



# IAM

## Flow control strategy Troubleshooting Guide

Version 12.0.18



## Change Log

Date	Change Description
April 2, 2019	Version 12.0.18 document release.

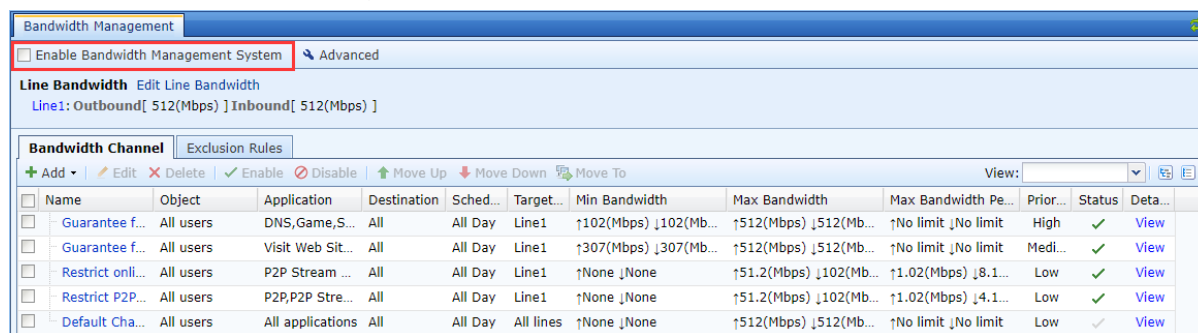
# CONTENT

Chapter 1 Common troubleshooting .....	1
1 Check if the configuration is correct.....	1
2 Analysis packet.....	5
3 Application recognition result analysis.....	5

# Chapter 1 Common troubleshooting

## 1 Check if the configuration is correct

- Check if Bandwidth Management System is turned on.



- Check if the database is updated to the latest.

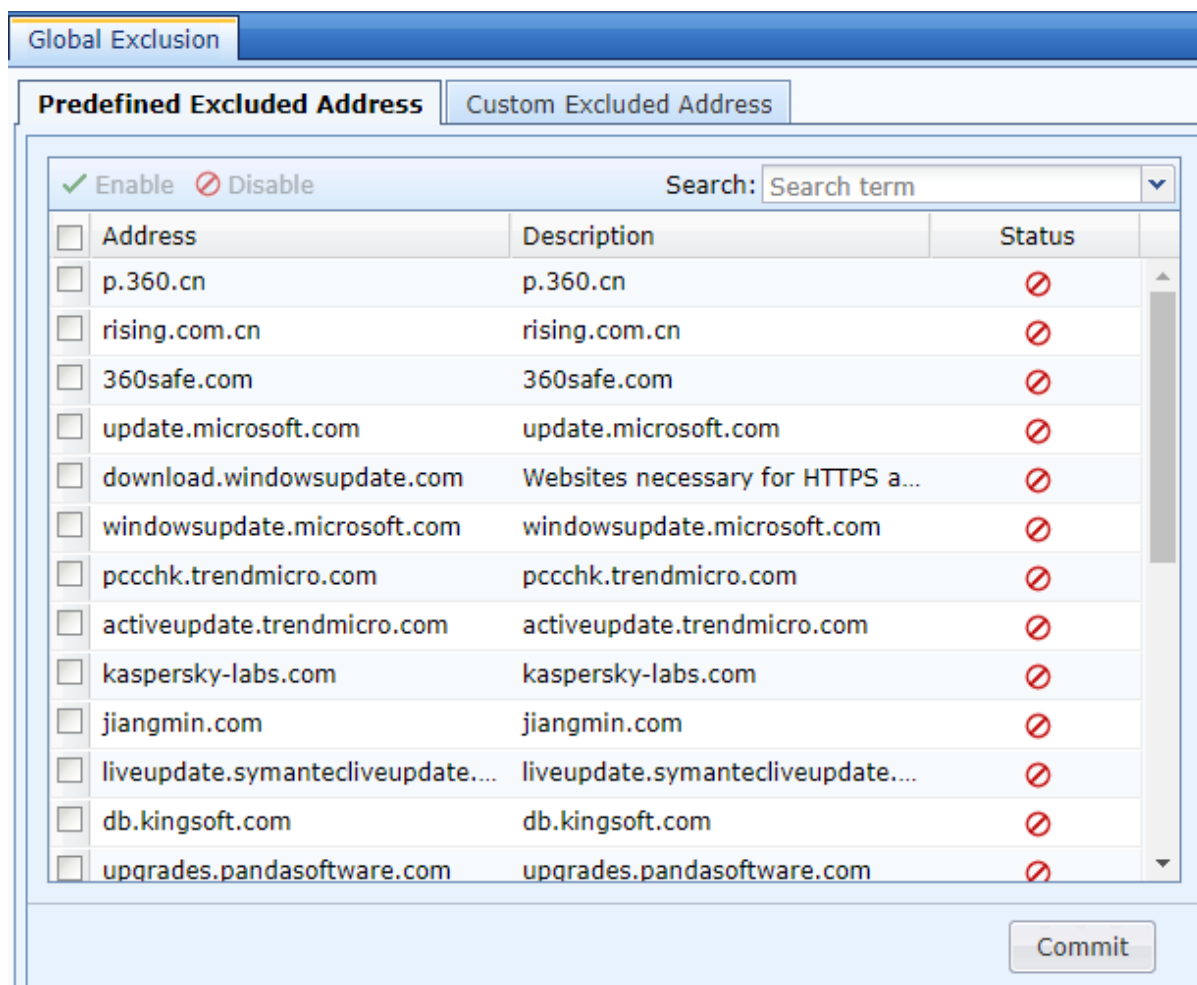
Auto Update						
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable <a href="#">Update Server</a> <a href="#">Refresh</a>						
No.	Database	Current Version	Latest Version	Update Service Expires On	Auto Update	Operation
1	Engine Zero	2019-03-26	2019-03-26	2019-12-19	✓	
2	URL Database	2019-03-25 09:00:00	2019-04-02	2019-12-19	✓	
3	System patch	SP_LFD SP_fsu SP_ume SP_ht...	SP_Vpnppp_AC12.0.16	Never expire	✓	
4	Application Signature Database	2019-03-25 12:34:56	2019-04-02	2019-12-19	✓	
5	Audit Rule Database	2019-03-21	2019-04-03	2019-12-19	✓	

- Check whether the IP or peer address is added to Global Exclusion. If the address is added to Global Exclusion, it will not enter the Bandwidth Channel.

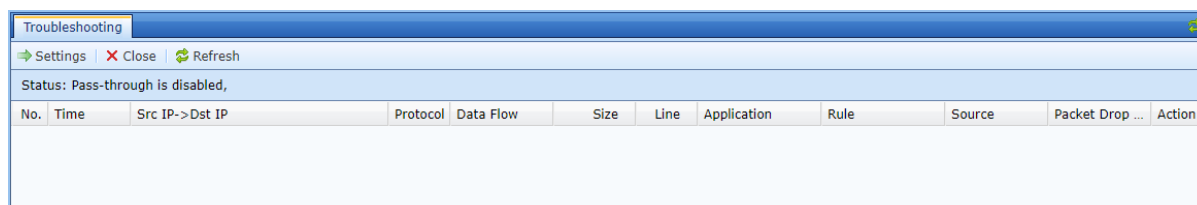
The screenshot shows a web-based configuration interface for 'Global Exclusion'. It has two tabs: 'Predefined Excluded Address' and 'Custom Excluded Address', with the latter being active. The interface includes a toolbar with '+ Add', '✓ Enable', '⊘ Disable', and '✗ Delete' buttons, along with a search bar labeled 'Search: Search term'. Below this is a table with columns for 'Address', 'Description', 'Status', and 'Delete'. One entry is visible: '192.168.1.0/255.255.255.0' with a green checkmark in the Status column and a red 'X' in the Delete column. A 'Commit' button is located at the bottom right of the window.

Address	Description	Status	Delete
192.168.1.0/255.255.255.0		✓	✗

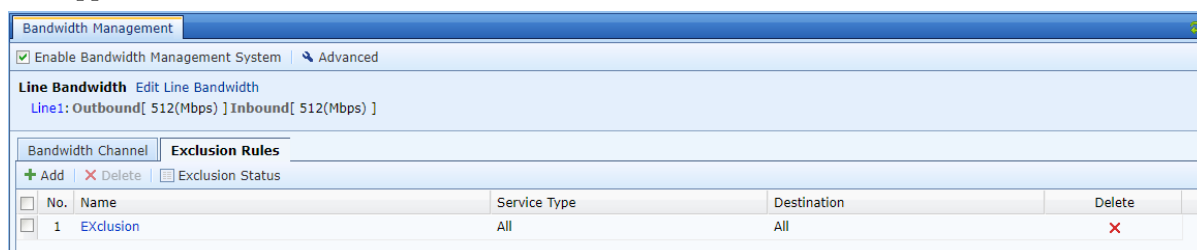
At the same time, when it is found that bandwidth limitations cannot be imposed on applications such as operating system updates or anti-virus software, please check if the address in Predefined Excluded Address is enabled.



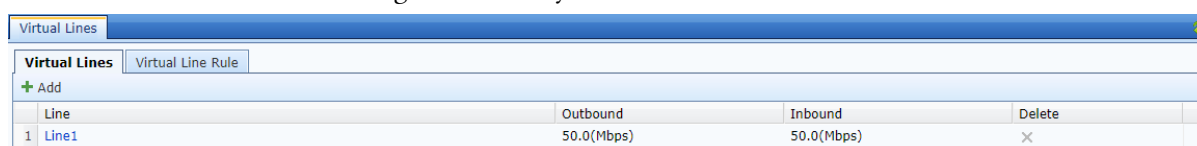
- Check if Troubleshooting is enabled. If Troubleshooting is enabled, traffic will not flow to Bandwidth Channel.



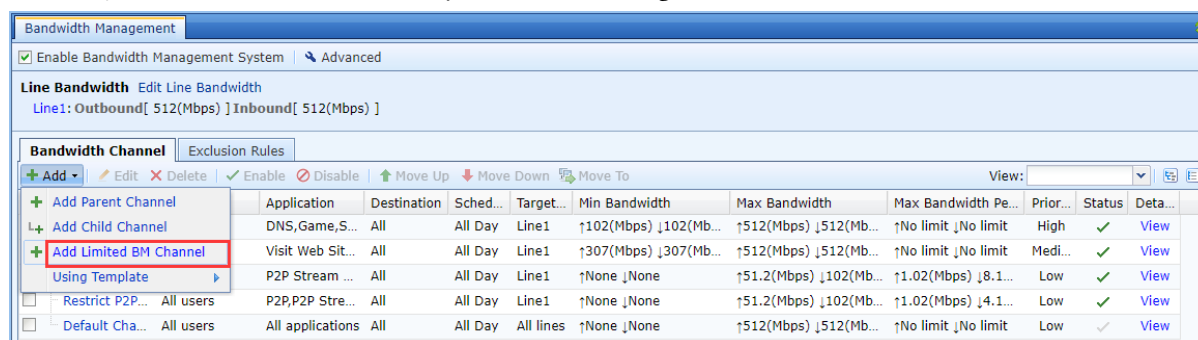
- Check whether Exclusion Rules is configured. If Exclusion Rules is configured, traffic of related applications will not enter Bandwidth Channel.



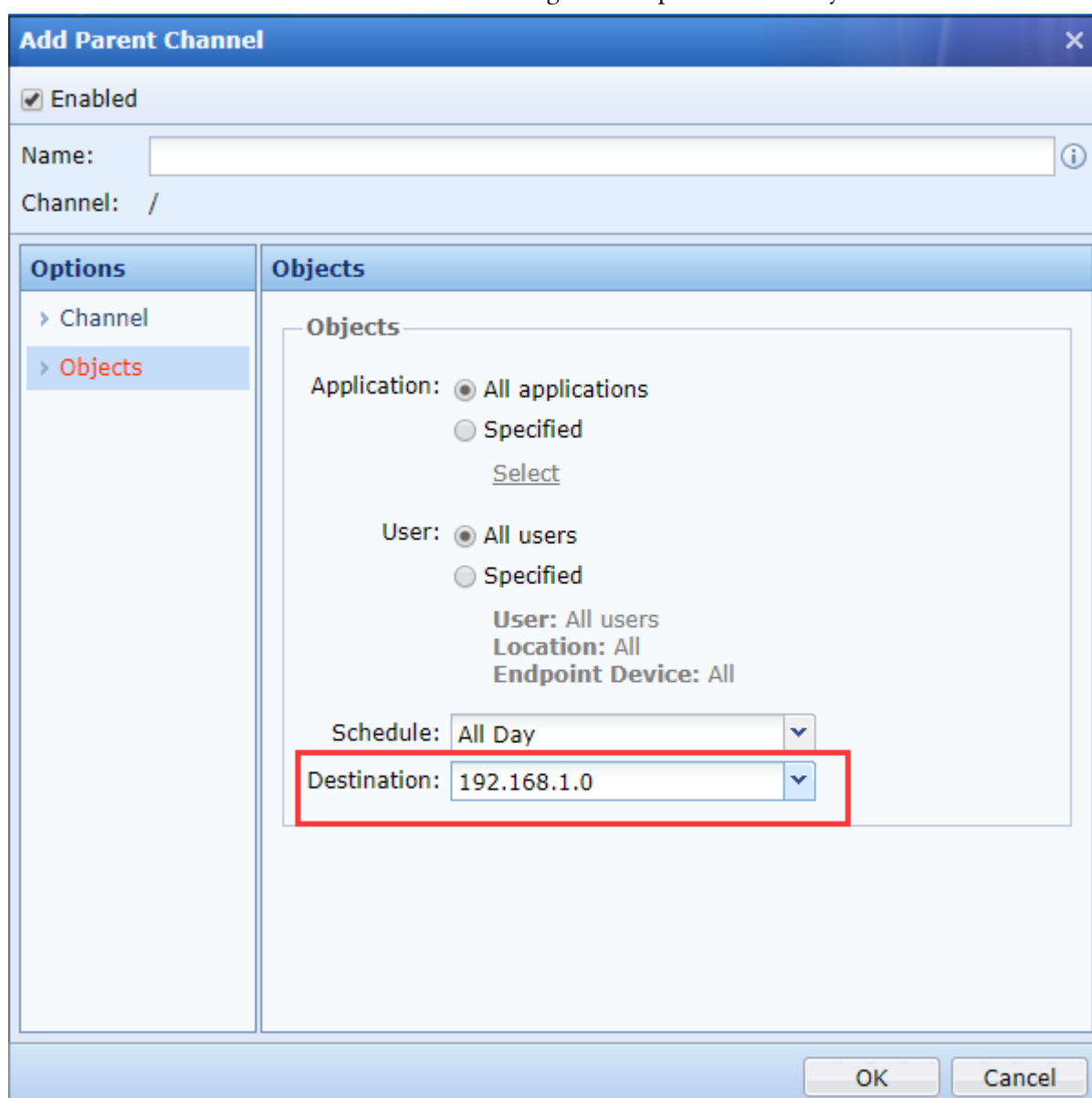
- Check if Virtual Line is configured correctly.



- Check if the Limited BM Channel is misconfigured, and the Limited BM Channel is used in conjunction with the Quota Policy, rather than being used to limit bandwidth alone.



- Check whether Destination is specified. The IAM restricts the network speed to limit the traffic from LAN to WAN. If Destination is specified, it means that the packet will enter the Bandwidth Channel when the peer address belongs to the Destination area. The same is true for Schedule, traffic will enter the Bandwidth Channel during the time period defined by the Schedule.

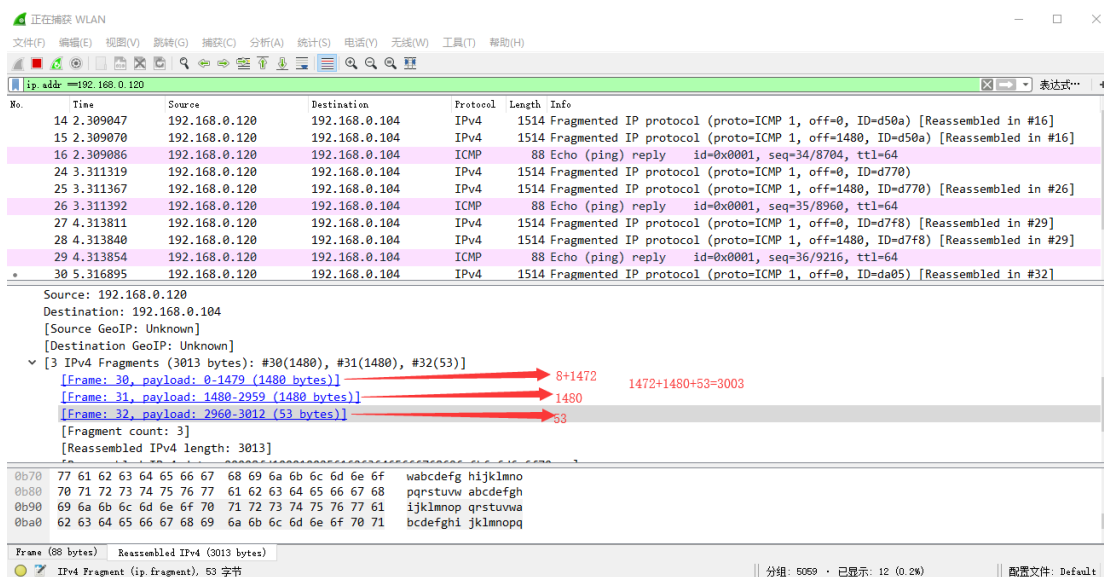


## 2 Analysis packet

- The capture packet analyzes whether the traffic passes through the device in both directions. If the traffic passes through the IAM device in one direction, traffic cannot be restricted.

No.	Time	Source	Destination	Protocol	Length	Info
20455	15:50:31.201405	54.169.70.12	10.60.20.73	TCP	66	443 → 58874 [SYN, ACK] Seq=0 Ack=1 Win=17922 Len=0 MSS=1452 SACK_PERM=1 WS=512
20456	15:50:31.201416	10.60.20.73	54.169.70.12	TCP	54	58874 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
20457	15:50:31.201421	54.169.70.12	10.60.20.73	TCP	66	443 → 58877 [SYN, ACK] Seq=0 Ack=1 Win=17922 Len=0 MSS=1452 SACK_PERM=1 WS=512
20459	15:50:31.201508	10.60.20.73	54.169.70.12	TCP	54	58877 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
20462	15:50:31.202975	54.169.70.12	10.60.20.73	TCP	66	443 → 58876 [SYN, ACK] Seq=0 Ack=1 Win=17922 Len=0 MSS=1452 SACK_PERM=1 WS=512
20463	15:50:31.202981	10.60.20.73	54.169.70.12	TCP	54	58876 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
20467	15:50:31.204594	54.169.70.12	10.60.20.73	TCP	66	443 → 58875 [SYN, ACK] Seq=0 Ack=1 Win=17922 Len=0 MSS=1452 SACK_PERM=1 WS=512
20468	15:50:31.204605	10.60.20.73	54.169.70.12	TCP	54	58875 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
20477	15:50:31.209242	54.169.70.12	10.60.20.73	TCP	1906	443 → 58852 [ACK] Seq=31247 Ack=1513 Win=21504 Len=1452 [TCP segment of a reassemb...

- Check whether the data packet is fragmented. If the data packet is fragmented, contact the network administrator to check whether the MTU value of each device network port is reasonable.



- Check if there is a multi-layer protocol. If there is a multi-layer protocol package, please open the Protocol Extension.

▶ Frame 1: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 172.31.19.102, Dst: 221.176.215.21
▶ User Datagram Protocol, Src Port: 12222 (12222), Dst Port: 12222 (12222)
▶ LWAPP Encapsulated Packet
▶ IEEE 802.11 QoS Data, Flags: .....T
▶ Logical-Link Control
▶ Internet Protocol Version 4, Src: 10.59.134.232, Dst: 111.62.242.42
▶ Transmission Control Protocol, Src Port: 35561 (35561), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

Analyze whether the packet direction is LAN to DMZ. Because the attributes of the DMZ are consistent with the LAN port, the traffic from the LAN to the DMZ will not enter the Bandwidth Channel, because the bandwidth of the IAM is controlled by the LAN to the WAN.

## 3 Application recognition result analysis

- When configuring the Bandwidth Channel Policy, please pay attention to whether the traffic flows into the Bandwidth Channel, and you can query it in Flow Control.



Flow Control							
Line1							
2019-04-03							
Realtime Rate							
Name	Users	Apps	Real-time Speed	Usage	Floating	Status	Details
Guarantee f...	0	0	None	↑0% ↓0%	-	✓	View
Guarantee f...	0	0	None	↑0% ↓0%	-	✓	View
Restrict onli...	0	0	None	↑0% ↓0%	-	✓	View
Restrict P2P...	0	0	None	↑0% ↓0%	-	✓	View
Default Cha...	0	0	None	↑0% ↓0%	-	✓	View

- Checking what the traffic is actually identified. With the development of the Internet, the data streams of various applications are rich in diversity. For example, using Thunder to download files, many files are downloaded in the same way as the Visit Web Site, so the data stream is identified. From the point of view, downloading the file using Thunder is actually similar to Visit Web Site, and has no connection with Thunder and Thunder related links, then the object we restrict should be the Visit Web Site rule.

Top Applications by Traffic							
Auto Refresh: 5 second(s) Refresh Filter							
Filter: Top 60, user group (/)							
No.	App Category	Line	Outbound(Bps)	Inbound(Bps)	Bidirectional	Percent	Top Users
1	Visit Web Site	All	29.09(Kb/s)	1.82(Mb/s)	1.85(Mb/s)	100%	192.168.19.89
2	RemoteDesktop	All	1(Kb/s)	320(b/s)	1.32(Kb/s)	0%	192.168.19.89
3	TeamViewer	All	320(b/s)	512(b/s)	832(b/s)	0%	192.168.19.89

- Check the application rules of the main traffic of an application. For example, some websites use HTTP and HTTPS resources. When accessing, some traffic will be identified as HTTP and SSL-related rules. If you need to limit the speed of the website, You need to limit both HTTP and SSL related rules.



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc