОС Astra Linux
jas-radius-server_1.0.0.xxx_ro_amd64.rpm	rpm-пакет установки JRS для среды РЕД ОС
jas-radius-server_1.0.0.xxx_alt_amd64.rpm	rpm-пакет установки JRS для среды ОС Альт

5. Установка JRS на платформе Windows

Чтобы установить JRS, выполните следующие действия.

1. Запустите на выполнение файл: **Aladdin.JasRadiusServer-1.0.0.xxx-x64.msi**. Отобразится следующее окно.

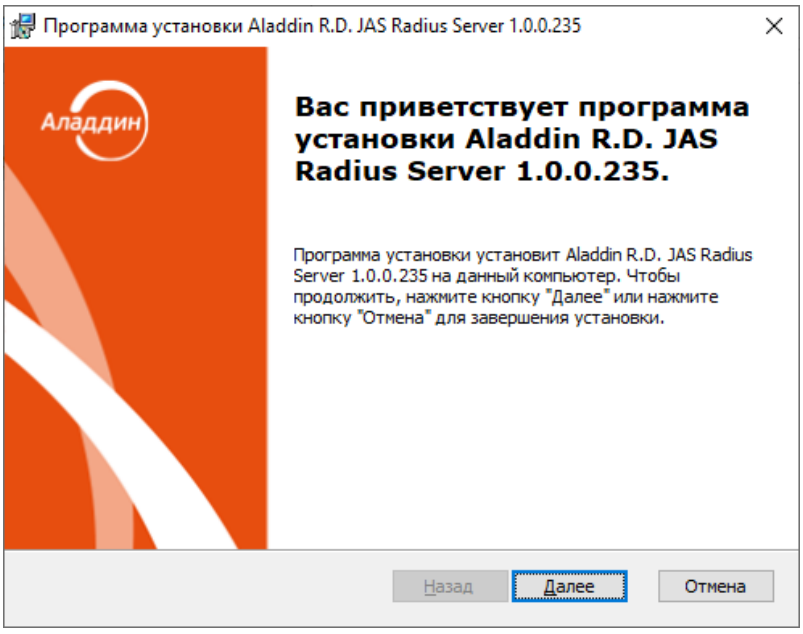

Рис. 1 – Окно приветствия мастера установки JRS

2. Нажмите **Далее**.

Отобразится следующее окно.

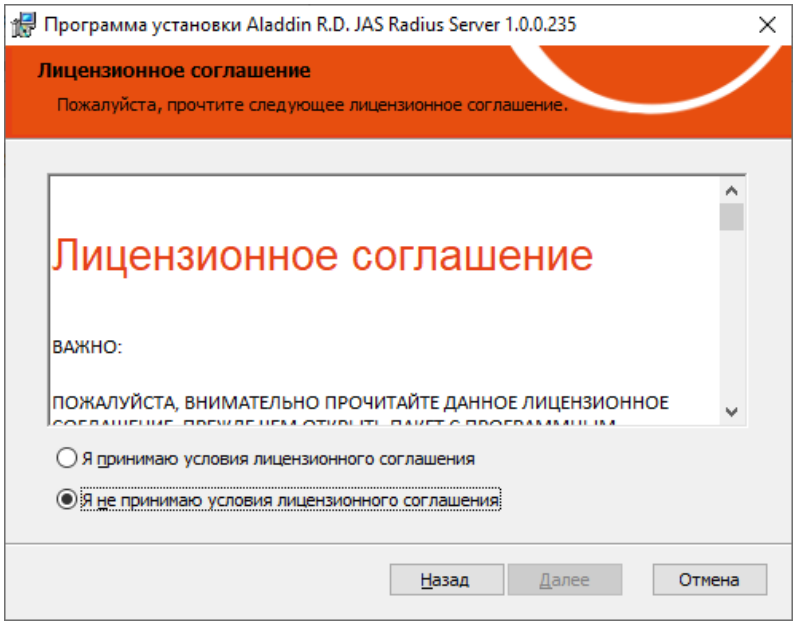

Рис. 2 – Окно лицензионного соглашения

3. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.
   На шаге выбора типа установки нажмите **Полная** и следуйте указаниям мастера до полной установки сервера.
   По завершении установки отобразится следующее окно.

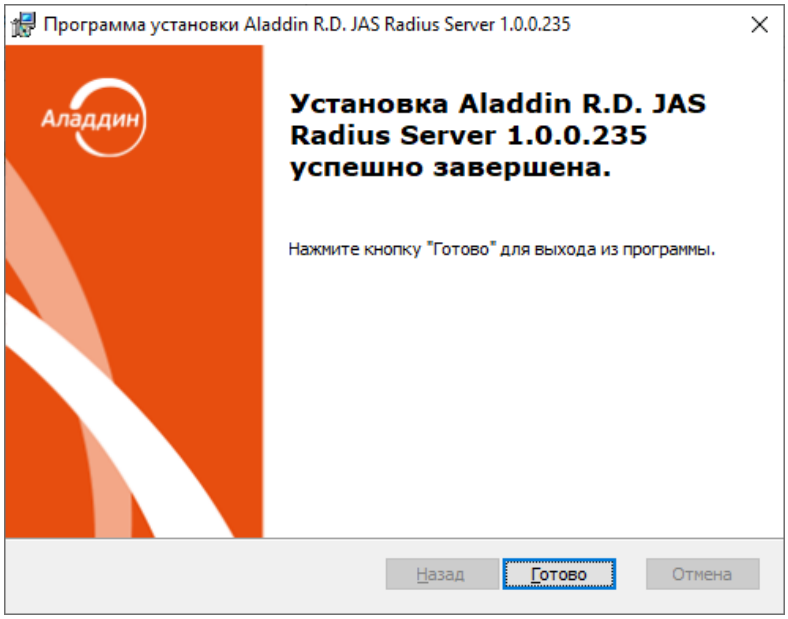

Рис. 3 – Окно завершения процедуры установки

По окончании установки JRS на компьютере будет запущена служба JasRadiusServer.

 **Важно!** Если JAS RADIUS Server и NPS установлены на одном сервере, важно, чтобы они слушали разные порты. В противном случае все пакеты будут проходить только через NPS, при этом в логе JRS ошибки не будут фиксироваться.

6. Установка JRS на платформе Linux

В зависимости от вида ОС Linux, под управлением которой работает хост, предназначенный для установки JRS, выполните соответствующую команду:

- ОС Astra Linux:

```
sudo dpkg -i jas-radius-server_1.0.0.xxx_al_amd64.deb
```

- ОС РЕД ОС:

```
sudo rpm –i jas-radius-server_1.0.0.xxx_ro_amd64.rpm
```

- ОС Альт:

```
sudo rpm –i jas-radius-server_1.0.0.xxx_alt_amd64.rpm
```

7. Удаление JRS

7.1 Удаление JRS в Windiows

Удаление JAS Radius Server выполняется стандартными средствами Windows, с использованием «Панели управления».

7.2 Удаление JRS в Linux

Для удаления JRS в на платформе Linux следует использовать стандартные пакетные менеджеры соответствующей ОС.

Например, для удаления JRS в Astra Linux выполните следующую команду:

```
sudo apt remove jas-radius-server
```

8. Настройка JRS

Настройка JRS осуществляется путем редактирование параметров в конфигурационном файле config.json

В случае платформы Windows конфигурационный файл располагается по следующему пути:

```
C:\ProgramData\Aladdin\JAS Radius Server\config.json
```

В случае платформы Linux конфигурационный файл располагается по следующему пути:

```
/etc/aladdin/jas-radius-server/config.json
```

После внесения изменений следует перезапустить службу JRS, для этого в зависимости от используемой платформы выполните следующие действия:

- **ОС Windows**: перезапустите службу JasRadiusServer (отображаемое имя "Aladdin JAS Radius Server")
- **ОС Linux:** перезапустите службу командой:

```
sudo systemctl restart jas-radius-server
```

9. Описание конфигурационного файла JRS

9.1 Пример файла config.json

Ниже приведен пример конфигурационного файла JRS config.json.

```
{
  "InboundInterface": "*:1812",
  "OutboundInterface": "*",

  "JasServiceUri": "http://192.168.10.55:8221/api/v4.1",
  "JasAuthType": "None",
  "JasUsername": "",
  "JasPassword": "",
  "JasTimeout": 50000,

  "DefaultUserDomain": "2019x64.test",

  "LdapConnections": [{
    "DomainName": "FQDN1.loc",
    "LdapServerUri": "Ldap://192.168.10.90",
    "LdapServerUsername": "fqdn1\\autotest",
    "LdapServerPassword": "123456qweRTY",
    "LdapType": "ActiveDirectory"
    "LdapContainer": "dc=fqdn1,dc=loc"
  }],
  "LdapAuthorizeGroupMember": [
    {
      "AccountSystemDomain": "FQDN1.loc",
      "Groups": [
  "FQDN1.loc\\Administrators"
],
      "ClassAttribute": "admins"
    },
    {
      "AccountSystemDomain": "FQDN1.loc",
      "Groups": [
  "FQDN1.loc\\users"
],
      "ClassAttribute": "users"
    }
  ],
  "ChallengeResponseRadiusAuth": true,
  "SecondFactorAuthFirst": true,
  "AllowChangeExpiredPassword": true,

  "CheckPasswordAgainstExternalRadiusServer": true,
  "ExternalRadiusServer": "192.168.10.90:1812",
  "ExternalRadiusServerSharedSecret": "shared-secret",
  "ExternalRadiusServerRetryCount": 3,
  "ExternalRadiusServerRetryDelay": 1000,
  "ExternalRadiusServerTimeout": 50000,

  "UserNotFoundAction": "Pass",
  "TokensNotFoundAction": "Reject",
  "CheckA2faTokenState": true,
  "A2faNotActivatedAction": "Reject",
  "AuthTypes": "OTP, Messaging, Push",
  "AuthTypeSelection": "Auto",
  "NotifyPushSuccess": true,
```

```
  "MessagingAdditionalInfo": "",
  "MessagingSystemId": "",
  "MessagingRetryDelay": 5000,
  "MessagingTtl": 180,

  "ReplyMessageCodePage": 65001,
  "Culture": "ru",
  "Clients": [{
    "RadiusClientAddress": "192.168.10.50",
    "RadiusClientName": "cisco",
    "RadiusClientSharedSecret": "shared-secret"
    },
    {
      "RadiusClientAddress": "192.168.10.1",
      "RadiusClientName": "localhost",
      "RadiusClientSharedSecret": "shared-secret"
    }
  ],
  "LocalizationCulture": "ru-RU",
  "Localization": [
  {
    "Culture": "ru-RU",
    "Select2FAMessage": "Выберите второй фактор: ",
    "OtpCodeMessage": "Введите OTP-код",
    "SMSCodeMessage": "Введите код из SMS",
    "SMSCodeMessageWithAttempts": "Введите код из SMS. Осталось попыток: ",
    "ExpiredPasswordMessage": "Срок действия пароля учетной записи истек. Смените
пароль или обратитесь к администратору",
    "NewPasswordNotMatchMessage": "Введенные пароли не совпадают",
    "NewPasswordComplexityMessage": "Пароль не соответствует требованиям сложности.
Если Вы не знаете требования к сложности пароля, обратитесь к администратору",
    "NewPasswordExpiredMessage": "Пароль пользователя истек. Введите новый пароль",
    "ConfirmPasswordMessage": "Подтвердите новый пароль",
    "MaxAttemptsExceededMessage": "Превышено максимальное количество попыток смены
пароля",
    "OtpName": "OTP",
    "MessagingName": "Messaging",
    "PushName": "Push"
  },
  {
    "Culture": "en-US",
    "Select2FAMessage": "Select 2FA method: ",
    "OtpCodeMessage": "Enter OTP code",
    "SMSCodeMessage": "Enter SMS code",
    "SMSCodeMessageWithAttempts": "Enter SMS code. Remaining attempts: ",
    "ExpiredPasswordMessage": "The user password has expired. Change your password
or contact your administrator",
    "NewPasswordNotMatchMessage": "The entered passwords do not match",
    "NewPasswordComplexityMessage": "The new password does not match the complexity
policy. If you do not know the password complexity requirements, contact your
administrator",
    "NewPasswordExpiredMessage": "User password has expired. Enter a new password",
    "ConfirmPasswordMessage": "Confirm new password",
    "MaxAttemptsExceededMessage": "The maximum number of attempts to change the
password has been exceeded",
    "OtpName": "OTP",
    "MessagingName": "Messaging",
    "PushName": "Push"
  }
],
  "HealthCheckConfig": {
    "Interfaces": "http://*:8323"
  },
  "ControlServiceWebApiConfig": {
    "SecurityType": "Basic",
    "Username": "admin",
```

```
    "Password": "password",
    "Addresses": [
      "http://localhost:8319"
    ]
  }
}
```

9.2 Описание параметров конфигурационного файла JRS

Ниже приведён перечень настроек JRS.

Табл. 6 – Настройки конфигурационного файла JRS

Настройка	Описание	Допустимые значения
InboundInterface	Сетевой интерфейс для входящих соединений. **Примечание.** Интерфейс используется для обработки запросов и ответа на входящие запросы к JRS.	Допускается указывать • `<IP>:<Port>` – конкретный сокет; • `*:<Port>` – все доступные адреса с конкретным портом; • `*` – все доступные интерфейсы
OutboundInterface	Сетевой интерфейс для исходящих соединений **Примечание.** С данного интерфейса JRS отправляет запросы на внешний RADIUS-сервер (см. параметр **ExternalRadiusServer**, ниже), если включена опция перенаправления (см. параметр **CheckPasswordAgainstExternalRadiusServer**, ниже).	Тот же формат, что и у параметра **InboundInterface** **Примечание.** Значение порта должно отличаться от порта в параметре **InboundInterface** .

JasServiceUri	Адрес сервера JAS. В зависимости от реализации сервера JAS (v 3.7.1, v4.1) следует указывать адрес соответствующего сетевого интерфейса *AuthenticationService* сервера JAS. Подробнее см.
	• Руководство по JAS 4.1 [1]
	• Руководство по JAS 3.7.1 [2]
		Строка – URL. Например:
		• **Для JAS v3.7.1:**
		`"http://<FQDN-имя сервера JAS>:8008/JASEngine/Default/AuthenticationService/rest"`
		• **Для JAS v4.1:**
		`"http://192.168.10.55:8221/api/v4.1"`

JasAuthType	Тип аутентификации JAS. Если не указаны имя пользователя и пароль для Windows-аутентификации, будут использованы учетные данные текущего пользователя. В зависимости от реализации сервера JAS (v 3.7.1, v4.1) и платформы набор допустимых опций аутентификации RADIUS-клиента на сетевом интерфейсе *AuthenticationService* может меняться. Подробнее см. • Руководство по JAS 4.1 [1] • Параметр **SecurityType**, Руководство по JAS 3.7.1 [2]	При аутентификации в JAS v 3.7.1 и v.4.1 на платформе Windows, допустимо одно из значений: • **"None"** • **"Basic"** • **"Windows"** **Примечания:** 1. Опция **Windows** включает в себя как Windows-аутентификацию, так и NTLM. Выбор протокола осуществляется автоматически 2. При интеграции с JAS v 4.1 на платформе Linux, допустимы значения **None** и **Basic**

Настройка	Описание	Допустимые значения
JasUsername	Имя пользователя, под которым JAS Radius Server будет подключаться к серверу JAS.	Строка – имя пользователя
JasPassword	Пароль пользователя, с которым JAS Radius Server будет подключаться к серверу JAS	Строка – пароль пользователя
JasTimeout	Ожидание ответа от сервера JAS (мс). По умолчанию: 50000	Число
SecurityProtocols	Поддерживаемые протоколы шифрования. По умолчанию поддерживаются все	Строка – лишние можно удалить **"Tls, Tls11, Tls12"**
Culture	Язык локализации сервера JRS (настройка влияет на язык и региональные параметры самого сервера JRS, например логи сторонних библиотек могут отображаться на указанном языке). По умолчанию **"ru"**	Строка: • **"ru"** (значение по умолчанию) • **"en"**
LdapConnections	Список (json-массив) настроек подключения к LDAP-серверам	
LdapConnections -> **DomainName**	Имя домена. Используется для проверки принадлежности пользователя группе, определённой в LDAP-справочнике, подробнее см. раздел «Настройка режимов аутентификации в JRS», с. 29	Строка. Например: **"FQDN1.loc"**
LdapConnections -> **LdapServerUri**	Адрес Ldap-сервера	Строка – URL. Например: **"Ldap://192.168.10.90"** или **"Ldaps://192.168.10.90"** (в случае подключения по защищённому протоколу)
LdapConnections -> **LdapType**	Тип LDAP	Строка: • **"ActiveDiretory"** • **"FreeIPA"**
LdapConnections -> **LdapContainer**	Точка подключения к LDAP-каталогу в случае, если подключение осуществляется не к корню домена	Строка, например: **"dc=fqdn1,dc=loc"**
LdapConnections -> **LdapServerUsername**	Имя пользователя для подключения к Ldap-серверу	Строка. 1) Доступные форматы для Active Directory:

Настройка	Описание	Допустимые значения
		a) DN (distinguished name), например: **`"CN=Administrator,CN=Users,DC=fqdn1,DC=com"`** б) Down-Level Logon Name, например: **`"fqdn1\\Administrator"`** **Примечание.** Удвоенный обратный слеш используется в связи с синтаксисом строковых значениях JSON: обратный слеш в значениях строк всегда «экранируется» в) UPN, например: Administrator@fqdn1.com 2) Допустимый формат для FreeIPA – только DN (distinguished name), например: **`"CN=Administrator,CN=Users,DC=fqdn1,DC=com"`**
LdapConnections -> **LdapServerPassword**	Пароль пользователя для подключения к Ldap-серверу	Строка
LdapAuthorizeGroupMember	Список групп для проверки членства Подробнее см. сценарии проверок в Табл. 7 с.29 и Табл. 8, с. 31. **Примечание.** Для возможности проверки принадлежности пользователя группе в AD и FreeIPA необходимо обеспечить наличие у пользователя, от чьего имени запускается сервер JRS соответствующих прав в ОС (по умолчанию данные права предоставлены всем пользователям). • В AD это -- List contents (право на перечисление объектов в контейнерах, которых находятся пользователь USER и группа GROUP), а также на права на чтение атрибута memberOf(Read group membership) пользователя USER; • Во FreeIPA это доступ атрибуту memberOf пользователя (Read User Membership), а также чтение Read groups (возможность получения группы из FreeIPA)	Массив json-объектов
LdapAuthorizeGroupMember -> **AccountSystemDomain**	Следует указать в каком из LDAP-каталогов, следует выполнять проверку принадлежности пользователя к группе. (Выбор следует осуществлять из доменных имен, ранее указанных в параметре **LdapConnections -> DomainName**, см. выше)	Строка. Например: **`"FQDN1.loc"`**

Настройка	Описание	Допустимые значения
LdapAuthorizeGroupMember -> **Groups**	Список групп, разделенных запятой, в которые должен входить пользователь для успешной аутентификации	Массив строк, например: `["FQDN.com\\Group1, FQDN.com\\Group2"]` **Примечание.** Удвоенный обратный слеш используется в связи с синтаксисом строковых значениях JSON: обратный слеш в значениях строк всегда «экранируется»
LdapAuthorizeGroupMember -> **ClassAttribute**	Значение, которое будет установлено в 25 атрибут RADIUS-пакета (RFC 2865, см. «Полезные web-ресурсы», [1], с. 64. Используется сторонними программами, такими, как Cisco ASA). Если не задано – значение атрибута не устанавливается.	Строка. Произвольное значение, например: `"users"`
SecondFactorAuthFirst	Приоритет аутентификации по второму фактору. Подробнее сценарии проверок см. в Табл. 7 с.29 и Табл. 8, с. 31. **Примечание.** Флаг удобен для предотвращения атаки на доменный пароль. При установке в true проверяться в первую очередь будет второй фактор, что защитит от перебора/блокировки доменного пароля.	Булева константа: • **true** – дополнительный фактор аутентификации (2FA) проверяется в первую очередь; • **false** (значение по умолчанию)
CheckPasswordAgainstExternalRadiusServer	Аутентификация с перенаправлением на внешний RADIUS-сервер (подробнее см. раздел «Настройка режимов аутентификации в JRS», с. 29, а также Табл. 7 с.29 и Табл. 8, с. 31).	Булева константа: • **true --** проверка значения доменного пароля осуществляется на внешнем RADIUS-сервере • **false** (значение по умолчанию) – проверка значения доменного пароля осуществляется на сервере JAS
ExternalRadiusServer	Адрес подключения к внешнему RADIUS-серверу	Строка в формате IP:Port, например: `"192.168.10.90:1812"`
ExternalRadiusServer SharedSecret	Секрет для взаимодействия с внешним RADIUS-сервером	Строка
ExternalRadiusServer RetryCount	Кол-во повторов отправки запросов на внешний RADIUS-сервер.	Число. Значение по умолчанию: **3**
ExternalRadiusServer RetryDelay	Задержка повторов отправки запросов на внешний RADIUS-сервер (мс)	Число. Значение по умолчанию: **1000**

Настройка	Описание	Допустимые значения
ExternalRadiusServer Timeout	Ожидание ответа от внешнего RADIUS-сервера (мс)	Число. Значение по умолчанию: **50000**
UserNotFoundAction	Действия JAS Radius Server, если указанный пользователь не найден в JAS-сервере. По умолчанию: **“Pass”**.	Строка: • **“Pass”** (продолжить обработку запроса, пропустить запрос, значение по умолчанию), • **“Reject”** (отклонить запрос, отказать в аутентификации)
TokensNotFoundAction	Действия JAS Radius Server, если у указанного пользователя нет активных OTP-аутентификаторов. По умолчанию: **“Reject”**.	Строка: • **“Pass”** (продолжить обработку запроса, пропустить запрос), • **“Reject”** (отклонить запрос, отказать в аутентификации, значение по умолчанию)
CheckA2faTokenState	Проверять статус активации токенов в A2FA	Булева константа: • **true** (значение по умолчанию) • **false**
A2faNotActivatedAction	Действия RadiusProxy, если у указанного пользователя нет ни одного активированного A2FA-токена. По умолчанию: **“Pass”**	Строка: • **“Pass”** (продолжить обработку запроса, пропустить запрос, значение по умолчанию), • **“Reject”** (отклонить запрос, отказать в аутентификации)
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 сервером JRS игнорируется. Примеры форматов указания полного имени пользователя (с именем домена): • **FQDN:** jasdomain.aladdin-rd.local\user • **NetBIOS:** jasdomain\user	Строка – имя домена

Настройка	Описание	Допустимые значения
	• **UPN:** user@jasdomain.aladdin-rd.local 3. В случае указания пустого значения **DefaultUserDomain** (по умолчанию) в JAS включается интеллектуальный механизм восстановления недостающего имени (по признаку 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	
ChallengeResponseRadiusAuth	Режим работы RADIUS-сервера. 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). Подробнее сценарии проверок см. в разделе «Настройка режимов аутентификации в JRS», с. 29.	Булева константа: • **true** • **false** (значение по умолчанию)
AuthTypes	Поддерживаемые типы аутентификации и их приоритет. **Важно!** Параметр использует три типа аутентификации (Messaging, OTP и Push) только при включении двухшаговой процедуры аутентификации (см. флаг "**ChallengeResponseRadiusAuth": true**, выше), в противном случае может быть использован либо метод OTP, либо метод Push, подробнее см. в разделе «Одношаговая процедура аутентификации» с. 29. 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**"	Строка. Значение по умолчанию: **"Messaging, OTP, Push"**
AuthTypeSelection	Режим выбора типа аутентификации. **Важно!** Параметр используется только при включении двухшаговой процедуры	Строка. • **“Auto”** • **“Manual”**

Настройка	Описание	Допустимые значения
	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**"	
NotifyPushSuccess	Отправлять в JAS уведомление об успешной PUSH-аутентификации.	Булева константа: • **true** (значение по умолчанию) • **false**
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.	Строка – текст сообщения
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 [4], [5], раздел «Настройка профиля выпуска Messaging-токенов») Допустимые значения: символьная строка Значение по умолчанию: пустая строка.	Строка – внешняя система
MessagingRetryDelay	Таймаут между попытками аутентификации посредством Messaging-токена (в миллисекундах), например 5000.	Число

Настройка	Описание	Допустимые значения
	Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **"ChallengeResponseRadiusAuth": true**, выше) 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. По умолчанию (т.е. если параметр не задан в конфигурационном файле JRS) 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)** или в профиле выпуска Messaging-токенов; см. руководство по функциями управления JMS [4], [5]).	
MessagingTtl	Время жизни для одноразового пароля (в секундах, напр. 180), в течение которого ответ пользователя будет актуальным. **Важно!** Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **"ChallengeResponseRadiusAuth": true**, выше). Если параметр не задан (пустое значение), 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 [4], [5]). Значение по умолчанию: пустая значение (не задано)	Число
AllowChangeExpiredPassword	Настройка возможности смены пароля пользователя через JAS при истечении срока действия пароля в домене. Допустимые значения: • **false** – смена пароля запрещена; • **true** – смена пароля разрешена; Значение по умолчанию: **false**	Булева константа: • **true** • **false** (по умолчанию)

Настройка	Описание	Допустимые значения

	Важно! Параметр используется только при включении двухшаговой процедуры аутентификации (см. флаг **"ChallengeResponseRadiusAuth": true**, выше).
	
	Примечание. Если опция смены пароля пользователя через JRS 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:
	• **для JAS v3.7** на платформе Windows файл: **`c:\Program Files\Aladdin\JaCarta Authentication Server\Aladdin.JAS.Engine.exe.config`**
	• **для JAS v4.1** на платформе Linux файл: **`/opt/jas-engine/Aladdin.JAS.Engine.dll.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"/>`	

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 качестве обозначения кодировок допускается использовать только их числовые 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. Руководство по JAS [1], [2], раздел «Выбор корректной кодировки диалогового запроса ReplyMessage при интеграции JAS со сторонними продуктами».	Число. Например: **65001** (значение по умолчанию, т.е. кодировка UTF8).
Clients	Настройки RADIUS-клиентов (JSON-массив)	JSON-массив
Clients ->	IP-адрес радиус-клиента	Строка.

Настройка	Описание	Допустимые значения
RadiusClientAddress		Например: `"192.168.10.50"`
Clients -> **RadiusClientName**	Имя радиус-клиента	Строка. Например: `"cisco"`
Clients -> **RadiusClientSharedSecret**	Значение «общего секрета» (Shared secret) RADIUS-клиента с JRS	Строка. Например: `"shared-secret"`
Clients -> **Config**	Секция (JSON-объект) переопределения настроек для отдельного RADIUS-клиента. Подробнее см. раздел «Переопределение настроек для RADIUS-клиентов», с. 28	Вложенный JSON-объект (опциональный)
LocalizationCulture	Выбор языка (кода языка), используемого для ответов Radius-клиентам (определяет секцию языка текстовок, см. ниже Localization -> **Culture**)	Строка. Например: **"ru-RU"** или **"en-US"**
Localization	Массив вариантов кастомизации текстовок. **Примечание.** Язык текстовок (русский/английский) определяется параметром **Culture (см. выше)**.	Массив JSON-объектов
Localization -> **Culture**	Код языка для текущей элемента JSON-массива *Localization*	Строка. Например: **"ru-RU"** или **"en-US"**
Localization -> **Select2FAMessage**	Сообщение выбора второго фактора	Строка Например: `"Выберите второй фактор: "`
Localization -> **OtpCodeMessage**	Сообщение ввода OTP	Строка Например: `"Введите OTP-код"`
Localization -> **SMSCodeMessage**	Сообщение ввода кода из СМС	Строка Например: `"Введите код из SMS"`
Localization -> **SMSCodeMessageWithAttempts**	Сообщение ввода кода из СМС с количеством оставшихся попыток	Строка Например: `"Введите код из SMS. Осталось попыток: "`

Настройка	Описание	Допустимые значения
Localization -> **ExpiredPasswordMessage**	Сообщение о истекшем сроке действия пароля	Строка Например: `"Срок действия пароля учетной записи истек. Смените пароль или обратитесь к администратору"`
Localization -> **NewPasswordNotMatchMessage**	Сообщение о несовпадении нового пароля и подтверждения	Строка Например: `"Введенные пароли не совпадают"`
Localization -> **NewPasswordComplexityMessage**	Сообщение о несоответствии сложности пароля политике	Строка Например: `"Пароль не соответствует требованиям сложности. Если Вы не знаете требования к сложности пароля, обратитесь к администратору"`
Localization -> **NewPasswordExpiredMessage**	Сообщение с запросом нового пароля	Строка Например: `"Пароль пользователя истек. Введите новый пароль"`
Localization -> **ConfirmPasswordMessage**	Сообщение с запросом подтверждения нового пароля	Строка Например: `"Подтвердите новый пароль"`
Localization -> **MaxAttemptsExceededMessage**	Сообщение о превышении количества неправильных попыток ввода пароля	Строка Например: `"Превышено максимальное количество попыток смены пароля"`
Localization ->	Название для OTP метода аутентификации	Строка

Настройка	Описание	Допустимые значения
OtpName		Например: `"OTP"`
Localization -> **MessagingName**	Название для Messaging метода аутентификации	Строка Например: `"Messaging"`
Localization -> **PushName**	Название для Push метода аутентификации	Строка Например: `"Push"`
HealthCheckConfig	Секция (JSON-объект) настройки интерфейсов с которых будет отдаваться статус JRS	JSON-объект
HealthCheckConfig -> **Interfaces**	Сетевой интерфейс для проверки статуса JRS	Конкретный IP:Port или все доступные интерфейсы. Например: `"http://*:8323"`
ControlServiceWebApi Config	Секция настроек интерфейса управления сервером (например, для подключения web-консоли сервера JRS).	JSON-объект
ControlServiceWebApi Config -> **SecurityType**	Тип аутентификации	Строка – **“None”** или **“Basic”** По умолчанию **“Basic”**
ControlServiceWebApi Config -> **Username**	Имя пользователя для доступа к API, исп. при типе аутентификации **“Basic”**	Строка. По умолчанию **“admin”**
ControlServiceWebApi Config -> **Password**	Пароль пользователя для доступа к API, исп. при типе аутентификации “Basic” (Порядок установки пароля см. в разделе «Установка пользователя и пароля для аутентификации в Web-консоли», с. 36)	Строка По умолчанию **“password”**
ControlServiceWebApi Config -> **Addresses**	Список интерфейсов для доступа к API	Массив строк в формате «IP:Port» Значение по умолчанию: **“localhost:8319”**
ControlServiceWebApi Config -> **Thumbprint**	Отпечаток сертификата, используемый при SSL	Строка

9.2.1 Переопределение настроек для RADIUS-клиентов

Для того чтобы переопределить настройки для отдельного (отдельных) RADIUS-клиента (ов), в соответствующем данному клиенту элементе JSON-массива "Clients" необходимо добавить JSON-объект "Config", содержащий переопределяемые настройки. Список настроек, доступных для переопределения:

- JasServiceUri
- JasAuthType
- JasUsername
- JasPassword
- JasTimeout
- LdapAuthorizeGroupMember (требует переопределения также вложенных параметров – *Groups* и *ClassAttribute*; второй, если предусмотрен)
- SetClassAttribute
- ClassAttributeValue
- SecondFactorAuthFirst
- CheckPasswordAgainstExternalRadiusServer
- ExternalRadiusServer
- ExternalRadiusServerSharedSecret
- ExternalRadiusServerRetryCount
- ExternalRadiusServerRetryDelay
- ExternalRadiusServerTimeout
- UserNotFoundAction
- TokensNotFoundAction
- DefaultUserDomain
- ChallengeResponseRadiusAuth
- AuthTypes
- AuthTypeSelection
- MessagingAdditionalInfo
- MessagingSystemId
- MessagingRetryDelay
- MessagingTtl
- AllowChangeExpiredPassword
- ReplyMessageCodePage
- NotifyPushSuccess
- LocalizationCulture

Пример переопределения настройки SecondFactorAuthFirst для клиента "cisco":

```
{
"InboundInterface": "…",
...
"Clients": [{
    "RadiusClientAddress": "192.168.10.50",
    "RadiusClientName": "cisco",
    "RadiusClientSharedSecret": "shared-secret",
    "Config": {
           "SecondFactorAuthFirst": true
        }
    },
    {
      "RadiusClientAddress": "192.168.10.1",
      "RadiusClientName": "localhost",
      "RadiusClientSharedSecret": "shared-secret"
    }
  ]
...
}
```

9.3 Настройка режимов аутентификации в JRS

9.3.1 Одношаговая процедура аутентификации

Одношаговая процедура аутентификации в JRS устанавливается значением параметра конфигурационного файла "ChallengeResponseRadiusAuth": false (см. Табл. 6, с. 16).

Данный порядок аутентификации установлен по умолчанию.

В зависимости от настройки параметра AuthTypes (OTP или Push) проверка выполняется следующим образом:

- Приоритет у **"OTP"** – с помощью OTP-токена выполняется проверка второго фактора так, как он определен параметром «Режим аутентификации» соответствующего профиля выпуска данного токена. (Режим аутентификации может включать в себя как просто значение OTP-кода, так и его различные сочетания с доменным паролем и PIN-кодом, подробнее см. руководство по функциями управления JMS [4], [5])
- Приоритет у **"Push"** – в процессе аутентификации пользователь вводит логин и доменный пароль, после чего подтверждает Push-аутентификацию в мобильном приложении.

Примечание. Messaging-токены (см. руководство по функциями управления JMS [4], [5]) не могут использоваться в сценарии одношаговой процедура аутентификации, поскольку требуют предварительного шага отправки логина пользователя, и если значение "Messaging" будет перечислено в параметре AuthTypes, то будет оно будет пропущено.

При установке значения параметра **LdapAuthorizeGroupMember** в одношаговой процедуре аутентификации будет выполнена также проверка принадлежности пользователя к группе (подробнее см. Табл. 7, ниже).

Табл. 7 – Сценарии (последовательности проверок) при одношаговой процедуре ("ChallengeResponseRadiusAuth": false)

№ п/п	SecondFactorAuthFirst	CheckPasswordAgainstExternalRadiusServer	LdapAuthorizeGroupMember	Сценарий
1	false	false	Пусто	• Для **"AuthTypes": "OTP"**—проверить OTP (или его комбинацию с паролем и PIN) в JAS. • Для **"AuthTypes": "Push"** – проверить доменный пароль в JAS, а затем выполнить подтверждение Push
2	false	false	Fqdn1.com\Admins	Выполнить базовые проверки (сценарий 1), а затем проверить принадлежность пользователя к группе Fqdn1.com\Admins
3	false	false	Fqdn1.com\Admins,Fqdn2.net\users	Выполнить базовые проверки (сценарий 1), а затем проверить принадлежность пользователя к группе Fqdn1.com\Admins **ИЛИ** группе Fqdn2.net\users
4	false	true	Пусто	• Для **"AuthTypes": "OTP"**—В поле аутентификационных данных вводится только доменный пароль, проверка которого выполняется на внешнем RADIUS-сервере. (Значения второго фактора не вводятся и в процессе аутентификации пользователя не используются). • Для **"AuthTypes": "Push"** –Выполнить сценарий 1, но с проверкой пароля на внешнем RADIUS-сервере)

№ п/п	SecondFactorAuthFirst	CheckPasswordAgainstExternalRadiusServer	LdapAuthorizeGroupMember	Сценарий
5	false	true	Fqdn1.com\Admins	Выполнить сценарий 4, а затем проверить принадлежность пользователя к группе Fqdn1.com\Admins
6	true	false	Пусто	• Для **"AuthTypes": "OTP"**— то же, что при сценарии 1. • Для **"AuthTypes": "Push"**— выполнить подтверждение Push, а затем проверить доменный пароль в JAS
7	true	true	Пусто	• Для **"AuthTypes": "OTP"** – то же, что при сценарии 4. • Для **"AuthTypes": "Push"** – выполнить подтверждение Push, а затем проверить доменный пароль во внешнем RADIUS-сервере
8	true	true	Fqdn1.com\Admins	Выполнить сценарий 7, а затем проверить принадлежность пользователя к группе Fqdn1.com\Admins

9.3.2 Двухшаговая процедура аутентификации

Двухшаговая процедура аутентификации включает в себя последовательную проверку доменного пароля и второго фактора аутентификации. Данный сценарий определяется флагом "ChallengeResponseRadiusAuth": true (см. Табл. 6, с. 16).

Предусматриваются ситуации, когда у пользователя может быть одновременно установлено несколько типов токенов для генерации одноразового пароля (включая OTP-, Messaging-, PUSH-токены), этот сценарий предусматривает дополнительный этап, связанный с выбором типа токена (типа второго фактора аутентификации), который может осуществляться как с участием пользователя, так и автоматически (см. параметр **AuthTypeSelection**)

Кроме того, на ход аутентификации влияют другие настройки конфигурационного файла (Табл. 6, с. 16), а именно следующие параметры:

- проверка доменных имени пользователя и пароля в JAS или в стороннем RADIUS-сервере – CheckPasswordAgainstExternalRadiusServer (false – проверка осуществляется в JAS, true – проверка осуществляется на внешнем RADIUS-сервере, настройки подключения к которому указаны в параметрах, начинающихся с ExternalRadiusServer…);
- проверка второго фактора (2FA) в первую очередь – SecondFactorAuthFirst (true – «второй фактор первым»);
- возможность смены истекшего пароля – AllowChangeExpiredPassword (true – разрешить смену пароля, т.е. в процессе аутентификации запускается дополнительная процедура смены устаревшего пароля);
- проверка принадлежности пользователя к группе, определенной в секции (JSON-массиве) LdapAuthorizeGroupMember (для возможности проверки в секции LdapConnections должны быть определены настройки подключения к соответствующему LDAP-каталогу, значение параметра DomainName которого совпадает с доменом в имени группы) ;
- установка способа выбора второго фактора аутентификации – ручного (по инициативе пользователя) или автоматического – AuthTypeSelection (Auto – автоматический, Manual – ручной);
- установка, при необходимости, значение параметра ClassAttribute (подробнее в Табл. 6, с. 16)).

Подробнее настройка сценариев (последовательностей аутентификационных проверок) описана в Табл. 8, ниже.

Табл. 8 – Сценарии (последовательности проверок) при двухшаговой процедуре ("ChallengeResponseRadiusAuth": true)

№ п/п	SecondFactorAuthFirst	CheckPasswordAgainstExternalRadiusServer	LdapAuthorizeGroupMember	Сценарий
1	false	false	Пусто	Проверить доменный пароль в JAS -> Проверить OTP
2	false	false	Fqdn1.com\Admins	Проверить доменный пароль в JAS -> Проверить OTP -> Проверить принадлежность пользователя к группе Fqdn1.com\Admins
3	false	false	Fqdn1.com\Admins,Fqdn2.net\users	Проверить доменный пароль в JAS -> Проверить OTP -> Проверить принадлежность пользователя к группе Fqdn1.com\Admins **ИЛИ** группе Fqdn2.net\users
4	false	true	Пусто	Проверить доменный пароль в RADIUS-сервере -> Проверить OTP
5	false	true	Fqdn1.com\Admins	Проверить доменный пароль в RADIUS-сервере -> Проверить OTP -> Проверить принадлежность пользователя к группе Fqdn1.com\Admins
6	true	false	Пусто	Проверить OTP -> Проверить доменный пароль в JAS
7	true	true	Пусто	Проверить OTP -> Проверить доменный пароль в RADIUS-сервере
8	true	true	Fqdn1.com\Admins	Проверить OTP -> Проверить доменный пароль в RADIUS-сервере -> Проверить принадлежность пользователя к группе Fqdn1.com\Admins

9.4 Проверка доступности JRS (healthy-статус)

Настройка Http API для проверки healthy-статуса сервера JRS (например для балансировщиков нагрузки в кластере Corosync) осуществляется с помощью параметра "HealthCheckConfig" конфигурационного файла, например:

```
…
"HealthCheckConfig": {
    "Interfaces": "http://*:8323”
}
```

При приведенном в этом примере значении настройки можно посмотреть статус по адресу:

```
http://localhost:8323/healthz
```

В случае штатной работы возвращается страница со строкой статуса (например «Healthy») и кодом состояния HTTP «200».

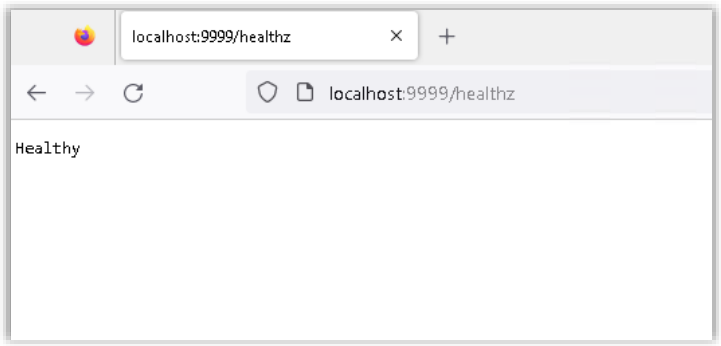

Рис. 4 – Страница отклика от исправно функционирующего сервера JRS

Сервис возвращает состояние JRS и его зависимостей: подключение к JAS, LDAP-каталогам, стороннему RADIUS-серверу. Состояние каждого из компонентов может быть одним из трех: Healthy, Degraded, Unhealthy. Если какой-то компонент находится в состоянии ошибки или ответ от него не пришел, то в этом случае у него будет установлен статус Unhealthy. Если сервис ответил, но время ответа превысило таймаут, данный сервис получает статус Degraded. В случае исправной работы– Healthy. Общий статус устанавливается следующим образом: если хотя бы один из компонентов вернул статус Unhealthy, то общий статус будет Unhealthy; если один из компонентов вернул статус Degraded, а остальные находятся в состоянии Healthy, то общий статус будет Degraded. Общий статус Healthy выставляется в случае, если все компоненты вернули Healthy.

9.5 Настройка параметров ведения журнала событий в JRS

Настройки параметров журналирования находятся в файле Aladdin.JasRadiusServer.log4net.

Сервер JRS 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.

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

Для изменения уровня журналирования необходимо указать в теге level одно из указанных выше значений.

Ниже приведен пример конфигурационного файла журналирования:

```
<?xml version="1.0" encoding="utf-8"?>
<log4net>
    <appender name="JasRadiusServer" type="log4net.Appender.RollingFileAppender">
        <file value="/var/log/aladdin/jas-radius-server/Engine.log"/>
```

```
        <appendToFile value="true"/>
        <encoding value="utf-8"/>
        <maxSizeRollBackups value="10"/>
        <maximumFileSize value="10MB"/>
        <rollingStyle value="Size"/>
        <datePattern value="yyyyMMdd"/>
        <layout type="log4net.Layout.PatternLayout">
            <conversionPattern value="%date [%property{ProcessId}] [%thread] %-
5level %logger - %message%newline"/>
        </layout>
    </appender>
    <appender name="Console" type="log4net.Appender.ConsoleAppender">
        <layout type="log4net.Layout.PatternLayout">
            <conversionPattern value="%date [%property{ProcessId}] [%thread] %-
5level %logger - %message%newline"/>
        </layout>
    </appender>
    <root>
        <level value="ALL"/>
        <appender-ref ref="JasRadiusServer"/>
        <appender-ref ref="Console" />
    </root>

</log4net>
```

10.Web-консоль сервера JRS

Web-консоль сервера JRS предоставляет графические средства конфигурирования сервера JRS

10.1 Дистрибутив

Табл. 9 – Установочные пакеты Web-консоли сервера JRS

ОС	Файл дистрибутива	Описание
Astra Linux	**aladdin-jrs-web-server-console_4.1.0.xxxx_x64.deb**	Серверное приложение Web-консоли сервера JRS, может устанавливаться как на сервер JRS, так и на другой компьютер в домене

10.2 Системные требования

Перечень требований к среде функционирования Web-консоли сервера JRS приведен в Формуляре [6], с. 64.

Примечание. Для корректного отображения информации в Web-консоли предъявляется дополнительное требование к минимальному разрешению видеоинтерфейса: 1280 x 720.

10.3 Установка Web-консоли

Порядок установки и первоначальной настройки web-консоли на хосте сервера JRS приведен для среды ОС Astra Linux 1.7.5.

Для установки Web-консоли сервера JRS выполните команду

```
dpkg -i aladdin-jrs-server-console_4.1.0.xxxx _x64.deb
```

После установки консоль становится доступной по адресу http://localhost:5020

Стартовая страница с приглашением имеет следующий вид.

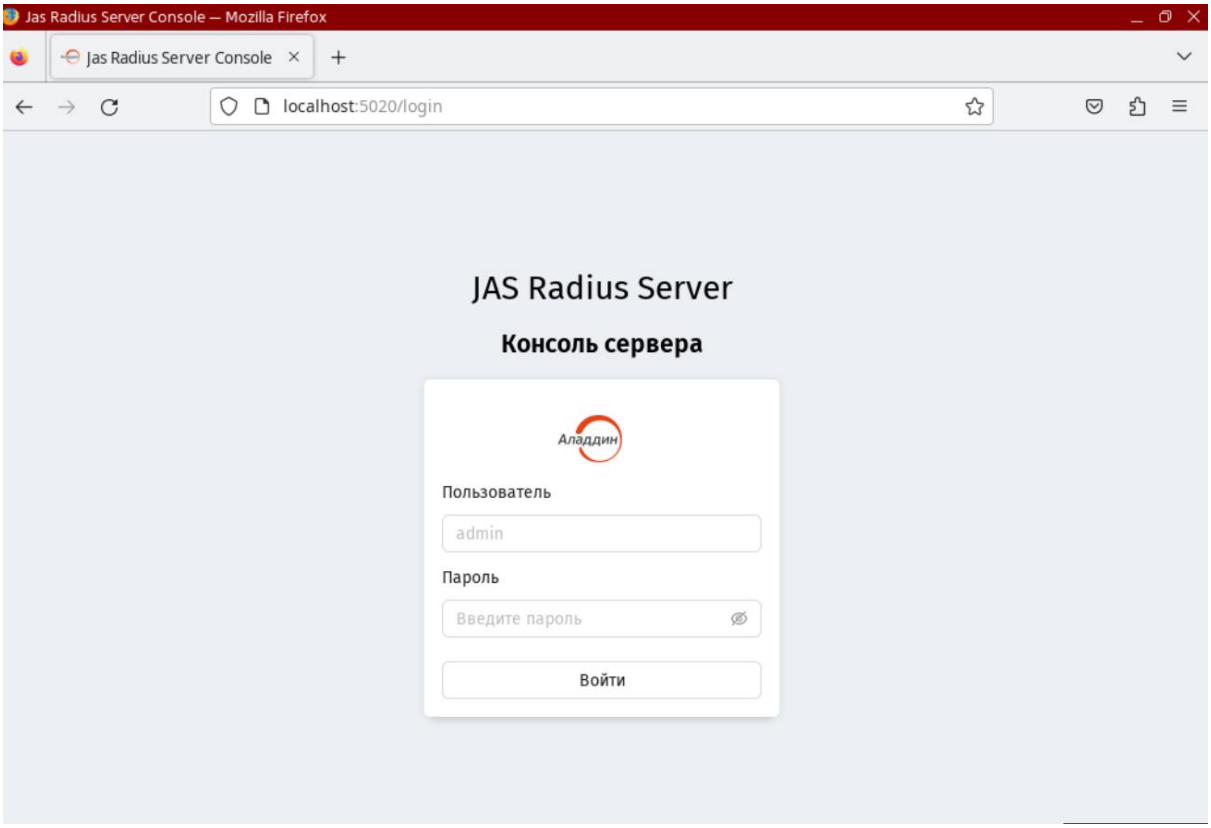

Рис. 5 – Приглашение для входа Web-консоли сервера JRS

10.4 Первоначальная настройка Web-консоли

Перед использование Web-консоли сервера JRS приложение необходимо с конфигурировать. Конфигурирование осуществляется путем редактирования конфигурационного файла.

Файл конфигурации серверного приложения Web-консоли доступен по пути `/etc/aladdin/jrs-web-server-console/appsettings.json`

Ниже приведён образец файла конфигурации web-консоли JRS.

```
{
  "AllowedHosts": "*",

  "Kestrel": {
    "Endpoints": {
      "Http": {
        "Url": "http://0.0.0.0:5020"
      }
    }
  },
```

```
  "CookiesSettings": {
    "KeysDir": "keys",
    "AccessTokenLifetime": 5,
    "RefreshTokenLifetime": 30
  },

  "ServerConnectionSettings": {
    "ControlApiUrl": "http://localhost:8319",
    "HealthCheckApiUrl": "http://localhost:8323",
    "PingTimeout": 5
  },

  "ResourceConsumptionLimitsSettings": {
    "CpuWarning": 40,
    "CpuBad": 75,
    "MemoryWarning": 400,
    "MemoryBad": 600
  }
}
```

Если web-консоль устанавливается на компьютере, отличном от сервера JRS, то в файле конфигурации в секции ServerConnectionSetttings необходимо изменить адреса подключения к серверу JRS (ControlApiUrl и HealthCheckApiUrl), например, как показано на рисунке ниже.

Рис. 6 – Корректировка адресов подключения к серверу JRS

Если необходимо изменить адрес и порт сервера web консоли по умолчанию, то в файле конфигурации необходимо изменить адрес консоли в секции Kestrel.

Рис. 7 – Корректировка адреса сервера web-консоли JRS

10.5 Установка пользователя и пароля для аутентификации в Web-консоли

Для обеспечения аутентификации в web-консоли необходимо установить имя пользователя и его пароля, которые указываются в файле конфигурации `/etc/aladdin/jas-radius-server/config.json` в секции `ControlServiceWebApiConfig`, как показано ниже.

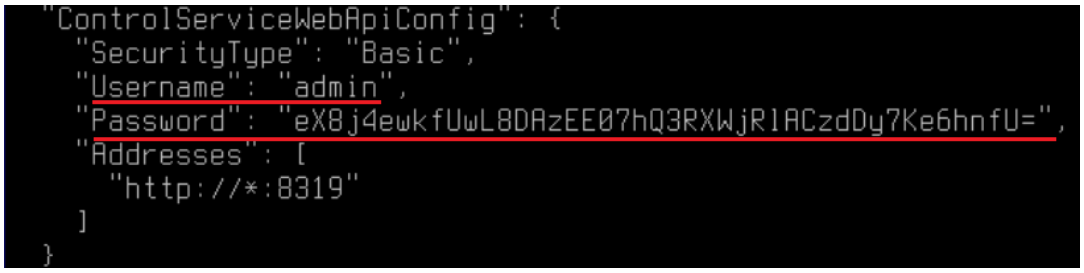

Рис. 8 – Место указания имени пользователя и его пароля для аутентификации в web-консоли

В параметре "Password" необходимо задать в явном виде пароль пользователя, после чего перезапустить демон следующей командой

```
systemctl restart jas-radius-server.service
```

После перезагрузки демона пароль в файле конфигурации демона будет зашифрован.

10.6 Проверка работы Web-консоли

Для аутентификации в консоли необходимо указать имя пользователя и его пароль, настроенные в разделе «Установка пользователя и пароля для аутентификации в Web-консоли», см. выше.

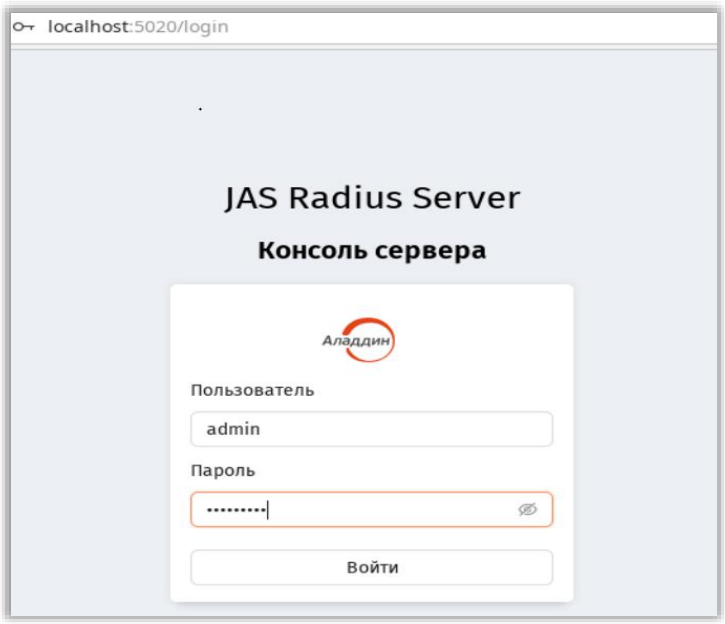

Рис. 9 – Аутентификация в web-консоли

После аутентификации можно приступать к конфигурированию сервера (подробнее см. раздел «Работа с Web-консолью сервера JRS», ниже)

11.Работа с Web-консолью сервера JRS

При открытии консоли страница принимает следующий вид.

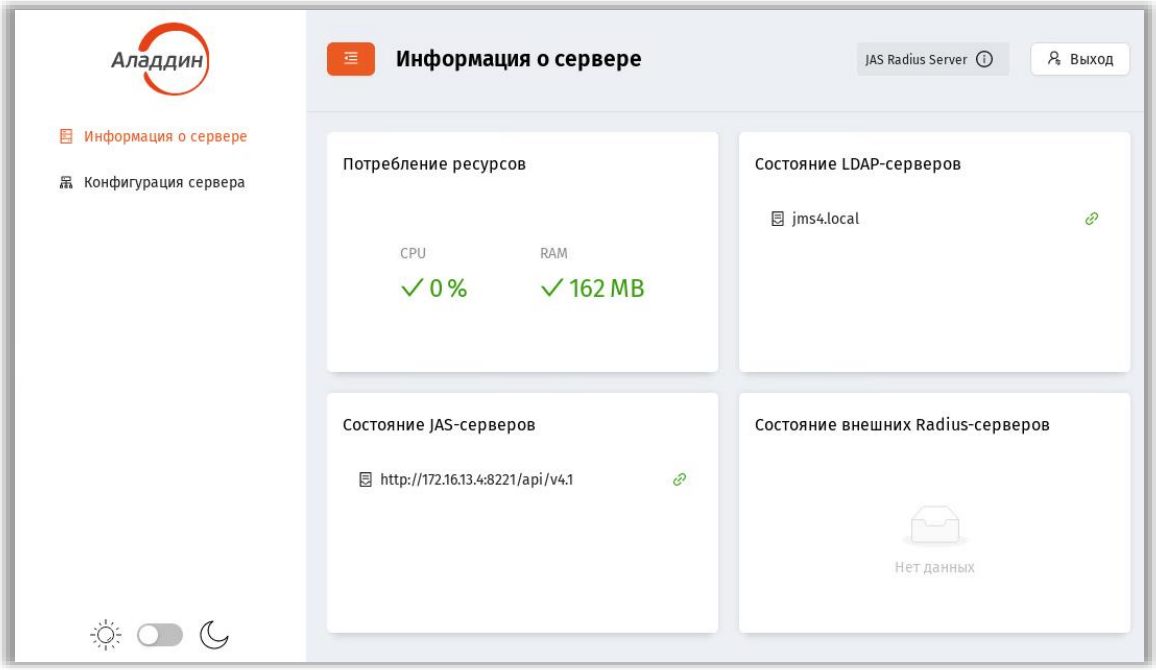

Рис. 10 – Стартовая страница web-консоли сервера JRS

Ниже описано назначение основных разделов web-консоли сервера JRS (табл. 10).

Табл. 10 – Разделы стартовой страницы web-консоли сервера JRS

Раздел	Описание и ссылка на соответствующий подраздел
Информация о сервере	Отображает статус сервера JRS, отображает его базовые настройки, информацию о подключении к серверам JAS и внешним RADIUS-серверам (подробнее см. «Информация о сервере», с. 38).
Конфигурация сервера	Позволяет в графическом интерфейсе выполнить настройку всех конфигурационных параметров сервера JRS. Подробнее см. «Конфигурация сервера», с. 39.

11.1 Информация о сервере

Раздел **Информация о сервере** web-консоли выглядит следующим образом (см. рис. 11).

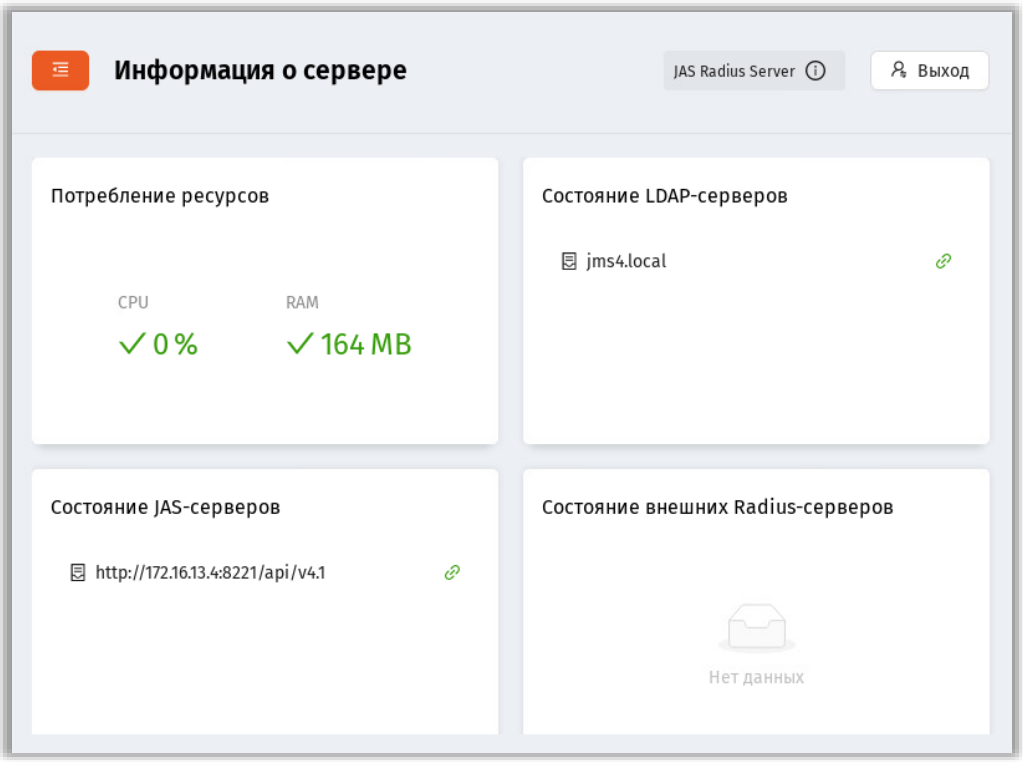

*Рис. 11 – Раздел **Информация о сервере***

Раздел **Информация о сервере** содержит следующие элементы (см. табл. 11).

Табл. 11 – Раздел Информация о сервере

Фрейм	Описание
Потребление ресурсов	Отображает занимаемую сервером оперативную память и потребление ресурсов процессора
Состояние LDAP-серверов	Отображает ресурсные системы, используемые сервером JRS и статус подключения к ним.
Состояние JAS-серверов	Отображает серверы JAS, используемые сервером JRS, и статус подключения к ним.
Состояние внешних RADIUS-серверов	Отображает внешние серверы RADIUS, используемые сервером JRS, и статус подключения к ним.

11.2 Конфигурация сервера

Раздел **Конфигурация сервера** выглядит следующим образом.

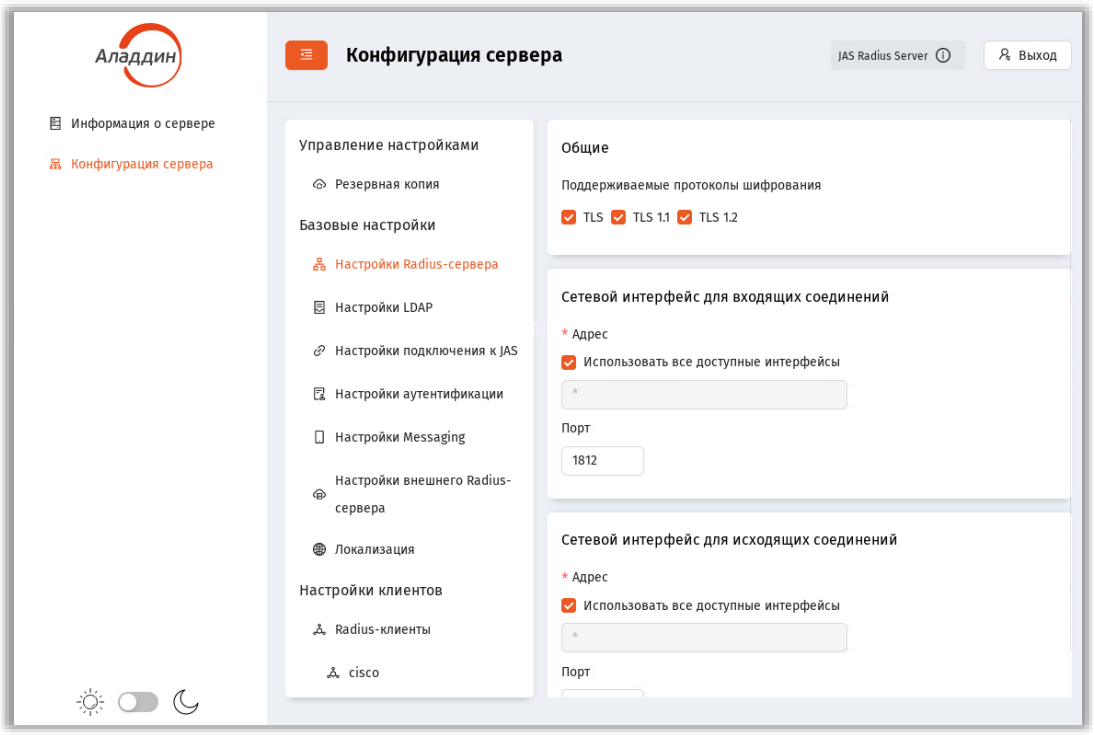

*Рис. 12 – Страница раздела **Конфигурация сервера***

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

Табл. 12 – Элементы раздела Конфигурация сервера

Элемент интерфейса	Описание
Секция **Управление настройками**	
Резервная копия	Позволяет сохранить или восстановить файл конфигурации сервера JRS. • Для сохранения резервной копии файла конфигурации нажмите **Экспорт**. Резервная копия json-файла конфигурации будет сохранена в каталог загрузок (download) браузера • Для восстановления конфигурации сервера JRS из резервной копии файла конфигурации нажмите **Импорт** и выберите резервный json-файл конфигурации сервера.
Секция **Базовые настройки**	
Настройки Radius-сервера	Позволяет выполнить основные настройки работы JRS по протоколу RADIUS, подробнее см. «Настройки RADIUS-сервера», с. 40

Элемент интерфейса	Описание
Настройки LDAP	Позволяет выполнить подключение к новым ресурсным системам и выполнить настройки связи с уже подключенными ресурсными системами, подробнее см. «Настройки LDAP», с. 42
Настройки подключения к JAS	Позволяет выполнить настройки подключения к серверу JaCarta Authentication Server (JAS, подробнее см. «Настройки подключения к JAS», с. 46
Настройки аутентификации	Позволяет настроить такие параметры аутентификации, как типы используемых аутентификаторов (OTP, Messsaging, Push), порядок их применения, сценарии одно- и двухшаговых процедур аутентификации и др., подробнее см. «Настройки аутентификации», с. 48
Настройки Messaging	Позволяет настроить параметры аутентификации типа Messaging, подробнее см. «Настройки Messaging», с. 51
Настройки внешнего Radius-сервера	Позволяет настроить параметры аутентификации с помощью внешнего RADIUS-сервера, подробнее см. «Настройки внешнего RADIUS-сервера», с. 53
Локализация	Позволяет настроить язык текстовых сообщений, используемых при взаимодействии с пользователем RADIUS-сервера, подробнее см. «Настройки локализации (языка пользовательского интерфейса RADIUS)», с. 55
Секция **Настройки клиентов**	
Radius-клиенты	Позволяет настроить параметры используемых RADIUS-клиентов, в частности переопределить установленные по умолчанию параметры в сервере JRS для выбранного RADIUS-клиента, подробнее см. «Настройки RADIUS-клиентов», с. 58
cisco	Типовая запись настройки RADIUS-клиента на примере межсетевого экрана Cisco ASA (может быть переопределена или удалена), подробнее см. «Настройки RADIUS-клиентов», с. 58
localhost	Типовая запись настройки RADIUS-клиента на примере локального хоста сервера JRS (может быть переопределена или удалена), подробнее см. «Настройки RADIUS-клиентов», с. 58

11.2.1 Настройки RADIUS-сервера

Страница **Настройка Radius-сервера** выглядит следующим образом.

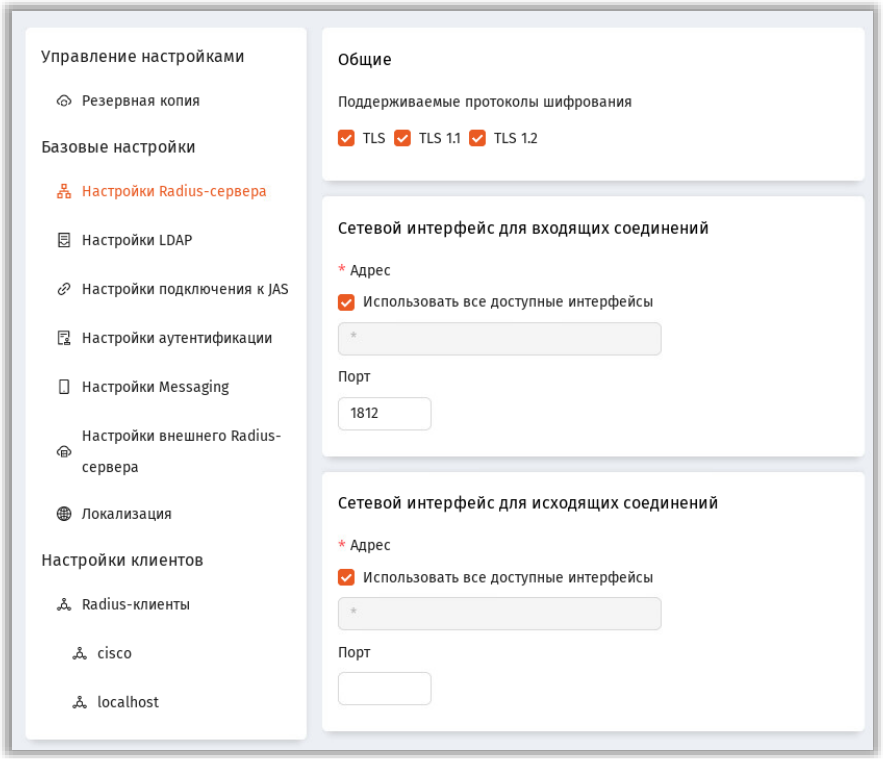

*Рис. 13 – Страница **Настройка Radius-сервера***

Выполните настройку, руководствуясь Табл. 13.

Табл. 13 – Настройки Radius-сервера

Настройка	Описание
<Фрейм> **Общие**	
Поддерживаемые протоколы	При необходимости настройте поддерживаемые протоколы шифрования SSL/TLS. • **TLS** – TLS 1.0 • **TLS 1.1** • **TLS 1.2** По умолчанию все флаги установлены. (Соответствует параметру *SecurityProtocols* конфигурационного файла)
<Фрейм> **Сетевой интерфейс для входящих соединений**	
Адрес	Укажите IP- адрес интерфейса для входящих соединений и порт сокета в поле **Порт** В случае если должны прослушиваться все доступные сокеты, установите флаг **Использовать все доступные интерфейсы** (Соответствует параметру *InboundInterface* конфигурационного файла)

Настройка	Описание
<Фрейм> **Сетевой интерфейс для исходящих соединений**	
Адрес	Укажите IP- адрес интерфейса для исходящих соединений и порт сокета в поле **Порт** В случае если должны использоваться все доступные сокеты, установите флаг **Использовать все доступные интерфейсы** (Соответствует параметру *OutboundInterface* конфигурационного файла)

По завершении настройки нажмите **Сохранить**.

11.2.2 Настройки LDAP

Страница **Настройки LDAP** выглядит следующим образом.

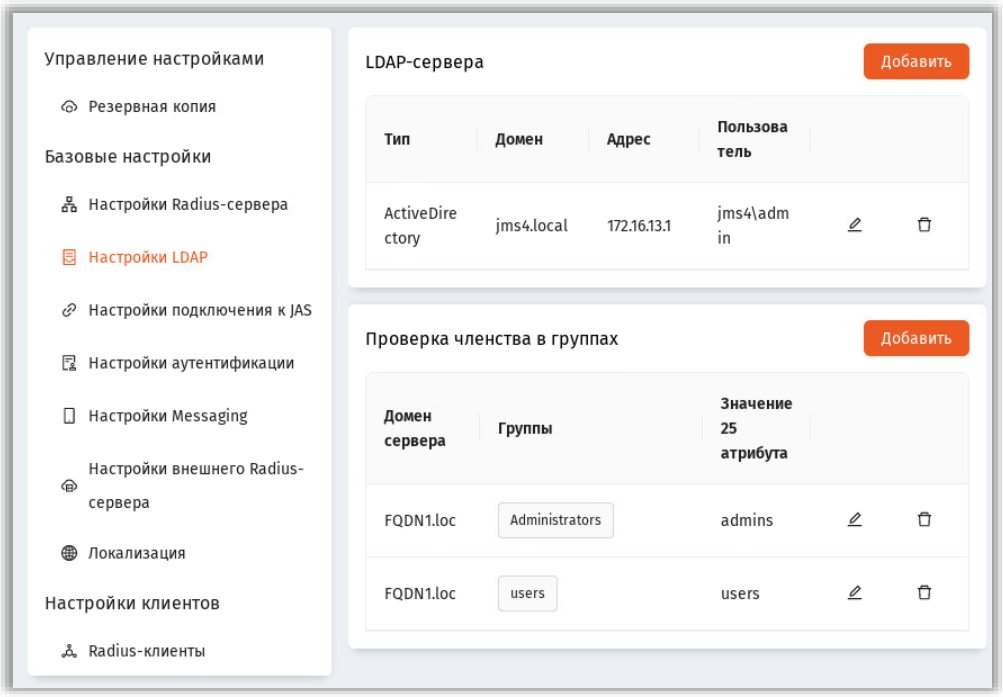

Рис. 14 – Страница Настройки LDAP

Выполните настройку, руководствуясь Табл. 14.

Табл. 14 – Настройки подключения к серверам LDAP

Настройка	Описание
<Секция> **LDAP-сервера**	
<Фрейм > **LDAP-сервера**	Таблица с параметрами подключенных LDAP-адресов. Во фрейме LDAP-сервера можно добавить, отредактировать или удалить параметры подключения к LDAP-серверу

Настройка	Описание
	(Параметр в конфигурационном файле: *LdapConnections*)
<Фрейм > **Проверка членства в группах**	Таблица определяет список групп для проверки принадлежности им пользователя, выполняющего аутентификацию. Таблица позволяет выполнять управление записями о членстве в группе (добавлять записи, редактировать и удалять). Порядок управления записями приведен на примере операции добавления (см. «Добавление правила проверки принадлежности группе», с. 45). (Параметр в конфигурационном файле: *LdapAuthorizeGroupMember*)

По завершении настройки нажмите **Сохранить**. (Внесение изменений в конфигурацию сервера потребует его автоматической перезагрузки.)

11.2.2.1 Подключение к LDAP-серверу (Добавить LDAP)

Для подключения к LDAP-серверу выполните следующие действия

1. В разделе **Конфигурация сервера** web-консоли выберите подраздел **Настройки LDAP** и во фрейме **LDAP-сервера** нажмите **Добавить**.

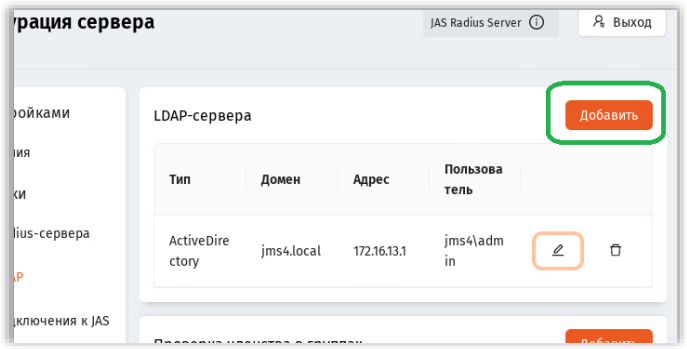

Рис. 15 – Добавление LDAP-сервера

2. Отобразится форма добавления LDAP-сервера.

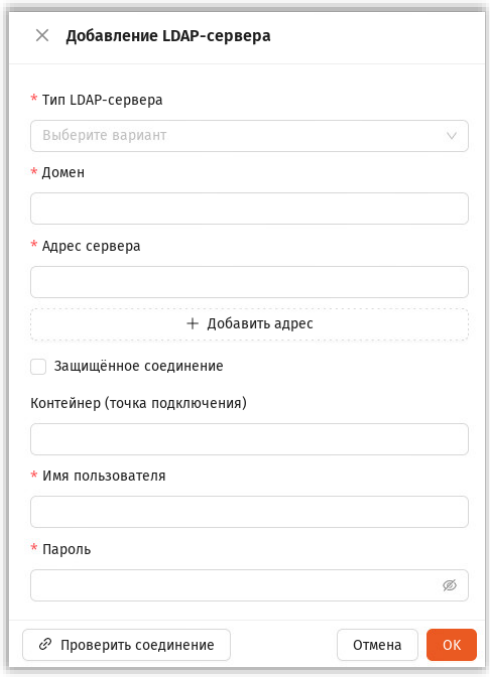

Рис. 16 – Форма параметров подключения к LDAP-серверу

3. Выполните настройки, руководствуясь Табл. 15.

Табл. 15 – Настройки подключения к LDAP-серверу

Элемент интерфейса	Описание
Тип LDAP-сервера	Выберите тип LDAP-сервера, к которому необходимо подключиться: • **ActiveDirectory** • **FreeIPA** • **ALD Pro** • **Samba AD** (Соответствует параметру *LdapConnections -> LdapType* конфигурационного файла, Табл. 6, с. 16.)
Домен	Введите полное доменное имя для подключаемого LDAP-сервера, например: *jms4.local* (Соответствует параметру *LdapConnections -> DomainName* конфигурационного файла, Табл. 6, с. 16.)*l*
Адрес сервера	Введите IP-адрес LDAP-сервера. (Соответствует параметру *LdapConnections -> LdapServerUri* конфигурационного файла, Табл. 6, с. 16.)
Защищённое соединение	Установите флаг, если подключение к серверу должно производиться по протоколу SSL/TLS. (в параметре *LdapConnections -> LdapServerUri* конфигурационного файла указывается протокол *Ldaps*, Табл. 6, с. 16.)

Элемент интерфейса	Описание
Контейнер (точка подключения)	Укажите имя контейнера в иерархической структуре LDAP-каталога, к которой необходимо подключиться. Формат указания точки подключения см. в описании параметра конфигурационного файла: *LdapConnections -> LdapContainer,* Табл. 6, с. 16
Имя пользователя	Имя пользователя для подключения к LDAP-серверу. Формат указания имени пользователя для разных типов LDAP см. в описании параметра конфигурационного файла: *LdapConnections -> LdapServerUsername,* Табл. 6, с. 16 **Примечание.** В форматах имени, где используется обратный слеш (например *fqdn1\Administrator*), при указании имени в web-консоли в отличие от конфигурационного файла слеш дублировать не следует
Пароль	Пароль пользователя для подключения к LDAP-серверу. (Соответствует параметру *LdapConnections -> LdapServerPassword* конфигурационного файла, Табл. 6, с. 16.)
<кнопка> **Проверить соединение**	Для проверки корректности указанных параметров нажмите кнопку **Проверить соединение**. При успешном соединении отобразится уведомление «Соединение успешно установлено!»

4. Для сохранения введенных данных нажмите **OK**.

11.2.2.2 Добавление правила проверки принадлежности группе

Для того чтобы добавить группу LDAP для проверки принадлежности ей пользователя, выполняющего аутентификацию на сервере, выполните следующие действия.

1. В разделе **Конфигурация сервера** web-консоли выберите подраздел **Настройки LDAP** и во фрейме **Проверка членства в группах** нажмите **Добавить**.

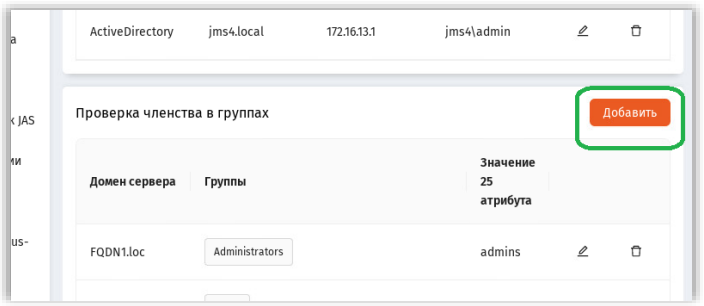

Рис. 17 – Добавление записи для проверки членства в группе LDAP

2. Отобразится форма добавления записи правила проверки членстве в группе LDAP.

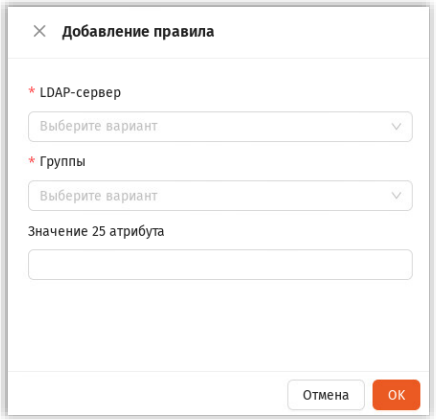

Рис. 18 – Форма добавления правила проверки принадлежности группе LDAP

3. Выполните настройки, руководствуясь Табл. 16.

Табл. 16 – Настройки правила проверки принадлежности группе LDAP

Элемент интерфейса	Описание
LDAP-сервер	Выберите LDAP-сервер, на котором определена группа (Параметр в конфигурационном файле: *LdapAuthorizeGroupMember -> AccountSystemDomain*, см. Табл. 6, с. 16.)
Группы	Выберите группу, на принадлежность которой следует проверять пользователя. (Параметр в конфигурационном файле: *LdapAuthorizeGroupMember -> Groups*, см. Табл. 6, с. 16.)
Значение 25 атрибута	Введите значение, руководствуясь описанием параметра *LdapAuthorizeGroupMember -> ClassAttribute* конфигурационного файла, Табл. 6, с. 16

4. Для сохранения введенных данных нажмите **OK**.

11.2.3 Настройки подключения к JAS

Для настройки подключения к серверу JaCarta Authentication Server (JAS) выполните следующие действия.

1. В web-консоли сервера JRS выберите раздел **Конфигурация сервера** и нажмите **Настройки подключения к JAS**.

Страница примет следующий вид

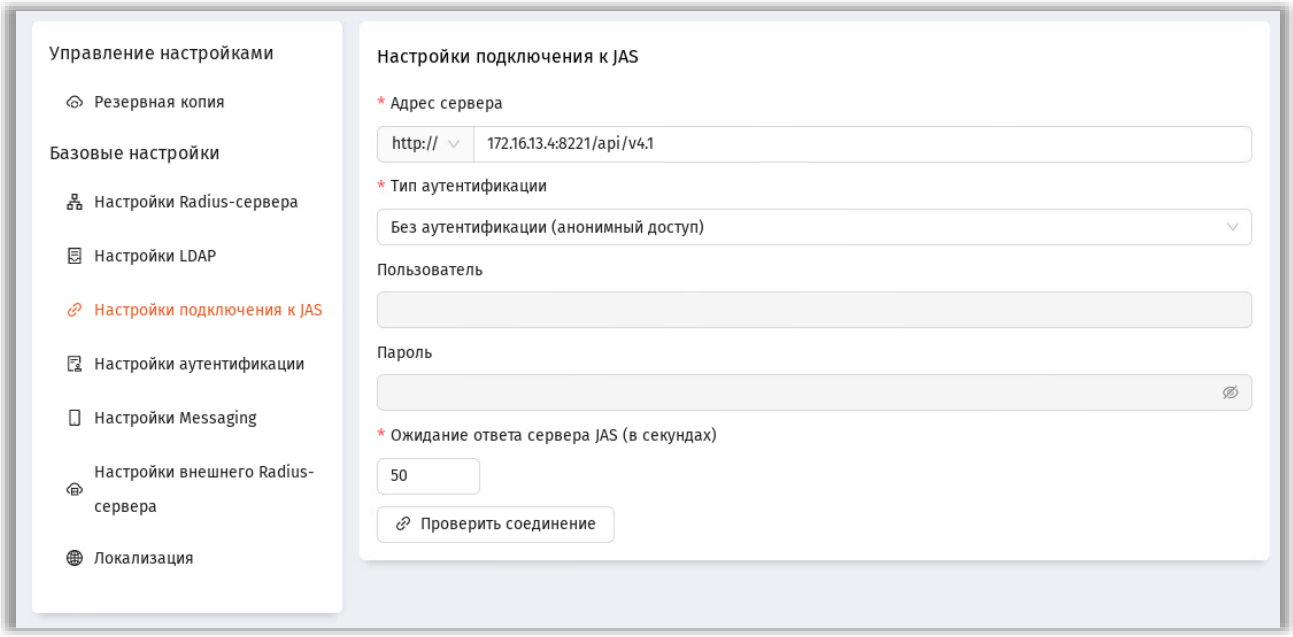

Рис. 19 – Страница настроек подключения к JAS

2. Выполните настройку, руководствуясь Табл. 17.

Табл. 17 – Настройки подключения к JAS

Настройка	Описание
<Секция> **Настройки подключения к JAS**	
Адрес сервера	Укажите в данном поле адрес в следующем формате `https://<FQDN-имя сервера>:<порт>/<путь к API>` где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com Подробнее см. описание параметра конфигурационного файла *JasServiceUri*, Табл. 6, с. 16
Тип аутентификации	Тип аутентификации на сервере JAS. Допустимые значения: • **Без аутентификации (анонимный доступ)** – значение по умолчанию, аутентификация отключена (none); • **Basic аутентификация (логин + пароль)** базовая http-аутентификация (пароль и логин передаются в теле запроса), ; • **Windows аутентификация** Подробнее см. описание параметра конфигурационного файла *JasAuthType*, Табл. 6, с. 16
Пользователь	Имя пользователя, от имени которого сервер JRS будет подключаться к серверу JAS (по интерфейсу **AdministrationService**). Поле доступно только при выбранном значении **Basic** в поле **Тип аутентификации** (выше)

Настройка	Описание
	(Соответствует параметру *JasUsername* конфигурационного файла, см. Табл. 6, с. 16)
Пароль	В случае если в поле **Имя пользователя** указано соответствующее значение, в поле **Пароль** следует указать пароль этого пользователя в соответствующей ресурсной системе (FreeIPA, Active Directory и др.) Поле доступно только при выбранном значении **Basic** в поле **Тип аутентификации** (выше) (Соответствует параметру *JasPassword* конфигурационного файла, см. Табл. 6, с. 16)
Ожидание ответа сервера JAS (в секундах)	Таймаут ожидания в секундах. (Соответствует параметру *JasTimeout* конфигурационного файла, см. Табл. 6, с. 16)
<кнопка> **Проверить соединение**	Для проверки корректности указанных параметров нажмите кнопку **Проверить соединение**. При успешном соединении отобразится уведомление «Соединение успешно установлено!»

По завершении настройки нажмите **Сохранить**. (Внесение изменений в конфигурацию сервера потребует его автоматической перезагрузки.)

11.2.4 Настройки аутентификации

Для настройки параметров аутентификации пользователей выполните следующие действия.

1. В web-консоли сервера JRS выберите раздел **Конфигурация сервера** -> **Настройки аутентификации**.
   Страница примет следующий вид

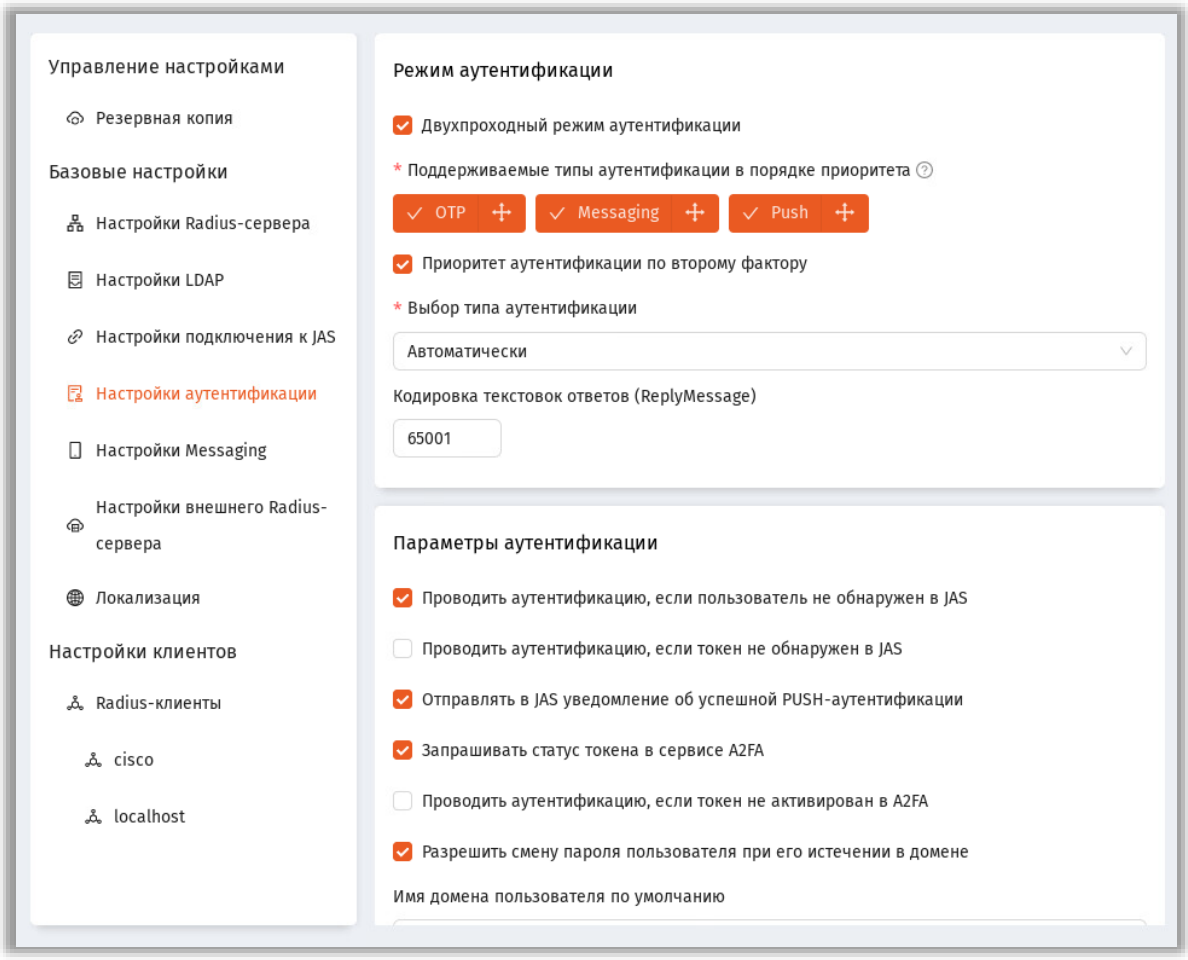

Рис. 20 – Страница Настройки аутентификации

2. Выполните настройки, руководствуясь Табл. 18.

Табл. 18 – Настройки аутентификации

Элемент интерфейса	Описание
<Фрейм> **Режим аутентификации**	
Двухпроходный режим аутентификации	Флаг, определяющий число шагов, в которое будет осуществляться аутентификация в системе JRS-JAS • **Флаг установлен** – двухшаговый режим аутентификации (перед вводом дополнительного параметра аутентификации, например OTP, на первом шаге процедуры вводится значение доменного пароля пользователя); • **Флаг сброшен** -- одношаговый режим аутентификации (значение дополнительного параметра аутентификации, например OTP, вводится за один шаг). Соответствует параметру конфигурационного файла *ChallengeResponseRadiusAuth*, см. Табл. 6, с. 16
Поддерживаемые типы аутентификации в порядке приоритета	Параметр определяет доступные пользователю типы аутентификации (Messaging, OTP, Push) и их приоритет.

Элемент интерфейса	Описание
	По умолчанию установлен следующий список с приоритетом в порядке убывания: OTP, Messaging, Push Включение и отключение метода осуществляется нажатием на галочке на «кнопке» соответствующего метода, изменение приоритета осуществляется методом «перетаскивания». **Важно!** При отключении флага **Двухпроходный режим аутентификации** может быть использован только один из двух типов аутентификации – OTP или Push. Соответствует параметру конфигурационного файла *AuthTypes*, см. Табл. 6, с. 16
Выбор типа аутентификации	Параметр позволяет установить выбора типа аутентификации (OTP, Messaging или Push) самому пользователю (значение **Вручную**) в интерфейсе его приложения, либо установить автоматический режим типа аутентификации (значение **Автоматически**, установлено по умолчанию) в соответствии со значением настройки **Поддерживаемые типы аутентификации в порядке приоритета** (выше) **Примечание.** Параметр доступен только при включении флага **Двухпроходный режим аутентификации** (выше) Соответствует параметру конфигурационного файла *AuthTypeSelection*, см. Табл. 6, с. 16
Кодировка текстовок ответов (ReplyMessage)	Кодировка текстовых сообщений (ReplyMessage), используемых в пользовательском диалоге при двухшаговой процедуре аутентификации. В качестве обозначения кодировок допускается использовать только их числовые обозначения, например: • **65001** – кодировка UTF8; • **1251** – Windows-1251; Значение по умолчанию: **65001** **Примечание.** Параметр доступен только при включении флага **Двухпроходный режим аутентификации** (выше) Соответствует параметру конфигурационного файла *ReplyMessageCodePage*, см. Табл. 6, с. 16
<Фрейм> **Параметры аутентификации**	
Проводить аутентификацию, если пользователь не обнаружен в JAS	Флаг установлен по умолчанию. Соответствует параметру конфигурационного файла *UserNotFoundAction*, см. Табл. 6, с. 16
Проводить аутентификацию, если токен не обнаружен в JAS	Флаг не установлен по умолчанию. Соответствует параметру конфигурационного файла *TokenNotFoundAction*, см. Табл. 6, с. 16

Элемент интерфейса	Описание
Отправлять в JAS уведомление об успешной PUSH-аутентификации	Флаг установлен по умолчанию. Соответствует параметру конфигурационного файла *NotifyPushSuccess*, см. Табл. 6, с. 16
Запрашивать статус токена в сервисе A2FA	Флаг установлен по умолчанию. Соответствует параметру конфигурационного файла *CheckA2faTokenState*, см. Табл. 6, с. 16
Проводить аутентификацию, если токен не активирован в A2FA	Флаг не установлен по умолчанию. Соответствует параметру конфигурационного файла *A2faNotActivatedAction*, см. Табл. 6, с. 16
Разрешить смену пароля пользователя при его истечении в домене	Флаг установлен по умолчанию. **Примечание.** Параметр доступен только при включении флага **Двухпроходный режим аутентификации** (выше) Соответствует параметру конфигурационного файла *AllowChangeExpiredPassword*, см. Табл. 6, с. 16
Имя домена пользователя по умолчанию	Данное значение добавляется к имени пользователя при аутентификации, например, в web-интерфейсе, если пользователь указал свое имя без домена. Подробнее см. в описании параметра конфигурационного файла *DefaultUserDomain*, см. Табл. 6, с. 16

3. В случае внесения изменений нажмите **Сохранить**, чтобы сохранить настройки.

11.2.5 Настройки Messaging

Для настройки параметров аутентификации методом Messaging выполните следующие действия.

1. В web-консоли сервера JRS выберите раздел **Конфигурация сервера** -> **Настройки Messaging**.

Страница примет следующий вид

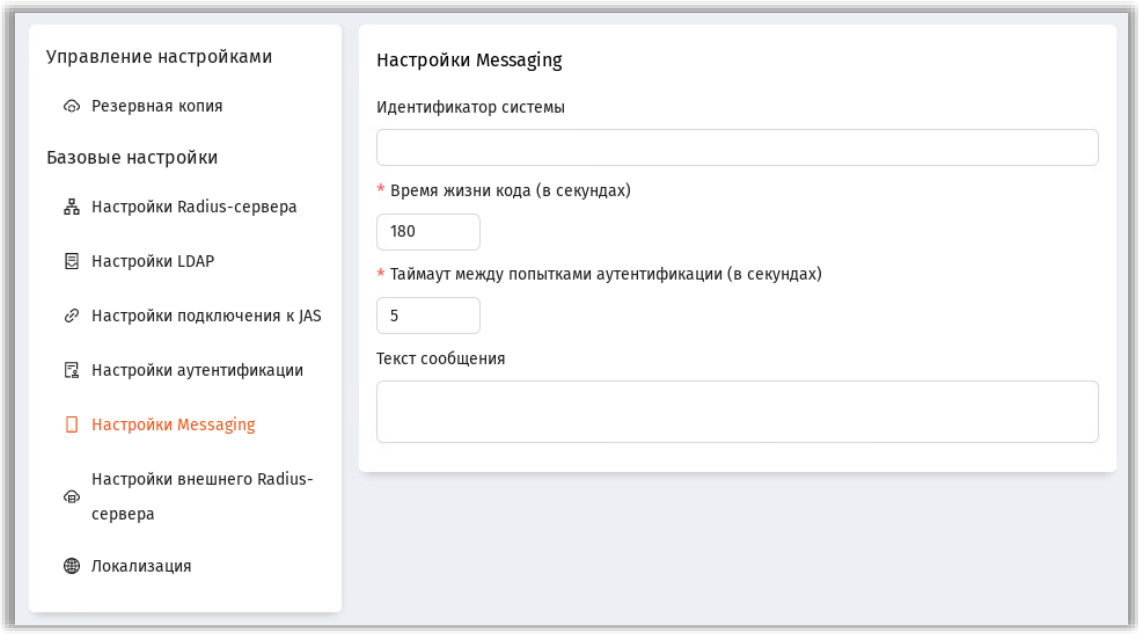

Рис. 21 – Настройки Messaging

2. Выполните настройки аутентификации методом Messaging, руководствуясь Табл. 19.

Табл. 19 – Настройка Messaging

Настройка	Описание
<Фрейм> **Настройки Messaging**	
Идентификатор системы	Идентификатор внешней системы, в которой будут искаться пользователи при аутентификации по Messaging. **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 [4], [5], раздел «Настройка профиля выпуска Messaging-токенов») Подробнее см. в описании параметра конфигурационного файла *MessagingSystemId*, см. Табл. 6, с. 16
Время жизни кода (в секундах)	Время жизни для одноразового пароля (One-Time Password), в течение которого ответ пользователя будет актуальным. Значение по умолчанию: **180** с Подробнее см. в описании параметра конфигурационного файла *MessagingTtl*, см. Табл. 6, с. 16

Настройка	Описание
Таймаут между попытками аутентификации (в секундах)	Таймаут между попытками аутентификации посредством Messaging-токена. Значение по умолчанию: **5** с 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. Подробнее см. в описании параметра конфигурационного файла *MessagingRetryDelay*, см. Табл. 6, с. 16
Текст сообщения	Текст, который будет отправляться в SMS пользователю вместе с кодом аутентификации для Messaging. Например "Код аутентификации для входа в систему XYZ" Значение по умолчанию: пустая строка. Подробнее см. в описании параметра конфигурационного файла *MessagingAdditionalInfo*, см. Табл. 6, с. 16

3. В случае внесения изменений нажмите **Сохранить**, чтобы сохранить настройки.

11.2.6 Настройки внешнего RADIUS-сервера

Для настройки параметров внешнего RADIUS-сервера выполните следующие действия.

1. В web-консоли сервера JRS выберите раздел **Конфигурация сервера** -> **Настройки внешнего Radius-сервера**.

Страница примет следующий вид.

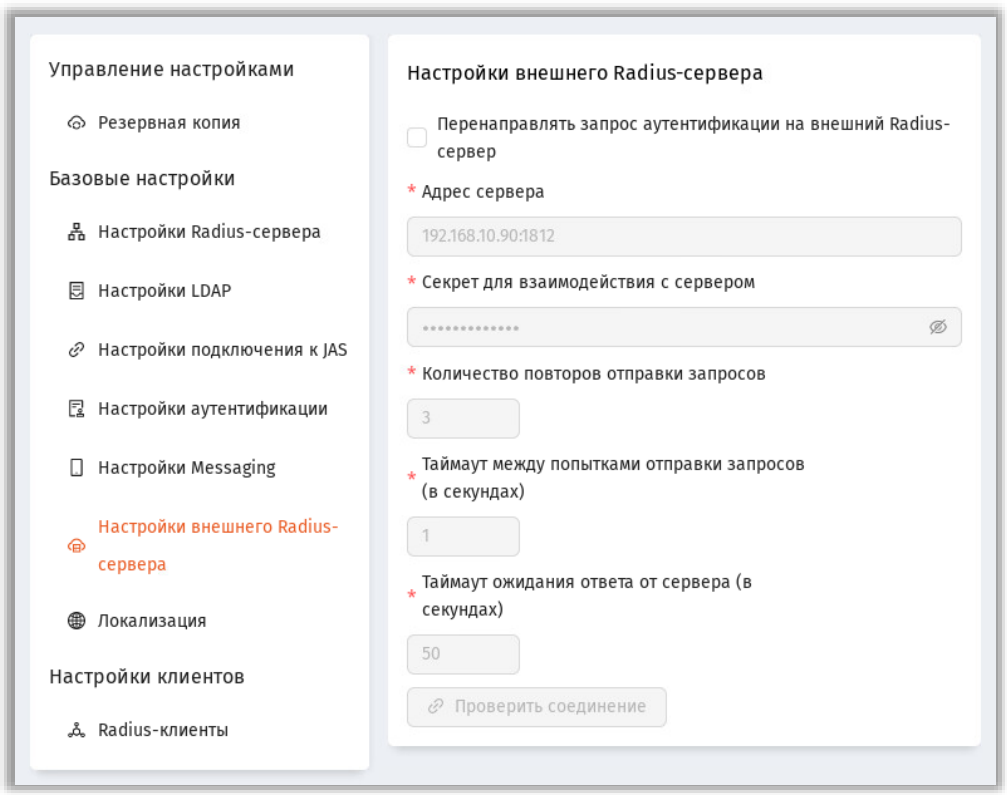

Рис. 22 – Страница настроек внешнего RADIUS-сервера

2. Выполните настройки, руководствуясь Табл. 20.

Табл. 20 – Настройки внешнего RADIUS-сервера

Элемент интерфейса	Описание
Перенаправлять запрос аутентификации на внешний Radius-сервер	Установите флаг, если аутентификацию (проверку значения доменного пароля) следует осуществлять на внешнем RADIUS-сервере. В противном случае проверка значения доменного пароля будет осуществляться на сервере JAS. По умолчанию флаг не установлен. Соответствует параметру конфигурационного файла *CheckPasswordAgainstExternalRadiusServer*, см. Табл. 6, с. 16. Подробнее логику сценариев аутентификации с использованием параметра *CheckPasswordAgainstExternalRadiusServer* см. в разделе «Настройка режимов аутентификации в JRS», с. 29, а также Табл. 7 с.29 и Табл. 8, с. 31)
Адрес сервера	Адрес подключения к внешнему RADIUS-серверу. Укажите адрес в формате IP:Port, например: **192.168.10.90:1812** Соответствует параметру конфигурационного файла *ExternalRadiusServer*, см. Табл. 6, с. 16.

Элемент интерфейса	Описание
Секрет для взаимодействия с сервером	Укажите секрет для взаимодействия с внешним RADIUS-сервером (следует узнать у администратора данного сервиса). Соответствует параметру конфигурационного файла *ExternalRadiusServerSharedSecret*, см. Табл. 6, с. 16.
Количество повторов отправки запросов	Кол-во повторов отправки запросов на внешний RADIUS-сервер. Значение по умолчанию: **3** Соответствует параметру конфигурационного файла *ExternalRadiusServerRetryCount*, см. Табл. 6, с. 16.
Таймаут между попытками отправки запросов (в секундах)	Задержка между повторами отправки запросов на внешний RADIUS-сервер. Значение по умолчанию: **1** Соответствует параметру конфигурационного файла *ExternalRadiusServerRetryDelay*, см. Табл. 6, с. 16.
Таймаут ожидания ответа от сервера (в секундах)	Максимальное время ожидание ответа от внешнего RADIUS-сервера. Значение по умолчанию: **50** Соответствует параметру конфигурационного файла *ExternalRadiusServerTimeout*, см. Табл. 6, с. 16.

3. В случае внесения изменений нажмите **Сохранить**, чтобы сохранить настройки.

11.2.7 Настройки локализации (языка пользовательского интерфейса RADIUS)

Для настройки языка сообщений при взаимодействии с пользователем RADIUS-сервера выполните следующие действия.

1. В web-консоли сервера JRS выберите раздел **Конфигурация сервера** -> **Локализация**.

Страница примет следующий вид.

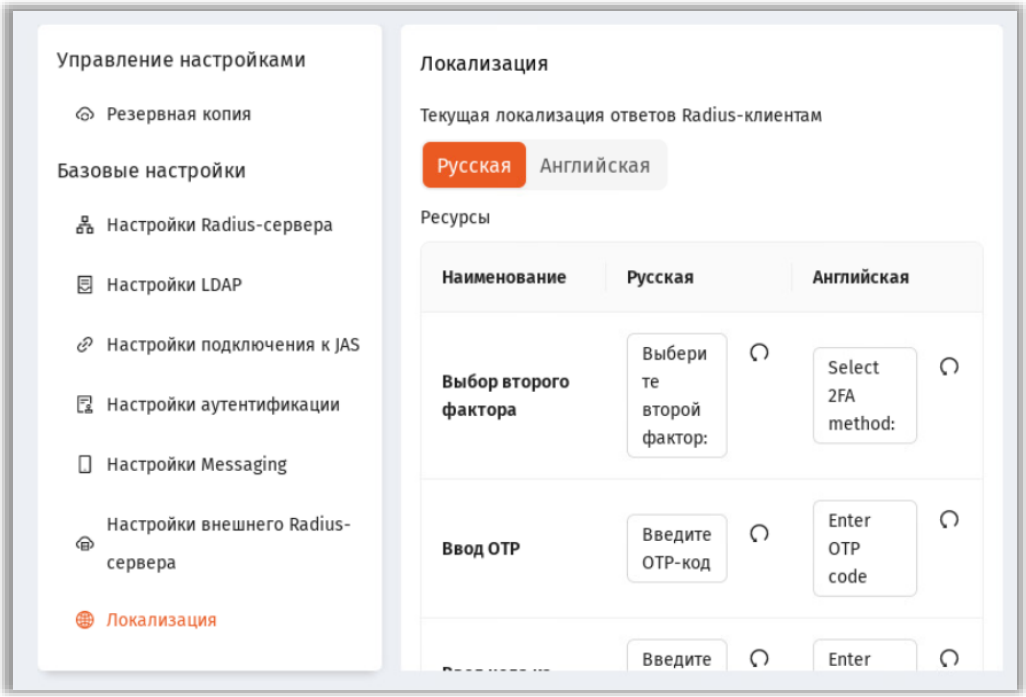

Рис. 23 – Страница локализации пользовательского интерфейса RADIUS

2. Выполните настройки, руководствуясь Табл. 21.

Табл. 21 – Настройка языка пользовательского интерфейса RADIUS

Элемент интерфейса	Описание
<Секция> **Текущая локализация ответов Radius-клиентам**	
Текущая локализация ответов Radius-клиентам	Выбор локализации (языка) текстового интерфейса для взаимодействия с пользователями RADIUS. Выберите необходимое значение • **Русская** (по умолчанию) • **Английская** Соответствует параметру конфигурационного файла *LocalizationCulture*, см. Табл. 6, с. 16.
<Секция> **Ресурсы** **Примечание.** Содержимое секции соответствует набору параметров в массиве JSON-объектов *Localization* конфигурационного файла, см. Табл. 6, с. 16.	
Выбор второго фактора	Текстовки для выбор пользователем второго фактора аутентификации. Значения по умолчанию: • Русская: Выберите второй фактор: • Английская: Select 2FA method:

Элемент интерфейса	Описание
Ввод OTP	Текстовки для приглашения ввести OTP. Значения по умолчанию: • Русская: Введите OTP-код • Английская: Enter OTP code
Ввод кода из СМС	Текстовки для приглашения ввести кода из СМС Значения по умолчанию: • Русская: Введите код из SMS • Английская: Enter SMS code
Ввод кода из СМС кол-вом оставшихся попыток	Текстовки для приглашения ввести кода из СМС с уведомлением о количестве оставшихся попыток Значения по умолчанию: • Русская: Введите код из SMS. Осталось попыток: • Английская: Enter SMS code. Remaining attempts:
Истёкший срок действия пароля	Текстовки для отображения истёкшего срока действия пароля Значения по умолчанию: • Русская: Срок действия пароля учетной записи истек. Смените пароль или обратитесь к администратору • Английская: The user password has expired. Change your password or contact your administrator
Несовпадение нового пароля и подтверждения	Текстовки для предупреждения о несовпадении нового пароля и подтверждения. Значения по умолчанию: • Русская: Введенные пароли не совпадают • Английская: The entered passwords do not match
Несоответствие сложности пароля политике	Текстовки для предупреждения о несоответствии сложности пароля политике. Значения по умолчанию: • Русская: Пароль не соответствует требованиям сложности. Если Вы не знаете требования к сложности пароля, обратитесь к администратору • Английская: The new password does not match the complexity policy. If you do not know the password complexity requirements, contact your administrator
Запрос нового пароля	Текстовки с запросом нового пароля. Значения по умолчанию: • Русская: Пароль пользователя истек. Введите новый пароль • Английская: User password has expired. Enter a new password
Запрос подтверждения нового пароля	Текстовки для запроса подтверждения нового пароля. Значения по умолчанию: • Русская: Подтвердите новый пароль • Английская: Confirm new password
Превышение кол-ва неправильных попыток ввода пароля	Текстовки для предупреждения о превышении числа неправильных попыток ввода пароля

Элемент интерфейса	Описание
	Значения по умолчанию: • Русская: Превышено максимальное количество попыток смены пароля • Английская: The maximum number of attempts to change the password has been exceeded
Метод аутентификации OTP	Текстовки для отображения метод аутентификации «OTP» Значения по умолчанию: • Русская: OTP • Английская: OTP
Метод аутентификации Messaging	Текстовки для отображения метод аутентификации «Messaging» Значения по умолчанию: • Русская: Messaging • Английская: Messaging
Метод аутентификации Push	Текстовки для отображения метод аутентификации «Push» Значения по умолчанию: • Русская: Push • Английская: Push

3. В случае внесения изменений нажмите **Сохранить**, чтобы сохранить настройки.

11.2.8 Настройки RADIUS-клиентов

Для настройки параметров RADIUS-клиентов выполните следующие действия.

1. В web-консоли сервера JRS выберите раздел **Конфигурация сервера** -> **Radius-клиенты**. Страница примет следующий вид.

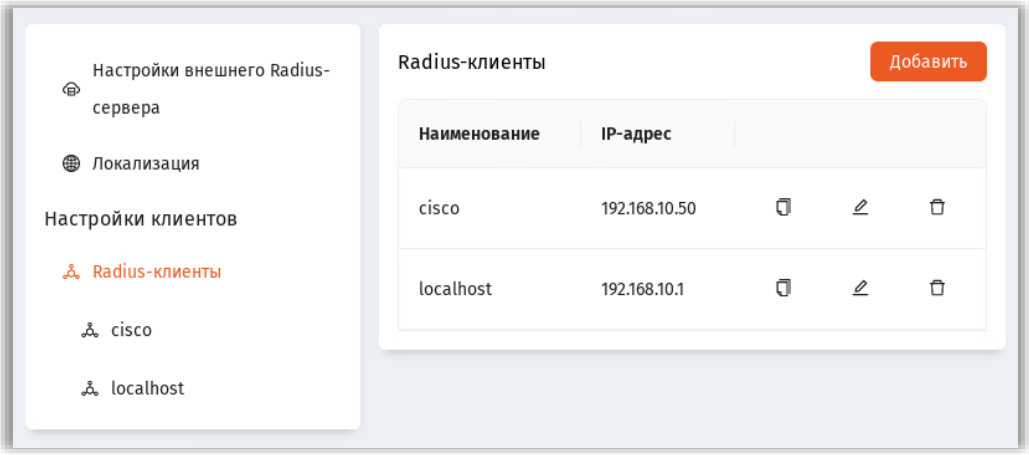

Рис. 24 – Страница настроек RADIUS-клиентов

2. В случае добавления нового RADIUS-клиента нажмите кнопку **Добавить**. Если необходимо отредактировать параметры уже определенных RADIUS-клиентов, в строке соответствующего клиента нажмите значок . Для удаления клиента нажмите значок «корзины».

Примечание. В качестве RADIUS-клиентов «по умолчанию» после инсталляции продукта определены два типовых случая:

1) межсетевой экран Cisco ASA с псевдонимом "cisco";
2) локальный хост сервера JRS с псевдонимом "localhost" (предполагается, что RADIUS-клиент будет располагаться прямо на нём, например для тестовых целей).

3. При редактировании или добавлении RADIUS-клиента откроется страница следующего вида.

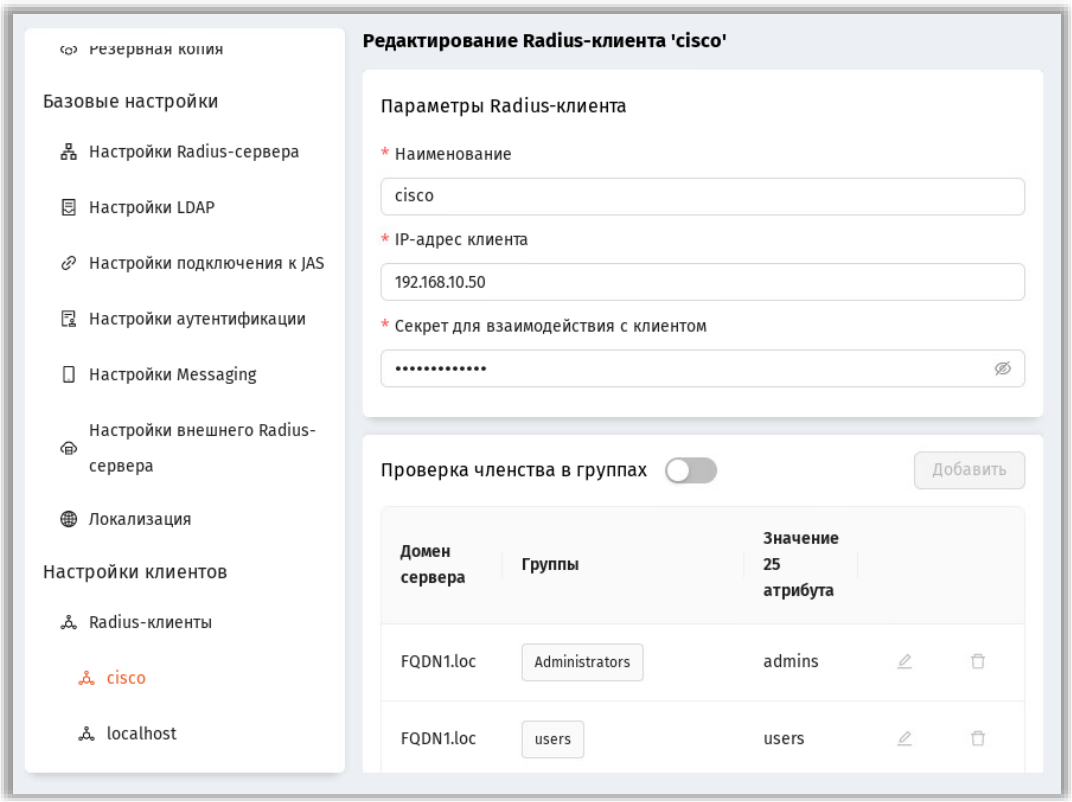

Рис. 25 – Страница редактирования параметров RADIUS-клиента

4. Выполните настройки, руководствуясь Табл. 22.

Табл. 22 – Настройка параметров RADIUS-клиентов

Элемент интерфейса	Описание
<Фрейм> **Параметры Radius-клиента**	
Наименование	Укажите псевдоним для данного RADIUS-клиента (используется только для отображения в графическом интерфейсе JRS) Например: **cisco** Соответствует параметру *Clients -> RadiusClientName* конфигурационного файла, см. Табл. 6, с. 16.
IP-адрес клиента	Укажите IP-адрес для данного RADIUS-клиента

Элемент интерфейса	Описание
	Например: **192.168.10.50** Соответствует параметру *Clients -> RadiusClientAddress* конфигурационного файла, см. Табл. 6, с. 16.
Секрет для взаимодействия с клиентом	Общий секрет (пароль) для взаимодействия RADIUS-сервера и RADIUS-клиента, Например: **shared-secret** Соответствует параметру *Clients -> RadiusClientSharedSecret* конфигурационного файла, см. Табл. 6, с. 16.
<Фрейм> **Проверка членства в группах** **Примечание.** В настоящей секции осуществляется переопределение параметров, установленных в сервере JRS «по умолчанию» для использования в RADIUS-клиентах. Суть процесса переопределения параметров описана в разделе «Переопределение настроек для RADIUS-клиентов», с. 28	
<Переключатель-флаг> **Проверка членства в группах**	Установите флаг, если параметры проверки пользователя на членство в группах в выбранном RADIUS-клиенте следует переопределить по сравнению с параметрами, установленными в сервере JRS по умолчанию для RADIUS-клиентов (данные настройки «по умолчанию» выполняются в разделе **Конфигурация сервера** -> **Настройки LDAP** -> **Проверка членства в группах** web-консоли JRS, см. раздел «Добавление правила проверки принадлежности группе», с. 45) Интерфейс переопределения настроек и параметры полностью повторяют указанных выше раздел Web-консоли.
<Фрейм> **Настройки подключения к JAS** **Примечание.** В настоящей секции осуществляется переопределение параметров подключения RADIUS-клиентов к серверу JAS, установленных в сервере JRS «по умолчанию». Суть процесса переопределения параметров описана в разделе «Переопределение настроек для RADIUS-клиентов», с. 28	
<Переключатель-флаг> **Настройки подключения к JAS**	Установите флаг, если параметры подключения к серверу JAS следует переопределить по сравнению с параметрами, установленными в сервере JRS по умолчанию для RADIUS-клиентов (данные настройки «по умолчанию» выполняются в разделе **Конфигурация сервера** -> **Настройки подключения к JAS** web-консоли JRS, см. раздел «Настройки подключения к JAS», с. 46) Интерфейс переопределения настроек и параметры полностью повторяют указанный выше раздел Web-консоли.
<Фрейм> **Режим аутентификации** **Примечание.** В настоящей секции осуществляется переопределение режима аутентификации пользователя в выбранном RADIUS-клиенте относительно аналогичных параметров, установленных в сервере JRS «по умолчанию». Суть процесса переопределения параметров описана в разделе «Переопределение настроек для RADIUS-клиентов», с. 28	

Элемент интерфейса	Описание
<Переключатель-флаг> **Режим аутентификации**	Установите флаг, если режим аутентификации пользователя в данном RADIUS-клиенте следует переопределить по сравнению с режимом, установленным в сервере JRS по умолчанию (данные настройки «по умолчанию» выполняются в разделе **Конфигурация сервера** -> **Настройки аутентификации -> Режим аутентификации** web-консоли JRS, см. раздел «Настройки аутентификации», с. 48) Интерфейс переопределения настроек аутентификации перечень измененяемых параметров полностью повторяют указанный выше раздел Web-консоли.
<Фрейм> **Параметры аутентификации** **Примечание.** В настоящей секции осуществляется переопределение параметров режимов аутентификации пользователя в выбранном RADIUS-клиенте относительно аналогичных параметров, установленных в сервере JRS «по умолчанию». Суть процесса переопределения параметров описана в разделе «Переопределение настроек для RADIUS-клиентов», с. 28	
<Переключатель-флаг> **Параметры аутентификации**	Установите флаг, если параметры аутентификации пользователя в данном RADIUS-клиенте следует переопределить по сравнению с параметрами, установленными в сервере JRS по умолчанию (данные настройки «по умолчанию» выполняются в разделе **Конфигурация сервера** -> **Настройки аутентификации -> Параметры аутентификации** web-консоли JRS, см. раздел «Настройки аутентификации», с. 48) Интерфейс переопределения параметров аутентификации и перечень настроек полностью повторяют указанный выше раздел Web-консоли.
<Фрейм> **Настройки messaging** **Примечание.** В настоящей секции осуществляется переопределение настроек Messaging в выбранном RADIUS-клиенте относительно аналогичных параметров, установленных в сервере JRS «по умолчанию». Суть процесса переопределения параметров описана в разделе «Переопределение настроек для RADIUS-клиентов», с. 28	
<Переключатель-флаг> **Настройки Messaging**	Установите флаг, если настройки Messaging в данном RADIUS-клиенте следует переопределить по сравнению с параметрами, установленными в сервере JRS по умолчанию (данные настройки «по умолчанию» выполняются в разделе **Конфигурация сервера** -> **Настройки Messaging** web-консоли JRS, см. раздел «Настройки Messaging», с. 51) Интерфейс переопределения настроек Messaging и перечень параметров полностью повторяют указанный выше раздел Web-консоли.
<Фрейм> **Настройки внешнего Radius-сервера** **Примечание.** В настоящей секции осуществляется переопределение настроек подключения к внешнему RADIUS-серверу в выбранном RADIUS-клиенте относительно аналогичных параметров, установленных в сервере JRS «по умолчанию». Суть процесса переопределения параметров описана в разделе «Переопределение настроек для RADIUS-клиентов», с. 28	

Элемент интерфейса	Описание
<Переключатель-флаг> **Настройки внешнего Radius-сервера**	Установите флаг, если настройки подключения к внешнему RADIUS-серверу в данном RADIUS-клиенте следует переопределить по сравнению с параметрами, установленными в сервере JRS по умолчанию (данные настройки «по умолчанию» выполняются в разделе **Конфигурация сервера** -> **Настройки внешнего Radius-сервера** web-консоли JRS, см. раздел «Настройки внешнего RADIUS-сервера», с. 53) Интерфейс переопределения настроек подключения к внешнему RADIUS-серверу и перечень параметров полностью повторяют указанный выше раздел Web-консоли.
<Фрейм> **Локализация** **Примечание.** В настоящей секции осуществляется переопределение выбора языка текстового интерфейса с пользователем (локализации) в выбранном RADIUS-клиенте относительно локализации, установленной в сервере JRS «по умолчанию». Суть процесса переопределения параметров описана в разделе «Переопределение настроек для RADIUS-клиентов», с. 28	
<Переключатель-флаг> **Локализация**	Установите флаг, если настройки локализации в данном RADIUS-клиенте следует переопределить по сравнению с параметрами, установленными в сервере JRS по умолчанию (данные настройки «по умолчанию» выполняются в разделе **Конфигурация сервера** -> **Локализация** web-консоли JRS, см. раздел «Настройки локализации (языка пользовательского интерфейса RADIUS)», с. 55) Интерфейс переопределения настроек локализации и перечень параметров полностью повторяют указанный выше раздел Web-консоли.

5. В случае внесения изменений нажмите **Сохранить**, чтобы сохранить настройки.

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 JaCarta Management System 4LX. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS) [Текст]. — «Аладдин Р.Д.». — Файл JMS-4LX Руководство Администратор 3.docx

2 JaCarta Management System v3.7. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS) [Текст]. — «Аладдин Р.Д.». — Файл JMS_x.x_AdminGuide_(Part3)_JAS_RU.docx

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

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

5 JaCarta Management System v3.7. Руководство администратора . Часть 2. Функции управления [Текст]. — «Аладдин Р.Д.». — Файл JMS_3.7_AdminGuide_(Part2)_Management_RU.docx

6 RU.АЛДЕ. 03.16.001-05 30 01-1. Формуляр [Текст]. — «Аладдин Р.Д.»

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

Полезные web-ресурсы

1 RFC 2865. Remote Authentication Dial In User Service (RADIUS) [5.25. Class. Description] https://www.rfc-editor.org/rfc/rfc2865#section-5.25

2 FIDO Alliance. Download Specifications. https://fidoalliance.org/download/

Регистрация изменений

Версия	Изменения
1.00	Исходная версия документа для JRS версии 1.0

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

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web: www.aladdin.ru