

# Table of Contents

How to use Audit Trail ..... 1

Where can you see the Audit Trail? ..... 1

Details of Major Filter ..... 2

[Datetime] ..... 2

[User] ..... 2

[Operator Level] ..... 3

[IP] ..... 3

[Category] ..... 3

[Target] ..... 3

[Action] ..... 3

[Save Filter] ..... 3

[CSV export] ..... 4

[Column Setting] ..... 4

## How to use Audit Trail

The Audit Trail is one of new features of BioStar 2.5.0 to find out all actions of the system administrator. This function helps you to check that which data is created, modified or deleted by the system administrator who login to BioStar 2.

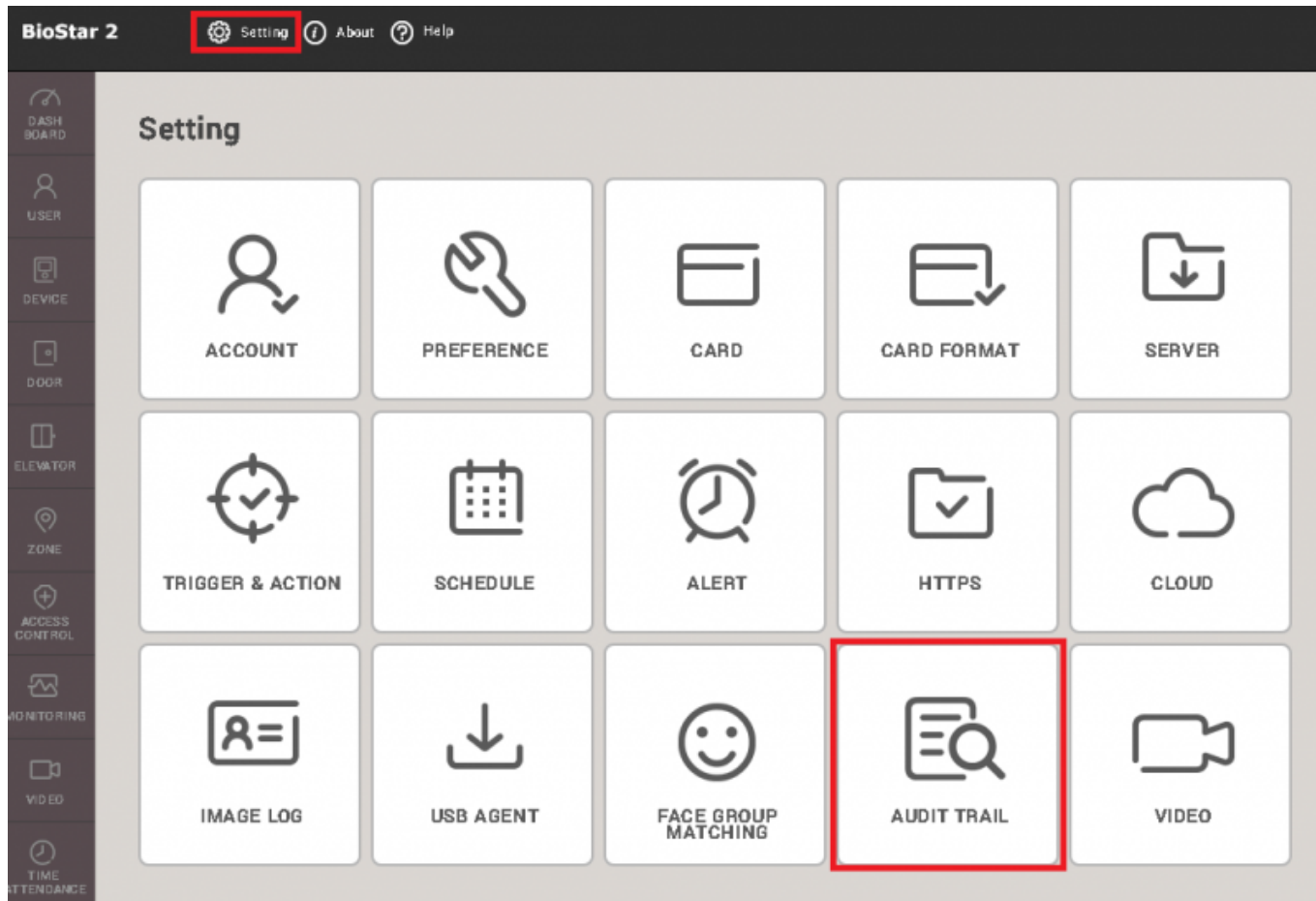
### Information about edited values are not shown:

The audit trail shows which items were edited, but it doesn't show what value it was changed to.

For example, if you changed the email address of a user, the log will show that the email address item was changed. However it will **not** show what email address it was changed to (i.e ethan@gmail.com to james@gmail.com)

## Where can you see the Audit Trail?

If you go to the **Setting** > **AUDIT TRAIL**, you can see the screen of Audit Trail.



Details of Major Filter

[Datetime]

Basically, you can check the records on Audit Trail for the last 1 month or 3 months.

Last 1 Month

Last 3 Months

Audit Trail

Filter

Datetime

2017/06/28 00:00 - 2017/09/28 23:59

User

None

Operator Level

None

IP

None

Datetime	User	Operator Level	IP
2017/09/28 11:40:51	Ethan(1111)	Administrator(1)	192.168.14.16
2017/09/28 11:22:27	hailey(123)	Administrator(1)	192.168.14.216
2017/09/28 07:38:38	Ethan(1111)	Administrator(1)	192.168.11.85
2017/09/28 07:38:35	Ethan(1111)	Administrator(1)	192.168.11.85
2017/09/28 07:38:35	Ethan(1111)	Administrator(1)	192.168.11.85

Moreover, you can set the specific period you want to check in the **Datetime** filter.

Last 1 Month

Last 3 Months

Audit Trail

Filter

Datetime

2017/06/28 00:00 - 2017/09/28 23:59

User

None

Operator Level

None

IP

None

Datetime	User	Operator Level	IP
2017/09/28 11:40:51	Ethan(1111)	Administrator(1)	192.168.14.16
2017/09/28 11:22:27	hailey(123)	Administrator(1)	192.168.14.216
2017/09/28 07:38:38	Ethan(1111)	Administrator(1)	192.168.11.85
2017/09/28 07:38:35	Ethan(1111)	Administrator(1)	192.168.11.85
2017/09/28 07:38:35	Ethan(1111)	Administrator(1)	192.168.11.85

[User]

You can search for Users with either user name or user ID. After entering the information on user, press **Enter** key. Then, you can see a list of items.

- <https://kb.supremainc.com/knowledge/>

## [Operator Level]

You can search for Operator Levels which are listed in Audit Trail. After entering the information on operator level, press **Enter** key. Then, you can see a list of items.

## [IP]

You can search for IP. After entering the information on IP, press **Enter** key. Then, you can see a list of items.

## [Category]

You can select multiple categories.

## [Target]

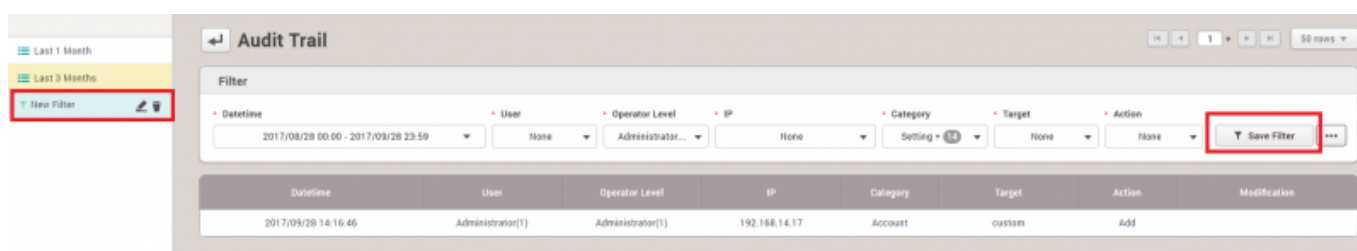
You can select certain target like devices, users.

## [Action]

You can select multiple categories.

## [Save Filter]

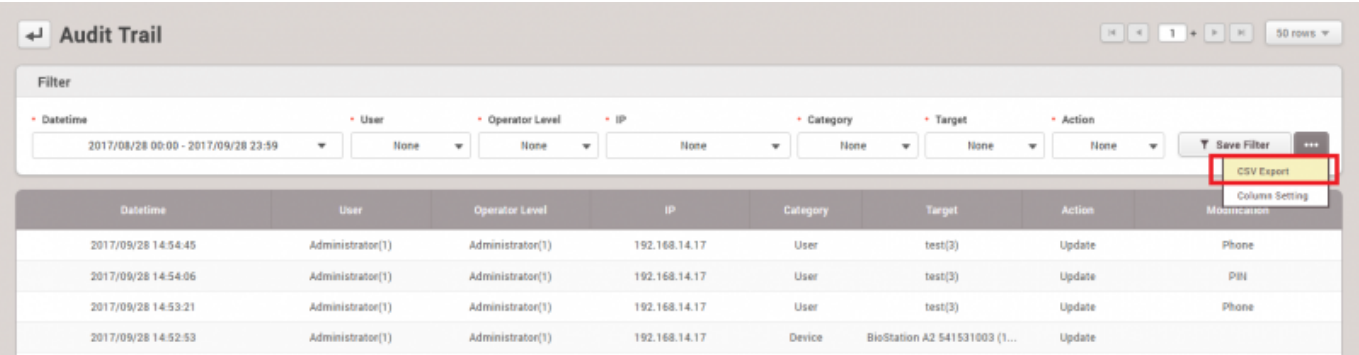
You can save the customized filter with the combination of filters.



In BioStar 2.5.0, you can make only one customized filter. In other word, you cannot save multiple customized filters. It will be improved in the future version of BioStar.

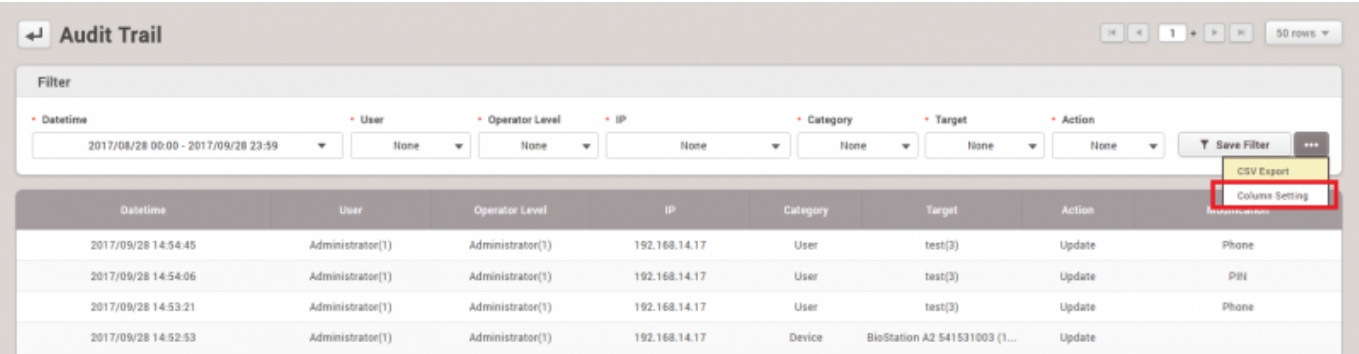
[CSV export]

You can export a \*.csv file.



[Column Setting]

You can select the columns you want to display from a column list.



From:  
<https://kb.supremainc.com/knowledge/> -

Permanent link:  
[https://kb.supremainc.com/knowledge/doku.php?id=en:how\\_to\\_use\\_audit\\_trail&rev=1507863178](https://kb.supremainc.com/knowledge/doku.php?id=en:how_to_use_audit_trail&rev=1507863178)

Last update: **2017/10/13 11:52**