

# CWA 2504, 55, vWLC

1.4.1391 WNAME . Cisco Cisco ISE, WNAME ISE . ISE .

- Cisco :

- - ;
- (WNAME);
- ( );
- RADIUS- .

, . DNS, SSL-. URL <http://1.1.1.1/> "".

, , CWA :

- RADIUS- (WNAME) ACL URL ;
- - ( );
- (WNAME);
- WNAME RADIUS CoA ;
- RADIUS- "";
- WNAME .

, .

CWA SSID, , , DHCP .

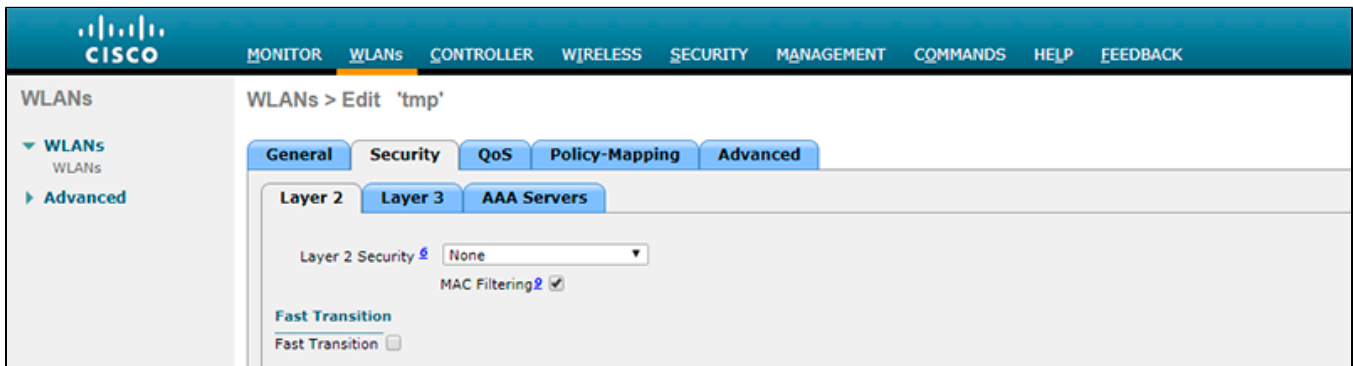
:

- 172.16.130.13 - RADIUS- WNAME;
- 172.16.130.5 8080 - WNAME, RADIUS CoA ;
- 10.208.144.213 - Cisco vWLC 8.0.140.0;
- 10.208.148.0/24 - ;
- SSID - tmp.

WNAME ,.. (- RADIUS-) . IP-, , IP-, .

1.

SSID "" , , -, DHCP, NAT,. SSID . L2 ("Layer 2 Security" "None"), "Mac Filtering" . Cisco.



L3 "Layer 3 Security" ( Web Auth).



" Servers" ( WNAME), Interim Update ( ).

**CISCO** MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs > Edit 'tmp'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

**Radius Servers**

Radius Server Overwrite interface ☐ Enabled

| Authentication Servers                      |                             | Accounting Servers                          |                             |
|---------------------------------------------|-----------------------------|---------------------------------------------|-----------------------------|
| <input checked="" type="checkbox"/> Enabled | IP:172.16.130.13, Port:1812 | <input checked="" type="checkbox"/> Enabled | IP:172.16.130.13, Port:1813 |
| Server 2                                    | None                        | Server 2                                    | None                        |
| Server 3                                    | None                        | Server 3                                    | None                        |
| Server 4                                    | None                        | Server 4                                    | None                        |
| Server 5                                    | None                        | Server 5                                    | None                        |
| Server 6                                    | None                        | Server 6                                    | None                        |

**Radius Server Accounting**

Interim Update ☒ Interim Interval 300

**LDAP Servers**

"Advanced" :

- Allow AAA Override;
- DHCP address assignment - Required;
- NAC State: RADIUS NAC ( ISE NAC).

"Client Exclusion".

**CISCO** MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

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 18 ☐ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl 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(15-1000000) ☐

Client user idle threshold (0-10000000) 0 Bytes

**DHCP**

DHCP Server ☐ Override

DHCP Addr. Assignment ☒ Required

**OEAP**

Split Tunnel ☐ Enabled

**Management Frame Protection (MFP)**

MFP Client Protection ☐ Optional

**DTIM Period (in beacon intervals)**

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

**NAC**

NAC State Radius NAC

Load Balancing and Band Select

ACL (), WNAME . ACL ( "wname\_cwa").



ACL WNAME : WNAME "wname-cwa" "cwa\_wname".

CISCO

MONITOR

WLANs

CONTROLLER

WIRELESS

SECURITY

MANAGEMENT

COMMANDS

HELP

FEEDBACK

Security

AAA

General

RADIUS

Authentication

Accounting

Fallback

DNS

Downloaded AVP

TACACS+

LDAP

Local Net Users

MAC Filtering

Disabled Clients

User Login Policies

AP Policies

Password Policies

Local EAP

Advanced EAP

Priority Order

Certificate

Access Control Lists

Access Control Lists

CPU Access Control Lists

FlexConnect ACLs

Layer2 ACLs

Access Control Lists

Enable Counters ☐

| Name                         | Type |                                     |
|------------------------------|------|-------------------------------------|
| <a href="#">welcome-wnam</a> | IPv4 | <input checked="" type="checkbox"/> |
| <a href="#">wnam_cwa</a>     | IPv4 | <input checked="" type="checkbox"/> |

Foot Notes

1. Counter configuration is global for acl and layer2acl.

ACL , DNS-. DNS- , . () .

!

ACL "Access Control Lists" , (.. ) .

, FlexConnect, wnam\_cwa "FlexConnect ACLs". ACL Wireless FlexConnect Groups ACL Mapping Policies.

Wireless

Access Points

All APs

Radios

802.11a/n/ac

802.11b/g/n

Dual-Band Radios

Global Configuration

Advanced

Mesh

RF Profiles

FlexConnect Groups

FlexConnect ACLs

OEAP ACLs

Network Lists

FlexConnect Groups > Edit 'HREAP1'

General

Local Authentication

Image Upgrade

ACL Mapping

Central DHCP

WLAN VLAN mapping

AAA VLAN-ACL mapping

WLAN-ACL mapping

Policies

Policies

Policy ACL wnam\_flex

Add

Policy Access Control Lists

wnam\_flex

☒

ACL - VLAN, WLAN .. .

. :.13 ( ) .5 ( CoA ).

**CISCO** MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

Security

Access Control Lists > Edit

General

Access List Name: wlan\_owa

Deny Counters: 0

| Seq | Action | Source IP/Mask                 | Destination IP/Mask            | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits |
|-----|--------|--------------------------------|--------------------------------|----------|-------------|-----------|------|-----------|----------------|
| 1   | Permit | 0.0.0.0 / 0.0.0.0              | 0.0.0.0 / 0.0.0.0              | UDP      | DNS         | Any       | Any  | Any       | 0              |
| 2   | Permit | 0.0.0.0 / 0.0.0.0              | 0.0.0.0 / 0.0.0.0              | UDP      | Any         | DNS       | Any  | Any       | 0              |
| 3   | Permit | 0.0.0.0 / 0.0.0.0              | 172.16.130.5 / 255.255.255.255 | Any      | Any         | Any       | Any  | Any       | 0              |
| 4   | Permit | 172.16.130.5 / 255.255.255.255 | 0.0.0.0 / 0.0.0.0              | Any      | Any         | Any       | Any  | Any       | 0              |
| 5   | Deny   | 0.0.0.0 / 0.0.0.0              | 0.0.0.0 / 0.0.0.0              | Any      | Any         | Any       | Any  | Any       | 0              |

"Auth Called Station ID Type" (AP MAC Address::SSID).

**CISCO** MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

Security

RADIUS Authentication Servers

Auth Called Station ID Type: AP MAC Address::SSID

Use AES Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Colon

| Network User                        | Management                          | Server Index | Server Address(Ipv4/Ipv6) | Port | IPSec    | Admin Status |
|-------------------------------------|-------------------------------------|--------------|---------------------------|------|----------|--------------|
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | 1            |                           | 1812 | Disabled | Enabled      |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | 2            |                           | 1812 | Disabled | Enabled      |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | 3            | 172.16.130.13             | 1812 | Disabled | Enabled      |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | 4            |                           | 1812 | Disabled | Enabled      |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 5            | 172.16.130.5              | 1812 | Disabled | Enabled      |

. /etc/freeradius/clients.conf (WNAM 1.6). "Support for RFC 3576" ( "Support for CoA").

**CISCO** MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

Security

RADIUS Authentication Servers > Edit

Server Index: 5

Server Address(Ipv4/Ipv6): 172.16.130.5

Shared Secret Format: ASCII

Shared Secret: \*\*\*

Confirm Shared Secret: \*\*\*

Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for RFC 3576: Enabled

Server Timeout: 2 seconds

Network User: ☒ Enable

Management: ☒ Enable

Realm List: [Realm List](#)

IPSec: ☐ Enable

- "RADIUS Accounting Servers" .

MONITOR
WLANS
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK

Security

AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP

RADIUS Accounting Servers

Acct Called Station ID Type
AP MAC Address:SSID
MAC Delimiter
Colon

| Network User                        | Server Index | Server Address(Ipv4/Ipv6) | Port | IPSec    | Admin Status                                |
|-------------------------------------|--------------|---------------------------|------|----------|---------------------------------------------|
| <input checked="" type="checkbox"/> | 1            | 172.16.130.13             | 1813 | Disabled | Enabled <input checked="" type="checkbox"/> |

( , ).

MONITOR
WLANS
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK

Security

AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists

RADIUS Accounting Servers > Edit

Server Index
1
Server Address(Ipv4/Ipv6)
172.16.130.13
Shared Secret Format
ASCII
Shared Secret
\*\*\*
Confirm Shared Secret
\*\*\*
Port Number
1813
Server Status
Enabled
Server Timeout
2 seconds
Network User
☒ Enable
Realm List
IPSec
☐ Enable

. WNAME.

## 2. WNAME

Cisco WLC ( " " "). , , .

Изменение сервера доступа

Параметры

RADIUS

TACACS+

Категории

Клиент

Тип

Cisco WLC

Имя устройства

wlc.2h

IP адрес (NAS-IP-Address)

10.208.144.213

Внешний IP адрес

192.168.1.1

Местоположение

HF lab r550a

Комментарий

Логин

Пароль

☒ Использовать счетчики аккаунтинга

получено 0 записей

☐ Менять местами счетчики приёма/передачи

☒ Определять имена устройств абонентов

☐ Принимать детализацию потоков NetFlow

получено 0 записей

Вкл.

Сохранить изменения

Закреть

RADIUS " " :

- cisco-avpair=url-redirect=http://\_\_wnam/cp/cisco?%URL%
- cisco-avpair=url-redirect-acl=wnam\_cwa



, , , cisco-avpair = url-redirect-acl=wnam\_cwa.

, ACL , . %URL% WNAM . , . WNAM HTTPS (80), URL .

RADIUS ( ) CoA.

Изменение сервера доступа

Параметры

RADIUS

TACACS+

Категории

Атрибуты предварительной авторизации

cisco-avpair=url-redirect=http://имя\_вашего\_сервера\_wnam/cp/cisco?%URL%  
cisco-avpair=url-redirect-acl=wnam\_cwa

Атрибуты CoA / пост-авторизации

Секретный ключ

Порт CoA

1700

( "" "). () , WNAM , RADIUS CoA ( ).

" ID" ( ) WLAN/SSID , . RADIUS- Airespace-Wlan-Id, .

Изменение площадки

Параметры

Авторизация

Перенаправление

Ограничения

Соцсети

RADIUS

Номер

4

Тип

Площадка

Адрес/название

HF WIFI LAN

Контактное лицо

Anton

Комментарий

Присвоенная IP подсеть

10.208.148.0/24

Тэг

Разрешенный сервер доступа

HF Lab r550a 10.208.144.213

Дополнительный ID на этом сервере

Категории

1

Вкл.

Удалить

Сохранить изменения

Закрыть

WNAM .

3.

WNAM    Wi-Fi .    WNAM .

## Параметры записи о сессии



|                      |                                            |                  |                      |
|----------------------|--------------------------------------------|------------------|----------------------|
| MAC                  | 24:0D:C2:B7:F9:B6                          | IP адрес         | 10.208.148.176       |
| Время начала         | 19.08.2017, 12:46:34                       | Время завершения | 19.08.2017, 12:48:14 |
| Длительность         | 0ч 1м 40с                                  | Сервер доступа   | 10.208.144.213       |
| Принято, байт        | 483203                                     | Отправлено, байт | 93159                |
| Площадка             | 4 HF WIFI LAN                              |                  |                      |
| Точка доступа        | 34:A8:4E:6A:C6:40 SSID=tmp (Cisco AP)      | Канал            |                      |
| Пользователь         | 24:0D:C2:B7:F9:B6 android-e4e5e79dad599c31 | 79995552211      |                      |
| Идентификатор сессии | d590d00a00000576fb089859-b7f9b6            |                  |                      |

Потоки данных в этой сессии

Параметры учетной записи пользователя

Заккрыть