

Service Managed Gateway™

Configuring MAC Address Filters



Issue 2.0
Date 11 May 2010

1	About this document	3
1.1	Scope	3
1.2	Readership	3
1.3	More information.....	3
1.4	Terminology	3
2	Introduction	4
2.1	What is a MAC address?	4
2.2	How MAC address filtering works	4
3	Managing MAC address filters.....	5
3.1	Creating a MAC address filter	5
3.2	Modifying a MAC address filter	8
3.3	Deleting a MAC address filter	9
3.4	Troubleshooting MAC address filters	9
3.4.1	Confirm that a filter matches network traffic.....	9
3.4.2	Confirm that packets from a device reach the SMG.....	10
4	Examples of MAC address filtering	12
4.1	Allowing only some devices to access the network	12
4.2	Preventing some devices from accessing the network	12
4.3	Permitting or block a class of devices.....	12

© 2010 Virtual Access (Irl) Ltd. This material is protected by copyright. No part of this material may be reproduced, distributed, or altered without the written consent of Virtual Access. All rights reserved. All trademarks, service marks, registered trademarks and registered service marks are the property of their respective owners. Virtual Access is an ISO 9001 certified company.

1 About this document

1.1 Scope

This document:

- explains how to create, modify, delete, and troubleshoot MAC address filters, and
- gives examples of how to use MAC address filters.

1.2 Readership

This document is for engineers who have previous experience configuring and managing Service Managed Gateways (SMGs).

1.3 More information

For more information, read about MAC address filters in the [Expert Web Full Reference Documentation](#). Browse to **System ->Filters-> mac address filters**.

1.4 Terminology

MAC address	A unique identifier that is programmed into a device when the device is manufactured.
--------------------	---

2 Introduction

To improve security, it is sometimes desirable to limit access to the Wide Area Network (WAN) to a set of approved users or devices. Occasionally, it might be necessary to prevent particular devices from accessing the network. MAC address filters allow you to control network access based on the network MAC address of a device.

The GW7000 series of Service Managed Gateways (SMGs) supports up to 100 filter entries.

The 6000 series of SMGs supports 5 filter entries.

You configure MAC address filtering in the Expert View section of the Service Managed Gateway web.

2.1 What is a MAC address?

A MAC address uniquely identifies a device on a Local Area Network (LAN). The MAC address is programmed into a device when the device is manufactured.

There are 12 hexadecimal digits in a MAC address:

- Digits 1-6 of a MAC address are the vendor ID
- Digits 7-12 of a MAC address are a unique device ID

2.2 How MAC address filtering works

When a local Ethernet port receives a packet, the packet is checked against the list of defined MAC address filters, from the top of the list to the bottom of the filter list.

The first filter that matches the packet determines whether or not the packet is permitted. If no filter matches, then the packet is either permitted by default or authenticated if port access control is enabled.

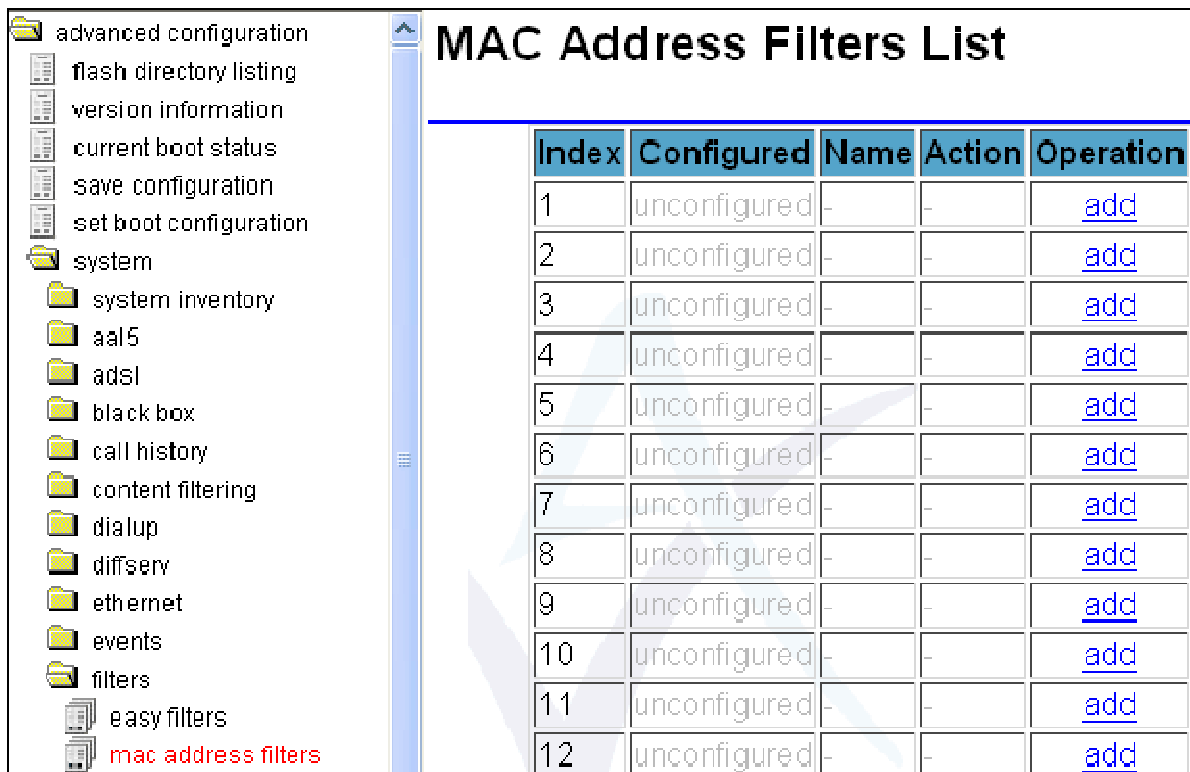
3 Managing MAC address filters

3.1 Creating a MAC address filter

On the SMG Start page, click **Advanced**.

In the Advanced menu, click **Expert View**.

In the Expert View menu, select **advanced configuration -> system -> filters-> mac address filters**. The MAC Address Filters List page appears.



Index	Configured	Name	Action	Operation
1	unconfigured	-	-	add
2	unconfigured	-	-	add
3	unconfigured	-	-	add
4	unconfigured	-	-	add
5	unconfigured	-	-	add
6	unconfigured	-	-	add
7	unconfigured	-	-	add
8	unconfigured	-	-	add
9	unconfigured	-	-	add
10	unconfigured	-	-	add
11	unconfigured	-	-	add
12	unconfigured	-	-	add

Figure 1: The MAC address filters list

In the Operation column, click **add** in the row of the filter that you want to create. The MAC Address Filters Entry page appears.

MAC Address Filters Entry 1

Configured	yes ▾
Name	Test
Action	pass ▾
Interface	any ▾
MAC Address	000000000000
MAC Address Mask	FFFFFFFFFFFF

Figure 2: The default values on the MAC address filters entry page

In the MAC Address Filters Entry page, set the configuration parameters that are described in Table 1 and click **Update**.

The filter takes effect immediately. You do not have to reload the SMG.

Field Name	Description	Command Line						
Configured	Enables a particular packet filter. <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">yes</td> <td>Enables a filter rule.</td> </tr> <tr> <td>no</td> <td>Disables a filter rule.</td> </tr> </table> Select yes to enable the filter.	yes	Enables a filter rule.	no	Disables a filter rule.	Set Ezpacket Configured		
yes	Enables a filter rule.							
no	Disables a filter rule.							
Name	Defines a descriptive name for the filter. Type a descriptive name that will help you remember what the filter does. The name does not affect how the filter works.	Set Ezpacket Name						
Action	Determines what action to take when a packet matches the filter. <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Pass</td> <td>Allows a packet through with no further action.</td> </tr> <tr> <td>Block</td> <td>Discards the packet immediately.</td> </tr> <tr> <td>Authenticate</td> <td>The packet will be permitted if the host has successfully passed 802.1x authentication, but not otherwise. This only applies when the 802.1x Access Control mechanism is enabled; otherwise, Authenticate is the same as Pass.</td> </tr> </table> <p>Note: when the 802.1x authentication module is enabled, Pass rules will bypass</p>	Pass	Allows a packet through with no further action.	Block	Discards the packet immediately.	Authenticate	The packet will be permitted if the host has successfully passed 802.1x authentication, but not otherwise. This only applies when the 802.1x Access Control mechanism is enabled; otherwise, Authenticate is the same as Pass.	Set Ezpacket Action
Pass	Allows a packet through with no further action.							
Block	Discards the packet immediately.							
Authenticate	The packet will be permitted if the host has successfully passed 802.1x authentication, but not otherwise. This only applies when the 802.1x Access Control mechanism is enabled; otherwise, Authenticate is the same as Pass.							

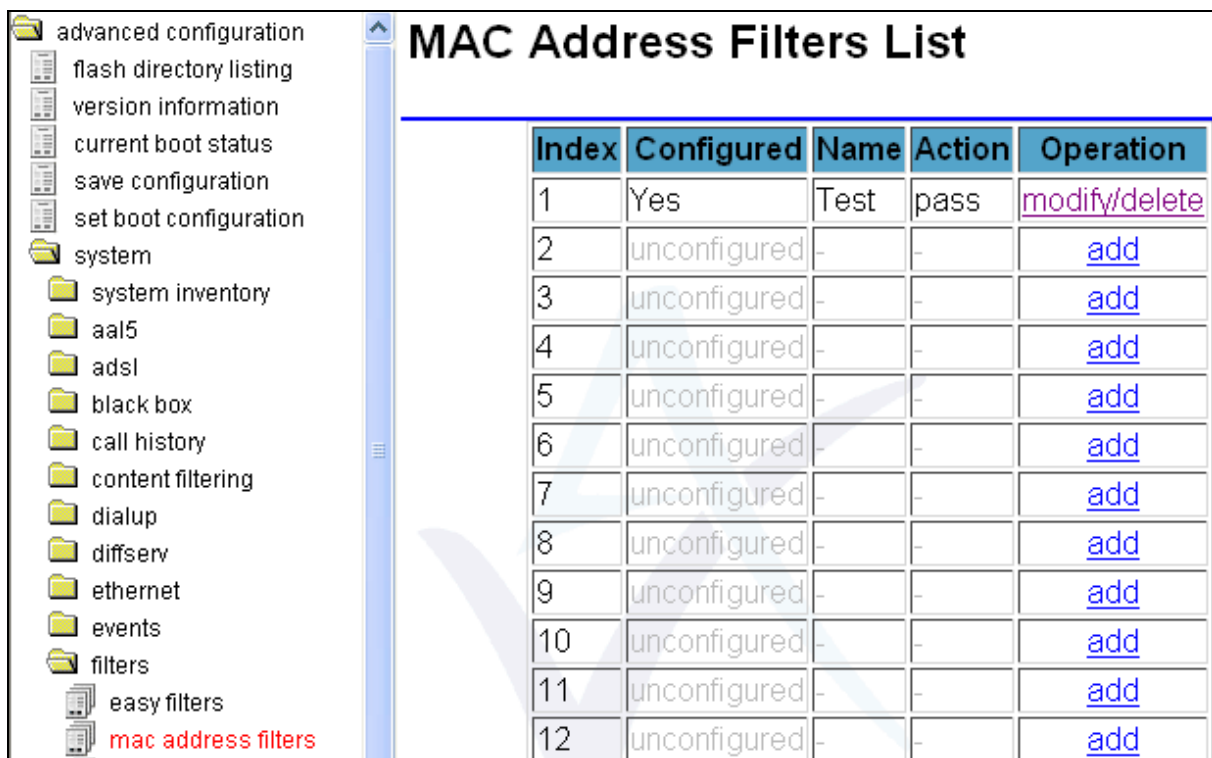
	<p>it completely.</p> <p>Typically, a secure configuration will have several low-numbered Pass or Authenticate filter rules that match specific devices on the port, and finish with a Block filter that matches everything else with a mask of 000000000000.</p>	
Interface	<p>The Interface field controls which external interfaces the filter will apply to.</p> <p>Eth-0 applies the filter to packets that arrive on the Eth-0 interface.</p> <p>Eth-1 applies the filter to packets that arrive on the Eth-1 interface.</p> <p>Eth-2 applies the filter to packets that arrive on the Eth-2 interface.</p> <p>Eth-3 applies the filter to packets that arrive on the Eth-3 interface.</p> <p>lan applies the filter to all packets that arrive on Ethernet ports that are not configured as WAN interfaces.</p> <p>wan applies the filter to all packets that arrive on Ethernet ports that are configured as WAN interfaces.</p> <p>Any applies the filter to any Ethernet port.</p>	Set Ezpacket Interface
MAC Address	<p>The MAC address defined here is compared against the remote device's MAC address when checking for a rule match.</p> <p>When you use a mask value of FFFFFFFF, then an exact match is required. If you use a less restrictive mask value, then only the portion included by the mask need match. The default value is 000000000000.</p> <p>Type the MAC address of the device or devices you want to match. The address must be 12 hexadecimal digits.</p> <p>Enter the address in the following format: AABCCDDEEFF.</p> <p>Type 0 to match all devices.</p>	Set Ezpacket Mac Address
MAC Address Mask	<p>The mask value you define here is used to indicate which portion of the MAC address is compared with the remote device's MAC address. A mask of FFFFFFFF means that an exact match is required.</p> <p>A mask of FFFFF00000 means that only the first three octets must match. In MAC addresses, the first three octets define the vendor while the remaining three octets uniquely identify devices from that vendor. This is useful, since it allows an</p>	Set Ezpacket Mac Mask

	<p>entire group of devices from a single manufacturer to be matched with a single filter rule. For example, all Voice over IP telephones from a particular vendor might be given full access, while PCs are forced to go through an authentication procedure first.</p> <p>Type a mask to filter the MAC addresses. The mask must be 12 hexadecimal digits. Type 0 to match all devices.</p> <p>To match only the device that is defined in the MAC Address field, use the default MAC address mask, FFFFFFFF.</p>	
--	---	--

Table 1: Fields and values for MAC address filter configuration

3.2 Modifying a MAC address filter

In the Expert View menu, select **advanced configuration** -> **system** -> **filters**-> **mac address filters**. The MAC Address Filters List page appears.



Index	Configured	Name	Action	Operation
1	Yes	Test	pass	modify/delete
2	unconfigured	-	-	add
3	unconfigured	-	-	add
4	unconfigured	-	-	add
5	unconfigured	-	-	add
6	unconfigured	-	-	add
7	unconfigured	-	-	add
8	unconfigured	-	-	add
9	unconfigured	-	-	add
10	unconfigured	-	-	add
11	unconfigured	-	-	add
12	unconfigured	-	-	add

Figure 3: The MAC address filters list

Click **modify/delete** in the row of the filter that you want to modify. The MAC Address Filters Entry page appears.

Figure 4: The MAC address filters entry page

In the MAC Address Filters Entry page, modify the configuration parameters and click **Update**.

The changes take effect immediately. You do not have to reload the SMG.

3.3 Deleting a MAC address filter

In the Expert View menu, select **advanced configuration** -> **system** -> **filters**-> **mac address filters**. The MAC Address Filters List page appears.

Click **modify/delete** in the row of the filter that you want to delete. The MAC Address Filters Entry page appears

In the MAC Address Filters Entry page, click **Delete**.

The changes take effect immediately. You do not have to reload the SMG.

3.4 Troubleshooting MAC address filters

3.4.1 Confirm that a filter matches network traffic

On the SMG start page, click **Advanced**.

In the Advanced menu, click **Expert View**.

In the Expert View menu, click **Operations** in the top menu of the web interface.

In the Operations menu, select **performance** -> **filter stats** -> **mac address filters**. The Active MAC Address Hits page appears.

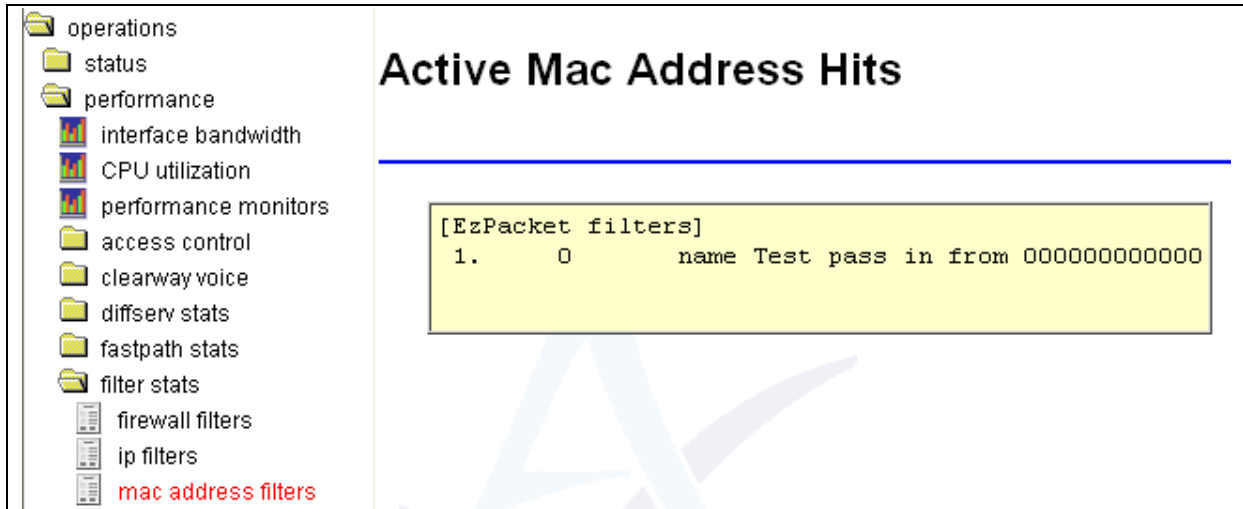


Figure 5: The active mac address hits page

The page lists all MAC address filters that are active and the number of packets that the filters have matched.

If a filter does not match network traffic, follow the procedure in section 3.2 to correct the problem.

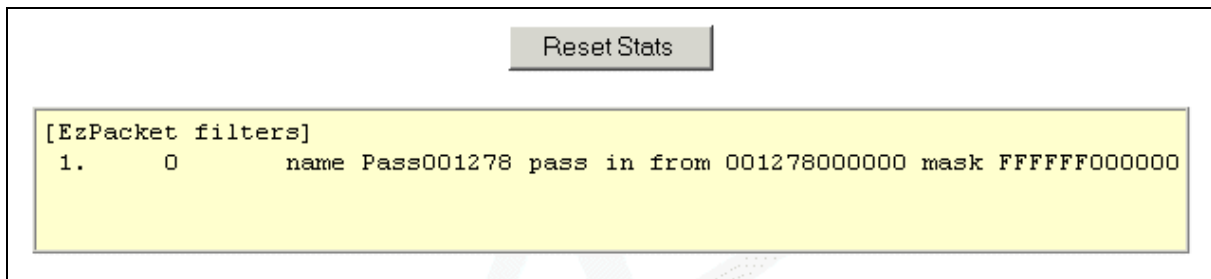


Figure 6: The active MAC address hits page.

3.4.2 Confirm that packets from a device reach the SMG

In the Expert View menu, click **Operations** in the top menu of the web interface.

In the Operations menu, select **performance** -> **filter stats**-> **mac address filter cache**. The MAC Address Filter Cache page appears.

The screenshot shows the 'Mac Address Filter Cache' page. On the left is a navigation menu with items like 'operations', 'status', 'performance', 'interface bandwidth', 'CPU utilization', 'performance monitors', 'access control', 'clearway voice', 'diffserv stats', 'fastpath stats', 'filter stats', 'firewall filters', 'ip filters', 'mac address filters', 'mac address filter cache' (highlighted in red), 'usage monitors', 'virtual routes', and 'advanced ip filters'. The main content area has the title 'Mac Address Filter Cache' and a control bar with 'View active MAC filter cache for' (set to 'All interfaces'), 'Refresh', and 'Clear Cache' buttons. Below is a table with the following data:

Port	Hits	MAC address	Last seen	IP	Status	Age
eth-0	10	00-03-ff-13-55-00	10.1.9.125	Pass	10 seconds	
eth-0	4	00-14-22-18-55-00	10.1.10.200	Pass	12 minutes	
eth-0	10	00-11-65-af-de-01	10.1.10.20	Pass	1 minute 57 seconds	
eth-0	10	00-03-ff-b8-5a-04	10.1.9.15	Pass	4 minutes 19 seconds	
eth-0	42	00-1a-a0-b6-5a-04	10.1.86.1	Pass	15 seconds	
eth-0	5	00-04-76-29-67-06	10.1.9.1	Pass	19 seconds	

Figure 7: The MAC address filter cache page

The page shows the device addresses that were seen on each port. The cache is flushed:

- when the configuration of the MAC address filters changes, or
- when you click **Clear Cache** on the MAC Address Filter Cache page.

The age is refreshed when the port receives another packet from the same MAC address.

If packets are not correctly passed, blocked, or sent for authentication, follow the procedure in section 3.2 to correct the problem.

4 Examples of MAC address filtering

4.1 Allowing only some devices to access the network

You can allow some devices to access the network and prevent most devices from accessing the network. For each MAC address that you allow to access the network, create a filter and set the filter action to PASS. Then create a catch-all filter at the end of the filter table to match all other traffic, and set the filter action to BLOCK.

4.2 Preventing some devices from accessing the network

You can deny access to the network to some devices and allow most devices to access the network. For each MAC address that you want to deny access to, create a filter and set the filter action to BLOCK. Any packet that does not match the MAC address in the filter passes through to the network.

4.3 Permitting or block a class of devices

Suppose that port authentication is enabled on the SMG. A certain class of Voice over IP (VoIP) phone that your company uses does not support authentication. So the VoIP phones are allowed unrestricted access to the network. One vendor provides all the VoIP phones, and the phones have MAC addresses in the form 001278xxxxxx.

Define a MAC address filter with the parameters shown in Figure 8.

Configured	<input type="text" value="yes"/>
Name	<input type="text" value="VoIPallowed"/>
Action	<input type="text" value="pass"/>
Interface	<input type="text" value="any"/>
MAC Address	<input type="text" value="001278000000"/>
MAC Address Mask	<input type="text" value="FFFFFF000000"/>
<input type="button" value="Update"/> <input type="button" value="Delete"/>	

Figure 8: An example of parameters to allow a class of device

Traffic from devices with MAC addresses that begin 001278 is passed. All other traffic will not match the filter and must undergo normal port authentication.

Note: This example increases security, but it is possible to bypass the filter by changing the network address of a blocked device. Only use this technique along with additional security measures.