



**Airscanner Mobile Firewall 3.0
User Manual**

1. Airscanner Mobile Firewall Basics

Airscanner Mobile Firewall 3.0 is an **IPv4** firewall designed to protect your Windows Mobile device from unauthorized external and internal access. The firewall is designed to block traffic at the IP and transport layers of the TCP/IP stack. The firewall works with 3 protocols: **ICMP**, **TCP** and **UDP** by **identifying the authorized list of ports that can communicate using the selected protocol.**

The **Traffic Flow** is specified as INBOUND and OUTBOUND traffic:

- **INBOUND:** Traffic that comes from the Network to the Device.
- **OUTBOUND:** Traffic that goes from Device out to the Network.

The firewall has a default mode of operation where internal, pre-defined rules are active while the firewall driver is loaded. However, you have granular control of the firewall's behavior and also of Default Mode operation via [Profiles](#).

1.2 Firewall Default Mode

The firewall starts in Default Mode when you switch to [Custom Mode profile](#).

In Default Mode, the firewall **blocks all inbound packets and allows all outbound packets.**

You can create your own rules only when working with a [Custom Mode profile](#). When conflicting rules are applied, one of the rules overrides the other depending on whether it is incoming or outgoing traffic. Only the packets that match the overriding rule are filtered according to the rule. **If the traffic does not match the overridden rule, it is processed according to the default behavior.** We will explain this later with some examples.

When the Allow and Block rules are applied in conjunction, traffic flow is controlled as follows:

- **For incoming traffic, all Block rules override the Allow rules.**
- **For outgoing traffic, all Allow rules override the Block rules.**

2. Mobile Firewall Features Reference

The following pages explain Airscanner Mobile Firewall's Graphical User Interface (GUI) features.

2.1 Main Screen and Menus

The Mobile Firewall GUI can fit in any screen resolution with minimum size of 240x240.


	<h3><u>Mobile Firewall Main Screen</u></h3> <p>The Main Screen has the following components:</p> <ol style="list-style-type: none">1. A device information panel with some items. (That panel is hidden on Square Screen Devices).2. A Main Menu that gives access to all GUI features.3. A panel that shows the current device IP and selected firewall profile.4. An Options Menu (see Figure 2).
---	--

Figure 1. Main Screen


	<h3><u>Options Menu</u></h3> <p>The Options Menu offers quick access to some of the firewall's most popular features.</p> <p>Not all features are present in the Options Menu.</p> <p>Note: The Disabled profile is only accessed via the Options Menu. It is not in the Main Menu.</p>
--	--

Figure 2. Options Menu



	<u>Tray Menu</u>
	<p>When you tap on the OK button (on the upper right corner of the firewall main screen), the firewall is minimized, but not closed.</p> <p>The Tray Menu offers the same options as the Options Menu.</p> <p>The Tray Icon shows the current selected firewall profile with a small sphere adjacent to the red Airscanner Icon.</p>
	

Figure 3. Tray Menu

2.2 Set Profile Menu



Airscanner Mobile Firewall has four operational modes, which are named as the following general profiles: **Block All**, **Trust All**, **Custom Mode** and **Disabled**.

You can have only one profile active at a time. When you switch to one of the profiles mentioned above, a group of rules is activated to configure the Firewall:

Block All

When the Firewall is running in the **Block All** profile, all network traffic is blocked. No [INBOUND](#) or [OUTBOUND](#) traffic is allowed on the covered protocols. This profile disables the firewall [Default Mode](#).

Trust All

When the Firewall is running in the **Trust All** profile, all network traffic is allowed. No restrictions are applied, although the Firewall is active and running. This profile disables the firewall [Default Mode](#).

Custom Mode

Custom mode allows you to create and activate your own rules. Custom mode comes with some predefined-rules (called Factory Rules, which are present in the **Custom Profiles Menu**) that the user can enable or disable. If you want to create your own rules you can use the **User Rules** option in the **Custom Profiles Menu**.

Then, when you switch to the Custom Mode profile, two groups of rules are applied: [Factory Rules](#) and [User Rules](#).

Custom Mode works together with [Default Mode](#). Thus, the default behavior is applied to traffic that is not covered by the rules.

If you want the Firewall to work only on Default Mode you simply switch to the **Custom Mode** profile and disable all rules via the [Custom Profiles Menu](#).

Disabled

This turns off the Firewall. You can switch to the Disabled profile via [Options Menu](#).

2.3 Custom Profiles Menu



The **Custom Profiles Menu** allows you to create and manage your own rules.



Factory Rules

When you select the **Factory Rules** option, you can enable/disable and view Factory rules. Other operations like Add or Delete are not allowed for this profile. When this rule is checked it is marked as enabled.

In the attached screen shot, the rule named as **External ICMP Echo Response** is disabled.

You can disable all rules if you want and only use only your own rules.

See Appendix B for an explanation about **Factory Rules**.

IMPORTANT: Changes are immediately applied to the firewall if the [Custom Mode profile](#) is the active profile.

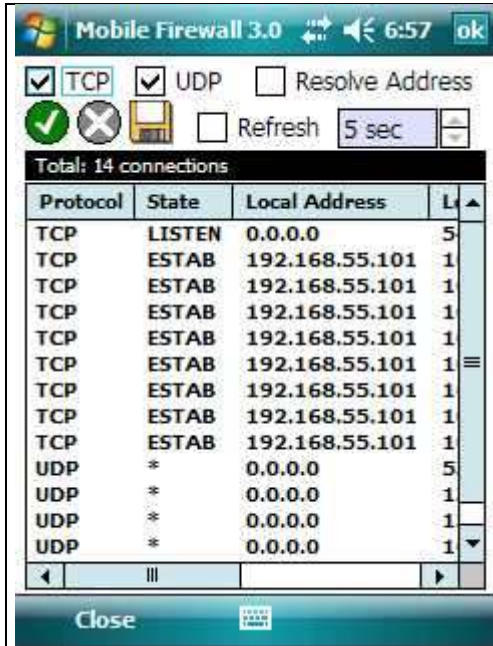


User Rules

When you select the **User** option, you can add, edit, delete, enable/disable and view your own rules.

IMPORTANT: Changes are immediately applied to the firewall if the [Custom Mode profile](#) is the active profile.

2.4 Tools Menu

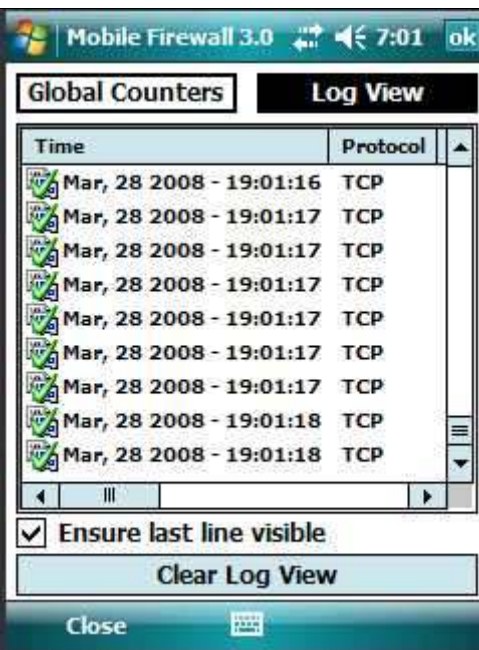
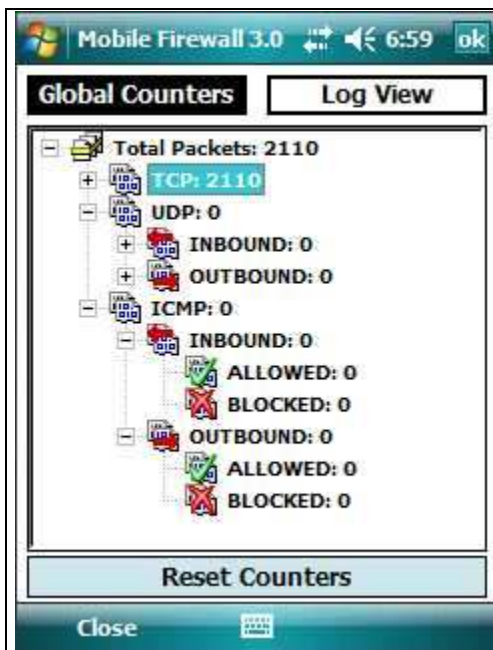


List Conn (“List connections”)

This feature allows you to view the current TCP/UDP resources being used.

You can save results in a file into the Personal Folder (\My Documents) any time. The file is a .text-formatted file.

Resolve Address – when this option is checked, IP addresses are translated to host names (if applicable).



Activity Log

This feature has two sub features:

Global Counters: shows a tally of all IP activity for TCP, UDP and ICMP protocols. Hitting the button labeled “Reset Counters” zeroes the counters.

Log View: shows up to the last 100 lines of log activity.

NOTE: Log Firewall Activity (in [Settings](#)) must be checked if you want the Activity Log do any logging.

2.5 Settings Option

	<h3 style="text-align: center;"><u>Settings</u></h3> <p>Load Firewall at Startup: Loads the firewall GUI and Firewall driver during a soft-reset.</p> <p>Log Firewall Activity: Enable/Disable firewall logs information to a file and Activity Log (Tools Menu). When this option is checked, a log file is saved into the personal folder; this is limited to the Max Size option. If you select “(do not log to file)” only Activity Log (Tools Menu) keeps logging.</p> <p>IMPORTANT: Logging activity to a file might make the device run slower.</p>
--	--

2.6 Log File

If you want to read the Log File, you should copy it to the Desktop computer and open it with a normal text editor.

The following is a sample from the log file:

	ACTION	PROTOCOL	DIRECTION	SOURCE	TARGET	SOURCE	TARGET	TYPE	CODE
	-----	-----	-----	-----	-----	-----	-----	-----	-----
[Feb, 17 2008 16:38:51]=>	ALLOWED	UDP	OUTBOUND	0.0.0.0	255.255.255.255	68	67	***	***
[Feb, 17 2008 16:38:51]=>	ALLOWED	UDP	INBOUND	0.0.0.0	255.255.255.255	68	67	***	***
[Feb, 17 2008 16:38:52]=>	ALLOWED	UDP	INBOUND	1.1.1.30	1.1.1.255	137	137	***	***
[Feb, 17 2008 16:38:52]=>	ALLOWED	UDP	OUTBOUND	1.1.1.30	1.1.1.255	137	137	***	***
[Feb, 17 2008 16:38:52]=>	ALLOWED	UDP	INBOUND	1.1.1.30	1.1.1.255	137	137	***	***
[Feb, 17 2008 16:39:16]=>	BLOCKED	TCP	INBOUND	169.254.2.2	169.254.2.1	990	1052	***	***
[Feb, 17 2008 16:39:17]=>	BLOCKED	TCP	INBOUND	169.254.2.2	169.254.2.1	990	1052	***	***
[Feb, 17 2008 16:39:18]=>	BLOCKED	ICMP	INBOUND	169.254.2.2	169.254.2.1	***	***	8	0

After date and time, the columns are explained as follows:

- **ACTION:** indicates if the packet was blocked or allowed
- **PROTOCOL:** can be TCP, UDP or ICMP.
- **SOURCE:** Source IP
- **TARGET:** Target IP
- **SOURCE:** Source PORT (for TCP and UDP)
- **TARGET:** Target PORT (for TCP and UDP)
- **TYPE:** ICMP [Type](#)
- **CODE:** ICMP [Code](#)

3. Creating Rules

You can create your own rules via the [Custom Profiles Menu](#), [User Rules](#) option. All rules that you create become active only when the current profile is [Custom Mode Profile](#).

As explained previously, when the firewall is operating in the [Custom Mode Profile](#) it works on [Default Mode](#) and follows rules defined in [Custom Profiles Menu](#) and [User Rules](#). . Then, **If the traffic does not match the overridden rule, it is processed according to the default behavior.**

3.1 Samples of Rules

The following subsections give some examples of how to create rules correctly.

Please keep two things in mind:

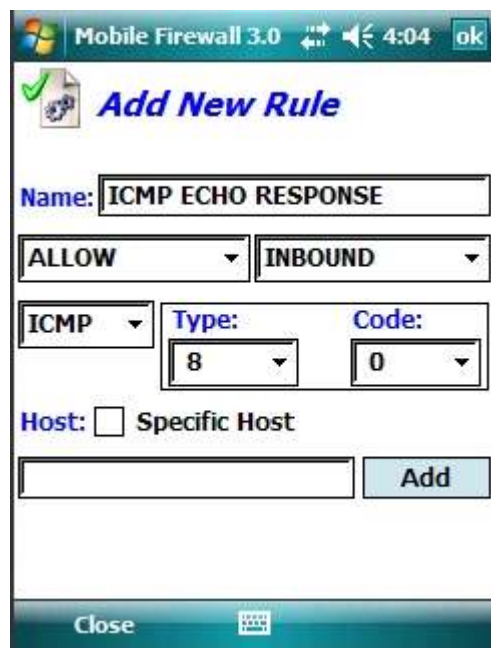
1. In Default Mode, the firewall **blocks all inbound packets and allows all outbound packets.**

2. When the rules are active:

For incoming traffic, all Block rules override the Allow rules.
For outgoing traffic, all Allow rules override the Block rules.

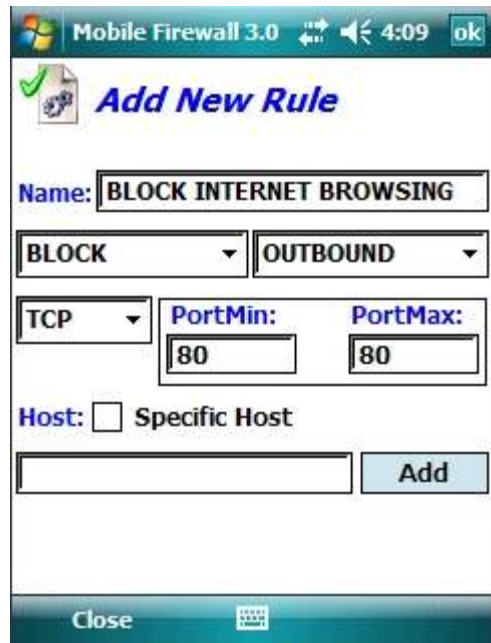
3.1.1 Allowing ICMP Echo Response

To allow ICMP echo response you must allow an [INBOUND](#) ICMP Echo Request. (Default Mode already allows the [OUTBOUND](#) ICMP Echo response):

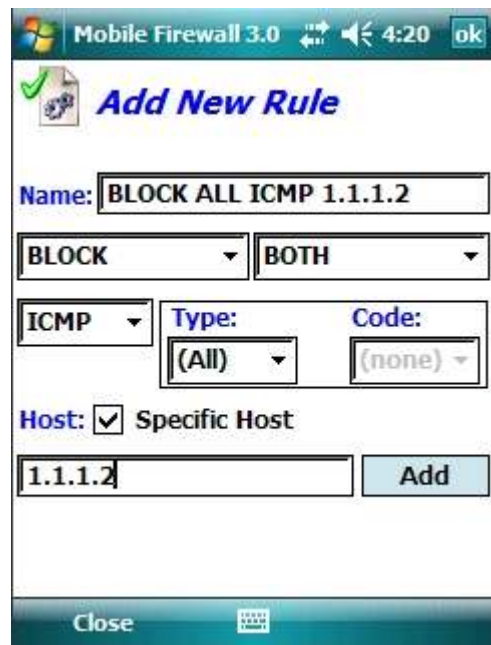


3.1.2 Blocking Internet Browsing

The [OUTBOUND](#) traffic is allowed (by default) on PORT 80. See the following screenshot on how to block it:



3.1.3 Blocking any ICMP communication from/to specific HOST (screenshot below)



For comments or questions, please contact us via our contact page at: <http://airscanner.com/contact.php>

Appendix A: ICMP Types and Codes

Above a list of all ICMP types and codes and its respective meanings:

ICMP Types		ICMP Codes	
0	Echo Reply	(none)	
3	Destination Unreachable	0	<i>Net Unreachable</i>
		1	<i>Host Unreachable</i>
		2	<i>Protocol Unreachable</i>
		3	<i>Port Unreachable</i>
		4	<i>Fragmentation Needed and Don't Fragment was Set</i>
		5	<i>Source Route Failed</i>
		6	<i>Destination Network Unknown</i>
		7	<i>Destination Host Unknown</i>
		8	<i>Source Host Isolated</i>
		9	<i>Communication with Network is Administratively Prohibited</i>
		10	<i>Communication with Host is Administratively Prohibited</i>
		11	<i>Destination Network Unreachable for Type of Service</i>
		12	<i>Destination Host Unreachable for Type of Service</i>
		13	<i>Communication Administratively Prohibited</i>
		14	<i>Host Precedence Violation</i>
15	<i>Precedence cutoff in effect</i>		
4	Source Quench	(none)	
5	Redirect	0	<i>Redirect Datagram for the Network (or subnet)</i>
		1	<i>Redirect Datagram for the Host</i>
		2	<i>Redirect Datagram for the Type of Service and Network</i>
		3	<i>Redirect Datagram for the Type of Service and Host</i>
6	Alternate Host Address	(none)	
8	Echo	(none)	
9	Router Advertisement	0	<i>Normal router advertisement</i>
		16	<i>Does not route common traffic</i>
10	Router Selection	(none)	
11	Time Exceeded	0	<i>Time to Live exceeded in Transit</i>
		1	<i>Fragment Reassembly Time Exceeded</i>
12	Parameter Problem	0	<i>Pointer indicates the error</i>
		1	<i>Missing a Required Option</i>
		2	<i>Bad Length</i>
13	Timestamp	(none)	
14	Timestamp Reply	(none)	
15	Information Request	(none)	
16	Information Reply	(none)	
17	Address Mask Request	(none)	
18	Address Mask Reply	(none)	
30	Traceroute	(none)	
31	Datagram Conversion Error	(none)	
32	Mobile Host Redirect	(none)	

33	IPv6 Where-Are-You	(none)
34	IPv6 I-Am-Here	(none)
35	Mobile Registration Request	(none)
36	Mobile Registration Reply	(none)
40	Authentication Failures	0 <i>Bad SPI</i>
		1 <i>Authentication Failed</i>
		2 <i>Decompression Failed</i>
		3 <i>Decryption Failed</i>
		4 <i>Need Authentication</i>
		5 <i>Need Authorization</i>

Appendix B: Factory Rules Description

On Custom Mode Profile Airscanner provides some rules, called Factory Rules. Some of them are disabled by default:

Rule	Type	Description
ActiveSync 4.x Rules	ALLOW	These 6 rules allow ActiveSync (Windows XP) or Mobile Center (VISTA) connect to device. They enable services like RAPI Requests, Time Server and Synchronization Information.
DHCP Unicast Response	ALLOW	Allows DHCP assigns IP address to device.
ICMP - Destination Unreachable	BLOCK	Blocks UDP port scanning by avoiding ICMP response.
ICMP – External Echo Request	ALLOW	Allow Pings to your device.
Internet Browsing	BLOCK	Block internet browsing when enabled
POP3 – Email	BLOCK	Block pocket outlook of getting emails.
SMTP – Email	BLOCK	Block pocket outlook of sending emails.
TCP Inbound Ports 0-1024	ALLOW	Allow TCP basic ports to be accessed.
UDP Broadcasting	BLOCK	Avoid UDP broadcast from external network.
UDP Ports 137-138	ALLOW	Enable UDP ports 137 (naming service) and 138 (NetBIOS datagram service).