

VIP

1.3.1151 WNAME () Wi-Fi. - VIP, :

- ;
- ;
- ;
- ;
- (captive portal) - (.).

, (, , -) (,).

() , "" "" , . , , VIP-. :

- WNAME;
- MAC-.

WNAME

:

1. "" "" " VIP".

Авторизация

Метод

Отправка СМС абоненту

Провайдер СМС

Kannel шлюз

Логин

wnam_user

Пароль

Тест

Настройки СМС

Заголовок

ORANGE

Текст

%CODE%

Ответный код

4 цифры

Запомнить авторизацию на

7 дней

Имя страницы

Отправка СМС абоненту (по умолчанию)

Выбор

☐ Авторизация сразу включает доступ

☐ Рекламные кампании

☒ Авторизованные становятся VIP

☐ Перезапрашивать номер или авторизацию

☐ Запрашивать ваучер как средство платного доступа

☐ Если номер телефона уже соответствует любому пользователю

Сохранить изменения

2. "" "VIP".

Параметры записи о пользователе

Общие

Ограничения

Категории

Оплата

Лог

Статус

Не блокирован

Сейчас заблокировать на

Заблокировать потом навсегда

VIP пользователь ?

☒

Длительность сессии

Игнорировать лимиты на суммы сессий

☐

Скорость сессии, кБит/с:

прием

передача

Счетчик СМС/звонков:

отправлено

1

подтверждено

1

Сбросить все активные сессии

Поместить в карантин

Сессии

Удалить

Сохранить изменения

Заккрыть

VIP- "".

Пользователи

Добавить пользователя

Выписать ваучер

Чёрные/белые списки

Сброс авторизации

Незавершенные авторизации

Карантинные

VIP

Созданные: ☐ за все время ☐ 5 минут ☐ 1 час ☐ сегодня

Применить

Показать 10 записей

Поиск:

MAC	Телефон	IP	Пользователь	Время создания	Последнее подключение
5C:ED:F4:07:9C:62	79639758313		5c:ed:f4:07:9c:62	19.01.2023 12:55:08	
B8:87:6E:A1:86:C2	79168550827	10.66.0.212	b8:87:6e:a1:86:c2	16.12.2022 13:55:28	27.12.2022 11:22:25
EC:A9:07:31:03:41	79037225040		EC:A9:07:31:03:41	18.10.2022 16:27:57	

WNAM , VIP- , , ("").

-

, VIP- (,) Wi-Fi - .

, , IP-. RADIUS WNAM.

-, Cisco WLC Mikrotik. -, FreeRADIUS WNAM, [/etc/freeradius/wnam-freeradius-bridge.pl](#)

, FreeRADIUS WNAM, : <http://www.netams.com/files/wnam/misc/wnam-freeradius-bridge.pl>.

Mikrotik - .

Interfaces Bridge Switch PPP Mesh IP MPLS Routing System Queues Files Log Radius New Terminal Tools MetaROUTER Partition Make Supout.rif Undo Redo Hide Menu Hide Passwords Safe Mode Design Skin Manual WinBox Graphs End-User License Logout	OKCancelApplyRemove	
	default	
	Name	mk1
	Hotspot Address	10.130.3.1
	DNS Name	mk.k18.netams.com
	HTML Directory	hotspot
	HTML Directory Override	
	Rate Limit (rx/tx)	
	HTTP Proxy	
	HTTP Proxy Port	0
	SMTP Server	
	Login By	☒ MAC ☐ Cookie ☐ HTTP CHAP ☐ HTTPS ☒ HTTP PAP ☐ Trial ☐ MAC Cookie
	MAC Auth. Mode	MAC as username
	MAC Auth. Password	
	HTTP Cookie Lifetime	3d 00:00:00
	SSL Certificate	none
	Split User Domain	☐
	Trial Uptime Limit	00:30:00
	Trial Uptime Reset	1d 00:00:00
	Trial User Profile	default1
	Use RADIUS	☒
	Default Domain	k18
	Location ID	
	Location Name	

MAC Format

XX:XX:XX:XX:XX:XX ▼

(MAC Auth. Password), (captiveportal_pass, password).

Cisco WLC MAC- "MAC Filtering" :

1. Cisco WLC "WLANs" "Security".

The screenshot shows the Cisco WLC configuration interface for editing a WLAN named 'tmp'. The left sidebar shows the navigation menu with 'WLANs' selected. The main content area has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. Under the 'Security' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'Layer 2' sub-tab is active, showing 'Layer 2 Security' set to 'None' and 'MAC Filtering' checked. There is also a 'Fast Transition' checkbox which is unchecked.

2. "Layer 3" .

The screenshot shows the same Cisco WLC configuration interface, but now the 'Layer 3' sub-tab is active. It displays various security options: 'Layer 3 Security' is set to 'Web Policy', and 'Authentication', 'Passthrough', 'Conditional Web Redirect', and 'Splash Page Web Redirect' are all unchecked. The 'On MAC Filter failure' option is selected. Below these, there are fields for 'Preauthentication ACL' (IPv4: wnam, IPv6: None, WebAuth FlexAcl: None), 'Sleeping Client' (unchecked), 'Over-ride Global Config' (checked), 'Web Auth type' (External(Re-direct to external server)), and 'URL' (http://172.16.130.5:8080/cp/cisco). At the bottom, there is a section for 'PN Pass-Through'.

"Allow AAA Override".



WLANs

- ▼ WLANs
- WLANs
- Advanced

WLANs > Edit 'tmp'

General Security QoS Policy-Mapping Advanced

Allow AAA Override	☒ Enabled
Coverage Hole Detection	☐ Enabled
Enable Session Timeout	☐
Aironet IE	☒ Enabled
Diagnostic Channel	☐ Enabled
Override Interface ACL	IPv4 None IPv6 None
P2P Blocking Action	Disabled
Client Exclusion	☐ Enabled
Maximum Allowed Clients	0
Static IP Tunneling	☐ Enabled
Wi-Fi Direct Clients Policy	Disabled
Maximum Allowed Clients Per AP Radio	200
Clear HotSpot Configuration	☐ Enabled
Client user idle timeout(15-100000)	☐
Client user idle threshold (0-10000000)	0 Bytes

Off Channel Scanning Defer

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☒ Required

OEAP

Split Tunnel (Printers) ☐ Enabled

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select