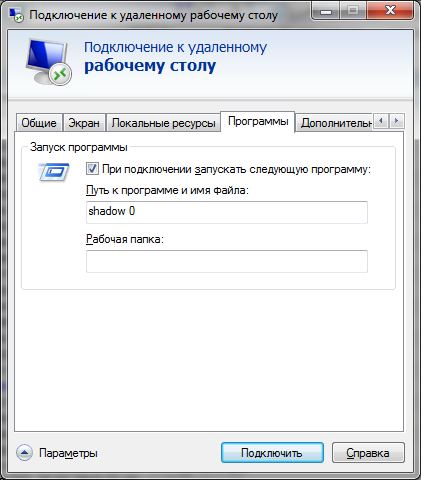
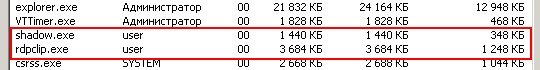
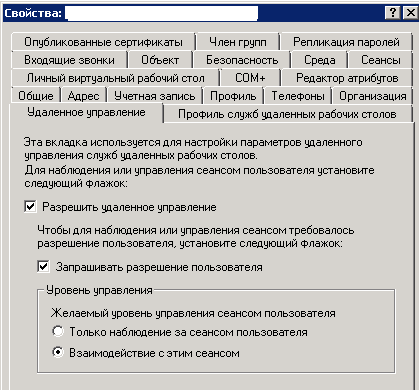
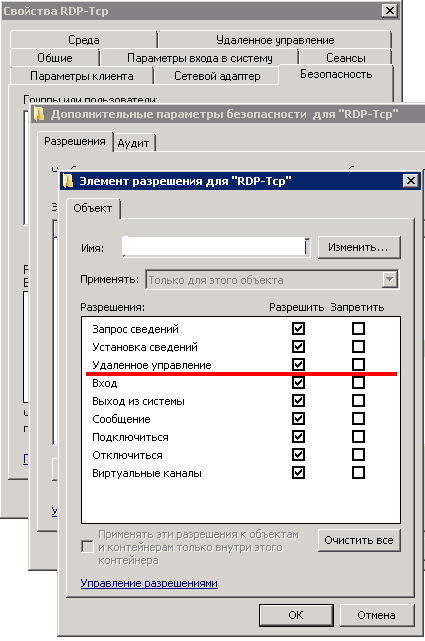
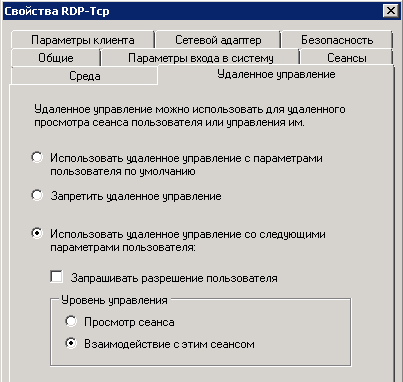
Удаленное управление сеансом пользователя windows стандартными средствами

* [Системное администрирование](https://habrahabr.ru/hub/sys_admin/" \o "Вы не подписаны на этот хаб),
* [Серверное администрирование](https://habrahabr.ru/hub/s_admin/)
* [Из песочницы](https://habrahabr.ru/sandbox/)

Однажды мне захотелось управлять одним из домашних компьютеров удаленно, но при этом взаимодействовать с текущим пользователем, но компьютер был довольно слабый и при запуске например TeamViewer’а нагрузка процессора поднималась до 98% и компьютер начинал заметно тормозить. Попробовал стандартный RDP, но тогда «выбивался» текущий пользователь и для входа локально приходилось набивать пароль. Но чуть позже мне случайно попалась команда **shadow**.  
  
*Наблюдать за другим сеансом служб удаленных рабочих столов.  
SHADOW {<имя сеанса> | <ID сеанса>} [/SERVER:<сервер>] [/V]  
<имя сеанса> Имя сеанса.  
<ID сеанса> Идентификатор сеанса.  
/SERVER:<сервер> Сервер терминалов (по умолчанию текущий).  
/V Отображение информации о выполненных действиях.*  
  
Например для управления консольным сеансом(пользователем который непосредственно сидит перед компьютером) текущего терминального сервера достаточно ввести команду *выполнить -* **shadow 0**. Выход осуществляется через **alt \*** на обычном компьютере и через **ctrl \*** на терминальном сервере.  
Но есть неприятная особенность: эта команда работает только из под rdp сессии. Но мой управляемый компьютер был под управлением windows xp поэтому пришлось расширить его возможности сделав из него терминальный сервер (в интернете полно статей как это можно сделать). Тогда все стало довольно просто, подключаемся любым пользователем с правами администратора по rdp и запускаем команду *выполнить -* **shadow 0** попадаем в консольный сеанс, собственно что мне и нужно было. Для уменьшения аппаратных затрат можно при создании rdp подключения выбрать функцию «**При подключении запускать следующую программу**» и там набрать **shadow 0** как на рисунке.  
  
  
  
Тогда получается что запускается всего 2 процесса.  
  
  
  
Для того что бы все это работало нам необходимо сначала включить RemoteRPC, например через реестр:   
  
*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]  
“AllowRemoteRPC”=dword:00000001*  
  
После этого можно будет через **Диспетчер служб удаленных рабочих столов** посмотреть какие пользователи залогинены на компьютере, какие у них id и какие процессы запущены (жаль только названия, нет информации о нагрузке).  
  
По умолчанию пользователю будет задаваться вопрос с разрешением управления, можно отключить вопрос или сделать только удаленное наблюдение, меняется через реестр:  
  
*[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services]  
«Shadow»=dword:0000000****x***  
  
Где **x** может иметь значения:  
0 — удаленное управление не разрешено  
1 -полный контроль с разрешения клиента  
2 -полный контроль без разрешения клиента  
3 -наблюдение за сеансом с разрешением клиента  
4 -наблюдение за сеансом без разрешения клиента  
  
По умолчания этой строчки вообще нет и её нужно будет создавать.  
  
Так же можно включить через групповые политики локальные или доменные. Для включения локально запускаем **gpedit.msc** — выбираем *административные шаблоны — добавление и удаление шаблонов*, добавляем *System.adm* из папки *WINDOWS\inf*  
  
Теперь настраиваем: *конфигурация компьютера — административные шаблоны — компоненты windows — службы терминалов — устанавливает правила для удаленного управления*. Для windows xp.  
  
И *конфигурация компьютера — административные шаблоны — компоненты windows- службы удаленных рабочих столов – узел сеансов удаленных рабочих столов – подключения – устанавливает правила удаленного управления для пользовательских сеансов служб удаленных рабочих столов*. Для windows 7.  
Все это работает и в домене, если у пользователя есть соответствующие права.  
  
В доменных настройках профиля пользователя тоже есть настройка подобных прав (я встречал эти настройки даже в домене win 2000)  
  
  
Если рассматривать терминальный сервер, то там через свойства RDP(через *конфигурация узла сеансов удаленных рабочих столов*) можно выставить любому пользователю права на удаленное управление,  
  
  
  
и отдельно настроить взаимодействие или управление удаленным сеансом.  
  
  
  
Для удобства можно подключаться через диспетчер задач  
