

Установка и настройка Indeed AM Log Server с хранилищем в SysLog

Информация

Файлы для Indeed AM Log Server расположены: *indeed AM\Indeed AM Log Server*
\<Номер версии>

- **IndeedAM.LogServer-x64.ru-ru.msi** - Пакет для установки Indeed Log Server.
- **IndeedAM.Server.EventLog-x64.ru-ru.msi** - Пакет для создания необходимой структуры журнала в Windows EventLog.

Информация

Indeed AM Admin Console не позволяет читать события из sysLog сервера. Для отображения журнала в Admin Console необходимо наличие своей БД (SQL-сервер или EventLog) для хранения событий Indeed AM LogServer.

Установка

1. Выполнить установку Indeed AM Log Server через запуск инсталлятора **Indeed.LogServer-x64.ru-ru.msi**.

2. Добавить привязку **https** в настройка **Default Web Site** в IIS Manager.

 Информация

Indeed Log Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для logserver.

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Установка sysLog сервера.

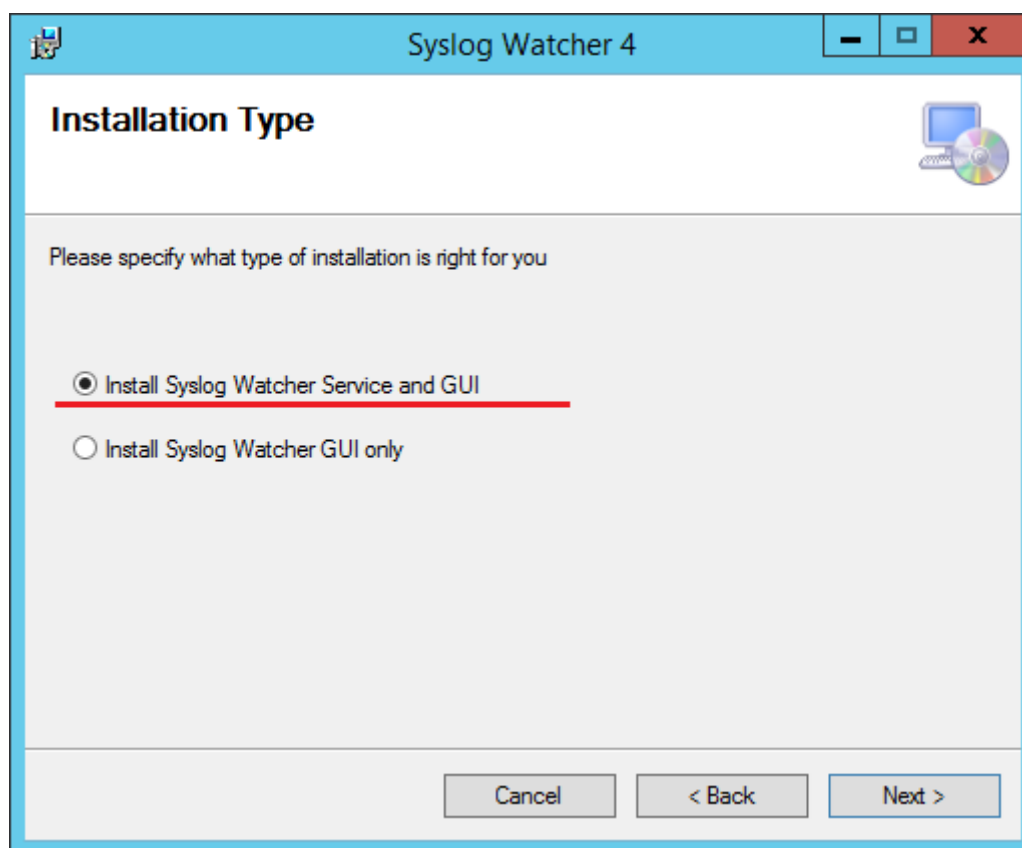
 Информация

Indeed AM Log Server поддерживает формат sys-log, вы можете использовать любой сервер, работающий с данным форматом. В качестве примера далее рассмотрена настройка sys-log сервера **Syslog Watcher v4.8.6**.

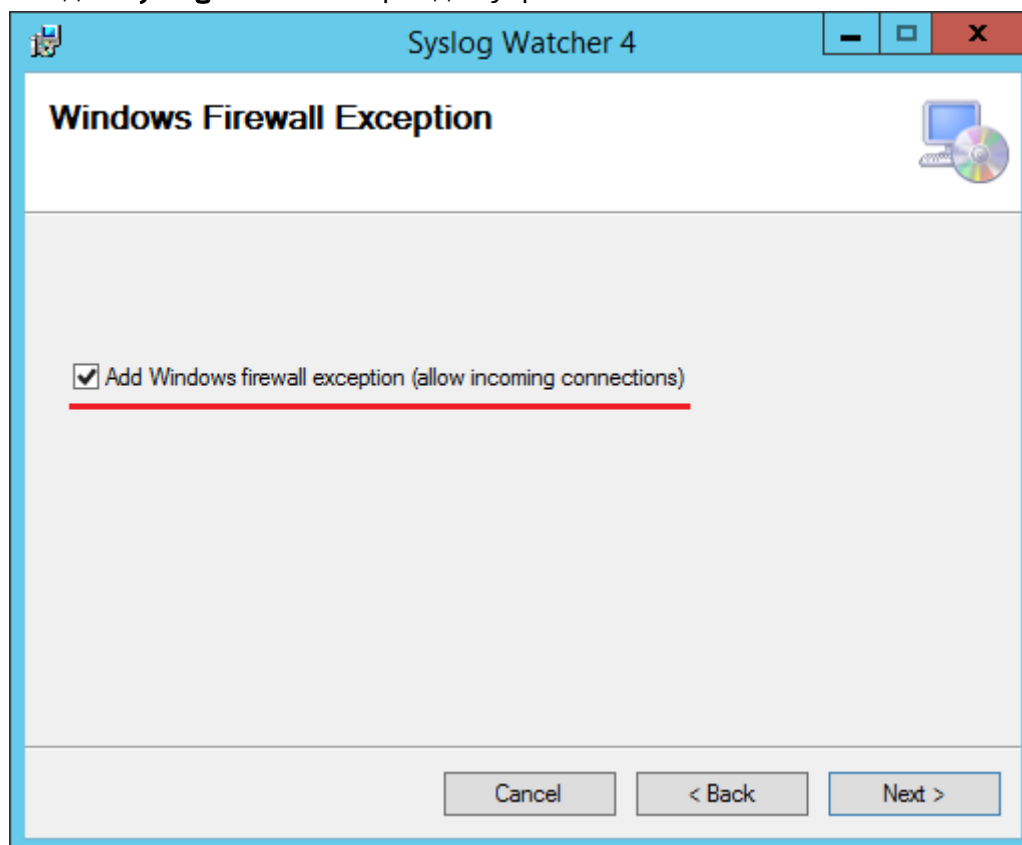
Вы можете скачать утилиту на официальном сайте <https://syslogwatcher.com>

1. Запустите установочный файл **SyslogWatcherSetup-*.*.win32.msi**.
2. В окне "**License Agreement**" примите лицензионное соглашение.

3. В окне "Installation Type" выбрать тип установки "Install Syslog Watcher Service and GUI".



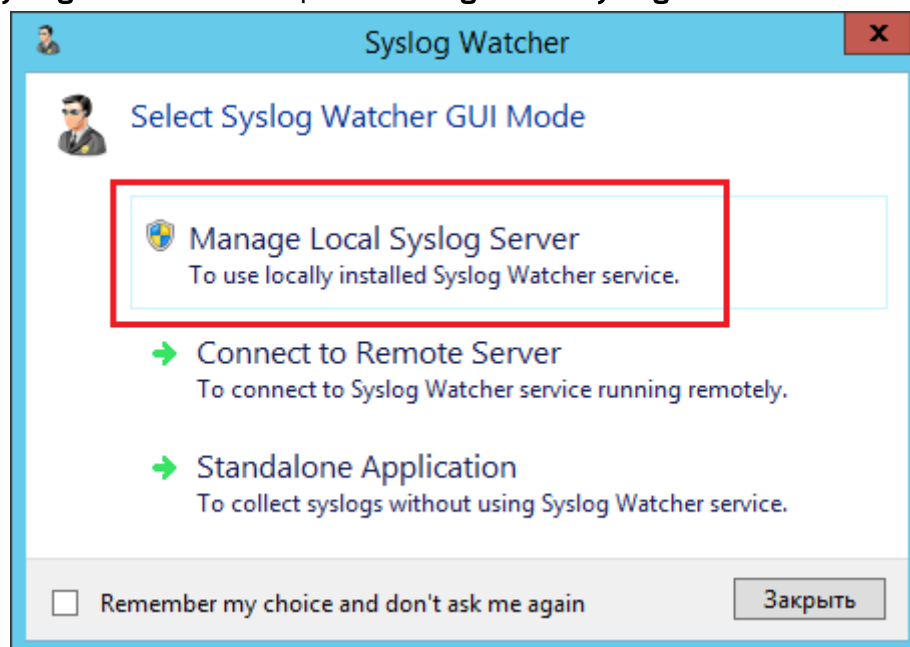
4. В окне "Select installation Folder" выбрать путь установки для **sys-log сервера**.
5. В окне "Windows Firewall Exception" разрешить добавление правила на все входящие соединения для **Syslog Watcher** в брандмауэр **Windows**.



6. В окне "Confirm Installation" нажать "Next" для подтверждения установки.
7. Дождаться завершения установки сервера.

Настройка sysLog сервера.

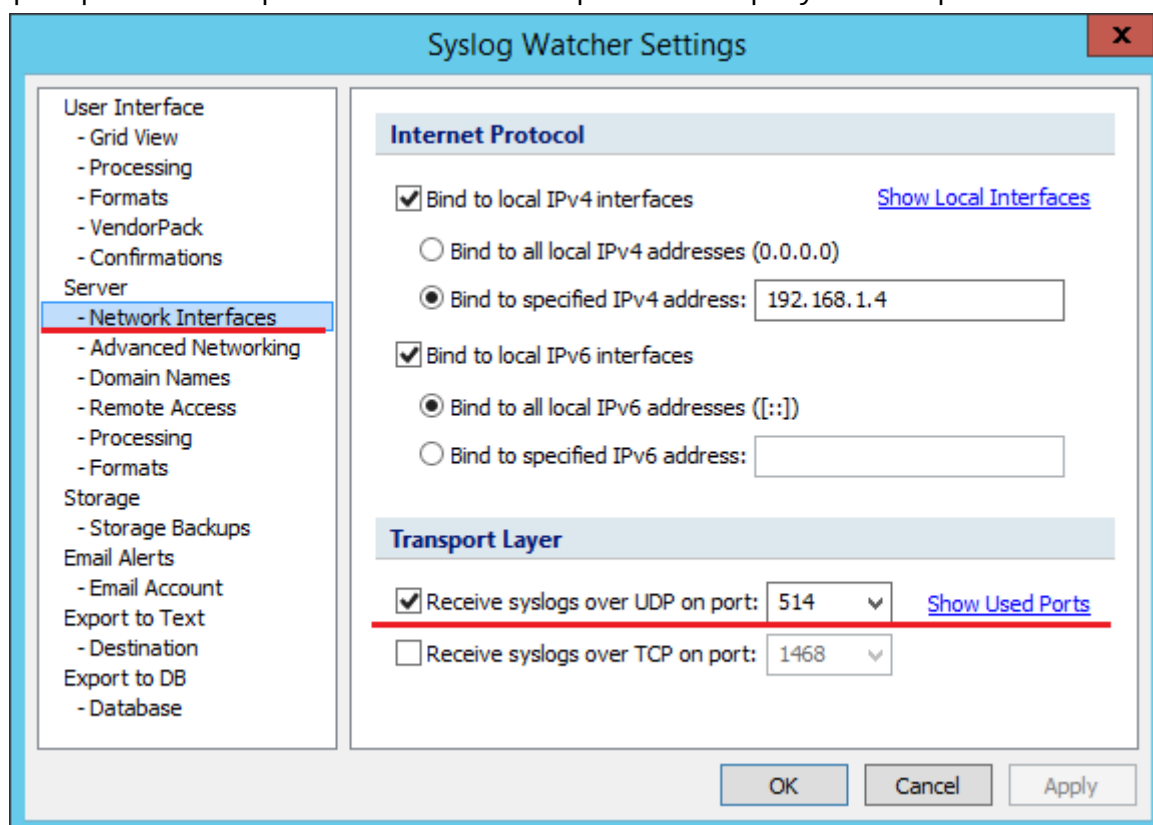
1. Запустите Syslog Watcher и выберите "Manage Local Syslog Server".



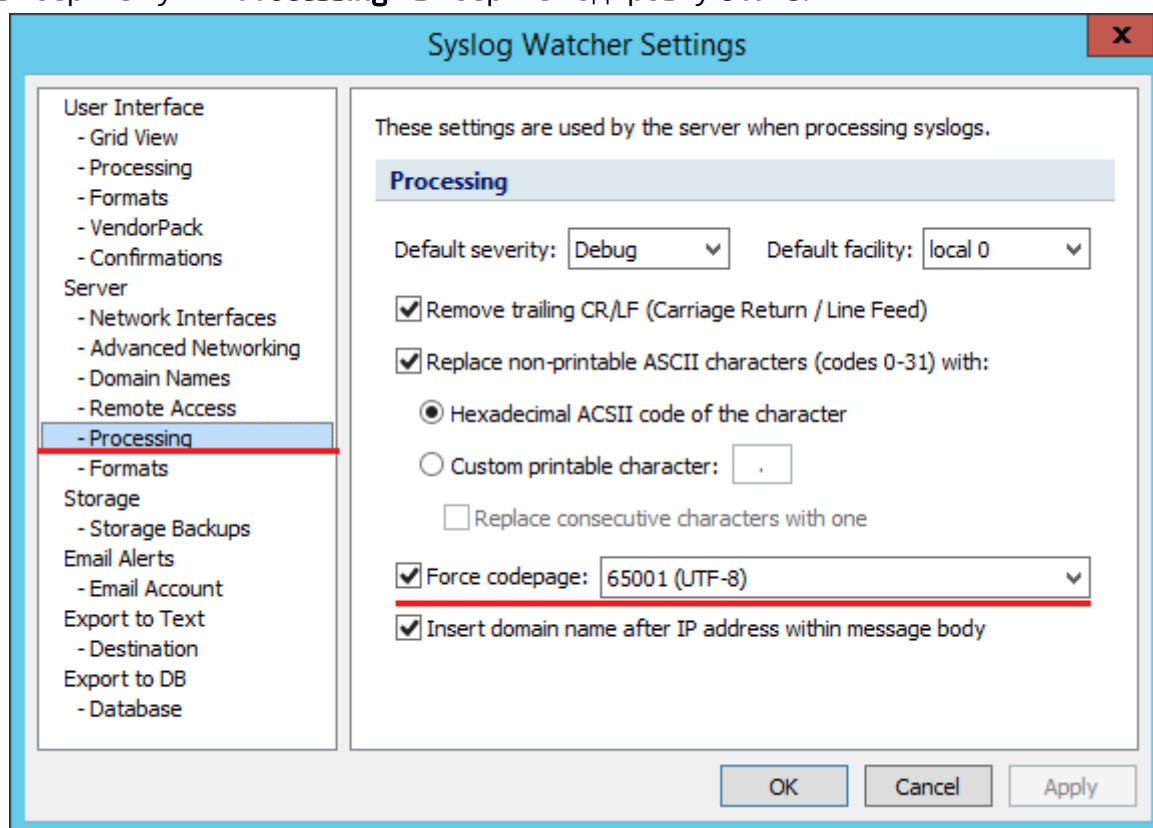
2. Нажмите "**Settings**" в верхнем меню программы.

a. Выберите пункт "**Network Interfaces**".

b. Проверьте что выбрано использование протокола udp и указан порт.



c. Выберите пункт "**Processing**". Выберите кодировку **UTF-8**.



Редактирование конфигурационного файла.

1. Откройте конфигурационный файл **sampleSyslog.config** (C:\inetpub\wwwroot\ils\targetConfigs\sampleSyslog.config).
2. Для тега **"Settings"** укажите данные для подключения к **sys-log**.

Пример настройки для Syslog Watcher

```
<Settings HostName="localhost" Port="514" Protocol="udp" />
```

3. Откройте конфигурационный файл **clientApps.config** (C:\inetpub\wwwroot\ils\clientApps.config).
4. Для блока с **"Application Id="ea"** в тегах **TargetId** и **ReadTargetId** указать **sampleSyslog**.



Информация

В тегах **ReadTargetId** указывается идентификатор хранилища откуда будет осуществляться чтение событий.

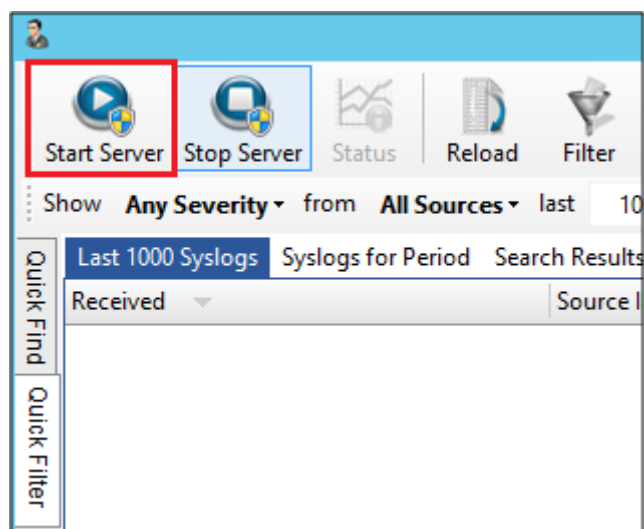
В блоке **WriteTargets**, в тегах **TargetId**, указывается идентификатор хранилища куда будет осуществляться запись событий.

Идентификаторы заданы в теге **<Targets>...</Targets>**, конфигурационные файлы для каждого типа находится в папке **targetConfigs** с соответствующим именем.

Пример

```
<Application Id="ea" SchemaId="eaSchema">
  <ReadTargetId>sampleSyslog</ReadTargetId>
  <WriteTargets>
    <TargetId>sampleSyslog</TargetId>
  </WriteTargets> <AccessControl>
<!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />--> <
/AccessControl>
</Application>
```

5. Нажмите "**Start Server**" в верхнем левом углу программы **Syslog Watcher**.



Пример отображения.

- Пример отображения в Syslog Watcher.

The screenshot displays the Syslog Watcher - Local Syslog Server application. The interface includes a top toolbar with icons for Start Server, Stop Server, Status, Reload, Filter, Find, Search, Import, Export, Delete, Reports, Storage, and Settings. Below the toolbar are buttons for Vendor Pack, Help, and Info. A status bar shows 'Show Any Severity' from LOG last 1000 messages, updated every 10 seconds, with an 'AutoScroll' checkbox checked. The main area is divided into two sections: 'Quick Find' and 'Quick Filter'. The 'Quick Find' section shows a table of the last 1000 syslogs. The 'Quick Filter' section shows a detailed message view for a specific log entry.

Received	Source IP	Source ...	Facility	Severity	Timestamp	Tag	Ori...	Message
26.11.2018 10:52:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server LogonByAuthenticatorSucceeded [indee...
26.11.2018 11:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server LogonByAuthenticatorSucceeded [indee...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473 r...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473 li...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473 li...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473 r...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473 r...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473 li...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473 li...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473 r...

Message View

Info / local 7 LOG (::1) 26 ноября 2018 г. 11:00:31.963

server LogonByAuthenticatorSucceeded [indeed@32473
requestApplication="Enterprise Management Console" requestUser="Admin Indeed" requestComputer="192.168.1.3"
logonMode="Windows Token" authComment=""] Пользователь был успешно аутентифицирован по предоставленному
аутентификатору.Приложение: Enterprise Management Console.Пользователь: Admin Indeed.Компьютер:
192.168.1.3.Способ входа: Windows Token.Комментарий аутентификатора: .

For Help, press F1 Service: Started (4.8.6) Tot: 10 Dsn: 10 Fil: 0 Sel: 1 UDP: 514 TCP: 1468