



**ПРОГРАММНЫЙ КОМПЛЕКС
РАСПРЕДЕЛЕННОЙ ПЕЧАТИ
«PRINT-X»**

**РУКОВОДСТВО ПО УСТАНОВКЕ
МОДУЛЯ ПЕЧАТИ, МОДУЛЯ
УПРАВЛЕНИЯ ЗАЯВКАМИ И МОДУЛЯ
ВИЗУАЛИЗАЦИИ**

Листов 30

Москва

2024



ВВЕДЕНИЕ

Данный документ представляет собой руководство системного администратора по установке программного продукта Print-X. Предполагается, что производящий установку системы обладает необходимыми навыками работы с MS IIS Web Server, MS SQL Server и необходимыми правами для подключения к серверам и выполнения необходимых операций на них.

ПРИМЕЧАНИЕ: Данный документ описывает установку комплексного продукта, состоящего из нескольких модулей; в зависимости от конкретной задачи, необходимо выделять инструкции только для требуемого модуля!

ТРЕБОВАНИЯ К СЕРВЕРУ

МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ

1 сервер для модулей Print-X и БД SQL [Модуля управления заявками]

- **Intel Core i3** и выше, 4 GB RAM, 100 GB HDD
- **MS Windows Server 2012** и выше (только 64 bit)
- **MS SQL Server 2017** и выше с поддержкой полнотекстовой индексации (Full-text Search) для русского языка
- **IIS 8** и выше
- **Oracle JAVA x32**
- **MS .NET Framework 4.8** и выше.

Возможно использование **MS SQL Server Express**, но для поддержки Full text Search необходима редакция **SQL Server with Advanced Services**. В состав дистрибутива Print-X входит **русская** версия MS SQL Server Express, поэтому для его установки требуется русская версия операционной системы. При необходимости использования англоязычной версии операционной системы необходимо будет установить MS SQL Server Express в английской редакции самостоятельно. Также при использовании **MS SQL Server Express** будут накладываться следующие ограничения (на примере **MS SQL 2017 Express**):

- на размер БД: 10 гигабайт
- на количество оперативной памяти: 1 Гигабайт
- на количество процессоров: 1 (или 4 ядра)
- **Windows Server** должен иметь следующие роли: **Web server** с включенным **WebSocket Protocol, Application Server, Web server (IIS) Support**
- Подключение к **Internet**
- Для администрирования необходим один из браузеров Microsoft Internet Explorer 11, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, Safari

РЕКОМЕНДУЕМЫЕ ТРЕБОВАНИЯ

2 сервера: 1 для модулей Print-X и 1 для БД SQL [Модуля управления заявками].

Для модулей Print-X:



- **Intel Core i5** и выше, 8+ GB RAM, 100 GB HDD
- **MS Windows Server 2012** и выше (только 64 bit)
- **IIS 8** и выше
- **MS .NET Framework 4.8** и выше
- **Windows Server** должен иметь следующие роли: **Web server** с включенным **WebSocket Protocol, Application Server, Web server (IIS) Support**
- Для администрирования необходим один из браузеров Microsoft Internet Explorer 11, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, Safari

Для БД SQL [Модуля управления заявками]:

- **Intel Core i5** и выше, 8+ GB RAM, 250 GB HDD
- **MS Windows Server 2012 64 bit** и выше
- **MS SQL Server 2017** и выше с поддержкой полнотекстовой индексации (Full-text Search) для русского языка. Возможно использование MS SQL Server Express, но для поддержки Full-text Search необходима редакция SQL Server with Advanced Services. В состав дистрибутива Print-X входит **русская** версия MS SQL Server Express, поэтому для его установки требуется русская версия операционной системы. При необходимости использования англоязычной версии операционной системы необходимо будет установить MS SQL Server Express в английской редакции самостоятельно. При использовании MS SQL Server Express ограничения аналогичны описанным выше
- **Oracle JAVA x32**
- Подключение к **Internet**

Важно: на всех серверах должен быть установлен один и тот же часовой пояс. Например, (UTC +3:00) Волгоград, Москва, Санкт-Петербург (RTZ 2).

Важно: все серверы и клиенты должны являться членами домена MS Active Directory.

Важно: в домене должен быть развернут центр сертификации, способный выдавать сертификаты серверам домена.

Важно: в домене должен существовать почтовый сервер для организации взаимодействия различных модулей Print-X и пользователей.

ПОРЯДОК УСТАНОВКИ СИСТЕМЫ

Для установки системы необходимо:

1. Подготовить учетную запись для запуска **Print-X. Модуль управления заявками** (опционально).
2. Восстановить чистую базу данных **Print-X. Модуль управления заявками** из бэкапа, настроить права доступа к базе данных.
3. Произвести предварительную настройку **Print-X. Модуль печати** (задать через программу Easy Config пароль учетной записи *admin и пароль для БД Firebird).
4. Настроить **Print-X. Модуль управления заявками** на веб-сервере IIS.
5. Настроить дополнительные сервисы **Print-X. Модуль управления заявками**: отправку почтовых и/или sms-уведомлений, интеграцию с ActiveDirectory, LDAP авторизацию, создание заявок по email и другие.
6. Настроить **Print-X. Модуль печати** согласно руководству администратора, включая настройку действий с отправкой сообщений электронной почты при возникновении событий.



7. Настроить **Print-X. Модуль панели состояния.**

Важно: соответствующие настройки и необходимые параметры описаны в Руководстве администратора.

УСТАНОВКА СИСТЕМЫ

Ниже будет описан процесс установки **ВСЕХ МОДУЛЕЙ СИСТЕМЫ** на примере **одного** чистого сервера на базе MS Windows Server 2012 R2 и MS SQL Server 2017 / MS SQL Management Studio 2017 с англоязычным интерфейсом.

Перед началом установки необходимо:

- установить на сервере .NET Framework 4.8;
- установить Google Chrome (либо другой удобный для работы веб-браузер, подходящий под технические требования);
- подготовить для последующей установки, но не устанавливать MS SQL Management Studio 2017.

ПОРЯДОК УСТАНОВКИ

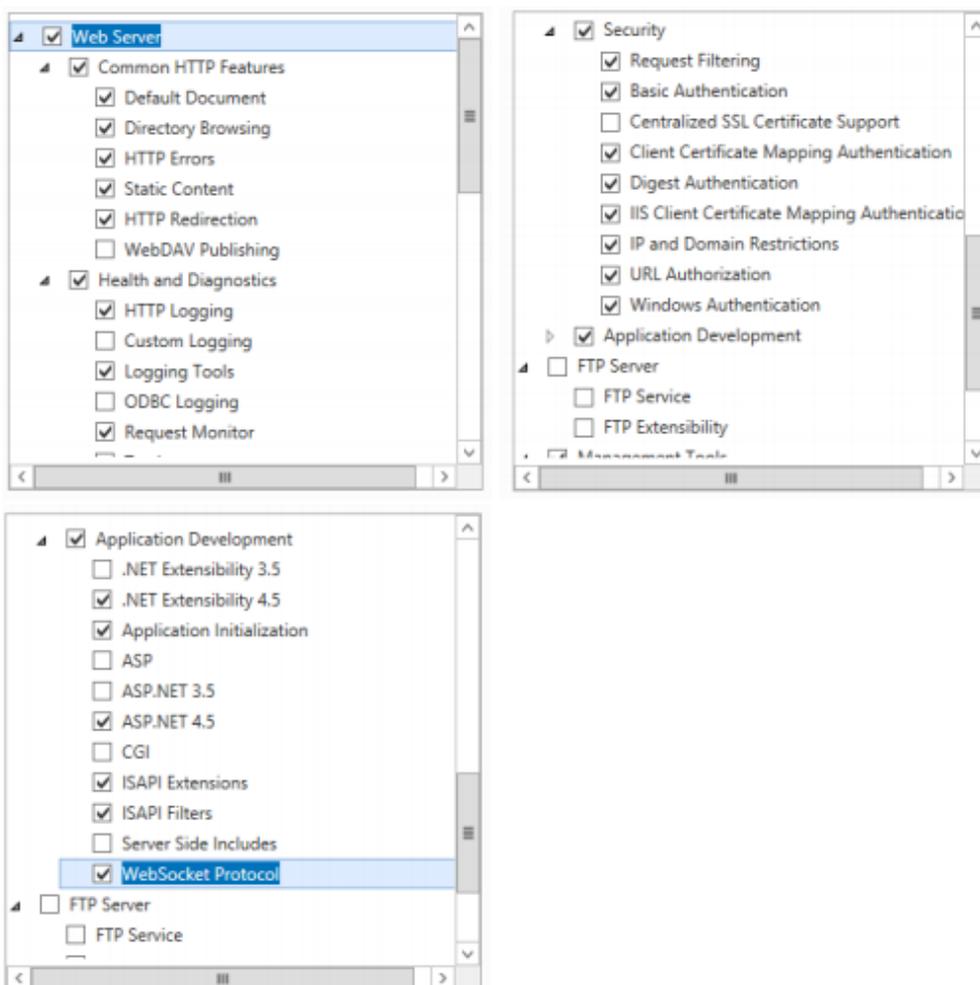
1. Запустить установку **Print-X** при помощи запуска **Print-X_full_5.2.14.48.exe** (или аналогичного дистрибутива другой версии).
2. Выбрать английский или русский язык.
3. Выбрать для установки все модули.
4. Установить **SQL EXPRESS**, не изменяя опции умолчанию. При установке **SQL EXPRESS** рекомендуется выбрать смешенный метод авторизации (Authentication Mode) и указать пароль пользователя **sa**.
5. После окончания установки **SQL EXPRESS**, закрыть окно **SQL Server Installation Center** и дождаться продолжения установки.
6. По окончании установки необходимо дождаться запуска **Easy Config** (не завершать программу установки) и задать пароль для доступа к WEB-интерфейсу Print-X. Модуль печати и пароль к БД Firebird (подробности см. в Руководстве администратора Print-X).
7. Выйти из программы **Easy Config** и закрыть программу установки нажатием на кнопку **Finish**.
8. Перезагрузить сервер.
9. Установить **MS SQL Management Studio 2017**, выбрав добавление компонентов к существующей инсталляции и указав в списке компонентов **Management Tools – Basic**.
10. Установить **IntraService Agent** (C:\Program Files\Print-X\web\iservice\IntraService Agent.msi).

Настройка Print-X Модуль управления заявками

ПОДГОТОВКА ВЕБ-СЕРВЕРА Print-X. Модуль управления заявками

Для установки Print-X. Модуль управления заявками необходимо подготовить web-server, установив необходимые роли и компоненты сервера. Ниже приведен пример настройки ролей и компонентов для Windows Server 2012 R2.

1. Запустите Server Manager либо из панели задач, либо, нажав Win+R, введите **servermanager** и нажмите ОК.
2. В открывшемся окне **Server Manager** в разделе **Dashboard** выберите **Add roles and features**, в открывшемся окне **Add roles and features Wizard** нажмите **Next, Next**.
3. В разделе **Server selection** выберите текущий сервер из списка **Server Pool** и нажмите **Next**.
4. В разделе **Server roles** выберите **Application server, Web server (IIS)** (в открывшемся окне нажмите **Add features**), нажмите **Next**.
5. В разделе **Features** отметьте, если не отмечено, **.NET Framework 4.5 Features** с компонентами по умолчанию, нажмите **Next, Next**.
6. В разделе **Application server / Role services** выберите **.NET Framework 4.5, Web Server (IIS) Support** (в открывшемся окне нажмите **Add features**), нажмите **Next, Next**.
7. В разделе **Web server role (IIS) / Role services** выберите компоненты, как показано на скриншотах ниже:



Здесь же установите **Management tools / IIS Management Console**, нажмите **Next**

8. На следующем экране **Confirmation** нажмите **Install** и дождитесь сообщения об окончании установки, после перезагрузите сервер для корректного применения изменений.

ПОДГОТОВКА УЧЕТНОЙ ЗАПИСИ ДЛЯ ЗАПУСКА Print-X. Модуль управления заявками

Пул приложений (Application pool), обслуживающий сайт системы на веб-сервере в MS Windows Server 2012/2016 может работать от имени следующих учетных записей:

- ApplicationPoolIdentity. Эта учетная запись используется как правило по умолчанию. Это встроенная учетная запись пула приложений, которая обычно выглядит так: IIS APPPOOL\poolname, где poolname – наименование соответствующего пула приложений. Например, для пула приложений Intraservice такая учетная запись имеет вид IIS APPPOOL\Intraservice
- Локальная учетная запись сервера. Здесь имеется в виду учетная запись, созданная на веб-сервере локально. Например, SERVER\IS_USER, SERVER\Intraservice и так далее.
- Доменная учетная запись. Здесь имеется в виду учетная запись, созданная в домене Active Directory специально для запуска приложения системы и просмотра содержимого домена



(для случая интеграции с Active Directory и авторизации в системе посредством Single Sign On). Также такая учетная запись может быть использована для подключения приложения к базе данных, расположенной на другом сервере.

Важно: в случае, если планируется запуск пула приложений от имени локальной учетной записи сервера или от доменной учетной записи, то конкретная учетная запись должна иметь полномочия **Log on as batch job** (вход в качестве пакетного задания) на сервере. Соответственно, необходимо создать в домене учетную запись, например, DOMAIN\Intracservice и дать ей полномочия **Log on as batch job** на сервере приложения. Для этого необходимо:

1. Откройте оснастку политик безопасности сервера.

Нажмите клавиши **Win+R**, введите **secpol.msc** и нажмите **OK**.

2. В открывшемся окне разверните раздел **Local policies** и выберите **User rights assignment**

3. В правой части окна найдите пункт **Log on as batch job**, два раза кликните по нему, добавьте учетную запись DOMAIN\Intracservice на вкладке **Local security settings** и нажмите **OK**.

ПОДГОТОВКА СЕРВЕРА БАЗ ДАННЫХ

Для работы системы необходимо, чтобы на сервере баз данных была включена интеграция с **CLR**.

Для того, чтобы проверить, включена ли интеграция, необходимо выполнить следующий запрос в **MS SQL Management Studio**:

```
SELECT * FROM sys.configurations
```

```
WHERE name = 'clr enabled'
```

- Если при выполнении запроса вернулось **clr enabled, value 1**, значит интеграция с **CLR** на сервере баз данных включена

configuration_id	name	value	minimum	maximum	value_in_use	description	is_dynamic	is_advanced
1	clr enabled	1	0	1	1	CLR user code execution enabled in the server	1	0

- Если же вернулось **value 0**, значит интеграция не включена. Чтобы ее включить, необходимо использовать хранимую процедуру **sp_configure**:

```
sp_configure 'show advanced options', 1;
```

```
GO
```

```
RECONFIGURE;
```

```
GO
```



```
sp_configure 'clr enabled', 1;
```

```
GO
```

```
RECONFIGURE;
```

```
GO
```

После выполнения процедуры вы должны увидеть следующее сообщение:

```
Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
```

```
Configuration option 'clr enabled' changed from 0 to 1. Run the RECONFIGURE statement to install.
```

Оно означает, что интеграция с CLR успешно включена.

Важно: Выполнение данных операций необходимо производить от имени учетной записи, имеющей полномочия системного администратора на сервере баз данных (роль **sysadmin**)

ВОССТАНОВЛЕНИЕ БАЗЫ ДАННЫХ Print-X. Модуль управления заявками ИЗ БЭКАПА

1. На сервере БД запустите **MS SQL Management Studio** и подключитесь к серверу БД под учетной записью, обладающей ролью **sysadmin** на сервере БД
2. Правой кнопкой кликните в дереве **Databases** и в выпадающем меню выберите **Restore files and filegroups**
3. В открывшемся окне укажите **Servionica** в качестве имени будущей базы данных в поле **To database**, затем установите переключатель **Source for restore** в положение **From device**, в открывшемся окне **Select backup devices**, нажав кнопку **Add** и выберите на диске файл бэкапа базы данных (например, is4_servionica_2012.bak).

Важно: Сразу после установки Print-X файл бэкапа расположен в каталоге C:\Program Files\Print-X\web\iservice

После выбора файла бэкапа нажмите **Ok** и закройте окно выбора файла бэкапа.

4. В окне **Restore files and filegroups** установите чекбокс напротив выбранного файла бэкапа базы данных и нажмите **OK**, после чего дождитесь сообщения об успешном восстановлении базы данных из бэкапа.

5. После восстановления базы данных, разверните ветку **Databases**, найдите базу **Servionica**, кликните по ней правой кнопкой мыши и выберите пункт **Properties** в выпадающем меню.

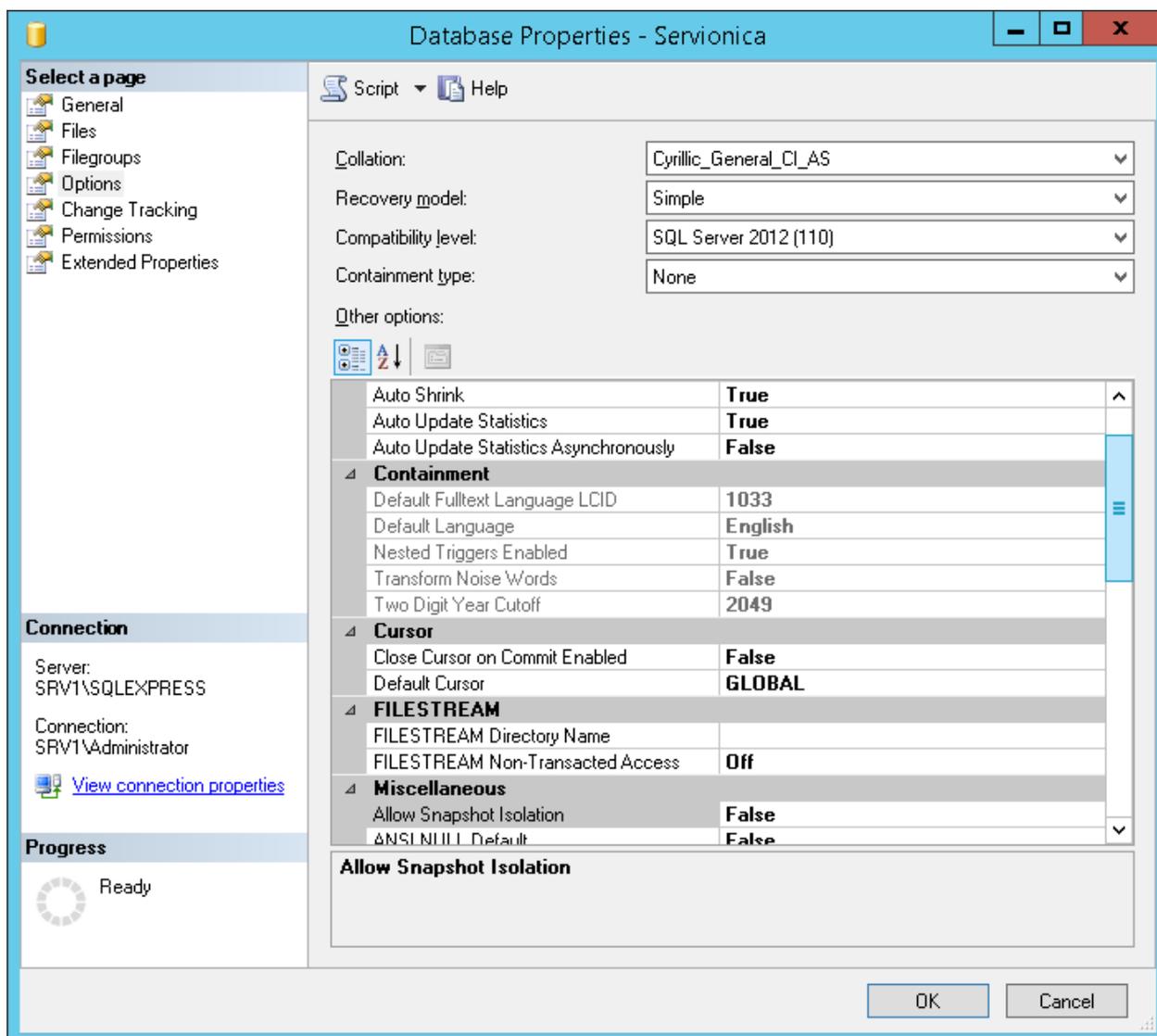
6. В окне **Database properties** выберите слева раздел **Options** и установите для базы данных следующие параметры:

а) **Collation:** Cyrillic_General_CI_AS (по умолчанию)

b) **Recovery model:** Simple

c) **Compatibility level:** 2012 (2014 или 2016 если БД развернута на MS SQL Server 2014 или 2016 соответственно)

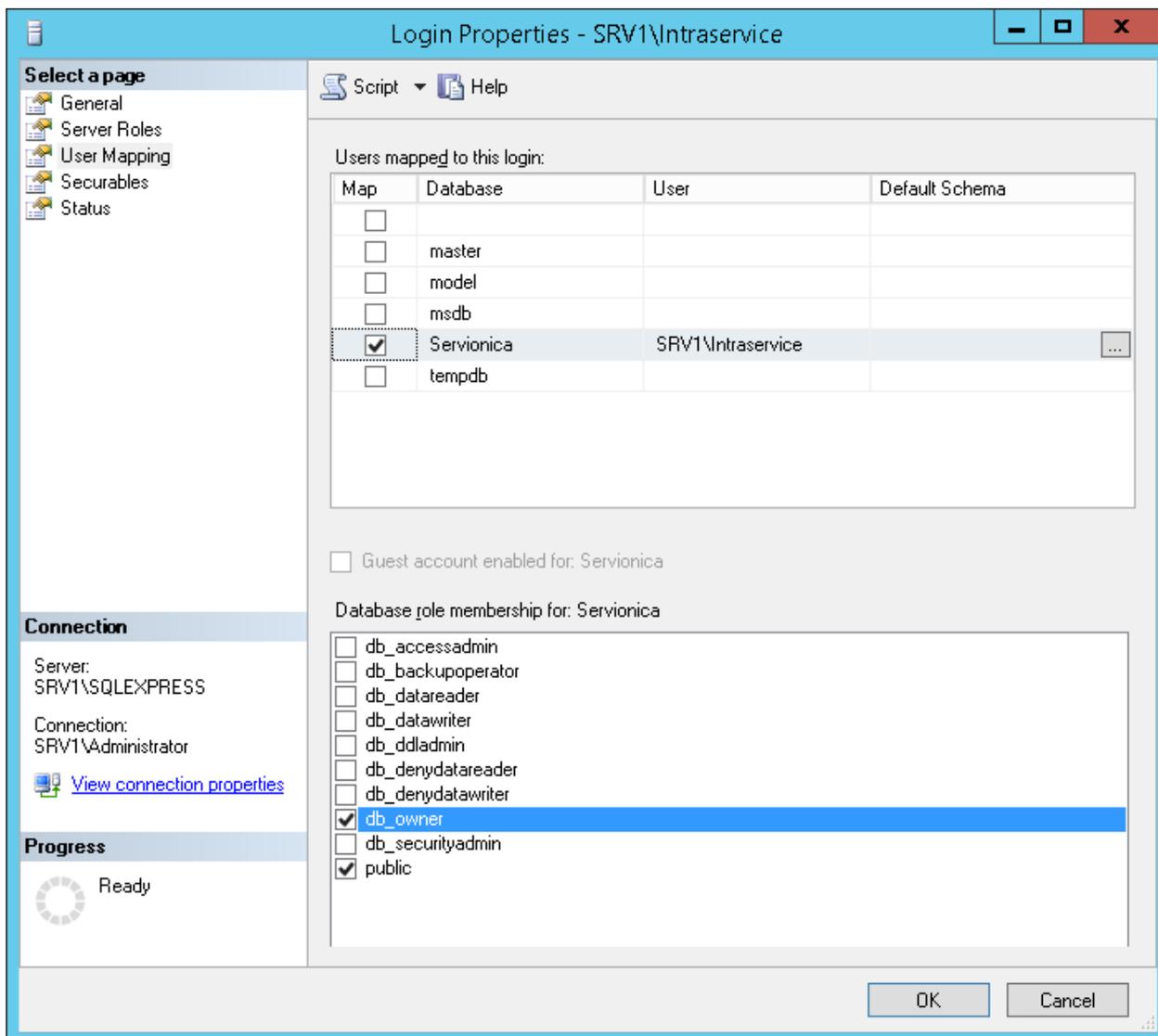
d) **Auto shrink:** True



НАСТРОЙКА ПРАВ ДОСТУПА К БАЗЕ ДАННЫХ

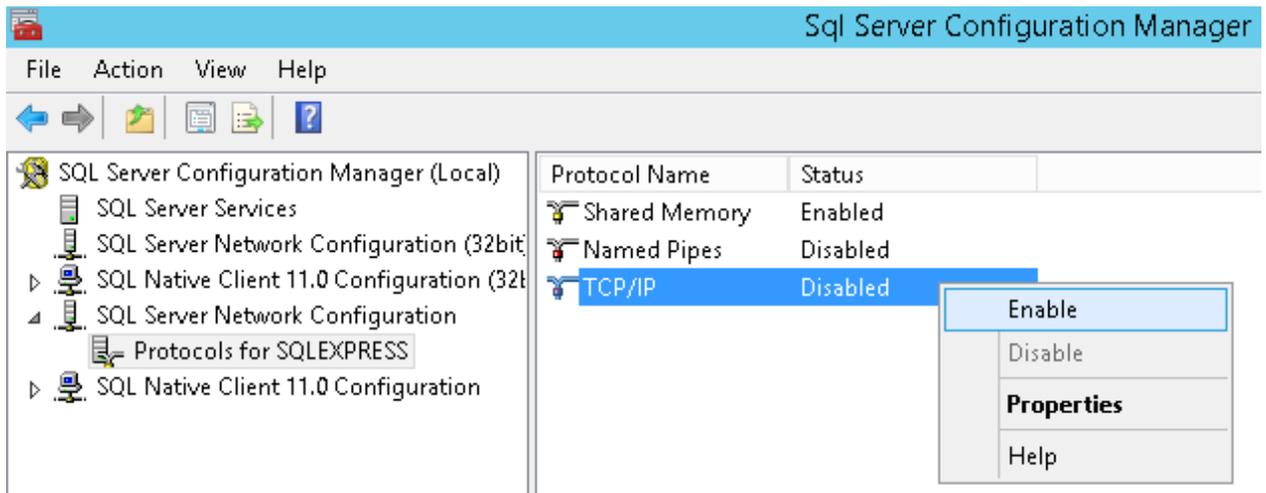
1. В **MS SQL Management Studio** разверните раздел **Security**, кликните правой кнопкой по разделу **Logins** и выберите в выпадающем меню **New Login**
2. В открывшемся окне нажмите кнопку **Search** рядом с полем **Login name**. В следующем окне выберите **Advanced**, далее **Search**, найдите созданную ранее учетную запись **DOMAIN\Intrасervice** и нажмите **OK**

3. Разверните раздел **Logins**, найдите добавленную только что учетную запись, кликните по ней правой кнопкой и выберите **Properties**
4. В разделе **User mapping** найдите развернутую из бэкапа базу данных **Servionica**, отметьте ее чекбоксом и ниже в поле **Database membership for:** установите чекбоксы **db_owner** и нажмите **OK**

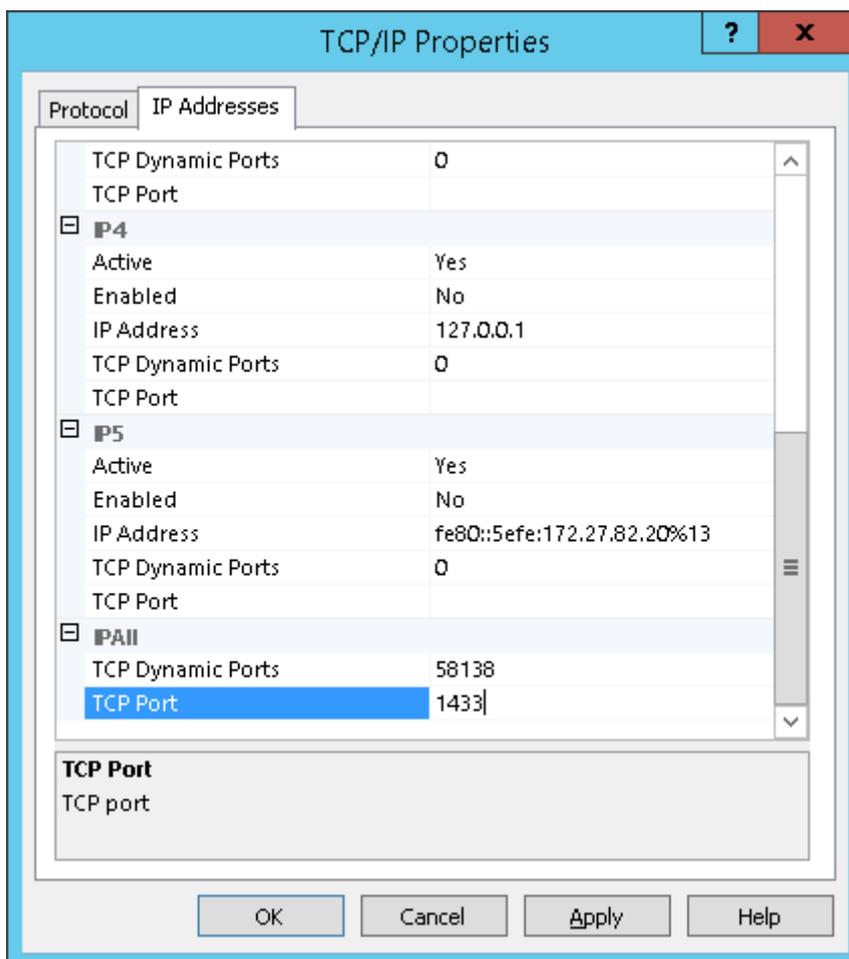


НАСТРОЙКА SQL СЕРВЕРА

1. Запустите **Sql Server Configuration Manager**
2. Разверните в левой панели узел **SQL Server Network Configuration**
3. Выберите **Protocols for SQLEXPRESS**
4. Кликните правой кнопкой по **TCP/IP** и выберите **Enable**

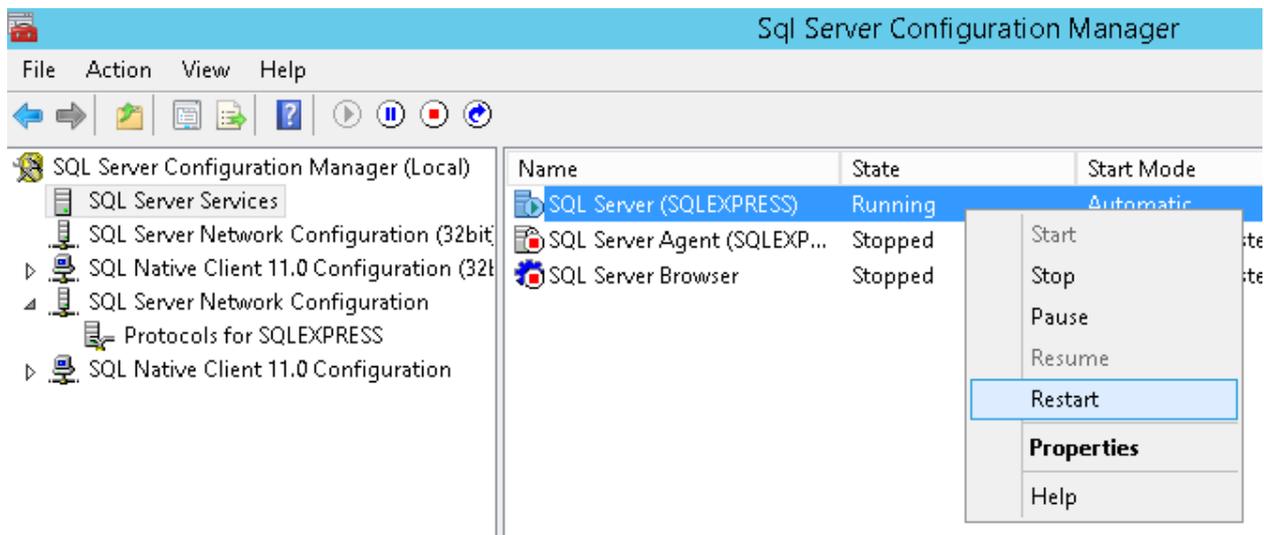


5. Кликните дважды протокол **TCP/IP** или выберите **Properties** в выпадающем меню
6. Перейдите на вкладку **IP Address**
7. В разделе IP All впишите **1433** в поле **TCP Port**



8. Нажмите **OK**
9. Выберите в левой панели **SQL Server Services**

10. Кликните правой кнопкой **SQL Server (SQLEXPRESS)** и выберите **Restart**



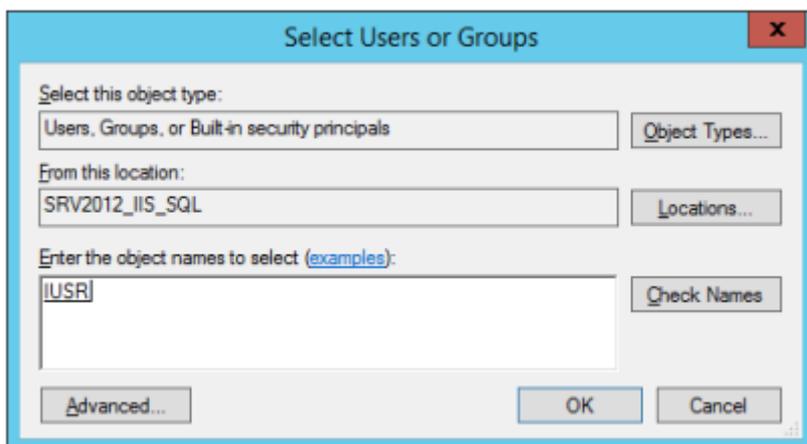
НАСТРОЙКА WEB-компонентов Print-X. Модуль управления заявками

СОЗДАНИЕ И НАСТРОЙКА САЙТА В КОНСОЛИ IIS

1. Для созданной ранее учетной записи DOMAIN\Intrasevice настройте права с полномочиями **modify** и **write** на следующие каталоги:

а) Каталог C:\Program Files\Print-X\web\iservice

*На данный каталог, помимо прочего, необходимо дать права на чтение встроенной учетной записи веб-сервера **IUSR**. Для этого необходимо вызвать диалоговое окно безопасности для каталога, перейти в режим редактирования существующих разрешений и добавить указанную учетную запись, введя **IUSR** в поле, как на скриншоте ниже и нажать **Check names**, после чего нажать **OK***



b) Каталог C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files

c) Каталог C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys

3. Откройте консоль управления IIS, нажав **Start menu / Administrative tools / Internet Information Services (IIS) Manager**. В разделе **Connections** разверните узел с именем сервера, кликните правой кнопкой по каталогу **Sites** и выберите **Add website**

4. Введите наименование сайта **Intraservice** в поле **Site name**. Система автоматически создаст пул приложений **Intraservice**

5. Введите путь к каталогу **Intraservice** с файлами приложения. Скорректируйте имя/адрес, по которому интерфейс будет доступен через веб-браузер.

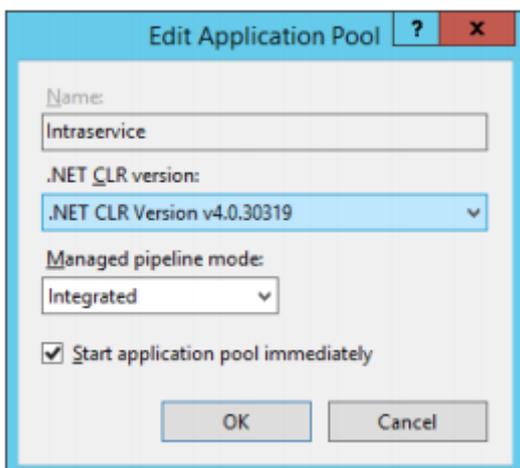
6. Установите порт **88**.

Важно: Путь к каталогу C:\Program Files\Print-X\web\iservice\Site

Поле **Host name** можно оставить пустым и в таком случае сайт будет доступен по имени/IP-адресу сервера, на котором произведена установка. Нажмите **OK**

6. Выберите созданный сайт **Intraservice** и перейдите в настройку аутентификации, выбрав **Authentication**. Убедитесь, что установлена только анонимная аутентификация **Anonymous authentication**

7. В разделе **Connections** в дереве слева перейдите к списку пулов приложений **Application Pools** и выберите пул **Intraservice**. Убедитесь, что значение в **.NET CLR Version** установлено так, как на скриншоте:



8. Измените учетную запись пула приложений на **DOMAIN\Intrасervice**. Для этого выберите пул приложений **Intrасervice**, кликните правой кнопкой и выберите **Advanced settings**. Найдите секцию **Process model** и в ней **Identity**. Измените учетную запись пула приложений с **ApplicationPoolIdentity** на **DOMAIN\Intrасervice**, введя логин и пароль в соответствующем окне в поле Custom Account. Нажмите **OK**

Важно: в системе предусмотрен функционал одновременной работы над заявкой нескольких пользователей, для корректной работы которого в пуле приложений значение параметра **Maximum Worker Processes** не должно быть установлено отличным от 1 (по умолчанию). Если же значение параметра отличное от единицы необходимо и вызвано какой-либо спецификой (балансировка нагрузки или подобное), то функционал одновременной работы над заявкой необходимо отключить через конфигурационный файл **web.config**, добавив параметр `<add key="hubConfig_Enable" value="false" />` в секцию `<appSettings>`.

Кроме того, не рекомендуется устанавливать для пула приложений ограничения по потребляемой памяти, т.к. это может негативно сказаться на работе системы в случае, если в системе ведется относительно активная работа с файлами в заявках. В такой ситуации в ряде случаев лимит потребления памяти, особенно если он относительно невелик, может достигаться пулом приложений достаточно часто, что приведет к частым перезагрузкам пула приложений.

В случаях, когда предполагается активная работа с файлами (много заявок с вложениями, скриншотами, к которым производится достаточно частый доступ), рекомендуется настраивать очистку (recycling) пула приложений не по памяти, а в определенное время, скажем, раз в сутки в 01:00

НАСТРОЙКА ПОДКЛЮЧЕНИЯ К БАЗЕ ДАННЫХ



После того, как web-сайт на IIS был создан, на SQL-сервере была развернута база данных и к ней были предоставлены права учетной записи пула приложений, необходимо настроить подключение сайта к базе данных:

1. Перейдите в каталог C:\Program Files\Print-X\web\iservice\Site в файловой структуре сервера, откройте конфигурационный файл приложения **web.config**. Найдите секцию **connectionStrings**, в ней строку подключения с ключом **IntraServiceConnectionString** и скорректируйте имя сервера и имя базы данных, чтобы они указывали на установленную базу данных.

Обычно параметр имеет примерный вид:

```
<add name="IntraServiceConnectionString" connectionString="Data Source=127.0.0.1,1433;Initial Catalog=Servionica;Integrated Security=True" providerName="System.Data.SqlClient" />
```

2. Для настройки подключения сайта к базе данных, нужно отредактировать следующие параметры:

а) **Data Source** – это имя/адрес SQL-сервера, нужно указать свой.

б) **Initial Catalog** – это имя БД на SQL-сервере. Нужно указать свою, в нашем случае **Servionica**

с) **Integrated Security=True** – параметр, отвечающий за возможность подключения к серверу баз данных от имени учетной записи пула приложений, как в данном случае. В ряде случаев, аналогичных рассматриваемому, когда сайт и база данных расположены на отдельных серверах, подключение сайта к базе данных может выполняться не только от имени доменной учетной записи пула приложений посредством **integrated security**, но и от имени встроенной учетной записи SQL-сервера. Для этого на сервере баз данных необходимо создать внутреннюю учетную запись, например, **sql_intraservice**, предоставить ей права на базу данных, как описано выше и указать реквизиты этой учетной записи в строке подключения в файле **web.config** в явном виде, например:

```
<add name="IntraServiceConnectionString" connectionString="Data Source=10.0.0.1,1433;Initial Catalog=Servionica;persist security info="True";User Id=sa;password=P@ssword" providerName="System.Data.SqlClient" />
```

ПРОВЕРКА РАБОТОСПОСОБНОСТИ Print-X. Модуль управления заявками

Для проверки правильности настройки введите в строке браузера http://server_address:88/, где **server_address** - это имя или IP-адрес сервера с настроенным модулем управления заявками. Если все сделано правильно, всем учетным записям выданы нужные права, то вы увидите форму авторизации в системе.

Попробуйте авторизоваться:

User: admin

Password: 12345

НАСТРОЙКА ДОПОЛНИТЕЛЬНЫХ СЕРВИСОВ

НАСТРОЙКА СКВОЗНОЙ WINDOWS И LDAP-АВТОРИЗАЦИИ

Система поддерживает авторизацию посредством механизма **Single Sign On**, когда авторизация происходит автоматически под текущей доменной учетной записью пользователя, минуя форму авторизации Модуля управления заявками. При этом, возможны два варианта использования такой системы:

- Система используется только в локальной сети и не имеет выхода наружу, доступ извне невозможен
- Одна и та же система используется как в локальной сети, так и доступна извне (например, извне работают внешние подрядчики, привлекаемые для выполнения заявок)

Для таких случаев возможна настройка и для сквозной авторизации в системе из локальной сети, и для авторизации извне с использованием одного веб-сервера.

НАСТРОЙКА ДЛЯ РАБОТЫ ТОЛЬКО ИЗ ЛОКАЛЬНОЙ СЕТИ

Для обеспечения сквозной авторизации **Single Sign On** должны выполняться следующие требования:

- Логин пользователя в Модуле управления заявками должен полностью совпадать с его доменным логином. Например, в домене DOMAIN пользователь имеет логин Ivan Petrov и такой же логин он должен иметь в Модуле управления заявками. Как правило, это требование выполняется автоматически в случае настройки функционала Синхронизации с Active Directory (см. раздел Настройки / Синхронизация с Active Directory в самой системе). При этом пароль пользователя в системе не обязательно должен совпадать с паролем пользователя в домене.
- Для сайта системы на веб-сервере **IIS** должна быть включена windows-аутентификация.
- Адрес сайта системы должен быть добавлен в зону местной интрасети (local intranet) в браузере Internet Explorer.

Необходимо выполнить следующие настройки:

1. В консоли управления **IIS** в разделе **Connections** выбрать **Intraservice** и перейти в раздел

Authentication. Отключить анонимную аутентификацию и включить Аутентификацию Windows:


Authentication

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

2. Внести изменения в файл **web.config**. Откройте каталог C:\Program Files\Print-X\web\iservice\Site с файлами приложения в файловой структуре сервера и откройте указанный файл любым текстовым редактором. Найдите секцию **appSettings** и настройте следующие параметры:

```
<add key="windowsAuthentication" value="true" />
```

Данный ключ отвечает непосредственно за возможность сквозной аутентификации Windows.

```
<add key="WindowsAuthenticationApplication" value="" />
```

```
<add key="LDAPAuthentication" value="true" />
```

Данный ключ отвечает за возможность авторизации в системе по доменным логину и паролю через форму авторизации самой системы (в данном случае доменный логин указывается без домена). После выхода из системы пользователь сможет авторизоваться как через сквозную авторизацию, так и введя доменный логин с паролем.

3. В этом же файле необходимо явно указать URL-адреса, при обращении к которым авторизация будет происходить посредством **Single Sign On**. В остальных случаях будет анонимная авторизация через форму.

Найдите секцию **windowsAuthenticationAddress** и укажите желаемые адреса для авторизации **Single Sign On**, например:

```
<windowsAuthenticationAddress>
```

```
<add key="address1" value="http://helpdesk" />
```

```
<add key="address2" value="http://server_IP" />
```

```
<add key="address3" value="http://helpdesk.domain.local/" />
```

```
</windowsAuthenticationAddress>
```

Значения данных параметров указываются именно с http:// или https://

После того, как вы выполните эти настройки, пользователи домена, зарегистрированные в системе, смогут авторизоваться в Модуле управления заявками автоматически по указанным выше адресам, не вводя логин и пароль.

НАСТРОЙКА ДЛЯ РАБОТЫ ИЗ ЛОКАЛЬНОЙ СЕТИ И ИЗВНЕ

Данная настройка предполагает возможность работы с системой как внутренним сотрудникам, так и внешним подрядчикам, используя различные механизмы авторизации в системе (single sign on для внутренних сотрудников, работающих в локальной сети и авторизацию по логину и паролю для внешних сотрудников, работающих извне локальной сети).

При такой настройке необходимо указать различные пути к системе для подразделений/пользователей, которые работают в локальной сети (адрес вида `http://helpdesk/`) и для подразделений/пользователей, которые работают извне (адрес вида `http://helpdesk.company.ru/`). Рекомендуем настраивать именно для подразделений. Это необходимо для корректного формирования ссылок на заявки в уведомлениях, отправляемых системой.

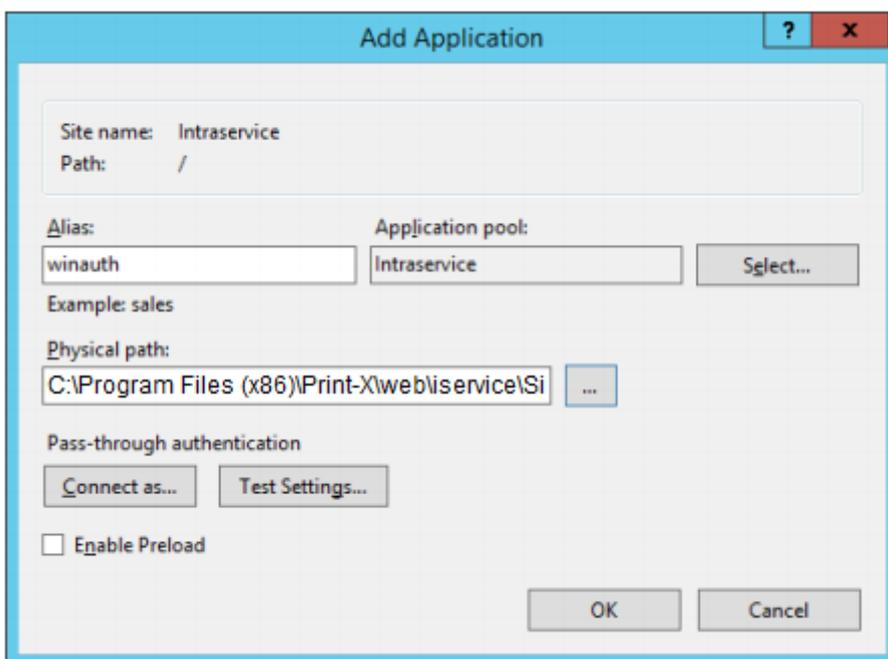
Для обеспечения возможности работы с одним физическим экземпляром системы и из локальной сети, и извне необходимо произвести следующую настройку:

1. Развернуть стандартный сайт на IIS по описанному выше сценарию, добавить адресные привязки для доступа из локальной сети и извне.

Например: для работы из локальной сети используем `http://helpdesk/`, для работы извне – `http://helpdesk.company.ru/`

2. Добавить к созданному сайту приложение. Выбрать сайт в консоли управления IIS, кликнуть по нему правой кнопкой и выбрать **Add Application**

3. Настроить для него тот же путь **Physical Path** (путь к каталогу с файлами), **Alias** – название приложения и **Application Pool** – тот же пул, который используется для сайта. Обычно выбирается пул по умолчанию.



4. Отредактировать файл **web.config**. Найти и настроить следующие параметры:

```
<add key="windowsAuthentication" value="true" />
```

Данный ключ отвечает непосредственно за возможность сквозной аутентификации Windows.

```
<add key="WindowsAuthenticationApplication" value="/winauth" />
```

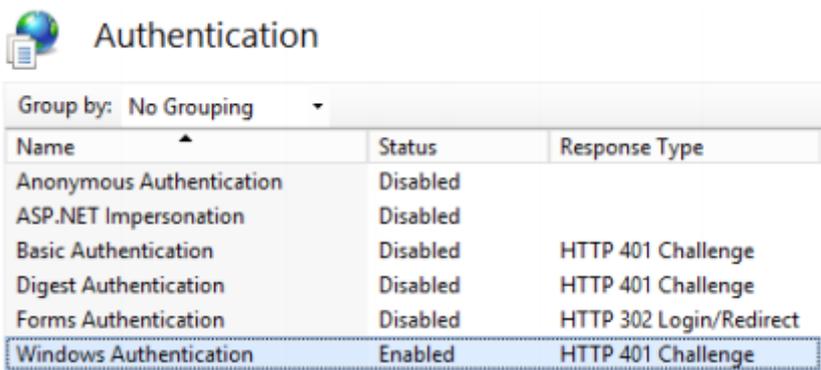
Значение данного ключа содержит / и Alias, заданный для приложения. В нашем случае Winauth. Функция данного ключа – непосредственно windows-авторизация в системе в случае, когда система настроена для доступа извне и изнутри локальной сети, при этом windows-авторизация при доступе извне невозможна.

```
<add key="LDAPAuthentication" value="true" />
```

Данный ключ отвечает за возможность авторизации в системе по доменным логину и паролю через форму авторизации самой системы (в данном случае доменный логин указывается без домена). После выхода из системы пользователь сможет авторизоваться как через сквозную авторизацию, так и введя доменный логин с паролем.

5. Аналогично с описанным выше в пункте 3 случае, необходимо указать URL-адреса для авторизации посредством **Single Sign On**

6. Для приложения Winauth отключить анонимную аутентификацию и включить аутентификацию Windows



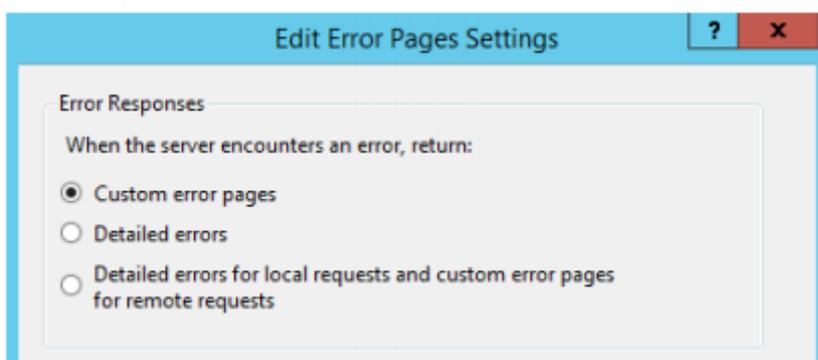
Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

7. Для сайта же, напротив, выключить аутентификацию Windows и включить анонимную аутентификацию


Authentication

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

8. Для приложения Winauth включить настраиваемые страницы ошибок. Выбрать приложение Winauth, дважды кликнуть по разделу **Error Pages**, выбрать Edit feature settings и установить значение, как показано ниже



После того, как выполнены все описанные выше настройки, авторизация в системе должна работать следующим образом:

- Single Sign On при обращении к системе по адресу <http://helpdesk> из локальной сети
- Анонимно путем ввода логина и пароля на форме авторизации при обращении к системе извне по адресу <http://helpdesk.company.local>

НАСТРОЙКА СЛУЖБЫ INTRASERVICE AGENT

Intraservice Agent – отдельная windows-служба, поставляемая вместе с дистрибутивом системы.

Предназначена для выполнения автоматизированных операций системы, таких как:

- Импорт писем из почтовых ящиков и создание заявок/добавление комментариев по email
- Отправка email, sms и push-уведомлений



- Регулярная синхронизация системы с Active Directory
- Проверка заявок на предмет истечения сроков реакции/выполнения и простановка соответствующих атрибутов для заявок
- Обслуживание системных таблиц: очистка таблицы уведомлений и логов с заданной периодичностью; удаление писем, не привязанных к заявкам с заданной периодичностью
- Автоматические переводы статусов заявок
- Эскалация заявок (фактические и превентивные уведомления)
- Рассылка данных по подпискам на шаблоны фильтров и результатов отчетов

Чтобы установить службу, необходимо запустить установочный файл **C:\Program Files\Print-X\web\iservice\IntraService Agent.msi** и выполнить ряд настроек.

Установка службы должна выполняться от имени учетной записи, имеющей полномочия на установку windows-служб на сервере. Например, от имени Администратора сервера или администратора домена.

1. Настроить запуск службы от имени доменной учетной записи DOMAIN\Intraservice. Запустить оснастку Services. Нажать комбинацию клавиш Win+R, ввести services.msc и нажать OK
2. В списке служб найти службу **Intraservice Agent**, кликнуть правой кнопкой, выбрать **Properties** и перейти на вкладку **Log On**
3. Изменить учетную запись по умолчанию, выбрав **This account** и указав учетную запись DOMAIN\Intraservice, далее ввести пароль от учетной записи и нажать OK. Службу пока запускать не нужно.
4. Настроить подключение службы к базе данных системы. Открыть конфигурационный файл **IntraService.Agent.Service.exe.config**, расположенный в каталоге, куда была установлена служба. Найти секцию **connectionStrings** и после **<clear />** вставить строку подключения, скопировав ее из файла **web.config**.

Выглядеть должно следующим образом:

```
<connectionStrings>
```

```
<clear />
```

```
    <add name="IntraServiceConnectionString" connectionString="Data  
Source=DB_server;Initial Catalog=IntraService;Integrated Security=True;"  
providerName="System.Data.SqlClient" />  
</connectionStrings>
```

5. Сохраните конфигурационный файл и запустите службу. Если служба запустилась и система не выдала сообщений об ошибках, то все настроено правильно.

Intraservice Agent может быть настроен на работу с несколькими базами данных одинаковых версий. Для этого необходимо добавить нужное количество "connection strings" с нужными параметрами и с разными значениями ключа **name**



При установке службы также автоматически создается одноименная ветка в **EventLog Windows** в разделе **Application and Services logs**, куда пишутся сообщения об ошибках в работе службы:

- таймауты
- подключения к БД, отсутствие доступа к БД, состояния службы, диагностическая информация в случае работы службы в режиме debug.

Кроме того, если служба по каким-то причинам не запускается (при попытке запуска службы возникает сообщение о невозможности запуска либо о том, что служба была запущена и сразу же остановлена, необходимо поискать сообщения об ошибках в **EventLog** в разделе **Windows Logs / Application**

НАСТРОЙКА ПЕРИОДА ОБСЛУЖИВАНИЯ

Все процедуры по обслуживанию базы данных (очистка таблиц логов, уведомлений, файлов и писем) выполняются службой внутри установленного сервисного интервала. На примере ниже сервисные операции будут выполняться в период с 22:00 до 05:00:

```
<!--Период времени, в который производится очистка таблиц (серверное время). Указывается как hh1:mm1-hh2:mm2, где hh1, mm1 - часы и минуты начала, hh2, mm2 - часы и минуты конца-->
```

```
<add key="ServiceMaintenancePeriod" value="22:00-05:00" />
```

НАСТРОЙКА АВТОМАТИЧЕСКОГО ПЕРЕВОДА СТАТУСОВ

Операция выполняется службой автоматически с заданной в конфигурационном файле периодичностью

```
<!--Время в секундах, через которое сервис пытается автоматически изменить статус заявки при соответствующих настройках сервиса (если 0, то отключено) [600]-->
```

```
<add key="AutomaticStatusChange_Time" value="600" />
```

НАСТРОЙКА СЛЕЖЕНИЯ ЗА ВРЕМЕНЕМ РЕАКЦИИ И ВЫПОЛНЕНИЯ

Операция выполняется службой автоматически с заданной в конфигурационном файле периодичностью

```
<!--Время в минутах, через которое сервис проверяет время реакции и время исполнения и генерирует
```

```
для них уведомления, либо корректирует дату. При значении 0 отключено [2]-->
```

```
<add key="SendReactionAndResolutionNotification_Time" value="2" />
```

НАСТРОЙКА АВТОМАТИЧЕСКИХ ПЕРЕВОДОВ СТАТУСОВ



Операция выполняется службой автоматически с заданной в конфигурационном файле периодичностью

<!--Время в секундах, через которое сервис пытается автоматически изменить статус заявки при соответствующих настройках сервиса (если 0, то отключено) [600]-->

<add key="AutomaticStatusChange_Time" value="600" />

НАСТРОЙКА АВТОМАТИЧЕСКОЙ ЭСКАЛАЦИИ ЗАЯВОК

Операция выполняется службой автоматически с заданной в конфигурационном файле периодичностью

<!--Время в минутах, через которое сервис запускает автоматическую эскалацию по созданным правилам. При значении 0 отключено [2]-->

<add key="CheckAutomaticEscalation_Time" value="2" />

НАСТРОЙКА АВТОМАТИЧЕСКОЙ ОЧИСТКИ ЛОГОВ И УВЕДОМЛЕНИЙ

Операции выполняются службой автоматически с заданной в конфигурационном файле периодичностью

Логи:

<!--Время в днях, соответствующее периодичности запуска очистки таблицы системного лога (т.е. куда пишет данный сервис). При значении 0 не запускается [2]-->

<add key="ClearLogTime" value="2" />

<!--Удалять данные если лог файла старше n дней [7]-->

<add key="ClearLogOlder" value="7" />

Уведомления:

<!--Время в днях, соответствующее периодичности запуска очистки таблицы уведомлений(в том числе и Push) (при значении 0 не запускается) [2]-->

<add key="ClearNotificationTime" value="2" />

<!--Удалять уведомления старше n дней [7] (в том числе и Push)-->

<add key="ClearNotificationsOlder" value="7" />

НАСТРОЙКА УДАЛЕНИЯ ПИСЕМ

<!--Время в днях, соответствующее периодичности запуска очистки таблицы импортированных писем. Удаляются только те письма, которые не связаны ни с какими заявками. При значении 0 не запускается [5]-->

```
<add key="ClearImportMailsTime" value="5" />
```

<!--Удалять данные, если письмо старше n дней [7]-->

```
<add key="ClearImportMailsOrder" value="7" />
```

НАСТРОЙКА УДАЛЕНИЯ ФАЙЛОВ

<!--Время в днях, периодичность запуска очистки таблицы TaskFile от непривязанных к заявкам файлов [1]-->

```
<add key="ClearTaskFileTime" value="1" />
```

<!--Удалять непривязанные к заявкам файлы старше n дней [3]-->

```
<add key="ClearTaskFileOlder" value="3" />
```

НАСТРОЙКИ ДЛЯ ОТПРАВКИ PUSH-УВЕДОМЛЕНИЙ

Для обеспечения функционала отправки push-уведомлений на мобильные устройства пользователей системы должны выполняться следующие требования:

- В системе должен быть подключен модуль API
- В профиле пользователя в системе должны быть привязаны мобильные устройства, на которых используется мобильное приложение Intraservice. Привязка устройства осуществляется в момент первого входа пользователем в систему через мобильное приложение, в этот момент фиксируется токен устройства
- Сервер, на котором установлена служба Intraservice Agent, которая отправляет уведомления, должен иметь выход в интернет для доступа к сервисам Apple и Google. Или же, как минимум, должен быть доступ с сервера наружу по портам: 443, 2195, 2196, 5223, 5228, 5229, 5230, 8080

АВТОМАТИЧЕСКОЕ СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ ПРИ ПЕРВОМ ВХОДЕ В СИСТЕМУ

Доменный пользователь при первом входе в систему может автоматически получать учетную запись в системе по ряду правил, определенных через веб-интерфейсе систем в разделе **Настройки / Синхронизация с Active Directory**. Для работы данного функционала необходимо настроить правила через интерфейс с помощью мастера настройки LDAP-профилей (отдельная документация доступна в разделе Синхронизация с Active Directory) и дождаться, либо произвести вручную первичную синхронизацию с доменом.

Если настроены профили синхронизации с доменом, произведена первичная синхронизация данных из домена и входящий в систему первый раз пользователь авторизован в домене и читается по одному из созданных LDAP-профилей, то пользователь будет автоматически создан в системе и привязан к тому подразделению, которое соответствует его LDAP -профилю.

НАСТРОЙКА СОЗДАНИЯ ПОДПИСОК НА ФИЛЬТРЫ И ОТЧЕТЫ

Для настройки данного функционала необходимо указать в настройках Путь к системе, для авторизации через веб-интерфейс. Указывается URL, по которому система доступа через браузер.

Раздел Настройки / Общие настройки / Константы / Путь к системе

В случае, если для системы настроена авторизация **Single Sign On**, то помимо указания пути к системе необходимо внести изменения в конфигурационный файл службы **Intraservice Agent**

1. Откройте конфигурационный файл и найдите группу параметров

```
<add key="useAD" value="false" />
<add key="domain" value="domain" />
<add key="username" value="username" />
<add key="password" value="password" />
```

2. Скорректируйте значения, указав реквизиты доменной учетной записи для прохождения службой windows-авторизации на веб-сервере.

Например, для текущего случая:

```
<add key="useAD" value="True" />
<add key="domain" value="domain" />
<add key="username" value="intraservice" />
<add key="password" value="password" />
```

Domain, username, password – реквизиты созданной ранее учетной записи DOMAIN\Intraservice

Сохраните файл и перезапустите службу

НАСТРОЙКА ОТПРАВКИ EMAIL-УВЕДОМЛЕНИЙ

Операция выполняется службой автоматически с заданной в конфигурационном файле периодичностью

```
<!--Время в секундах, через которое сервис отправляет уведомления (если 0, то отключено) [60]->
```

```
<add key="SendNotifications_Time" value="60" />
```

Чтобы настроить отправку email-уведомлений выполните следующие действия через веб-интерфейс системы:

1. Зайдите в меню **Настройки / SMTP/SMS шлюз**
2. Настройте SMTP, указав необходимые данные для подключения к почтовому серверу и



выбрав, при необходимости, алгоритм шифрования.

- a) По умолчанию при авторизации без шифрования SSL, TLS, STARTTLS используется порт 25.
- b) SSL – нужно указать порт 587
- c) TLS / STARTTLS – нужно указать порт 465
- d) IMAP – порт 993

3. При необходимости, проверить корректность настройки SMTP нажатием кнопки **Проверить**, где будет предложено отправить тестовое сообщение на введенный адрес.

НАСТРОЙКА СОЗДАНИЯ ЗАЯВОК ПО EMAIL

Операция выполняется службой автоматически с заданной в конфигурационном файле периодичностью. Перейдите в каталог **C:\Program Files (x86)\Intravision\IntraService Agent** (точное название каталога зависит от версии агента) в файловой структуре сервера, откройте конфигурационный файл **IntraService.Agent.Service.exe.config**

Следующий параметр отвечает за период обработки почтовых сообщений:

`<!--Время в секундах, характеризующее частоту проверки почтовых ящиков [60]-->`

`<add key="UpdateTime" value="60" />`

Чтобы настроить создание заявок по email, выполните следующие действия через веб-интерфейс системы:

1. В разделе **Настройки / Импорт заявок** создайте новый почтовый аккаунт:

a) **Название аккаунта** – отображаемое название профиля (From Yandex). Установите галочку «Заявки по письму».

b) **Сервер** – адрес mail-сервера (для тестирования: imap.yandex.ru);

c) **Порт** – порт подключения к mail серверу. 110 для POP3 и 143 для IMAP по умолчанию без шифрования. При использовании шифрования SSL, TLS, STARTTLS нужно указывать соответствующий порт, в зависимости от алгоритма шифрования и типа почтового сервера.

Например, SSL/TLS для IMAP – 993 (для тестирования через imap.yandex.ru указываем порт 993).

d) **Тип** - тип сервера. Pop3/IMAP (для тестирования: IMAP, тип авторизации – SSL, тип аутентификации – Обычный пароль)

e) **Логин** - логин для входа на mail сервер (уточните точный логин, иногда требуется вводить с @домен.зона) (для тестирования: printxtest);

f) **Пароль** - пароль для доступа к почтовому ящику (для тестирования: mkHTS6t3NaeUY6N555);



g) **Сервис** – сервис, в котором будут создаваться заявки с этого почтового ящика (для тестирования: Сервис 1, Тип заявки – Заявка от принтера);

h) **Статус** – статус, в котором будут создаваться все новые заявки по письмам для этого ящика.

i) **Создавать заявки от незарегистрированных пользователей** – опция, позволяющая принимать заявки по email не только от тех, кто уже заведен в систему, но и от обратившихся впервые. Может быть настроена автоматическая привязка таких пользователей к подразделению по домену отправителя или же привязка в одно конкретное подразделение. (для тестирования необходимо установить и указать пользователем по умолчанию Администратора)

Загруженные письма хранятся в таблице ImportMails в базе данных системы. Обработанное письмо в таблице имеет следующие статусы:

- Статус 15. По письму создана заявка
- Статус 18. По письму добавлен комментарий
- Статус 7. Письмо обработано, но не создана заявка, не добавлен комментарий

Лог обработки входящей почты (создание заявок по письму) также записывается в базу данных и доступен в системе в разделе Настройки / Системный лог.

Настройка Print-X Модуль печати

Важно: Подробное руководство по настройке содержится в Руководстве администратора системы Print-X.

Для настройки Print-X. Модуль печати необходимо проделать следующие шаги:

1. Открыть интерфейс администратора по адресу <http://localhost:8080> и авторизоваться в интерфейсе с учетной записью ***admin** и паролем, указанным в процессе предварительной настройки при помощи **Easy Config**.
2. Указать E-mail администратора.
3. Настроить часовой пояс.
4. Указать информацию о Заказчике.
5. Получить и установить лицензии.
6. Настроить исходящий SMTP-сервер.
7. Настроить сервер проверки подлинности.
8. Синхронизировать пользователей Active Directory (достаточно добавить только Base DN).
9. Настроить очереди.
10. Добавить, активировать и настроить принтеры.
11. Настроить в разделе «Уведомления о событии» действия при возникновении событий. Необходимо настроить отправку электронной почты при возникновении каждого из событий в списке «Событие». Параметры настройки:
 - Получатель: printxtest@yandex.ru
 - Тема: в соответствии с наименованием события
 - Сообщение: описание возникшей проблемы с перечислением всех передаваемых параметров в строгой последовательности и разделенных точкой с запятой. Обращаем внимание, что параметры в подсказке разделены только запятой. Пример сообщения:

⚙️ Действие события: Все принтеры

Включено:

Событие: Cover open or Paper jam

Действие: Отправить эл. почту

Задержка: * 0 минуты

Повторение: * 0

Получатель: * printxtest@yandex.ru
 Параметры: %PRINTER_CONTACT%

Тема: * Cover open or Paper jam

Сообщение: * У принтера открыта крышка или произошло замятие бумаги.
 ====
 {PRN.IP_ADDRESS};{PRN.NAME};{PRN.SERIAL_NUMBER};{PRN.MODEL};{PRN.LOCATION};{PRN.PRINTER_MONO};
 {PRN.PRINTER_COLOR};{PRN.COPIER_MONO};{PRN.COPIER_COLOR};{PRN.SCANNER};{SUPPLY.INFO};{ALERT.CODE};
 {ALERT.SEVERITY};{ALERT.TRAINING};{ALERT.ALERTGROUP};{ALERT.TIME}

Параметры: {PRN.IP_ADDRESS}, {PRN.NAME}, {PRN.SERIAL_NUMBER}, {PRN.MODEL}, {PRN.LOCATION}, {PRN.PRINTER_MONO},
 {PRN.PRINTER_COLOR}, {PRN.COPIER_MONO}, {PRN.COPIER_COLOR}, {PRN.SCANNER}, {SUPPLY.INFO}, {ALERT.CODE},
 {ALERT.SEVERITY}, {ALERT.TRAINING}, {ALERT.ALERTGROUP}, {ALERT.TIME}

Настройка Print-X Панель состояния

Производим настройку Панели состояний. Для этого необходимо:

1. Открыть в любом текстовом редакторе файл C:\Program Files\Print-X\Apache\conf\httpd.conf
2. После строки Listen 0.0.0.0:8090 добавить строку:
Listen 0.0.0.0:8081
3. После последней закрывающей директивы </VirtualHost> добавить строки:
<VirtualHost *:8081>
ServerName DNS-имя сервера
DocumentRoot "C:/Program Files/Print-X/web/spanel/public_html"
DirectoryIndex index.php
</VirtualHost>
<Directory "C:/Program Files/Print-X/web/spanel/public_html">
AddOutputFilterByType DEFLATE text/html
AddOutputFilterByType DEFLATE text/css
AddOutputFilterByType DEFLATE application/x-javascript
AddOutputFilterByType DEFLATE application/javascript
Options FollowSymLinks ExecCGI
</Directory>

В качестве параметра **ServerName** необходимо указать DNS-имя сервера с установленным Print-X.



Важно: После того, как **Print-X Модуль печати** сконфигурирован, имя сервера будет указано в качестве `ServerName` внутри других секций `<VirtualHost>`

4. В разделе «Настройки: Внешние системы» **Модуля печати:**

- в общих настройках необходимо найти пункт «Внешние системы»
- добавить новую внешнюю систему
- ввести название (любое), в поле «Рамки» необходимо указать "printers". ID клиента и секретный ключ создадутся автоматически
- ID клиента сохранить в конфигурационный файл `C:\Program Files\Print-X\web\spanel\protected\config\main.php`

myQServerUrl – url подключения к API **Модуля печати**, должен быть обязательно `https` для корректной работы `oauth2`

myQGrantType – без изменений

myQOAuthClient - ID клиента

myQOAuthSecret - секретный ключ

SDServerUrl - url подключения к API **Модуля управления заявками**

SDServerUsername – имя пользователя для авторизации в **Модуле управления заявками**

SDServerPassword – пароль для авторизации в **Модуле управления заявками**

5. Перезапустить сервис Apache.

Доступ к Панели состояний осуществляется по адресу <http://localhost:8081>