

# (SIEM)

1.6.3092:3197M WNAME ( ) Syslog SNMP. ( ) :

- AUDIT\_EVENT ( - , , ( ) ;
- ENDPOINT\_EVENT ( - ( ) ( ) );
- TACACS\_EVENT ( TACACS+ , , );
- ADC\_EVENT ( - Active Directory).

SIEM .

:

- Syslog RFC 5424 TCP UDP 514 ( );
- SNMP Trap RFC 3416 UDP 162 ( 2c).

Syslog/TLS, SNMPv3, , , support@netams.com

WNAME . . , , ( ) . "" "" " , , .

## Нотификации

Нотификации позволяют зарегистрировать обработчик, который будет вызываться при наступлении заданного типа событий. При этом происходит уведомление внешней системы, что можно использовать, например, при интеграции с CRM системами, оффлайн-рекламе, ИБ-аудите и т.п.

Создать нотификацию

Показывать: 10 записей на странице

Быстрый поиск:

Название	Тип	Обработчик	Статус	Кол-во срабатываний
Данные не найдены				

Нет записей

Предыдущая

Следующая

## Изменение нотификации

×

Параметры

Площадки

Обработчик

### Условие срабатывания

☐ Ассоциация с беспроводной сетью

☐ Редирект на портал

☐ Запрос авторизации

☐ Подтверждение авторизации

☐ Запуск сессии

☐ Останов сессии

☒ Событие аудита

☒ Событие эндпоинта

☒ Событие TACACS+

☒ Событие коннектора с AD

### Название

syslog-siem

( ), ( , ).

! SNMP Syslog , " " " " .

" " .

## Изменение нотификации



Параметры

Площадки

Обработчик

☒ Для всех площадок

Для этих площадок:

- ☐ 999 LAB Mercury City Tower
- ☐ 1000 IXCellerate guest Wi-Fi
- ☐ 1002 Castorama\_7121\_MOW\_KOTELNIKI
- ☐ 1003 Castorama\_7170\_MOW\_ELECTROSTAL
- ☐ 1004 Mercury guest Wi-Fi

Срабатывать для каждого события



Вкл.

Сохранить изменения

Закрыть

( SNMP- " Trap SNMP ).

Изменение нотификации

Параметры

Площадки

Обработчик

☐ Скрипт

☐ Запрос GET

☐ Запрос POST

☐ Уведомлять Radar

☐ Отправлять событие в SYSLOG

☒ Отправлять Trap по SNMP

Трап сервер

1.1.1.1

Отправлять

☐ MAC

☐ ID площадки

☐ ID сессии

Комьюнити (v2c)

public

☐ Объект "пользователь"

☐ Объект "площадка"

☐ Объект "сессия"

Тестовый запуск

Вкл.

Сохранить изменения

Закрыть

Syslog- " SYSLOG" - CEF ().

Изменение нотификации

Параметры

Площадки

Обработчик

☐ Скрипт

☐ Запрос GET

☐ Запрос POST

☐ Уведомлять Radar

☒ Отправлять событие в SYSLOG

☐ Отправлять Trap по SNMP

☐ Email

Хост

10.1.1.100

Порт

514

Протокол

☒ UDP ☐ TCP

Отправлять

☐ CEF (упрощенный)

☐ MAC

☐ ID площадки

☐ ID сессии

☒ CEF (расширенный)

☐ Объект "пользователь"

☐ Объект "площадка"

☐ Объект "сессия"

Syslog- , (TCP, UDP).

" " , .

WNAM , - - wnam.log :

```
11:58:38.184 DEBUG [NotificationService.java:244] - Execute notification
'snmp1', handler SNMP, event type ENDPOINT_EVENT, object: {FAIL;48:FD:A3:75:C8:
F4;PAP;not-allowed-pap-mac-state}
11:58:38.184 DEBUG [NotificationService.java:320] - Notification SNMP type
ENDPOINT_EVENT to: 1.1.1.1 on: {AccessServer=hAP [R20 Mikrotik LAB],
AuthState=FAIL, AuthenticationProfile=, AuthorizationProfile=Default reject,
FailReason=not-allowed-pap-mac-state, Identity=48:FD:A3:75:C8:F4, MAC=48:FD:A3:
75:C8:F4, Method=PAP, NasAddress=hap, RemoteIp=10.130.129.66, SiteName=change
address ZZZ, Timestamp=06.02.2023 11:58:38, Type=ENDPOINT_EVENT, TypeStr= }

11:58:38.186 DEBUG [NotificationService.java:244] - Execute notification
'syslog1', handler SYSLOG, event type ENDPOINT_EVENT, object: {FAIL;48:FD:A3:75:
C8:F4;PAP;not-allowed-pap-mac-state}
11:58:38.186 DEBUG [NotificationService.java:375] - Notification SYSLOG type
ENDPOINT_EVENT to: 1.1.1.1 on: {AccessServer=hAP [R20 Mikrotik LAB],
AuthState=FAIL, AuthenticationProfile=, AuthorizationProfile=Default reject,
FailReason=not-allowed-pap-mac-state, Identity=48:FD:A3:75:C8:F4, MAC=48:FD:A3:
75:C8:F4, Method=PAP, NasAddress=hap, RemoteIp=10.130.129.66, SiteName=change
address ZZZ, Timestamp=06.02.2023 11:58:38, Type=ENDPOINT_EVENT, TypeStr= }
```

SNMP- IANA "" 1.3.6.1.4.1.23099.

Syslog- , Common Event Format, .

:

CEF:0/NETAMS/WNAM/1.6/ENDPOINT\_EVENT/Endpoint rejected/6/app=EAP\_PEAP cs1=EAP/AD  
cs3=c19800-2 [WLAB] act=Rejected cs2=FNM Wi-Fi dst=10.241.200.6 cs5=WNAM-09  
suser=cisco-wifi-phone2 src=10.241.200.32 cs4=c19800-2:172.16.130.46 smac=94:83:  
C4:14:25:96  
externalId=06C8F10A00001D774342764C message=OK;94:83:C4:14:25:96;EAP\_PEAP;

:

CEF:0 - CEF,0

NETAMS -

WNAM -

1.6 -

- :

TACACS_EVENT	: , ,
AUDIT_EVENT	: - WNAM,
ADC_EVENT	:
ENDPOINT_EVENT	:

- , " "

- (severity)

, "=", , :

act	, Authenticated Rejected
app	, PAP EAP_PEAP
smac	
suser	Identity
src	IP
externalId	
cs1	
cs2	
cs3	(NAS)
dst	IP (NAS)
cs4	(NAS)
cs5	
message	, ;