



УТВЕРЖДЕН

RU.АЛДЕ.03.16.001-05 32 01-1-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ JACARTA MANAGEMENT SYSTEM 4LX

Руководство администратора. Часть 1

Установка и настройка

RU.АЛДЕ.03.16.001-05 32 01-1

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

Версия продукта	4LX
Версия документа	1.0
Статус	Служебный
Дата	21 октября 2021 г.
Листов	54

Оглавление

1.	О документе	4
1.1	Назначение документа	4
1.2	На кого ориентирован данный документ	4
1.3	Соглашения по оформлению	4
1.4	Обозначения и сокращения	5
1.5	Авторские права, товарные знаки, ограничения	6
1.6	Лицензионное соглашение	7
2.	Введение	10
2.1	Приемка изделия	10
2.2	Общие сведения	10
2.3	Состав JMS	10
3.	Описание пакета установки	11
4.	Системные требования	11
5.	Установка и первоначальная настройка	11
5.1	Начальные условия для развертывания JMS	11
5.2	Установка и первоначальная настройка сервера и консольного агента JMS	12
5.2.1	Подготовительные действия	12
5.2.2	Установка компонентов сервера JMS	13
5.3	Установка и первоначальная настройка серверного web-приложения Консоль управления JMS	15
5.3.1	Подготовительные действия	15
5.3.2	Установка серверного компонента Консоли управления JMS	15
5.4	Установка и первоначальная настройка JMS Web Agent (JWA)	17
5.4.1	Подготовительные действия	17
5.4.2	Установка JWA	18
5.5	Проверка работы web-приложения Консоль управления JMS	19
6.	Порядок обновления компонентов JMS	21
6.1	Остановка служб компонентов JMS	21
6.2	Резервное копирование БД JMS	22
6.3	Удаление компонентов JMS	22
6.4	Установка новой версии сервера JMS (в рамках обновления продукта)	22
6.5	Обновление БД JMS	22
6.6	Установка остальных компонентов JMS (в рамках обновления продукта)	22
6.7	Запуск и проверка работоспособности компонентов JMS	22
7.	Журналы диагностики JMS	22

8. Обеспечение целостности и защиты от несанкционированного доступа файлов ПО JMS	23
9. Настройка функций безопасности среды функционирования объекта оценки (JMS)	23
10. Установка и настройка плагина СКЗИ «Крипто БД» для JMS	23
11. Утилита сбора диагностической информации о JMS	26
12. Настройка SSL для доступа к ресурсной системе	28
13. Активация продукта	29
Приложение 1. Параметры файла первоначальной конфигурации сервера JMS	33
Секция service	33
Секция database	33
Секция accountSystem	34
Секция primaryUser	36
Секция licenses	36
Секция sts	36
Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal	37
Приложение 3. Инструкция по сборке расширения rJava для СУБД PostgreSQL 9.6 под ОС Astra Linux Орел или Смоленск	48
Контакты, техническая поддержка	51
Список литературы	52
Регистрация изменений	53

1. О документе

1.1 Назначение документа

Настоящий документ является частью руководства администратора и представляет собой описание операций по установке и настройке системы управления средствами аутентификации и защищенными носителями информации JaCarta Management System 4LX для среды функционирования Linux (далее – JMS).





1.2 На кого ориентирован данный документ

Документ предназначен для администраторов корпоративной информационной системы управления средствами аутентификации.

1.3 Соглашения по оформлению

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

Табл. 1 – Элементы оформления

Выделение	Используется для выделения наименований полей, кнопок, секций, вкладок экранных форм
<code>file.exe</code>	Используется для выделения имен файлов, каталогов, текстов программ
[1]	Ссылка на пункт в списке литературы (приведен в конце документа)
Гиперссылка	Используется для выделения внешних ссылок
Ссылка, с. 4	Используется для выделения перекрестных ссылок
	Важная информация
	Ссылка, примечание, заметка
	Совет
	Рекомендация

1.4 Обозначения и сокращения

Табл. 2– Обозначения и сокращения

JMS	То же, что «Программное обеспечение JaCarta Management System 4LX»
USB	Universal Serial Bus, универсальная последовательная шина
Клиент JMS	Web-приложение, предназначенное для управления электронными ключами и защищенными носителями информации на рабочих станциях конечных пользователей.
Консольный агент	Приложение, предназначенное для конфигурирования сервера JMS. Устанавливается вместе с компонентом JMS Server
ПО	Программное обеспечение
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации

1.5 Авторские права, товарные знаки, ограничения

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

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

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

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

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

Ограничение ответственности

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

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

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

программного обеспечения и документации на него преследуется по закону.

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

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

Государственное регулирование и экспортный контроль

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

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

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

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

1.6 Лицензионное соглашение

ВАЖНО:

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

ВСЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ НАСТОЯЩЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (включая без ограничений библиотеки, утилиты, файлы для скачивания с Web-сайта, CD-ROM, Руководства, описания и др. документацию), далее «ПО», «Продукт»), ПРЕДОСТАВЛЯЕМЫЕ КОМПАНИЕЙ АО «Аладдин Р.Д.» (или любым дочерним предприятием – каждое из них упоминаемое как «КОМПАНИЯ») ПОДЧИНЯЮТСЯ И БУДУТ ПОДЧИНЯТЬСЯ УСЛОВИЯМ, ОГОВОРЕННЫМ В ДАННОМ СОГЛАШЕНИИ. ОТКРЫВАЯ ПАКЕТ, СОДЕРЖАЩИЙ ПРОДУКТ И/ИЛИ ЗАГРУЖАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ как определено далее по тексту) И/ИЛИ УСТАНОВЛИВАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ВАШ КОМПЬЮТЕР И/ИЛИ ИСПОЛЬЗУЯ ДАННЫЙ ПРОДУКТ, ВЫ ПРИНИМАЕТЕ ДАННОЕ СОГЛАШЕНИЕ И СОГЛАШАЕТЕСЬ С ЕГО УСЛОВИЯМИ. ЕСЛИ ВЫ НЕ СОГЛАСНЫ С ДАННЫМ СОГЛАШЕНИЕМ, НЕ ОТКРЫВАЙТЕ ЭТОТ ПАКЕТ И/ИЛИ НЕ ЗАГРУЖАЙТЕ И/ИЛИ НЕ УСТАНОВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НЕЗАМЕДЛИТЕЛЬНО (не позднее 7 дней с даты получения этого пакета) ВЕРНИТЕ ЭТОТ ПРОДУКТ В АЛАДДИН Р.Д., СОТРИТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВСЕ ЕГО ЧАСТИ В СВОЕМ КОМПЬЮТЕРЕ И НЕ ИСПОЛЬЗУЙТЕ ЕГО НИКОИМ ОБРАЗОМ.

Лицензионное соглашение на использование программного обеспечения.

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

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

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

1. Предмет Соглашения

- 1.1. Предметом настоящего Соглашения является передача Правообладателем конечному Пользователю неисключительного права на использование ПО. ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Все условия, оговоренные далее, относятся как к ПО в целом, так и ко всем его компонентам в отдельности. Данное соглашение не передает Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничего в данном Соглашении не подтверждает отказ компании Аладдин Р.Д. от прав на интеллектуальную собственность по какому бы то ни было законодательству.
- 1.2. Компания Аладдин Р.Д. сохраняет за собой все права, явным образом не предоставленные Вам настоящим Лицензионным договором. Настоящий Лицензионный договор не предоставляет Вам никаких прав на товарные знаки Компании Аладдин Р.Д..

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

2. Имущественные права

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

3. Условия использования

- 3.1. ПО может быть использовано только в строгом соответствии с документами, инструкциями и рекомендациями Правообладателя, относящимися к данному ПО.
- 3.2. ПО может предоставляться на нескольких носителях, в том числе с помощью сети интернет. Независимо от количества носителей, на которых Вы получили ПО, Вы имеете право использовать ПО только в объеме предоставленной Вам Лицензии.
- 3.3. После уплаты Вами соответствующего вознаграждения компания Аладдин Р.Д. настоящим предоставляет Вам, а Вы получаете 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 нелегальным программным обеспечением.
- 5.4. ПО и обновления предоставляются такими, каковы они есть, и Компания Аладдин Р.Д. не предоставляет на них никаких гарантий.
- Компания Аладдин Р.Д. не гарантирует и не может гарантировать работоспособность ПО и результаты, которые Вы можете получить, используя ПО.
- 5.5. За исключением гарантий и условий, которые не могут быть исключены или ограничены в соответствии с применимым законодательством, Компания Аладдин Р.Д. не предоставляет Вам никаких гарантий (в том числе явно выраженных или подразумеваемых в статутном или общем праве или обычаями делового оборота) ни на что, включая, без ограничения, гарантии о не нарушении прав третьих лиц, товарной пригодности, интегрируемости, удовлетворительного качества и годности к использованию ПО. Все риски, связанные с качеством работы и работоспособностью ПО, возлагаются на Вас.
- 5.6. Компания Аладдин Р.Д. не предоставляет никаких гарантий относительно программами для ЭВМ других производителей, которые могут предоставляться в составе ПО.
- 6. Исключение косвенных убытков**
- Стороны признают, что Продукт по сути своей сложный и не может быть полностью лишен ошибок. КОМПАНИЯ АЛАДДИН Р.Д. НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ, ПОБОЧНЫЕ ИЛИ ПОТЕНЦИАЛЬНЫЕ УБЫТКИ), ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЕННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ КАКОГО-ЛИБО ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОЙ КОМПОНЕНТЫ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АЛАДДИН Р.Д. ПИСЬМЕННО УВЕДОМЛЕН О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.
- 7. Ограничение ответственности**
- В СЛУЧАЕ ЕСЛИ, НЕСМОТЯ НА УСЛОВИЯ ДАННОГО СОГЛАШЕНИЯ, КОМПАНИЯ АЛАДДИН Р.Д. ПРИЗНАНА ОТВЕТСТВЕННОЙ ЗА УБЫТКИ НА ОСНОВАНИИ КАКИХ-ЛИБО ДЕФЕКТОВ ИЛИ НЕСООТВЕТСТВИЯ ЕГО ПРОДУКТОВ, ПОЛНАЯ ОТВЕТСТВЕННОСТЬ ЗА КАЖДУЮ ЕДИНИЦУ ДЕФЕКТНЫХ ПРОДУКТОВ НЕ БУДЕТ ПРЕВЫШАТЬ СУММУ, ВЫПЛАЧЕННУЮ КОМПАНИИ АЛАДДИН Р.Д. ЗА ЭТИ ДЕФЕКТНЫЕ ПРОДУКТЫ.
- Компания Аладдин Р.Д. ни при каких обстоятельствах не несет перед Вами никакой ответственности за убытки, вынужденные перерывы в деловой активности, потерю деловых либо иных данных или информации, претензии или расходы, реальный ущерб, а также упущенную выгоду и утраченные сбережения, вызванные использованием или 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 УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

2. Введение

2.1 Приемка изделия

Перед установкой Изделия (JMS) необходимо убедиться, что:


1. комплектность Изделия соответствует комплектности поставки, указанной в Формуляре [3];
2. на носителях информации, входящих в состав поставки, отсутствуют сколы, царапины, целостность этикеток и пломб не нарушены;
3. контрольные суммы дистрибутива соответствуют заявленным в Формуляре [3].

2.2 Общие сведения

JMS - система, предназначенная для внедрения и учета аппаратных средств аутентификации и защищенных носителей информации (ЗНИ) пользователей в масштабах предприятия.

JMS обеспечивает:

- централизованное управление средствами аутентификации и ЗНИ в течение всего их жизненного цикла (инициализация/выпуск, ввод в эксплуатацию/выдача, обслуживание, вывод из эксплуатации/блокирование);
- учет средств аутентификации и ЗНИ, аудит их использования;
- автоматизацию типовых операций и сценариев администрирования в соответствии с политиками безопасности, принятыми в организации;
- быстрое и самостоятельное решение проблем пользователей без обращения к администраторам.

 В настоящем документе описание настроек JMS представлено на примере операционной системы Astra Linux Special Edition (ОС ЧН Смоленск 1.6).

2.3 Состав JMS

Система JMS развертывается на нескольких компьютерах с ОС Linux и включает в себя следующие компоненты:

- сервер JMS (демон-процесс eap-engine.service) – сервер бизнес-логики JMS;
- консольный агент JMS (процесс Aladdin.EAP.Agent.Terminal) – утилита динамического конфигурирования сервера JMS (всегда устанавливается на том же хосте, что и Сервер JMS);
- серверный компонент web-консоли управления JMS (демон-процесс eap-web-admin.service);
- компонент JMS Web Agent или JWA (демон-процесс jwa-service.service) – устанавливается на тех компьютерах с ОС Linux, на которых будет выполняться физическое обращение к электронным ключам и защищенным носителям информации (ЗНИ), а именно: на компьютерах с web-приложениями Консоль управления JMS и Клиент JMS.

3. Описание пакета установки

Дистрибутив JMS включает следующие пакеты установки (табл. 3).

Табл. 3 - Дистрибутив JMS

ОС	Файл дистрибутива	Описание
Astra Linux	aladdin-eap-engine_x.x.x.xxxx-x64.deb	Серверная часть JMS (сервер бизнес-логики, консольный агент JMS – утилита динамического конфигурирования сервера JMS)
РЕД ОС	aladdin-eap-engine_x.x.x.xxxx_x64.rpm	
ОС Альт	aladdin-eap-engine_x.x.x.xxxx_alt_x64.rpm	
Astra Linux	aladdin-eap-web-admin_x.x.x.xxxx_x64.deb	Серверный компонент, реализующий web-приложение «Консоль управления JMS»
РЕД ОС	aladdin-eap-web-admin_x.x.x.xxxx_x64.rpm	
ОС Альт	aladdin-eap-web-admin_x.x.x.xxxx_alt_x64.rpm	
Astra Linux	aladdin-jms-web-agent_x.x.x.xxx_x64.deb	JMS Web Agent (JWA)
РЕД ОС, ОС Альт	aladdin-jms-web-agent_x.x.x.xxxx_x64.rpm	

4. Системные требования

Полный перечень требований к среде функционирования компонентов JMS приведен в Формуляре [3].

5. Установка и первоначальная настройка

5.1 Начальные условия для развертывания JMS

Для развертывания продукта должны быть выполнены следующие начальные условия.

1. В сетевой доступности для сервера JMS должна быть установлена служба управления учетными записями FreeIPA (сервер). При установке рекомендуется использовать руководство поставщика сервиса <https://wiki.astralinux.ru/display/doc/FreeIPA>.



Примечание. В настоящем руководстве в качестве примера IP-адреса сервера FreeIPA указывается 192.168.10.1; в качестве имени домена FreeIPA указывается freeipa.aladdin.local.

2. На компьютерах, на которых предполагается устанавливать сервер JMS, сервер СУБД, JMS-клиенты и консоль управления JMS, должен быть установлен клиентский компонент FreeIPA. Все перечисленные типы компьютеров следует зарегистрировать в одном и том же домене

FreeIPA. При установке рекомендуется использовать руководство поставщика сервиса <https://wiki.astralinux.ru/display/doc/FreeIPA>.

3. В сетевой доступности для сервера JMS должен быть установлен сервер СУБД PostgreSQL версии 9.6.10. При установке могут быть полезны рекомендации поставщика СУБД, см. <https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362076>.
4. На компьютерах, на которых предполагается устанавливать сервер JMS, в зависимости от операционной системы должно быть установлено соответствующее дополнительное ПО поддержки протокола NTLM SSP (Табл. 4).

Табл. 4 – Пакеты дополнительного ПО поддержки NTLM SSP для разных версий ОС Linux

ОС	Имя файла дистрибутива дополнительного ПО
Astra Linux	gss-ntlmssp_0.7.0-3_amd64
ОС Альт	gssntlmssp-0.7.0-alt1.M80P.2.x86_64
РЕД ОС	gssntlmssp-0.7.0-2.el7.x86_64

Кроме перечисленных выше подготовительных действий, может быть подготовлен сертификат для подсистемы аутентификации JMS (для подписывания JWT-токенов) со следующими параметрами:

- сертификат должен быть выпущен для хоста сервера JMS (в сертификате должно быть указано доменное имя данного хоста в каталоге FreeIPA);
- назначение ключа подписи:

```
keyUsage = digitalSignature, keyEncipherment
```

В результате выпуска сертификата должен быть получен файл контейнера сертификата с закрытым ключом (файл .pfx).



Примечание. В настоящем руководстве в качестве примера JWT-сертификата используется самоподписанный сертификат.

В случае если сертификат для подсистемы аутентификации JMS не установлен, то используется подпись JWT-токенов внутренними ключами сервера JMS (подробнее см. использование команды `Aladdin.EAP.Agent.Terminal jwt configure --useCertificate false`, раздел «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 37)

5.2 Установка и первоначальная настройка сервера и консольного агента JMS



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

5.2.1 Подготовительные действия

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

1. Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки JMS, следующие файлы:
 - aladdin-eap-engine_x.x.x.xxxx-x64.deb
 - InitialConfiguration.ini

2. В предварительно созданную папку (в текущем документе в качестве примера используется папка `/opt/licenses`) скопируйте файл лицензии (с расширением `.lic`), полученный у поставщика продукта.
3. В папке с `deb`-файлом сервера создайте файл первоначальной конфигурации сервера JMS `InitialConfiguration.ini` по следующему образцу:

```
[service]
execPath=/opt/eap-engine/Aladdin.EAP.Engine
integrationManagerUrls=http://*:8120
controlManagerUrls=http://localhost:8119
authenticationManagerUrls=http://*:8121
clientManagerUrls=http://*:8122

[database]
type=PostgreSQL
serverAddress=freeipa.aladdin.local
serverPort=5432
databaseName=JMS4DB
serverLogin=postgres
serverPassword=P@ssw0rd
databaseLogin=postgres
databasePassword=P@ssw0rd

[accountSystem]
type=FreeIPA
serverAddress=192.168.10.1
serverPort=389
container=dc=aladdin,dc=local
userName=uid=admin,cn=users,cn=accounts,dc=aladdin,dc=local
password=P@ssw0rd

[primaryUser]
accountName=admin

[licenses]
path=/opt/licenses/EAP.lic

[sts]
certificateThumbprint=4CEFFDE06B759319EA9946D78BEB28A25C3DB14D
```

В параметре `path` из секции `[licenses]` укажите имя файла лицензии вместе с полным путем к нему, созданного на шаге 2.

Назначение остальных параметров файла конфигурации приведено в разделе «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 33.

4. На хосте с установленной СУБД PostgreSQL следует установить дополнительный компонент с помощью следующей команды:

```
apt install postgresql-contrib
```

5.2.2 Установка компонентов сервера JMS

1. Установите на текущем хосте сервер JMS с помощью следующей команды:

```
dpkg -i /var/jms4/distr/aladdin-eap-engine_x.x.x.xxxx-x64.deb
```

По окончании успешной установки должна отобразиться информация следующего вида:

```

dpkg: предупреждение: анализ файла «/var/lib/dpkg/tmp.ci/control» около строки 9 пакета «eap-engine»:
отсутствует description
dpkg: предупреждение: анализ файла «/var/lib/dpkg/tmp.ci/control» около строки 9 пакета «eap-engine»:
отсутствует maintainer
Выбор ранее не выбранного пакета eap-engine.
(Чтение базы данных ... на данный момент установлено 149393 файла и каталога.)
Подготовка к распаковке .../eap-engine-4.0.0.5100.deb ...
Распаковывается eap-engine (4.0.0.5100) ...
Настраивается пакет eap-engine (4.0.0.5100) ...
[Unit]
Description=EAP Engine Service
DefaultDependencies=no
[Service]
Type=simple
RemainAfterExit=no
ExecStart=/usr/bin/sudo /opt/eap-engine/Aladdin.EAP.Engine
WorkingDirectory=/opt/eap-engine
User=root
Group=root
[Install]
WantedBy=multi-user.target
Created symlink /etc/systemd/system/multi-user.target.wants/eap-engine.service → /etc/systemd/system/eap-engine.service.

```

Рис. 1 – Информация в консоли в случае успешной установки сервера JMS

2. Выполните начальное конфигурирование сервера JMS с помощью следующей команды консольного агента:

```

/opt/eap-engine/eap-agent/Aladdin.EAP.Agent.Terminal server initialize -p
/var/jms4/conf/InitialConfiguration.ini

```



Примечание. Полное описание команд консольного агента см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 37.

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

```

Чтение лицензий из директории /opt/licenses...
/opt/eap-engine/HostConfig.xml
Конфигурация базы данных...
База данных JMS4DB создана успешно.
Остановка EAP-сервиса...
Конфигурация EAP-сервиса...
Запуск EAP-сервиса...
EAP-сервис запущен.
Запуск мастера-настройки...
Инициализация сервера завершена успешно.
root@jmsserver:/opt/licenses# █

```

Рис. 2 – Сообщение в консоли об успешной начальной настройке сервера JMS

3. Проверьте статус службы сервера JMS следующей командой.

```

systemctl status eap-engine

```

Состояние должно быть «active (running)»:

```

root@jmsserver:/opt/licenses# systemctl status eap-engine
● eap-engine.service - EAP Engine Service
   Loaded: loaded (/etc/systemd/system/eap-engine.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-04-01 12:46:42 MSK; 40s ago
     Main PID: 14782 (sudo)
       Tasks: 33 (limit: 4915)
    CGroup: /system.slice/eap-engine.service
            └─14782 /usr/bin/sudo /opt/eap-engine/Aladdin.EAP.Engine
              └─14784 /opt/eap-engine/Aladdin.EAP.Engine

apr 01 12:46:53 jmsserver.aladdin.local Aladdin.EAP.Engine[14784]: ConfigurationManager: Изм

```

Рис. 3 – Отображение статуса службы сервера JMS

4. Проверьте статус сервера бизнес-логики JMS с помощью следующей команды консольного агента

```
/opt/eap-engine/eap-agent/Aladdin.EAP.Agent.Terminal server status
```

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

5.3 Установка и первоначальная настройка серверного web-приложения Консоль управления JMS

5.3.1 Подготовительные действия

Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки серверного Web-приложения, файл `aladdin-eap-web-admin_x.x.x.xxxx_x64.deb`

5.3.2 Установка серверного компонента Консоли управления JMS



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

1. Установите серверный компонент web-приложения Консоль управления JMS с помощью следующей команды:

```
dpkg -i /var/jms4/distr/aladdin-eap-web-admin_x.x.x.xxxx_x64.deb
```

По окончании успешной установки должна отобразиться информация следующего вида:

```
Настраивается пакет eap-admin-web (4.0.0.30) ...
[Unit]
Description=EAP WebAdmin Service
DefaultDependencies=no
[Service]
Type=simple
RemainAfterExit=no
Restart=always
RestartSec=10
ExecStart=/opt/eap-admin-web/Aladdin.EAP.Admin.Web
WorkingDirectory=/opt/eap-admin-web
User=root
Group=root
[Install]
WantedBy=multi-user.target
Created symlink /etc/systemd/system/multi-user.target.wants/eap-web-admin.service → /etc/sys
```

Рис. 4 – Информация в консоли в случае успешной установки серверного web-приложение Консоль управления JMS

2. В папке `/opt/eap-admin-web/` отредактируйте файл `appsettings.json`. Исходная версия данного файла конфигурации выглядит следующим образом:

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "AllowedHosts": "*",
```



```
"IntegrationApiUrl": "http://localhost:8120",
"AuthenticationApiUrl": "http://localhost:8121",

"Kestrel": {
  "Endpoints": {
    "Http": {
      "Url": "http://0.0.0.0:5000"
    }
  }
}
```

В случае если серверный компонент консоли управления JMS установлен на хосте, отличном от хоста с сервером JMS, то в полях *IntegrationApiUrl* и *AuthenticationApiUrl* следует указать адрес хоста с сервером JMS (номера портов следует сохранить прежними).

Настройку адреса в параметре *Url* следует выполнять следующим образом:

- если необходимо обеспечить обработку запросов, поступающих только на IPv4-интерфейсы хоста, то в адресе следует указать `http://0.0.0.0:5000` (значение по умолчанию);
- если необходимо обеспечить обработку запросов, поступающих только на IPv6-интерфейсы хоста, то в адресе следует указать `http://[::]:5000`;
- если необходимо обеспечить обработку запросов, поступающих на все IPv4- и IPv6-интерфейсы хоста, то в адресе следует указать `http://*:5000`;
- если необходимо обеспечить обработку запросов, поступающих только с локального хоста, то в адресе следует указать `http://localhost:5000` либо `http://127.0.0.1:5000` (`http://[::1]:5000` для IPv6);
- если необходимо обеспечить обработку запросов, поступающих на конкретный интерфейс хоста, то в адресе следует указать адрес данного сетевого интерфейса, например `http://192.168.1.100:5000`;
- в случае если для подключения к серверу используется протоколы SSL/TLS, то следует указать префикс `https` вместо `http`.

При необходимости ограничить поступления запросов из внешней сети по IP-адресам, используйте встроенные сетевые средства операционной системы или внешний межсетевой экран.

3. Перезапустите службу серверного компонента консоли управления JMS, выполнив следующую команду:

```
systemctl restart eap-web-admin
```

4. Проверьте статус службы.

```
systemctl status eap-web-admin
```

Состояние должно быть «active (running)»:


```
● eap-web-admin.service - EAP WebAdmin Service
   Loaded: loaded (/etc/systemd/system/eap-web-admin.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-04-01 12:51:40 MSK; 8s ago
     Main PID: 15105 (Aladdin.EAP.Adm)
        Tasks: 18 (limit: 4915)
   CGroup: /system.slice/eap-web-admin.service
           └─15105 /opt/eap-admin-web/Aladdin.EAP.Admin.Web

app 01 12:51:40 jmsserver.aladdin.local systemd[1]: Stopped EAP WebAdmin Service.
app 01 12:51:40 jmsserver.aladdin.local systemd[1]: Started EAP WebAdmin Service.
app 01 12:51:41 jmsserver.aladdin.local Aladdin.EAP.Admin.Web[15105]: info: Microsoft.Hosting.L
```

Рис. 5 – Отображение статуса службы серверного компонента консоли управления JMS

- Для проверки корректности установки web-приложения Консоль управления JMS на хосте с сервером JMS запустите веб-браузер Firefox и введите в нем адрес, установленный на шаге 2 в конфигурационном файле `appsettings.json` для атрибута `Url` (по умолчанию <http://localhost:5000>).
Отобразится страница следующего вида.

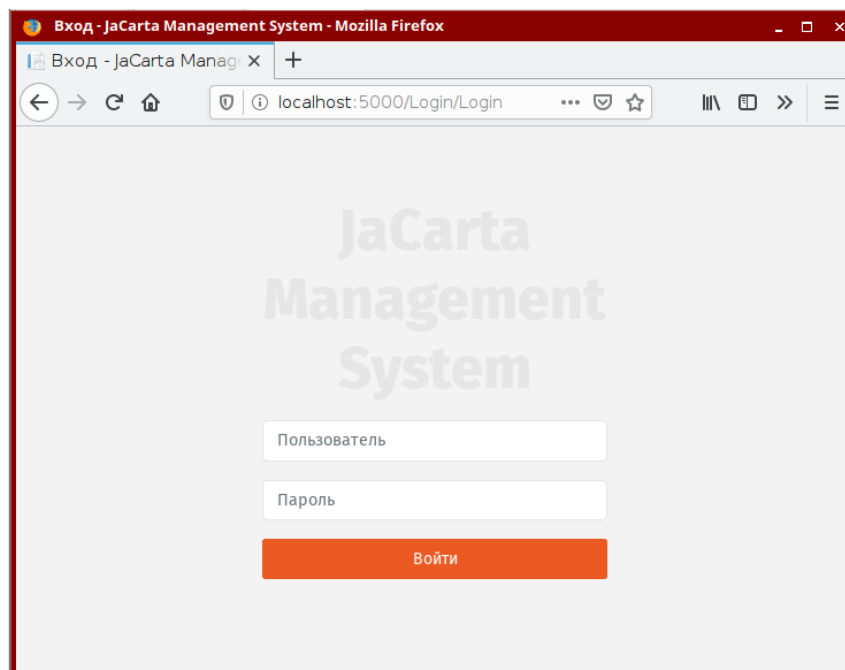


Рис. 6 – Стартовая страница Web-приложения Консоль управления JMS

5.4 Установка и первоначальная настройка JMS Web Agent (JWA)

Компонент JWA следует устанавливать на компьютерах, предназначенных для работы из клиентских web-приложений (Клиент JMS и Консоль управления JMS).



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

5.4.1 Подготовительные действия

Для подготовки к развертыванию компонента JMS Web Agent (JWA) выполните следующие действия.

- Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки JWA, следующие файлы:
 - `jsrcks11-2_x.x.x.xxx_al1.6_x64.deb` – единая библиотека JaCarta;

- aladdin-jms-web-agent_x.x.x.xxx_x64.deb – файл дистрибутива JWA.
2. Для корректной работы Единой библиотеки JaCarta установите фоновую службу PC/SC следующей командой:

```
apt install pcscd
```

3. Установите единую библиотеку JaCarta следующей командой:

```
dpkg -i jcpkcs11-2_x.x.x.xxx_all1.6_x64.deb
```

При успешной установке должна отобразиться информация следующего вида:

```
Распаковывается jcpkcs11-2 (2.7.0.461) ...
Настраивается пакет jcpkcs11-2 (2.7.0.461) ...
searching for Info.plist to update...
checking /etc/libccid_Info.plist
updating /etc/libccid_Info.plist
update_ifd_ccid_bundle.sh [user.warning] No need to update any section
update_ifd_ccid_bundle.sh [user.warning] No need to update any section
update_ifd_ccid_bundle.sh [user.warning] No need to update any section
update_ifd_ccid_bundle.sh [user.warning] No need to update any section
checking updated /etc/libccid_Info.plist
pcscd version 1.8.24.
[ ok ] Restarting pcscd (via systemctl): pcscd.service.
```

Рис. 7 – Индикация успешной установки единой библиотеки JaCarta

5.4.2 Установка JWA

1. Установите компонент JMS Web Agent (JWA), выполнив следующую команду

```
dpkg -i /var/jms4/distr/aladdin-jms-web-agent_x.x.x.xxx_x64.deb
```

По окончании успешной установки должна отобразиться информация следующего вида:

```
ExecStart=/usr/bin/sudo /opt/jms-client/Aladdin.JMS.WebAgent
WorkingDirectory=/opt/jms-client
User=root
Group=root
[Install]
WantedBy=multi-user.target
Set Aladdin JMS Web Agent to start at boot ...
Running jwa-service ...
Created symlink /etc/systemd/system/multi-user.target.wants/jwa-service.service → /etc/sys
```

Рис. 8 – Индикация успешной установки компонент JMS Web Agent

2. Выполните остановку демона JWA командой:

```
systemctl stop jwa-service
```

3. Выполните конфигурирование компонента JWA на текущем хосте с помощью команды следующего вида

```
<путь>/Aladdin.JMS.WebAgent --jms-host <Сервер_JMS> --jms-web-host
<Сервер_JMS_Web_Admin>
```

где <путь> – путь к исполняемому файлу JWA;
 <Сервер_JMS> – FQDN-имя сервера JMS;
 <Сервер_JMS_Web_Admin> – FQDN-имя сервера с серверным компонентом «Консоль управления JMS».

Например:

```
/opt/jms-client/Aladdin.JMS.WebAgent --jms-host jmsserver.aladdin.local --jms-web-host jmsserver.aladdin.local
```

По окончании успешного конфигурирования в консоли должна отобразиться строка «Configuration appsettings.json is updated».

4. Запустите демон JWA командой:

```
systemctl start jwa-service
```

5. Для проверки корректности работы службы JWA на данном хосте запустите веб-браузер Firefox и перейдите в нем по адресу <https://localhost:5600>. Отобразится страница следующего вида.

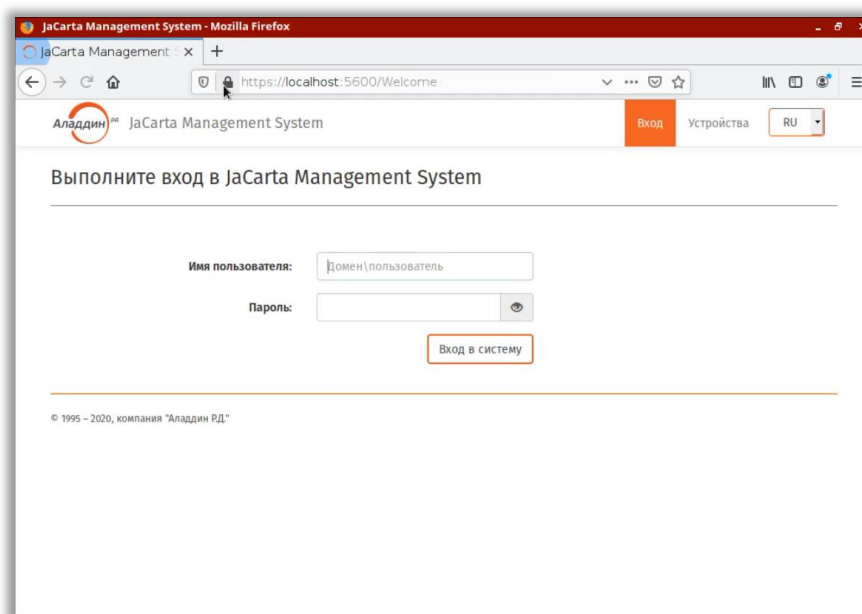


Рис. 9 – Стартовая страница Web-приложения Консоль управления JMS

6. При необходимости выполните дополнительную настройку компонента JWA путем редактирования файла `/etc/aladdin/jwa-service/appsettings.json`

5.5 Проверка работы web-приложения Консоль управления JMS

1. С внешней машины в веб-браузере выполните подключение к веб-консоли JMS по адресу

```
http://<IP-адрес_сервера_web-консоли>:5000
```

где `<IP-адрес_сервера_web-консоли>` – IP-адрес или FQDN-имя компьютера с установленным серверным web-приложением Консоль управления JMS.



Примечание. В случае настройки защищенного соединения по SSL/TLS в адресе укажите `https://`

Отобразится страница следующего вида.

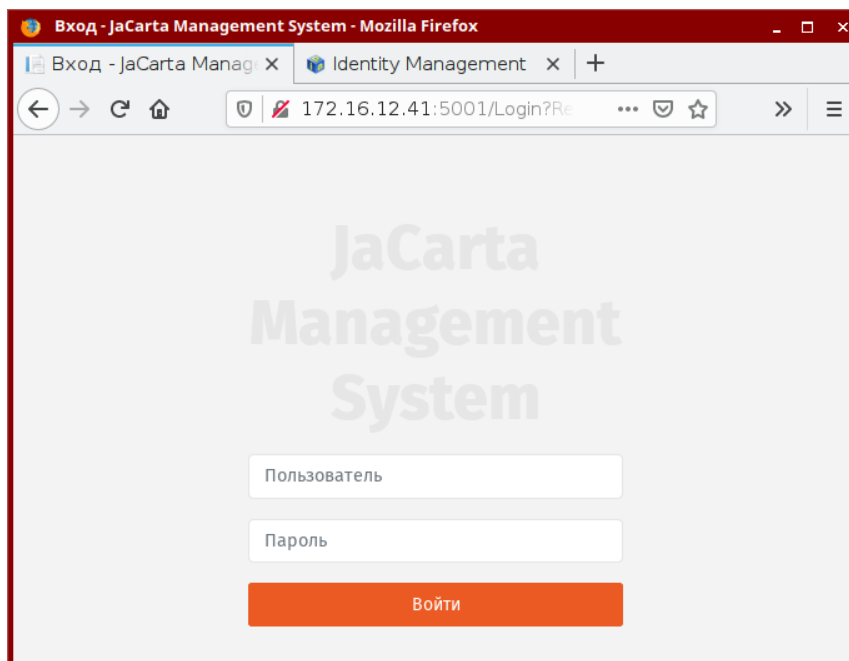


Рис. 10 – Доступ к web-консоли JMS с внешнего компьютера

2. В поле **Пользователь** введите логин пользователя в формате:
<имя_ресурсной_системы>\<имя_пользователя>,
где <имя_ресурсной_системы> – значение, указанное в поле [accountSystem] -> name
файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной
конфигурации сервера JMS», с. 33).
Например:

```
astratest.local\admin
```

После ввода аутентификационных данных отобразится страница следующего вида.

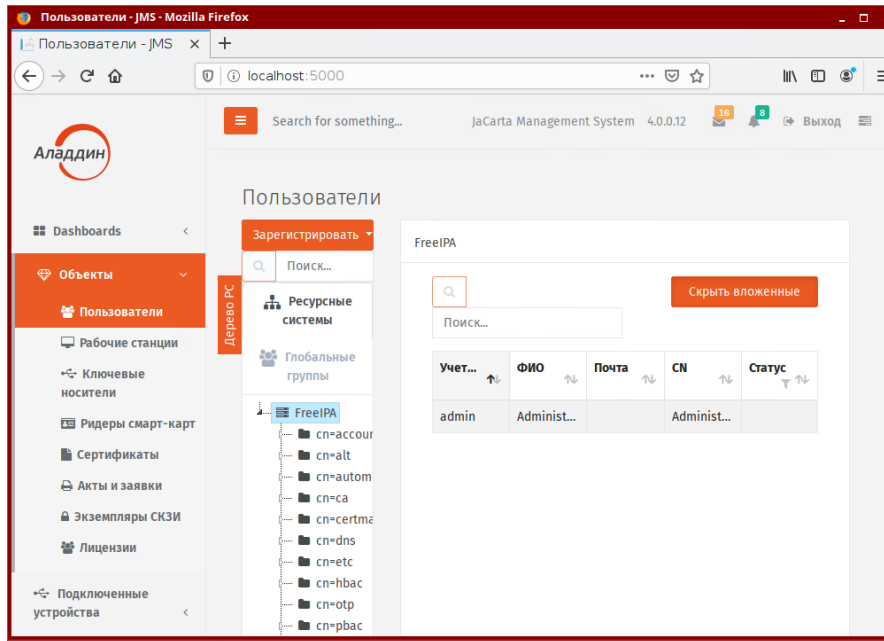


Рис. 11 – Стартовая страница web-приложения Консоль управления JMS

Web-приложение Консоль управления JMS готово к работе.

6. Порядок обновления компонентов JMS

Обновление JMS осуществляется в следующем порядке:

1. «Остановка служб компонентов JMS», с. 21;
2. «Резервное копирование БД JMS», с. 22;
3. «Удаление компонентов JMS», с. 22;
4. «Установка новой версии сервера JMS (в рамках обновления продукта)», с. 22;
5. «Обновление БД JMS», с. 22;
6. «Установка остальных компонентов JMS (в рамках обновления продукта)», с. 22;
7. «Запуск и проверка работоспособности компонентов JMS», с. 22.

6.1 Остановка служб компонентов JMS

Выполните остановку служб компонентов следующими командами.

1. Для остановки серверного компонента web-приложения Консоль управления JMS выполните команду:

```
systemctl stop eap-web-admin
```

2. Для остановки службы сервера JMS выполните команду:

```
systemctl stop eap-engine
```

3. Для остановки службы компонента JWA выполните команду:

```
systemctl stop jwa-service
```

6.2 Резервное копирование БД JMS

Выполните резервное копирование БД JMS средствами СУБД (PostgreSQL).

6.3 Удаление компонентов JMS

Для удаления компонентов JMS выполните следующие команды.

1. Для удаления серверного компонента web-приложения Консоль управления JMS выполните команду:

```
apt remove eap-web-admin
```

2. Для удаления сервера JMS и консольного агента выполните команду:

```
apt remove eap-engine
```

3. Для удаления службы компонента JWA выполните команду:

```
apt remove aladdin.jms.webagent
```

6.4 Установка новой версии сервера JMS (в рамках обновления продукта)

Установите новую версию компонента `aladdin-eap-engine_x.x.x.xxxx.deb` (при обновлении сервера не потребуется повторно создавать и настраивать файл первоначальной конфигурации `InitialConfiguration.ini`: системный конфигурационный файл сервера JMS при обновлении продукта берется в качестве исходного при конфигурировании новой версии продукта).

6.5 Обновление БД JMS

Для обновления БД JMS выполните следующую команду консольного агента:

```
/opt/eap-engine/eap-agent/Aladdin.EAP.Agent.Terminal server update
```

6.6 Установка остальных компонентов JMS (в рамках обновления продукта)

Для установки остальных компонентов новой версии JMS выполните следующие действия.

1. Установите новую версию серверного компонента web-приложения Консоль управления JMS (по аналогии с разделом «Установка серверного компонента Консоли управления JMS», с. 15)
2. Установите компонент JWA на всех хостах с клиентскими web-приложениями JMS (Клиент JMS и Консоль управления JMS), руководствуясь разделом «Установка JWA», с. 18.

6.7 Запуск и проверка работоспособности компонентов JMS

Выполните запуск и проверку работы компонентов JMS в соответствии описаниями в разделе «Установка и первоначальная настройка», с. 11.

7. Журналы диагностики JMS


Файлы журналов диагностики JMS записываются по умолчанию в каталог `/var/log/aladdin`, в частности в каталоги:

- `/var/log/aladdin/eap-engine` – журнал диагностики сервера JMS;
- `/var/log/aladdin/eap-agent` – журнал диагностики консольного агента сервера JMS;

- /var/log/aladdin/eap-admin-web – журнал диагностики серверного компонента консоли управления JMS;
- /var/log/aladdin/jwa-service – журнал диагностики JWA.

8. Обеспечение целостности и защиты от несанкционированного доступа файлов ПО JMS

Чтобы обеспечить целостность ПО JMS, директории для установки его компонентов не должны быть доступны пользователям, не являющимся администраторами сервера (хоста).

 **Примечание.** Директории для развертывания компонентов указываются в разделах настоящего документа с описанием установки продукта.

9. Настройка функций безопасности среды функционирования объекта оценки (JMS)

Для защиты информации, хранящейся в БД ПО JMS, следует установить и настроить наложенное криптографическое средство защиты информации (СКЗИ) «Крипто БД».

Установку и настройку СКЗИ «Крипто БД» для работы с JMS следует производить в соответствии разделом «Установка и настройка плагина СКЗИ «Крипто БД» для JMS», ниже.

Для обеспечения работы компонентов JMS, взаимодействующих с аппаратными средствами аутентификации и ЗНИ, требуется установка и настройка ПК «Единый Клиент JaCarta» [4].

В остальном объект оценки (JMS) не накладывает дополнительных требований к настройке среды функционирования.

Для управления настройкой элементов среды функционирования (операционных систем) объекта оценки следует использовать документацию из комплекта поставки данных ОС.

10. Установка и настройка плагина СКЗИ «Крипто БД» для JMS

СКЗИ «Крипто БД» предназначено для обеспечения конфиденциальности и контроля целостности информации, хранящейся в таблицах баз данных СУБД PostgreSQL, посредством криптографического преобразования и имитозащиты.

Использование наложенного сертифицированного СКЗИ «Крипто БД» для защиты таблиц БД JMS является обязательным для сертифицированной версии ПО JMS.

Для интеграции ПО JMS с СКЗИ «Крипто БД» необходимо выполнить следующие шаги.

1. Установить плагины для eap-engine и eap-agent:

```
sudo apt-get install ./eap-agent-cryptodb.1.0.0.deb
sudo apt-get install ./eap-engine-cryptodb.1.0.0.deb
```

2. Перезагрузить сервис JMS:

```
sudo systemctl stop eap-engine
sudo systemctl start eap-engine
```

3. Выполнить сборку и настройку pljava-расширения для СУБД PostgreSQL (см. «Приложение 3. Инструкция по сборке расширения pljava для СУБД PostgreSQL 9.6 под ОС Astra Linux Орел или Смоленск», с. 48)

4. Убедиться, что для текущей БД JMS рljava успешно проинициализирована и работает (в БД есть схема sqlj)
5. Выгрузить текущую конфигурацию JMS при помощи команды консольного агента:

```
Aladdin.EAP.Agent.Terminal cryptodb config --path /tmp/EAPDB.xml
```

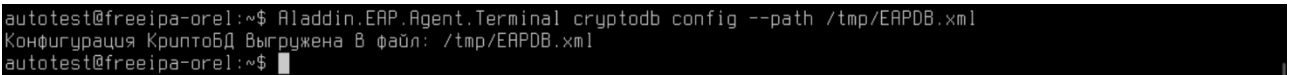


Рис. 12 – Индикация успешной выгрузки конфигурации Крипто БД в файл

6. Перед шифрование базы данных настоятельно рекомендуется остановить сервис JMS:

```
sudo systemctl stop eap-engine
```

7. При помощи Мастера Конфигурирования КриптоБД выполнить подключение к СУБД PostgreSQL. Указать опцию создания новой учетной записи администратора безопасности:

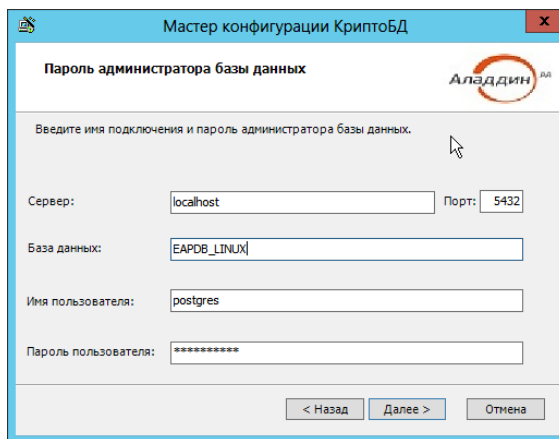


Рис. 13 – Мастер конфигурирования СКЗИ «Крипто БД»

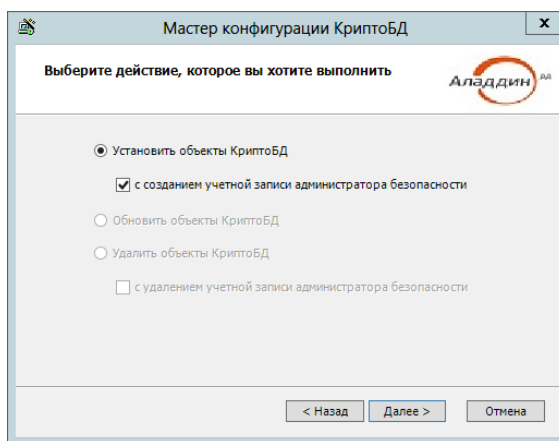


Рис. 14 – Окно выбора действия в конфигураторе СКЗИ «Крипто БД»

8. Ввести имя администратора, пароль и схему для хранения объектов «Крипто БД»:

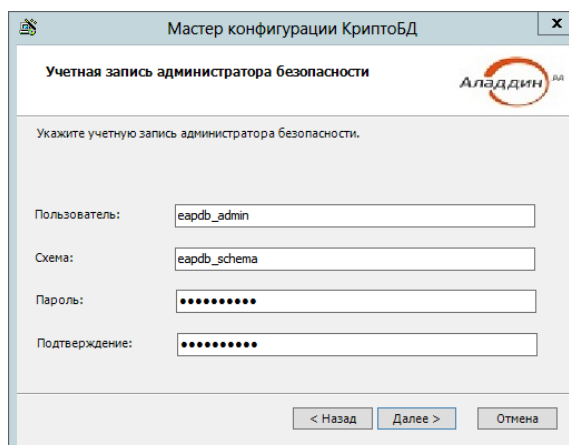


Рис. 15 – Окно создания учетной записи администратора безопасности СКЗИ «Крипто БД»

9. На следующем шаге указать путь к ранее выгруженному файлу конфигурации и пароль к серверу ключей (пароль контейнера по умолчанию – 1234567890)

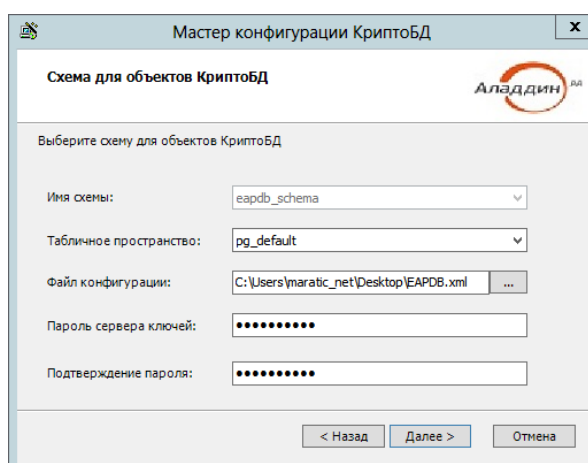


Рис. 16 – Окно формирования схемы объектов СКЗИ «Крипто БД» для БД JMS

10. Далее выполняется развертывание объектов «Крипто БД».
11. После успешного развертывания необходимо открыть Консоль КриптоБД и подключиться к ней с использованием только что созданного администратора. Убедиться, что обе таблицы зашифровались:

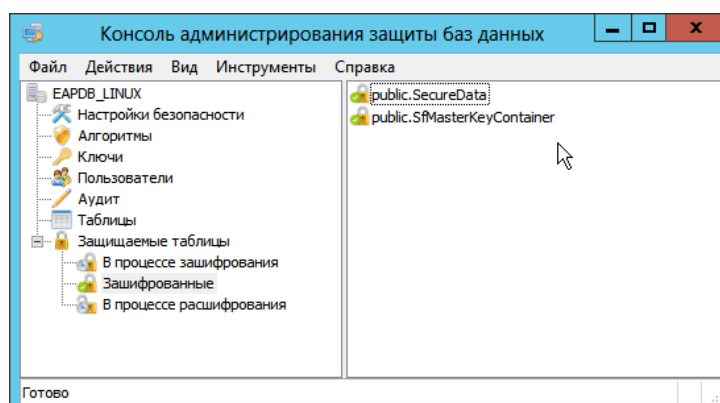


Рис. 17 – Проверка состава зашифрованных таблиц

12. Смонтировать КриптоБД
13. Запустить сервис JMS:

```
sudo systemctl start eap-engine
```

14. При помощи консольного агента убедиться, что «Крипто БД» готова к работе – Сервер ключей КриптоБД должен быть запущен:

```
Aladdin.EAP.Agent.Terminal cryptodb status
```

```
autotest@freeipa-orel:~$ Aladdin.EAP.Agent.Terminal cryptodb status
Текущее состояние КриптоБД: Mounted [Сервер ключей КриптоБД запущен. Работа JMS с шифрованными данными разрешена]
autotest@freeipa-orel:~$
```

Рис. 18 – Индикация успешной запуски сервера ключей Крипто БД

11. Утилита сбора диагностической информации о JMS

В состав каждого из компонентов JMS (сервера JMS, серверного web-приложения консоли управления) входит утилита сбора диагностической информации *Aladdin.EAP.DiagInfo.Terminal*, которая позволяет произвести диагностику установленного компонента (или всех установленных на данном хосте). Утилита устанавливается автоматически вместе с устанавливаемым компонентом из дистрибутива. Сбор диагностической информации упаковывается в архивный zip-файл с указанным местом расположения. Опционально предусмотрена генерация отчета о сборе диагностической информации.

Утилита служит для помощи в случаях сложного отказа системы с привлечением специалистов службы поддержки компании-производителя. По окончании процедуры сбора диагностической информации полученные файлы следует направить в службу поддержки компании «Аладдин».

Чтобы выполнить сбор диагностической информации, выполните следующие действия.

1. Проверьте корректность конфигурационного файла */opt/eap-diaginfo/Configuration/ProductConfiguration.json*, установленного по умолчанию:

```
[
  {
    "ProductName": "Aladdin R.D. JMS Server",
    "Path": "/opt/eap-engine",
    "LogConfigurationFile": "Aladdin.EAP.Engine.log4net",
    "OutputFormat": "Json",
    "ConfigFiles": [
      "*.config",
      "*.xml",
      "*.json",
      "/etc/aladdin/eap-engine/AppSettings.json"
    ]
  },
  {
    "ProductName": "Aladdin R.D. JMS Agent-Terminal",
    "Path": "/opt/eap-engine/eap-agent",
    "LogConfigurationFile": "Aladdin.EAP.Agent.Terminal.log4net",
    "OutputFormat": "Json",
    "ConfigFiles": [
      "*.config",
      "*.xml",
      "*.json"
    ]
  },
  {
    "ProductName": "Aladdin R.D. JMS Web Admin",
    "Path": "/opt/eap-web-admin",
    "LogConfigurationFile": "log4net.config",
    "OutputFormat": "Json",
    "ConfigFiles": [
```

```

        "*.config",
        "*.xml",
        "*.json"
    ]
}
]
    
```

При необходимости внесите коррективы в конфигурационный файл. Описание параметров конфигурационного файла приведено в Табл. 5.

Табл. 5 – Параметры конфигурационного файла утилиты сбора диагностической информации

Параметр	Описание
ProductName	Наименование компонента продукта
Path	Путь к компоненту продукта
LogConfigurationFile	Путь к конфигурационному файлу подсистемы логгирования относительно пути к компоненту
OutputFormat	Тип конечных сериализуемых данных Json/XML (к примеру, информация об окружении)
ConfigFiles	Маска для определения конфигурационных файлов в папке с компонентом продукта, полный путь к конфигурационному файлу

- Запустите на выполнение утилиту диагностики (*Aladdin.EAP.DiagInfo.Terminal*) командой следующего вида.

```

sudo /opt/eap-diaginfo/Aladdin.EAP.DiagInfo.Terminal --zip /mnt/documents/JMS_4LX-Distrib/_diags/2021_09_01_JMS4LX_diags.zip --report /mnt/documents/JMS_4LX-Distrib/_diags/2021_09_01_JMS4LX_diags_report.txt
    
```

Ключи команды приведены в Табл. 6 (ниже).

В случае успешного выполнения производится выдача следующего вида.

```

-Aladdin R.D. JMS Web Admin
 1. Окружение - Выполнено
 2. Информация о файлах - Выполнено
 3. Конфигурационные файлы - Выполнено
 4. Лог-файлы - Выполнено

-Сохранение результатов
 1. Создание архива - Выполнено

Архив с данными диагностики сохранён по пути '/mnt/documents/JMS_4LX-Distrib/_diags/2021_09_01_JMS4LX_diags.zip'
Отчёт сохранён по пути '/mnt/documents/JMS_4LX-Distrib/_diags/2021_09_01_JMS4LX_diags_report.txt'
    
```

Рис. 19 – Выдача утилиты сбора диагностической информации

Табл. 6 – Ключи команды *Aladdin.EAP.DiagInfo.Terminal* с примерами использования

Ключ команды	Описание	Обязателен	Значение ключа по умолчанию	Пример
--zip	Путь к конечному Zip-архиву	Нет	'<личная папка пользователя>/JMS Diagnostic Data/<yyyy.mm.dd_hh-mm>_DiagnosticData.zip'	--zip /home/admin/diagnosticData.zip
--report	Путь к конечному файлу отчёта	Нет	Нет	--report /home/admin/diagnosticReport.txt

12. Настройка SSL для доступа к ресурсной системе

Для корректной работы с Samba AD или AD через SSL необходимо чтобы используемый серверный сертификат был доверенным и параметр `serverAddress` (см. секцию [accountSystem] файла конфигурации, см «Секция accountSystem», с. 34) совпадал с CN сертификата или Subject Alternative Name. В общем случае, если машина с сервером JMS не заведена в домен Samba AD или AD, следует выполнить следящий набор действий:

1. Добавить доменное имя машины с Samba AD в `/etc/hosts` серверной машины JMS.
2. Получить корневой сертификат ресурсной системы. Для Samba AD найти его можно командой «`sudo find / -name ca.pem`», обычно он находится в `/var/lib/samba/private/tls`. Для AD необходимо экспортировать корневой сертификат в формате «Base-64 encoded x.509»
3. После чего полученный сертификат необходимо сделать доверенным на машине с сервером JMS в соответствии с установленной на ней операционной системой:
 - Astra Linux
 - Убедиться, что установлен пакет `ca-certificates` (если нет, то поставить - "`apt-get install ca-certificates`")
 - Скопировать сертификат в `/usr/local/share/ca-certificates/`
 - Выполнить "`update-ca-certificates`"
 - РЕД ОС
 - Убедиться, что установлен пакет `ca-certificates` (если нет, то поставить - "`yum install ca-certificates`")
 - Выполнить "`update-ca-trust force-enable`"
 - Скопировать сертификат в `/etc/pki/ca-trust/source/anchors/`
 - Выполнить "`update-ca-trust extract`"
 - Alt Linux
 - Убедиться, что установлен пакет `ca-certificates` (если нет, то поставить - "`apt-get install ca-certificates`")
 - Скопировать сертификат в `/etc/pki/ca-trust/source/anchors/`
 - Выполнить "`update-ca-trust`"

Если же есть необходимость использовать Samba AD без SSL, то необходимо убедиться, что строка «`ldap server require strong auth = no`» присутствует в `/etc/samba/smb.conf`, если нет, то добавить её. Эта настройка отвечает за требование SSL со стороны Samba AD при подключении.

13. Активация продукта

Изначально продукт поставляется с «активационной» лицензией. После установки такой лицензии работа продукта в полнофункциональном режиме возможна лишь на протяжении «активационного» периода, определённого в такой лицензии (обычно 2 недели, Рис. 20).

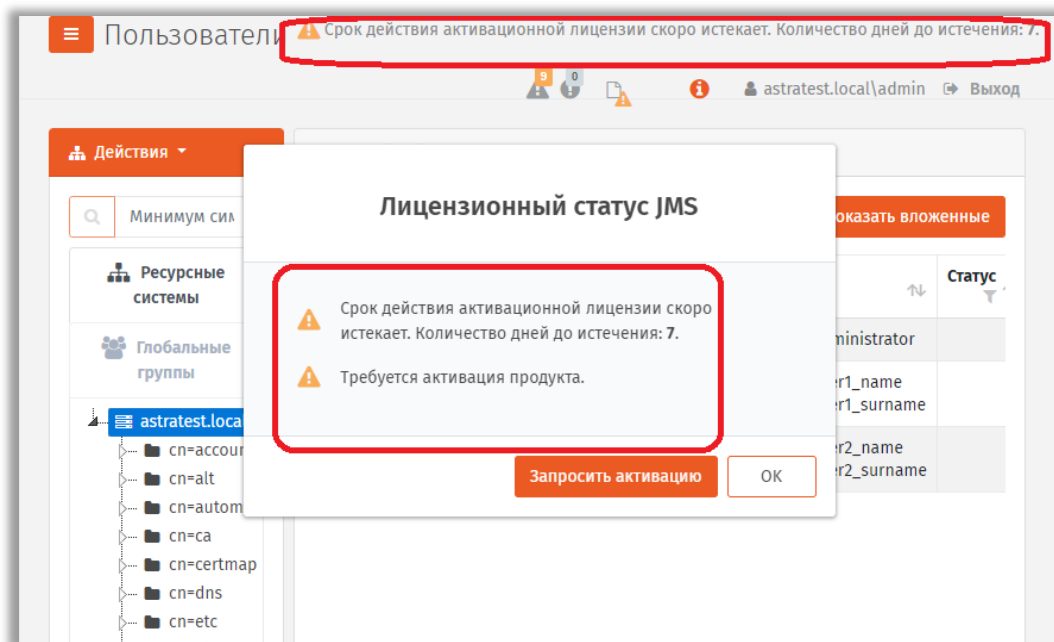


Рис. 20 – Отображение признаков активационной лицензии в консоли управления JMS

По окончании активационного периода все основные функции продукта (кроме возможности замены/установки лицензии) блокируются до момента установки постоянной лицензии, Рис. 21.

Примечание. Активационный период обеспечивает функционирование продукта в тестовом режиме и не входит в фактически оплаченный период действия пользовательской лицензии на продукт.

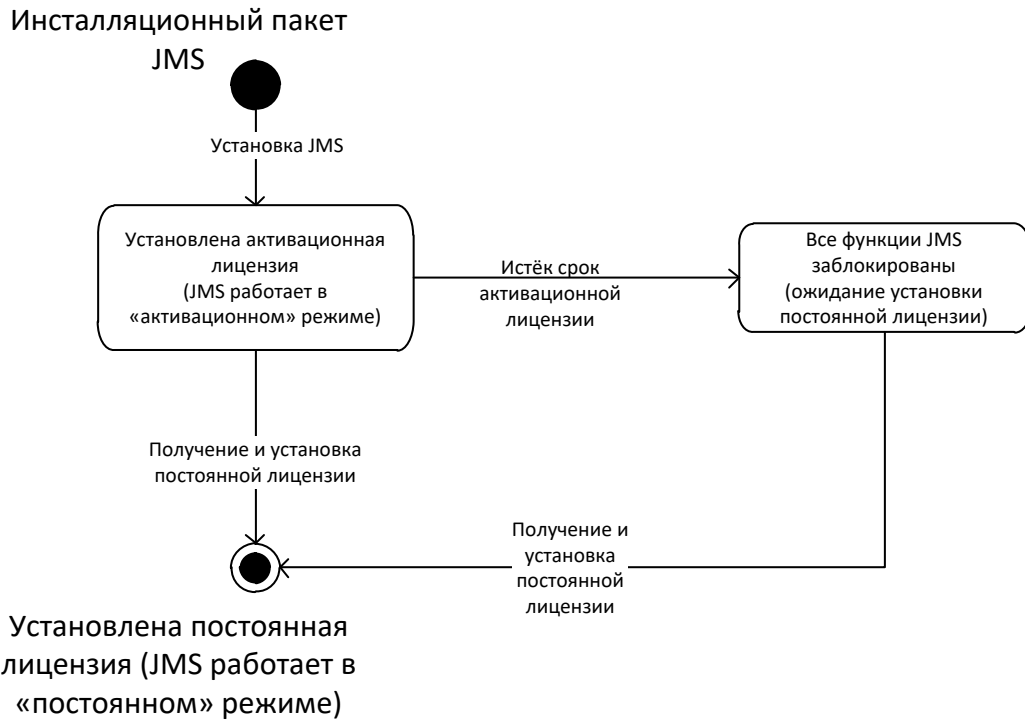


Рис. 21 – Диаграмма переходов для процедуры активации JMS

Для перевода продукта в режим обычной работы («постоянный» режим), следует установить постоянную лицензию (выдается производителем пользователю JMS после создания им файла «Запрос на активацию», который генерируется в интерактивном режиме из консоли управления JMS).

Для формирования запроса на получение постоянной лицензии в окне лицензионного статуса (Рис. 22) следует нажать **Запросить активацию**.

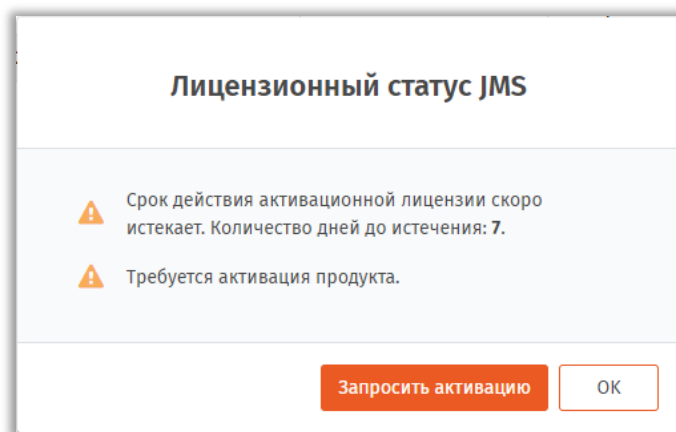


Рис. 22 – Окно лицензионного статуса в Консоли управления JMS

При этом отобразится окно следующего вида (Рис. 23).

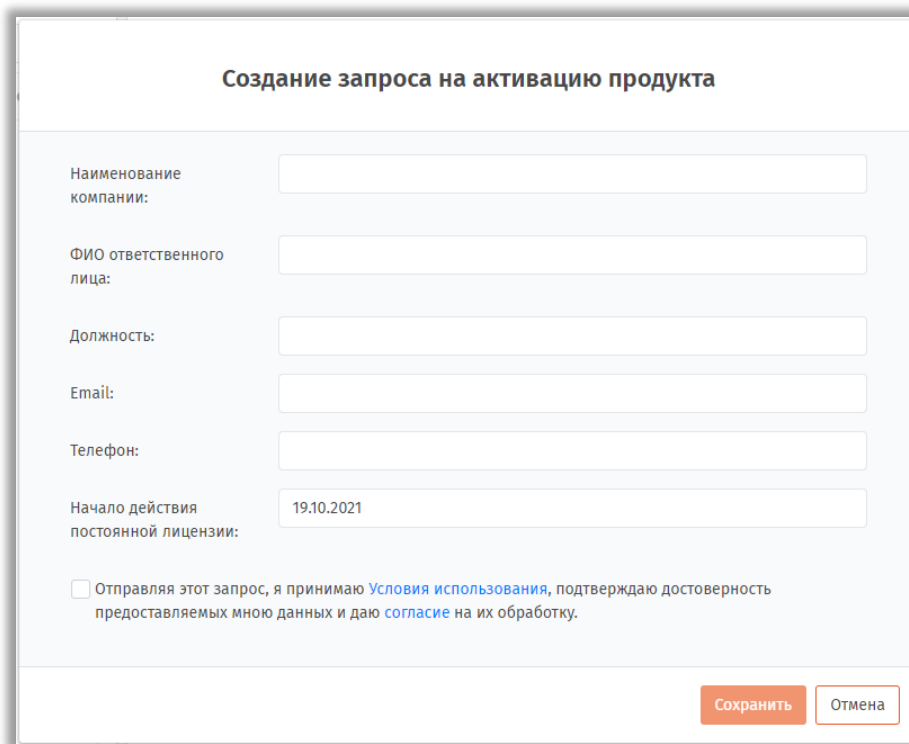


Рис. 23 – Форма запроса учетных данных пользователя JMS

Примечания:

1. Окно запроса лицензионного статуса можно вызвать в любой момент времени, нажав значок лицензии в верхнем правом углу страницы Консоли управления JMS (Рис. 24);
2. Запрос на активацию можно сформировать также с помощью команды `licenses replace` консольного агента; подробное описание формата команды см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 37.

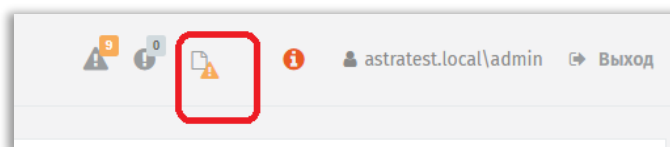


Рис. 24 – Значок для вызова запроса на активацию в неактивированной версии JMS

Заполните поля формы создания запроса на активацию, отметьте флаг согласия с условиями использования продукта и обработки данных и нажмите **Сохранить**. PDF-файл (*JMS_Activation_request.pdf*) с запросом на постоянную лицензию будет автоматически сохранен в папку загрузок web-браузера.

Полученный файл следует отправить по адресу JmsLic@aladdin.ru.

После получения ответа с файлом постоянной лицензии, его следует установить в JMS с помощью команды `licenses replace` консольного агента, например:

```
Aladdin.EAP.Agent.Terminal licenses replace -p /var/jms4/distr/Test_Production_Full.lic
```

На запрос команды имени имя пользователя введите логин пользователя с ролью *Оператор* (в случае начальной установки допускается введение имени пользователя с ролью *Администратор ИБ*) в формате:

```
<имя_ресурсной_системы>\<имя_пользователя>,
```

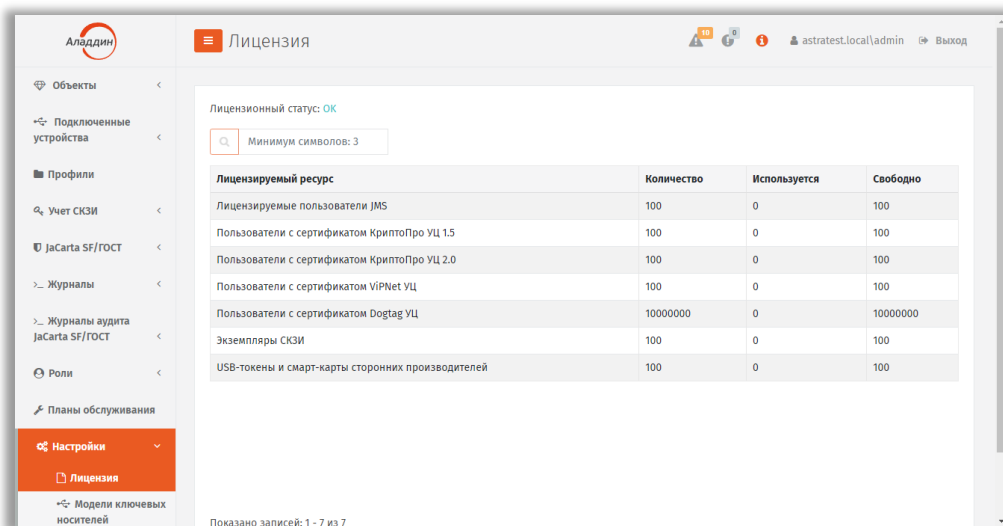
где <имя_ресурсной_системы> – значение, указанное в поле [accountSystem] -> name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 33); и пароль данного пользователя:

```
root@lx-jms4:/var/jms4/distr# Aladdin.EAP.Agent.Terminal licenses replace -p /var/jms4/distr/Test_Production_Full.lic
Введите имя пользователя:
astratest.local\admin
Введите пароль:
Лицензия 3 по пути /var/jms4/distr/Test_Production_Full.lic успешно зарегистрирована.
```

Рис. 25 – Консольный диалог при замене лицензии

Подробное описание формата команды см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 37

Вступившие в силу параметры новой лицензии можно посмотреть в консоли управления в разделе **Настройки -> Лицензия** консоли управления JMS (Рис. 26).



Лицензируемый ресурс	Количество	Используется	Свободно
Лицензируемые пользователи JMS	100	0	100
Пользователи с сертификатом КриптоПро УЦ 1.5	100	0	100
Пользователи с сертификатом КриптоПро УЦ 2.0	100	0	100
Пользователи с сертификатом ViPNet УЦ	100	0	100
Пользователи с сертификатом Dogtag УЦ	10000000	0	10000000
Экземпляры СКЗИ	100	0	100
USB-токены и смарт-карты сторонних производителей	100	0	100

Рис. 26 – Отображение параметров лицензии

Приложение 1. Параметры файла первоначальной конфигурации сервера JMS

Секция service

Настройки сервиса JMS.

Имя настройки	Обязательность наличия	Описание
execPath	Да	Путь до исполняемого файла сервера JMS.
integrationManagerUrls	Нет	Адреса Admin WebAPI: административного API. Можно задать несколько адресов через «;». Для возможности использования API извне, один из адресов должен содержать внешний URL, либо с IP сервера, либо с его доменным именем. Например, « http://localhost:8120 ; http://192.168.2.202:8120 », если машина с сервером JMS имеет IP 192.168.2.202. Значение по умолчанию: http://*:8120
controlManagerUrls	Нет	Адреса Control WebAPI, используемого агентом сервера. Можно задать несколько адресов через «;». Значение по умолчанию: http://localhost:8119
authenticationManagerUrls	Нет	Адреса для Auth WebAPI: общей точки аутентификации для других API. Можно задать несколько адресов через «;». Значение по умолчанию: http://*:8121
clientManagerUrls	Нет	Адреса для Client WebAPI: клиентского API. Можно задать несколько адресов через «;». Значение по умолчанию: http://*:8122
keytabpath	Нет	Путь к KeyTab файлу для Kerberos-аутентификации.

Секция database


Настройки базы данных JMS.

Имя настройки	Обязательность наличия	Описание
type	Да	Тип СУБД. На данный момент поддерживается только одно значение: PostgreSQL
serverAddress	Да	Адрес сервера БД
serverPort	Да	Порт сервера БД
databaseName	Да	Имя создаваемой БД

databaseLogin	Да	Имя пользователя, которое будет использоваться сервером JMS для доступа с создаваемой БД
databasePassword	Да	Пароль пользователя
serverLogin	Нет	Имя пользователя-администратора, который будет использоваться мастером развертывания для создания БД. Если параметр не задан – будет использоваться режим развертывания без наличия административных прав, требующий предварительное создание пустой БД JMS при помощи скриптов.
serverPassword	Нет	Пароль пользователя для мастера развертывания. Не используется в режиме развертывания без наличия административных прав на СУБД.
isCivic	Нет	Флаг отвечающий за режим работы с КН SF/ГОСТ (по умолчанию "true", т.е. гражданский режим)

Секция accountSystem

Настройки первичной ресурсной системы.

Имя настройки	Обязательность наличия	Описание
type	Да	Тип ресурсной системы. В текущей версии поддерживаются только значения: «FreeIPA», «AD», «SambaAD»
name	Нет	Имя ресурсной системы, которое используется внутри JMS. Применяется для идентификации ресурсной системы, например, при аутентификации пользователя. По умолчанию – значение параметра «type».  Примечание. Если в конфигурационном файле опущен параметр «name», то при аутентификации пользователя в качестве доменной части имени следует указывать значение, заданное в параметре «type». Например, если type=FreeIPA, то в качестве логина пользователя admin следует указать «FreeIPA\admin». Если же параметр «name» указан явно (например «astratest.local»), то в качестве доменной части имени пользователя следует указать это значение, например «astratest.local\admin»
description	Нет	Описание ресурсной системы, которое используется внутри JMS. По умолчанию – «».
serverAddress	Да	Адрес сервера ресурсной системы
serverPort	Да	Порт сервера ресурсной системы. При использовании Samba AD или AD с SSL порт сервера по умолчанию – 636, без SSL – 389. Для FreeIPA – 389.
useSsl	Нет	Определяет, будет ли использоваться SSL при подключении к ресурсной системе. На данный момент актуально только

		<p>для Samba AD и AD. Подробнее см. в разделе «Настройка SSL для доступа к ресурсной системе», с. 28.</p> <p>По умолчанию – «false».</p>
container	Да	Контейнер, который будет считаться корневым для ресурсной системы.
userName	Да	<p>Имя пользователя для доступа к ресурсной системе.</p> <p>Для FreeIPA необходимо задавать полное Distinguished Name (DN) пользователя.</p> <p>Для Samba AD необходимо задавать имя с префиксом в виде netBIOSName домена. Пример: домен “fqdn5.com” и пользователь “Administrator” -> userName “FQDN5\Administrator”. При этом опция disableSambaUsernamePrefix должна быть отключена.</p> <p>Для AD, в общем случае, подойдёт и имя пользователя в чистом виде (без указания домена), и имя пользователя в формате необходимом Samba AD. Однако, при выборе необходимо учитывать значение опции disableSambaUsernamePrefix:</p> <ul style="list-style-type: none"> • “true” – “Administrator” или “FQDN2\Administrator”; • “false” – “FQDN2\Administrator”.
password	Да	Пароль пользователя.
disabledContainers	Нет	<p>Список имён контейнеров ресурсной системы разделённых запятыми, которые должны быть проигнорированы JMS. Актуально для Samba AD.</p> <p>По умолчанию – «».</p> <p>Пример – «Program Data,System,Application».</p>
mapping	Нет	<p>Определяет, будет ли использоваться маппинг идентификаторов для контейнеров в PC (true/false). Актуально только при использовании FreeIPA.</p> <p>По умолчанию – «true».</p>
attributes	Нет	<p>Наименования регистрируемых атрибутов PC, перечисленные через запятую (к примеру, «sn,ou,givenName»).</p> <p>Для регистрации всех поддерживаемых атрибутов PC следует указать «*»</p> <p>По умолчанию – «*»</p>
disabledContainers	Нет	<p>Список имён контейнеров ресурсной системы разделённых запятыми, которые должны быть проигнорированы JMS. Актуально для Samba AD и AD.</p> <p>По умолчанию – «».</p> <p>Пример – «Program Data,System,Application».</p>

Секция primaryUser

Параметры создания первичного пользователя JMS.

Имя настройки	Обязательность наличия	Описание
accountName	Да	Имя аккаунта пользователя в первичной ресурсной системе. На основе этого аккаунта в JMS будет создан первый пользователь с административными правами.

Секция licenses

Параметры поиска файлов лицензий JMS.

Имя настройки	Обязательность наличия	Описание
path	Да	Имя файла лицензии, включая полный путь к нему. Например. /opt/licenses/EAP.lic

Секция sts

Параметры поиска сертификата для подписывания JWT токенов.

Имя настройки	Обязательность наличия	Описание
certificateThumbprint	Да	Отпечаток, по которому будет производиться поиск сертификата для подписывания JWT токенов. Поиск производится в хранилище CurrentUser\My.

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

Синтаксис команды:

```
sudo [<путь_к_файлу_агента>/] Aladdin.EAP.Agent.Terminal <команда> [[<параметр>]
[<ключ>] [<аргумент>]] ... [[<параметр>] [<ключ>] [<аргумент>]]
```

Для получения справки из консоли следует ввести следующую команду:



```
sudo <путь_к_файлу_агента>/ Aladdin.EAP.Agent.Terminal --help
```


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

```
sudo Aladdin.EAP.Agent.Terminal --help
```


Полный перечень *команд*, *параметров* и *ключей* консольного агента приведен в Табл. 7.

Табл. 7 – Справочник команд консольного агента Aladdin.EAP.Agent.Terminal

Команда	Параметр	Описание
applet (настройка поддерживаемых приложений в ЭК; влияет на число типов профилей инициализации ЭК, отображаемых в Консоли управления JMS)	show	Табличное отображение включённых приложений (апплетов), для отображения соответствующих профилей в Консоли управления JMS. Пример выдачи команды на терминале:  <pre>autotest@astra:~\$ sudo Aladdin.EAP.Agent.Terminal applet show 1. [*] PKI JaCarta PKI 2. [] PKI/B10 JaCarta PKI/B10 3. [] PRO eToken PRO 32/64k 4. [] ProJava eToken Pro Java 72k, JaCarta PR 5. [] GOCT JaCarta GOCT, eToken GOCT 6. [*] GOCT 2 JaCarta-2 GOCT 7. [*] SF JaCarta SF/GOCT 8. [] STORAGE JaCarta LT 9. [] RuToken ECP Rutoken ЭЦП, Rutoken ЭЦП 2.0 10. [] RuToken Lite Rutoken Lite 11. [] RuToken S Rutoken S 12. [] ESMART ESMART Token 13. [] ESMART GOCT ESMART Token GOCT 14. [] ФКН JaCarta CryptoPro 15. [] UserStore Локальное хранилище пользовател</pre> Числовой идентификатор приложения (апплета) отображается слева. Звездочкой [*] отображается включенное приложение.
	enable	Включить приложения (апплеты) с указанными числовыми идентификаторами. Для получения идентификаторов приложений следует выполнить команду с параметром Show (выше). Идентификаторы перечисляются через пробел, например: <pre>sudo Aladdin.EAP.Agent.Terminal applet enable 3 4</pre> Для включения всех приложений в качестве идентификатора следует указать <i>all</i> , например: <pre>sudo Aladdin.EAP.Agent.Terminal applet enable all</pre>  Примечание. После включения приложений происходит автоматическая перезагрузка сервера JMS.
	disable	Отключить приложения (апплеты) с указанными числовыми идентификаторами. Синтаксис команды аналогичен синтаксису команды с параметром enable (выше).


Команда	Параметр	Описание
		 Примечание. После отключения приложений происходит автоматическая перезагрузка сервера JMS.
certificates (управление сертификатами, используемыми в подсистеме аутентификации JMS, т.е. для подписи JWT-токенов)	list	Выводит краткую информацию о сертификатах в хранилище CurrentUser\My Пример выдачи: <pre>autotest@astra:~\$ sudo Aladdin.EAP.Agent.Terminal certificates Listing certificate from 'My' certificate store (location: CurrentUser\My) Thumbprint: C7B7C9E133BF5D194CCF7F027FF301DC3F9068D2 Done.</pre>
	install	Устанавливает сертификат в хранилище CurrentUser\My. В качестве входных параметров (ключи --path и --password) передается pfx-файл контейнера сертификата с закрытым ключом и его пароль. Ключи: <ul style="list-style-type: none"> • --path (обязательный) – имя pfx-файла с его путем в файловой системе; • --password (обязательный) – пароль pfx-файла. Пример команды: <pre>sudo Aladdin.EAP.Agent.Terminal certificates install --path /mnt/hgfs/SmolenskShared/example.pfx --password 123456</pre>
	remove	Удаляет сертификат с указанным отпечатком из хранилища CurrentUser\My. Отпечаток можно получить в результате выполнения команды с параметром list . Ключи: <ul style="list-style-type: none"> • -t (обязательный) – отпечаток сертификата в шестнадцатеричном формате (см. Выдачу команды с параметром list); Пример команды: <pre>sudo Aladdin.EAP.Agent.Terminal certificates remove -t C7B7C9E133BF5D194CCF7F027FF301DC3F9068D2</pre>
jwt (управление параметрами подписи JWT-токенов)	show	Отображает текущие настройки подписи JWT-токенов. Не требует ключей. Пример выдачи: <pre>autotest@astra:~\$ sudo Aladdin.EAP.Agent.Terminal jwt show Use certificate: False Thumbprint: C7B7C9E133BF5D194CCF7F027FF301DC3F9068D2</pre>
	configure	Задаёт настройки подписи JWT-токенов. Ключи: <ul style="list-style-type: none"> • --useCertificate (опциональный) – флаг необходимости использования сертификата ключа подписи для подписывания JWT-токенов; • -t (опциональный) – отпечаток сертификата в шестнадцатеричном формате (см. Выдачу команды с параметром list);

Команда	Параметр	Описание
		<p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal jwt configure --useCertificate true -t C7B7C9E133BF5D194CCF7F027FF301DC3F9068D2</pre> <p>– включение использования подписи JWT-токенов ассиметричным ключом с указанием соответствующего сертификата</p> <pre>sudo Aladdin.EAP.Agent.Terminal jwt configure --useCertificate false</pre> <p>– включение использования подписи JWT-токенов так называемым «симметричным ключом» (symmetric signing of JWT).</p>
<p>licenses (управление лицензиями JMS)</p>	<p>list</p>	<p>Выводит информацию о текущих зарегистрированных лицензиях.</p> <p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal list</pre> <p>Фрагмент выдачи:</p> <pre>autotest@astra:~\$ sudo Aladdin.EAP.Agent.Terminal list Id: 1 Comment: Purpose: ProductId: 0x0811 ProductName: Enterprise Application Platform</pre> <p>Значение параметра «Id:» (внутренний идентификатор лицензии) может быть использовано в команде <code>remove</code> для удаления.</p>
	<p>register</p>	<p>Регистрирует лицензию в JMS.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • -p (обязательный) – имя файла лицензии (.lic) с его путем в файловой системе; <p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal licenses register -p /mnt/hgfs/SmolenskShared/Licenses/EAP.lic</pre> <p> Примечание. Перед регистрацией новой лицензии следует удалить ранее зарегистрированную (см. команду <code>licenses remove</code>)</p>
	<p>remove</p>	<p>Удаляет лицензию из JMS. В качестве аргумента принимает внутренний идентификатор лицензии (можно получить с помощью команды <code>list</code>).</p> <p>Ключи:</p> <ul style="list-style-type: none"> • -i (обязательный) – внутренний идентификатор лицензии (можно получить с помощью команды с параметром <code>list</code>). <p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal licenses remove -i 1</pre>


Команда	Параметр	Описание
	replace	<p>Заменяет существующую лицензию в JMS на новую.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • -p (обязательный) – полный путь к файлу лицензии (включая имя файла) <p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal licenses replace -p /mnt/hgfs/SmolenskShared/Licenses/EAP.lic</pre> <p> Примечание. Команда требует ввода:</p> <ul style="list-style-type: none"> • логина пользователя с ролью Оператор в формате: <имя_ресурсной_системы>\<имя_пользователя>, где <имя_ресурсной_системы> – значение, указанное в поле [accountSystem] -> name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 33) • и его пароля
	request	<p>Генерирует запрос на активацию продукта в формате PDF. В качестве аргументов принимает контактную информацию (название компании, ответственное лицо, должность, e-mail, контактный телефон), дату начала действие постоянной лицензии и имя файла запроса, который будет сгенерирован.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • -o (обязательный) – полный путь к формируемому файлу запроса (включая имя) • -c (обязательный) – название компании • -f (обязательный) – ФИО ответственного лица • -t (обязательный) – Должность ответственного лица • -e (обязательный) – адрес электронной почты ответственного лица • -p (обязательный) – телефон ответственного лица • -d (обязательный) – дата начала действия постоянной лицензии <p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal licenses request \ -o /home/autotest/JMS_Activation_request.pdf \ -c "Horns&Hooves" \ -f "Ivan Petrov" \ -t Manager \ -e test@test.com \ -p +79991234567 \ -d 03.05.2021</pre>
server (управление сервером JMS)	status	Вывод текущего статуса сервера. (Не требует ключей.)
	<ul style="list-style-type: none"> • start • stop • pause • continue 	<p>Управление статусом сервера. (Не требует ключей.)</p> <ul style="list-style-type: none"> • start – запуск сервера • stop – остановка сервера • pause – приостановление работы сервера • continue – восстановить работу сервера после установки на паузу <p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal server stop</pre>



Команда	Параметр	Описание
	<p>initialize</p>	<p>Инициализирует сервер JMS: выполняет последовательную настройку всех параметров конфигурации сервера JMS, определенную в ini-файле конфигурации (передается в параметре ключа -p). Пример ini-файла см. в разделе «Подготовительные действия», с. 12.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • -p (обязательный) – файл (.ini) конфигурации сервера JMS вместе с путём в файловой системе. <p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal server initialize -p /mnt/hgfs/SmolenskShared/conf.ini</pre>
	<p>update</p>	<p>Выполняет проверку на необходимость обновления базы данных, и если требуется обновление, предлагает его выполнить.</p> <pre>autotest@freeipa-orel:~\$ sudo Aladdin.EAP.Agent.Terminal server update Current database version: 4.0.0.30 Actual database version: 4.0.0.30 Updating database is not required.</pre> <p>Если после проверки требуется обновление базы данных, то программа сообщит об этом и даст выбор, обновлять ли сейчас базу данных или нет.</p> <pre>autotest@freeipa-orel:~\$ sudo Aladdin.EAP.Agent.Terminal server update Current database version: 4.0.0.29 Actual database version: 4.0.0.30 Updating database is required Backup database before update! Start update database? [y/n]</pre> <p>После нажатия клавиши «n» или любой другой, отличающийся от «y» обновление базы данных будет отменено.</p> <pre>autotest@freeipa-orel:~\$ sudo Aladdin.EAP.Agent.Terminal server update Current database version: 4.0.0.29 Actual database version: 4.0.0.30 Updating database is required Backup database before update! Start update database? [y/n] n Update database canceled</pre> <p>После нажатия клавиши «y» будет запущено обновление базы данных до актуальной версии.</p> <pre>Current database version: 4.0.0.29 Actual database version: 4.0.0.30 Updating database is required Backup database before update! Start update database? [y/n] y Stopping eap-engine... -Добавление поддержки расширенных идентификаторов контейнеров - Finished Update database finished success Starting eap-engine...</pre>

Команда	Параметр	Описание
smtp (настройка подключения к smtp-серверу для отправки email-уведомлений)	show	Отображает текущие настройки подключения к smtp-серверу.
	<ul style="list-style-type: none"> • enable • disable 	Включает/отключает отправку email-уведомлений. <ul style="list-style-type: none"> • enable – включение отправки уведомлений; • disable – отключение отправки уведомлений
	configure	Задаёт настройки подключения к smtp-серверу. <p>Ключи:</p> <ul style="list-style-type: none"> • -h, --host (опциональный) – адрес smtp-сервера (например -h 192.168.3.136); • -p, --port (опциональный) – порт smtp-сервера (например: -p 25); • --username (опциональный) – имя учетной записи smtp-сервера, от имени которой будет выполняться отправка email-уведомлений (для тестовых smtp-серверов, таких как smtp4dev, указывать не обязательно); • --password (опциональный) – пароль пользователя для учетной записи smtp-сервера от имени которой будет выполняться отправка email-уведомлений; • --ssl (опциональный) – флаг необходимости использования ssl при подключении к smtp-серверу. Допустимые значения: <ul style="list-style-type: none"> – true – false (Например: --ssl false) • --from (опциональный) – содержимое поля «from» для отправляемых email-уведомлений (например: --from jms@local.com); • --encoding (опциональный) – кодировка письма. . Допустимые значения: <ul style="list-style-type: none"> – utf-8; – cp-1252; (Например: --encoding cp-1251) <p>Пример команды:</p> <pre style="border: 1px dashed black; padding: 5px;">sudo Aladdin.EAP.Agent.Terminal smtp configure -h 192.168.3.136 -p 25 --ssl false --from jms@local.com</pre>
test	Совершает попытку отправить тестовое email-уведомление с текущими настройками подключения к smtp-серверу (см. параметр configure).	
syslog (настройка регистрации событий на сервере syslog)	show	Отображает текущие настройки подключения к syslog-серверу.
	<ul style="list-style-type: none"> • enable • disable 	Включает/отключает регистрацию событий на сервере syslog. <ul style="list-style-type: none"> • enable – включение регистраций; • disable – отключение регистрации
	configure	Задаёт настройки подключения к серверу syslog. <p>Ключи:</p> <ul style="list-style-type: none"> • -h, --host (опциональный) – адрес syslog-сервера (например -h 192.168.3.137); • -p, --port (опциональный) – порт, на котором syslog-сервер «слушает» (например: -p 25); • --ssl (опциональный) – флаг необходимости использования ssl при подключении к syslog-серверу. Допустимые значения: <ul style="list-style-type: none"> – true

Команда	Параметр	Описание
		<ul style="list-style-type: none"> - false (Например: --ssl false) • --protocol (опциональный) – протокол отправки. Допустимые значения <ul style="list-style-type: none"> - TCP или 0 – для использования протокола TCP (использование: --protocol 0), - UDP или 1 – для использования протокола UDP (использование: --protocol 1), • --appname (опциональный) – текстовый идентификатор приложения (используется в выходных данных Syslog для идентификации приложения). Значение по умолчанию: JMS; • --framing (опциональный) – спецификация Syslog для работы с сервером. Допустимые значения: <ul style="list-style-type: none"> - OctetCounting или 0 для OctetCounting (RFC5424), использование: --framing 0 - NonTransparentFraming или 1 для NonTransparentFraming (RFC3164), использование: --framing 1; <p> Примечание. Рекомендуется использовать RFC5424, т.к. стандарт RF3164 подразумевает, что сообщение может содержать только печатные символы из таблицы ASCII с кодами в диапазоне от 32 до 126. При выборе RFC3164 невозможна передача кириллицы</p> <p>Пример команды:</p> <pre style="border: 1px dashed black; padding: 5px;">sudo Aladdin.EAP.Agent.Terminal syslog configure -h 192.168.3.136 -p 25 --ssl false --protocol 1 --framing 0</pre>
	test	<p>Совершает попытку отправить тестовое сообщение с текущими настройками подключения к серверу syslog (см. параметр configure).</p>
<p>userproperty (работа с атрибутами пользователя в ресурсной системе)</p>	show	<p>Отображает текущую конфигурация зарегистрированных атрибутов пользователей в ресурсной системе.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • --accountsystem (обязательный) – имя ресурсной системы указанное в поле [accountSystem] -> name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 33) <p>astratest</p> <p>Примеры команды:</p> <pre style="border: 1px dashed black; padding: 5px;">Aladdin.EAP.Agent.Terminal userproperty show --accountsystem astratest.local</pre> <p>Пример выдачи:</p> <pre style="background-color: #f0f0f0; padding: 5px;">autotest@freipa-orel:~\$ sudo Aladdin.EAP.Agent.Terminal userproperty show 1. (*) businessCategory 2. (*) carLicense 3. (*) departmentNumber 4. (*) display 5. (*) employeeType 7. (*) givenName 8. (*) homePhone 9. (*) homePostalAddress 11. (*) labeledURI 12. (*) mail 13. (*) mobile 14. (*) o 16. (*) roidNumber 17. (*) uid 18. (*) x509UniqueIdentifier 19. (*) preferred 21. (*) krbCanonicalName 22. (*) krbUPEEnabled 23. (*) krbPrincipalExpiration 24. (*) krbPassw 26. (*) krbLastPwdChange 27. (*) krbPrincipaAliases 28. (*) krbLastSuccessfulAuth 29. (*) krbLastF 31. (*) krbLastAdminUnlock 32. (*) krbRl lovedToDelegato 33. (*) krbPrincipalAuthInd 34. (*) title 36. (*) registeredAddress 37. (*) destinationIndicator 38. (*) preferredDeliveryMethod 39. (*) telepho 41. (*) internationalISDNNumber 42. (*) facsimileTelephoneNumber 43. (*) street 44. (*) postalOffi 46. (*) postalAddress 47. (*) physicalDeliveryOfficeName 48. (*) ou 49. (*) st 51. (*) telephoneNumber 52. (*) description 53. (*) sn 54. (*) cn</pre> <p>Для обозначения зарегистрированных атрибутов используется символ «*». Идентификаторы атрибутов могут быть использованы в остальных командах управления атрибутами.</p>

Команда	Параметр	Описание
	register	<p>Регистрирует атрибуты пользователя в ресурсной системы с указанными идентификаторами (см. команду userproperty show) или все поддерживаемые атрибуты (при использовании вместо идентификаторов ключа «all»). Может быть указано несколько идентификаторов через пробел.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • --accountsystem (обязательный) – имя ресурсной системы указанное в поле [accountSystem] -> name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 33) • --properties (обязательный) – идентификаторы атрибутов из команды «show» <p>Примеры команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal userproperty register -- accountsystem astratest.local --properties 3 4</pre> <pre>sudo sudo Aladdin.EAP.Agent.Terminal userproperty register -- accountsystem astratest.local --properties all</pre> <p>После регистрации атрибутов происходит автоматическая перезагрузка сервера JMS.</p>
	unregister	<p>Отменяет регистрацию атрибутов с указанными идентификаторами (см. команду userproperty show). Может быть указано несколько идентификаторов через пробел.</p> <p>Пример команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal userproperty unregister 15 4</pre> <p>После отмены регистрации атрибутов происходит автоматическая перезагрузка сервера JMS.</p>
cryptodb (команда взаимодействия с СКЗИ КриптоБД)	status	<p>Отображает текущий статус подключения к КриптоБД</p> <p>Пример выдачи:</p> <pre>autotest@freeipa-ore1:~\$ Aladdin.EAP.Agent.Terminal cryptodb status Текущее состояние КриптоБД: Mounted [Сервер ключей КриптоБД запущен. Работа JMS с шифрованными данными разрешена] autotest@freeipa-ore1:~\$ █</pre>
	config	<p>Выполняет выгрузку информации о текущей инсталляции JMS для последующего импорта в Консоль конфигурирования КриптоБД с целью настройки шифрования БД.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • -p, --path – путь к xml-файлу с конфигурацией КриптоБД (обязательный параметр) • -l, --login – имя пользователя БД Postgres, используемый JMS при работе с КриптоБД (опциональный). Если не указан, то используется текущий логин JMS • -m, --mask – маска (10 Байт) для отображения зашифрованных данных (при доступе неавторизованных пользователей). В текущей версии продукта указанное в команде значение игнорируется и подставляется значение 0000000000. <p>Пример выдачи:</p> <pre>autotest@freeipa-ore1:~\$ Aladdin.EAP.Agent.Terminal cryptodb config --path /tmp/EAPDB.xml Конфигурация КриптоБД Выгружена в файл: /tmp/EAPDB.xml autotest@freeipa-ore1:~\$ █</pre>
	list	<p>Производит добавление плана обслуживания в очередь выполнения.</p>

Команда	Параметр	Описание
<p>maintenance (управление планами обслуживания)</p>		<p>Пример выдачи:</p> <pre>root@freeipa-orel:/home/autotest# Aladdin.EAP.Agent.Terminal maintenance list - План обслуживания ключевых носителей, GUID '4578a30a-e423-f2ef-b235-75e564b0b679' - План обслуживания по умолчанию, GUID '553aa527-94c4-40ef-84be-1de5b4bfb7a7' - План обслуживания рабочих станций, GUID '3288fd0d-2f4b-412a-bd8c-292a1e11fc05' - План обслуживания сертификатов, GUID 'b786028a-22aa-47ae-a024-c36f4aff19fc' - План обслуживания синхронизации атрибутов пользователя, GUID 'db552aab-c10a-4c4f-ab16-6f2bbd76fdf5'</pre>
	<p>run</p>	<p>Производит добавление плана обслуживания в очередь выполнения.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • -g, --guid (обязательный) – GUID идентификатор плана обслуживания • -p, --parameters (опциональный) – параметры для указанного плана обслуживания. Параметры могут перечисляться через пробел и указываются в формате "<i>param1=value1</i>" "<i>param2=value2</i>" ... "<i>paramN=valueN</i>" <p> Примечания:</p> <ol style="list-style-type: none"> 1. В случае если в строке отдельного параметра (для ключа -p) отсутствуют пробелы допускается его указание без кавычек, например <i>param1=value1</i> 2. При пропуске опционального ключа -p будут использованы параметры из БД JMS, т.е. их значения на момент последней настройки соответствующего плана обслуживания через консоль управления JMS. Если из консоли управления JMS изменений плана не проводилось, то будут использованы значения, установленные по умолчанию при развёртывании сервера JMS. Для гарантирования устойчивости выполнения планов обслуживания JMS рекомендуется значение ключа -p всегда указывать явно. <p>Примеры команды:</p> <pre>sudo Aladdin.EAP.Agent.Terminal maintenance run -g 78960243-7a21-62aa-a02b-73622a5f39b1 -p "AccountSystemName=fqdn2.com" "ParentObjectId="</pre> <pre>sudo Aladdin.EAP.Agent.Terminal maintenance run -g 78960243-7a21-62aa-a02b-73622a5f39b1 -p "AccountSystemName=fqdn2.com" ParentObjectId=</pre> <p>Пример выдачи:</p> <pre>root@freeipa-orel:/home/autotest# Aladdin.EAP.Agent.Terminal maintenance run -g 553aa527-94c4-40ef-84be-1de5b4bfb7a7 План обслуживания с идентификатором '553aa527-94c4-40ef-84be-1de5b4bfb7a7' добавлен в очередь на выполнение.</pre>
	<p>cancel</p>	<p>Производит отмену выполнения ранее добавленного в очередь плана обслуживания.</p> <p>Ключ:</p> <ul style="list-style-type: none"> • -g, --guid (обязательный) – GUID идентификатор плана обслуживания. <p>Пример выдачи:</p> <pre>root@freeipa-orel:/home/autotest# Aladdin.EAP.Agent.Terminal maintenance cancel -g 553aa527-94c4-40ef-84be-1de5b4bfb7a7 Отмена выполнения плана обслуживания с идентификатором '553aa527-94c4-40ef-84be-1de5b4bfb7a7' выполнена успешно.</pre>
<p>status</p>	<p>Производит получение текущего состояния плана обслуживания.</p> <p>Ключ:</p> <ul style="list-style-type: none"> • -g, --guid (обязательный) – GUID идентификатор плана обслуживания. <p>Пример выдачи:</p>	

Команда	Параметр	Описание
		<p> Примечание. В качестве файла конфигурации ресурсной системы следует использовать файл в формате файла первоначальной конфигурации, содержащий секцию [accountSystem] (образец файла приведен в разделе «Установка и первоначальная настройка сервера и консольного агента JMS», с. 12. Описание параметров секции [accountSystem] файла приведено в разделе «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», «Секция accountSystem», с. 34)</p>
	<p>update</p>	<p>Позволяет обновить информацию о зарегистрированной ресурсной системы.</p> <p>Ключи:</p> <ul style="list-style-type: none"> • -p, --path (обязательный) – путь (включая имя файла) к файлу конфигурации ресурсной системы <p> Примечание. В качестве файла конфигурации ресурсной системы следует использовать файл в формате файла первоначальной конфигурации, содержащий секцию [accountSystem]</p> <ul style="list-style-type: none"> • --accountsystem (обязательный) – имя ресурсной системы указанное в поле [accountSystem] -> name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», «Секция accountSystem», с. 34)

Приложение 3. Инструкция по сборке расширения rjjava для СУБД PostgreSQL 9.6 под ОС Astra Linux Орел или Смоленск

Для сборки расширения rjjava для для СУБД PostgreSQL 9.6 необходимо выполнить следующие шаги.

1. Убедиться в установке компонентов СУБД PostgreSQL 9.6 и их настройки

- postgresql-9.6 (9.6.20-astrace1)
- postgresql-contrib-9.6 (9.6.20-astrace1)

Установить утилиту pgadmin3

2. Установить дополнительные пакеты

- libssl1.0-dev (1.0.2u-1~deb9u1)
- postgresql-common (200astra)
- postgresql-server-dev-9.6 (9.6.20-astrace1)
- postgresql-server-dev-all (200astra)
- krb5-multidev (1.15.2-2.astra5)
- libkrb5-dev (1.15.2-2.astra5)
- g++ (4:6.3.0-4)
- g++-6 (6.3.0-18+deb9u1)
- gcc (4:6.3.0-4)
- gcc-6 (6.3.0-18+deb9u1)
- maven (3.3.9-4)

3. Установить java

- openjdk-8-jdk (8u232-b09-1~deb9u1)
- openjdk-8-jdk-headless (8u232-b09-1~deb9u1)
- openjdk-8-jre (8u232-b09-1~deb9u1)

Проверить работу всех инструментов

```
g++ --version
gcc --version
```

Выдача:

```
gcc (Debian 6.3.0-18+deb9u1) 6.3.0 20170516
```

```
Copyright (C) 2016 Free Software Foundation, Inc.
```

```
java -version
```

Выдача:

```
openjdk version "1.8.0_232"
```

```
OpenJDK Runtime Environment (build 1.8.0_232-8u232-b09-1~deb9u1-b09)
```

```
OpenJDK 64-Bit Server VM (build 25.232-b09, mixed mode)
```

```
mvn --version
```


Выдача:

Apache Maven 3.3.9

Maven home: /usr/share/maven

Java version: 1.8.0_232, vendor: AstraLinuxCE

Java home: /usr/lib/jvm/java-8-openjdk-amd64/jre

Default locale: ru_RU, platform encoding: UTF-8

OS name: "linux", version: "4.15.3-3-generic", arch: "amd64", family: "unix"

pg_config

4. Скачать и распаковать https://github.com/tada/pljava/releases/tag/V1_5_2 (Также поддерживается сборка pljava 1.5.7)
5. Зайти в распакованную папку pljava-1_5_2 в нем должен быть pom.xml
6. ТОЛЬКО ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ Astra Linux Смоленск!

В следующем заголовочном файле

```
sudo nano /usr/include/postgresql/9.6/server/utils/errcodes.h
```

Добавить строчку – выделено цветом (если ее еще не было):

```
#define ERRCODE_INSUFFICIENT_PRIVILEGE_RBT MAKE_SQLSTATE('4','2','5','0','1')  
#define ERRCODE_INSUFFICIENT_PRIVILEGE MAKE_SQLSTATE('4','2','5','0','1')
```

7. Выполнить

```
mvn -X -Pwnosign clean install
```

Ошибки компиляции про несуществующие значения enum можно игнорировать. Общий статус всех шагов сборки должно быть «УСПЕШНО»

8. Зайти в директорию Рабочий стол/pljava/pljava-1_5_2/pljava-packaging/target
9. Выполнить

```
sudo java -jar ./pljava-pg9.6-amd64-Linux-gpp.jar
```

Должно выполняться копирование бинарников pljava в директорию postgres

10. Зайти через pgAdmin в СУБД PostgreSQL, выполнить запросы (убедиться, что пути к so и jar правильные)

```
SET pljava.libjvm_location TO '/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/amd64/server/libjvm.so';  
  
ALTER SYSTEM  
SET pljava.libjvm_location TO '/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/amd64/server/libjvm.so';
```

```
SET pljava.classpath TO '/usr/share/postgresql/9.6/pljava/pljava-1.5.2.jar';  
  
CREATE EXTENSION pljava;  
  
GRANT USAGE ON LANGUAGE JAVA TO public;  
GRANT USAGE ON SCHEMA sqlj TO public;  
GRANT USAGE ON SCHEMA public TO postgres;
```

Не должно быть ошибок загрузки JAVA

11. В pgAdmin -> Logins -> делаем администратора «Крипто БД» суперпользователем postgres (временно, после шифрования таблиц - можно убрать)
12. Далее можно приступать к созданию объектов «Крипто БД» и интеграции ее к JMS.

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 RU.АЛДЕ.03.16.001-05 34 01. Руководство пользователя [Текст]. – «Аладдин Р.Д.»

- 2 RU.АЛДЕ.03.16.001-05 32 01-2. Руководство администратора. Часть 2. Функции управления [Текст]. – «Аладдин Р.Д.»

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

- 4 Единый Клиент JaCarta. Руководство администратора для операционных систем семейства Linux [Текст]. – «Аладдин Р.Д.»

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа.

Коротко о компании

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

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

Основные направления

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

Лицензии

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



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

© АО «Аладдин Р. Д.», 1995–2022. Все права защищены
Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web:
www.aladdin.ru