

[Windows 10](#)[Устройства](#)[Приложения+игры](#)[Загрузки](#)[Инструкции](#)[Windows 10](#)[Windows 10 Mobile](#)[Предыдущие версии](#)

Все о брандмауэре Windows

Применимо к Windows 8.1

Что такое брандмауэр?

Брандмауэр — это программа или оборудование, которое препятствует злоумышленникам и некоторым типам вредоносных программ получать доступ к компьютеру по сети или через Интернет. Для этого брандмауэр проверяет данные, поступающие из Интернета или по сети, и блокирует их или разрешает передачу на компьютер.

Брандмауэр отличается от антивирусного и антивредоносного приложений. Брандмауэр защищает от червей и злоумышленников, антивирусные программы защищают от вирусов, а антивредоносное ПО защищает от вредоносных программ. Необходимо использовать все три типа защиты. Можно воспользоваться Защитником Windows (это антивирусное и антивредоносное ПО поставляется вместе с Windows 8) или использовать другое приложение для защиты от вирусов и вредоносных программ.

На компьютере должно работать только одно приложение брандмауэра (в дополнение к брандмауэру, который обычно встраивается в сетевой маршрутизатор). Наличие нескольких приложений брандмауэра на компьютере может вызывать конфликты и проблемы.

Брандмауэр Windows входит в комплект Windows и по умолчанию включен.

Работа брандмауэра показана на следующем рисунке.



Брандмауэр создает барьер между Интернетом и компьютером

Рекомендуется использовать следующие параметры брандмауэра по умолчанию.

- Брандмауэр включен для всех сетевых подключений.
- Брандмауэр блокирует все входящие подключения, кроме явно разрешенных пользователем.
- Брандмауэр включен для всех типов сетей (частные, публичные и доменные).

Примечание.

Компьютеры под управлением Windows RT или Windows 8 нельзя присоединить к домену. Вы можете присоединить к домену только компьютеры под управлением Windows 8 Профессиональная или Windows 8 Корпоративная.

Включение и отключение брандмауэра Windows

Брандмауэр Windows не следует отключать, пока не включен другой брандмауэр. Отключение брандмауэра Windows может повысить уязвимость компьютера (и сети) к червям и злоумышленникам.

1. Откройте брандмауэр Windows. Для этого быстро проведите пальцем от правого края экрана и коснитесь элемента **Поиск**. (Если вы используете мышь, поместите курсор в правый верхний угол экрана, затем переместите его вниз и щелкните **Поиск**.) После этого в поле поиска введите **брандмауэр**, а затем выберите элемент **Брандмауэр Windows**.

2. Выберите пункт **Включение и отключение брандмауэра Windows**.  Требуется разрешение администратора. Вам может потребоваться ввести пароль учетной записи администратора или подтвердить выбор.

3. Выполните одно из указанных ниже действий.


- Щелкните или коснитесь **Включить брандмауэр Windows** для каждого типа сети, в котором нужно включить защиту, а затем нажмите **ОК**.
- Щелкните или коснитесь **Отключить брандмауэр Windows (не рекомендуется)** для каждого типа сети, в котором нужно отключить защиту, а затем нажмите **ОК**.

Примечание.

Если компьютер подключен к сети, параметры политики сети могут помешать выполнению данных действий. За дополнительными сведениями обращайтесь к администратору.

Общие сведения о параметрах брандмауэра Windows

Для каждого типа сети (публичные, частные, доменные) можно настроить четыре параметра. Эти параметры можно найти, выполнив следующие действия.

1. Откройте брандмауэр Windows. Для этого быстро проведите пальцем от правого края экрана и коснитесь элемента **Поиск**. (Если вы используете мышь, поместите курсор в правый верхний угол экрана, затем переместите его вниз и щелкните **Поиск**.) После этого в поле поиска введите **брандмауэр**, а затем выберите элемент **БрандмауэрWindows**.
2. Выберите пункт **Включение и отключение брандмауэра Windows**.  Вам может потребоваться ввести пароль учетной записи администратора или подтвердить выбор.

Далее описывается назначение параметров и условия их использования.

- **Включить брандмауэр Windows**. Эта настройка выбрана по умолчанию. Когда брандмауэр Windows включен, большинство приложений не могут получать данные через брандмауэр. Чтобы разрешить приложению получение данных, добавьте его в список разрешенных, как описано в следующем разделе. В частности, вы не сможете получать фотографии через приложение передачи мгновенных сообщений, пока это приложение не будет добавлено в список разрешенных.
- **Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ**. Этот параметр блокирует все неожиданные попытки подключения к компьютеру. Используйте его, чтобы обеспечить максимальную защиту компьютера, например при подключении к публичной сети в гостинице или в аэропорту. При блокировке всех входящих подключений можно просматривать большинство веб-страниц, отправлять и принимать электронную почту, а также отправлять и принимать мгновенные сообщения.
- **Уведомлять, когда брандмауэр Windows блокирует новое приложение**. Если установлен этот флажок, то брандмауэр Windows уведомляет пользователя о блокировке нового приложения и дает возможность отменить блокировку.
- **Отключить брандмауэр Windows (не рекомендуется)**. Не выбирайте этот параметр, если на компьютере не работает другое приложение брандмауэра.

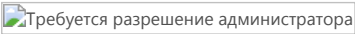
Примечание.

Если некоторые параметры брандмауэра недоступны, а компьютер подключен к домену, то, возможно, этими параметрами управляет системный администратор посредством групповой политики.

Разрешение получения данных через брандмауэр для приложения

По умолчанию брандмауэр Windows блокирует большинство приложений, чтобы повысить безопасность компьютера. Для полноценной работы некоторых приложений может потребоваться получение данных через брандмауэр.

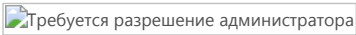
Прежде чем разрешать приложению получать данные через брандмауэр, необходимо оценить все риски, связанные с таким подключением. Подробнее: [В чем состоит риск при открытии приложениям доступа через брандмауэр?](#)

1. Откройте брандмауэр Windows. Для этого быстро проведите пальцем от правого края экрана и коснитесь элемента **Поиск**. (Если вы используете мышь, поместите курсор в правый верхний угол экрана, затем переместите его вниз и щелкните **Поиск**.) После этого в поле поиска введите **брандмауэр**, а затем выберите элемент **БрандмауэрWindows**.
2. Коснитесь или щелкните **Разрешение взаимодействия с приложением или компонентом в брандмауэре Windows**.
3. Нажмите кнопку **Изменить параметры**.  Вам может потребоваться ввести пароль учетной записи администратора или подтвердить выбор.
4. Установите флажок рядом с приложением, которое следует разрешить, выберите типы сетей, в которых вы хотите разрешить обмен данными, и нажмите **ОК**.

Открытие порта в брандмауэре Windows

Если брандмауэр Windows блокирует приложение, а вы хотите разрешить этому приложению получение данных через брандмауэр, то для этого нужно выбрать приложение в списке разрешенных, как описано в предыдущем разделе.

Если приложение отсутствует в списке, то может понадобиться открыть порт (приложения получают данные через брандмауэр посредством портов). Например, чтобы играть с друзьями в многопользовательскую игру по Интернету, необходимо открыть порт для этой игры так, чтобы брандмауэр разрешал передачу ее данных на компьютер. Порт остается открытым постоянно, поэтому закрывайте порты, если они больше не требуются.

1. Откройте брандмауэр Windows. Для этого быстро проведите пальцем от правого края экрана и коснитесь элемента **Поиск**. (Если вы используете мышь, поместите курсор в правый верхний угол экрана, затем переместите его вниз и щелкните **Поиск**.) После этого в поле поиска введите **брандмауэр**, а затем выберите элемент **БрандмауэрWindows**.
2. Выберите пункт **Дополнительные параметры**.  Вам может потребоваться ввести пароль учетной записи администратора или подтвердить выбор.
3. В левой части диалогового окна **Брандмауэр Windows в режиме повышенной безопасности** выберите ссылку **Правила для входящих подключений**, а затем в правой части окна нажмите кнопку **Создать правило**.

4. Следуйте инструкциям на экране.

Нужна дополнительная справка?

Узнайте все о [безопасности](#), [конфиденциальности](#) и [учетных записях](#).

Задайте вопрос на [форумах сообщества](#).

Привет из Сиятла!

Россия

[Заявления об отказе](#)

[Условия использования](#)

[Товарные знаки](#)

© 2016 Microsoft

[Конфиденциальность и файлы cookie](#)

[Карта сайта](#)