

# How to Configure the Barracuda Access Monitor

https://campus.barracuda.com/doc/46894677/

In the Barracuda Access Monitor, you can configure connectivity settings, Health Agent authentication, and notification and log parameters. You can also modify some registry settings according to your requirements. The configuration of the Barracuda Access Monitor is done in the **Advanced Settings** section.

### **Configure the Barracuda Access Monitor**

- 1. Launch the Access Monitor by left-clicking the red cross icon in the system tray.
- 2. In the **Configuration** menu, select **Settings** to open the **Advanced Settings** window.

lealth Agent	Health Agent Connectivity		
lealth Agent	Assess Casteri Castina IDs from Desistar		
valuation Deculto	Access Control Service IPs from Registry		
Evaluation Results	Access Control Service IPs from DHCP	10.17.88.102:44000	
	ICMP Connectivity Checking	Yes	
onfiguration	Offline Check	No	
conniguration	Health Agent Authentication		
ettings	Use Basic Authentication	Yes	
	Use NTLM Authentication	Yes	
	Check Access Control Trust Relationship	No	
	NAC Client Settings		
	UseDefaultQuarantine Ruleset	No	
	On Power Resume Auto Quarantine	No	
	On Power Resume Quarantine Load Only	Yes	
	Use enhanced health state detection	No	-
	Detect installed OS Hotfixes	Yes	
	Use Cache for list of Hotfixes	Yes	
	Notification Settings		
	Healthy	Yes	
	Quarantine	Yes	
	Log Settings		
	Barracuda Network Access Client Logging	Yes	
	Rarracuda Health Agent Logging	No	

Within the Barracuda Access Monitor Advanced Settings menu, you can modify the following



parameters:

#### **Health Agent Connectivity**

This section holds all configuration items regarding the connectivity of the Barracuda Access Monitor.

• Access Control Server IPs From Registry – This dialog allows you to create, edit, and delete Access Control Server IP addresses stored within the registry. You can configure as many Access Control Server IP addresses as required to ensure continuous connectivity.

Advanced Policy Server IPs							
The following list shows fixed IPs for the Barracuda Health Agent to evaluate its health state. These are stored in the registry at: (HKEY_USERSDEFAULT\Software\Phion\phionha\PolSrv)							
Entry	IP / Domain name						
1	10.0.10.70						
New	Edit Delete Save Cancel						

The configured IP addresses are then stored in the registry:

- Path HKEY\_USERS\.Default\Software\phion\phionha\PolSrv
- **Key** N (enumeration)
- Value IP or Hostname of an Access Control Server
- Access Control Server IPs From DHCP When the Barracuda Networks DHCP server is configured to distribute the Access Control Server IP addresses using DHCP, these addresses are listed in an advanced dialog. If required, clear the Access Control Server IP addresses received through DHCP by clicking Clear Policy IPs.

Кеу	Value	Lease Expires		
ip0	10.20.30.40	10/13/2008 7:14:56 PM		
			Clear Policy IPs	ОК

- **ICMP Connectivity Checking** The Barracuda Access Monitor can determine the connectivity to the Access Control Server using ICMP packets. It is recommended to enable this feature when connecting to the Access Control Server through a VPN connection because otherwise the connectivity may not work as expected.
  - $^\circ\,$  If enabled, the Barracuda Access Monitor sends an ICMP packet to the Access Control Server before connecting and starting a health evaluation. If the ICMP packet returns



successfully, the Barracuda Access Monitor connects to the Access Control Server and starts the health evaluation.

- If disabled, the Barracuda Access Monitor starts immediately connecting to the Access Control Server, instead of checking for connectivity first.
- $\circ\,$  To edit this option manually, modify the following registry key:
  - **Path** HKEY\_USERS\.Default\Software\phion\phionha\settings
  - Key ICMPProbing
  - Value 0 (disabled); 1 (enabled, default)
    - When **ICMP Connectivity Checking** is enabled, the firewall must be configured to pass ICMP packets through; otherwise, the Barracuda Access Monitor will not connect to the Access Control Server.
- Offline Check This option lets you disable the Health Agent if no network connection is active. This prevents the local firewall from unintentionally entering quarantine mode. The default value is 0 (the Health agent is not disabled when offline).
  - You can enable or disable quarantine in offline mode using the UseOfflineQuarantineMode registry key. The defauilt value is 1 (quarantine in offline mode is enabled).
  - You may configure whether to display the health dialog window or not using the ShowAgentDlg registry key. Default value is 1 (the dialog is displayed).
  - $\circ\,$  To edit this option manually, modify the following registry key:
    - Path HKEY\_USERS\.Default\Software\phion\phionha\settings
    - **Key** UseConnectionState
    - Value 0 (disabled); 1 (enabled, default)

#### **Connectivity Timeout Settings**

You can manipulate the timeout periods for the Barracuda Access Monitor's connection to the Access Control Server by using registry switches. Reduce the default values in

HKEY\_USERS\.Default\Software\phion\phionha\settings in order to get a more reactive client behavior.

- **Key** WaitForNextTry
- Value [Timeout value in milliseconds, default value is 30000 (30 sec)]

and:

- Key WaitForNextLocalComputerAuth
- Value [Timeout value in milliseconds, default value is 60000 (30 sec)]

Connection wait time for the Access Control Server, if VPN is active:

- **Key** WaitForNextVPNTry
- Value [Timeout value in milliseconds, default value is 1000 (1 sec)]



The waiting time for the next user prompt, if **Cancel** was clicked in the basic authentication request:

- **Key** WaitCancel
- Value [Timeout value in milliseconds, default value is 3600000]

#### Health Agent Authentication

• Use Basic Authentication – This option specifies if basic user-and-password or certificate authentication should be used in case the NTLM authentication fails. Defaults to 1 (basic user-and-password authentication is used). To edit this option manually, modify the UseBasicAuthFallback registry key in

.DEFAULT\Software\Phion\phionha\settings\. Default value is 1 (enabled).

- Use NTLM Authentication By enabling this option, the Barracuda Access Monitor will use the Windows user credentials provided by NTLM for authentication. Defaults to 1 (NTLM is used). To edit this option manually, modify the UseNTLM registry key: Default value is (disabled).
- **Check Access Control Trust Relationship** By enabling this option, the Barracuda Network Access Client will check the Access Control Service X509 trust relationship.

#### **NAC Client Settings**

- Use Default Quarantined Ruleset Enable this option to automatically start the firewall with the default quarantine ruleset.
- **On Power Resume Auto Quarantine** Enable this option to automatically load the quarantine ruleset when recovering from Standby/Hibernate.
- On Power Resume Quarantine Load Only Only load the quarantine ruleset; do not terminate existing connections. This option only applies when On Power Resume Auto Quarantine is enabled.
- Use enhanced health state detection Specifies if enhanced health state checks by using the OESIS Framework (OPSWAT) should be carried out.
- **Detect installed OS Hotfixes** Specifies if the installed OS hotfixes should be considered for health check.
- Use Cache for list of Hotfixes Specifies if the list of hotfixes that were loaded in the last session are initially used for health check and the new list is loaded in the background.

#### **Notification Settings**

- **Healthy** Enable this option to display a notification pop-up whenever the state 'Healthy' is reached.
- **Quarantine** Enable this option to display a notification pop-up whenever the state 'Quarantine' is reached.

#### Log Settings

Enables /disables logging for the Barracuda Network Access Client. For more information, see <u>Network</u> <u>Access Client Logging</u>.



### Advanced Setting for the Access Control Service Port

It is possible to change the default port of 44000 through which the Access Monitor reaches the Access Control Server by manipulating the DefaultPort registry key in .DEFAULT\Software\Phion\phionha\settings\

## Barracuda Network Access Client



### Figures

- 1. access\_monitor\_advanced.png
- 2. ip\_from\_reg.png
- 3. ip\_from\_dhcp.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.