InfoWatch MS Teams Adapter. Руководство по установке, конфигурированию и эксплуатации

09/06/2022

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 4

2 Общие сведения об адаптере 5

2.1 Общая схема работы 5

3 Подготовка к установке адаптера 6

3.1 Настройка приложения в Microsoft Azure 6

3.2 Установка плагина в Traffic Monitor 14

4 Установка адаптера 16

5 Доступ к защищенному API 22

6 Конфигурирование адаптера 25

6.1 appsettings.json 25

6.2 settings.json 25

6.2.1 FileQueueSettings - настройки файловой очереди 25

6.2.2 ChatRoomSettings - Настройки обработки чат комнат 26

6.2.3 GraphApiSettings – Настройки подключения к GraphApi 27

6.2.4 SubscriptionsSettings – Настройки подписок на чаты MsTeams 27

6.2.5 TmConnectionSettings – Настройки подключения к IW TM 28

6.2.6 HttpProxySettings – Настройки прокси (для исходящих подключений) 28

6.2.7 DetailManagerSettings – Настройки для дозаполнения событий дополнительными данными 29

6.2.8 StringTemplateSettings – Настройки шаблонов для автозамены вложений текстом, и генерация имен вложений 29

6.2.9 StatisticsSettings – Настройки счетчиков статистики 30

6.2.10 UISettings - Настройки для доступа к административной панели 31

7 Сбор статистики адаптером 32

8 Работа в консоли управления адаптера 36

8.1 Интерфейс адаптера 36

8.2 Общие действия 37

8.2.1 Вход в консоль управления 37

8.2.2 Смена пароля администратора 38

8.2.3 Просмотр системного журнала 39

8.3 Статистика 39

8.4 Подключение к Grath API (MS Teams) 41

8.5 Подключение к Traffic Monitor 42
8.6 Настройка агрегации чатов 42
8.7 Настройка прокси-сервера 43
9 Получение событий в Traffic Monitor 44

1 Введение

В настоящем руководстве представлены сведения по установке, настройке и администрированию Infowatch MS Teams Adapter.

Аудитория

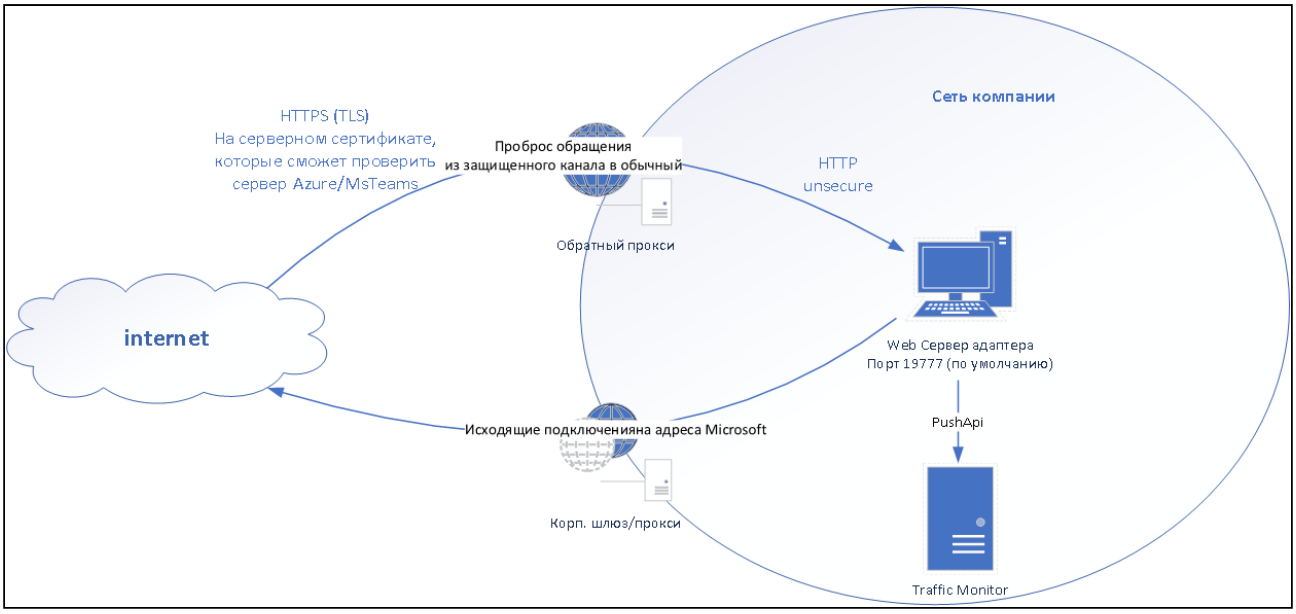
Информация, содержащаяся в данном Руководстве, предназначена для пользователей облачной платформы Microsoft Azure, выполняющих установку и администрирование InfoWatch MS Teams Adapter, плагина для него и настраивающих интеграцию с комплексом InfoWatch Traffic Monitor. Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных системы Microsoft Windows, а также навыками администрирования сервера InfoWatch Traffic Monitor.

2 Общие сведения об адаптере

2.1 Общая схема работы

Адаптер представляет собой web-сервер, принимающий реплики чатов мессенджера MS Teams. Затем реплики агрегируются в события и отправляются в TM по протоколу pushApi.
В качестве механизма получения данных из MS Teams используется механизм получения оповещений по подписке. При запуске адаптера осуществляется авторизация на серверах Microsoft и создание подписки на получение уведомлений с сообщениями чатов MS Teams. При регистрации подписки указывается внешний интернет-адрес, по которому доступен адаптер. Таким образом на сервере Microsoft становится известно, где находится адаптер.

Общая схема встраивания адаптера в сеть компании выглядит следующим образом:



Для работы адаптера необходимо обеспечить:

- Внешний адрес в сети Internet, доступный по протоколу HTTPS с валидным сертификатом;

> **Важно!**
>
> Протокол HTTP не поддерживается серверами Microsoft

- Обратный прокси, который будет ретранслировать полученные от серверов Microsoft обращения на сервер адаптера. При этом обращение должно быть распаковано из HTTPS в обычный HTTP запрос;
- Доступ в сеть Internet с сервера адаптера.

3 Подготовка к установке адаптера

Адаптер может быть установлен на сервере с ОС Microsoft Windows Server 2016 или более новой версии.

Перед началом установки Адаптера необходимо:

1. Установить платформы разработки .NET Desktop Runtime 5 и затем ASP.NET Core Runtime 5 (https://dotnet.microsoft.com/download/dotnet/5.0).
2. Выполнить подготовительные действия в виде настройки приложения в Microsoft Azure.
3. Установить плагин в Traffic Monitor.

Для облегчения процесса установки заполните шаблон по параметрам, которые необходимо будет ввести в инсталлятор адаптера. Значения этих параметров вы получите по мере прохождения шагов пунктов 1 и 2:

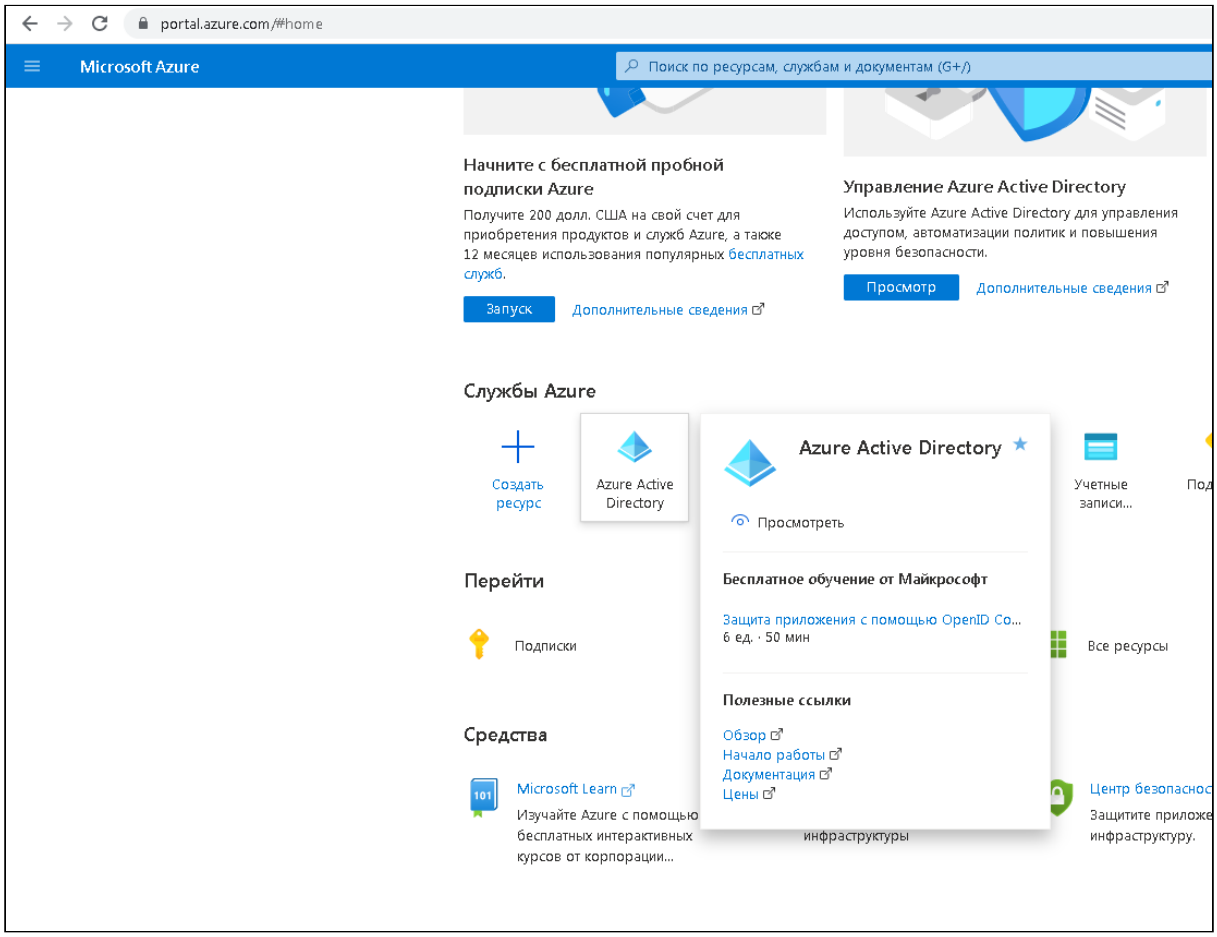
Описание	Значение
Внешний адрес в сети интернет для адаптера	
Идентификатор клиента в Azure AD (`TenantId`)	
Идентификатор приложения в Azure AD (`ClientId`)	
Идентификатор приложения в Azure AD (`ClientSecret`)	
Адрес сервера Traffic Monitor	
Порт ТМ протокола PushApi	по умолчанию: 9101
Токен доступа к ТМ	
Серверный сертификат открытого ключа ТМ – сертификат, на котором поднимается защищенный канал между адаптером и ТМ	

3.1 Настройка приложения в Microsoft Azure

Выполните действия:

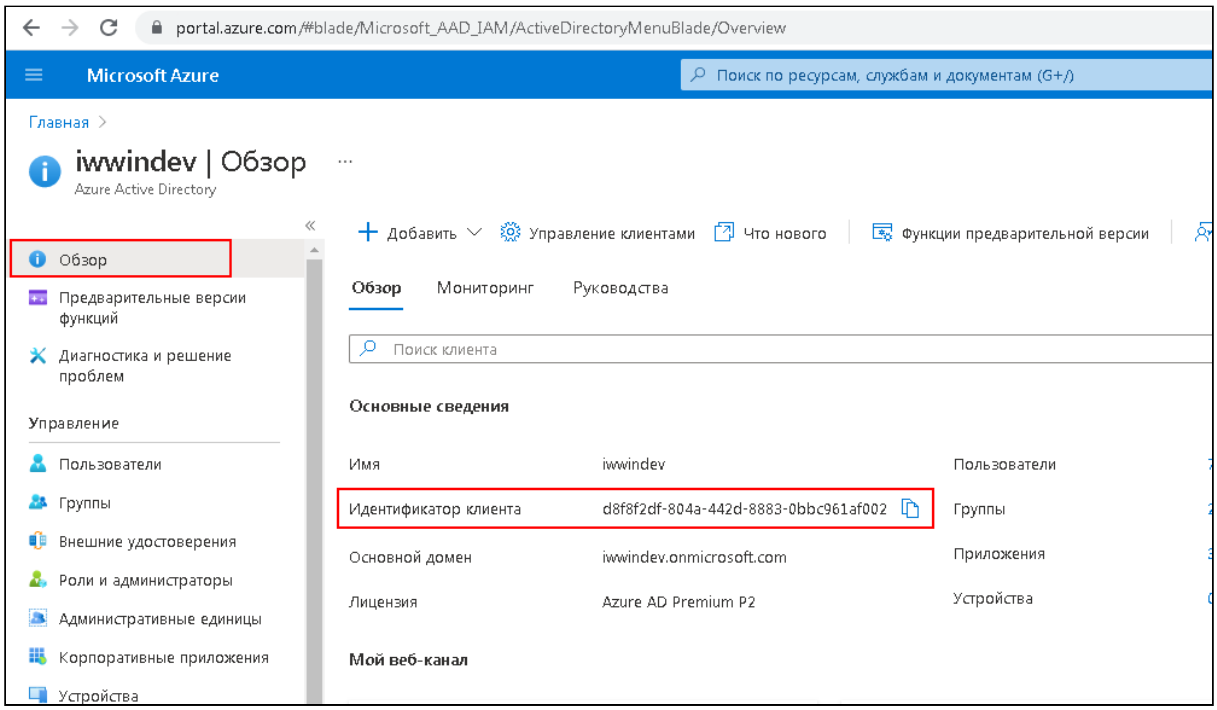
1. Перейдите на портал Azure по адресу https://portal.azure.com/

2. Зайдите в раздел службы Azure Active Directory:

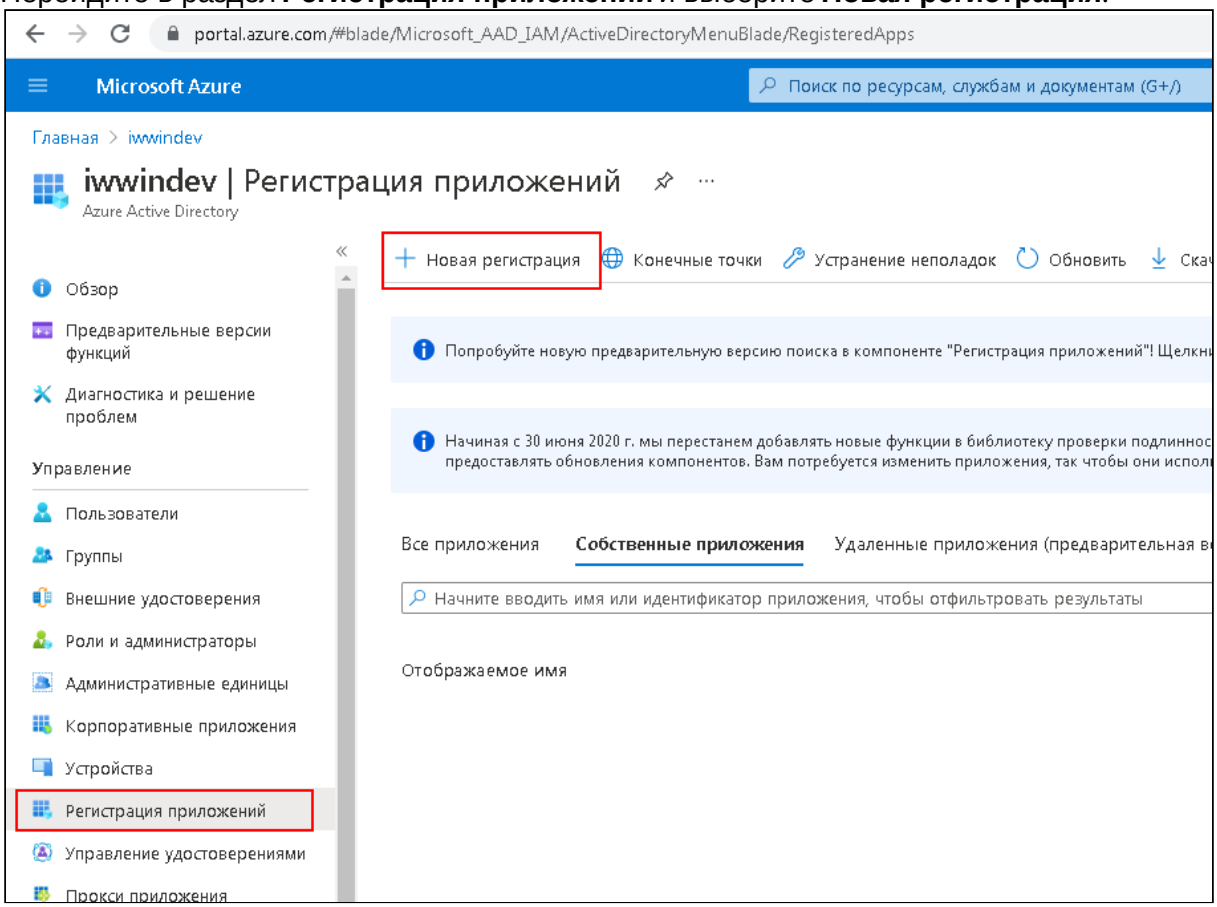


3. В разделе **Обзор** скопируйте значение параметра `Идентификатор клиента`. Можете вставить скопированное значение в параметр `“TenantId”` в предложенной ранее

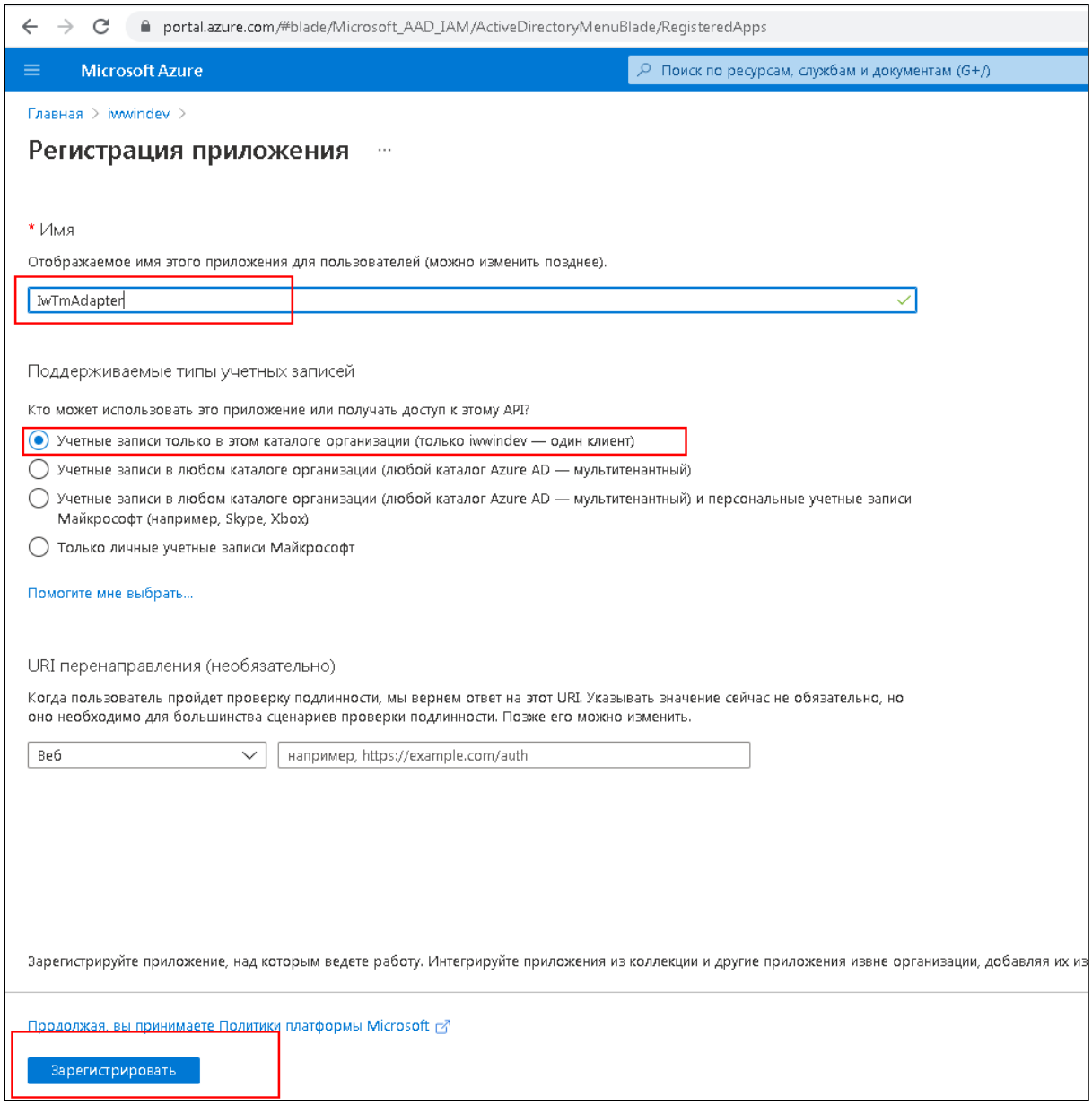
шаблоне



4. Перейдите в раздел **Регистрация приложений** и выберите **Новая регистрация**.

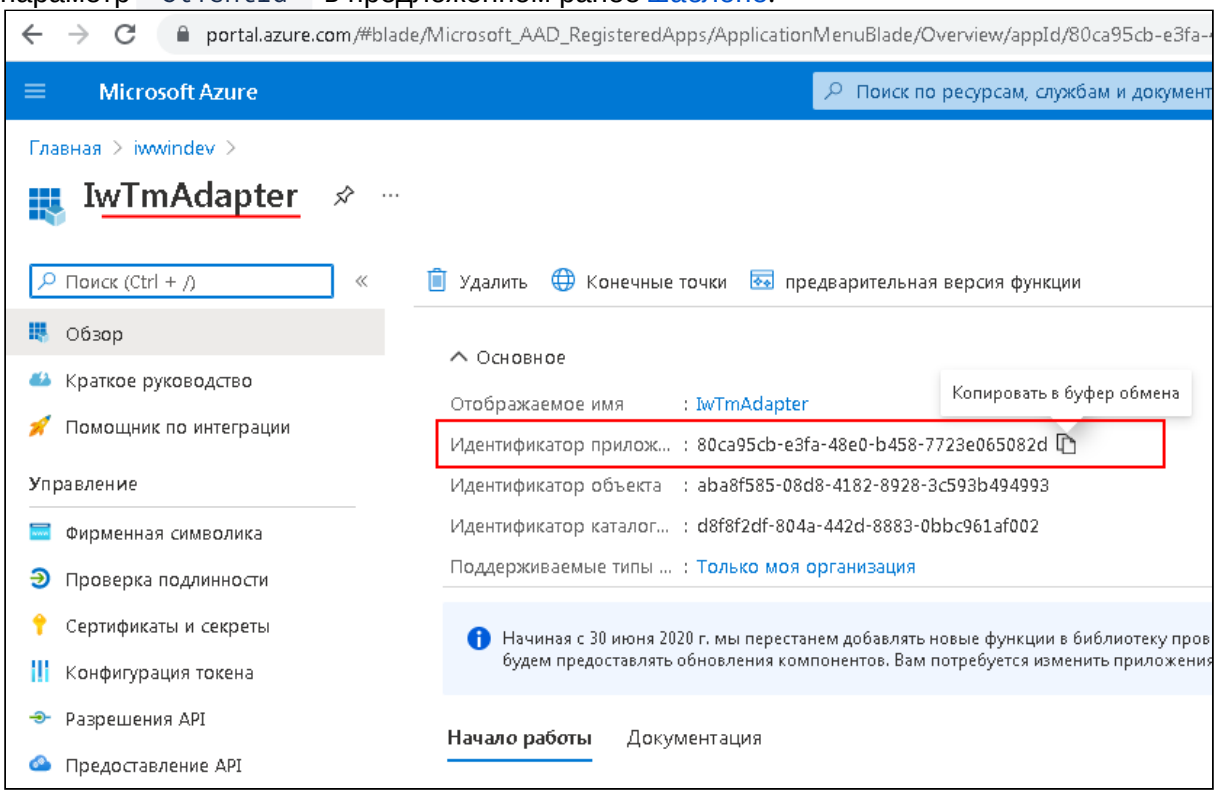


5. Зарегистрируйте новое приложение, введя **Имя** приложения и указав опцию ***Только для каталога организации***.

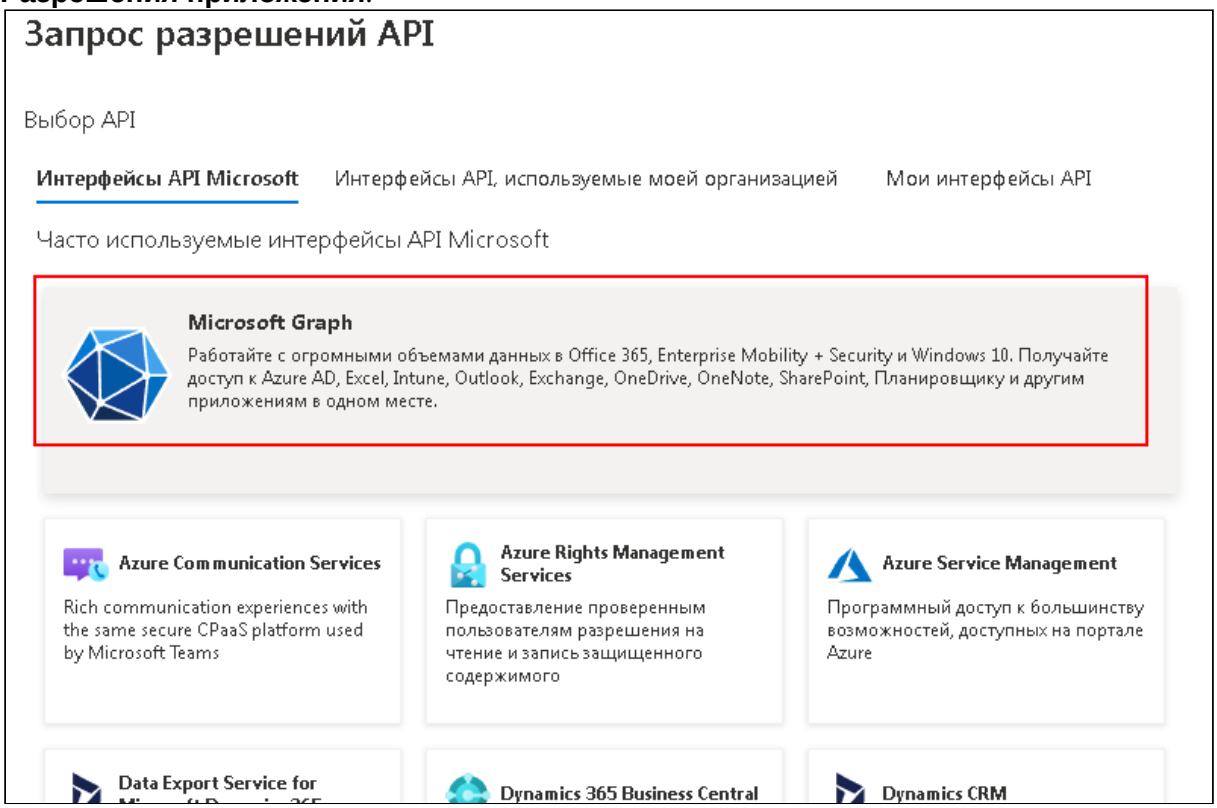


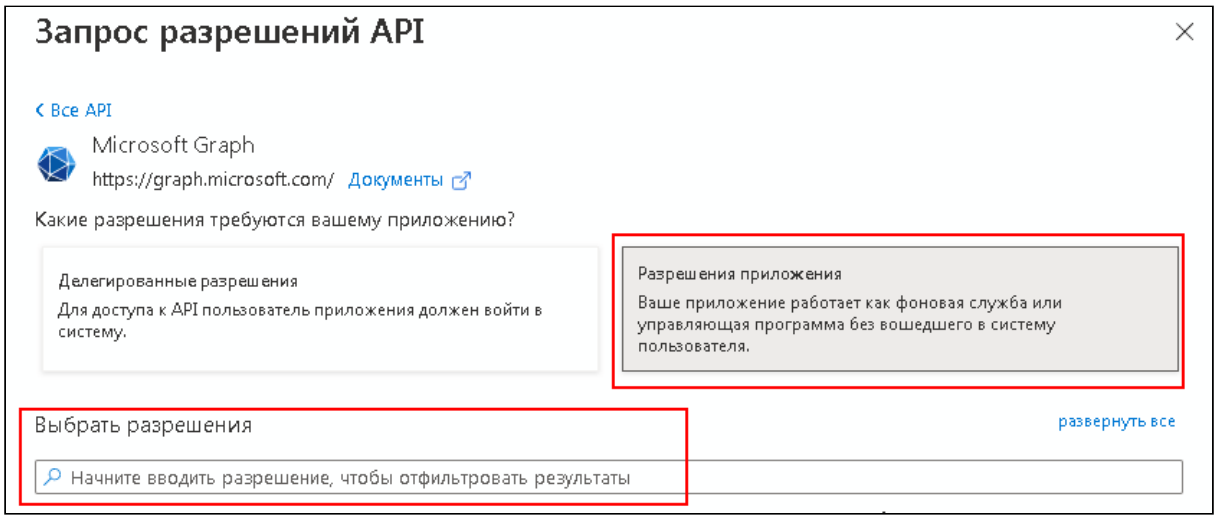
6. Находясь в настройках зарегистрированного приложения, скопируйте значение параметра `Идентификатор приложения`. Можете вставить скопированное значение в

параметр `“ClientId”` в предложенном ранее шаблоне.



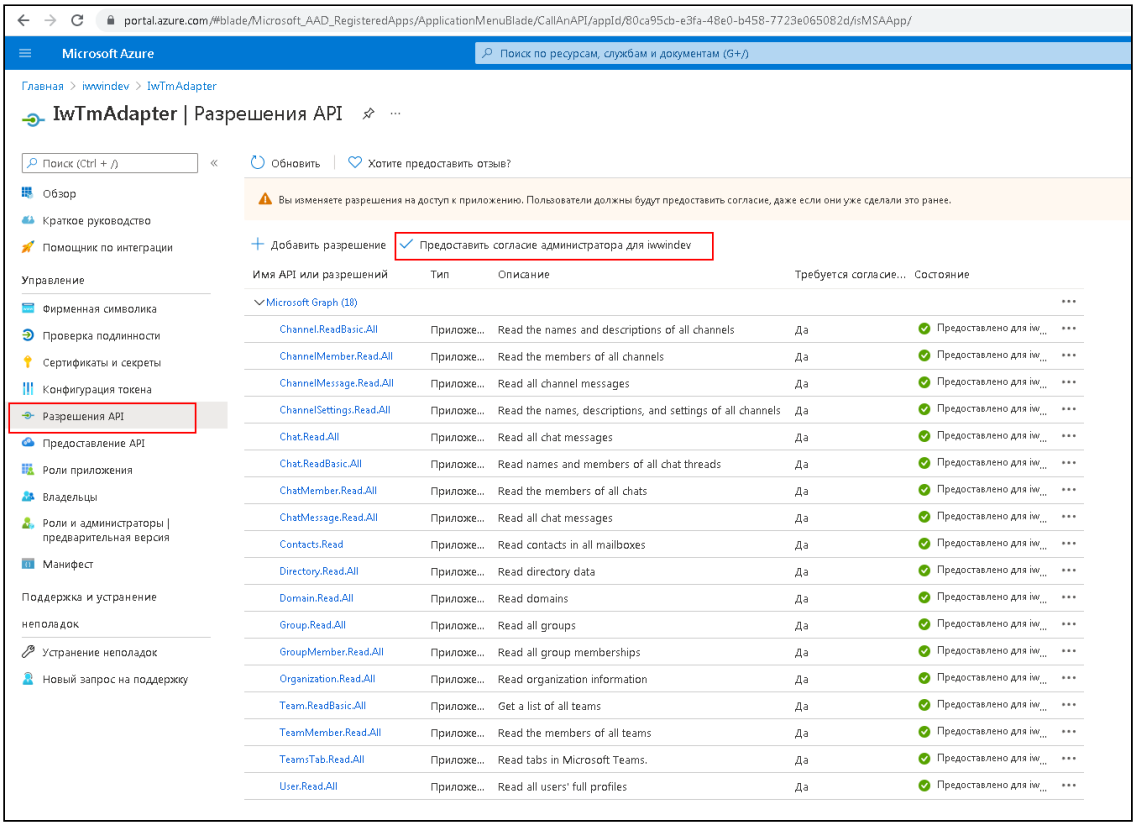
7. Перейдите в раздел **Разрешения API**, чтобы выставить нужные права для адаптера. Нажмите **Добавить разрешения**, далее выберите **Microsoft Graph**, и затем **Разрешения приложения**.



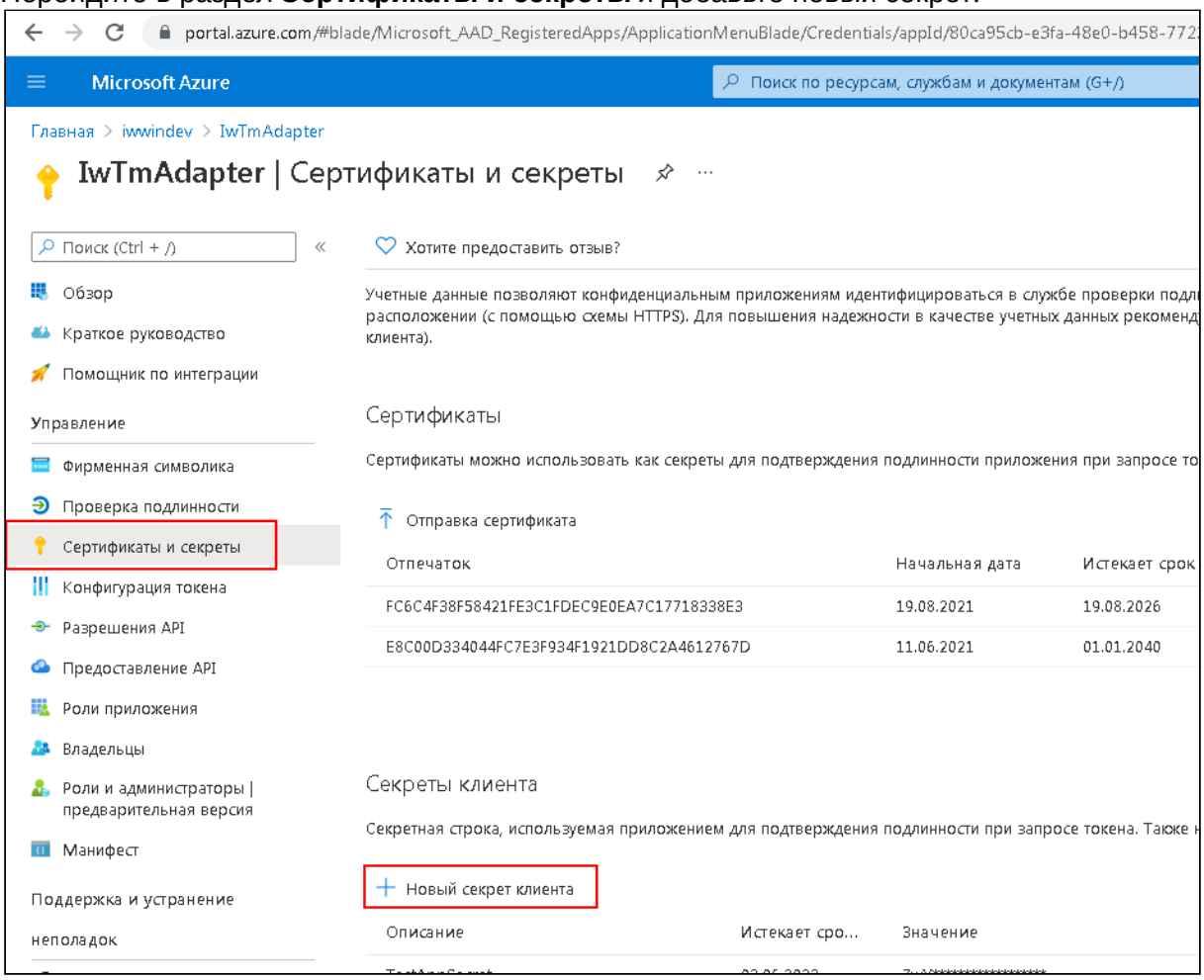


8. Используя строку поиска, добавьте следующие значения:
   - Application.Read.All
   - Channel.ReadBasic.All
   - ChannelMember.Read.All
   - ChannelMessage.Read.All
   - ChannelSettings.Read.All
   - Chat.Read.All
   - Chat.ReadBasic.All
   - ChatMember.Read.All
   - ChatMessage.Read.All
   - Directory.Read.All
   - Domain.Read.All
   - Files.Read.All
   - Group.Read.All
   - GroupMember.Read.All
   - Organization.Read.All
   - Team.ReadBasic.All
   - TeamMember.Read.All
   - TeamsTab.Read.All
   - User.Read.All
   - Sites.Read.All

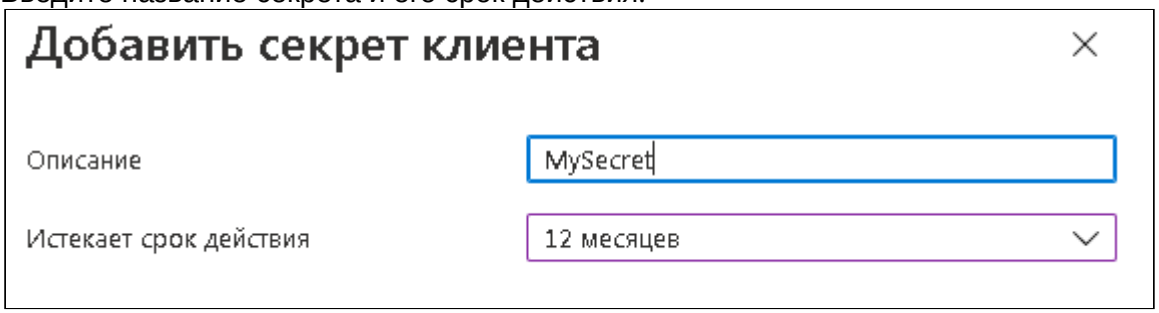
   и нажмите **Предоставить согласие администратора**:


portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/appId/80ca95cb-e3fa-48e0-b458-7723e065082d/isMSAApp/
Microsoft Azure
Поиск по ресурсам, службам и документам (G+/)
Главная > iwwindev > IwTmAdapter
IwTmAdapter | Разрешения API
Поиск (Ctrl + /)
Обзор
Краткое руководство
Помощник по интеграции
Управление
Фирменная символика
Проверка подлинности
Сертификаты и секреты
Конфигурация токена
Разрешения API
Предоставление API
Роли приложения
Владельцы
Роли и администраторы | предварительная версия
Манифест
Поддержка и устранение неполадок
Устранение неполадок
Новый запрос на поддержку
Обновить
Хотите предоставить отзыв?
Вы изменяете разрешения на доступ к приложению. Пользователи должны будут предоставить согласие, даже если они уже сделали это ранее.
Добавить разрешение
Предоставить согласие администратора для iwwindev
Имя API или разрешений
Тип
Описание
Требуется согласие...
Состояние
Microsoft Graph (18)
Channel.ReadBasic.All
Приложе...
Read the names and descriptions of all channels
Да
Предоставлено для iw...
ChannelMember.Read.All
Приложе...
Read the members of all channels
Да
Предоставлено для iw...
ChannelMessage.Read.All
Приложе...
Read all channel messages
Да
Предоставлено для iw...
ChannelSettings.Read.All
Приложе...
Read the names, descriptions, and settings of all channels
Да
Предоставлено для iw...
Chat.Read.All
Приложе...
Read all chat messages
Да
Предоставлено для iw...
Chat.ReadBasic.All
Приложе...
Read names and members of all chat threads
Да
Предоставлено для iw...
ChatMember.Read.All
Приложе...
Read the members of all chats
Да
Предоставлено для iw...
ChatMessage.Read.All
Приложе...
Read all chat messages
Да
Предоставлено для iw...
Contacts.Read
Приложе...
Read contacts in all mailboxes
Да
Предоставлено для iw...
Directory.Read.All
Приложе...
Read directory data
Да
Предоставлено для iw...
Domain.Read.All
Приложе...
Read domains
Да
Предоставлено для iw...
Group.Read.All
Приложе...
Read all groups
Да
Предоставлено для iw...
GroupMember.Read.All
Приложе...
Read all group memberships
Да
Предоставлено для iw...
Organization.Read.All
Приложе...
Read organization information
Да
Предоставлено для iw...
Team.ReadBasic.All
Приложе...
Get a list of all teams
Да
Предоставлено для iw...
TeamMember.Read.All
Приложе...
Read the members of all teams
Да
Предоставлено для iw...
TeamsTab.Read.All
Приложе...
Read tabs in Microsoft Teams.
Да
Предоставлено для iw...
User.Read.All
Приложе...
Read all users' full profiles
Да
Предоставлено для iw...

9. Перейдите в раздел **Сертификаты и секреты** и добавьте новый секрет:

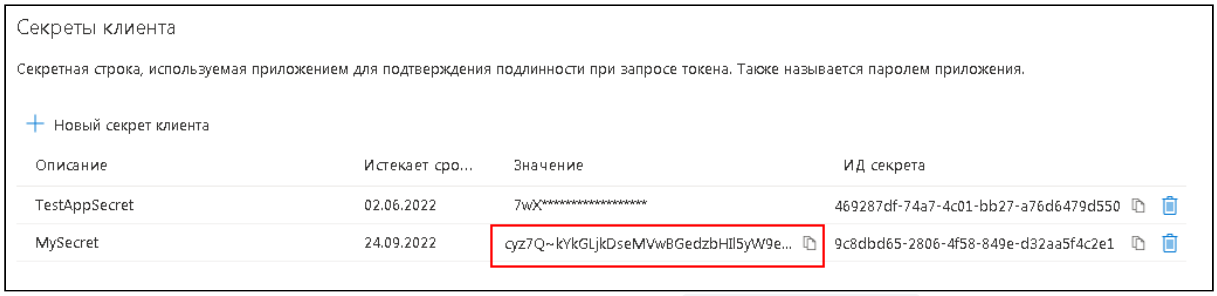


10. Введите название секрета и его срок действия:



После добавления секрет появится в списке секретов приложения.

> **Важно!**
>
> Немедленно скопируйте значение секрета, так как оно полностью появляется всего один раз.

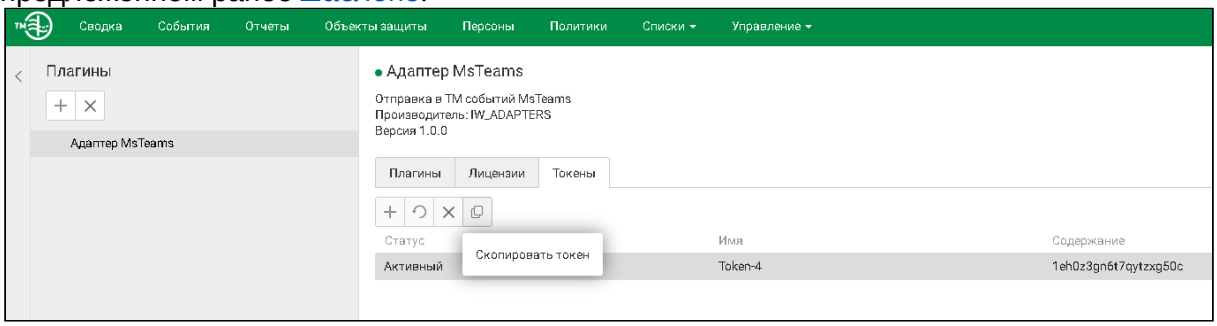


Можете вставить скопированное значение в параметр `“ClientSecret”` в предложенном ранее шаблоне.

3.2 Установка плагина в Traffic Monitor

Чтобы установить плагин Адаптера:

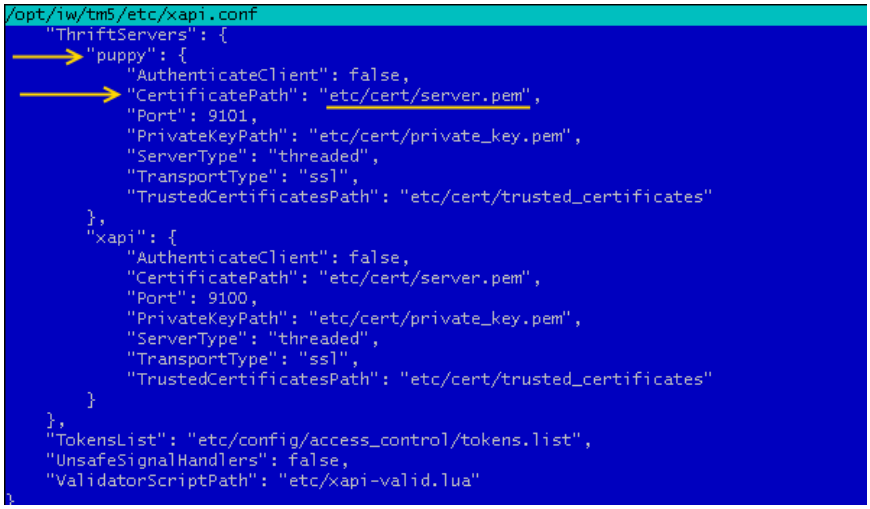
1. Откройте консоль управления ТМ, перейдите в раздел **Плагины**.
2. Нажмите [+] для добавления плагина.
3. Выберите файл плагина и загрузите его.
4. Перейдите в загруженном плагине на вкладку **Токены.** Выберите и скопируйте токен доступа. Можете вставить скопированное значение в параметр `Токен доступа к ТМ` в предложенном ранее шаблоне.



5. Загрузите действующую лицензию для адаптера. Она должна содержать:

```
"Features": [
    {
        "common_name": "IW_ADAPTERS",
        "object_type": "im_msteams",
        "protocol": "*"
    }
],
```

6. Откройте на редактирование файл конфигурации `/opt/iw/tm5/etc/xapi.conf` на сервере ТМ.
7. Скопируйте полное имя файла, который указан в параметре `CertificatePath` секции `puppy`, а также номер порта ТМ:

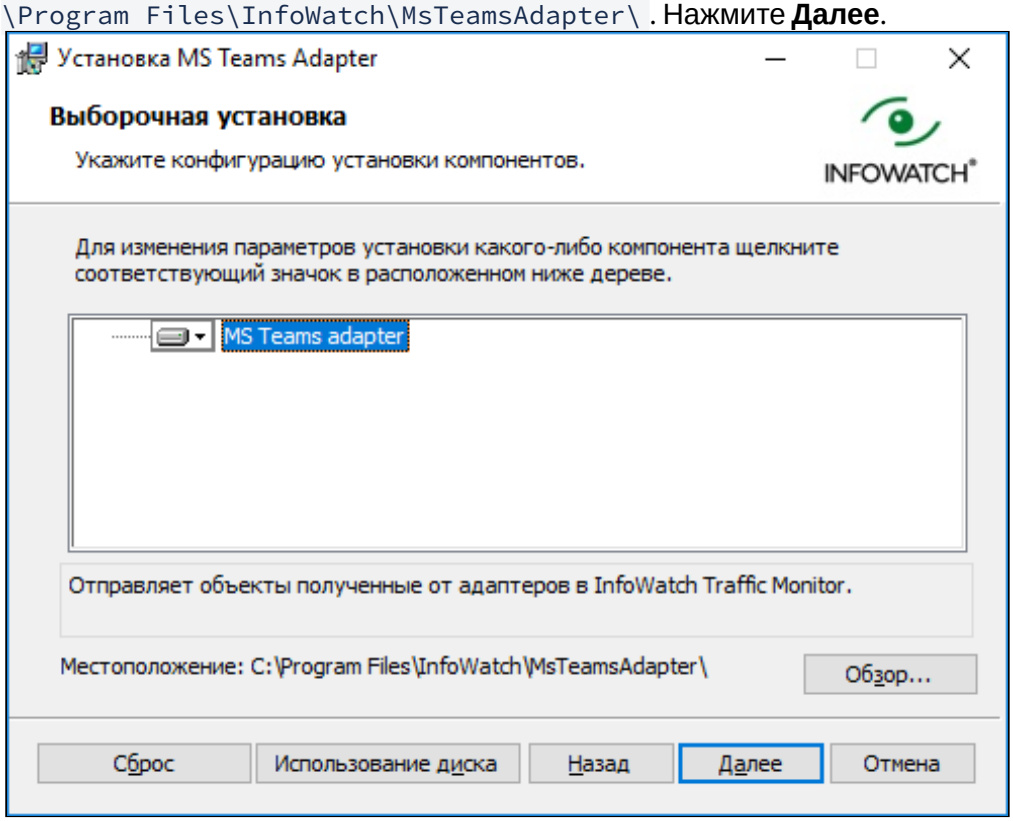


Можете вставить скопированные значения в параметры `Серверный сертификат открытого ключа ТМ` и `Порт ТМ протокола PushApi` в предложенном ранее шаблоне.

4 Установка адаптера

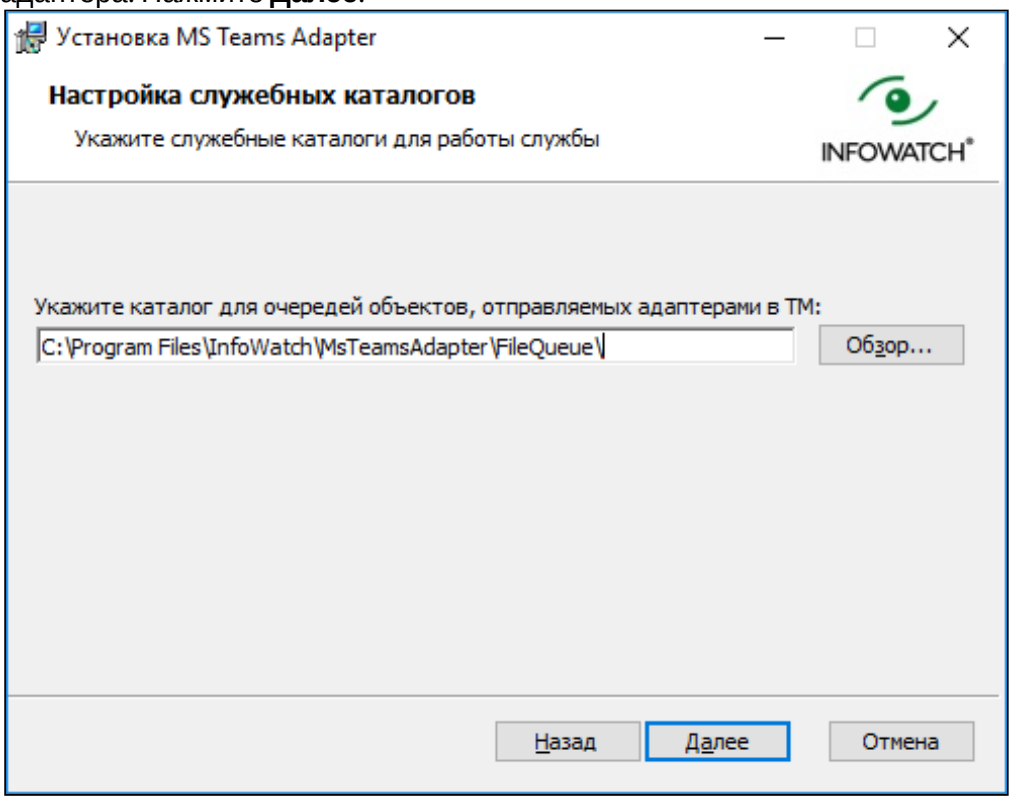
Выполните шаги:

1. Запустите полученный файл **Win.Setup.msi**.
2. Примите лицензионное соглашение.
3. Выберите каталог установки адаптера. По умолчанию установка производится в `C:\Program Files\InfoWatch\MsTeamsAdapter\`. Нажмите **Далее**.

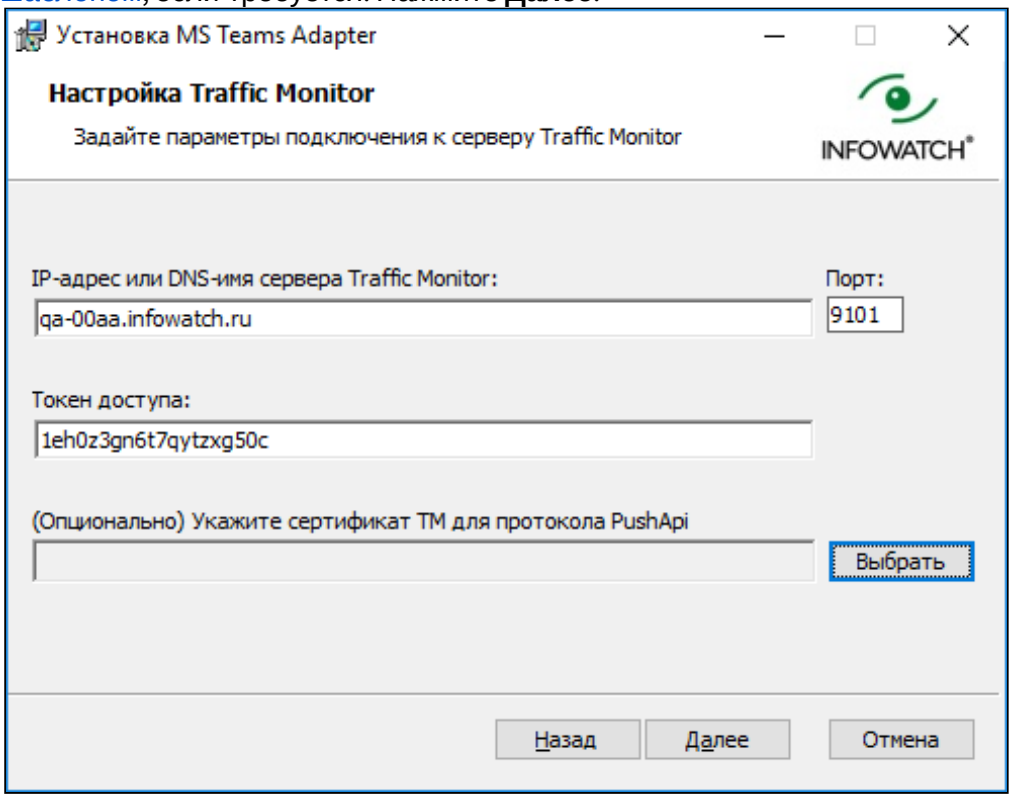


4. Укажите каталог для хранения файловой очереди событий, отправляемых в ТМ. По умолчанию каталог FileQueue располагается внутри каталога установки

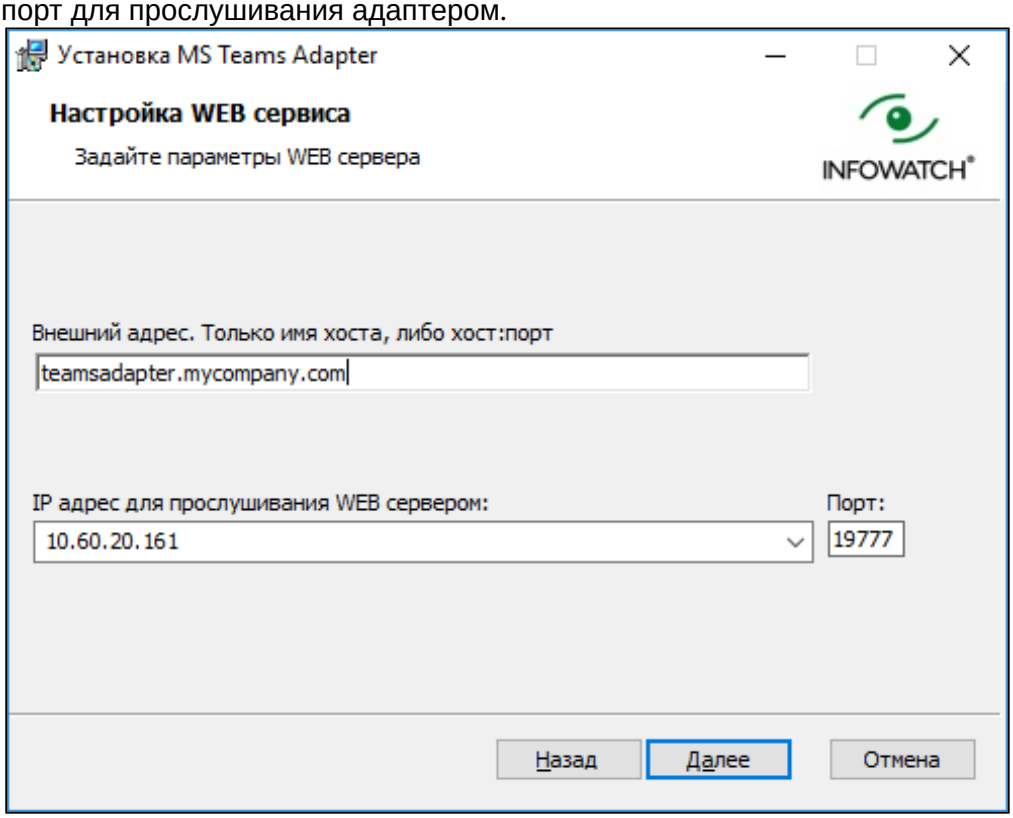
адаптера. Нажмите **Далее**.



5. Укажите адрес ТМ, порт и токен доступа к нему. Также с целью повышения безопасности в области доверия канала между ТМ и адаптером рекомендуется указать опциональный параметр **Сертификат ТМ для протокола PushApi.** Воспользуйтесь шаблоном, если требуется. Нажмите **Далее**.

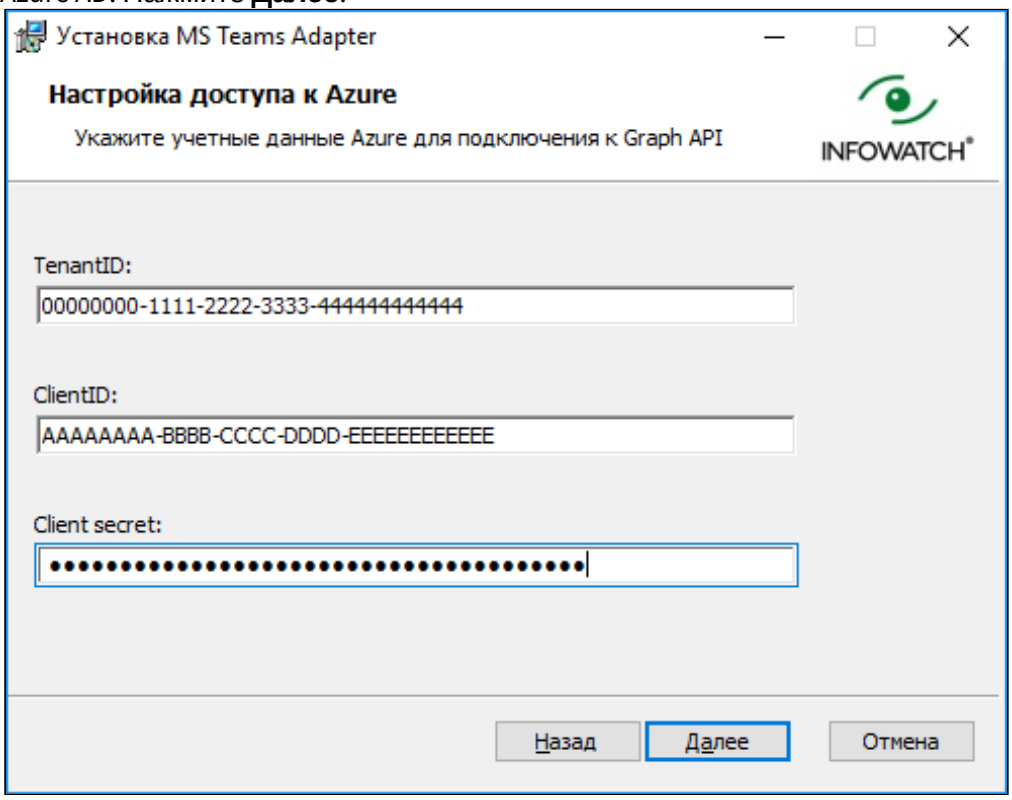


6. Настройте сетевые параметры, указав:
   - внешний адрес, который будет выделен в инфраструктуре компании для доступа к API адаптера и взаимодействия с серверами Microsoft извне;
   - IP-адрес для доступа только с локальных адресов сети;
   - порт для прослушивания адаптером.

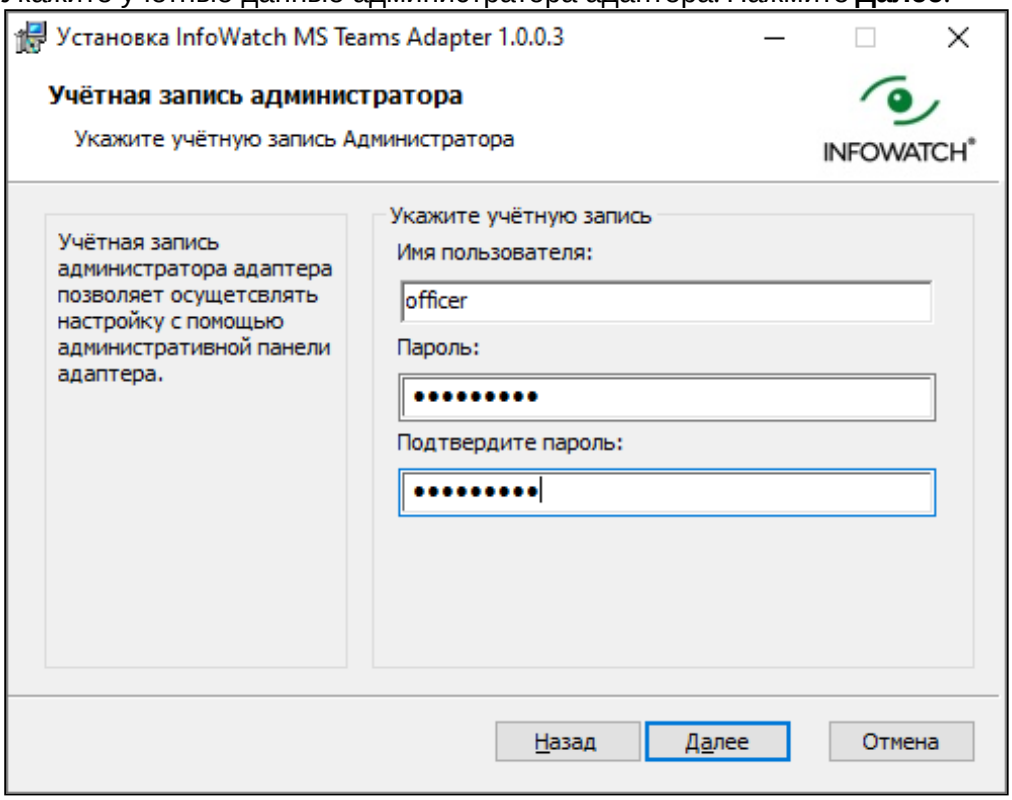


Нажмите **Далее**.

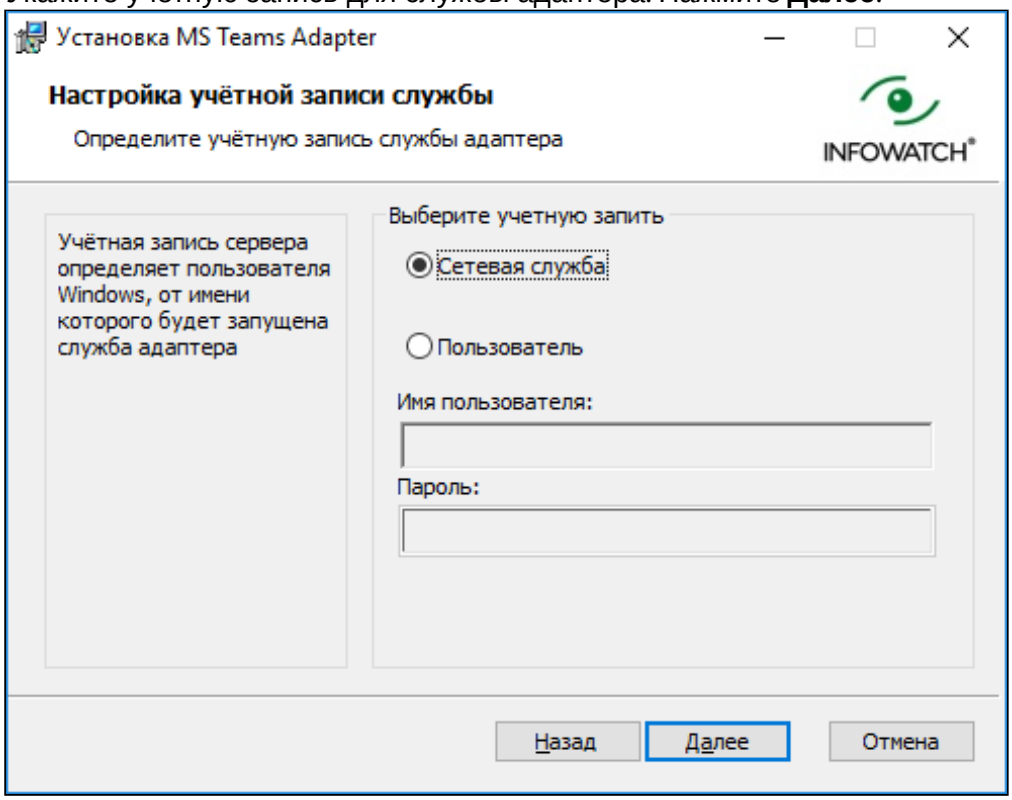
7. Введите учетные данные Azure, которые были получены при регистрации приложения в Azure AD. Нажмите **Далее**.



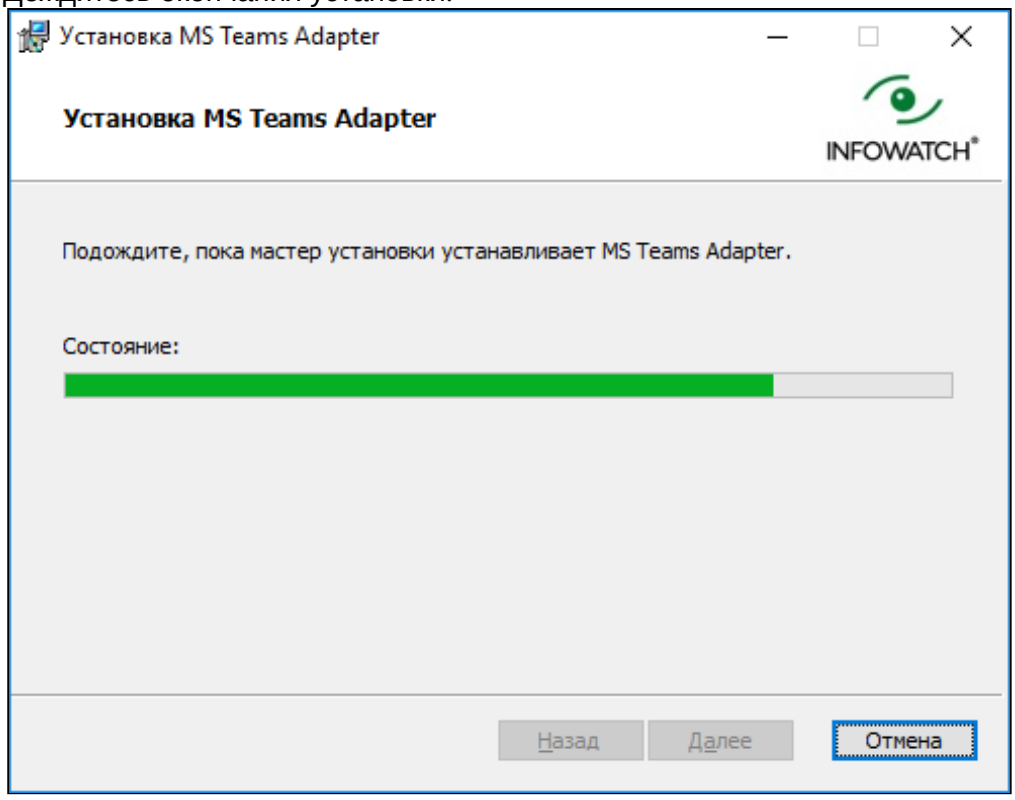
8. Укажите учетные данные администратора адаптера. Нажмите **Далее**.



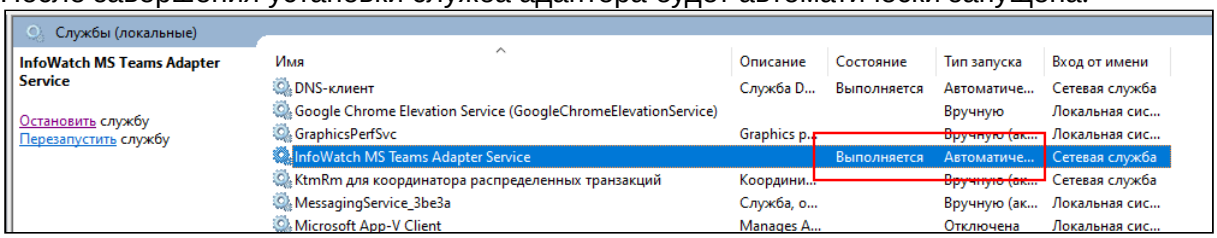
9. Укажите учетную запись для службы адаптера. Нажмите **Далее**.



10. Дождитесь окончания установки.



11. После завершения установки служба адаптера будет автоматически запущена.



5 Доступ к защищенному API

После запуска адаптер будет функционировать, но при этом не будет получать уведомлений от серверов Microsoft с текстами чатов Microsoft Teams. Эта ситуация происходит вследствие того, что компания Microsoft обеспокоена безопасностью данных своих пользователей, а API-интерфейсы Microsoft Teams в используемых адаптером Microsoft Graph получают доступ к конфиденциальным данным, и поэтому считаются защищенными API-интерфейсами. Таким образом, эти API требуют дополнительной проверки, помимо разрешений и согласия, прежде чем вы сможете их использовать.

Дополнительная информация по защищённому API - https://docs.microsoft.com/ru-ru/graph/teams-protected-apis

1. Для предоставления доступа перейдите на страницу https://aka.ms/teamsgraph/requestaccess

> **Важно!**
>
> Стоит обратить внимание, что на момент написания документации (февраль 2022 года) в данной форме есть пометка «*Мы рассматриваем запросы на доступ каждые две недели*».

2. Заполните форму запроса, предоставив следующую информацию:
   - Контактный адрес электронной почты;
   - Имя издателя приложения;
   - Имя приложения;
   - Идентификатор приложения, который получили в процессе регистрации в Azure);
   - Кратко описать приложение, и для чего ему необходим доступ к защищенному API;
   - Указать как приложение сохраняет данные, полученные по защищенному API;
   - Указать идентификатор Tenant ID;

   и нажмите **Next**

Request access to protected APIs in Microsoft Graph

Microsoft Teams APIs in Microsoft Graph that access sensitive data are considered protected APIs. These APIs require that you have additional validation, beyond permissions and consent, before you can use them. See https://aka.ms/teamsgraph/protectedAPIs for more details.

To request access to these protected APIs, complete the following request form. We review access requests every other week.

...

* Required

1. Your email address and any others you want to list as an owner (semicolon separated) *

Alexey.[redacted]@infowatch.com

2. May we contact you about your app's use of non-protected APIs? (E.g., reliability issues, advanced notice of breaking changes, throttling, etc) *

- (●) Yes
- ( ) No

3. Publisher name *

ISC InfoWatch

4. App name *

DKS Teams Adapter

5. App id(s) to enable application permissions for *

60263[redacted]2387

6. What does your app do? Why does it exist? (2-3 sentences explaining to an admin who has never heard of your app what it is and why they want it) *

The app is capturing all messages and files transfering of MS Teams and sent to InfoWatch Traffic Monitor (DLP system).

7. Why does your app need read access to all messages in the tenant? (If you don't, you don't need protected APIs) *

Analysis of all messages in the DLP system.

8. Data retention - select one of these options: *

- ○ This app will not make a copy of Microsoft Teams messages.
- ◉ It is obvious to any admin installing this app that it will make a copy of Microsoft Teams messages.
- ○ This app will store a copy or summary of message metadata but will not make a copy of the message body, the subject lines, or any attachments. This is disclosed in the app's privacy policy.
- ○ This app should not be allowed application permissions for reading messages. (You do not need protected APIs)

9. What are the tenant ID's that this app needs to run in? (semicolon-separated. Put "all" if you're writing software for other organizations to use.) *

55c4[redacted]9b52

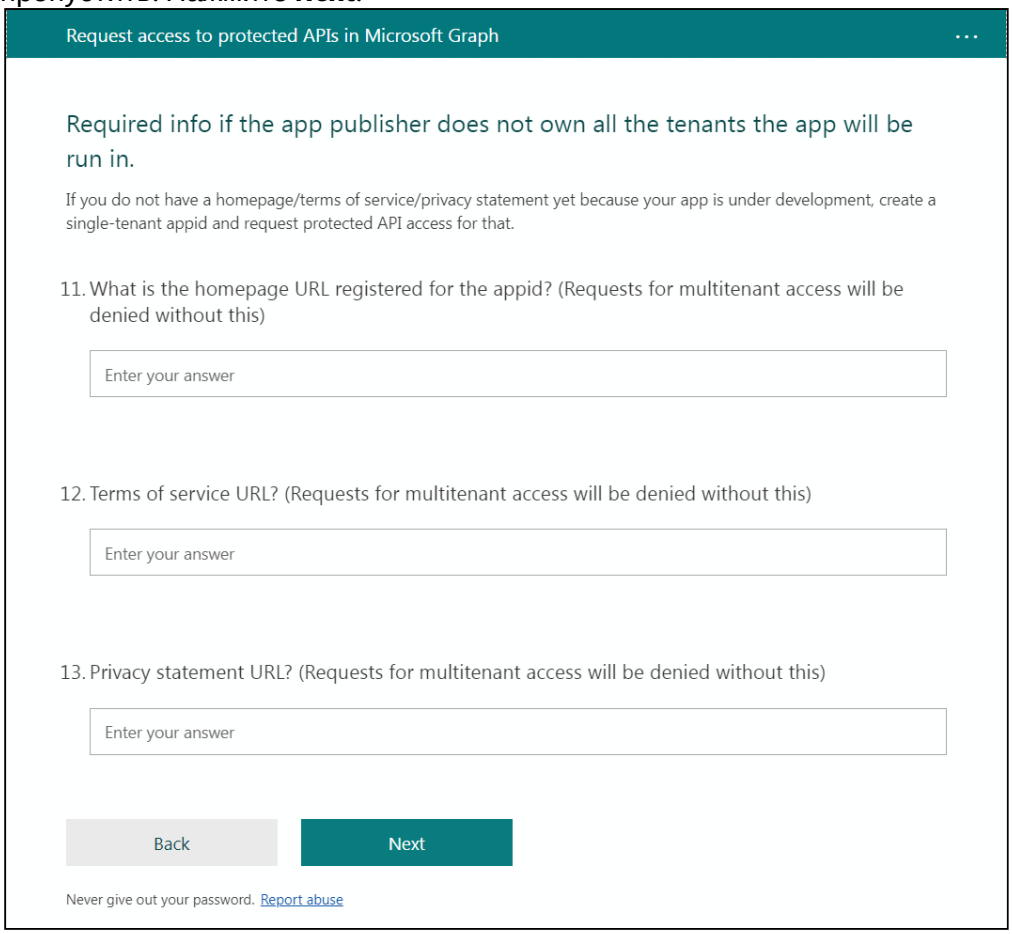
10. Does your organization own all those tenants? (if no, your answer above should be "all", or you should get the tenant owner to submit the request) *

- ◉ Yes
- ○ No

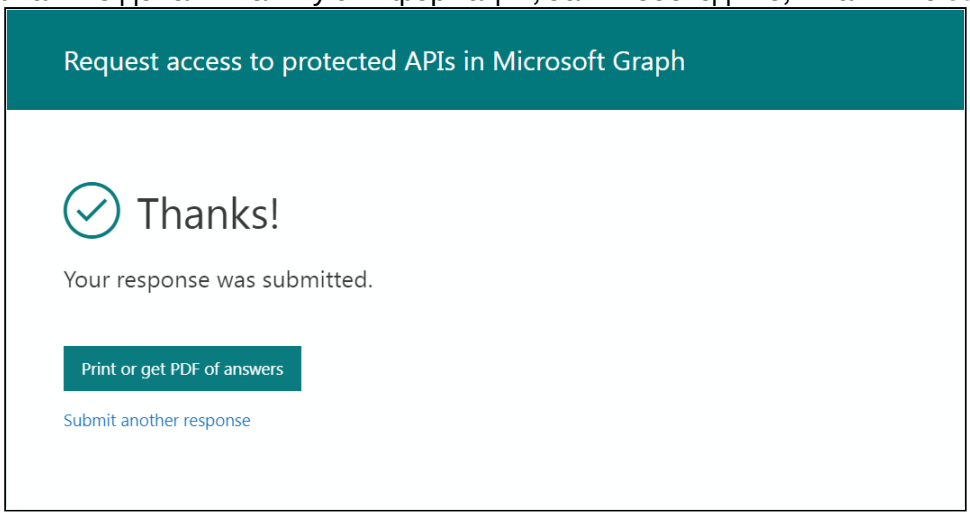
Next

Never give out your password. Report abuse

3. Вторая страница заполняется для приложений, который являются multitenant. Но поскольку приложение регистрируется в Azure как single tenant, данный раздел можно пропустить. Нажмите **Next**.



4. Укажите дополнительную информации, если необходимо, и нажмите **Submit**.



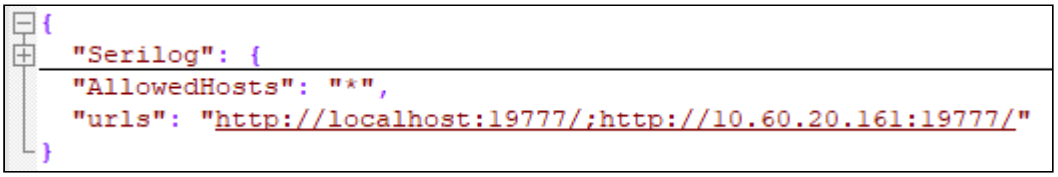
6 Конфигурирование адаптера

Настройки адаптера хранятся в двух файлах конфигурации:

- appsettings.json
- settings.json

6.1 appsettings.json

В файле содержится настройка логирования, указывается локальный IP-адрес и порт для функционирования web-сервера адаптера.
Если у сервера, на котором установлен адаптер, изменился IP-адрес либо требуется изменить порт прослушивания web-сервера, необходимо внести соответствующие правки в параметр `urls` данного файла:



6.2 settings.json

Файл содержит основные настройки адаптера, разбитые по группам:

- `FileQueueSettings` – настройки файловой очереди;
- `ChatRoomSettings` - настройки обработки чат-комнат;
- `GraphApiSettings` – настройки подключения к GraphApi;
- `SubscriptionsSettings` – настройки подписок на чаты MS Teams;
- `TmConnectionSettings` – настройки подключения к TM;
- `HttpProxySettings` – настройки прокси (для исходящих подключений);
- `DetailManagerSettings` – настройки для дозаполнения событий дополнительными данными;
- `StringTemplateSettings` – настройки шаблонов для автозамены вложений текстом и генерация имен вложений;
- `X509CertificateManagerSettings` – служебные настройки;
- `DebugSettings` – служебные настройки;
- `StatisticsSettings` - настройки счетчиков статистики;
- `UISettings` - настройки для доступа к административной панели;

6.2.1 FileQueueSettings - настройки файловой очереди

```
"FileQueueSettings": {
  "BasePath": "C:\\Program Files\\InfoWatch\\MsTeamsAdapter\\FileQueue\\",
  "MaxTryReservation": 5
},
```

- `BasePath` - указывается путь до каталога, в котором содержатся события, отправляемые адаптером в TM
- `MaxTryReservation` – количество попыток создания каталога события

6.2.2 ChatRoomSettings - Настройки обработки чат комнат

```
"ChatRoomSettings": {
  "TextChatRoomSettings": {
      "MessagesCountForSend": 10,
      "AddCodeSnippetAsText": true
  },
  "FileChatRoomSettings": {
      "SendCodeSnippetAsFile": true
  },
  "ProcessAttachmentsAsFiles": true,
  "IdleRoomTimeBeforeSendSec": 120,
  "AzurePortalUrlHost": "portal.azure.com",
  "AzurePortalUrlPath": "",
  "AzurePortalUrlFragment": "blade/Microsoft_AAD_IAM/UserDetailsMenuBlade/Profile/userId/{0}",
  "PushApiServiceName": "im_msteams",
  "IdContactType": "azureId",
  "AddUserPrincipalNameAsAuth": false,
  "ResolveChatMembers": true,
  "ResolveUserDetails": false,
  "RoomWorkerTaskCount": 4
},
```

- `TextChatRoomSettings` - настройки, влияющие на формирование событий текстовых чатов
    - MessagesCountForSend - количество сообщений в комнате, по достижению которого сообщения передаются в ТМ. Возможные значения: целое число более 1
    - AddCodeSnippetAsText - вставлять содержимое вложений code-snippet в текст реплики. Если false, то будет вставлено имя вложения с указанном языком, но без содержимого. Возможные значения: true или false
- `FileChatRoomSettings` - настройки влияющие на формирование событий передачи файлов
    - SendCodeSnippetAsFile - добавлять содержимое вложений code-snippet как передаваемый файл. Если false, то вложения такого типа будут игнорироваться при формировании события передачи файла. Возможные значения true или false
- `ProcessAttachmentsAsFiles` - обрабатывать вложения для формирования события передачи файлов. Если false, то события передачи файлов формироваться не будут. Возможные значения true или false
- `IdleRoomTimeBeforeSendSec` - время простоя комнаты в секундах с момента получения последнего сообщения перед отправкой сообщений в ТМ (без достижения лимита сообщений). Возможные значения: целое число более 1
- `MessagesCountForSend` - количество сообщений в комнате, по достижению которого сообщения передаются в ТМ. Возможные значения: целое число более 1
- `AzurePortalUrlHost, AzurePortalUrlPath, AzurePortalUrlFragment` – служебные параметры требуемые для корректного формирования адреса страницы пользователя AzureId при его отображении в ТМ
- `PushApiServiceName` – служебный параметр, используемый для корректного формирования события ТМ
- `IdContactType` – служебный параметр, используемый для корректного формирования события ТМ
- `AddUserPrincipalNameAsAuth` – добавлять при формировании события ТМ, PrincipalName пользователя Azure AD как контакт auth, в случае если у пользователя отсутствует адрес электронной почты. Используется вместе только если `ResolveUserDetails` указано в true. Возможные значения true или false

- `ResolveChatMembers` – осуществлять ли при формировании события ТМ получение всех участников отправляемого чата (добавляются в получатели события). Возможные значения true или false
- `ResolveUserDetails` – осуществлять ли доуточнение информации о пользователе. Использовать только если `AddUserPrincipalNameAsAuth` установлено в true. Возможные значения true или false
- `RoomWorkerTaskCount` - служебный параметр. Внутреннее количество обработчиков чат-комнат

6.2.3 GraphApiSettings – Настройки подключения к GraphApi

```
"GraphApiSettings": {
  "TenantId": "00000000-1111-2222-3333-444444444444",
  "ClientId": "AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE",
  "ClientSecret": "xxxxxxxxxyyyyyyyyyyyzzzzzzzzzzzzzzzzz",
  "TokenValidatorMode": 1
},
```

- `TenantId, ClientId, ClientSecret` – учетные данные из Azure AD
- `TokenValidatorMode` – режим проверки токенов безопасности. Токен безопасности – уникальная для каждого получаемого от серверов Microsoft оповещения строка, необходимая для обеспечения дополнительных проверок. Возможно три режима:
  - 0 – не проверять токены
  - 1 – проверять все полученные токены
  - Число больше 1 – проверять только каждый N (указанное число) токен

Параметр `ClientSecret` не хранится на постоянной основе в содержимом settings.json файла. Он используется только для установки нового значения секрета. После своего запуска адаптер сохраняет значение `ClientSecret` в шифрованном хранилище и обнуляет значение параметра в файле конфигурации.

6.2.4 SubscriptionsSettings – Настройки подписок на чаты MsTeams

```
"SubscriptionsSettings": [
  {
    "NotificationUrl": "https://teamsadapter.mycompany.com/api/notification",
    "ChangeType": "created,updated",
    "Resource": "teams/getAllMessages",
    "IncludeResourceData": true,
    "LifetimeMinutes": 15,
    "RenewBeforeExpirationMin": 5,
    "RetryIfErrorSec": 30
  },
  {
    "NotificationUrl": "https://teamsadapter.mycompany.com/api/notification",
    "ChangeType": "created,updated",
    "Resource": "chats/getAllMessages",
    "IncludeResourceData": true,
    "LifetimeMinutes": 15,
    "RenewBeforeExpirationMin": 5,
    "RetryIfErrorSec": 30
  }
],
```

Подписки на ресурсы MS Teams. В каждой подписке значимым является параметр `NotificationUrl` - URL сервиса адаптера, на который сервера Microsoft осуществляют отправку оповещений с репликами чатов. Допускается протокол только https. Адрес обязан заканчиваться на /api/notification.

Остальные параметры служебные и необходимы для корректного функционирования адаптера.

6.2.5 TmConnectionSettings – Настройки подключения к IW TM

```
"TmConnectionSettings": {
  "HostName": "qa-00aa.infowatch.ru",
  "Port": 9101,
  "VendorName": "IW_ADAPTERS",
  "AccessToken": "1eh0z3gn6t7qytzxg50c",
  "ConnectionsCount": 4,
  "OperationTimeoutSec": 20,
  "ReconnectDelaySec": 5,
  "TmPushApiServerCertValidate": true,
  "TmPushApiServerCertHash": null
},
```

- `HostName` - имя хоста TM. Указывается имя либо ip адрес Traffic Monitor
- `Port` – порт PushApi сервиса со стороны TM. По умолчанию 9101. Возможные значения от 1 до 65535
- `VendorName` - компания-разработчик плагина. Используется для авторизации на TM и для связи с лицензией.
- `AccessToken` - токен доступа к TM
- `ConnectionsCount` – количество подключений. Возможные значения: целое число от 1
- `OperationTimeoutSec` – таймаут подключения в секундах
- `ReconnectDelaySec` – время ожидания перед попыткой повторного подключения. Возможные значения: целое число от 1
- `TmPushApiServerCertValidate` - выполнять ли проверку сертификата TM, если он задан. Возможные значения true или false
- `TmPushApiServerCertHash` – хеш серверного сертификата используемого в TM в сервисе PushApi. Используется для увеличения надежности подключения "Адаптер - TM". Если значение не указано, сертификат TM не проверяется адаптером

Параметры `AccessToken` и `TmPushApiServerCertHash` не хранятся на постоянной основе в содержимом файла **settings.json**. Они используются только для установки нового значения.
После своего запуска адаптер сохраняет значения `AccessToken` и `TmPushApiServerCertHash` в шифрованном хранилище и обнуляет значение параметра в файле конфигурации.

6.2.6 HttpProxySettings – Настройки прокси (для исходящих подключений)

```
"HttpProxySettings": {
  "DefaultProxy": true,
  "Address": null,
  "DefaultCredentials": true,
  "Credentials": {
    "UserName": "user",
    "Password": "pswd",
    "Domain": ""
  }
},
```

- `DefaultProxy` - использовать системный прокси адрес. Если true, значение Address игнорируется
- `Address` – адрес прокси сервера
- `DefaultCredentials` – использовать системные учетные данные. Если true, значение Credentials игнорируется
- `Credentials` – учетные данные для прокси сервера

Параметр `Credentials.Password` не хранится на постоянной основе в содержимом **settings.json**. Данный параметр используется только для установки нового значения пароля пользователя прокси-сервера.
После своего запуска адаптер сохраняет значение `Credentials.Password` в шифрованном хранилище и обнуляет значение параметра в файле конфигурации.

6.2.7 DetailManagerSettings – Настройки для дозаполнения событий дополнительными данными

```
"DetailManagerSettings": {
  "ReadAllUsersOnStart": false,
  "MembersCacheItemExpirationMin": 10
},
```

- `ReadAllUsersOnStart` – загружать расширенную информацию о пользователях при старте адаптера. Рекомендуется значение false. Возможные значения true или false
- `MembersCacheItemExpirationMin` - срок жизни записи об участниках группы в кэше (чтобы постоянно не опрашивать MsTeams) в минутах. Возможные значения: целое число от 1

6.2.8 StringTemplateSettings – Настройки шаблонов для автозамены вложений текстом, и генерация имен вложений

```
"StringTemplateSettings": {
  "CodeSnippetFileName": "{2}.{4}",
  "CodeSnippetFileNameTextReplace": "<p>code-snippet: {5}</p>",
  "ReferenceFileNameTextReplace": "<p>File transfer: {3}</p>",
  "MessageReplyTemplate": "<blockquote><p>{6}</p><p>{5}</p></blockquote>",
  "EmbeddedImageFileName": "image-{1:yyyyMMddHHmmssffff}.png",
  "EmbeddedImageFileNameTextReplace": "<p>Image transfer: {4}</p>",
},
```

- `CodeSnippetFileName` – шаблон для имен файлов вложения "Фрагмент-кода"
- `CodeSnippetFileNameTextReplace` - шаблон для текста замены вложения "фрагмент-кода" в реплике
- `ReferenceFileNameTextReplace` - шаблон для текста замены вложения "ссылка на файл" в реплике
- `MessageReplyTemplate` - шаблон для оформления цитируемых сообщений
- `EmbeddedImageFileName` – шаблон для имен файлов внедреных вложений (например, изображения вставленные из буфера обмена)
- `EmbeddedImageFileNameTextReplace` - шаблон для текста замены внедренных вложений в реплике

6.2.9 StatisticsSettings – Настройки счетчиков статистики

```
"StatisticsSettings": {
  "WriteStatisticsToLogMin": 30,
  "NotificationIn": {
    "Enabled": true,
    "InvervalLifeTimeMin": 10,
    "HistoryIntervalCount": 144,
    "ShowCurrentInHistory": false
  },
  "NotificationProcessErr": {
    "Enabled": true,
    "InvervalLifeTimeMin": 10,
    "HistoryIntervalCount": 144,
    "ShowCurrentInHistory": false
  },
  "MessageProcess": {
    "Enabled": true,
    "InvervalLifeTimeMin": 10,
    "HistoryIntervalCount": 144,
    "ShowCurrentInHistory": false
  },
  "MessageProcessError": {
  "MessageText": {
  "MessagesWithAttaches": {
  "FileEventGenerated": {
  "ChatEventGenerated": {
  "EventGenerateError": {
  "Files": {
  "FilesSizeinBytes": {
  "PostedInTm": {
  "PostedInTmError": {
}
```

- `WriteStatisticsToLogMin` - интервал времени в минутах, по истечении которого осуществляется запись значения счетчиков в файл журнала адаптера. Если указано значение 0 - запись в лог не выполняется. Возможные значения: целое число от 0;

Для каждого счетчика доступны следующие параметры:

- `Enabled` - включить счетчик. Возможные значения true или false
- `InvervalLifeTimeMin` - время в минутах, по истечении которого создается исторический интервал. Возможные значения: целое число от 1
- `HistoryIntervalCount` - количество хранимых интервалов истории. Возможные значения: целое число от 1
- `ShowCurrentInHistory` - отображать текущее значение счетчика в истории интервалов. Возможные значения true или false

6.2.10 UISettings - Настройки для доступа к административной панели

```
"UISettings": {
  "Login": null,
  "Password": null,
  "AllowUI": true,
  "AdditionalAllowedSubNets": ""
}
```

- `Login` - логин для доступа в консоль
- `Password` - пароль для доступа в консоль
- `AllowUI` - разрешить доступ к консоли. Возможные значения true или false
- `AdditionalAllowedSubNets` - дополнительно разрешенные адреса для API получения статистики и консоли, задается адресом сети и ее маской. Например: 10.60.0.0/16 или 192.168.12.34/32. Перечисление не поддерживается.

Параметры `Login` и `Password` не хранятся на постоянной основе в содержимом **settings.json**.
Данные параметры используется только для установки нового значения.
После своего запуска адаптер сохраняет значения `Login` и `Password` в шифрованном хранилище и обнуляет значения параметров в файле конфигурации.

7 Сбор статистики адаптером

В процессе своей работы адаптер собирает и считает различные данные. Доступны следующие счетчики:

- `NotificationIn` - количество входящих уведомлений, полученных от серверов Microsoft. В одном уведомлении может быть более 1 реплики чата;
- `NotificationProcessErr` - количество ошибок при обработке уведомлений;
- `MessageProcess` - суммарное количество реплик чата, полученных из уведомлений;
- `MessageProcessError` - количество ошибок обработки реплик из уведомлений;
- `MessageText` - количество реплик чата с текстовым содержимым (по факту все реплики, т.к., например, передача файла также формирует текстовую реплику с именем передаваемого файла);
- `MessagesWithAttaches` - количество реплик с вложением/вложениями. В одной реплике может быть более одного вложения, но при этом счетчик увеличится на 1. Также не все вложения отправляются как файлы, но счетчик все равно увеличится;
- `FileEventGenerated` - количество сгенерированных событий передачи файлов. В одном событии может быть более одного файла;
- `Files` - общее количество файлов в событиях передачи файлов;
- `FilesSizeinBytes` - общий размер файлов в байтах, которые добавлены в события передачи файлов;
- `ChatEventGenerated` - количество сгенерированных событий общения в чате;
- `EventGenerateError` - количество ошибок генерирации события;
- `PostedInTm` - количество событий, успешно отправленных в TM;
- `PostedInTmError` - количество ошибок при отправке в TM;

Значения счетчиков активны только на момент работы адаптера, и при его перезагрузке счетчики обнуляются.

Настройка счетчиков статистики осуществляется в файле **settings.json**, раздел `StatisticsSettings`.

Посмотреть результаты параметры счетчиков можно двумя способами:

- в журнале работы адаптера
- через запрос к API статистики адаптера

Журнал работы адаптера по умолчанию располагается в папке установки, подпапка `Logs`. В текстовых файлах журнала записи счетчиков статистики выглядят следующим образом:

```
2021-11-01 13:22:58.496 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'NotificationIn': 191
2021-11-01 13:22:58.497 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'NotificationProcessErr': 165
2021-11-01 13:22:58.497 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'MessageProcess': 17
2021-11-01 13:22:58.497 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'MessageProcessError': 0
2021-11-01 13:22:58.497 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
```

```
'MessageText': 17
2021-11-01 13:22:58.497 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'MessagesWithAttaches': 1
2021-11-01 13:22:58.497 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'FileEventGenerated': 1
2021-11-01 13:22:58.497 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'ChatEventGenerated': 3
2021-11-01 13:22:58.498 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'EventGenerateError': 0
2021-11-01 13:22:58.498 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter 'Files': 1
2021-11-01 13:22:58.498 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'FilesSizeinBytes': 52489
2021-11-01 13:22:58.498 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter 'PostedInTm':
4
2021-11-01 13:22:58.498 +03:00 [INFOR]:46
[InfoWatch.Adapter.Statistics.StatisticsManager] Counter
'PostedInTmError': 0
```

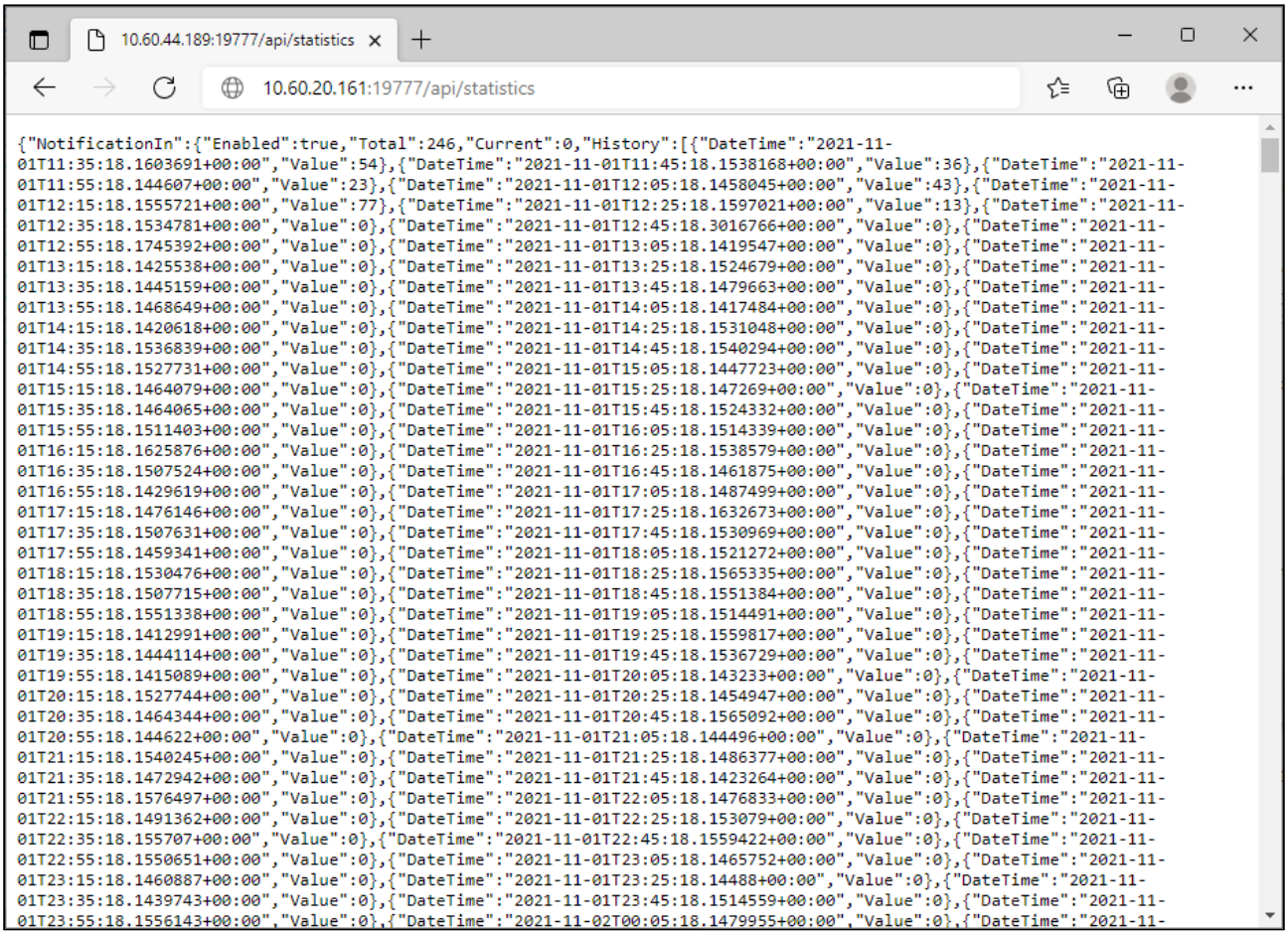
После добавления записи счетчика в журнал значение счетчика обнуляется и считается заново.

API адаптера по получению статистики располагается по адресу http://localhost:19777/api/statistics либо http://ip:port/api/statistics , где ip и порт - аналогичные указанные при установке адаптера (также их можно посмотреть в файле конфигурации **appsettings.json**, параметр `urls`)

По умолчанию страница API получения статистики доступна только для локальных вызовов.

В файле конфигурации **settings.json**, раздел `UISettings` , можно указать дополнительную подсеть, адресам которой будет разрешен доступ к API статистики и консоли.

Если перейти в браузере по адресу API откроется страница, в которой содержится json-файл с данными счетчиков статистики.



{"NotificationIn":{"Enabled":true,"Total":246,"Current":0,"History":[{"DateTime":"2021-11-01T11:35:18.1603691+00:00","Value":54},{"DateTime":"2021-11-01T11:45:18.1538168+00:00","Value":36},{"DateTime":"2021-11-01T11:55:18.144607+00:00","Value":23},{"DateTime":"2021-11-01T12:05:18.1458045+00:00","Value":43},{"DateTime":"2021-11-01T12:15:18.1555721+00:00","Value":77},{"DateTime":"2021-11-01T12:25:18.1597021+00:00","Value":13},{"DateTime":"2021-11-01T12:35:18.1534781+00:00","Value":0},{"DateTime":"2021-11-01T12:45:18.3016766+00:00","Value":0},{"DateTime":"2021-11-01T12:55:18.1745392+00:00","Value":0},{"DateTime":"2021-11-01T13:05:18.1419547+00:00","Value":0},{"DateTime":"2021-11-01T13:15:18.1425538+00:00","Value":0},{"DateTime":"2021-11-01T13:25:18.1524679+00:00","Value":0},{"DateTime":"2021-11-01T13:35:18.1445159+00:00","Value":0},{"DateTime":"2021-11-01T13:45:18.1479663+00:00","Value":0},{"DateTime":"2021-11-01T13:55:18.1468649+00:00","Value":0},{"DateTime":"2021-11-01T14:05:18.1417484+00:00","Value":0},{"DateTime":"2021-11-01T14:15:18.1420618+00:00","Value":0},{"DateTime":"2021-11-01T14:25:18.1531048+00:00","Value":0},{"DateTime":"2021-11-01T14:35:18.1536839+00:00","Value":0},{"DateTime":"2021-11-01T14:45:18.1540294+00:00","Value":0},{"DateTime":"2021-11-01T14:55:18.1527731+00:00","Value":0},{"DateTime":"2021-11-01T15:05:18.1447723+00:00","Value":0},{"DateTime":"2021-11-01T15:15:18.1464079+00:00","Value":0},{"DateTime":"2021-11-01T15:25:18.147269+00:00","Value":0},{"DateTime":"2021-11-01T15:35:18.1464065+00:00","Value":0},{"DateTime":"2021-11-01T15:45:18.1524332+00:00","Value":0},{"DateTime":"2021-11-01T15:55:18.1511403+00:00","Value":0},{"DateTime":"2021-11-01T16:05:18.1514339+00:00","Value":0},{"DateTime":"2021-11-01T16:15:18.1625876+00:00","Value":0},{"DateTime":"2021-11-01T16:25:18.1538579+00:00","Value":0},{"DateTime":"2021-11-01T16:35:18.1507524+00:00","Value":0},{"DateTime":"2021-11-01T16:45:18.1461875+00:00","Value":0},{"DateTime":"2021-11-01T16:55:18.1429619+00:00","Value":0},{"DateTime":"2021-11-01T17:05:18.1487499+00:00","Value":0},{"DateTime":"2021-11-01T17:15:18.1476146+00:00","Value":0},{"DateTime":"2021-11-01T17:25:18.1632673+00:00","Value":0},{"DateTime":"2021-11-01T17:35:18.1507631+00:00","Value":0},{"DateTime":"2021-11-01T17:45:18.1530969+00:00","Value":0},{"DateTime":"2021-11-01T17:55:18.1459341+00:00","Value":0},{"DateTime":"2021-11-01T18:05:18.1521272+00:00","Value":0},{"DateTime":"2021-11-01T18:15:18.1530476+00:00","Value":0},{"DateTime":"2021-11-01T18:25:18.1565335+00:00","Value":0},{"DateTime":"2021-11-01T18:35:18.1507715+00:00","Value":0},{"DateTime":"2021-11-01T18:45:18.1551384+00:00","Value":0},{"DateTime":"2021-11-01T18:55:18.1551338+00:00","Value":0},{"DateTime":"2021-11-01T19:05:18.1514491+00:00","Value":0},{"DateTime":"2021-11-01T19:15:18.1412991+00:00","Value":0},{"DateTime":"2021-11-01T19:25:18.1559817+00:00","Value":0},{"DateTime":"2021-11-01T19:35:18.1444114+00:00","Value":0},{"DateTime":"2021-11-01T19:45:18.1536729+00:00","Value":0},{"DateTime":"2021-11-01T19:55:18.1415089+00:00","Value":0},{"DateTime":"2021-11-01T20:05:18.143233+00:00","Value":0},{"DateTime":"2021-11-01T20:15:18.1527744+00:00","Value":0},{"DateTime":"2021-11-01T20:25:18.1454947+00:00","Value":0},{"DateTime":"2021-11-01T20:35:18.1464344+00:00","Value":0},{"DateTime":"2021-11-01T20:45:18.1565092+00:00","Value":0},{"DateTime":"2021-11-01T20:55:18.144622+00:00","Value":0},{"DateTime":"2021-11-01T21:05:18.144496+00:00","Value":0},{"DateTime":"2021-11-01T21:15:18.1540245+00:00","Value":0},{"DateTime":"2021-11-01T21:25:18.1486377+00:00","Value":0},{"DateTime":"2021-11-01T21:35:18.1472942+00:00","Value":0},{"DateTime":"2021-11-01T21:45:18.1423264+00:00","Value":0},{"DateTime":"2021-11-01T21:55:18.1576497+00:00","Value":0},{"DateTime":"2021-11-01T22:05:18.1476833+00:00","Value":0},{"DateTime":"2021-11-01T22:15:18.1491362+00:00","Value":0},{"DateTime":"2021-11-01T22:25:18.153079+00:00","Value":0},{"DateTime":"2021-11-01T22:35:18.155707+00:00","Value":0},{"DateTime":"2021-11-01T22:45:18.1559422+00:00","Value":0},{"DateTime":"2021-11-01T22:55:18.1550651+00:00","Value":0},{"DateTime":"2021-11-01T23:05:18.1465752+00:00","Value":0},{"DateTime":"2021-11-01T23:15:18.1460887+00:00","Value":0},{"DateTime":"2021-11-01T23:25:18.14488+00:00","Value":0},{"DateTime":"2021-11-01T23:35:18.1439743+00:00","Value":0},{"DateTime":"2021-11-01T23:45:18.1514559+00:00","Value":0},{"DateTime":"2021-11-01T23:55:18.1556143+00:00","Value":0},{"DateTime":"2021-11-02T00:05:18.1479955+00:00","Value":0},{"DateTime":"2021-11-

Структура данного json-файл выглядит следующим образом:



где каждый счетчик содержит следующие параметры:

- `Enabled` - активен ли указанный счетчик;
- `Total` - общее значение счетчика за время работы адаптера;
- `Current` - текущее значение счетчика, на момент формирования Json;
- `History` - данные исторических интервалов. Период формирования интервала, а также их количество настраиваются в настройках счетчика. При формировании интервала указывается время его создания, в качестве значения берется значение параметра `Current`. После формирования интервала параметр `Current` обнуляется.

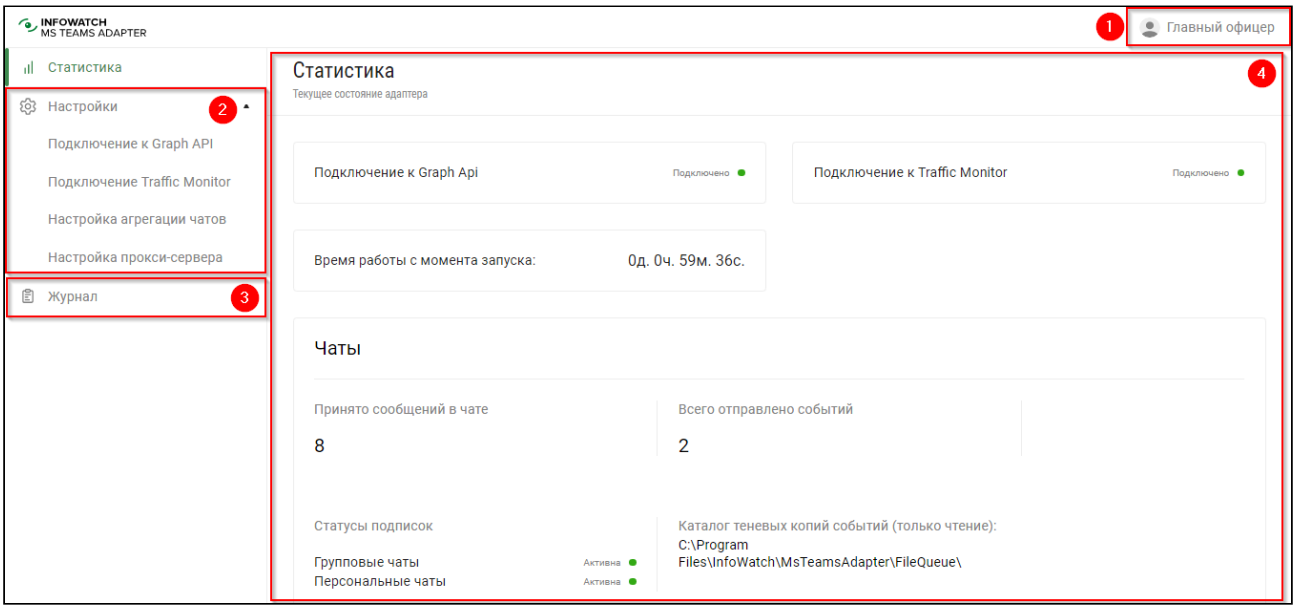
8 Работа в консоли управления адаптера

В этом разделе:

- Интерфейс адаптера;
- Общие действия;
- Статистика;
- Подключение к Grath API (MS Teams);
- Подключение к Traffic Monitor;
- Настройка агрегации чатов;
- Настройка прокси-сервера

8.1 Интерфейс адаптера

Окно интерфейса адаптера содержит несколько областей с настройками и данными (на примере раздела **Статистика**).



Элементы окна:

Номер на схеме	Элемент окна	Описание элемента
1	Меню пользователя	Пользовательское меню, в котором вы можете: • сменить пароль (см. "Смена пароля администратора"); • выбрать язык интерфейса : *Русский* или *Английский*; • узнать контактные данные компании InfoWatch и службы поддержки; • выйти из консоли управления адаптера.

Номер на схеме	Элемент окна	Описание элемента
2	Настройки адаптера	Сетевые настройки адаптера для соединения: • с сервером MS Teams; • с сервером Traffic Monitor; • с прокси-сервером.
3	Журнал адаптера	Записи лог-файла адаптера (см. "Просмотр системного журнала")
4	Статистика адаптера	Сведения по полученным из MS Teams данным и отправленным в Traffic Monitor событиям

8.2 Общие действия

В этом разделе:

- Вход в консоль управления
- Смена пароля администратора
- Просмотр системного журнала

8.2.1 Вход в консоль управления

Для доступа в консоль управления адаптера перейдите по адресу http://localhost:19777/Admin/.

Важно!

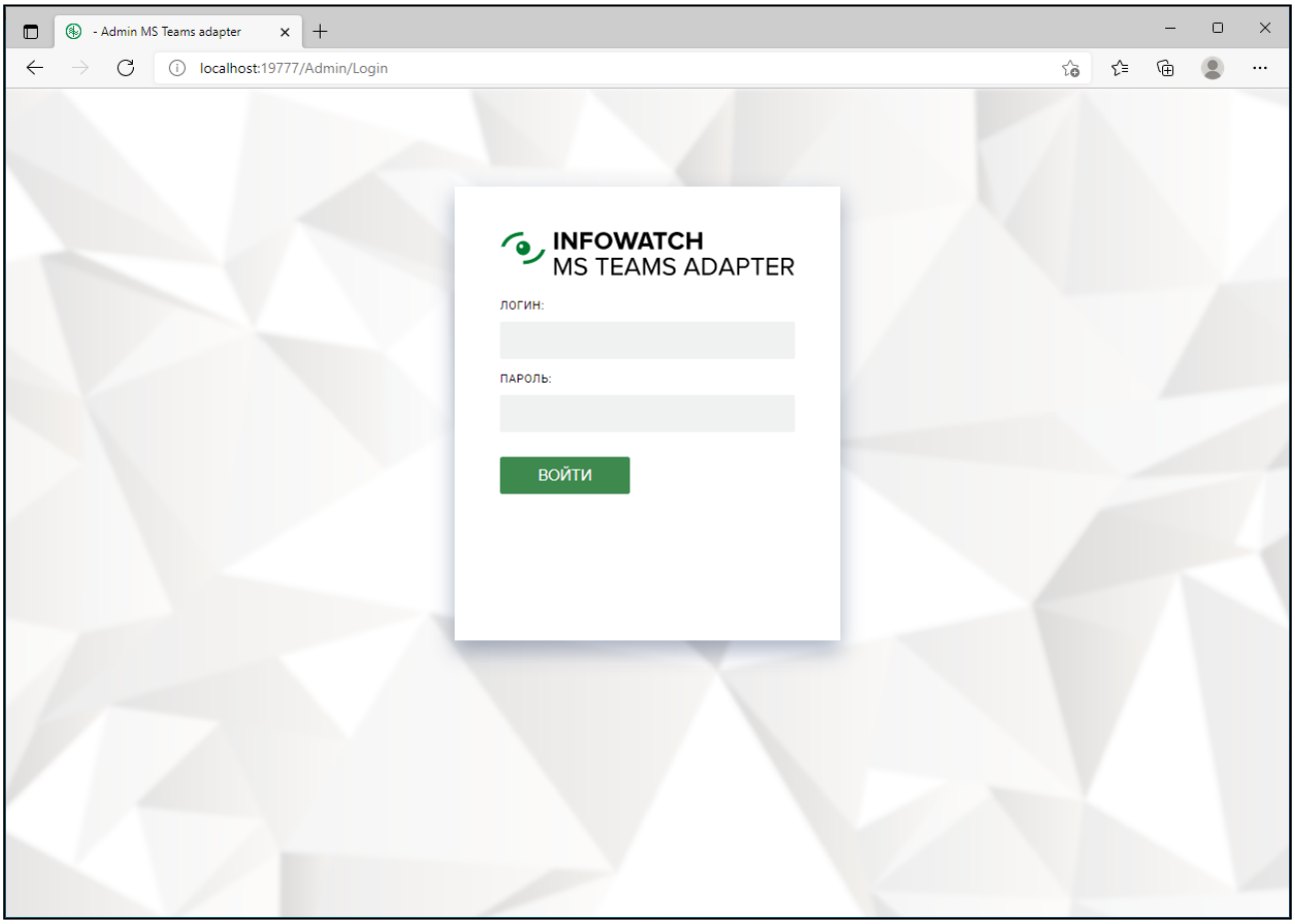
Если в процессе установки порт прослушивания веб-сервера был указан отличным от порта по умолчанию (19777), то укажите соответствующий номер порта в адресной строке.

Доступ к панели доступен только с компьютера, на который производилась установка адаптера. Во всех остальных случаях будет ответ "*Only local call*":



Чтобы открыть доступ с других компьютеров к API статистики и консоли управления, необходимо указать дополнительную подсеть в файле конфигурации settings.json, раздел UISettings.

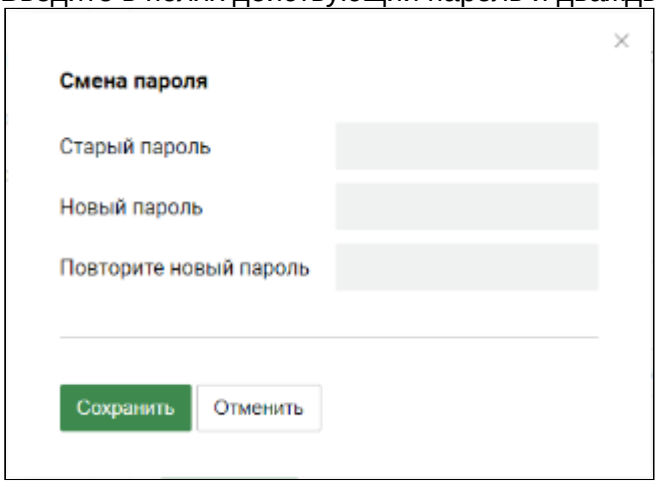
Если обращение осуществляется с локального компьютера или разрешенного в файле конфигурации адреса, то будет отображена страница авторизации в консоль управления. Введите учетные данные администратора, указанные при установке на шаге 8.



8.2.2 Смена пароля администратора

Чтобы сменить пароль по умолчанию или скомпрометированный пароль:

1. Перейдите в **Меню пользователя - > Смена пароля**.
2. Введите в полях действующий пароль и дважды новый пароль.

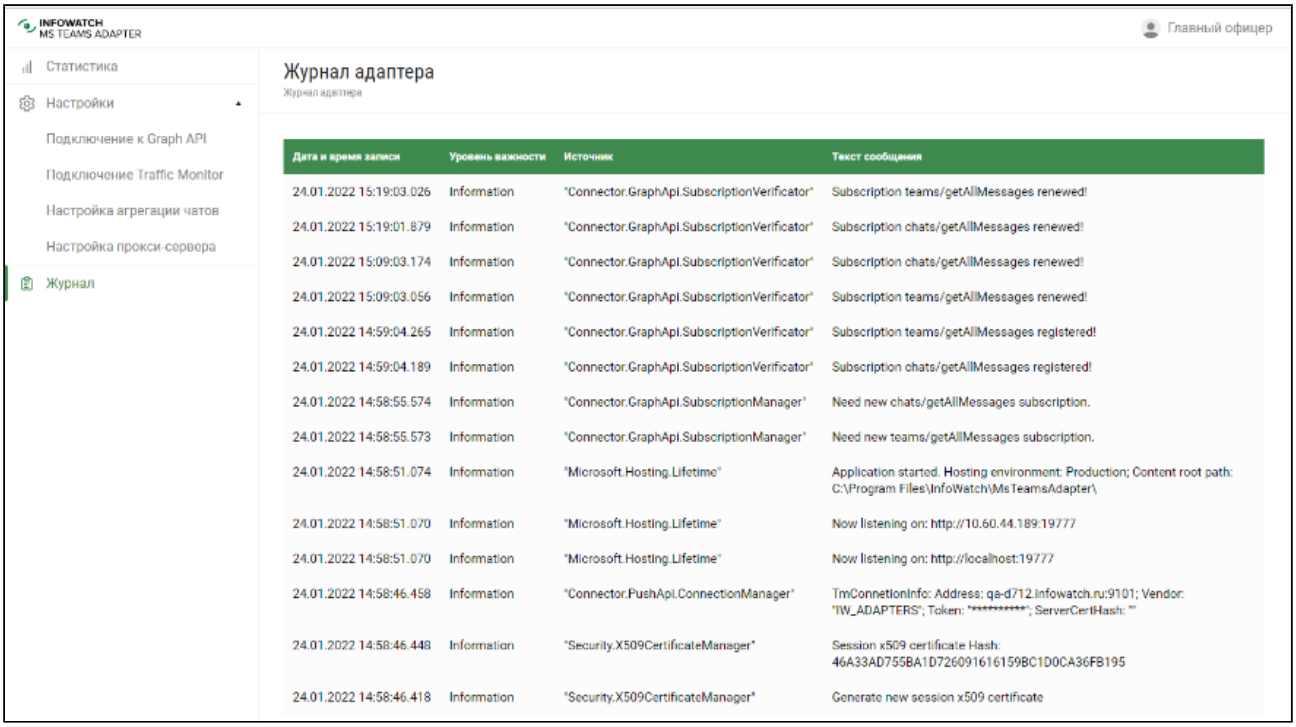


3. Нажмите **Сохранить**.

4. Выйдите и заново Войдите в консоль управления под новыми учетными данными.

8.2.3 Просмотр системного журнала

В разделе Журнал адаптера собираются системные логи адаптера. Они могут быть предоставлены службе технической поддержки для решения проблем, сбоев в работе и тд. На странице отображаются последние 100 записей лога.



8.3 Статистика

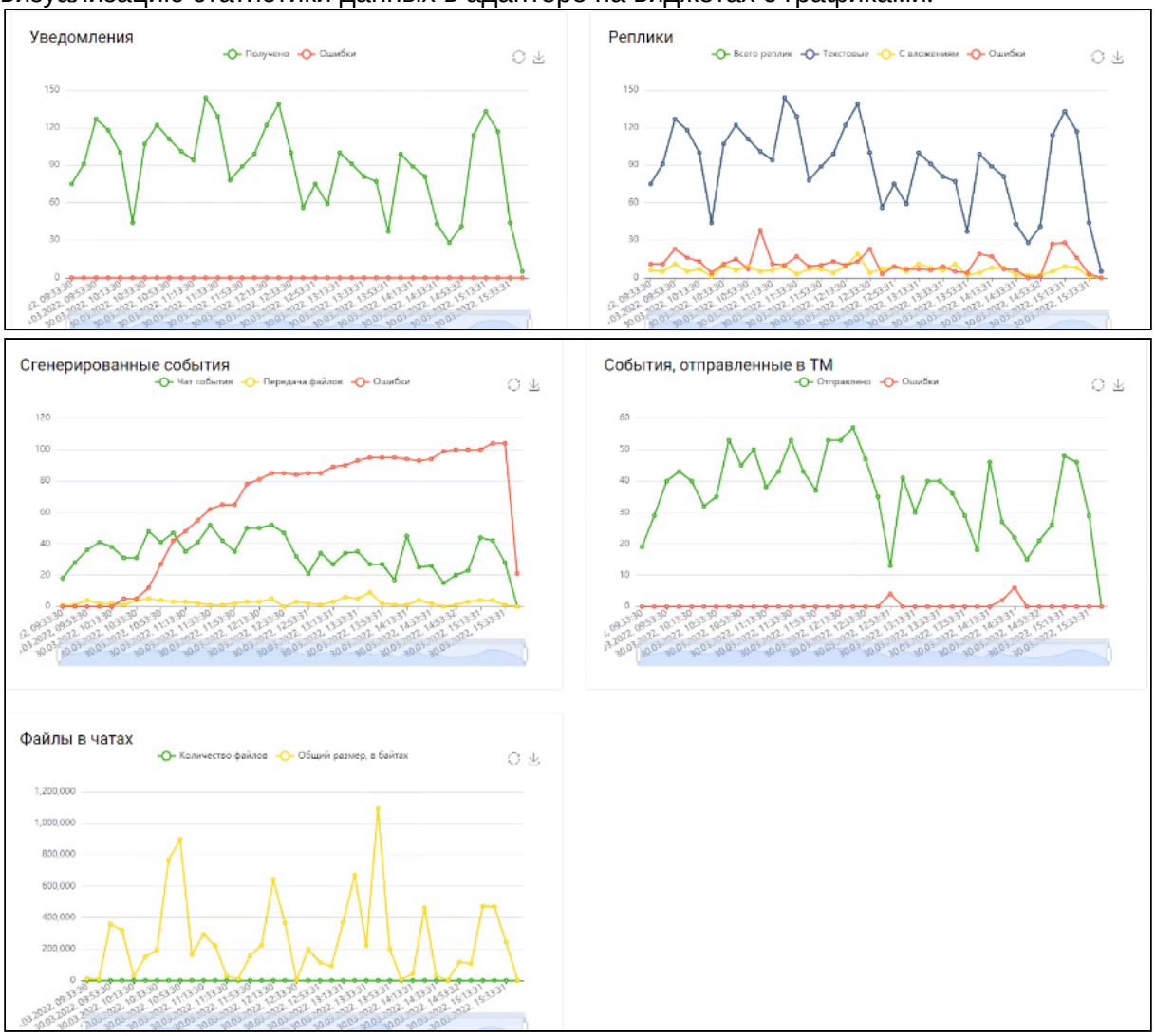
На главной странице **Статистика** отображаются:

- статусы подключения к приемнику и источнику данных. Необходимо убедиться, чтобы статусы были в состоянии **Подключено** .

> **Важно!**
>
> Если подключение не устанавливается, необходимо проверить логи. Такая ситуация возможна, если данные Azure AD, настройки прокси-сервера или для доступа к TM были введены с ошибкой на этапе установки.

- время работы адаптера с момента запуска;
- количество принятых реплик;
- количество отправленных событий в TM;
- состояние подписок;
- адрес каталога, где хранятся теневые копии событий (только для чтения);

- визуализацию статистики данных в адаптере на виджетах с графиками:



По умолчанию горизонтальная шкала графиков разбита на 144 интервала длительностью 10 минут каждый, что в сумме дает 24 часа. Такова история отображения статистики.

На виджете можно:

-  - обновить данные отображения;
-  - выгрузить данные в виде файла .png;
- уточнить данные, наведя указатель мыши на график;
- изменить масштаб графиков.

Виджеты статистики отображают количество:

Уведомления	• входящих уведомлений; • ошибок при обработке уведомлений.
Реплики	• реплик из уведомлений; • ошибок обработки реплик; • реплик с текстовым содержимым;

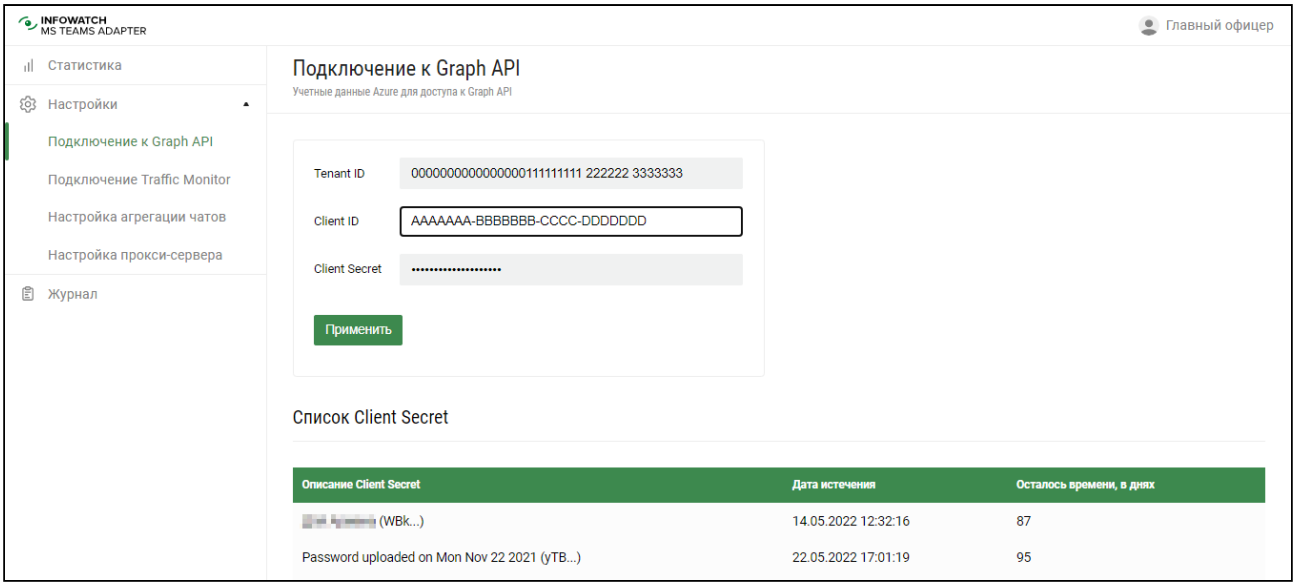
	• реплик с вложениями.
Сгенерированные события	• сгенерированных событий передачи файлов; • сгенерированных событий общения в чате; • ошибок генерации события.
События, отправленные в TM	• событий, успешно отправленных в TM; • ошибок при отправке в TM.
Файлы в чатах	файлов в событиях и их размер в байтах

Адаптер передает в TM события отправки сообщений с датой отправки, начиная с момента подключения адаптера к MS Teams.

> **Примечание:**
>
> Возможна ситуация, когда адаптер получил данные не обо всех участниках чата. В событиях чата, полученных адаптером, будут только те пользователи, которые непосредственно писали сообщения в чат.
>
> Если адаптер не получил передаваемый файл (например, его передал участник чата, который зарегистрирован в Azure AD другой компании), то в логи будет добавлена запись с типом `warning` об этом, а адаптер продолжит обработку трафика из этого чата.

8.4 Подключение к Grath API (MS Teams)

На странице указаны учетные данные Azure, необходимые для доступа к Graph API. Если учетные данные корректны и верны, отображается список известных секретов, имеющих ограниченный срок действия, для указанного ClientId и количество дней до их истечения. Если срок действия секрета истек, необходимо получить новый в Azure.



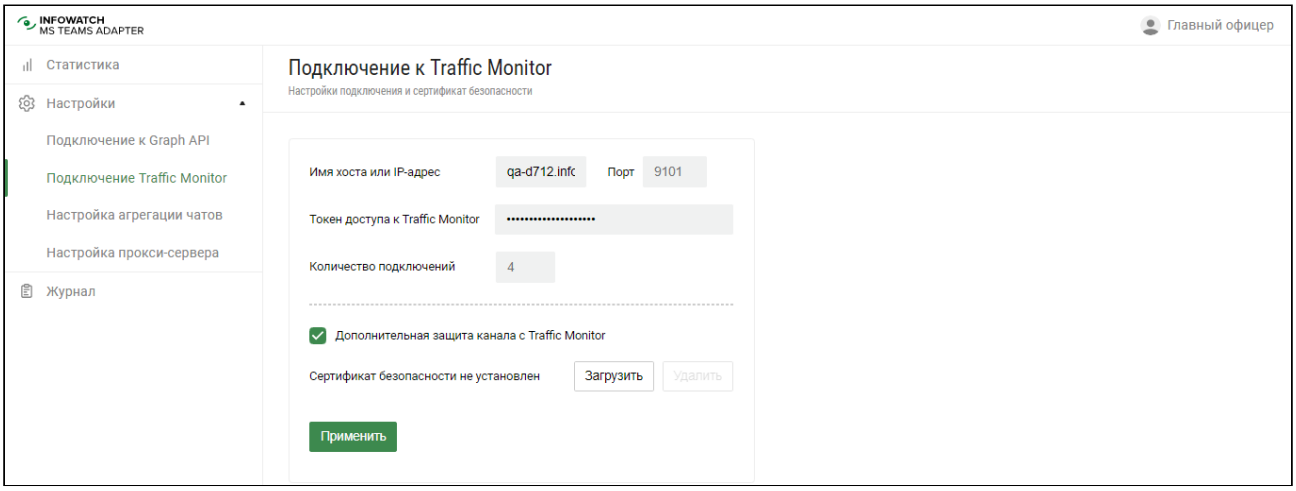
Если учетные данные в Azure изменились, введите новые данные в поля Tenant ID, Client ID, Client Secret и нажмите **Применить**.

8.5 Подключение к Traffic Monitor

На странице указаны учетные данные для доступа к Infowatch Traffic Monitor, количество подключений (в диапазоне от 1 до 32). Для увеличения надежности подключения можно указать сертификат открытого ключа формата .pem, .cer, .crt (на выбор), используемого на стороне ТМ.

Если установить флаг **Дополнительная защита канала с Traffic Monitor** , не указывая при этом сертификат, то он сертификат ТМ не будет проверяться адаптером.

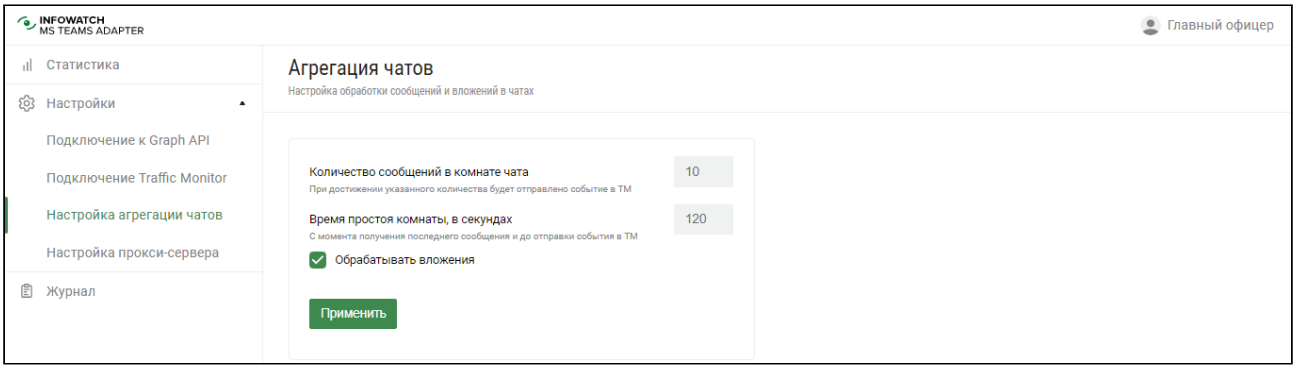
Если установить флаг **Дополнительная защита канала с Traffic Monitor** и выбрать сертификат, то в процессе инициализации TLS-канала при подключении адаптера к ТМ будет проверен сертификат. В случае отличия связь установлена не будет.



8.6 Настройка агрегации чатов

На странице содержатся настройки обработки чатов. Можно задать следующие параметры:

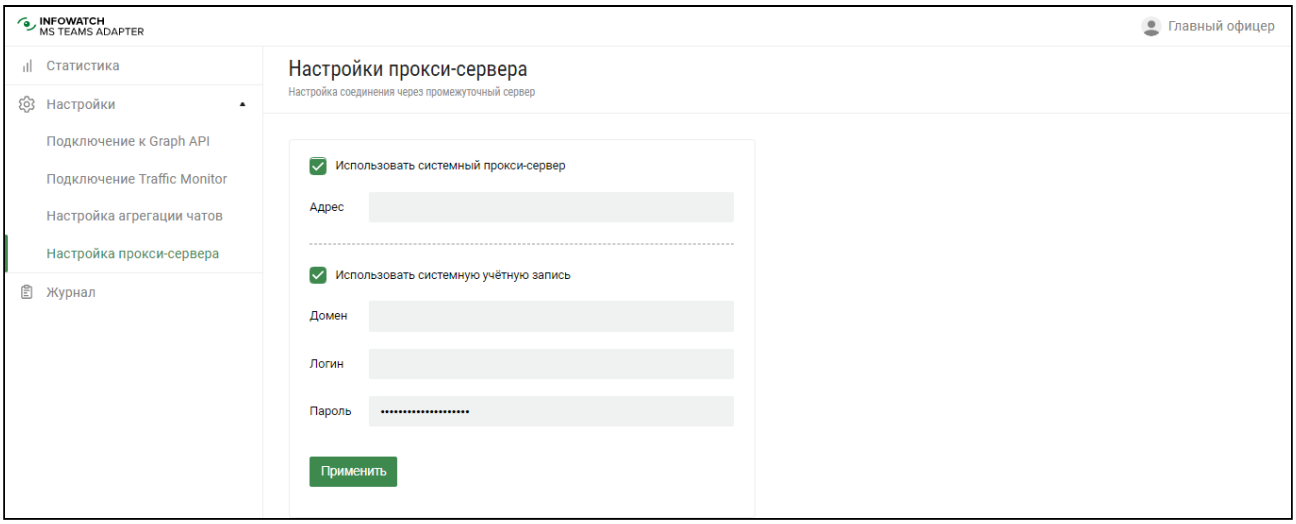
- **Количество сообщений в комнате** - количество сообщений, по достижению которого сообщения одной комнаты передаются в ТМ. Указывается значение от 1 до 256;
- **Время простоя комнаты** в секундах - время с момента получения последнего сообщения перед отправкой сообщений в ТМ (без достижения лимита сообщений). Указывается значение от 1 до 3600;
- **Обрабатывать вложения** - флаг для формирования события передачи файлов. Если не установлен, события передачи файлов формироваться не будут.



8.7 Настройка прокси-сервера

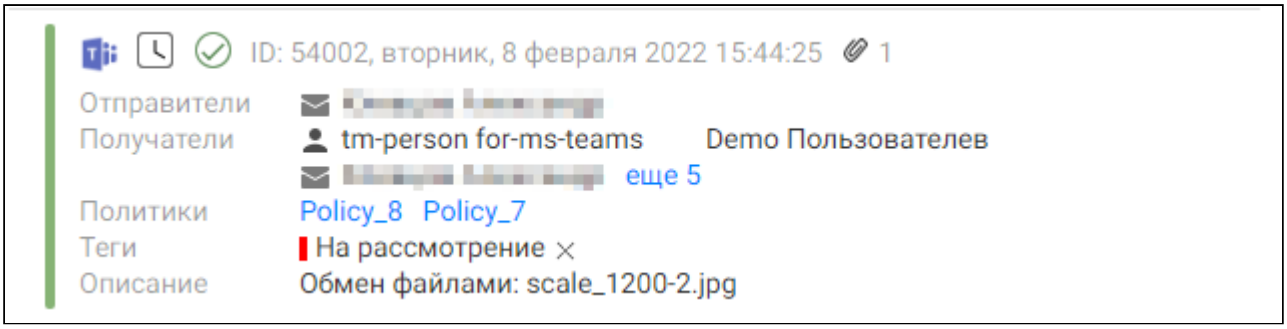
На странице указываются настройки прокси-сервера, используемые адаптером:

- Адрес прокси-сервера вида http://proxyhost:port
  Если установлен флаг **Использовать системный прокси-сервер**, значение этого адреса будет проигнорировано.
- Учетные данные прокси-сервера: домен, логин, пароль.
  Если установлен флаг **Использовать системную учётную запись**, эти данные будут проигнорированы.

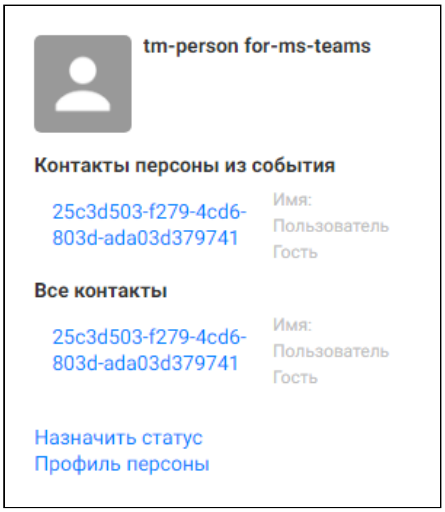


9 Получение событий в Traffic Monitor

Адаптер отправляет сообщения личных и групповых чатов на анализ в Traffic Monitor при наличии установленной лицензии, начиная с момента подключения адаптера к MS Teams. В карточке события могут быть указаны все извлеченные при перехвате контакты: ФИО пользователя, адрес электронной почты и тд.



В случае отсутствия адреса электронной почты, например, если участвует гостевой пользователь MS Teams, то будет указан контакт Аккаунт в Azure AD.



Если во время отправки событий происходили сбои связи с сервером Traffic Monitor, адаптер будет досылать события после установления связи. События за период потери связи с MS Teams (Grath API) досланы не будут.

Важно!

Если на компьютере с установленным агентом DM настроено правило запрета использования приложения Skype, веб-версия MS Teams тоже будет недоступна.