

User Agent Policies

<https://campus.barracuda.com/doc/98225121/>

User agent policies allow you to create rules to allow or block clients based on the information included in their user agent string. You can add browser / operating system combinations, or you can define generic user agent patterns. The selected user agents and the generic user agent patterns are combined with a Boolean OR. Keep in mind that the user agent strings can be overridden on the client.

User Agent Shared Policy Profiles							
Name	Origin	Refer...	Description				
0 WINPOL1	Local	0					

WINPOL1							
User Agent Policy Profile				References			
Name	Description	Action	Content Match	Source	Destination	Application	User
0 UserAgentDefault	The default User Agent poli...	Block		Any 0.0.0.0/0	Any 0.0.0.0/0	Any	Any

For information on how to customize default policy profiles, see [How to Configure Policy Profiles](#).

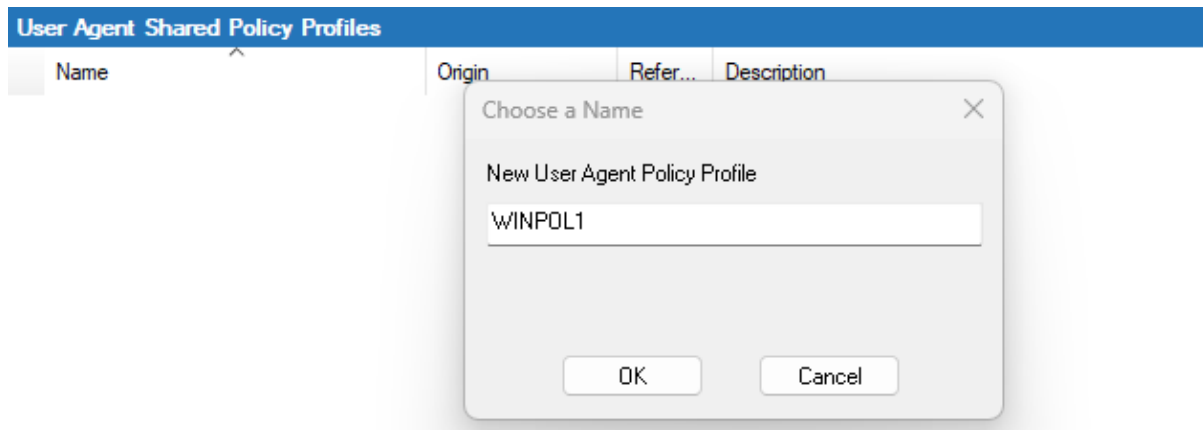
Before You Begin

Make sure that SSL Inspection is enabled in the **Security Settings**. For more information, see [How to Configure Outbound TLS Inspection](#).

Create a User Agent Policy Profile

Create an explicit user agent policy profile to match your individual requirements.

1. (On the Control Center) Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Global Firewall Objects**.
2. Click **Lock**.
3. In the left menu, expand **Policy Profiles**.
4. Select **User Agent**.
5. To add a new policy profile, click the plus icon (+) at the top right of the window, enter a profile name, and click **OK**.



6. Click **Send Changes** and **Activate**.

The policy profile now appears in the **User Agent Shared Policy Profiles** list, and you can create explicit policies for it.

Create an Explicit User Agent Policy


1. (On the Control Center) Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Global Firewall Objects**.
2. (On a CloudGen Firewall) Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. In the left menu, expand **Policy Profiles**.
5. Select **User Agent**.
6. Select the profile you wish to create the policy for. The policy list appears under the corresponding tab in the lower window.
7. To add a new policy, click the plus icon (+) at the top right of the lower window. You can also right-click the list and select **Add Policy**.
8. Specify values for the following:
 - **Name** – Enter a descriptive name for the explicit policy.
 - **Description** – Enter a description for the policy.
 - **Action** – Select either **Allow** or **Block**.
 - **User Agent** – Click + to open the user agents list and select the agents the policy should apply to.
 - **User Agent Patterns** – Click + to add specific patterns. User agent patterns may contain the * and ? wildcard.
 - **Source / Destination IP/Network Criteria** – Select the source and destination network, or select **<Explicit Network>** and enter an IP address / network or a domain that gets resolved to an IP address for the matching.
 - **Application Criteria** – Define the application match condition. Add an application the policy should apply to, or create explicit applications. To open the selection menu, double-click the corresponding field. Selecting applications in the application editor works similar

to the process in the objects configuration for the application rule set. For more information, see [How to Create an Application Object](#) and [How to Create a Custom Application Object](#).






- **Users** – Select the users or groups the policy should apply to.

☒ User Agent



General

Name	WINPOL1
Description	
Action	 Block

User Agent Match

User Agents	<div>  Name ^  Microsoft OneDrive Windows 1...</div>
User Agent Patterns	<div>  User Agent Pattern ^ Click + to add user agents patterns as a matching criteria. Leave blank to not use user agent patterns as matching criteria.</div>

Criteria

Source IP/Network Criteria	 Trusted Next-Hop Netw... ▼ ...
Destination IP/Network Criteria	 Trusted LAN Networks ▼ ...
Application Criteria	Any ▼ ... Match for any Application
Users	All Authenticated Users ▼ ... X509Subject=CN=?* user=?*

9. Click **OK**.

10. Click **Send Changes** and **Activate**.

The policy is now listed in the lower window and can be selected as **Policy** in your forwarding rules. For more information, see the last step in [How to Configure Policy Profiles](#).

Figures

1. ua-pol_overview.png
2. +.ico.png
3. ua_new.png
4. add_ico.png
5. ua_exp.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.