USER MANUAL CYBERALARM

SecureMe2

User Manual

SecureMe2 B.V.
• Gieterijstraat 40, 2984 AB Ridderkerk
• Tel: +31 (0)85 0605424
• www.secureme2.eu
• info@secureme2.eu
• Chamber of Commerce number: 68838557
• VAT: NL857613698B01

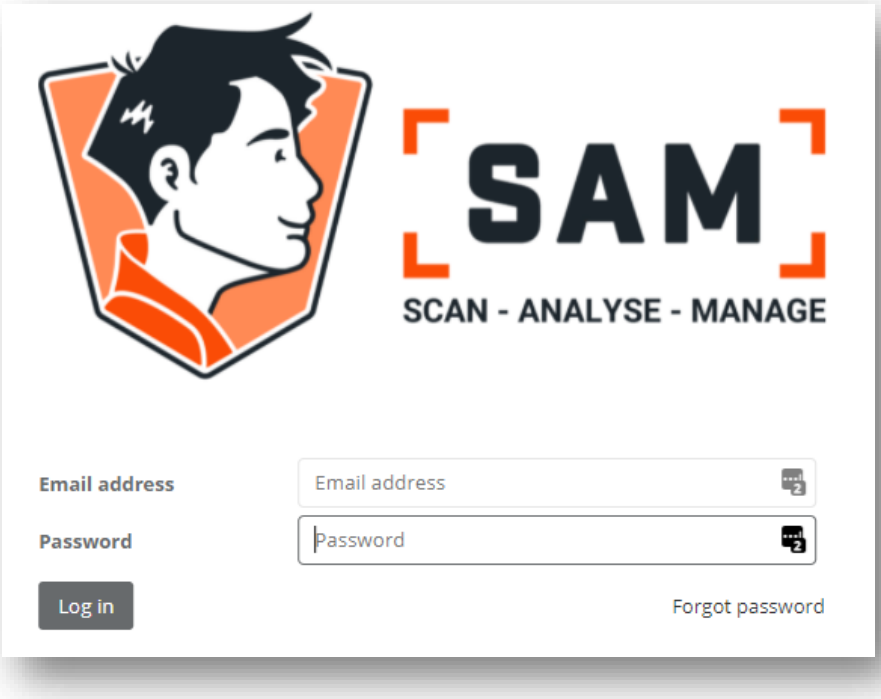
INHOUD

1 logging in to My Cyberalarm 3
2 Overview page 4
2.1 Alarms 5
2.2 Action buttons 6
2.3 Whitelisting 7
2.4 Notifications 7
2.5 Logging out 8
3 Contact 8

Edit date: 03-09-2021

1 LOGGING IN TO MY CYBERALARM

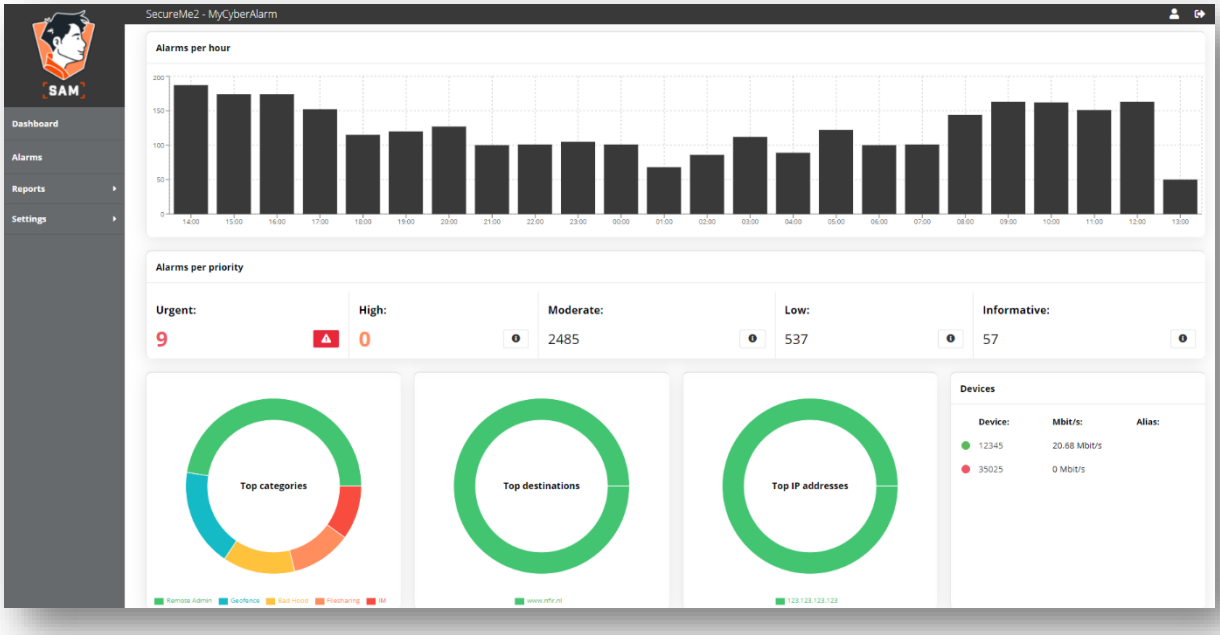
To adjust your settings for My CyberAlarm, or settings related to the use and customization of notifications, you can log into your own SAM portal. Go to www.mycyberalarm.eu. By means of the login page you will then access your own overview page.



2 OVERVIEW PAGE

All your notifications are clearly summarized on your own overview page. Here you can see the number of notifications that have taken place in the past hour. And also an overview of any notifications categorized per priority. You can click on these prio notifications and receive a detailed overview of the report.

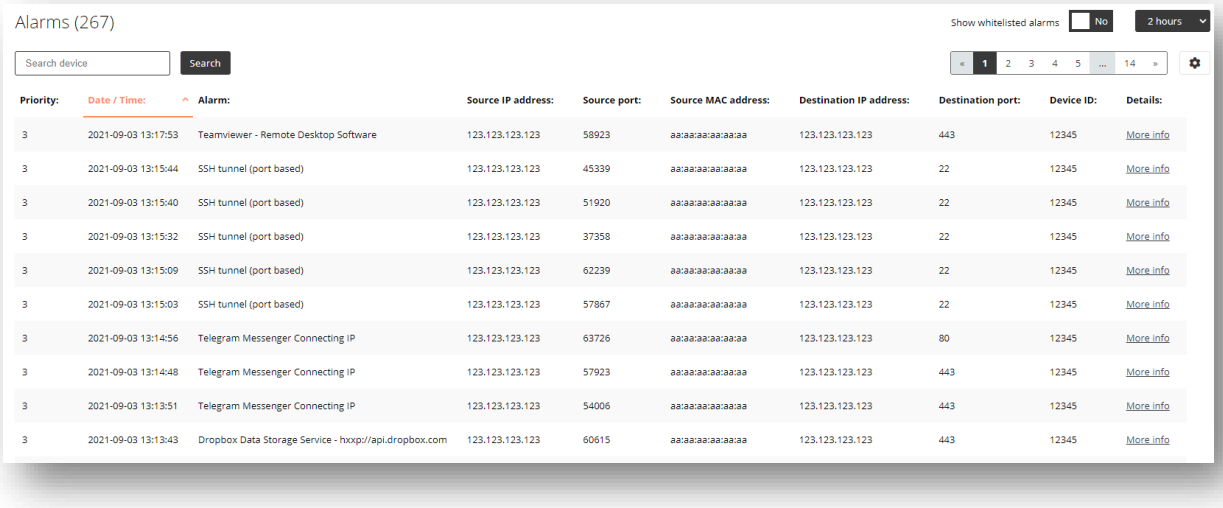
If you have multiple SAM connections, you can see at a glance whether these are all Online.



If you notice that a SAM device is offline, please contact your IT manager immediately. There may have been maintenance activities and SAM can no longer pass on the reports. If you still have questions, you can always contact Secureme2.

2.1 ALARMS

Viewing the details of your prio messages is possible by clicking on 'Alarms' in the task bar on the left of your portal. You can do the same by clicking on a prio message in the overview. The details screen gives you specific information about a particular notification.



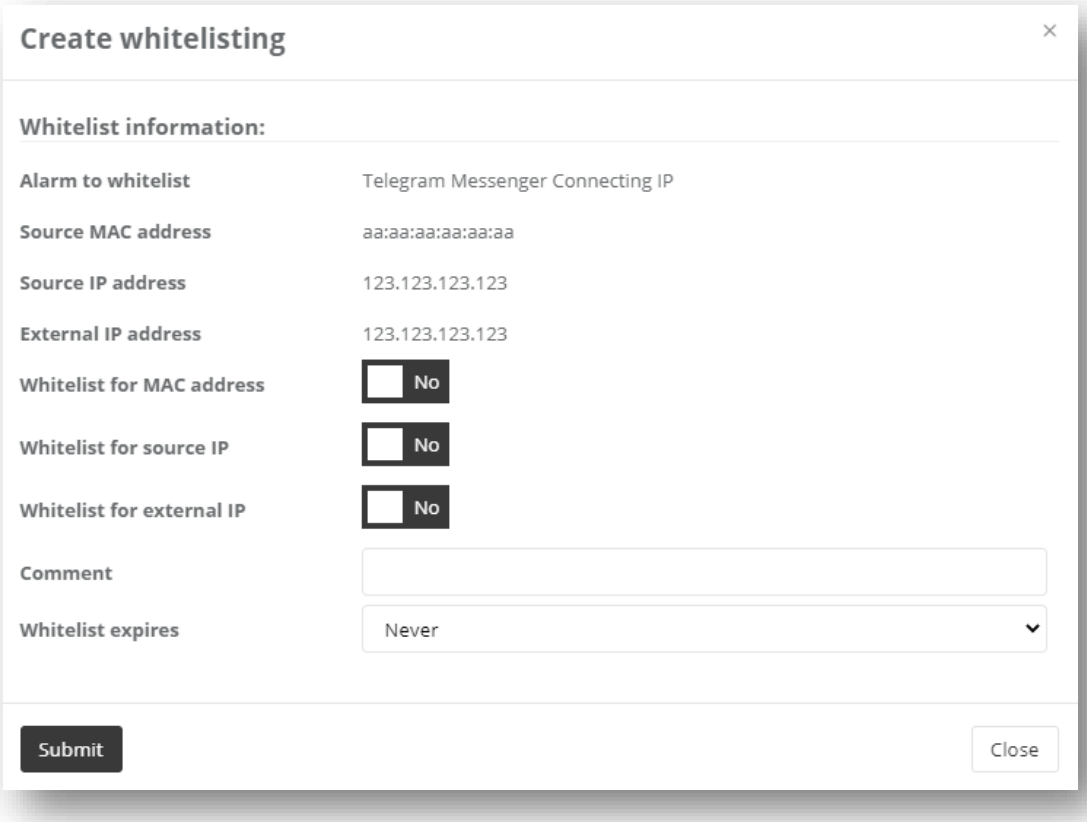
Priority:	Date / Time:	Alarm:	Source IP address:	Source port:	Source MAC address:	Destination IP address:	Destination port:	Device ID:	Details:
3	2021-09-03 13:17:53	Teamviewer - Remote Desktop Software	123.123.123.123	58923	aa:aa:aa:aa:aa:aa	123.123.123.123	443	12345	More info
3	2021-09-03 13:15:44	SSH tunnel (port based)	123.123.123.123	45339	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	More info
3	2021-09-03 13:15:40	SSH tunnel (port based)	123.123.123.123	51920	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	More info
3	2021-09-03 13:15:32	SSH tunnel (port based)	123.123.123.123	37358	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	More info
3	2021-09-03 13:15:09	SSH tunnel (port based)	123.123.123.123	62239	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	More info
3	2021-09-03 13:15:03	SSH tunnel (port based)	123.123.123.123	57867	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	More info
3	2021-09-03 13:14:56	Telegram Messenger Connecting IP	123.123.123.123	63726	aa:aa:aa:aa:aa:aa	123.123.123.123	80	12345	More info
3	2021-09-03 13:14:48	Telegram Messenger Connecting IP	123.123.123.123	57923	aa:aa:aa:aa:aa:aa	123.123.123.123	443	12345	More info
3	2021-09-03 13:13:51	Telegram Messenger Connecting IP	123.123.123.123	54006	aa:aa:aa:aa:aa:aa	123.123.123.123	443	12345	More info
3	2021-09-03 13:13:43	Dropbox Data Storage Service - hxxp://api.dropbox.com	123.123.123.123	60615	aa:aa:aa:aa:aa:aa	123.123.123.123	443	12345	More info

In the Details overview you will see an IP number under Source - details. This address is a specific address of a computer, printer or other device connected to your network. Any threats come from the device with this specific IP address. It is advisable to investigate the cause as soon as possible and to ensure that this potential threat cannot be spread any further.

You can also use the Details button behind the message. This gives you detailed information about the notification and you can look it up in Virustotal and MalewarePedia. If you're having trouble doing this, you can also use the 'Support' option. You then contact a Secureme2 employee.

2.2 ACTION BUTTONS

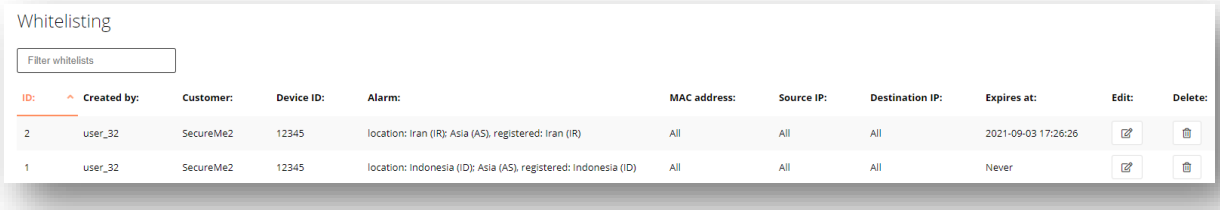
It may be a notification known to you in some cases. This means that a report is generated but that this is a valid connection or application for your company. In that case you can place the message on your Whitelist by means of the 'Whitelist alarm' button behind the message. You will then no longer receive such notifications on your dashboard.



If you are not sure whether such a report is valid, please contact your IT manager or Secureme2. They can advise you whether it is wise to accept this report. It is strongly recommended to use Whitelisting carefully..

2.3 WHITELISTING

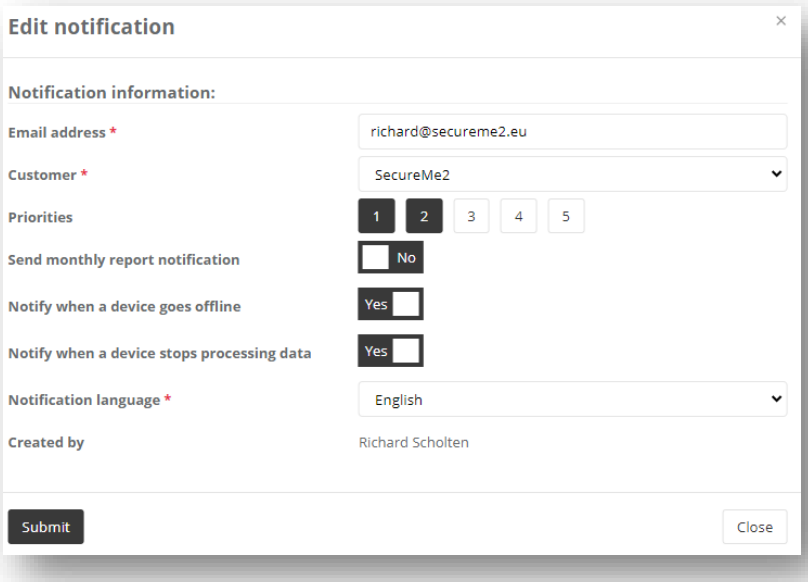
Viewing your disabled notifications, also known as Whitelisting, can be found in your task bar on your overview page under 'Settings'. All notifications that are valid according to you or your IT partner, can be included in this list. Any notifications included in this list will no longer appear as a notification in your portal.



If it is nevertheless desirable to receive a certain message, you can turn it off at any time by simply removing these rules. You can do this easily by using the trash can button at the end of the relevant rule under Actions. From that moment on, the rule is no longer included in the Whitelist and you will receive notifications again for this specific notification.

2.4 NOTIFICATIONS

In your portal it is possible to manage the reports found by SAM. In the task bar on your overview page you can click on the option 'Settings' under 'Notifications'. In the Active Notifications overview you can see at which Email address the notifications are received and which prio notifications are passed on. You can also indicate whether you wish to receive a monthly report.



If desired, you can specify multiple Email addresses where the same or different priority messages should be sent. You can also indicate here whether a monthly report should be received. Through 'New notifications' you can easily create these notification rules yourself. It is also possible to modify existing notifications or to delete them..

It is strongly recommended to have at least 1 Email address which receives all notifications

2.5 LOGGING OUT

As soon as you have been able to analyze your reports, postpone actions or give priority to the report, do not forget to log out properly.

3 CONTACT

Should you have any questions and/or comments regarding this manual, please contact Securme2 at any time. Although the manual has been compiled with care, you may still have more specific questions when setting up or evaluating your reports. In that case, you can always contact your IT manager or one of the colleagues at Secureme2..