

Сервер авторизации (xauth)

Модуль «Сервер авторизации (Xauth)» расположен в Меню «Пользователи и статистика».

Данный модуль отвечает за сервер авторизации Пользователей Xauth, по средствам которого Пользователи могут быть авторизованы на «ИКС» через утилиту авторизации Xauth.

Данный модуль содержит три вкладки:

1. Сервер авторизации
2. Настройки
3. Журнал

Сервер авторизации

На вкладке **Сервер авторизации** отображаются:

- статус сервера (запущен/выключен);
- кнопка «Включить» / «Выключить». Позволяет запустить и остановить сервер авторизации соответственно. По умолчанию сервер авторизации запущен;
- журнал событий за текущую дату.

ООО "Организация" > Сервер авторизации Администратор

Сервер авторизации | Настройки | Журнал

Сервер авторизации
Отвечает за авторизацию пользователей запущен
Выключить

Журнал ↓ ↑ ↻

- User User2 autologged from 192.168.17.19
13:30:49
- [uid: 0] TLS is started
13:30:49
- [uid: 0] new connection from 192.168.17.19
13:30:49
- config loaded
13:30:07
- Listening on 0.0.0.0:4888
13:30:01
- config loaded
13:30:01
- locale loaded
13:30:01
- started
13:30:01


Настройки

На вкладке **Настройки** представлен выбор «Автоматически создавать разрешающее правило». Если флаг установлен, то в разрешающих правилах [межсетевого экрана](#) будет добавлено правило «Доступ для программы авторизации» (Направление – Входящие на ИКС; Источник – Локальные сети, DMZ сети; Назначение – self; Протокол –TCP; Порт назначения – Порт программы авторизации; Интерфейс – Внутренние интерфейсы, VPN-интерфейсы, DMZ). Если флаг не установлен, то данное правило будет удалено из разрешающих правил межсетевого экрана.

ООО "Организация" > Xauth > Настройки

Xauth **Настройки** Журнал



- Запретить множественную авторизацию с одним логином
- Автоматически создавать разрешающее правило

 Доступ для Xauth


Журнал



На вкладке **Журнал** отображается сводка всех системных сообщений модуля с указанием даты и времени.

Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

ООО "Организация" > Сервер авторизации > Журнал Администратор   3

Сервер авторизации Настройки **Журнал**

09.09.2019 - 09.09.2019 **Сегодня** Неделя Месяц Другой период ▾ 

 Экспорт Удалить логи 

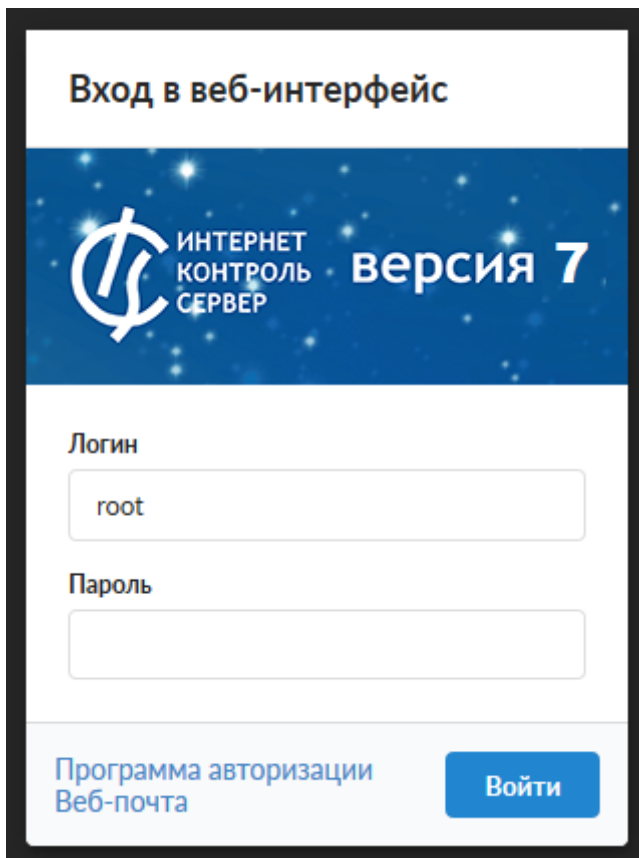
↓↑
User User2 autologged from 192.168.17.19 15:30:46
[uid: 0] TLS is started 15:30:46
[uid: 0] new connection from 192.168.17.19 15:30:46
config loaded 15:30:07
Listening on 0.0.0.0:4888 15:30:01
config loaded 15:30:01
locale loaded 15:30:01
started 15:30:01
exiting 15:29:59

« < Стр 1 из 1 > »

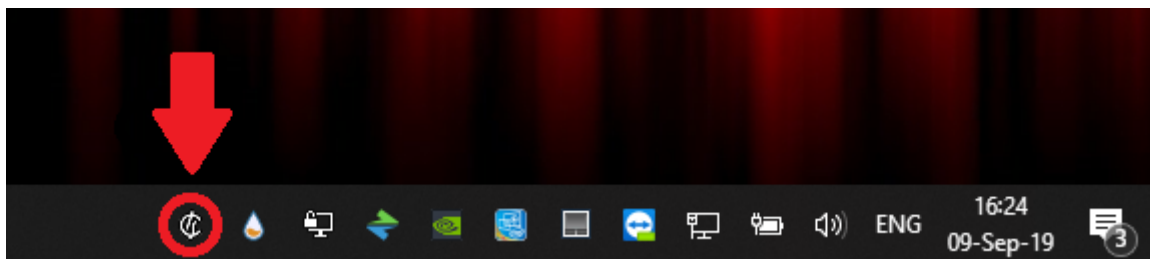
Показаны записи 1 - 9 из 9

Утилита авторизации Xauth

Утилита авторизации Xauth (далее «клиент Xauth») предназначена для авторизации пользователей на ИКС. Скачать утилиту можно кликнув по ссылке «Программа авторизации» на странице входа в веб-интерфейс ИКС.

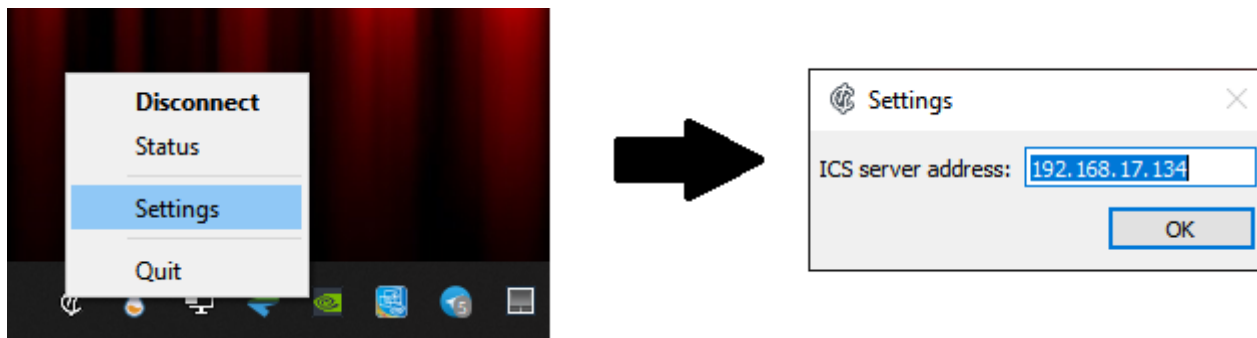


После скачивания клиент Xauth можно запускать. Установки утилита не требует и поставляется непосредственно в виде исполняемого файла. После запуска при загрузке на короткое время появится логотип ИКС, после этого программа продолжит работу в минимизированном виде в трее.



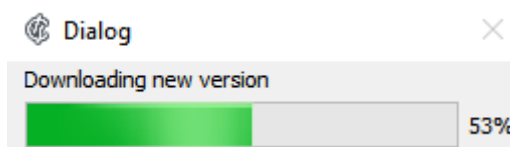
Подключение к серверу авторизации

Для подключения к серверу авторизации клиент Xauth по умолчанию попытается использовать маршрут до шлюза по умолчанию. Изменить адрес сервера авторизации можно кликнув правой кнопкой мыши по иконке клиента Xauth и выбрав меню настройки (settings) изменить адрес в строке ввода на необходимый. Затем необходимо переподключиться к новому серверу нажав «Отключиться» (Disconnect) и «Подключиться» (Connect) в том же меню.



Обновление клиента Xauth

При подключении к серверу клиент Xauth проверит наличие обновлений для себя. Если таковых не обнаружится, то программа продолжит работу. В противном случае автоматически запустится процесс загрузки новой версии. Обычно этот процесс не занимает много времени и зависит от скорости подключения к серверу. Во время процесса скачивания появляется полоса прогресса, которая отображается текущий процент загруженных данных.



После загрузки программа автоматически завершится, осуществит обновление и снова включится. Следует обратить внимание, что вновь запущенная программа будет использовать шлюз по умолчанию для подключения, таким образом, если адрес сервера авторизации был изменен, операцию по изменению адреса необходимо повторить.

Авторизация пользователя

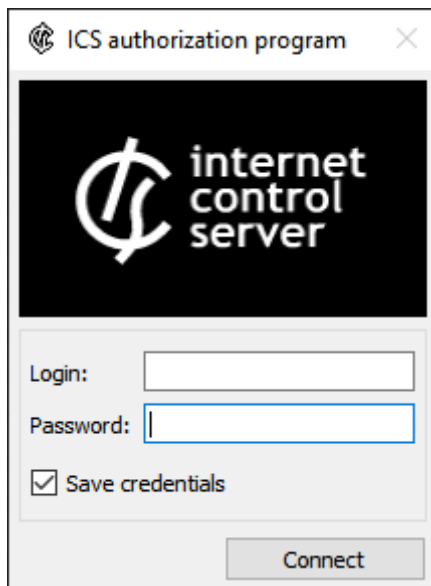
Клиент Xauth позволяет провести авторизацию тремя способами:

- По IP-адресу устройства на котором запущен клиент Xauth
- С использованием доменной авторизации
- По логину и паролю пользователя

В первую очередь происходит попытка авторизации по IP-адресу. Авторизация по IP-адресу используется, если в ИКС существует пользователь, которому назначен IP-адрес машины на которой запущен клиент Xauth.

В случае если авторизация по IP-адресу не была осуществлена, то происходит попытка авторизации через домен. Для данного типа авторизации должен быть настроен домен.

Если оба вышеперечисленных способа не были осуществлены, то пользователю будет предложено ввести логин и пароль для авторизации, которые назначены ему при создании в ИКС.



Ключи запуска клиента Xauth

Клиент Xauth может быть запущен без каких-либо дополнительных параметров, в таком случае поведение программы будет совпадать с описанным выше. Однако в некоторых ситуациях может требоваться иное поведение программы, например при автоматическом и/или удаленном запуске. В таких случаях утилиту можно запускать с одним или несколькими следующими ключами:

- **-server** [server ip]: ключ для задания сервера авторизации по умолчанию;
- **-noauto** : отключение авторизации по IP-адресу (см. пункт «Авторизация пользователя»);
- **-nodomain** : отключение авторизации через домен (см. пункт «Авторизация пользователя»);
- **-nomanual** : отключение авторизации по логину и паролю (см. пункт «Авторизация пользователя»);
- **-nosave** : не сохранять данные, введенные на форме авторизации через логин и пароль
- **-logs** [NONE, DEBUG, INFO]: уровень логирования, если уровень логирования отличается от NONE (по умолчанию), то создается папка logs в той же директории, что и исполняемый файл и туда помещаются логи работы утилиты.

Мониторинг соединений

Служба мониторинга соединений предназначена для постоянного слежения за состоянием соединений, осуществляемых конечным устройством с установленным клиентом Xauth.

Со стороны клиента, в общем случае, не требуется выполнять каких-либо настроек для работы данной службы. Однако существует несколько ключей запуска клиента Xauth, которые влияют на ее работу:

- **-nomonitor** : отключает мониторинг соединений на клиенте;
- **-delay** [delay]: регулировка времени между сканированиями соединений в миллисекундах, значение по умолчанию - 1000 (1 сек.).

Web-интерфейс мониторинга соединений

Данные мониторинга соединений можно просматривать через интерфейс ИКС, для этого необходимо перейти в меню Пользователи и Статистика → Пользователи, выбрать пользователя на машине которого запущен клиент Xauth и перейти во вкладку «Приложения».

ООО "Организация" > Пользователи > TestUser1 > Приложения Администратор 1

Правила и ограничения Почта и телефония Перенаправления OpenVPN **Приложения** Статистика События

Запретить доступ

Приложения и процессы	Соединения	Протокол	ID родительского процесса
NVIDIA Web Helper.exe			
NetDrive2.exe			
System			
TeamViewer_Service.exe			
Telegram.exe			
Не определен			
Video.UI.exe			
9752	192.168.17.19:62311 → 95.100.188.12:443	TCP	616
[System Process]			
dasHost.exe			
firefox.exe			
nvcontainer.exe			
svchost.exe			
xauth.exe			
14704	192.168.17.19:50830 → 192.168.17.134:...	TCP	9244

На данной странице соединения сгруппированы по приложениям, которые эти соединения установили.

Можно посмотреть:

- приложение, установившее соединение
- PID процесса
- основную информацию о соединении (IP-адреса, порты, протокол)
- PID родительского процесса

Также на данной странице можно заблокировать соединения, установленные приложением. Блокаровка осуществляется средствами службы Application Firewall.

From: <https://doc-old.a-real.ru/> - **Документация**

Permanent link: <https://doc-old.a-real.ru/doku.php?id=ics70:xauth&rev=1573397036>

Last update: **2020/01/27 16:28**

