

How to configure RS to block IM and P2P connection

1. Setup RS gateway ready, and make sure RS gateway can connect to Internet.
2. Enter RS gateway web management page, and select **Policy Object** → **Application Blocking** (**RS-1200: IM/P2P Blocking**)

The screenshot shows the Air Live web management interface. The left sidebar contains a menu with the following items: System, Interface, Policy Object, Address, Service, Schedule, QoS, Authentication, Content Blocking, Application Blocking (highlighted with a red box), Virtual Server, VPN, Policy, Mail Security, IDP, Anomaly Flow IP, and Monitor. The main content area is titled "Policy Object > Application Blocking > Setting". It includes a section for "Application Signature Definitions" with a "Update NOW" button. Below this is a table for "Application Blocking" with columns for Name, Application, and Configure. A "New Entry" button is located below the table.

3. Click "**Update NOW**" to renew application signature. Click "**New Entry**" to create new blocking rule.

The screenshot shows the "Add Application Blocking" form in the Air Live web management interface. The left sidebar is the same as in the previous screenshot. The main content area is titled "Policy Object > Application Blocking > Setting". The form has a "Name" field with the value "Application_1" and a "(Max. 16 characters)" label. Below the name field are three sections of checkboxes for selecting applications to block:

- Instant Messaging Login (☐ Select All)**
 - ☒ MSN
 - ☐ Skype
 - ☐ WebIM
 - ☒ Yahoo
 - ☐ Google Talk
 - ☐ AliSoft
 - ☐ ICQ/AIM
 - ☐ Gadu-Gadu
 - ☐ Fetion
 - ☐ QQ/TM2008
 - ☐ Rediff
- Instant Messaging File Transfer (☐ Select All)**
 - ☐ MSN
 - ☐ Google Talk
 - ☐ Yahoo
 - ☐ Gadu-Gadu
 - ☐ ICQ/AIM
 - ☐ QQ
- Peer-to-Peer Application (☐ Select All)**
 - ☒ Edonkey
 - ☐ KuGoo
 - ☐ iMesh
 - ☐ QQDownload
 - ☐ Morpheus
 - ☒ Bit Torrent
 - ☐ AppleJuice
 - ☐ MUTE
 - ☐ Ares
 - ☐ Limewire
 - ☐ WinMX
 - ☐ AudioGalaxy
 - ☐ Thunder5
 - ☐ Shareaza
 - ☐ KaZaa
 - ☐ Foxy
 - ☐ DirectConnect
 - ☐ GoGoBox
 - ☐ BearShare
 - ☐ Clubbox

4. Assign a rule name and select the application that you want to block; click OK to save the setting.

Air Live® Policy Object > Application Blocking > Setting www.airlive.com

Add Application Blocking

Name: (Max. 16 characters)

☐ Select All

☒ MSN ☒ Yahoo ☐ ICQ/AIM ☐ QQ/TM2008
☐ Skype ☐ Google Talk ☐ Gadu-Gadu ☐ Rediff
☐ WebIM ☐ AliSoft ☐ Fetion

☐ Select All

☐ MSN ☐ Yahoo ☐ ICQ/AIM ☐ QQ
☐ Google Talk ☐ Gadu-Gadu

☐ Select All

☒ Edonkey ☒ Bit Torrent ☐ WinMX ☐ Foxy
☐ KuGoo ☐ AppleJuice ☐ AudioGalaxy ☐ DirectConnect
☐ Mesh ☐ MUTE ☐ Thunder5 ☐ GoGoBox
☐ QQDownload ☐ Ares ☐ Shareaza ☐ BearShare
☐ Morpheus ☐ LimeWire ☐ KaZaa ☐ Clubbox

Air Live® Policy Object > Application Blocking > Setting www.airlive.com

Application Signature Definitions

Last updated on : 09/09/30 14:06:28 (Update signature definitions every one hour)
Current version : 3.8.7 (Signature definitions updated at 09/09/22 15:27:04)
Update signature definitions immediately (Use TCP port: 80 and UDP port: 53) **Update NOW**

Application Blocking

Name	Application	Configure
Application_1	MSN,Yahoo,Edonkey...	Modify Remove

New Entry

5. Select **Policy** → **Outgoing**. Click “**New Entry**” to create a new policy rule.

6. Dropdown the menu of Application Blocking (RS-1200: IM/P2P Blocking) in Outgoing Policy rule page, and select the rule name you just created. Click OK to save setting, and RS gateway will start to block application connection.

The screenshot shows the Air Live web interface with the 'Policy > Outgoing' page. The left sidebar contains a navigation menu with the following items: System, Interface, Policy Object, Policy, Outgoing (selected), Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN, DMZ To LAN, Mail Security, IDP, Anomaly Flow IP, and Monitor. The main content area is titled 'Add New Policy' and contains a form with the following fields:

- Comment: (Max. 32 characters)
- Source Address: Inside_Any
- Destination Address: Outside_Any
- Service: ANY
- Schedule: None
- Authentication User: None
- Trunk: None
- Action, WAN Port: PERMIT ALL
- Traffic Log: ☐ Enable
- Statistics: ☐ Enable
- IDP: ☐ Enable
- Content Blocking: ☐ Enable
- Application Blocking: Application_1 (highlighted with a red box)
- QoS: None
- MAX. Bandwidth Per Source IP: Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
- MAX. Concurrent Sessions Per IP: 0 (Range: 1 - 99999, 0: means unlimited)
- MAX. Concurrent Sessions: 0 (Range: 1 - 99999, 0: means unlimited)

At the bottom right of the form, there are two buttons: OK and Cancel.