

Windows Defender Firewall

Control Panel > System and Security > Windows Defender Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks

Not connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:

On

Incoming connections:

Block all connections to apps that are not on the list of allowed apps

Active private networks:

None

Notification state:

Notify me when Windows Defender Firewall blocks a new app

Guest or public networks

Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:

On

Incoming connections:

Block all connections to apps that are not on the list of allowed apps

Active public networks:

XPON-FA88

Notification state:

Notify me when Windows Defender Firewall blocks a new app

See also

Security and Maintenance

Network and Sharing Center

Customize Settings

Control Panel > System and Security > Windows Defender Firewall > Customize Settings

Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app

Turn off Windows Defender Firewall (not recommended)

Public network settings

Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app

Turn off Windows Defender Firewall (not recommended)

OK

Cancel

## Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

### Allowed apps and features:

Name	Private	Public
<input checked="" type="checkbox"/> Get Help	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Google Chrome	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> HomeGroup	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> iSCSI Service	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Key Management Service	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Mail and Calendar	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> mDNS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Media Center Extenders	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Microsoft 365 (Office)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Microsoft Content	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Microsoft Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Microsoft Edge WebView2 Runtime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Details...

Remove

Allow another app...

OK

Cancel

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security on Local Computer

Overview

**Domain Profile**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

**Private Profile**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

**Public Profile is Active**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

[Windows Defender Firewall Properties](#)

Getting Started

**Authenticate communications between computers**

Create connection security rules to specify how and when connections between computers are protected by using Internet Protocol security (IPsec).

[Connection Security Rules](#)

**View and create firewall rules**

Create firewall rules to allow or block connections to specified programs or ports. You can also create rules to allow or block connections based on the type of traffic, the source or destination IP address, or the protocol used. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

**Actions**

- Windows Defender Firewall with Advanced Security on Local Computer
- Import Policy...
- Export Policy...
- Restore Default Policy
- Diagnose / Repair
- View
- Refresh
- Properties
- Help

Windows Defender Firewall with Advanced Security

FileActionViewHelp

Windows Defender Firewall with Advanced Security

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Name	Group	Profile
adb.exe		Public
adb.exe		Private
adb.exe		Private
adb.exe		Public
Android Studio		Private
Android Studio		Private
Apache HTTP Server		Private
Apache HTTP Server		Public
Apache HTTP Server		Public
Apache HTTP Server		Private
armored alliance		Private
armored alliance		Private
armored alliance		Public
armored alliance		Public
broker.exe		Private
broker.exe		Private
DVDPlayer		Private
DVDPlayer		Private
EaseUS Data Recovery Wizard		All
Microsoft Office Outlook		Private
Microsoft Visual Studio 2019		Private
Microsoft Visual Studio 2019		Private
Microsoft Visual Studio 2019		Public
Microsoft Visual Studio 2019		Public
mysqld		Private
mysqld		Private
mysqld		Public
mysqld		Public
netsimd.exe		Private
netsimd.exe		Private
Skype for Business		Private
Skype for Business		Private

Inbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

Windows Defender Firewall with Advanced Security

FileActionViewHelp

Windows Defender Firewall with Advanced Security

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Outbound Rules

Name	Group	Profile
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All
Skype	{78E1CD88-49E3-476E-B926-...	All
Skype	{78E1CD88-49E3-476E-B926-...	All
3D Viewer	3D Viewer	All
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...
App Installer	App Installer	All
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All
Captive Portal Flow	Captive Portal Flow	All
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain
Cloud Identity (TCP-Out)	Cloud Identity	All
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...
Core Networking - DNS (UDP-Out)	Core Networking	All
Core Networking - Dynamic Host Config...	Core Networking	All
Core Networking - Dynamic Host Config...	Core Networking	All
Core Networking - Group Policy (LSASS-...	Core Networking	Domain
Core Networking - Group Policy (NP-Out)	Core Networking	Domain
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain
Core Networking - Internet Group Mana...	Core Networking	All
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All
Core Networking - IPv6 (IPv6-Out)	Core Networking	All
Core Networking - Multicast Listener Do...	Core Networking	All
Core Networking - Multicast Listener Qu...	Core Networking	All

Actions

Outbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

## Rule Type

Select the type of firewall rule to create.

### Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

- ☐ **Program**  
Rule that controls connections for a program.
- ☒ **Port**  
Rule that controls connections for a TCP or UDP port.
- ☐ **Predefined:**  

@FirewallAPI.dll,-80200

  
Rule that controls connections for a Windows experience.
- ☐ **Custom**  
Custom rule.

< Back

Next >

Cancel

## Protocol and Ports

Specify the protocols and ports to which this rule applies.

### Steps:

- Rule Type
- Protocol and Ports**
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

- ☒ **TCP**
- ☐ **UDP**

Does this rule apply to all remote ports or specific remote ports?

- ☒ **All remote ports**
- ☐ **Specific remote ports:**

Example: 80, 443, 5000-5010

< Back

Next >

Cancel

**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

**Steps:**

- Rule Type
- Protocol and Ports
- Action
- Computers
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

- ☐ **Allow the connection**  
This includes connections that are protected with IPsec as well as those are not.
- ☒ **Allow the connection if it is secure**  
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
- ☐ **Block the connection**

Customize...

< Back

Next >

Cancel

## Profile

Specify the profiles for which this rule applies.

### Steps:

- Rule Type
- Protocol and Ports
- Action
- Computers
- Profile
- Name

When does this rule apply?

- ☒ **Domain**  
Applies when a computer is connected to its corporate domain.
- ☒ **Private**  
Applies when a computer is connected to a private network location, such as a home or work place.
- ☒ **Public**  
Applies when a computer is connected to a public network location.

< Back

Next >

Cancel



Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Outbound Rules

Name	Group	Profile
Basic Firewall Rule Tasks		All
@FirewallAPI.dll, -80204	@FirewallAPI.dll, -80200	All
Skype	{78E1CD88-49E3-476E-B926-...	All
Skype	{78E1CD88-49E3-476E-B926-...	All
3D Viewer	3D Viewer	All
AllJoyn Router (TCP-Out)	AllJoyn Router	Domain...
AllJoyn Router (UDP-Out)	AllJoyn Router	Domain...
App Installer	App Installer	All
BranchCache Content Retrieval (HTTP-Out)	BranchCache - Content Retr...	All
BranchCache Hosted Cache Client (HTTP-Out)	BranchCache - Hosted Cach...	All
BranchCache Hosted Cache Server (HTTP-Out)	BranchCache - Hosted Cach...	All
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All
Captive Portal Flow	Captive Portal Flow	All
Cast to Device functionality (qWave-TCP-Out)	Cast to Device functionality	Private...
Cast to Device functionality (qWave-UDP-Out)	Cast to Device functionality	Private...
Cast to Device streaming server (RTP-Streaming-Out)	Cast to Device functionality	Public
Cast to Device streaming server (RTP-Streaming-Out)	Cast to Device functionality	Private
Cast to Device streaming server (RTP-Streaming-Out)	Cast to Device functionality	Domain
Cloud Identity (TCP-Out)	Cloud Identity	All
Connected Devices Platform - Wi-Fi Direct	Connected Devices Platform	Public
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domain...
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domain...
Core Networking - DNS (UDP-Out)	Core Networking	All
Core Networking - Dynamic Host Configuration Protocol	Core Networking	All
Core Networking - Dynamic Host Configuration Protocol	Core Networking	All
Core Networking - Group Policy (LSASS-Out)	Core Networking	Domain
Core Networking - Group Policy (NP-Out)	Core Networking	Domain
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain
Core Networking - Internet Group Management Protocol	Core Networking	All
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All
Core Networking - IPv6 (IPv6-Out)	Core Networking	All
Core Networking - Multicast Listener Discovery	Core Networking	All

Actions

Outbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Basic Firewall Rule Tasks

- Disable Rule
- Cut
- Copy
- Delete
- Properties
- Help