Не открываются общие сетевые SMB папки в Windows 10/11

Если вы из Windows 10 или 11 не можете открыть сетевые папки на других сетевых устройствах (NAS, Samba сервера Linux) или на компьютерах со старыми версиями Windows (Windows 7/ XP /2003), скорее всего проблема связана с тем, что в вашей версии Windows отключена поддержка устаревших и небезопасных версий протокола SMB (используется в Windows для доступа к общим сетевым папкам и файлам). В современных версиях Windows 10 и в Windows 11 по-умолчанию отключен протокол SMBv1 и анонимный (гостевой) доступ к сетевым папкам по протоколу SMBv2 и SMBv3.

Microsoft планомерно отключает старые и небезопасные версии протокола SMB во всех последний версиях Windows. Начиная с Windows 10 1709 и Windows Server 2019 (как в Datacenter так и в Standard редакциях) в операционной системе по умолчанию отключен протокол SMBv1 (помните атаку шифровальщика WannaCry, которая как раз и реализовалась через дыру в SMBv1).

Конкретные действия, которые нужно предпринять зависят от ошибки, которая появляется в Windows при доступе к общей сетевой папке и от настроек удаленного SMB сервера, на котором хранятся общие папки.

Вы не можете получить гостевой доступ к общей папке без проверки подлинности

Начиная с версии Windows 10 1709 (Fall Creators Update) Enterprise и Education пользователи стали жаловаться, что при попытке открыть сетевую папку на соседнем компьютере стала появляться ошибка:

```
Вы не можете получить доступ к этой общей папке, так как политики безопасности вашей организации
```

```
An error occurred while reconnecting Y: to
\\nas1\share Microsoft Windows Network: You can’t access this shared folder because your organiz
```

Вы не можете получить доступ к этой общей папке, так как политики безопасности вашей ор

При этом на других компьютерах со старыми версиями Windows 8.1/7 или на Windows 10 с билдом до 1709, эти же сетевые каталоги открываются нормально. Причина в том, что в современных билдах Windows 10 (начиная с 1709) по умолчанию запрещен сетевой доступ к сетевым папкам под гостевой учетной записью по протоколу SMBv2 (и ниже). Гостевой (анонимный) доступ подразумевают доступ к сетевой папке без аутентификации. При доступе под гостевым аккаунтом по протоколу SMBv1/v2 не применяются такие методы защиты трафика, как SMB подписывание и шифрование, что делает вашу сессию уязвимой против MiTM (man-in-the-middle) атак.

При попытке открыть сетевую папку под гостем по протоколу SMB2, в журнале клиента SMB (Microsoft-Windows-SMBClient) фиксируется ошибка:

```
Log Name: Microsoft-Windows-SmbClient/Security
Source: Microsoft-Windows-SMBClient
Event ID: 31017
Rejected an insecure guest logon.
```

Данная ошибка говорит о том, что ваш компьютер (клиент) блокирует не аутентифицированный доступ под аккаунтом guest.

Чаще всего с этой проблемой можно столкнуться при использовании старых версий NAS (обычно для простоты настройки на них включают гостевой доступ) или при доступе к сетевым папкам на старых версиях Windows 7/2008 R2 или Windows XP /2003 с настроенным анонимным (гостевым) доступом (см. таблицу поддерживаемых версий SMB в разных версиях Windows).

Microsoft рекомендует изменить настройки на удаленном компьютере или NAS устройстве, который раздает сетевые папки. Желательно переключить сетевой ресурс в режим SMBv3. А если поддерживается только протокол SMBv2, тогда нужно настроить доступ с аутентификацией. Это самый правильный и безопасный способ исправить проблему.

В зависимости от устройства, на котором хранятся сетевые папки, вы должны отключить на них гостевой доступ.

- **NAS устройство** – отключите гостевой доступ в настройках вашего NAS устройства (зависит от модели);
- **Samba сервер на Linux** — если вы раздаете SMB папку с Linux, добавьте в в секции [global] конфигурационного файла smb.conf строку: `map to guest = never`

А в секции с описанием сетевой папки запретить анонимный доступ: `guest ok = no`

- **В Windows** вы можете включить общий доступ к сетевым папкам и принтерам с парольной защитой в разделе Control Panel\All Control Panel Items\Network and Sharing Center\Advanced sharing settings. Для All Networks (Все сети) в секции “Общий доступ с парольной защитой” (Password Protected Sharing) измените значение на “**Включить общий доступ с парольной защитой**” (Turn on password protected sharing). В этом случае анонимный (гостевой) доступ к папкам будет отключен и вам придется создать локальных пользователей, предоставить им доступ к сетевым папкам и принтерам и использовать эти аккаунты для сетевого доступа к общим папкам на этом компьютере..
  Windows 10 Включить общий доступ с парольной защитой

Есть другой способ – изменить настройки вашего SMB клиента и разрешить доступ с него на сетевые папки под гостевой учетной записью.

Этот способ нужно использовать только как временный (!!!), т.к. доступ к папкам без проверки подлинности существенно снижает уровень безопасности ваших данных.

Чтобы разрешить гостевой доступ с вашего компьютера, откройте редактор локальных групповых политик (gpedit.msc) и перейдите в раздел: Конфигурация компьютера -> Административные шаблоны -> Сеть -> Рабочая станция Lanman (**Computer Configuration ->Administrative templates -> Network (Сеть) -> Lanman Workstation**). Включите политику **Enable insecure guest logons (Включить небезопасные гостевые входы)**.

Windows 10 политика Включить небезопасные гостевые входы

Обновите настройки групповых политик в Windows с помощью команды:

```
gpupdate /force
```

В Windows 10 Home, в которой нет редактора локальной GPO,вы можете внести аналогичное изменение через редактор реестра вручную::

```
 HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters “AllowInsecureGuestAuth”=dwo
```

Или такими командами:

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters /v AllowInsecureGuestAuth /t reg_dword /d 00000001 /f
reg add HKLM\Software\Policies\Microsoft\Windows\LanmanWorkstation /v AllowInsecureGuestAuth /t reg_dword /d 00000001 /f
```

Вашей системе необходимо использовать SMB2 или более позднюю

Другая возможная проблема при доступе к сетевой папке из Windows 10 – поддержка на стороне сервера только протокола SMBv1. Т.к. клиент SMBv1 по умолчанию отключен в Windows 10, то при попытке открыть шару или подключить сетевой диск вы можете получить ошибку:

```
Не удалось выполнить сопоставление сетевого диска из-за следующей ошибки.
Вы не можете подключиться к общей папке, так как она небезопасна. Эта общая папка работает по ус
Вашей системе необходимо использовать SMB2 или более позднюю версию.
```

```
You can’t connect to the file share because it’s not secure. This share requires the obsolete SM
```

Эта общая папка работает по устаревшему протоколу SMB1, который небезопасен и может по

При этом соседние устройства SMB могут не отображаться в сетевом окружении и при открытии сетевых папок по UNC пути может появляться ошибка 0x80070035.

Сообщение об ошибки явно указывает, что сетевая папка поддерживает только SMBv1 для доступа к файлам. В этом случае нужно попытаться перенастроить удаленное SMB устройство для поддержки как минимум SMBv2 (правильный и безопасный путь).

Если сетевые папки раздает Samba сервер на Linux, вы можете указать минимально поддерживаемую версию SMB в файле smb.conf так:

```
[global]
server min protocol = SMB2_10
client max protocol = SMB3
client min protocol = SMB2_10
encrypt passwords = true
restrict anonymous = 2
```

В Windows 7/Windows Server 2008 R2 вы можете отключить SMBv1 и разрешить SMBv2 так через реестр:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -
Type DWORD -Value 0 –Force
```

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -
Type DWORD -Value 1 –Force
```

В Windows 8.1 отключите SMBv1, разрешите SMBv2 и SMBv3 и проверьте что для вашего сетевого подключения используется частный или доменный профиль:

```
Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol"
Set-SmbServerConfiguration –EnableSMB2Protocol $true
```

Если ваше сетевое устройство (NAS, Windows XP, Windows Server 2003), поддерживает только протокол SMB1, в Windows 10 вы можете включить отдельный компонент SMB1Protocol-Client. **Но это не рекомендуется!!!**

Если удаленное устройство требует использовать SMBv1 для подключения, и этот протокол отключен в вашем устройстве Windows, в Event Viewer появляется ошибка:

```
Log Name: Microsoft-Windows-SmbClient/Security
Source: Microsoft-Windows-SMBClient
Event ID: 32000
Description:  SMB1 negotiate response received from remote device when SMB1 cannot be negotiated
```

Запустите консоль PowerShell и проверьте, что SMB1Protocol-Client отключен (`State: Disabled`):

```
Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol-Client
```

Включите поддержку протокола SMBv1 (потребуется перезагрузка):

```
Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol-Client
```

powershell - Enable-WindowsOptionalFeature SMB1Protocol-Client

Также вы можете включить/отключить SMBv1 в Windows 10 и 11 из меню `optionalfeatures.exe` -> SMB 1.0/CIFS File Sharing Support –> SMB 1.0/CIFS Client.

включить клиент smbv1 в windows 11

В Windows 10 1709 и выше клиент SMBv1 автоматически удаляется, если он не использовался более 15 дней (за это отвечает компонент SMB 1.0/CIFS Automatic Removal).

В этом примере я включил только SMBv1 клиент. Не включайте компонент SMB1Protocol-Server, если ваш компьютер не используется устаревшими клиентами в качестве сервера для хранения общих папок.

После установке клиента SMBv1, вы должны без проблем подключиться к общей сетевой папке или принтеру. Однако, нужно понимать, что использование данного обходного

решения не рекомендовано, т.к. подвергает снижает уровень безопасности.

Нет доступа к сетевой папке, у вас нет прав доступа

При подключении к сетевой папке на другом компьютере может появится ошибка:

```
Нет доступа к \\ComputerName\Share. Возможно у вас нет прав на использование этого сетевого ресу
```

```
Network Error
Windows cannot access \\PC12\Share
You do not have permissions to access \\PC12\Share. Contact your network administrator to reques
```

windows не открывается сетевая папка нет доступа

При появлении это ошибки нужно:

1. Убедиться, что пользователю, под которым вы подключаетесь к сетевой папке, предоставлены права доступа на сервере. Откройте свойства общей папке на сервере и убедитесь что у вашего пользователя есть права доступа.
   Проверьте разрешения сетевой шары на сервере с помощью PowerShell:
   `Get-SmbShareAccess -Name "tools"`
   Затем проверьте NTFS разрешения:
   `get-acl C:\tools\ |fl`
   проверьте разрешения доступа на сетевую папку с помощью powershell
   Если нужно, отредактируйте разрешения в свойствах папки.
2. Проверьте, что вы используете правильные имя пользователя и пароль для доступа к сетевой папки. Если имя и пароль не запрашиваются, попробуйте удалить сохраненные пароли для доступа к сетевой папке в диспетчере учетных записей Windows. Выполните команду `rundll32.exe keymgr.dll, KRShowKeyMgr` и удалите сохраненные учетные данные для доступа к сетевой папке.
   очистити сохраненные пароли для доступа к сетевым папкам
   При следующем подключении к сетевой папки появится запрос имени и пароля. Укажите имя пользователя для доступа к папке. Можете сохранить его в Credential Manager или добавить вручную.

Дополнительные способы проверки доступа к сетевой папке в Windows

В этом разделе указаны дополнительные способы диагностики при проблема с открытием сетевые папок в Windows:

- Убедитесь, что удаленный разрешает входящие подключения к сетевым папкам по протоколу SMB (порт TCP 445). Проверить доступность порта 445 на удаленном компьютер можно с помощью команды Test-NetConnection: `Test-NetConnection -ComputerName ImyaKomputera -Port 445`
  проверить доступность 445 TCP порта SMB для доступа к общим папкам
  Если командлет вернет, `TcpTestSucceeded : False`, значит доступ к сетевым папка на удаленном компьютере блокируется файерволом. Подключение может блокироваться антивирусом или файерволом (сторонним или встроенным Windows Defender Firewall). Если используется Windows Defender, включите на сервере правило **File and Printer Sharing** (Control Panel\System and Security\Windows Defender Firewall\Allowed apps\Allow apps to communicate through Windows Firewall) для всех трех профилей.
  правило windows defender для доступа к общим сетевым папкам в windows firewall
  Или создайте правило файервола с помощью PowerShell: `New-NetFirewallRule -DisplayName "AllowFileSharingSMB"  -Direction Inbound -Protocol TCP –LocalPort 445 -Action Allow`
- Если вы не можете открыть сетевые папки, попробуйте очистить сохраненные пароли в Windows Credential, удалить сетевые папки (команда `Net Use * /delete`) и подключить их заново
- Проверьте использовать для доступа IP адрес удаленного компьютера вместо его имени, например `Win+R` -> `\\192.168.120.12` -> Ok.
- Убедитесь что ваши компьютер находятся в рабочей группе с одинаковым именем. Имя рабочей группы на компьютере можно узнать так: `Get-WmiObject Win32_ComputerSystem).domain`
- Сбросьте настройки TCP/IP стека и обновите IP адрес на вашем компьютере: `netsh int ip reset`
  `netsh winsock reset`
  `ipconfig /flushdns`
  `ipconfig /release`
  `ipconfig /renew`

Revision #1
Created 2026-11-19 12:39:37 UTC by Admin
Updated 2026-11-19 12:41:36 UTC by Admin