Event Log Proxy

Компонент **RutokenKeyBox Event Log Proxy** позволяет записывать события с нескольких серверов Indeed Certificate Manager в единый журнал Windows Event Log.

Компонент устанавливается на одном из серверов Рутокен KeyBox или на отдельной рабочей станции (в домене или вне его). Системные требования для установки компонента совпадают с требованиями к серверу Рутокен KeyBox.

Для установки и настройки Рутокен KeyBox Event Log Proxy выполните следующие действия:

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Установите компонент **RutokenKeyBox.EventLog.Proxy.msi** из дистрибутива (располагающемся в каталоге RutokenKeyBox.Server) и выполните его установку следуя указаниям Мастера.
3. Откройте в редакторе Блокнот, запущенном от имени администратора, файл конфигурации Event Log Proxy — **C:\inetpub\wwwroot\eventlogproxy\Web.config**
4. Сервер Рутокен KeyBox использует Windows авторизацию в случае инсталляции RutokenKeyBox на ОС Windows и авторизацию по сертификатам в случае инсталляции на ОС семейства Linux.
   - При использовании Windows авторизации (инсталляция на Windows Server):
     - В параметре **allow users** укажите учетную запись из домена, в котором установлен Event Log Proxy, например, сервисную учетную запись Рутокен KeyBox для работы с Active Directory (**servicecm**).
       Пример заполненной секции:

       ```
       <authentication mode="Windows" />
       <authorization>
           <deny users="?" />
           <allow users="DEMO\servicecm" />
           <deny users="*" />
       </authorization>
       ```
   - При использовании авторизации по сертификату (инсталляция на ОС семейства Linux):
     - Параметру **authentication** укажите значение **"None"**, а также закомментируйте секцию **authorization**.
       Пример заполненной секции:

       ```
       <authentication mode="None" />
       <!--
           <authorization>
               <deny users="?"/>
               <allow users="*" />
               <deny users="*" />
           </authorization>
       -->
       ```
     - В секции **appSettings** параметру **authorizeByCertificate** укажите значение **"True"**, а в параметре **allowedCertificateThumbprints** укажите отпечаток сертификата, разрешенного к предъявлению сервером Рутокен KeyBox.

       Улучшенный ключ (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности клиента** (Client Authentication).

       Пример заполненной секции:

       ```
       <appSettings>
           <add key="authorizeByCertificate" value="true" />
           <add key="allowedCertificateThumbprints" value="aba8b93d73343f2182e3c1c40482b2ae2d75b6ec"
       />
       </appSettings>
       ```
5. **Сохраните** изменения в файле и закройте файл конфигурации.