Теневое подключение к рабочему столу (сеансу) пользователя Windows

date23.06.2022

user [itpro](https://winitpro.ru/index.php/author/itpro/" \o "Записи itpro)

directory [Windows 10](https://winitpro.ru/index.php/category/windows-10/), [Windows 11](https://winitpro.ru/index.php/category/windows-11/)

comments [комментариев 78](https://winitpro.ru/index.php/2018/07/11/rdp-shadow-k-rabochemu-stolu-polzovatelya-windows-10/#comments)

Вы можете использовать возможности теневых подключений (Remote Desktop Shadowing) для удалённого подключение к сессиям пользователей на компьютерах Windows. Это функционал является по сути аналогом Remote Assistance и позволяет администраторам удаленно просматривать и взаимодействовать с рабочим столом пользователей как на десктопных версиях (Windows 11 или 10), так и на RDS серверах Windows Server.

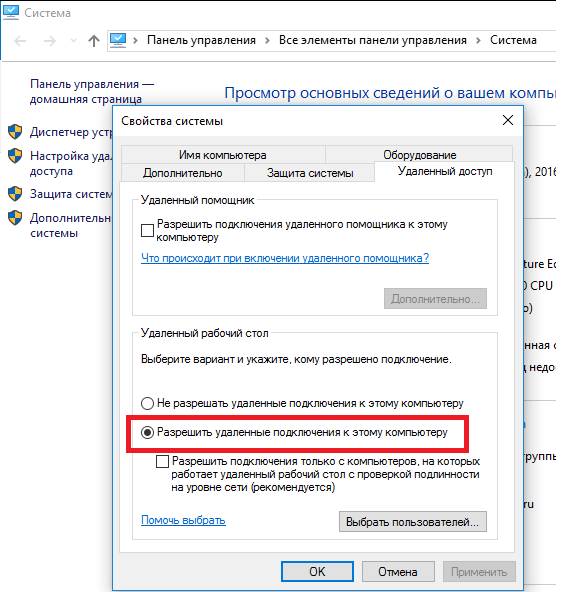
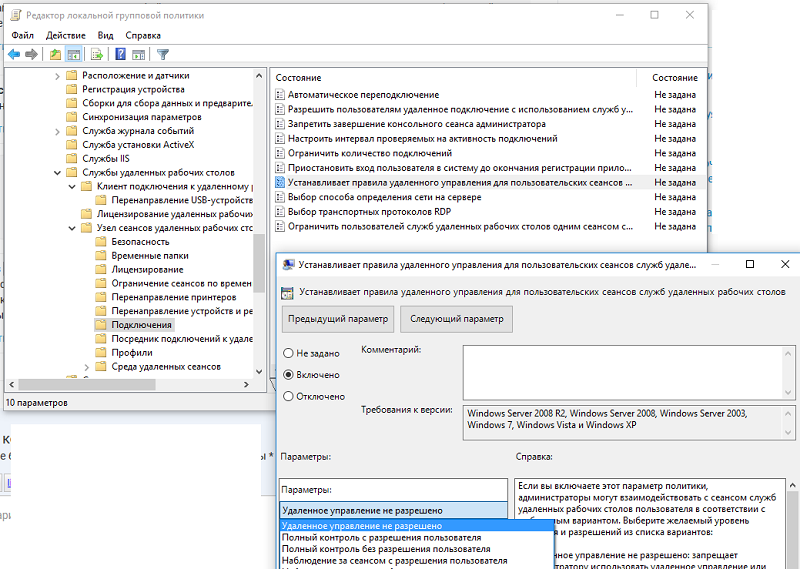
**Содержание:**

* [Настройка клиентов Windows для удаленного подключения через теневые сессии](https://winitpro.ru/index.php/2018/07/11/rdp-shadow-k-rabochemu-stolu-polzovatelya-windows-10/#h2_1)
* [Удаленное подключение к сессии пользователя Windows через RDP Shadowing](https://winitpro.ru/index.php/2018/07/11/rdp-shadow-k-rabochemu-stolu-polzovatelya-windows-10/#h2_2)

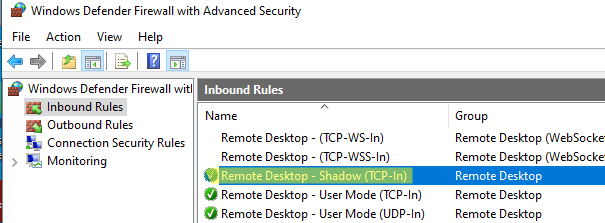
[Remote Desktop Shadowing](https://winitpro.ru/index.php/2014/02/12/rds-shadow-v-windows-2012-r2/) часто используется администраторами для оказания поддержки пользователям [RDS ферм Windows Server](https://winitpro.ru/index.php/2022/02/17/ustanovka-nastrojka-remote-desktop-services-rds-windows-server/).

Настройка клиентов Windows для удаленного подключения через теневые сессии

Вам нужно определенным образом настроить компьютеры, к которым вы хотите подключаться через теневое подключение.

1. [Включите удаленный рабочий стол (RDP)](https://winitpro.ru/index.php/2013/04/29/kak-vklyuchit-udalennyj-rabochij-stol-v-windows-8/) на компьютерах пользователей (вручную или через GPO);
2. Ваша учетная запись должна обладать правами локального администратора на компьютере пользователей (вы можете [добавить пользователя в группу администраторов вручную или с помощью групповых политик](https://winitpro.ru/index.php/2019/11/27/gpo-dobavit-v-gruppu-lok-admins/));
3. Настройте режим теневого подключения (нужно ли запрашивать подтверждение пользователя, и возможно управления в сессии или только наблюдение). Можно настроить режим через групповую политику “**Установить правила удаленного управления для пользовательских сеансов служб удаленных рабочих столов”**(Set rules for remote control of Remote Desktop Services user sessions) в разделе **Конфигурация компьютера -> Административные шаблоны –> Компоненты Windows –> Службы удаленных рабочих столов –> Узел сеансов удаленных рабочих столов –> Подключения** (Policies -> Administrative Templates -> Windows components -> Remote Desktop Services -> Remote Session Host -> Connections).  
   Доступны 5 режимов:**0** – запретить удаленное управление;  
   **1** — полный контроль с разрешения пользователя;  
   **2** — полный контроль без разрешения пользователя;  
   **3** — наблюдение за сеансом с разрешения пользователя;  
   **4** — наблюдение за сеансом без разрешения пользователя.
4. Вы можете включить нужный режим напрямую в реестре. Отредактируйте реестр вручную или с помощью команды (в этом примере мы установили 4 режим – разрешить просмотр сеанса пользователя без уведомления): reg add "HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v Shadow /t REG\_DWORD /d 4

По умолчанию данный теневое подключение выполняется в режиме полного контроля с разрешения пользователя.

1. Настройте правила Windows Defender Firewall, разрешающие трафик теневых подключений по сети. Для трафика session shadowing в Windows вместо [стандартного порта 3389/RDP](https://winitpro.ru/index.php/2010/09/17/nomer-porta-rdp-v-windows/) используются порты **139/TCP**, **445/TCP** и диапазон динамических **RPC портов** (49152 по 6553). Чтобы разрешить входящий трафик теневых подключений, нужно включить два преднастроненных правила в Windows: File and Printer Sharing (SMB-In) и Remote Desktop - Shadow (TCP-In) . Последнее правило разрешает удаленный доступ к процессу RdpSa.exe . Вы можете [включить правила Windows Defender на компьютерах пользователей через GPO](https://winitpro.ru/index.php/2018/12/06/nastrojka-pravil-windows-firewall-gpo/) или с помощью [PowerShell командлета Enable-NetFirewallRule](https://winitpro.ru/index.php/2019/09/25/upravlenie-windows-firewall-powershell/).

Удаленное подключение к сессии пользователя Windows через RDP Shadowing

Рассмотрим, как удаленно подключиться рабочему столу сессии другого пользователя на удаленном компьютере Windows через теневые подключения RDP. В этом примере я покажу, как подключиться с компьютера Windows 11 к сессии пользователя на рабочей станции пользователя с Windows 10.

Для теневого подключения к сессии пользователя используется стандартная RDP утилита **mstsc.exe**. Формат команды такой:

Mstsc.exe /shadow:<ID сессии> /v:<Имя или IP адрес компьютера>

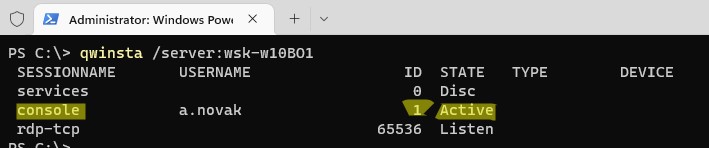
Также можно использовать одну из опций:

* **/prompt** – запросить имя и пароль пользователя, под которым выполняется подключение (если не указано, подключение выполняется под текущим пользователем).
* **/control** – режим взаимодействия с сеансом пользователя. Если параметр не задан, вы подключитесь в режиме просмотра (наблюдения) сессии пользователя, т.е. вы не сможете управлять его мышью и вводить данные с клавиатуры;
* **/noConsentPrompt** – не запрашивать у пользователя подтверждение на подключение к сессии.

Теперь нужно [узнать имя пользователя и ID его сессии](https://winitpro.ru/index.php/2021/03/25/poluchit-imya-polzovatelya-na-udalennom-kompyutere/) на удаленном компьютере (если пользователь работает непосредственно за консолью компьютера, то ID его сессии всегда будет равно 1).

Выведем список сессий пользователей на удаленном компьютере (это может быть как десктопный компьютер с Windows 11/10 или [Windows Server с ролью Remote Desktop Services Host (RDSH).](https://winitpro.ru/index.php/2021/06/17/ustanovka-standalone-rdsh-windows-server-workgroup/)

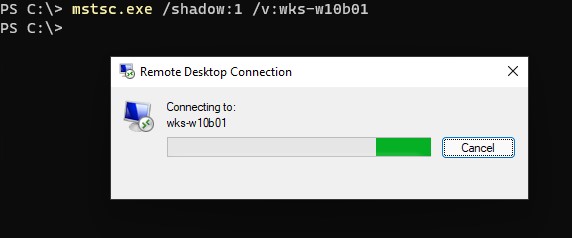
qwinsta /server:wks-w10b01



В данном примере видно, что на компьютере залогинен один пользователь a.novak, который работает непосредственно за компьютером ( SESSIONNAME=console ). Идентификатор сессии ID=**1**.

Чтобы подключиться к рабочему столу этого пользователя через теневое подключение, выполните команду:

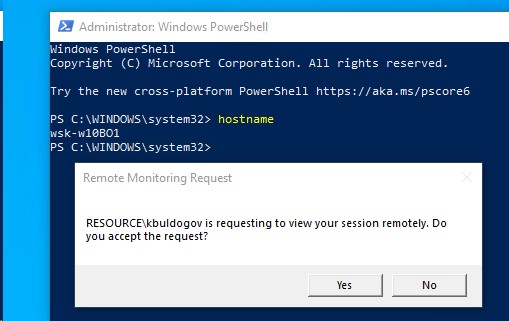
mstsc.exe /shadow:1 /v:wks-w10b01



На экране пользователя Windows появится запрос подтверждения подключения администратора к его сеансу:

Запрос на удаленное подключение

Username запрашивает удаленный просмотр вашего сеанса. Вы принимаете этот запрос.

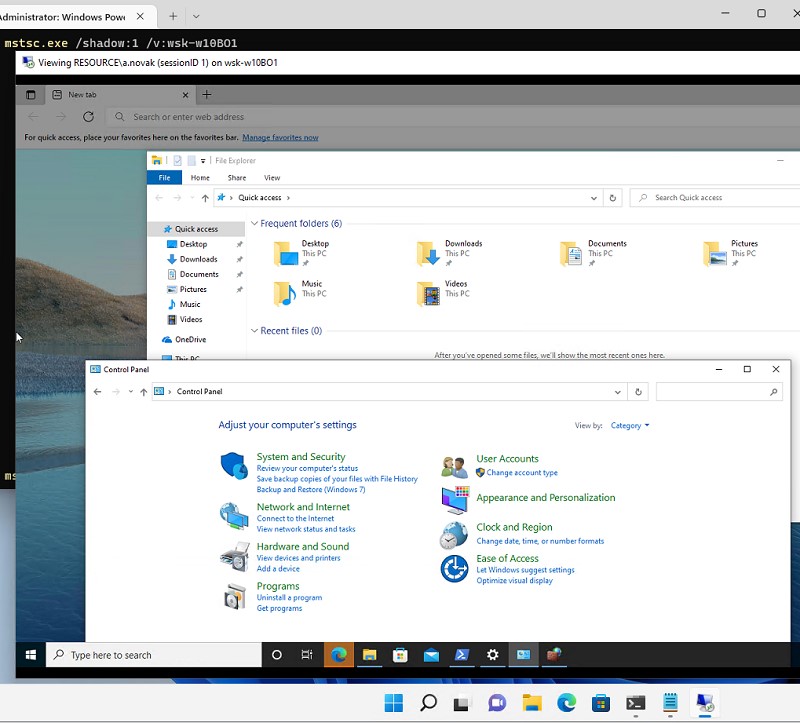


Если служба TermService на удаленном компьютере отключена, то при попытке удалённого подключения через RDP shadow появится ошибка:

The version of Windows running on this server does not support user shadowing



Если пользователь разрешит соединение, вы подключитесь к его консольному сеансу и увидите его рабочий стол. Вы будете видеть все действия пользователя, но не сможете взаимодействовать с его сессией. Если вы хотите управлять его сессией, добавьте в команду параметр /control. В этом случае надпись в заголовке окна сменится с Viewing username (sessionID 1) on computername на Controlling…

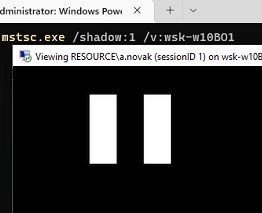


В данном случае вы подключились непосредственно подключиться к консольной сессии пользователя без блокировки его сеанса. При удаленном подключении к Windows 10 через обычный RDP, то сессия локального отключается (даже если вы включите возможность использования [нескольких одновременных RDP сессий в Windows 10](https://winitpro.ru/index.php/2015/09/02/neskolko-rdp-sessij-v-windows-10/)).

Если сессия пользователя [заблокирована](https://winitpro.ru/index.php/2020/09/10/blokirovka-ekrana-pri-neaktivnosti-gpo/), или появляется запрос повышения привилегий UAC, то без исопльзования режима mstsc /control окно с теневой сессией становится черным и на нем появляется символ паузы.

Теневая сессия переходит в приостановленное состояние, если у пользователя появляется запрос UAC на Secure desktop. После того, как пользователь подтвердит действие UAC, ваша сессия возобновится.

PromptOnSecureDesktop это один из параметров, доступных в [групповых политиках UAC](https://winitpro.ru/index.php/2016/05/16/polzunok-user-account-control-i-nastrojki-gruppovyx-politik/).



Чтобы развернуть окно теневой сессии во весь экран, воспользуйтесь комбинацией клавиш **Ctrl + Alt + Break.**

Для завершения теневой сессии нажмите на компьютере alt+\* (или ctrl+\* на RDS сервере).

Вы можете оповестить пользователя о том, что кто-то удаленно подключится к его сессии через теневое подключение с помощью следующего PowerShell скрипта:  
while($true){  
if (Get-Process -Name "RdpSa" -ErrorAction SilentlyContinue){[console]::beep(1000,500);Write-Host "RdpSa is running at $(Get-Date)"}  
Start-Sleep -Seconds 1

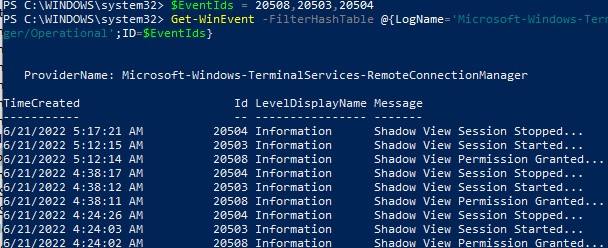
}  
В данном примере мы оповещаем пользователя звуковым оповещением, но вы можете [вывести всплывающее уведомление на рабочий стол](https://winitpro.ru/index.php/2018/10/02/uvedomleniya-polzovateley-is-powershell/). Можно [запустить этот PowerShell скрипт как службу Windows](https://winitpro.ru/index.php/2019/04/03/zapusk-powershell-skripta-kak-sluzhby-windows/).

Вы можете получить историю теневых подключений к компьютеру пользователя из журнала событий Windows. Все интересующие вас логи находятся в разделе **Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational**:Event Viewer

* Event ID **20508** — Shadow View Permission Granted
* Event ID **20503** — Shadow View Session Started
* Event ID **20504** — Shadow View Session Stopped

Вы можете получить логи теневых подключений к компьютеру с помощью PowerShell:

$EventIds = 20508,20503,20504  
Get-WinEvent -FilterHashTable @{LogName='Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational';ID=$EventIds}



Подробнее про [анализ логов RDP подключений](https://winitpro.ru/index.php/2018/09/25/analizing-rdp-logs-windows-terminal-rds/) рассказано в отдельной статье.

Функционал теневого подключения Remote Desktop Shadowing работает в Windows 11/10/ 8.1 и Windows Server 2022/2019/2016/2012 R2. Таким образом Remote Desktop Shadowing можно использовать как аналог Remote Assistance (Удаленный помощник) или TeamViewer/Anydesk для локальной или корпоративной сети.