



WorksPad™

Руководство по установке и конфигурированию

Версия для Windows

Версия 5.2.2 – Сентябрь 2022

РуПост (RuPost, LLC.)

© 2022 РуПост (RuPost, LLC.). Все права защищены.

РуПост, RuPost, WorksPad, логотип WorksPad являются торговыми марками или зарегистрированными торговыми марками РуПост (RuPost, LLC.) в США, России и других странах.

Названия прочих компаний и продуктов, упомянутые здесь, могут являться товарными знаками соответствующих компаний.

Продукты сторонних фирм упоминаются исключительно в информационных целях и конфигурирования зависимостей WorksPad. Компания РуПост не несет ответственности за эксплуатационные качества и использование этих продуктов. Все договоренности, соглашения или гарантийные обязательства, при наличии таковых, заключаются непосредственно между поставщиком и потенциальными пользователями. При составлении данного руководства были предприняты все усилия для обеспечения достоверности и точности информации. Данное руководство является предметом изменений в соответствии с динамикой развития продукта и может не содержать наиболее последних версий копий экранов, имен параметров и других характеристик продукта. РуПост не несет ответственности за опечатки или описки.

Официальный веб-сайт: <http://www.workspad.ru>.

Содержание

1. Введение	5
2. Компоненты WorksPad и их назначение	6
3. Управление лицензиями	7
4. Системные требования	8
5. Варианты топологии системы	9
5.1. Односерверная топология.....	9
5.2. Многосерверная топология.....	10
6. Подготовка инфраструктуры	11
6.1. Добавление роли Веб-сервер (IIS)	11
6.2. Установка Microsoft ASP.NET Core	11
6.3. Установка Microsoft SQL Server.....	12
6.4. Настройка интеграции с Microsoft Exchange	12
6.4.1. Настройка политики регулирования Microsoft Exchange.....	12
6.4.1.1. Настройка политики регулирования для Microsoft Exchange 2010.....	12
6.4.1.2. Настройка политики регулирования для Microsoft Exchange 2013 и выше	13
6.4.2. Настройка Autodiscover	13
6.4.3. Создание системной учётной записи для почтовых push-уведомлений	13
6.5. Настройка интеграции с CommuniGate Pro	14
6.5.1. Установка скриптов и настройка правил для входящей почты.....	14
6.5.2. Создание системной учётной записи для почтовых push-уведомлений	15
6.6. Настройка интеграции с Microsoft SharePoint.....	16
6.7. Настройка интеграции с InfoWatch Traffic Monitor.....	16
6.8. Рекомендованная конфигурация портов	17
7. Действия перед началом установки	19
7.1. Создание системной учётной записи для служб WorksPad.....	19
7.2. Создание базы данных в Microsoft SQL Server.....	19
7.3. Создание корневой папки для клиентских журналов событий	19
7.4. Создание корневой папки для FileBox.....	19
7.5. Создание корневой папки для опубликованных файлов	20
8. Установка системы	21
8.1. Параметры установленной системы.....	27
8.2. Первоначальная настройка системы	28

9. Создание кластера WorksPad	29
10. Конфигурирование системы.....	30
10.1. Конфигурирование Gateway Service	30
10.1.1. Настройка локального администратора.....	30
10.1.2. Настройка Browser Proxy.....	30
10.1.3. Настройка прокси-сервера для Telegram	31
10.1.4. Настройка прокси-сервера для Microsoft Bot Framework.....	31
10.2. Конфигурирование Archiver Service	32
11. Поддержка	33

1. Введение

WorksPad представляет собой клиент-серверную систему удалённого доступа с мобильных устройств к ресурсам корпоративной сети организации.

Клиентское приложение WorksPad позволяет получить доступ с мобильных устройств по сети Интернет к почтовым службам, файловым хранилищам, веб-ресурсам, размещенным внутри корпоративной сети, без необходимости публикации таких ресурсов в Интернет.

Серверная часть системы реализована в виде набора компонентов, работающих под управлением операционных систем семейства Microsoft Windows Server.

Пользователями системы WorksPad могут быть только пользователи домена LDAP.

Данный документ описывает требования, настройки и действия, необходимые для развёртывания серверной части системы WorksPad в корпоративной сети организации.

2. Компоненты WorksPad и их назначение

WorksPad состоит из следующих компонентов – сервисов:

- **Gateway Service** – сервис, принимающий информацию от клиентских приложений и веб-приложений WorksPad. Работает по протоколам HTTPS, WSS и TCP. Основными задачами данного сервиса являются:
 - Первичная аутентификация пользователя;
 - Регистрация пользовательских устройств;
 - Выполнение операций над файлами и папками (общие папки SMB, библиотеки документов SharePoint, папки WebDAV);
 - Выполнение операций над сообщениями электронной почты, контактами, календарными событиями и другой почтовой функциональностью;
 - Обеспечение взаимодействия пользователей с чат-ботами;
 - Обработка запросов от веб-браузеров клиентских приложений WorksPad;
 - Журналирование запросов пользователей.
- **Share Service** – сервис, который предназначен для выполнения операций над внешними ссылками. Получает запросы от Gateway и Сайта внешнего доступа по протоколу HTTPS. Также сервис отправляет запросы на Gateway.
- **Notification Service** – сервис, который предназначен для отправки push-уведомлений клиентским приложениям WorksPad, а также для отправки служебных уведомлений администраторам системы WorksPad. Работает по протоколу HTTPS.
- **Archiver Service** – сервис, который занимается архивированием журнала событий сервера WorksPad. По умолчанию архивирование запускается каждый день в 2:00 и имеет ограничение продолжительности выполнения равное 3 часам.

Компонент **Admin API** представляет собой веб-приложение, которое позволяет управлять системой WorksPad посредством использования веб-API. Доступ к функциональности Admin API имеют пользователи с системной ролью «Администратор» или с какой-либо пользовательской ролью администрирования в системе WorksPad.

Компонент **Chatbot API** представляет собой веб-приложение, которое позволяет чат-ботам взаимодействовать с пользователями WorksPad и сторонних мессенджеров (Telegram, Microsoft Teams) посредством использования веб-API.

Кроме вышеуказанных компонентов, в состав WorksPad входят веб-приложения Консоль администратора (**Administration Console**), Пользовательский портал (**User Portal**) и Сайт внешнего доступа (**External Access Site**). Доступ к веб-приложениям Консоль администратора и Пользовательский портал регулируется ролями WorksPad: к Консоли администратора имеют доступ только пользователи с системной ролью «Администратор» или с какой-либо пользовательской ролью администрирования в системе WorksPad. Соответственно к пользовательскому portalу имеют доступ только пользователи с системной ролью «Пользователь». Пользователи WorksPad могут владеть несколькими ролями одновременно.

3. Управление лицензиями

Управление лицензиями WorksPad осуществляется при помощи лицензионных файлов с расширением **.lic**.

Просмотреть параметры текущей лицензии, а также загрузить новую лицензию можно при помощи Консоли администратора в разделе «Информация». Подробнее см. Руководство администратора.

4. Системные требования

Компоненты сервера WorksPad функционируют под управлением ОС **Microsoft Windows Server 2012 или более поздней версии**. На всех серверах должен быть развернут **Microsoft ASP.NET Core 5.0**.

Для хранения служебной информации WorksPad использует **Microsoft SQL Server 2008 R2 или более поздней версии**.

Для работы с общими папками SMB, WorksPad использует протокол **SMB версий 2.0.2, 2.1.0 и 3.0.0**.

Для работы с библиотеками документов SharePoint (SharePoint Document Libraries), WorksPad требует наличия **Microsoft SharePoint Server 2010 или более поздней версии**.

Для работы почтовой функциональности, WorksPad поддерживает следующие типы почтовых серверов:

- **RuPost**
- **Zimbra 8.8 или более поздней версии;**
- **Microsoft Exchange Server 2010 SP1 или более поздней версии;**
- **CommuniGate Pro 6.0 или более поздней версии.**

Система WorksPad поддерживает интеграцию с DLP-системой **InfoWatch Traffic Monitor 6.5 или более поздней версии**.

Аутентификация пользователей WorksPad осуществляется при помощи **LDAP** (Microsoft Active Directory, ALD Pro, FreeIPA, OpenLDAP).

Требования к объему оперативной памяти и дисковому пространству зависят от варианта развертывания и ожидаемого числа пользователей. Подробнее о вариантах конфигурации см. раздел [Варианты топологии системы](#).

Ниже приведены минимальные системные требования при развёртывании всех компонентов WorksPad на одном сервере и для обслуживания до 200 пользователей:

Процессор: 4-ядерный,

Оперативная память: 8 ГБ,

Дисковое пространство: 1 ГБ (без учета объема пользовательских и опубликованных файлов).

5. Варианты топологии системы

5.1. Односерверная топология

С точки зрения безопасности рекомендуется разворачивать систему во внутренней сети организации.

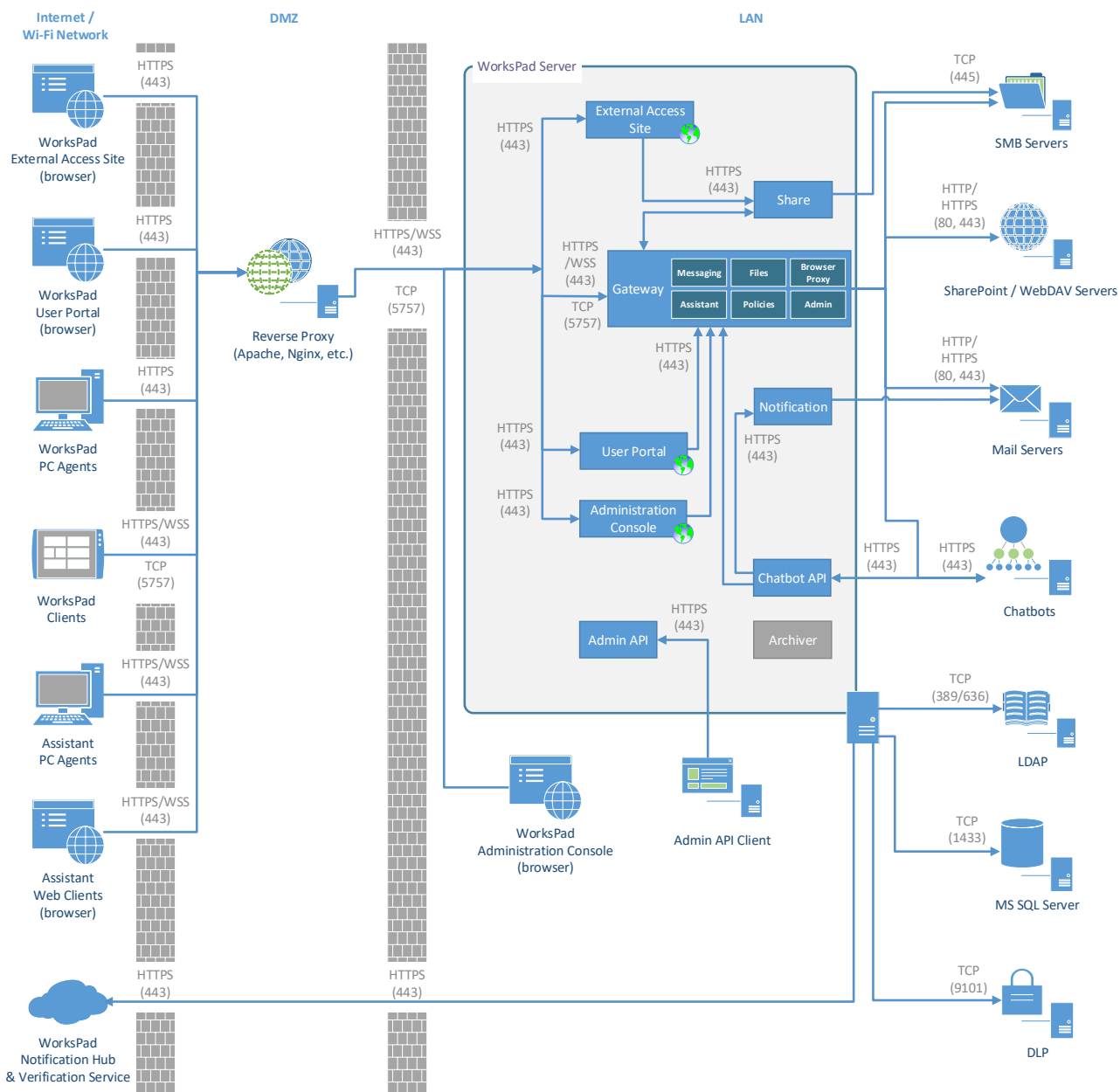


Диаграмма 1. Пример односерверной конфигурации WorksPad.

Для доступа к системе из Интернета можно воспользоваться существующим прокси-сервером в DMZ или VPN-подключением, если таковые имеются.

Доступ к Консоли администратора, Admin API и Chatbot API рекомендуется предоставлять только из внутренней сети организации.

5.2. Многосерверная топология

Для обслуживания большого количества пользователей рекомендуется использовать кластер серверов WorksPad. Использование кластера позволяет легко масштабировать систему, балансировать нагрузку, а также повышает её отказоустойчивость.

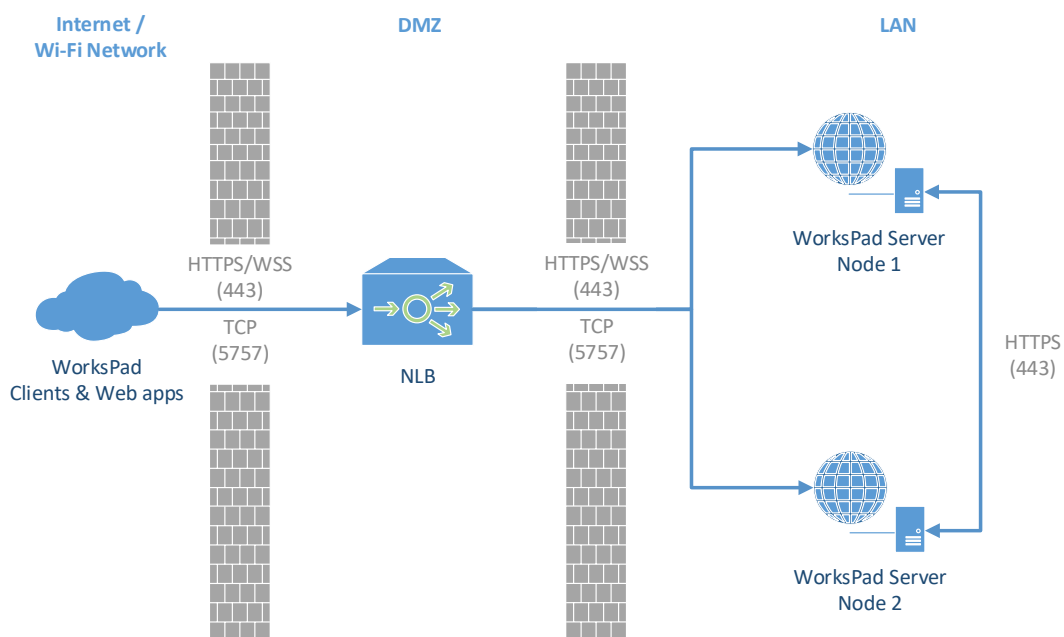


Диаграмма 2. Пример кластера WorksPad из двух узлов.

В качестве входной точки для клиентских приложений WorksPad необходимо использовать адрес аппаратного или программного балансировщика нагрузки (NLB), который будет распределять запросы между узлами кластера.

Все узлы кластера WorksPad должны использовать единую базу данных. Рекомендуется использовать кластер Microsoft SQL Server.

Убедитесь, что со всех узлов кластера доступны ресурсы организации (файловые хранилища, почтовые сервера и т.д.), интегрированные с сервером WorksPad.

6. Подготовка инфраструктуры

Подготовка инфраструктуры включает в себя следующие шаги:

- Установка серверов (аппаратных или виртуальных) с ОС Microsoft Windows Server 2012 или более поздних версий.
- Развертывание роли Internet Information Server (IIS)
- Установка Microsoft ASP.NET Core 5.0 на всех серверах, где планируется использовать компоненты WorksPad.
- Развертывание и настройка Microsoft SQL Server 2008 R2 или более поздней версии.
- Настройка интеграции с Microsoft Exchange, если требуется.
- Настройка интеграции с CommuniGate Pro, если требуется.
- Настройка интеграции с Microsoft SharePoint, если требуется.
- Настройка интеграции с InfoWatch Traffic Monitor, если требуется.
- Настройка сетевых портов для всех серверов, в тех случаях, когда этого требует текущая инфраструктура. Подробнее см. раздел [Рекомендованная конфигурация портов](#).

6.1. Добавление роли Веб-сервер (IIS)

Для работы сервера WorksPad требуется развертывание роли Веб-сервер (IIS). Добавьте эту роль на каждом сервере, где будут развернуты компоненты системы. Необходимо установить следующие службы роли:

- Веб-сервер
 - Основные возможности HTTP
 - Ошибки HTTP
 - Перенаправление HTTP
 - Стандартный документ
 - Статическое содержимое
 - Разработка приложений
 - ASP.NET («ASP.NET 4.5» в Windows Server 2012 и выше)
 - Протокол WebSocket
 - Расширения ISAPI
 - Расширяемость .NET («Расширяемость .NET 4.5» в Windows Server 2012 и выше)
 - Фильтры ISAPI
 - Безопасность
 - Фильтрация запросов
 - Производительность
 - Сжатие статического содержимого
- Средства управления
 - Консоль управления IIS

6.2. Установка Microsoft ASP.NET Core

Все компоненты WorksPad работают в среде выполнения ASP.NET Core версии 5.0.

Загрузите и установите пакет размещения (Hosting Bundle) для ASP.NET Core. Ссылка на официальный дистрибутив:

<https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-aspnetcore-5.0.9-windows-hosting-bundle-installer>

Внимание! Если пакет размещения устанавливается до установки служб IIS, то его нужно восстановить. После установки служб IIS запустите установщик пакета размещения еще раз.

6.3. Установка Microsoft SQL Server

Для работы WorksPad требуется SQL Server 2008 R2 или более поздней версии. Поддерживается любая редакция, включая SQL Server Express. Однако, следует учитывать, что Express-версия накладывает ограничения на объем используемой оперативной памяти (максимум 1 ГБ) и максимальный объем базы данных (не более 10 ГБ).

WorksPad требует только механизм базы данных, однако рекомендуется разворачивать и консоль управления сервером баз данных.

SQL сервер допустимо размещать локально, на том же сервере, где расположены компоненты сервера WorksPad. Более сложные варианты топологии, например, множественная установка компонентов с использованием балансировки нагрузки, может потребовать выделения отдельного сервера (отказоустойчивого кластера) для размещения базы данных.

6.4. Настройка интеграции с Microsoft Exchange

Данный этап необходим, если для обеспечения почтовой функциональности системы WorksPad планируется использовать почтовый сервер Microsoft Exchange или почтовые службы Office 365. В противном случае можете пропустить этот шаг.

6.4.1. Настройка политики регулирования Microsoft Exchange

Внимание! Администратор не может устанавливать политики регулирования для Office 365.

Для работы WorksPad с сервером Exchange рекомендуется снять ограничения, накладываемые политикой регулирования клиентов Microsoft Exchange по умолчанию. В противном случае, в связи с довольно низкими порогами политик установленных по умолчанию для Exchange Web Services, возможны временные отказы в обслуживании запросов (или более медленное их обслуживание) со стороны Exchange Server. Вероятность срабатывания политик высока для ящиков больших размеров, особенно при первоначальной синхронизации.

Ниже представлено описание шагов, которые необходимо выполнить администратору для снятия ограничений в зависимости от версии Exchange.

6.4.1.1. Настройка политики регулирования для Microsoft Exchange 2010

Для настройки политики регулирования клиентов на Microsoft Exchange 2010 необходимо выполнить следующие шаги:

1. Войти на Exchange Server от имени учётной записи администратора и запустить Exchange Management Shell

2. Для создания новой политики регулирования, необходимо выполнить следующую команду:
`New-ThrottlingPolicy WorksPadPolicy -EWSMaxConcurrency $null -EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null -EWSMaxSubscriptions $null -EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null`
3. Выполните следующую команду для применения новой политики ко всем владельцам почтовых ящиков, к которым обращаются пользователи WorksPad:
`Set-Mailbox "<user login>" -ThrottlingPolicy WorksPadPolicy`
4. Для применения новой политики к [системной учётной записи для push-уведомлений](#) выполните следующую команду:
`Set-ThrottlingPolicyAssociation -Identity "<user login>" -ThrottlingPolicy WorksPadPolicy`

6.4.1.2. Настройка политики регулирования для Microsoft Exchange 2013 и выше

Для настройки политики регулирования клиентов на Microsoft Exchange 2013 и выше необходимо выполнить следующие шаги:

1. Войдите на сервер где установлен Microsoft Exchange Server от имени учётной записи администратора и запустить Exchange Management Shell
2. Для создания новой политики регулирования, необходимо выполнить следующую команду:
`New-ThrottlingPolicy WorksPadPolicy -RCAMaxConcurrency Unlimited -EWSMaxConcurrency Unlimited -EWSMaxSubscriptions Unlimited -SPAMaxConcurrency Unlimited -EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited`
3. Выполните следующую команду для применения новой политики ко всем владельцам почтовых ящиков, к которым обращаются пользователи WorksPad:
`Set-Mailbox "<user login>" -ThrottlingPolicy WorksPadPolicy`
4. Для применения новой политики к [системной учётной записи для push-уведомлений](#) выполните следующую команду:
`Set-ThrottlingPolicyAssociation -Identity "<user login>" -ThrottlingPolicy WorksPadPolicy`

6.4.2. Настройка Autodiscover

Данный этап необходим, если планируется использовать push-уведомления о почтовых событиях в клиентских приложениях WorksPad. В противном случае можете пропустить этот шаг.

Автообнаружение (Autodiscover) используется для определения связей между CAS (Client Access Server) и адресами электронной почты. Это является необходимым требованием для корректной работы почтовых уведомлений.

Необходимо чтобы служба автообнаружения Exchange была доступна с сервера, где развёрнута служба WorksPad Notification Service.

6.4.3. Создание системной учётной записи для почтовых push-уведомлений

Данный этап необходим, если планируется использовать push-уведомления о почтовых событиях в клиентских приложениях WorksPad. В противном случае можете пропустить этот шаг.

Для получения и обработки почтовых уведомлений от сервера Exchange необходимо иметь системную учётную запись с правами на олицетворение (роль ApplicationImpersonation) в Microsoft Exchange. Данная учётная запись позволяет создавать от имени пользователя подписки на получение почтовых уведомлений от Exchange, а также получать необходимую для отправки push-уведомлений информацию.

Создайте системную учётную запись, например, «WPNotification». Учётной записи рекомендуется задать надёжный пароль. **Срок действия пароля должен быть не ограничен. Имя и пароль** этой учетной записи должны оставаться **неизменными**.

Далее представлено описание шагов, которые необходимо выполнить администратору Microsoft Exchange для предоставления необходимых прав системной учётной записи:

1. Войдите на сервер Microsoft Exchange Server от имени учётной записи администратора и запустите Exchange Management Shell
2. Для предоставления системной учётной записи прав на олицетворение выполните следующую команду:

```
New-ManagementRoleAssignment -Name "WorksPad Notification Admin" -  
Role:ApplicationImpersonation -User "<user login>"
```

Внимание! Для данной системной учётной записи крайне рекомендуется снять ограничения, накладываемые политикой регулирования клиентов Microsoft Exchange по умолчанию (не применимо к Office 365). Подробнее см. раздел [«Настройка политики регулирования Microsoft Exchange»](#).

6.5. Настройка интеграции с CommuniGate Pro

Данный этап необходим, если для обеспечения почтовой функциональности системы WorksPad планируется использовать почтовый сервер CommuniGate Pro. В противном случае можете пропустить этот шаг.

6.5.1. Установка скриптов и настройка правил для входящей почты

Данный этап необходим, если планируется использовать push-уведомления о почтовых событиях в клиентских приложениях WorksPad. В противном случае можете пропустить этот шаг.

Для получения и обработки почтовых уведомлений от сервера CommuniGate Pro необходимо установить специальные скрипты из пакета WorksPad CGP Push Sender¹, а также настроить правила для входящей почты.

Примечание. Правила для входящей почты должны быть настроены для всех доменов, пользователи которых добавлены в систему WorksPad.

Перед установкой скрипта «workspad-pushhandler.sppr» из пакета WorksPad CGP Push Sender необходимо его подготовить. Для этого выполните указанные ниже действия:

1. Откройте на редактирование файл «workspad-pushhandler.sppr».

¹ Для получения пакета свяжитесь с вашим поставщиком решения WorksPad.

- Укажите в файле URL-адрес службы WorksPad Notification Service, отредактировав указанный в нём шаблон «https://<WorksPadServer>/Notification/SendCgpPush» (например, «https://192.168.10.10/Notification/SendCgpPush»).
- Сохраните файл.

Далее представлено описание шагов, которые необходимо выполнить администратору CommuniGate Pro для установки скриптов и настройки правил для входящей почты:

- Войдите в интерфейс Администратора CommuniGate Pro от имени учётной записи администратора.
- Перейдите в раздел «Пользователи» – «Интерфейсы».
- На открывшейся странице загрузите файл «workspad-pushsender.wcgp».
- Перейдите в раздел «Пользователи» – «PBX».
- На открывшейся странице загрузите файл «workspad-pushhandler.sppr».
- Перейдите в раздел «Пользователи» – «Домены».
- В представленной таблице нажмите на имя домена, в котором необходимо настроить правила входящей почты.
- Перейдите в раздел «Почта» выбранного домена.
- На открывшейся странице создайте следующее правило:

Приоритет	Имя	
7	PushMail	
Данные	Операция	Параметр
-	-	-
Действие	Параметр	
Обратиться по URL	http://127.0.0.1:8100/sys/workspad-pushsender.wcgp?type=mailIn&sub=^s&fromFull=^F&from=^E&to=^R&rcpt=^r&messageld=^I	

6.5.2. Создание системной учётной записи для почтовых push-уведомлений

Данный этап необходим, если планируется использовать push-уведомления о почтовых событиях в клиентских приложениях WorksPad. В противном случае можете пропустить этот шаг.

Для получения и обработки почтовых уведомлений от сервера CommuniGate Pro необходимо иметь системную учётную запись с правом доступа «**Полный доступ ко всем Папкам**». Данная учётная запись позволяет получать необходимую для отправки push-уведомлений информацию.

Примечание. Система WorksPad не использует системную учётную запись для изменения настроек сервера CommuniGate Pro и данных её пользователей. Предоставленные права доступа используются только для получения информации о новых входящих сообщениях, которая необходима для работы push-уведомлений.

Создайте системную учётную запись, например, «WPNotification». Учётной записи рекомендуется задать надёжный пароль. **Срок действия пароля должен быть не ограничен. Имя и пароль** этой учётной записи должны оставаться **неизменными**.

Далее представлено описание шагов, которые необходимо выполнить администратору CommuniGate Pro для предоставления необходимых прав системной учётной записи:

1. Войдите в интерфейс Администратора CommuniGate Pro от имени учётной записи администратора.
2. Перейдите в раздел «Пользователи» – «Домены» и в представленной там таблице нажмите на имя домена, в котором была создана системная учётная запись для работы функциональности push-уведомлений.
3. В открывшемся разделе «Объекты» нажмите на имя системной учётной записи пользователя.
4. Нажмите на ссылку «Права Доступа», которая расположена в правом верхнем углу открывшейся страницы.
5. Выберите для пользователя следующие группу прав доступа – **«Может менять установки Всех Доменов и Пользователей»**.
6. В разделе **«Объекты»** укажите право доступа – **«Полный доступ ко всем Папкам»**.
7. Нажмите кнопку «Модифицировать».

6.6. Настройка интеграции с Microsoft SharePoint

Данный этап необходим, если с помощью системы WorksPad планируется обеспечить доступ к библиотекам документов Microsoft SharePoint или SharePoint Online. В противном случае можете пропустить этот шаг.

Для доступа к документам, размещенным на порталах Microsoft SharePoint пользователи должны обладать соответствующими правами. Следующие разрешения должны быть предоставлены пользователям на каждом портале SharePoint в зависимости от желаемого режима доступа:

Режим	Описание режима	Разрешения SharePoint
«Чтение»	Чтение и скачивание документов на мобильное устройство	View Items, Browse Directories, View Pages, Use Remote Interfaces, Open
«Совместная работа»	«Чтение» + Загрузка документов: добавление с возможностью замены без удаления	+ Add Items, Edit Items
«Редактирование»	«Совместная работа» + Удаление	+ Delete Items

6.7. Настройка интеграции с InfoWatch Traffic Monitor

Данный этап необходим, если планируется интеграция системы WorksPad с DLP-системой InfoWatch Traffic Monitor (IWTM). В противном случае можете пропустить этот шаг.

В рамках интеграции с DLP-системой, сервер WorksPad отправляет теньевые копии файлов, скачиваемых на мобильные устройства, на сервер IWTM. Для настройки взаимодействия сервера WorksPad с DLP-системой IWTM необходимо установить плагин WorksPad TM Adapter² в систему IWTM. Подробнее об интеграции WorksPad с DLP-системой смотрите в «Руководстве по интеграции с InfoWatch Traffic Monitor».

² Для получения плагина свяжитесь с вашим поставщиком решения WorksPad.

6.8. Рекомендованная конфигурация портов

Для работы компонентов WorksPad необходимо открыть ряд сетевых портов из внешних сетей к серверу WorksPad, от сервера WorksPad к внутренним ресурсам и системам (серверу БД, контроллерам домена, почтовым серверам и пр.). Также для работы некоторых компонентов системы может потребоваться открытие сетевых портов от серверов WorksPad в Интернет. В таблице ниже представлен перечень необходимых портов с указанием компонентов WorksPad и внешних систем.

Порт	Протокол	Источник	Точка обращения
443	HTTPS, WSS	Интернет, интранет	Reverse Proxy
5757	TCP	Интернет, интранет	Reverse Proxy
443	HTTPS	Reverse Proxy	Administration Console
443	HTTPS	Reverse Proxy	User Portal
443	HTTPS	Reverse Proxy	External Access Site
443	HTTPS, WSS	Reverse Proxy	Gateway Service
5757	TCP	Reverse Proxy	Gateway Service
443	HTTPS	Reverse Proxy	Admin API
443	HTTPS	Administration Console	Gateway Service
443	HTTPS	User Portal	Gateway Service
443	HTTPS	External Access Site	Share Service
443	HTTPS	Gateway Service	Share Service
443	HTTPS	Share Service	Gateway Service
80, 443	HTTP, HTTPS	Gateway Service	Серверы Microsoft SharePoint
80, 443	WebDAV	Gateway Service	Серверы WebDAV
445	SMB	Gateway Service	Файловые серверы (SMB)
993	IMAP	Gateway Service	Почтовые серверы RuPost
465	SMTP	Gateway Service	Почтовые серверы RuPost
443	CalDAV, CardDAV	Gateway Service	Почтовые серверы RuPost
143	IMAP	Gateway Service	Почтовые серверы Zimbra
587	SMTP	Gateway Service	Почтовые серверы Zimbra
443	CalDAV, CardDAV	Gateway Service	Почтовые серверы Zimbra
80, 443	HTTP, HTTPS	Gateway Service, Notification Service	Почтовые серверы Microsoft Exchange

8100, 9100	HTTP, HTTPS	Gateway Service, Notification Service	Почтовые серверы CommuniGate Pro
443	HTTP, HTTPS	Почтовый сервер CommuniGate Pro	Notification Service
9101	TCP	Gateway Service	DLP-система InfoWatch Traffic Monitor
443	HTTPS	Gateway Service, Chatbot API	Чат-боты
443	HTTPS	Chatbot API	Gateway Service
443	HTTPS	Chatbot API	Notification Service
443	HTTPS	Чат-боты	Chatbot API
1433	TCP	Gateway Service, Notification Service, Share Service, Archiver Service, Admin API, Chatbot API	Microsoft SQL Server
389, 636	TCP	Gateway Service, Admin API	Контроллер домена (LDAP)
80, 443*	TCP	Gateway Service	Интернет, интранет
443**	HTTPS	Gateway Service, Admin API	Интернет (WorksPad Verification Service)
443***	HTTPS	Notification Service	Интернет (WorksPad Notification Hub)

* Порты и IP-адреса устанавливаются в зависимости от расположения веб-ресурсов, к которым необходимо предоставить доступ через встроенный веб-браузер WorksPad.

** Необходимо для активации лицензий. Сервер WorksPad Verification Service: ivs.workspad.com.

*** Необходимо для работы push-уведомлений. Серверы назначения зависят от выбранного региона расположения сервиса уведомлений WorksPad Notification Hub (настраивается в Консоли администратора). Серверы WorksPad Notification Hub в регионе «Европа»: push-eu-01p.workspad.com, push-eu-02p.workspad.com.

Следует обратить внимание, что в таблице описаны порты, требующиеся для работы непосредственно компонентов WorksPad, однако, для взаимодействия серверов, являющихся членами домена LDAP, может потребоваться настройка и других сетевых портов/протоколов. Например, `tcp/135`, `tcp/137`, `tcp/3268`, `tcp/3269`, `tcp/42`, `tcp/445`, `tcp/464`, `tcp/49152-65535`, `tcp/88`, `tcp/ldap`, `tcp/ldaps`, `tcp/netbios-ssn`, `udp/389`, `udp/445`, `udp/464`, `udp/88`, `udp/domain`, `udp/nameserver`, `udp/netbios-dgm`, `udp/netbios-ns`, `udp/ntp`.

Подробное рассмотрение сетевого взаимодействия между серверами в инфраструктуре домена LDAP выходит за рамки данного руководства.

7. Действия перед началом установки

Перед установкой системы WorksPad необходимо предварительно выполнить следующие действия:

- Создать в LDAP системную учётную запись для служб WorksPad.
- Создать базу данных в Microsoft SQL Server.
- Создать корневую папку для клиентских журналов событий, если планируется использовать хранилище клиентских журналов событий.
- Создать корневую папку для FileBox, если планируется использовать WorksPad FileBox.
- Создать корневую папку для опубликованных файлов, если планируется использовать функциональность внешних ссылок.

7.1. Создание системной учётной записи для служб WorksPad

Для первой установки системы WorksPad необходимо создать в LDAP учётную запись, от имени которой будут работать службы WorksPad, например, «WPService». Учётной записи рекомендуется задать надёжный пароль. Срок действия пароля должен быть не ограничен. Имя и пароль этой учетной записи должны оставаться неизменными. Учётная запись должна иметь права локального администратора и права на вход в качестве службы на каждом сервере, где будут развёрнуты компоненты системы. Данная учётная запись должна иметь права владельца (db_owner) на базу данных WorksPad.

7.2. Создание базы данных в Microsoft SQL Server

Необходимо предварительно создать пустую базу данных в Microsoft SQL Server. Во время первой установки туда будут добавлены все необходимые компоненты базы данных для системы WorksPad. Рекомендуемое название базы данных – «WorksPad». Поскольку компоненты WorksPad, которые взаимодействуют с базой данных, работают от имени [учётной записи для служб WorksPad](#), то убедитесь, что данный пользователь имеет права владельца на базу данных WorksPad.

7.3. Создание корневой папки для клиентских журналов событий

Данные действия необходимо выполнить, только если планируется использование хранилища клиентских журналов событий WorksPad.

Создайте сетевую папку SMB – корневой путь к клиентским журналам событий. В этой папке в последующем будут сохраняться клиентские журналы событий, отправленные пользователями на сервер из клиентских приложений WorksPad. В качестве имени для папки можно использовать, например, «WorksPadClientLogs». На папку необходимо предоставить **полные права доступа** пользователю, который в последующем будет использоваться для взаимодействия с данной папкой.

7.4. Создание корневой папки для FileBox

Данные действия необходимо выполнить, только если планируется использование WorksPad FileBox.

Создайте общую папку SMB – **корневой путь к пользовательским папкам**. В этой папке в последующем будут создаваться персональные папки пользователей WorksPad. В качестве имени для папки можно использовать, например, «WorksPadFileBox». На данную папку необходимо предоставить **полные права доступа пользователям всех доменов** (группы «Domain Users» всех доменов, пользователи которых будут работать с системой WorksPad).

7.5. Создание корневой папки для опубликованных файлов

Данные действия необходимо выполнить, только если планируется использование функциональности внешних ссылок WorksPad.

Создайте общую папку SMB – **корневой путь к опубликованным файлам**. В этой папке в последующем будут размещены опубликованные по внешним ссылкам файлы. В качестве имени для папки можно использовать, например, «WorksPadShareBox». На папку необходимо предоставить **полные права доступа** пользователю, который в последующем будет использоваться для взаимодействия с данной папкой.

8. Установка системы

Чтобы установить компоненты WorksPad запустите файл дистрибутива.

Внимание! Программу установки необходимо запускать от имени [учётной записи для служб WorksPad](#).

Программа установки выполнена в виде мастера. Каждое окно содержит набор кнопок для управления процессом установки. Кратко поясним их назначение:

- **Далее** – принять действие и перейти к следующему шагу процедуры установки.
- **Назад** – вернуться на предыдущий шаг установки.
- **Отмена** – отказаться от установки продукта.
- **Готово** – завершить процедуру установки программы на компьютер.

Рассмотрим подробно каждый шаг процедуры установки программы.

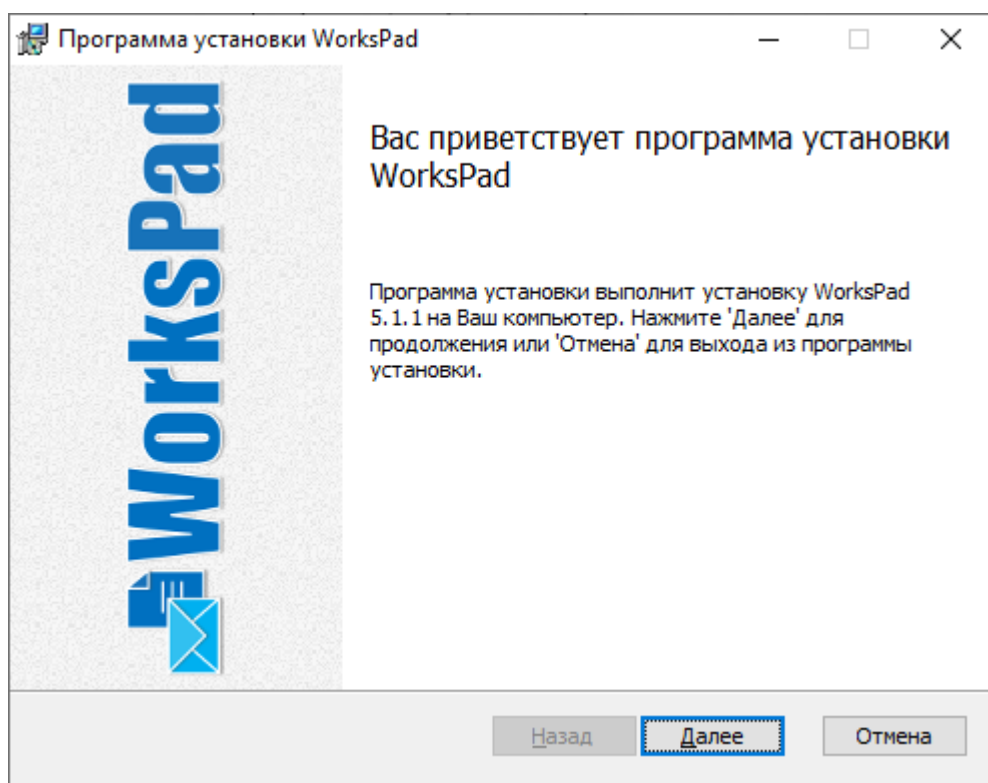
Шаг 1. Проверка соответствия системы необходимым условиям установки

Перед установкой компонентов WorksPad на компьютере проверяется соответствие операционной системы, пакетов обновлений (Service Pack) и программного обеспечения программным требованиям для установки.

Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление. После вашего ознакомления с ним программа установки будет завершена. Установите недостающие компоненты, после чего запустите программу установки WorksPad повторно.

Шаг 2. Стартовое окно процедуры установки

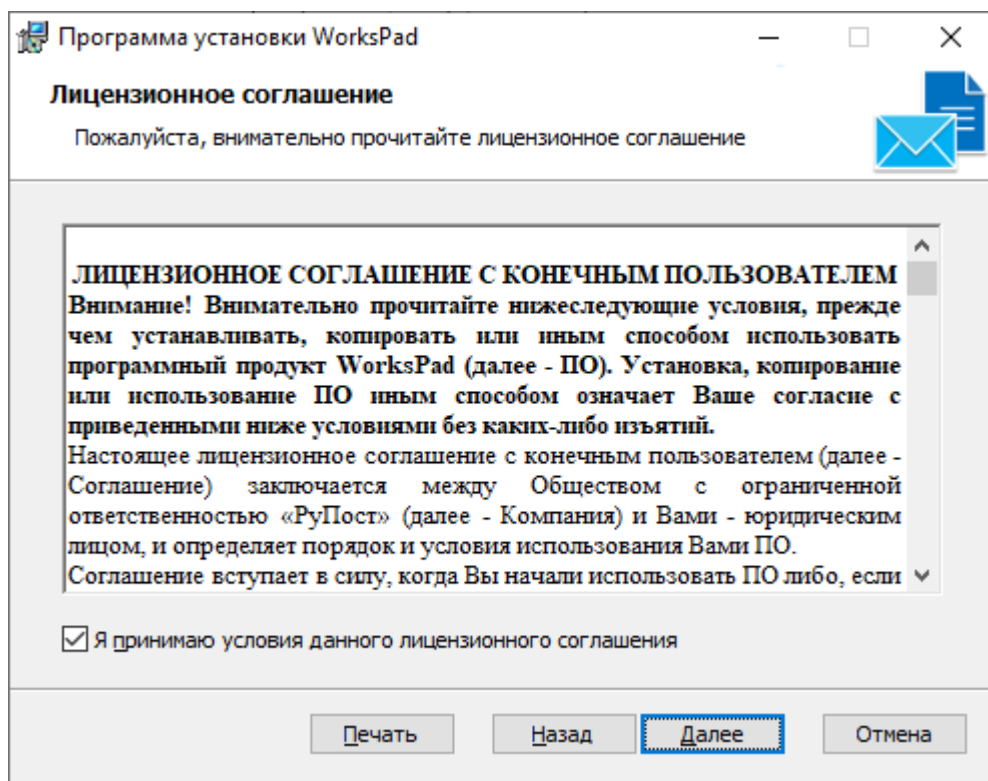
Если ваша система полностью соответствует предъявляемым требованиям, сразу после запуска файла дистрибутива на экране будет открыто стартовое окно, содержащее информацию о начале установки WorksPad на компьютер.



Для продолжения установки нажмите на кнопку «**Далее**». Отказ от установки продукта выполняется по кнопке «**Отмена**».

Шаг 3. Просмотр лицензионного соглашения

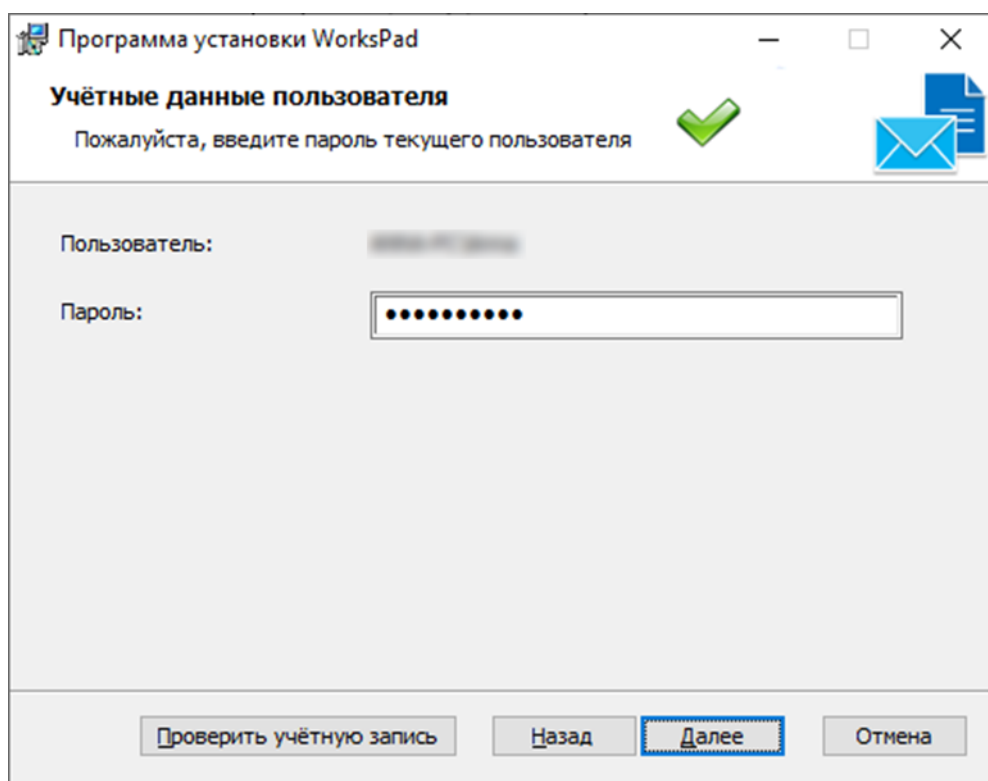
Следующее окно программы установки содержит лицензионное соглашение, которое заключается между вами и «РуПост». Внимательно прочтите его, и, при условии, что вы согласны со всеми пунктами соглашения, поставьте галочку рядом с фразой «**Я принимаю условия данного лицензионного соглашения**» и нажмите на кнопку «**Далее**». Установка будет продолжена.



Для отказа от установки нажмите на кнопку «Отмена».

Шаг 4. Ввод данных служебной учётной записи пользователя

На этом шаге установки необходимо ввести **пароль текущей учётной записи пользователя**. Это необходимо для запуска выше перечисленных служб от имени текущего пользователя. Если установка выполняется впервые, эта служебная учётная запись пользователя будет заведена в системе WorksPad как первый администратор.



После ввода пароля нажмите кнопку «**Проверить учётную запись**». По окончании проверки параметров учётной записи в LDAP в верхней части данного окна программы установки будет отображена соответствующая результату иконка. Ниже представлены возможные варианты с пояснениями:



– Параметры учётной записи указаны верно.



– Параметры учётной записи указаны не верно.

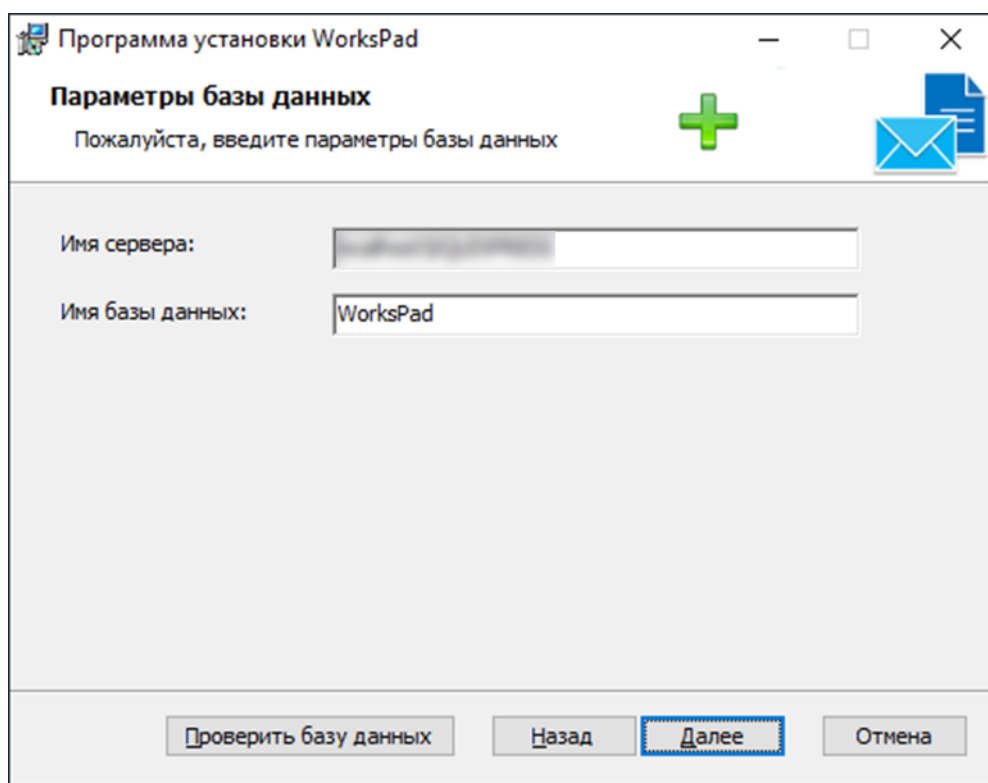
При положительном результате проверки учётной записи в LDAP кнопка «**Далее**» станет активна. Нажмите её для продолжения установки.

Шаг 5. Ввод параметров базы данных

На данном этапе установки необходимо указать параметры доступа к базе данных для системы WorksPad (база данных должна быть уже создана).

Необходимо ввести следующие параметры:

- **Имя сервера** – название сервера, на котором расположена база данных.
- **Имя базы данных** – название базы данных.



После заполнения необходимых полей нажмите кнопку «**Проверить базу данных**». По завершению проверки соединения и состояния базы данных в верхней части данного окна программы установки будет отображена соответствующая результату иконка. Ниже представлены возможные варианты с пояснениями:



– Доступна пустая база данных. Во время установки будут созданы все необходимые компоненты базы данных. **Все ранее созданные компоненты базы данных будут удалены.** Также на следующем шаге программы установки необходимо будет произвести начальные настройки системы.



– База данных доступна, но требует обновления компонентов для совместимости с устанавливаемой версией программы. Во время установки программы будут созданы дополнительные компоненты базы данных³. **Существующие в базе данные сохранятся.**



– База данных доступна, и соответствует данной версии программы.



– База данных недоступна.

В случае успешного соединения с базой данных кнопка «**Далее**» будет активна. Нажмите её для продолжения установки.

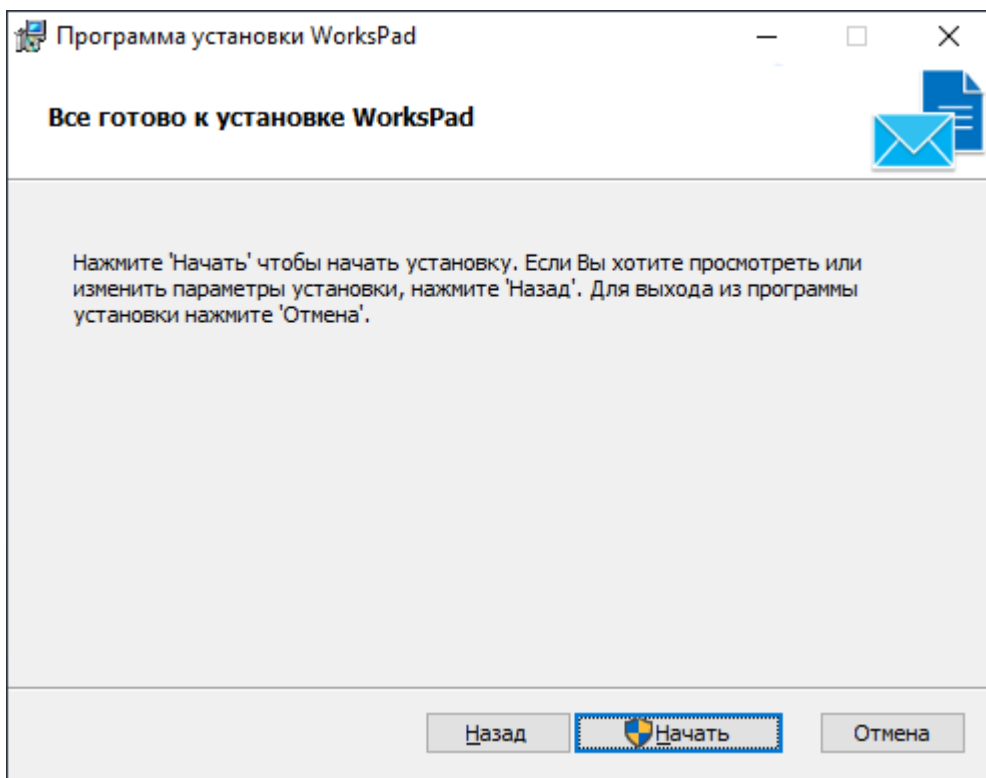
Шаг 6. Подтверждение установки программы

На данном этапе вам будет предложено:

³ Рекомендуется предварительно **создать резервную копию** базы данных.

- Начать установку. Для этого нажмите кнопку **«Начать»**.
- Вернуться к изменению или просмотру параметров установки. Для этого нажмите кнопку **«Назад»**.
- Выйти из программы установки. Для этого нажмите кнопку **«Отмена»**.

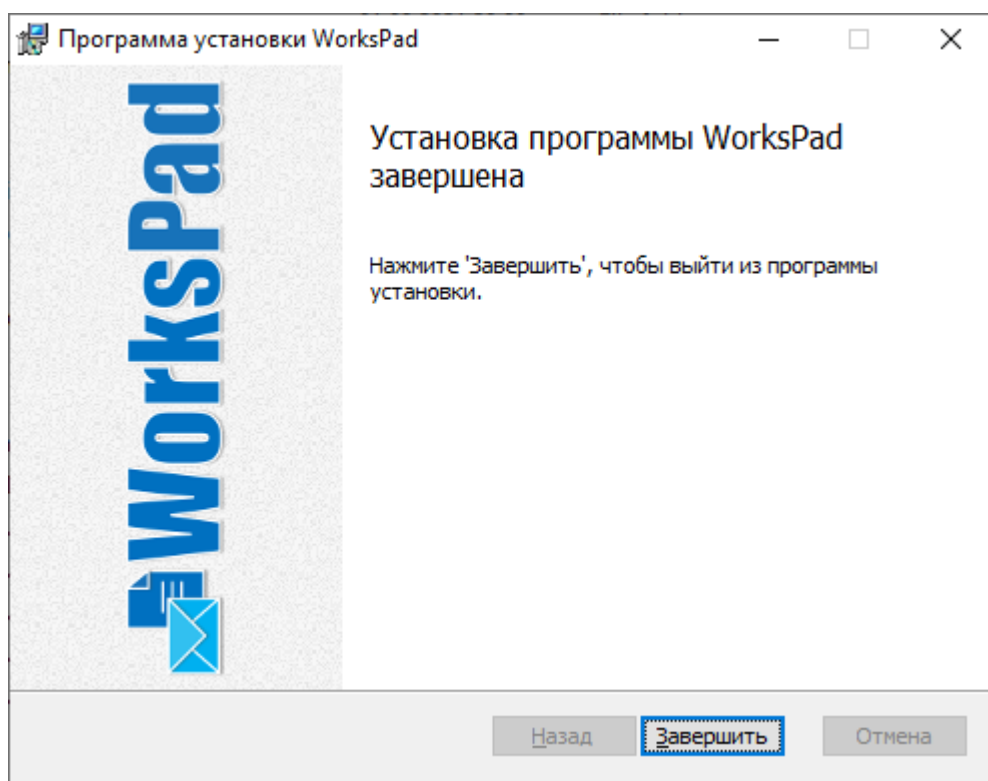
Для продолжения установки нажмите кнопку **«Начать»**.



Установка программы занимает некоторое время. Дождитесь ее завершения.

Шаг 7. Завершение процедуры установки

Окно завершения установки содержит информацию об окончании процесса установки компонентов WorksPad на ваш компьютер.



Нажмите кнопку «**Завершить**» для завершения работы программы установки.

В следующем разделе подробно описаны параметры установленной системы.

8.1. Параметры установленной системы

Компоненты сервера WorksPad устанавливаются в директорию «WorksPad», расположенную в корневом каталоге системного диска.

В результате установки сервера, в IIS создаётся сайт «WorksPad» с указанными ниже приложениями.

Приложение в IIS	Компонент сервера WorksPad	Удостоверение пула приложений
/adminapi	Admin API	Учётная запись для служб WorksPad
/admin	Administration Console	ApplicationPoolIdentity
/chatbotapi	Chatbot API	Учётная запись для служб WorksPad
/external	External Access Site	ApplicationPoolIdentity
/	Gateway Service	Учётная запись для служб WorksPad
/notification	Notification Service	Учётная запись для служб WorksPad
/share	Share Service	Учётная запись для служб WorksPad
/user	User Portal	ApplicationPoolIdentity

Для компонента Archiver Service создаётся служба Windows «WorksPad Archiver», которая работает от имени [учётной записи для служб WorksPad](#).

Во время первой установки сервера WorksPad создаётся специальный **сертификат безопасности**. Он служит для обеспечения конфиденциальности информации, хранимой в системе. В случае использования кластера серверов WorksPad, данный сертификат необходимо самостоятельно установить на другие сервера. Подробнее см. раздел [Создание кластера WorksPad](#).

8.2. Первоначальная настройка системы

Для первоначальной настройки системы WorksPad используется специальная учётная запись «`local\admin`» (локальный администратор). Пароль по умолчанию «`wpAdmin123`». Используйте её для входа в Консоль администратор сразу после установки системы.

Используя данную учётную запись зарегистрируйте в системе первый домен (LDAP). После этого добавьте в систему одного из пользователей этого домена, назначив ему роль «Администратор». Дальнейшую настройку системы производите от имени добавленного пользователя. Отключите учётную запись локального администратора. Подробнее см. раздел [Настройка локального администратора](#).

Рекомендуется изменить SSL-сертификат, используемый по умолчанию для Browser Proxy, на действительный сертификат для вашего домена, выпущенный доверенным центром сертификации. Подробнее см. раздел [Настройка Browser Proxy](#). Этот же сертификат используйте для сайта «WorksPad» в IIS.

Установите лицензию WorksPad используя Консоль администратора. Подробнее см. Руководство администратора.

9. Создание кластера WorksPad

Подробное описание кластера WorksPad представлено в разделе [Многосерверная топология](#).

При установке нового узла WorksPad укажите базу данных, которую использовали при первом развёртывании системы.

Между всеми узлами системы необходимо открыть доступ по порту **443**. Данный порт используется для взаимодействия компонентов сервера WorksPad между собой.

На всех узлах кластера должен быть развёрнут сертификат безопасности. Он автоматически создаётся при первом развёртывании системы. Для добавления сертификата на новый узел необходимо выполнить следующие действия:

1. Выполните экспорт сертификата безопасности на первом узле WorksPad. Для этого в терминале первого узла выполните указанную ниже команду:

```
dotnet \WorksPad\CertTool\WorksPadCertTool.dll export --t <thumbprint> --f \tmp\sec_cert.pfx --p <password>
```

Замените **<thumbprint>** на хэш сертификата безопасности. Его можно посмотреть в Консоли администратора в разделе «Общие настройки» (подробнее см. Руководство администратора).
Замените **<password>** на пароль, которым будет защищён файл сертификата.
Внимание! Команду необходимо выполнять от имени [учётной записи для служб WorksPad](#).
2. Скопируйте файл сертификата безопасности «\tmp\sec_cert.pfx» на сервер нового узла WorksPad в папку «\tmp».
3. Добавьте сертификат безопасности в хранилище сертификатов нового узла. Для этого в терминале нового узла выполните указанную ниже команду:

```
dotnet \WorksPad\CertTool\WorksPadCertTool.dll addseccert --f \tmp\sec_cert.pfx --p <password>
```

Замените **<password>** на пароль, которым защищён файл сертификата.
Внимание! Команду необходимо выполнять от имени [учётной записи для служб WorksPad](#).

После установки нового узла WorksPad, его компоненты автоматически регистрируют себя в системе.

Подключите новый узел к балансировщику нагрузки для обработки **HTTPS/WSS** трафика по порту **443** и **TCP** трафика по порту **5757**.

На балансировщике нагрузки используйте действительный сертификат для вашего домена, выпущенный доверенным центром сертификации.

Балансировщик нагрузки необходимо использовать в режиме сохранения сессии (session persistence). Например, на основе IP-адреса источника.

10. Конфигурирование системы

После установки системы WorksPad, некоторые компоненты системы можно настроить вручную, изменяя их параметры в соответствии с Вашими требованиями. Ниже представлено описание по настройке каждого из этих компонентов.

10.1. Конфигурирование Gateway Service

Чтобы произвести настройку Gateway Service необходимо открыть файл конфигурации службы «\WorksPad\GatewayService\appsettings.json».

Внимание! После изменения конфигурационного файла необходимо перезапустить службу в IIS.

10.1.1. Настройка локального администратора

Параметры учётной записи **локального администратора** «local\admin» расположены в секции «**LocalAdmin**» файла конфигурации.

Пример (представлена часть конфигурационного файла):

```
"LocalAdmin": {  
  "Enabled": true,  
  "Password": "wpAdmin123"  
},
```

Для разрешения/запрета использования данной учётной записи измените значение параметра «**LocalAdmin/Enabled**» на true или false соответственно. Для смены пароля учётной записи измените значение параметра «**LocalAdmin/Password**» на любое необходимое.

10.1.2. Настройка Browser Proxy

Параметры Browser Proxy расположены в секции «**BrowserProxy**» файла конфигурации.

Пример (представлена часть конфигурационного файла):

```
"BrowserProxy": {  
  "Enabled": true,  
  "LoggingTag": "ClientConnectionError, ClientRequestError, HttpProxyError, IOError",  
  "ListenIP": "0.0.0.0",  
  "ListenPort": "5757",  
  "Certificate": {  
    "Path": "../SslCert.pfx",  
    "Password": "Wp.$$L",  
    "AllowInvalid": true  
  }  
},
```

Для включения/отключения данной функциональности измените значение параметра «**BrowserProxy/Enabled**» на true или false соответственно.

Для смены прослушиваемого IP-адреса измените значение параметра «**BrowserProxy/ListenIP**». Для смены прослушиваемого порта измените значение параметра «**BrowserProxy/ListenPort**».

Параметры SSL-сертификат для Browser Proxy расположены в секции «**BrowserProxy/Certificate**».

Поддерживаются различные источники сертификата:

- Файл «.pfx». Настраиваемые параметры:
 - «**BrowserProxy/Certificate/Path**» – путь к файлу сертификата в формате «.pfx».
 - «**BrowserProxy/Certificate/Password**» – пароль для доступа к данным сертификата.
- Файлы «.pem»/«.crt» и «.key».
 - «**BrowserProxy/Certificate/Path**» – путь к файлу в формате «.pem»/«.crt».
 - «**BrowserProxy/Certificate/KeyPath**» – путь к файлу в формате «.key».
 - «**BrowserProxy/Certificate/Password**» – пароль для доступа к данным сертификата.
- Хранилище сертификатов.
 - «**BrowserProxy/Certificate/Subject**» – имя субъекта для сертификата.
 - «**BrowserProxy/Certificate/Store**» – название хранилища сертификатов («My» – личное или «WebHosting» – размещение веб-служб).
 - «**BrowserProxy/Certificate/Location**» – название расположения хранилища («LocalMachine» – локальный компьютер или «CurrentUser» – текущий пользователь).

Для разрешения/запрета использования ненадёжного сертификата (например, самозаверенного) измените значение параметра «**BrowserProxy/Certificate/AllowInvalid**» на «true» или «false» соответственно.

10.1.3. Настройка прокси-сервера для Telegram

Параметры прокси-сервера для соединения Gateway Service с сервером Telegram расположены в секции «**Telegram**» файла конфигурации.

Пример (представлена часть конфигурационного файла):

```
"Telegram": {  
  "ProxyAddress": "http://localhost:8888"  
},
```

В значении параметра «**Telegram/ProxyAddress**» указывается URL-адрес прокси-сервера.

Примечание. Прокси-сервер должен работать в режиме «без аутентификации».

10.1.4. Настройка прокси-сервера для Microsoft Bot Framework

Параметры прокси-сервера для соединения Gateway Service с сервером Microsoft Bot Framework расположены в секции «**MsBotFramework**» файла конфигурации.

Пример (представлена часть конфигурационного файла):

```
"MsBotFramework": {  
  "ProxyAddress": "http://localhost:8888"  
},
```

В значении параметра «**MsBotFramework/ProxyAddress**» указывается URL-адрес прокси-сервера.

Примечание. Прокси-сервер должен работать в режиме «без аутентификации».

10.2. Конфигурирование Archiver Service

Чтобы произвести настройку Archiver Service необходимо открыть файл конфигурации службы «\WorksPad\ArchiverService\appsettings.json».

Внимание! После изменения конфигурационного файла необходимо перезапустить службу в IIS.

Пример (представлена часть конфигурационного файла):

```
"StartTime": "02:00",  
"MaxDuration": "3" // In hours
```

В значении параметра «**StartTime**» указывается время (в формате – «часы:минуты») запуска задачи архивирования журнала событий.

В значении параметра «**MaxDuration**» указывается максимальное время (в часах) выполнения задачи архивирования журнала событий.

11. Поддержка

В случае возникновения любых вопросов или проблем во время установки, пожалуйста, свяжитесь со службой технической поддержки WorksPad по адресу support@workspad.com или разместите свой запрос на веб-сайте <https://support.workspad.com>.