INTRASERVICE. РУКОВОДСТВО ПО УСТАНОВКЕ

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данный документ представляет собой руководство системного администратора по установке программного продукта Intraservice. 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.

ТРЕБОВАНИЯ К СЕРВЕРНОЙ ПЛОЩАДКЕ И РАБОЧЕМУ МЕСТУ ПОЛЬЗОВАТЕЛЯ

МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ

1 сервер для WEB и SQL

Intel Core i3 и выше, 8+ GB RAM, 100 GB HDD

MS Windows Server 2012 и выше, MS SQL Server 2012 и выше с поддержкой полнотекстовой индексации (Full-text Search) для русского языка, IIS 8 и выше, MS .NET Framework 4.5.1 и выше.

Возможно использование MS SQL Server Express, но для поддержки Full text Search необходима редакция SQL Server with Advanced Services. Также при использовании MS SQL Server Express будут накладываться следующие ограничения (на примере MS SQL 2012 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

РЕКОМЕНДУЕМЫЕ ТРЕБОВАНИЯ

2 сервера: 1 для WEB и 1 для SQL.

Для WEB:

Intel Core i5 и выше, 8+ GB RAM, 100 GB HDD

MS Windows Server 2012 64 bit и выше, IIS 8 и выше, MS .NET Framework 4.5.1 и выше

Windows Server должен иметь следующие роли:

Web server с включенным WebSocket Protocol, Application Server, Web server (IIS) Support

Для SQL:

Intel Core i5 и выше, 8+ GB RAM, 250 GB HDD

MS Windows Server 2012 64 bit и выше, MS SQL Server 2012 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. При использовании MS SQL Server Express ограничения аналогичны описанным выше.

> ***Важно:*** *при настройке с двумя различными серверами для web и sql на обоих серверах должен быть установлен один и тот же часовой пояс. Например,* ***(UTC +3:00) Волгоград, Москва, Санкт-Петербург (RTZ 2)***

ТРЕБОВАНИЯ К РАБОЧЕМУ МЕСТУ ПОЛЬЗОВАТЕЛЯ

Рабочее место пользователя должно быть оборудовано любым современным браузером (Microsoft Internet Explorer 9+ (Internet Explorer 11 для администратора или пользователя с доступом на редактирование статей в Базе Знаний), Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, Safari) и подключено к интернету (или к локальной сети, если система используется локально) со скоростью не менее 512 Кбит/сек.

СОВМЕСТИМОСТЬ С БОЛЕЕ РАННИМИ ВЕРСИЯМИ СИСТЕМЫ INTRASERVICE

Текущие версии системы совместимы с ранними версиями системы только в рамках текущей ветки релиза. Например, версия 4.1 совместима с версией 4.45 и может быть обновлена до указанной версии. Если же у вас используется более старая версия, например, релиз 3.XX или 2.XX, то эти версии несовместимы с актуальными и могут использоваться только раздельно при соответствующей настройке веб-сервера.

ПОРЯДОК УСТАНОВКИ СИСТЕМЫ

Для установки системы необходимо:

1. Подготовить учетную запись для запуска веб-приложения (опционально)
2. Восстановить чистую базу данных из бэкапа, настроить права доступа к базе данных
3. Скопировать файлы приложения в выбранный каталог, настроить приложение на веб-сервере IIS
4. Настроить дополнительные сервисы: отправку почтовых и/или sms-уведомлений, интеграцию с ActiveDirectory, LDAP авторизацию, создание заявок по email и другие.

УСТАНОВКА СИСТЕМЫ

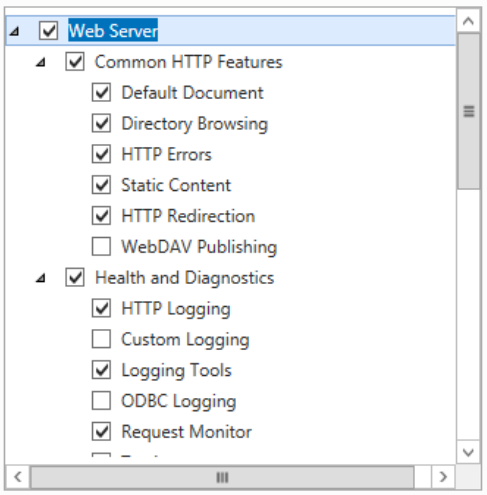
Ниже будет описан процесс установки системы на примере чистых серверов на базе MS Windows Server 2012 R2/2016, находящихся в домене и MS SQL Server 2012 / MS SQL Management Studio 2012 с англоязычным интерфейсом.

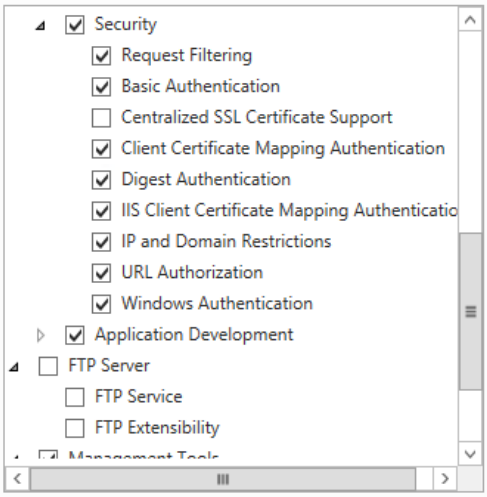
ПОДГОТОВКА ВЕБ-СЕРВЕРА

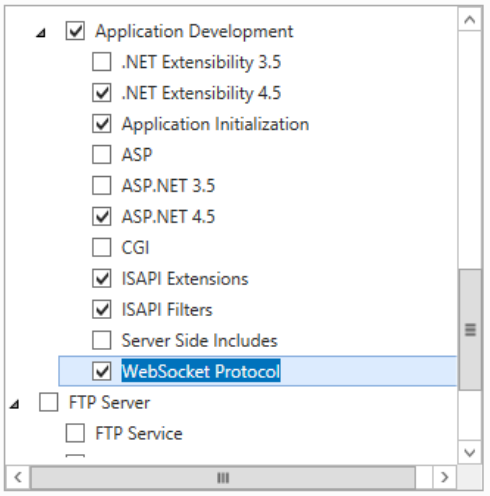
Для установки системы необходимо подготовить web-server, установив необходимые роли и компоненты сервера. Ниже приведены примеры настройки ролей и компонентов для Windows Server 2012 R2 и Windows Server 2016

ДЛЯ WINDOWS 2012

1. Запустите **Server Manager** либо с панели задач, либо, нажав Win+R, введите **servermanager** и нажмите **OK**
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** должны быть выбраны компоненты по умолчанию. Если это не так, то установите как показано на скриншотах ниже:





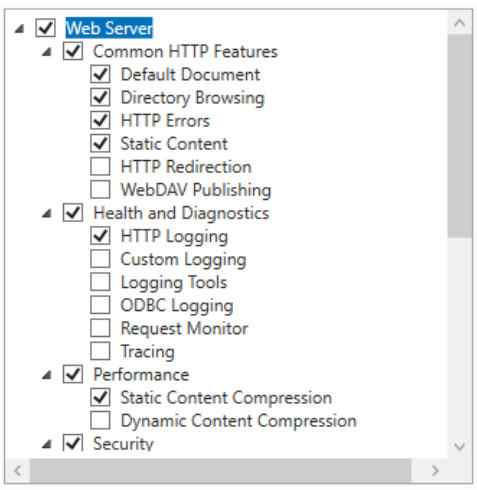


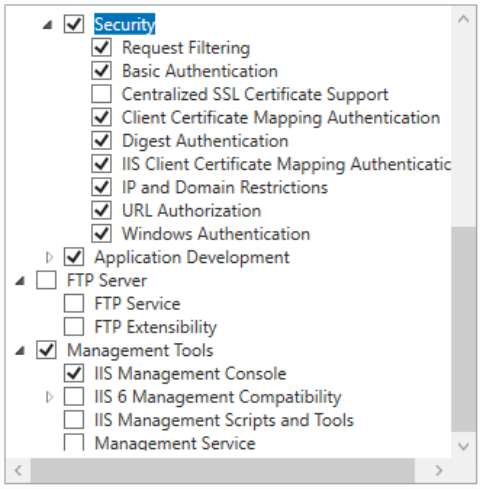
Здесь же установите **Management tools / IIS Management Console**, нажмите **Next**

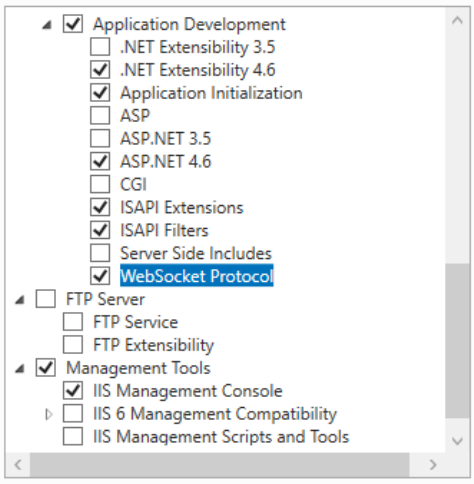
8. На следующем экране **Confirmation** нажмите **Install** и дождитесь сообщения об окончании установки, после перезагрузите сервер для корректного применения изменений.

ДЛЯ WINDOWS 2016

1. Запустите **Server Manager** либо с панели задач, либо, нажав Win+R, введите **servermanager** и нажмите **OK**
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 **Web server (IIS)** (в открывшемся окне нажмите **Add features**), нажмите **Next**
5. В разделе **Features** выберите **.NET Framework 4.6 Features** с компонентами по умолчанию, нажмите **Next**, **Next**
6. В разделе **Web server role (IIS) / Role services** должны быть выбраны компоненты по умолчанию. Если это не так, то установите как показано на скриншотах ниже:







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

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

ПОДГОТОВКА УЧЕТНОЙ ЗАПИСИ ДЛЯ ЗАПУСКА САЙТА

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 (см. раздел Рекомендуемые требования)

> ***Важно:*** *в случае, если планируется запуск пула приложений от локальной учетной записи сервера или от доменной учетной записи, то конкретная учетная запись должна иметь полномочия* ***Log on as batch job (пакетный вход)*** *на сервере.*

Далее будет описан процесс установки системы на 2 раздельных сервера для приложения и базы данных с запуском приложения от имени доменной учетной записи и подключением к БД от ее имени.

Соответственно, необходимо создать в домене учетную запись, например, **DOMAIN\Intraservice** 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 и добавьте учетную запись **DOMAIN\Intraservice** на вкладке **Local security settings**, 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

Results | Messages

	configuration_id	name	value	minimum	maximum	value_in_use	description	is_dynamic	is_advanced
1	1562	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.

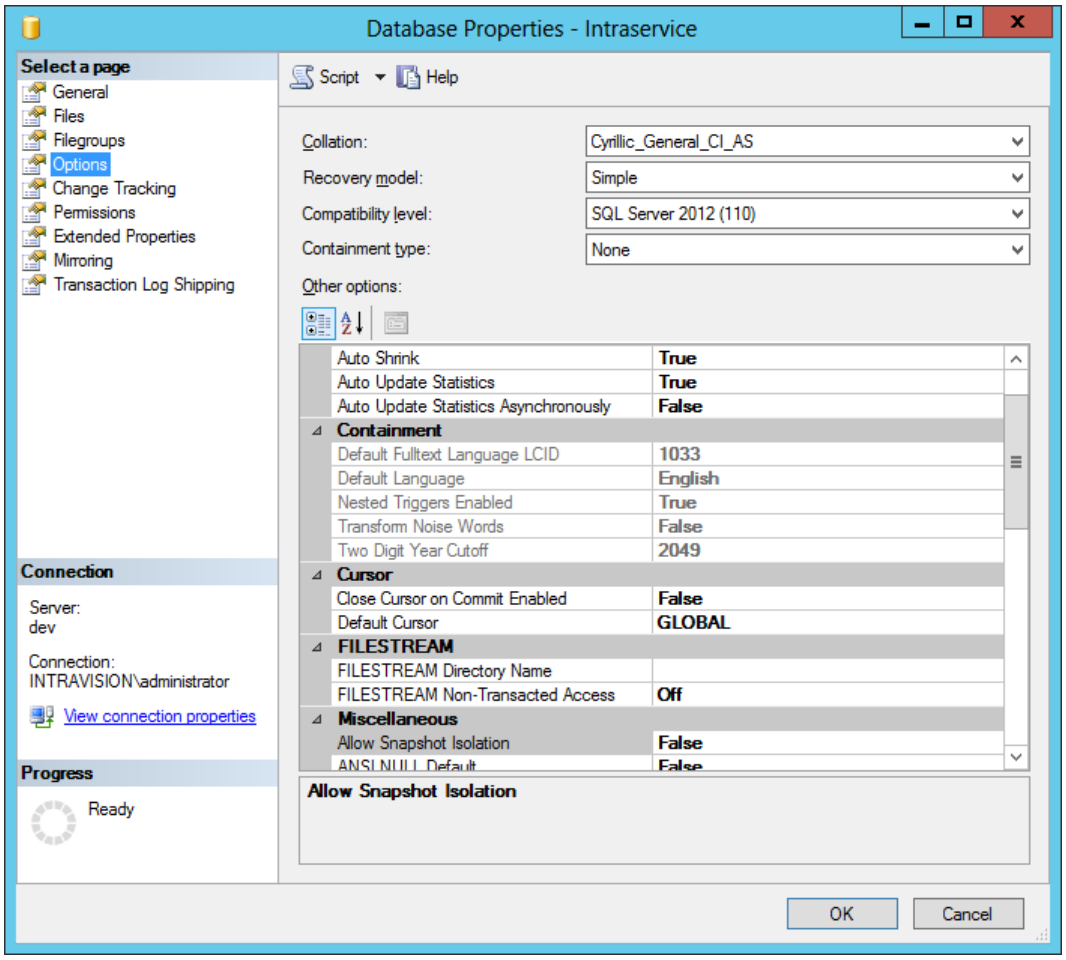
> ***Важно:*** *Выполнение данных операций необходимо производить от имени учетной записи, имеющей полномочия системного администратора на сервере баз данных (роль **sysadmin**)*

ВОССТАНОВЛЕНИЕ БАЗЫ ДАННЫХ ИЗ БЭКАПА

1. На сервере БД запустите MS SQL Management Studio и подключитесь к нужному серверу БД под учетной записью, обладающей ролью sysadmin на сервере БД

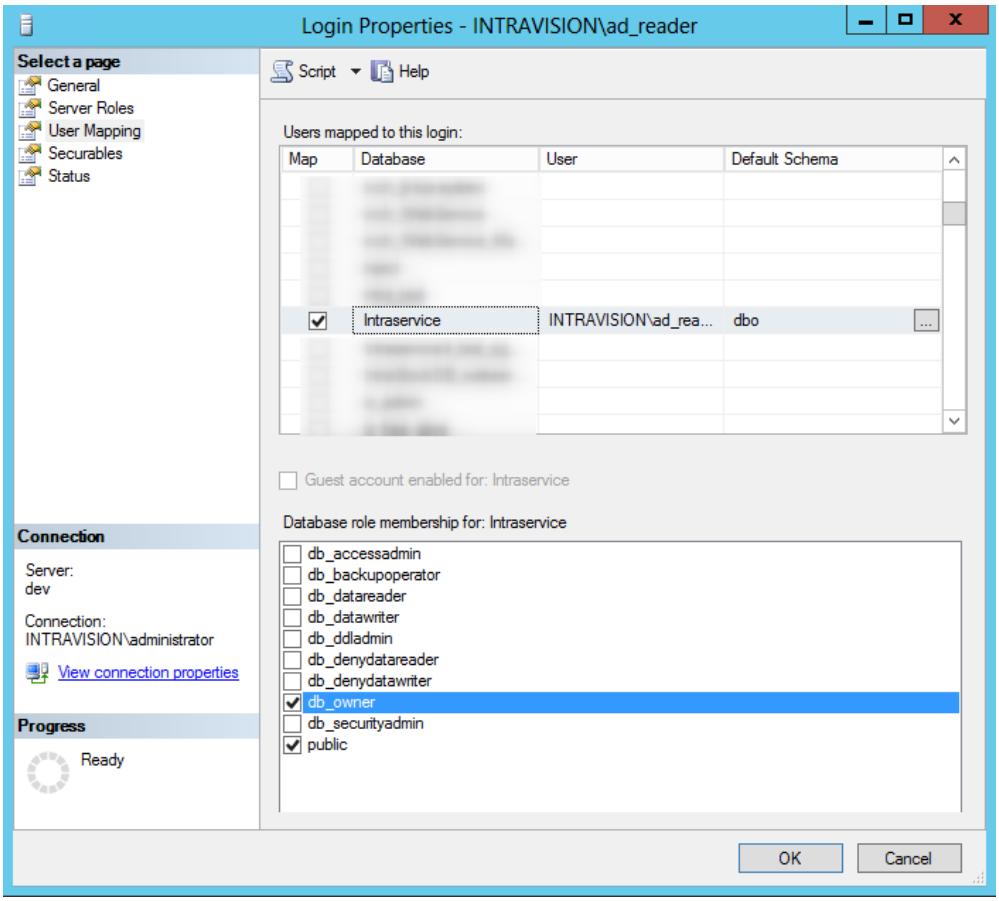
2. Правой кнопкой кликните по каталогу **Databases** и в выпадающем меню выберите **Restore files and filegroups**
3. В открывшемся окне укажите **Intraservice** в качестве имени будущей базы данных в поле **To database**, затем установите переключатель **Source for restore** в положение **From device**, в открывшемся окне **Select backup devices** выберите файл бэкапа, нажав кнопку **Add** и выберите на диске файл бэкапа базы данных. Файл должен быть предварительно скопирован на сервер БД, на котором выполняется развертывание базы данных. 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 содержимое каталога **Databases**, найдите базу **Intraservice**, кликните по ней правой кнопкой мыши и выберите пункт **Properties** в выпадающем меню.
6. В окне **database properties** выберите раздел Options и установите для базы данных следующие параметры:

a. **Recovery model:** Simple
b. **Compatibility level:** 2012 (2014 или 2016 если БД развернута на MS SQL Server 2014 или 2016 соответственно)
c. **Auto shrink:** True
d. **Collation:** Cyrillic_General_CI_AS (по умолчанию обычно так)



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** и найдите созданную ранее учетную запись **DOMAIN\Intraservice**, 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 **Intraservice**, отметьте ее чекбоксом и ниже в поле **Database membership for:** установите чекбокс **db_owner** и нажмите **OK**



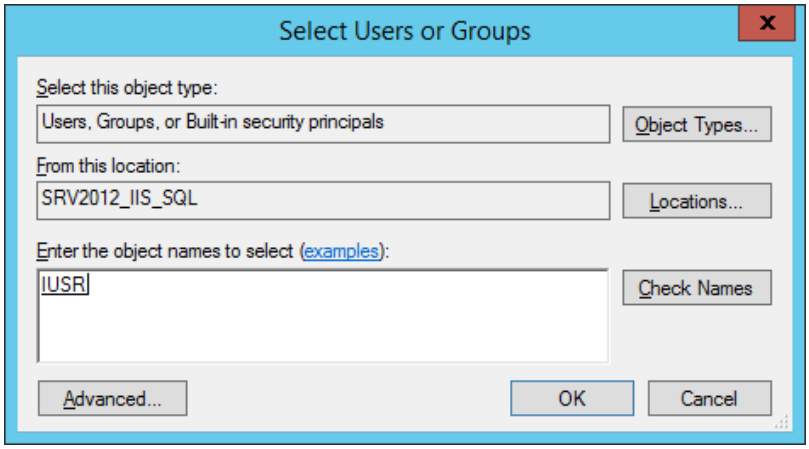
НАСТРОЙКА САЙТА НА ВЕБ-СЕРВЕРЕ

СОЗДАНИЕ И НАСТРОЙКА САЙТА В КОНСОЛИ IIS

1. Создайте каталог **Intraservice** в файловой структуре веб-сервера. Скопируйте в этот каталог содержимое каталога внутри zip-архива, поставляемого с дистрибутивом ПО. Как правило, такой архив в дистрибутиве всего один и содержит именно файлы приложения для развертывания сайта на веб-сервере IIS.

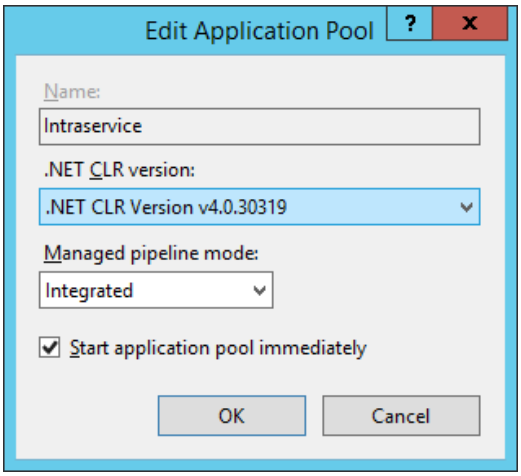
2. Для созданной ранее учетной записи **DOMAIN\Intraservice** настройте права с полномочиями **modify** и **write** на следующие каталоги:
   a. Каталог **Intraservice** с файлами для развертывания, созданный на предыдущем шаге

   > *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) Manage**r. В разделе **Connection** 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 для развертывания приложения. При необходимости, скорректируйте имя/адрес, по которому будет доступен сайт через веб-браузер.
   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** 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\Intrasrevice**. Для этого выберите пул приложений **Intraservice**, кликните правой кнопкой и выберите **Advanced settings**.
   Найдите секцию **Process model** и в ней **Identity**. Измените учетную запись пула приложений с **ApplicationPoolIdentity** на **DOMAIN\Intraservice**, введя логин и пароль в соответствующем окне в поле **Custom Account**.
   Нажмите **OK**

> ***Важно:*** *в системе предусмотрен функционал одновременной работы над заявкой, 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 **Intraservice** 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 базу данных **IntraService**.
   Обычно параметр имеет примерный вид:

   <add name=IntraServiceConnectionString connectionString=Data Source=DB_server;Initial Catalog=Intraservice4;Integrated Security=True providerName=System.Data.SqlClient/>

2. Для настройки подключения сайта к базе данных, нужно отредактировать следующие параметры:
   a. **Data Source** – это имя/адрес SQL-сервера, нужно указать свой.
   b. **Initial Catalog** – это имя БД на SQL-сервере. Нужно указать свою, в нашем случае Intraservice
   c. **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=DB_server;Initial Catalog=Intraservice;User Id=sql_intraservice; password=пароль providerName=System.Data.SqlClient/>*

ПРОВЕРКА РАБОТОСПОСОБНОСТИ САЙТА

Для проверки правильности настройки сайта введите в строке браузера http://server_address/, где server_address - это имя или IP-адрес сервера с настроенным сайтом Intraservice. 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 самой системы. При этом, возможны два варианта использования такой системы:

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

Для таких случаев возможна настройка и для сквозной авторизации в системе из локальной сети, и для авторизации из вне используя одну физическую площадку на веб-сервере.

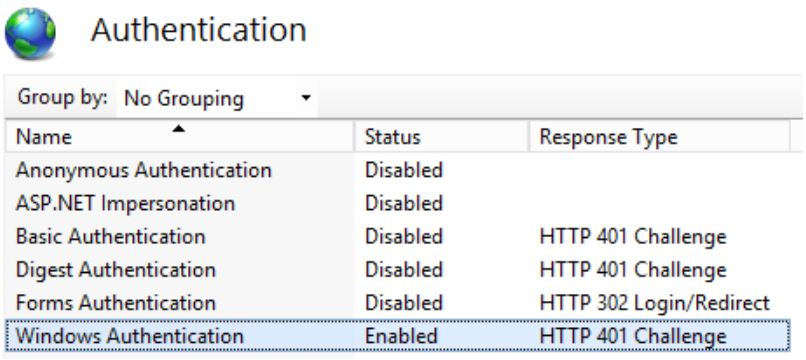
НАСТРОЙКА ДЛЯ РАБОТЫ ТОЛЬКО ИЗ ЛОКАЛЬНОЙ СЕТИ

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

- Логин пользователя в системе Intraservice должен полностью совпадать с его доменным логином. Например, в домене **DOMAIN** пользователь имеет логин **Ivan Petrov** и такой же логин должен иметь в системе Intraservice. 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 IntraService 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 сайт Intraservice и перейти в раздел **Authentication**. Отключить анонимную аутентификацию и включить Аутентификацию Windows:



2. Внести изменения в файл **web.config** сайта. Откройте каталог Intraservice 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 происходит 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 IntraService автоматически по указанным выше адресам, не вводя логин и пароль.

НАСТРОЙКА ДЛЯ РАБОТЫ ИЗ ЛОКАЛЬНОЙ СЕТИ И ИЗ ВНЕ

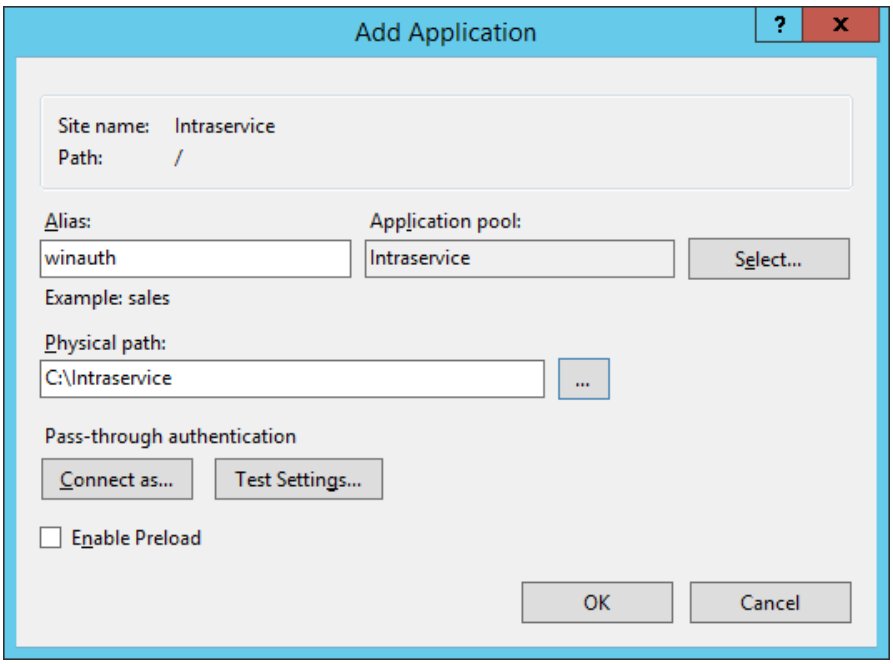
Данная настройка предполагает возможность работы с системой как внутренним сотрудникам, так и внешним подрядчикам, используя различные механизмы авторизации в системе (single sign on для внутренних сотрудников, работающих в локальной сети и авторизацию по логину и паролю в Intraservice для внешних сотрудников, работающих из вне 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 из вне (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 из вне необходимо произвести следующую настройку:

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

Например: для работы из локальной сети используем http://helpdesk/, для работы из вне – 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 по умолчанию.



4. Отредактировать **web.config** файл приложения. Открыть файл в каталоге Intraservice, ранее созданном при настройке сайта, найти и настроить следующие параметры:

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

Данный ключ отвечает непосредственно за возможность сквозной аутентификации Windows.

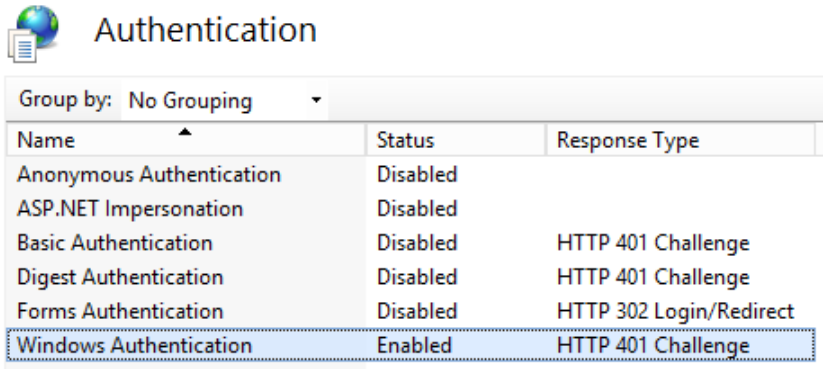
```
<add key="WindowsAuthenticationApplication" value="/winauth" />
```

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

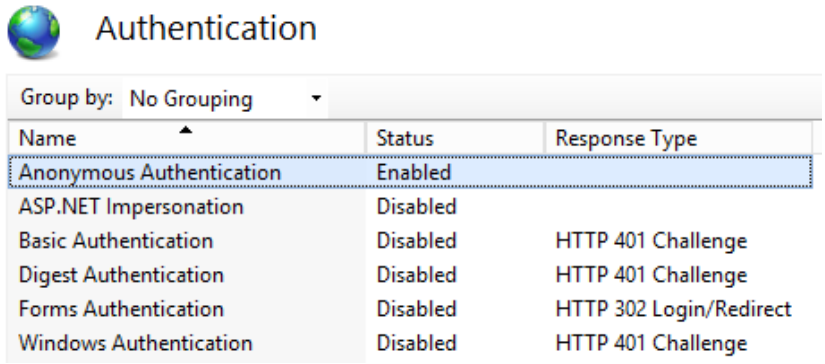
```
<add key="LDAPAuthentication" value="true" />
```

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.

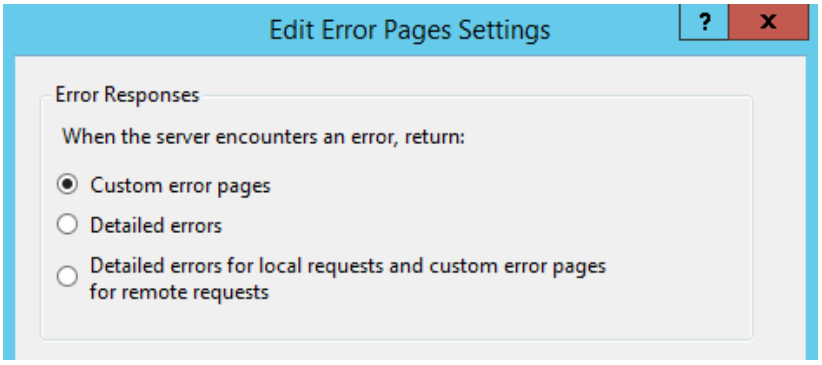
5. Аналогично с описанным выше случаем в пункте 3, необходимо указать URL-адреса для авторизации посредством Single Sign On
6. Для приложения **Winauth** отключить анонимную аутентификацию и включить аутентификацию Windows



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



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, должны 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 из вне 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, необходим запустить установочный файл из дистрибутива (как правило, это .msi-файл с названием **IntraService Agent_version.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 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** сайта.
   Выглядеть должно будет 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 соотвествующих 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 значенни 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

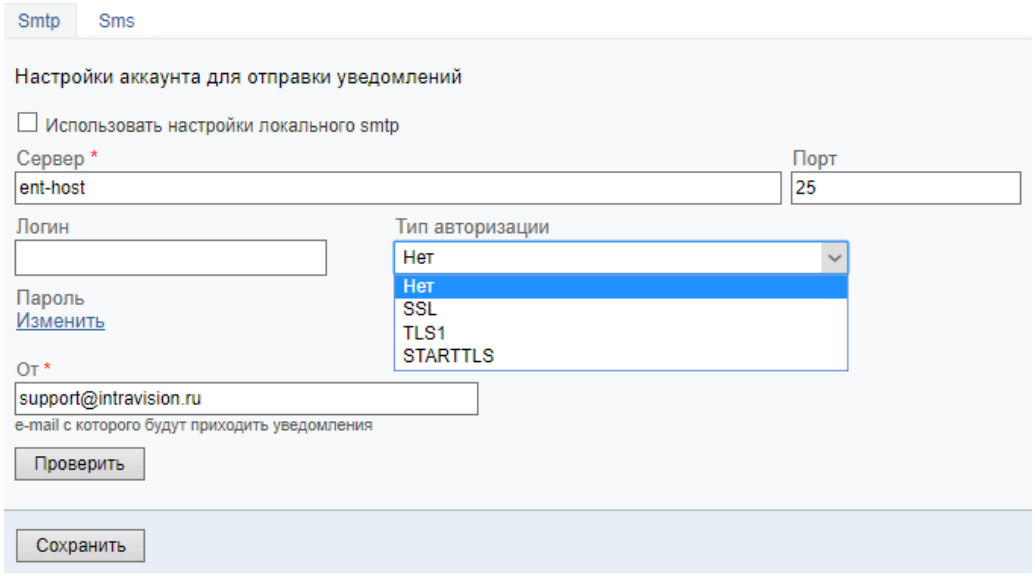
НАСТРОЙКА ОТПРАВКИ EMAIL-УВЕДОМЛЕНИЙ

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



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

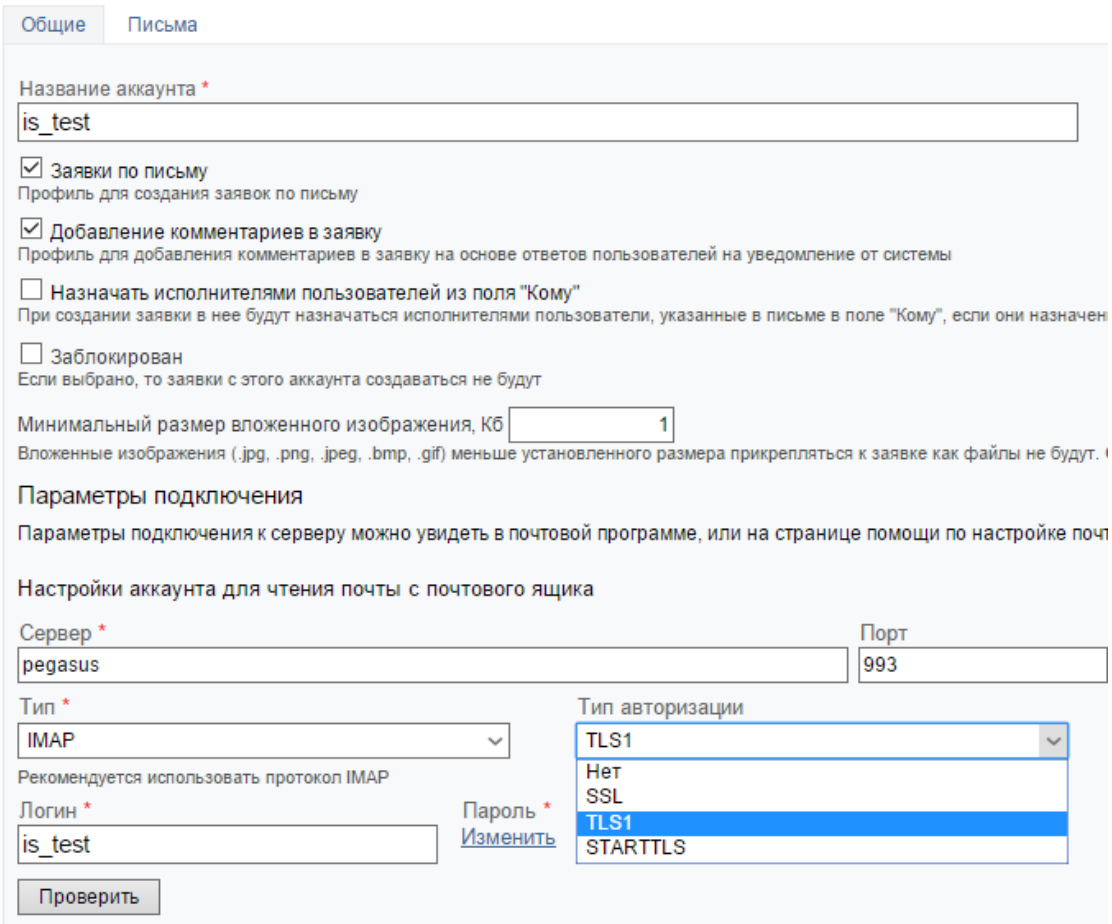
НАСТРОЙКА СОЗДАНИЯ ЗАЯВОК ПО EMAIL

Операция выполняется службой автоматически с заданной в конфигурационном файле периодичностью

```
<!--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 профиль (профили) для почтовых ящиков, с которых будут приниматься письма:



   a. Название аккаунта – отображаемое название профиля;

   b. Сервер – адрес mail-сервера;

   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.

   d. Тип - тип сервера. **Pop3/IMAP**

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

f. Пароль - пароль для доступа к почтовому ящику;

g. Сервис – сервис, в котором будут создаваться заявки с этого почтового ящика;

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.

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**.

API

В системе есть API, разработанное по стандартам REST. Документация доступна отдельно на сайте продукта в разделе «Поддержка»: https://intraservice.ru/support/

Доступ к API приобретается отдельно.

РУКОВОДСТВО ПО ОБСЛУЖИВАНИЮ

РЕКОМЕНДАЦИИ ПО РЕЗЕРВНОМУ КОПИРОВАНИЮ

Рекомендованные настройки резервного копирования зависят от наличия свободных дисковых мощностей и требований по надежности, но для простоты мы рекомендуем хранить 5 ежедневных бэкапов (например, выполняемых ночью в рабочие дни) и 3 ежемесячных (например, выполняемых 1 числа каждого месяца).

> *Мы настоятельно рекомендуем делать ручные бэкапы (как базы, так и файлов системы) при обновлении релизов системы, при выполнении любых скриптов на базе данных системы (в том числе и при удалении устаревших данных) и перед выполнением самостоятельных доработок системы.*

Процедура резервного копирования подробно описана в документации к MS SQL серверу: http://msdn.microsoft.com/en-us/library/ms175477.aspx.

Процедура восстановления системы из бэкапа аналогична действию при установке системы (см. выше). Бэкапы рекомендуется хранить на отдельных дисках.

УДАЛЕНИЕ СТАРЫХ ДАННЫХ

В ходе длительной и интенсивной эксплуатации системы объем данных по заявкам может привести к ухудшению производительности системы и к уменьшению объема свободного дискового пространства. Для решения этих проблем рекомендуется удалять устаревшие данные, предварительно сделав бэкап базы данных системы.

Мы рекомендуем в первую очередь пробовать удалять файлы к заявкам, так как основную часть размера базы данных системы составляют именно эти данные.

УДАЛЕНИЕ СТАРЫХ ФАЙЛОВ К ЗАЯВКАМ

Наибольший объем данных, скорее всего, будут занимать прикрепленные к заявкам файлы. Можно удалить только файлы (заявки по-прежнему будут доступны). Для удаления файлов необходимо выполнить хранимую процедуру на базе данных системы:

```
exec up_DeleteOldTaskFiles 'N'
```

Где **N** – количество дней. Данная команда удалит все прикрепленные к заявкам файлы, старше **N** дней от текущей даты. Сами заявки будут доступны в системе.

> ***Пример:*** *база данных нашей системы за 8 лет использования накопила порядка 110 000 заявок и имеет размер порядка 45 гигабайт. Для уменьшения размера базы данных мы приняли решение удалить все файлы к заявкам, старше 5 лет.*
>
> *Для этого мы запускаем вручную либо через планировщик заданий в MS SQL Management Studio следующий запрос-вызов указанной выше процедуры:*
>
> *exec up_DeleteOldTaskFiles '1825', где 1825 – количество дней в 5 годах.*

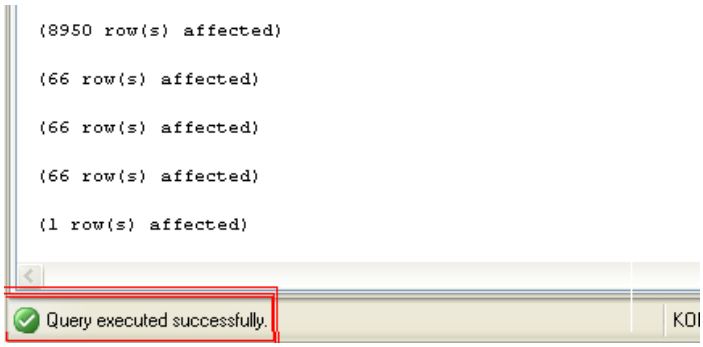
УДАЛЕНИЕ СТАРЫХ ЗАЯВОК

Для удаления старых заявок необходимо в MS SQL Management Studio выполнить специальную хранимую процедуру на базе данных системы с параметром:

```
exec up_DeleteOldTasks 'N'
```

Где **N** – количество дней. Данная команда удалит все заявки вместе с файлами и письма из раздела импорт заявок, по которым были созданы заявки старше **N** дней от текущей даты.

После выполнения команды вы должны увидеть сообщения как на скриншоте:



В противном случае просим прислать нам заявку по email на support@intraservice.ru с логом выполнения данной процедуры.

После выполнения команд удаления данных система может не сразу показать освободившееся место. Мы рекомендуем выполнить операцию **Shrink** на базе данных.

Если после выполнения операции Shrink размер базы данных не уменьшился, мы рекомендуем

выполнить для базы данных следующую команду:

backup log <имя базы> with truncate_only

и повторить операцию Shrink

Дополнительную экономию места на диске может дать перевод модели сохранения транзакций из режима Full в модель Simple (если это не было сделано ранее на этапе развертывания базы данных системы).

ВОЗМОЖНЫЕ ПРОБЛЕМЫ

ВЕБ-ИНТЕРФЕЙС СИСТЕМЫ

В ряде случаев, когда при работе с системой через веб-интерфейс могут наблюдаться ошибки, типа: «Непредвиденная ошибка. Обратитесь к Администратору», «Internal Server Error» и другие необходимо смотреть в специальную таблицу **IntraLog** в базе данных для более детальной диагностики.

1. При восстановлении либо после переноса БД на MS SQL Server 2017 после выполнения всех настроек при создании и сохранении объекта (например, заявки) возникает ошибка: “An error occurred in the Microsoft .NET Framework while trying to load assembly id 65539. The server may be running out of resources, or the assembly may not be trusted. Run the query again, or check documentation to see how to solve the assembly trust issues. For more information about this error: System.IO.FileLoadException: Не удалось загрузить файл или сборку "sqlregex, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null…”

> ***Решение:*** *MS SQL Server 2017 имеет изменения в требованиях безопасности и по умолчанию может не доверять базам данных, «пришедшим» с неизвестных серверов и запрещать выполнение пользовательских CLR-сборок. Чтобы этого избежать, нужно принудительно*

включить доверие к базе данных и разрешить выполнение пользовательских CLR-сборок. Для этого необходимо выполнить следующие команды:

```
ALTER DATABASE [Intraservice] SET TRUSTWORTHY ON
ALTER AUTHORIZATION ON DATABASE::[Intraservice] TO sa
```

2. При попытке сохранения какого-либо объекта сообщение: “Execution of user code in the .NET Framework is disabled. Enable "clr enabled" configuration option”

Решение: *необходимо, используя Microsoft SQL Management Studio, выполнить следующие команды:*

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'clr enabled', 1;
GO
RECONFIGURE;
GO
```

Если в результате выполнения запроса вы увидите подобное 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.

то это значит, что интеграция с CLR включена.

3. Система падает, при попытке обратиться – ошибка сервера **503**. В **EventLog** windows сообщения вида **”Cryptographic exception”**

Решение*: Отсутствуют права на каталог* ***MachineKeys*** *для учетной записи, от которой работает пул приложений.*

4. При обращении к странице ошибка:
Parser Error Message: Could not load file or assembly 'System.Core, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' or one of its dependencies. The system cannot find the file specified.

Решение: *Проверить права на каталоги, описанные в разделе* ***Настройка сайта на веб-сервере***

5. При обращении к системе ошибка:
   HTTP Error 500.0 - Internal Server Error The page cannot be displayed because an internal server error has occurred. Detailed Error InformationModule IsapiModule Notification ExecuteRequestHandler Handler ivp Error Code 0x800700c1 Requested URL http://system_path/dashboard.ivp

> ***Решение:*** *После установки .NET 4.5.1 или выше перезагрузить сервер и проверить установку компонентов при подготовке веб-сервера*

6. При обращении к системе сообщение:
   Возникла непредвиденная ошибка, обратитесь к администратору.

> ***Решение:*** *сделать выборку из таблицы* ***IntraLog*** *базы данных системы, отфильтровав её по id пользователя, у которого возникает ошибка и прислать результат запроса по email на support@intraservice.ru*
>
> *SELECT * FROM IntraLog*
> *WHERE UserId = <id> ORDER BY TimeStamp DESC*

7. При попытке открыть заявку, в таблице IntraLog сообщение **Must declare the scalar variable "@taskid"**

> ***Решение:*** *Вероятно, используется MS SQL 2012 SP4. Если это так, то необходимо:*
>
> - *подключиться к серверу БД через MS SQL Management Studio, открыть БД Intraservice и в разделе Programmability / Functions / Table-valued Functions и найти функцию uf_GetStatusDatesForDuration*
> - *На функции кликнуть правой кнопкой, выбрать* ***Modify****. Попробовать нажать F5 – скорее всего внизу появятся несколько строчек сообщений красным цветом с описанием проблемы Must declare scalar variable @taskid*
> - *В том же окне редактирования функции между BEGIN и RETURN заменить все упоминания (всего 3) переменной @taskid на @taskId, как указано выше по тексту при объявлении переменной.*
> - *Нажать F5 – должно появиться* ***Commands completed successfully.***

8. Ошибка **0x80005000** при windows-авторизации
   В некоторых случаях пользователь, синхронизированный с Active Directory, не авторизуется в системе, получая данную ошибку.

> ***Возможное решение:***
>
> *Убедиться, что LDAP-путь, указанный в настройках синхронизации, не содержит объектов, в имени которых фигурируют символы, отличные от букв и цифр (кавычки, слеши и так далее).*

Также убедиться, что пользователь не входит в группу, в названии которой также фигурируют подобные символы.

Убедиться, что пользователь не входит в группу вне пределов указанного в системе LDAP-пути, в адресе которой (Distinguished name вида CN=Group,OU=department,DC=domain,DC=local) также отсутствуют подобные символы.

Рекомендуется переименовывать проблемные с этой точки зрения объекты.

СЛУЖБА INTRASERVICE AGENT

1. Служба не запускается, выдается сообщение:
   an unhandled exception (system.security.securityException) occurred in intraservice.agent.service.exe
   затем ошибка "Служба не ответила на запрос своевременно" (1053)

Решение: *дать учетной записи пула приложений системы права на ветку реестра*

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog

2. Не работает функционал отправки уведомлений или импорта писем, в EventLog сообщение:
   Exception: Index 0 is out of range.
   Stack: at System.Configuration.ConfigurationElementCollection.BaseGet(Int32 index)
   at System.Configuration.ConnectionStringSettingsCollection.get_Item(Int32 index)…

Решение: *В конфигурационном файле отсутствует строка подключения службы к базе данных системы. Исправить.*

3. Не работает функционал отправки уведомлений или импорта писем, в EventLog сообщение:
   Database access error: Data Source=(DB_server);Initial Catalog=IntraService;Integrated Security=True; Error: System.Data.SqlClient.SqlException (0x80131904): Cannot open database "IntraService" requested by the login. The login failed.
   Login failed for user 'DOMAIN\Intraservice'.

Решение: *отсутствуют права у указанной учетной записи, от которой работает служба, на подключение к базе данных. Проверить и скорректировать.*