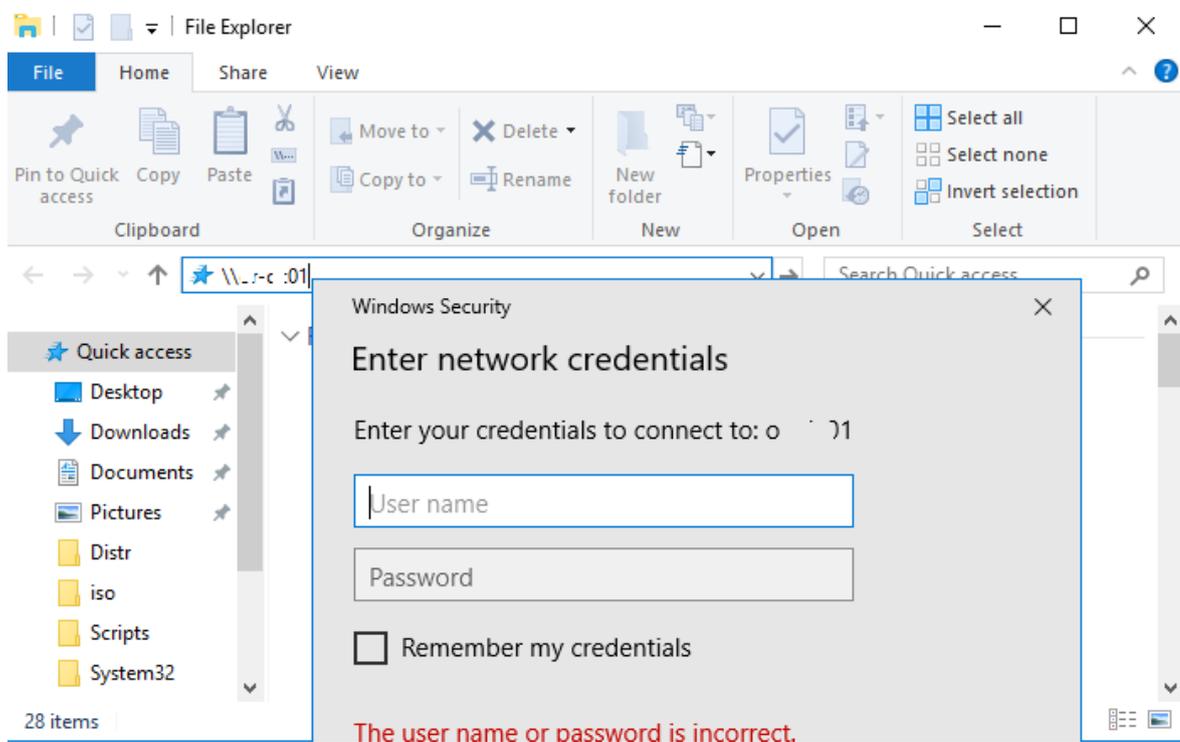


Управление доступом к ресурсам сети

По умолчанию, при доступе к общей сетевой папке на сервере, включенном в домен Active Directory, с компьютеров из рабочей группы (не добавленных в домен) у пользователя появляется запрос на ввод пароля доменной учетной записи. Попробуем разобраться, как разрешить анонимный доступ к общим сетевым папкам и принтерам на доменном сервере с компьютеров рабочей группы без авторизации на примере Windows 10 / Windows Server 2008-2016.



С точки зрения безопасности не рекомендуется открывать анонимный сетевой доступ для гостевого аккаунта. Тем более нельзя включать анонимный доступ на контроллерах домена. Поэтому перед включением анонимного доступа попробуйте выбрать более правильный путь – включение компьютеров рабочей группы в домен, или [создайте](#) для всех пользователей рабочей группы персональные учётные записи в домене. Это гораздо правильнее с точки зрения предоставления и управления доступом.

Локальные политики анонимного доступа

На сервере (компьютере), к которому вы хотите предоставить общий доступ неавторизованным пользователям нужно открыть редактор локальной групповой политики – gpedit.msc.

Перейдите в раздел **Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности** (Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options)

Настройте следующие политики:

- **Учетные записи: Состояние учётной записи 'Гость'** (Accounts: Guest Account Status): Включен (Enabled);
- **Сетевой доступ: разрешить применение разрешений "Для всех" к анонимным пользователям** (Network access: Let Everyone permissions apply to anonymous users): Включен (Enabled);
- **Сетевой доступ: Не разрешать перечисление учетных записей SAM и общих ресурсов** (Network access: Do not allow anonymous enumeration of SAM accounts and shares): Отключен (Disabled).

Редактор локальной групповой политики

Файл Действие Вид Справка

Политика "Локальный компьютер"

- Конфигурация компьютера
 - Конфигурация программ
 - Конфигурация Windows
 - Политика разрешения имен
 - Сценарии (запуск/завершение)
 - Развернутые принтеры
 - Параметры безопасности
 - Политики учетных записей
 - Локальные политики
 - Политика аудита
 - Назначение прав пользователя
 - Параметры безопасности
 - Монитор брандмауэра Защитника Windows
 - Политики диспетчера списка сетей
 - Политики открытого ключа
 - Политики ограниченного использования п...
 - Политики управления приложениями
 - Политики IP-безопасности на "Локальный"
 - Конфигурация расширенной политики ауд...
 - QoS на основе политики
 - Административные шаблоны
 - Конфигурация пользователя
 - Конфигурация программ
 - Конфигурация Windows
 - Административные шаблоны

Политика	Параметр безопасности
Учетные записи: Состояние учетной записи 'Гость'	Включен
Учетные записи: Состояние учетной записи 'Администратор'	Включен
Учетные записи: разрешить использование пустых паролей только при консольном в...	Включен
Учетные записи: Переименование учетной записи гостя	Гость
Учетные записи: Переименование учетной записи администратора	admin
Учетные записи: блокировать учетные записи Майкрософт	Не определено
Устройства: разрешить форматирование и извлечение съемных носителей	Администраторы
Устройства: разрешить доступ к дисководам компакт-дисков только локальным поль...	Отключен
Устройства: разрешить доступ к дисководам гибких дисков только локальным пользо...	Отключен
Устройства: разрешать отстыковку без входа в систему	Включен
Устройства: запретить пользователям установку драйверов принтера	Отключен
Системные объекты: учитывать регистр для подсистем, отличных от Windows	Включен
Системные объекты: усилить разрешения по умолчанию для внутренних системных ...	Включен
Системная криптография: обязательное применение сильной защиты ключей поль...	Не определено
Системная криптография: использовать FIPS-совместимые алгоритмы для шифрова...	Отключен
Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-служб...	Не определено
Сетевой сервер (Майкрософт): попытка S4U2Self получить информацию об утвержде...	Не определено
Сетевой доступ: удаленно доступные пути реестра	System\CurrentControlS...
Сетевой доступ: удаленно доступные пути и вложенные пути реестра	System\CurrentControlS...
Сетевой доступ: разрешать применение разрешений "Для всех" к анонимным пользо...	Включен
Сетевой доступ: разрешать анонимный доступ к общим ресурсам	Не определено
Сетевой доступ: разрешать анонимный доступ к именованным каналам	Не определено
Сетевой доступ: ограничить количество клиентов, которым разрешены удаленные в...	Не определено
Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой про...	Отключен
Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов ...	Отключен
Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пол...	Включен

В целях безопасности желательно также открыть политику **“Запретить локальный вход”** (Deny log on locally) в разделе *Локальные политики* -> *Назначение прав пользователя* и убедиться, что в политике указана учетная запись **“Гость”**.

Затем проверьте, что в этом же разделе в политике **“Доступ к компьютеру из сети”** (Access this computer from network) присутствует запись **Гость**, а в политике **“Отказаться в доступе к этому компьютеру из сети”** (Deny access to this computer from the network) учетка **Гость** не должна быть указана.

Также убедитесь, что включен общий доступ к сетевым папкам в разделе **Параметры** -> **Сеть и Интернет** -> **Ваше сетевое подключение** (Ethernet или Wi-Fi) -> **Изменение расширенных параметров общего доступа** (Settings -> Network & Internet -> Ethernet -> Change advanced sharing options). В секции **“Все сети”** должен быть выбрана настройка **“Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках”** и выбрать **“Отключить парольную защиту (если вы доверяете всем устройствам в вашей сети)”**

Все сети ⬆

Общий доступ к общедоступным папкам ⬆

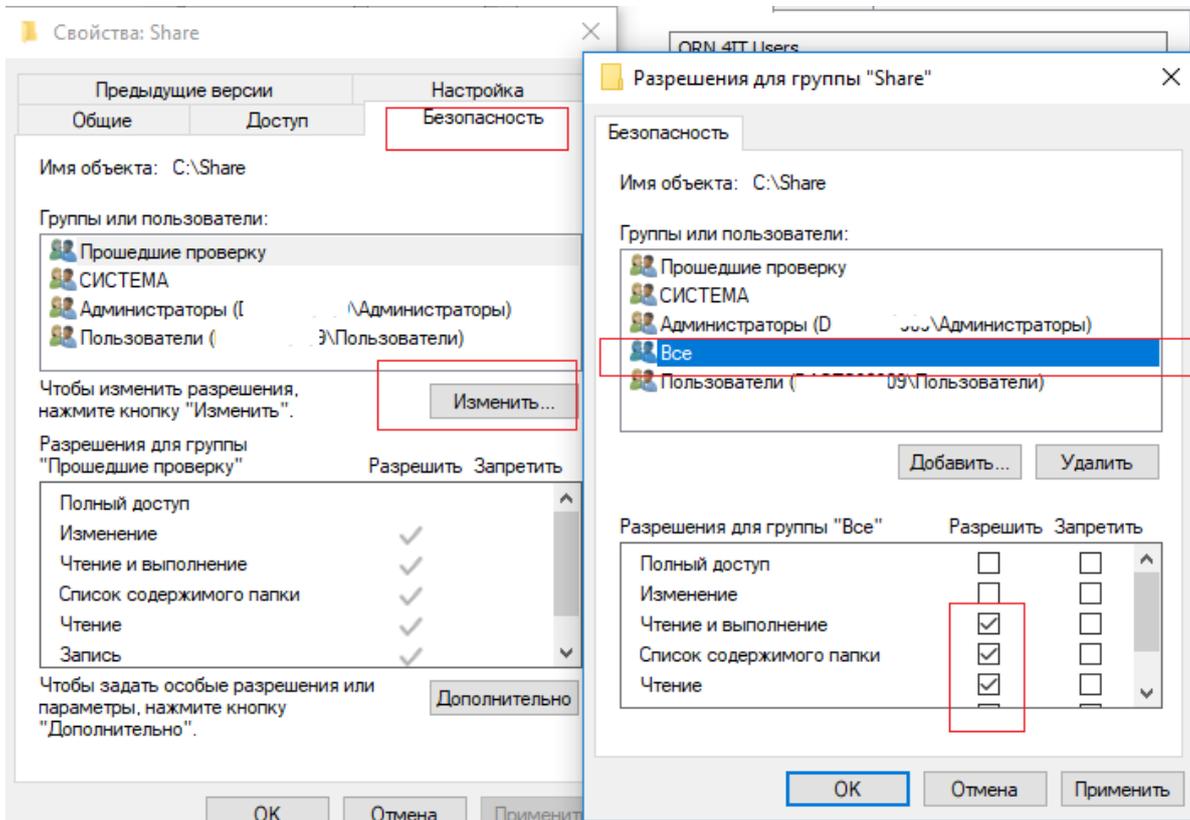
Если включен общий доступ к общедоступным папкам, пользователи сети (включая членов домашней группы) могут получать доступ к файлам в таких папках.

Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках

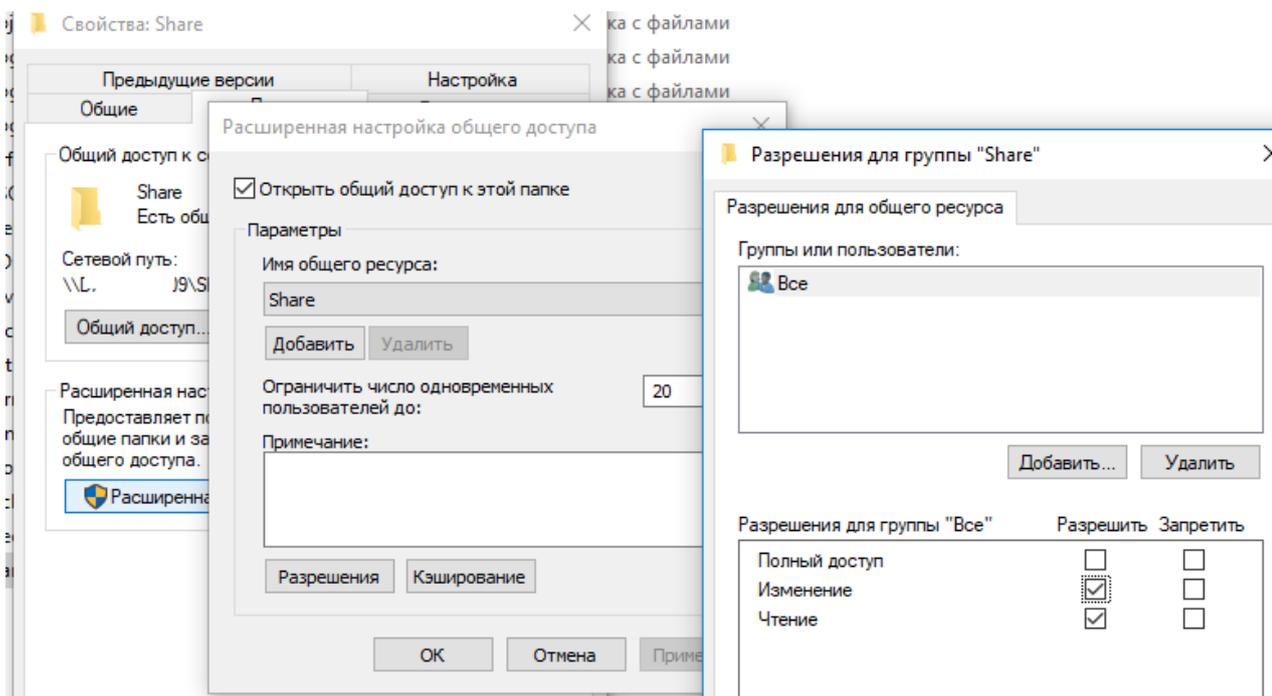
Отключить общий доступ (люди, выполнившие вход на этот компьютер, все равно будут иметь доступ к общедоступным папкам)

Настройка анонимного доступа к общей папке

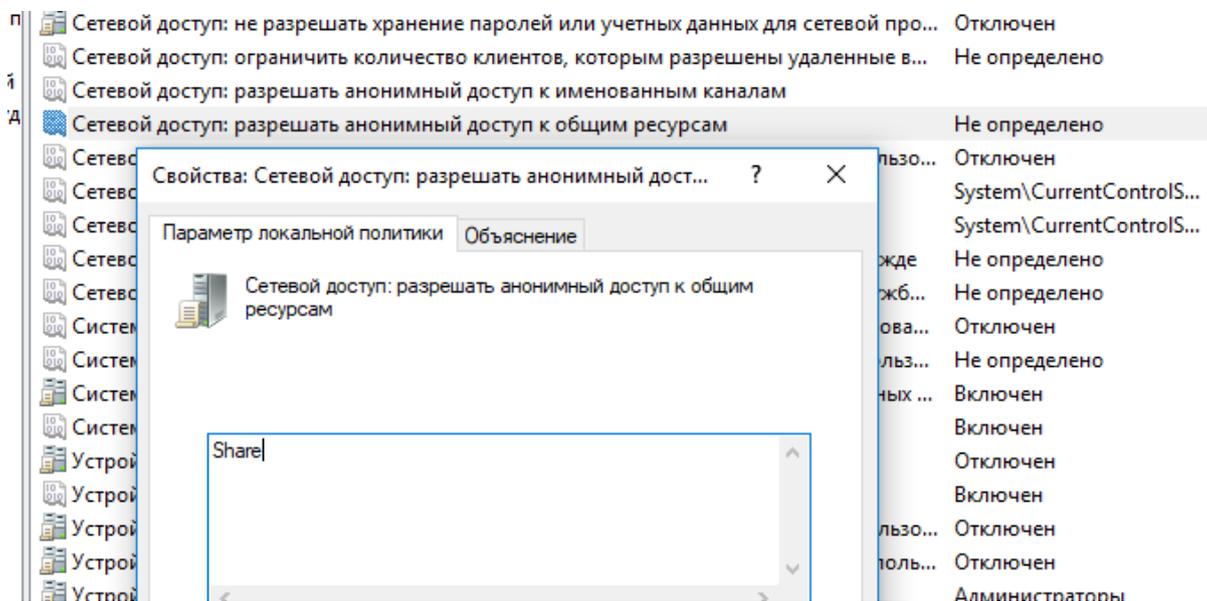
Теперь нужно настроить разрешения доступа на общей папке, к которой вы хотите предоставить **общий доступ**. Откройте свойства папки в настройках NTFS разрешений (вкладка **Безопасность**) предоставьте права чтения (и, если нужно, изменения) для локальной группы **«Все»** («Everyone»). Для этого нажмите кнопку **Изменить** -> **Добавить** -> **Все** и выберите необходимые привилегии анонимных пользователей. Я предоставил доступ только на чтение.



Также на вкладке Доступ нужно предоставить права анонимным пользователям на доступ к шаре (Доступ -> Расширенная настройка -> Разрешения). Проверьте, что у группы **Все** есть право на **Изменение** и **Чтение**.

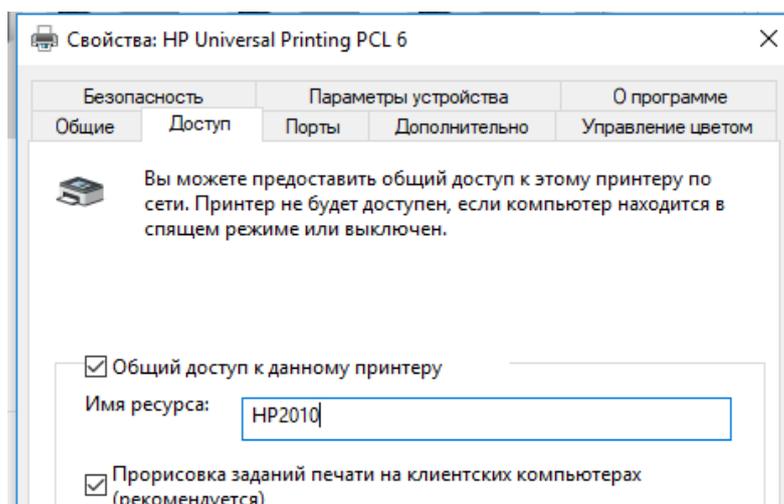


Теперь в редакторе локальных политик в секции Локальные политики -> **Параметры безопасности** нужно в политике "Сетевой доступ: разрешать анонимный доступ к общим ресурсам" (Network access: Shares that can be accessed anonymous) указать имя сетевой папки, к которой вы хотите предоставить анонимный доступ (в моем примере имя сетевой папки – Share).

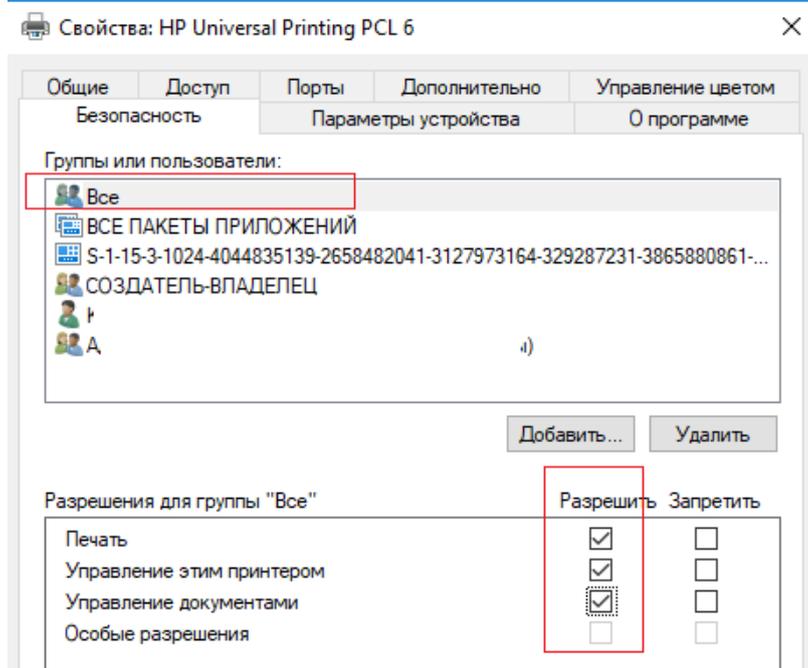


Предоставление анонимного доступа к общему сетевому принтеру

Чтобы разрешить анонимный доступ к сетевому принтеру на вашем компьютере, нужно открыть свойства общего принтера в Панели управления (Панель управления\Оборудование и звук\Устройства и принтеры). На вкладке доступа отметьте опцию **“Прорисовка задания печати на клиентских компьютерах”** (Render print jobs on client computers).



Затем на вкладке безопасность для группы “Все” отметить все галки.



После выполнения этих действий вы сможете подключаться к общей папке (\\servername\share) и принтеру на доменном компьютере с компьютеров рабочей группы без ввода имени пользователя и пароля, т.е. анонимно.