# Фильтрация процессов и ФС

## Запрет запуска процессов

Для PAM Gateway реализован механизм запрета запуска процессов пользователями.

При каждом запуске процесса выполняется ряд проверок. Запуск процесса разрешен, если хотя бы одна из проверок пройдена:

- Если пользователь это `LOCAL_SYSTEM`, `LOCAL_SERVICE` или `NETWORK_SERVICE`
- Если пользователь является администратором на сервере RDS
- Если родительским процессом является один из известных системных (`svchost.exe`, `winlogon.exe`, `userinit.exe`, `rdpinit.exe`)
- Старт процесса разрешен в конфигурационном файле `processprotection.settings.json`

Если ни одна из проверок не пройдена, то запуск процесса запрещён.

Конфигурация разрешенных процессов настраивается в файле `C:\Program Files\Indeed PAM\Gateway\ProcessCreateHook\processprotection.settings.json`

Пример файла:

```
{
  "ApplicationPaths": [
    "C:\\Program Files\\Internet Explorer\\IEXPLORE.EXE",
    "C:\\Program Files (x86)\\Internet Explorer\\IEXPLORE.EXE",
  ],

  "ParentProcessPaths": [
    "C:\\Program Files\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
    "C:\\Program Files\\Internet Explorer\\IEXPLORE.EXE",
    "C:\\Program Files (x86)\\Internet Explorer\\IEXPLORE.EXE",
  ]
}
```

Параметры:

- **ApplicationPaths** — пути до исполняемых файлов, которые можно запускать
- **ParentProcessPaths** — пути до исполняемых файлов, процессы которых могут запускать приложения из ApplicationPaths.

## Защита критичных файлов

Для PAM Gateway реализован механизм разграничения прав для доступа к файлам на уровне процессов.

Пользователи локальной группы администраторов имеют доступ к любым файлам из любых процессов. Остальные пользователи могут открывать любые файлы из любых процессов, кроме уязвимых файлов. Для уязвимых файлов выполняется проверка процесса: если процесс находится в списке разрешенных, то доступ разрешается, иначе - запрещается.

Конфигурация защиты уязвимых файлов настраивается в файле `C:\Program Files\Indeed PAM\Gateway\Service\filesprotection.settings.json`

По умолчанию в конфигурационный файл добавлены уязвимые файлы PAM, дополнительная настройка не требуется.

Пример файла:

```
{
  "VulnerableFiles": [
    {
      "Path": "C:\\Program Files\\Indeed PAM\\Gateway\\ProxyApp\\appsettings.json",
      "AllowedProcesses": [
        "C:\\Program Files\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ]
    },
    {
      "Path": "C:\\Program Files\\Indeed PAM\\SSH Proxy\\SshProxy\\",
      "AllowedProcesses": [
        "C:\\Program Files\\Indeed PAM\\SSH Proxy\\SshProxy\\Pam.SshProxy.Service.exe"
      ]
    }
  ]
}
```

Параметры:

- **VulnerableFiles** — список уязвимых файлов.
- **Path** — путь к уязвимому файлу. Можно указывать как конкретный файл, так и директорию.
- **AllowedProcesses** — список процессов, которым разрешен доступ к файлу. Указываются конкретные исполняемые модули.

После изменения конфигурационного файла требуется перезапуск службы Pam.Service