

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]	3
[Operator Level]	3
[IP]	3
[Category]	3
[Target]	3
[Action]	4
[Save Filter]	4
[CSV export]	4
[Column Setting]	4

How to use Audit Trail

The Audit Trail is one of BioStar 2 Version 2.5.0 new features. This new feature allows the system administrator to see all actions taken in BioStar 2. This function helps administrative-level users to check specific data created, modified, or deleted by the system administrator who logs in to BioStar 2.

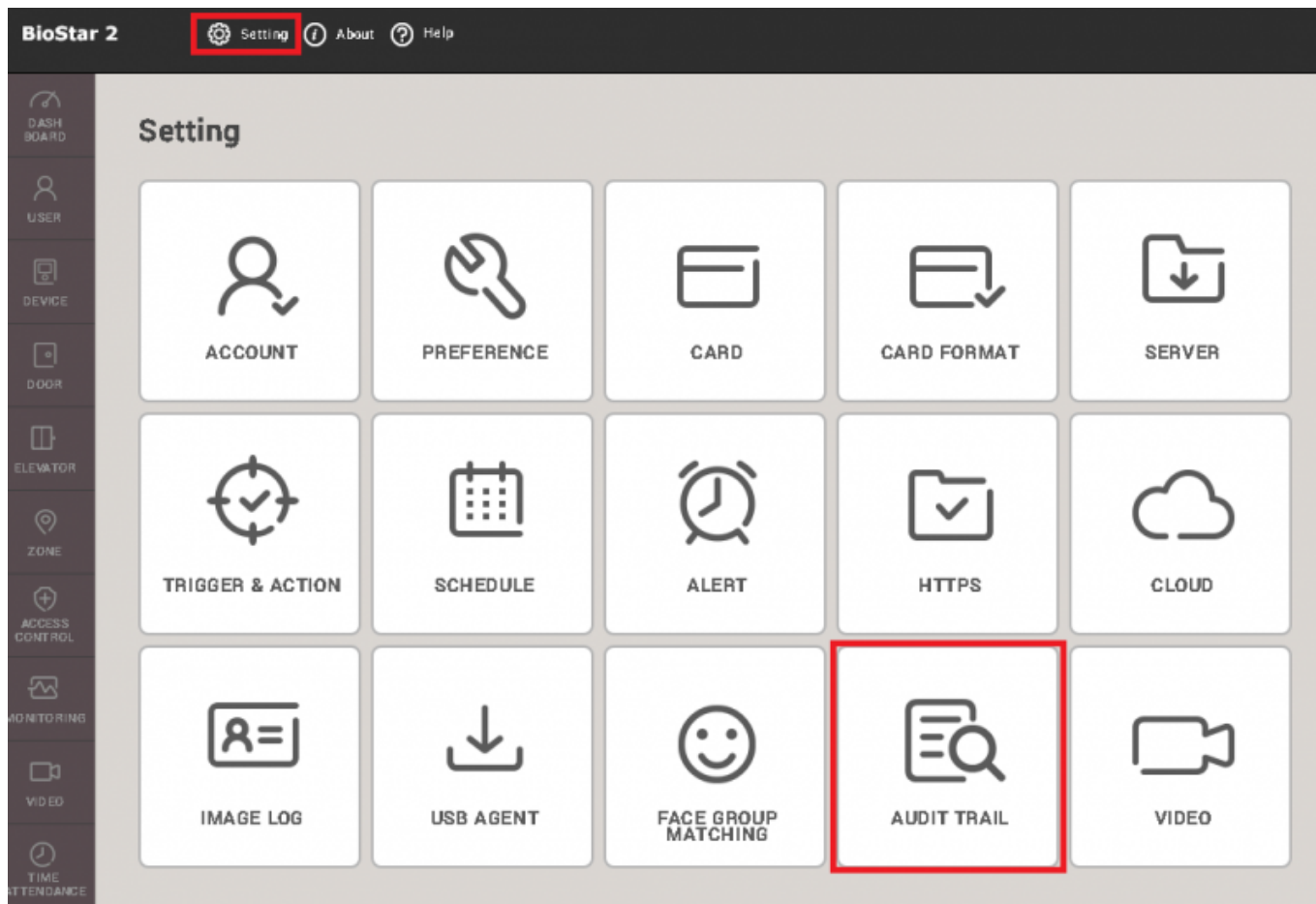
Previously saved information before the edit will not be shown:

The audit trail shows which items were edited but will not show the original value before making the change.

For example, if you changed a user's email address, the log would state in the modification column Email. However it will **not** show email address information: such as originally ethan@gmail.com changed into james@gmail.com

Where can you see the Audit Trail?

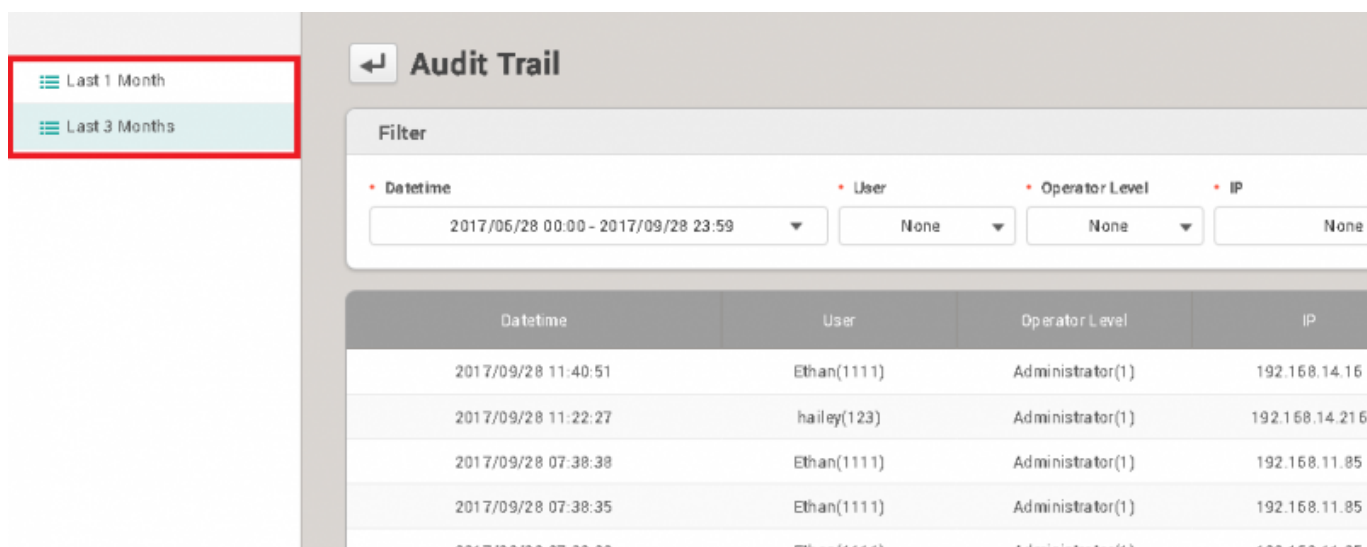
If you go to the **Setting** → **AUDIT TRAIL**, you can see Audit Trail menu.



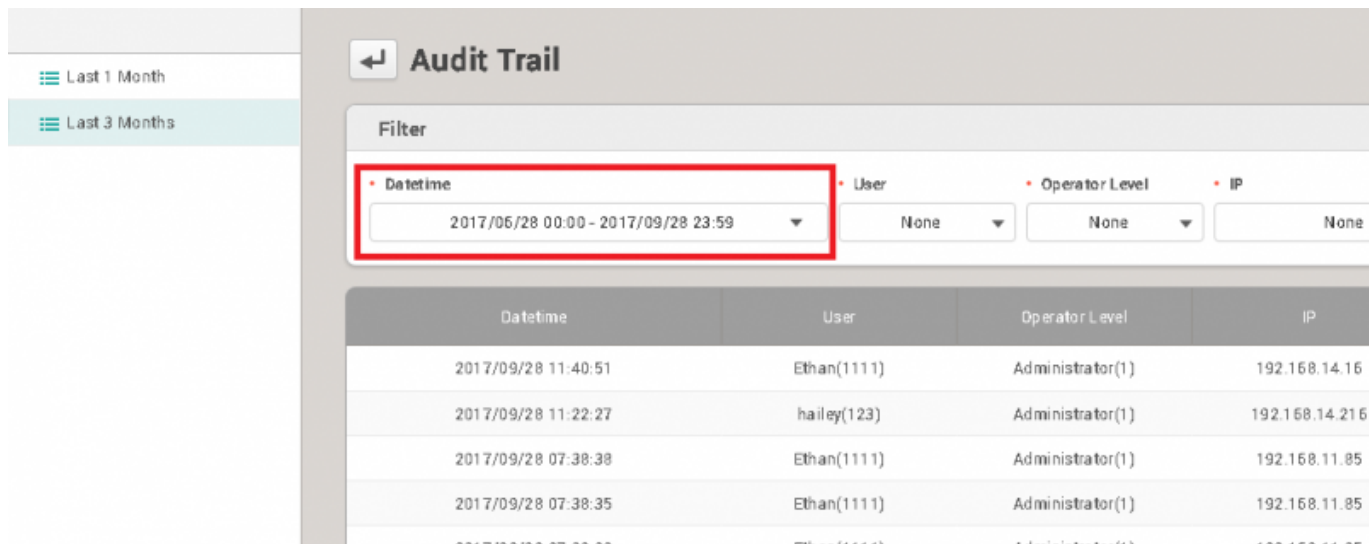
Details of Major Filter

[Datetime]

You can easily check the records on Audit Trail by clicking the last 1 month or 3 months.



You can also set the specific period you want to check in the **Datetime** filter.



The screenshot shows the 'Audit Trail' interface. On the left, there are two filter buttons: 'Last 1 Month' and 'Last 3 Months'. The main area has a 'Filter' section with four dropdown menus: 'Datetime', 'User', 'Operator Level', and 'IP'. The 'Datetime' dropdown is highlighted with a red box and shows the range '2017/06/28 00:00 - 2017/09/28 23:59'. Below the filters is a table with four columns: 'Datetime', 'User', 'Operator Level', and 'IP'. The table contains five rows of data.

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 07:38:30	Ethan(1111)	Administrator(1)	192.168.11.85

[User]

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

[Operator Level]

You can search for Operator Level 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]

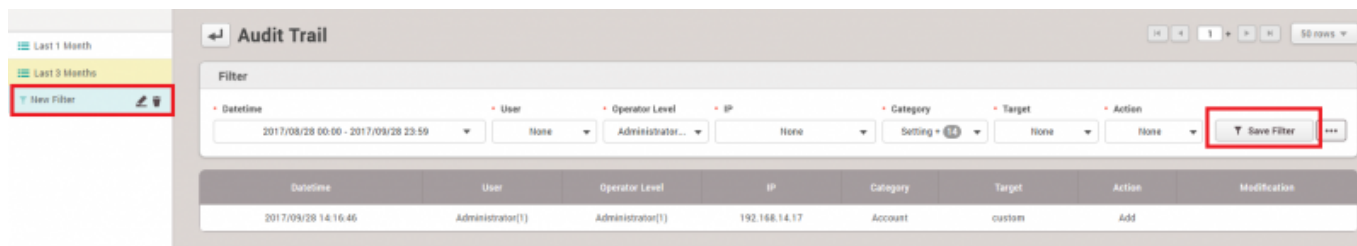
You can select certain targets like devices, users.

[Action]

You can select multiple categories.

[Save Filter]

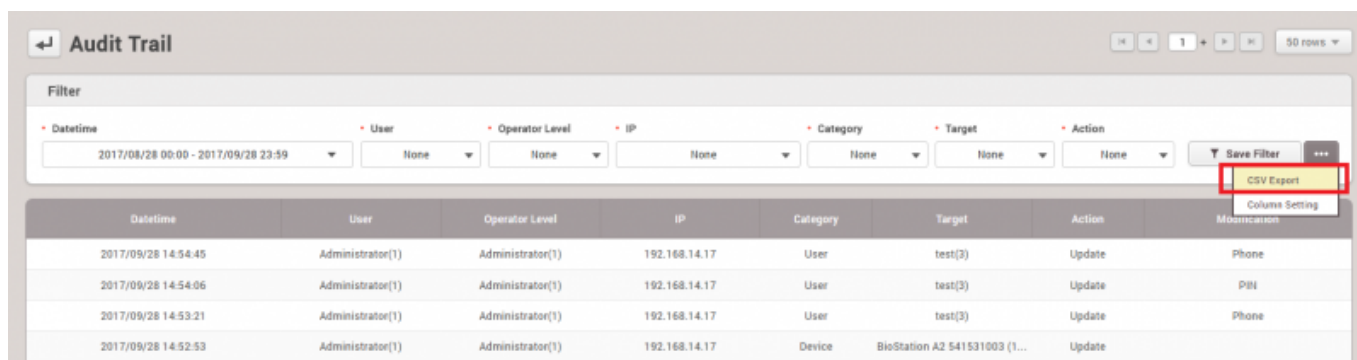
You can save the customized filter with a combination of filters.



In BioStar 2.5.0, you can make only one customized filter. In other words, 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.

Audit Trail

50 rows

Filter

Datetime

2017/08/28 00:00 - 2017/09/28 23:59

User

None

Operator Level

None

IP

None

Category

None

Target

None

Action

None

Save Filter

CSV Export

Column Setting

Datetime	User	Operator Level	IP	Category	Target	Action	
2017/09/28 14:54:45	Administrator(1)	Administrator(1)	192.168.14.17	User	test(3)	Update	Phone
2017/09/28 14:54:06	Administrator(1)	Administrator(1)	192.168.14.17	User	test(3)	Update	PIN
2017/09/28 14:53:21	Administrator(1)	Administrator(1)	192.168.14.17	User	test(3)	Update	Phone
2017/09/28 14:52:53	Administrator(1)	Administrator(1)	192.168.14.17	Device	BioStation A2 541531003 (1...	Update	

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

Permanent link:
https://kb.supremainc.com/knowledge/doku.php?id=en:how_to_use_audit_trail

Last update: **2022/12/28 14:29**