

## **CONFIGURAZIONE WI-FI ARUBA: ACCESS POINT E TERMINALI**

<b>MATRICE DELLE REVISIONI</b>					
REVISION	DATA	DESCRIZION	REDAZION	VERIFICATA	APPROVATA
00	14.10.2024	1a emissione	Gruppo di lavoro	RSGI/RQ/RSPPGA/RSTRUUTT	DG/DS/DA/DSS
01	31.10.2024	Modifica Par.4, Par.5.1.1, Par.5.1.4	Gruppo di lavoro	RSGI/RQ/RSPPGA/RSTRUUTT	DG/DS/DA/DSS

access point e terminali

**IO\_XX\_00\_XX**

Pagina 2 di 51

ISTRUZIONE OPERATIVA

14/10/2024

<b>GRUPPO DI LAVORO PER LA REDAZIONE</b>		
<i>Cognome e nome</i>	<i>Qualifica</i>	<i>Struttura di appartenenza</i>
Predonzan Tomaso	Network administrator	ASUGI
Monti Maurizio	Network administrator	ASUGI
Chiffi Francesco	System Senior Expert	BV-Tech

## INDICE

1. SCOPO .....	4
2. AMBITO DI APPLICAZIONE .....	4
3. ACRONIMI E DEFINIZIONI .....	4
4. RESPONSABILITÀ .....	4
5. MODALITÀ ESECUTIVE .....	5
5.1. CONFIGURAZIONE DELL'INFRASTRUTTURA .....	5
5.1.1. ARCHITETTURA DELL'INFRASTRUTTURA WI-FI .....	5
5.1.2. ACCESSO AL MOBILITY CONDUCTOR .....	7
5.1.3. CONFIGURAZIONE ACCESS POINT .....	11
5.1.3.1. WLAN .....	11
5.1.3.1.1. DETTAGLIO WLAN - GENERAL .....	12
5.1.3.1.2. DETTAGLIO WLAN – VLANS .....	13
5.1.3.1.3. DETTAGLIO WLAN – SECURITY .....	14
5.1.3.1.4. DETTAGLIO WLAN – ACCESS .....	15
5.1.3.2. ROLES & POLICIES .....	16
5.1.3.2.1. DETTAGLIO ROLES & POLICIES - ROLES .....	17
5.1.3.2.2. DETTAGLIO ROLES & POLICIES - POLICIES .....	17
5.1.3.2.3. DETTAGLIO ROLES & POLICIES - APPLICATIONS .....	18
5.1.3.2.4. DETTAGLIO ROLES & POLICIES - ALIASES .....	18
5.1.3.3. ACCESS POINTS .....	19
5.1.3.3.1. DETTAGLIO ACCES POINTS – CAMPUS APS .....	19
5.1.3.4. AP GROUPS .....	22
5.1.3.4.1. DETTAGLIO AP GROUPS - APS .....	22
5.1.3.5. AUTHENTICATION .....	23
5.1.3.5.1. DETTAGLIO AUTH SERVERS .....	24
5.1.3.6. SERVICES .....	27
5.1.3.7. INTERFACES .....	28
5.1.3.8. CONTROLLERS .....	29
5.1.3.9. SYSTEM .....	29
5.1.3.10. TASKS .....	30
5.1.3.11. REDUNDANCY .....	31
5.1.3.12. IOT32 .....	32
5.1.4. AGGIUNTA DI UN NUOVO ACCESS POINT .....	33
5.2. CONFIGURAZIONE DEI TERMINALI .....	34
5.2.1. PROCEDURA CONFIGURAZIONE TERMINALE .....	34
5.2.2. VERIFICA CONNESSIONE TERMINALE .....	46
5.2.2.1. CLIENT .....	46
5.2.2.2. WLAN .....	48
6. GESTIONE DELLA DOCUMENTAZIONE .....	49
7. RIFERIMENTI (NORMATIVI E BIBLIOGRAFICI) .....	49
7.1. ARUBAOS .....	49
7.2. WI-FI CONTROLLER .....	49
7.3. ACCESS POINT .....	49
8. DOCUMENTI COLLEGATI .....	49
9. ALLEGATI (SE PRESENTI) .....	49
10. INDICE DELLE FIGURE .....	50

## 1. SCOPO

Scopo del presente documento è la definizione delle istruzioni operative relative a:

- Configurazione access point.
- Configurazione terminali.

## 2. AMBITO DI APPLICAZIONE

L'ambito di applicazione del presente documento è inerente alla configurazione dei 'Wireless Controller', degli 'Access point' e dei terminali che devono usufruire della rete wireless gestita dagli apparati precedentemente citati.

### NOTA BENE:

- Tutti i parametri e le configurazioni per le quali non venga esplicitamente indicata una azione di modifica nel presente documento, devono essere lasciati inalterati ai valori di default già presenti. La modifica di tali valori potrebbe causare anomalie di funzionamento.

## 3. ACRONIMI E DEFINIZIONI

- **802.1X:** standard IEEE che fornisce un meccanismo di autenticazione dei dispositivi che vogliono collegarsi tramite uno switch o un access point Wi-Fi ad una rete LAN o WLAN<sup>1</sup>.
- **Aruba Mobility Conductor:** dispositivo centralizzato per la gestione dei wireless Controller e relativi access point.<sup>2</sup>
- **Aruba Wireless Controller:** dispositivo centralizzato per la gestione degli access point<sup>3</sup>.
- **Aruba Access Point:** dispositivo periferico per la gestione della connettività Wi-Fi<sup>4</sup>.

## 4. RESPONSABILITÀ

- ASUGI:
  - Tomaso Predonzan
  - Maurizio Monti
  - Borut Jarc
- BVTECH:
  - Mauro Apolloni
  - Francesco Chiffi
- INSIEL:
  - Christian Zorzi

<sup>1</sup> [https://it.wikipedia.org/wiki/IEEE\\_802.1x](https://it.wikipedia.org/wiki/IEEE_802.1x)

<sup>2</sup> <https://www.arubanetworks.com/it/prodotti/wireless/Controller/mobility-Conductor/>

<sup>3</sup> <https://www.arubanetworks.com/it/prodotti/wireless/Controller/>

<sup>4</sup> <https://www.hpe.com/it/it/aruba-access-points.html>

## 5. MODALITÀ ESECUTIVE

### 5.1. CONFIGURAZIONE DELL'INFRASTRUTTURA

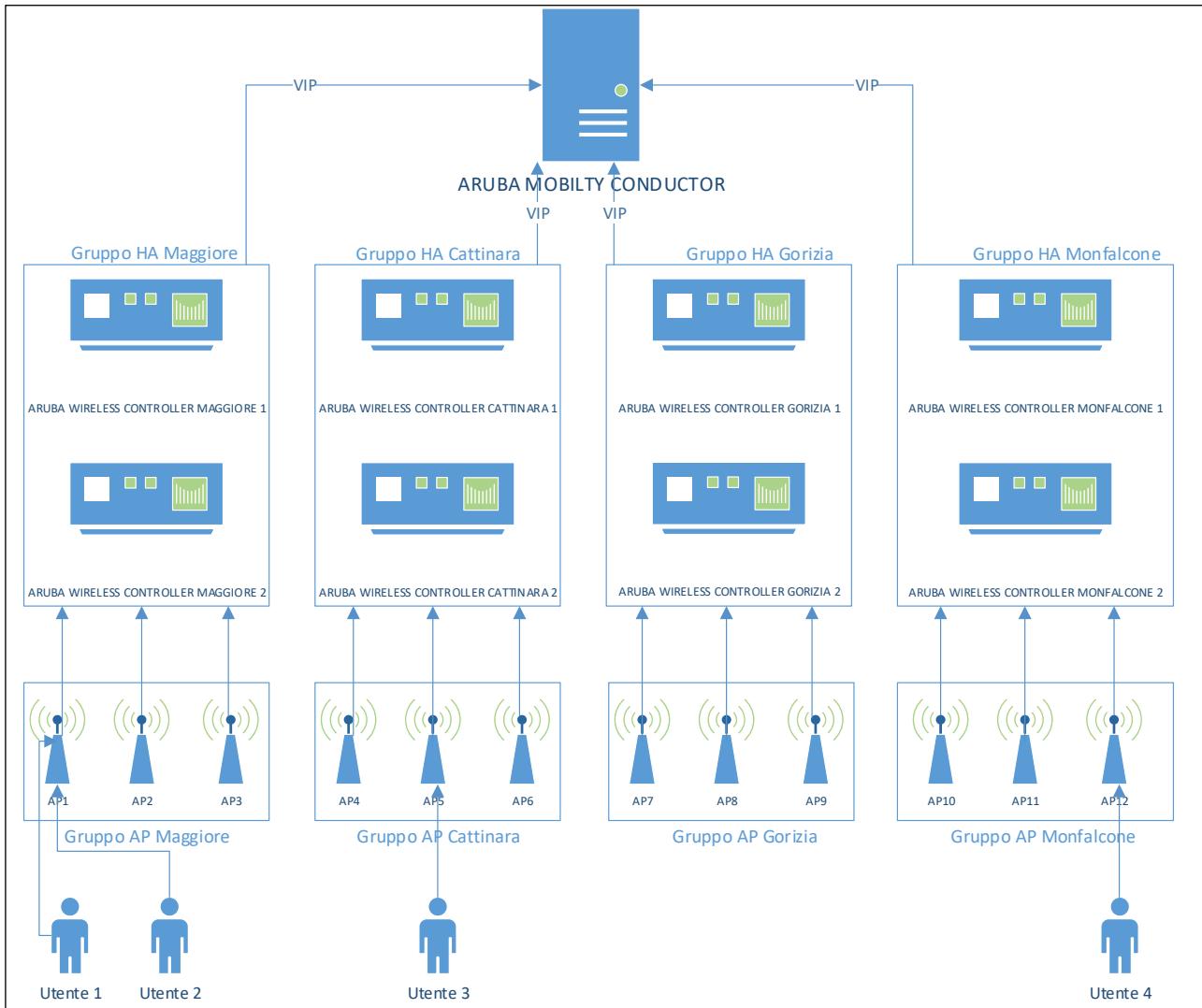
#### 5.1.1. ARCHITETTURA DELL'INFRASTRUTTURA WI-FI

L'infrastruttura si può suddividere in tre componenti principali:

- La componente core costituita dall' 'Aruba Mobility Conductor' che è in carico ad INSIEL.
- La componente perimetrale, costituita dagli 'Aruba Wireless Controller' (ARCN9240) disposti presso le varie sedi di ASUGI, nello specifico al momento in cui viene redatto il presente documento ne sono presenti complessivamente 8:
  - Ospedale Cattinara (Trieste): 2 Wireless Controller dotati di doppio modulo di alimentazione connessi su sistemi di alimentazione differenziata.
  - Ospedale Monfalcone: 2 Wireless Controller dotati di doppio modulo di alimentazione.
  - Ospedale Gorizia: 2 Wireless Controller dotati di doppio modulo di alimentazione.
  - Ospedale Maggiore (Trieste): 2 Wireless Controller dotati di doppio modulo di alimentazione connessi su sistemi di alimentazione differenziata.
- sono disposti in coppia per assicurare ridondanza in caso di malfunzionamento di uno di essi (alta affidabilità). Come si evince, essi sono disposti su base geografica. Utilizzano, ognuno una aggregazione di due fibre a 10 GBPS per il collegamento verso il 'Mobility Conductor', per la gestione degli 'Access point' e per la gestione del traffico effettivo di rete.
- La componente di accesso, costituita dagli Access Point, (ARUBA AP515) disposti nelle varie sedi secondo le conformazioni degli ambienti e le necessità locali.

In breve, il 'Mobility Conductor' consente la gestione centralizzata di tutti i 'Wireless Controller', che a loro volta si occupano di gestire gli 'Access point' secondo criteri che saranno dettagliati in seguito.

Di seguito un diagramma logico dell'infrastruttura:

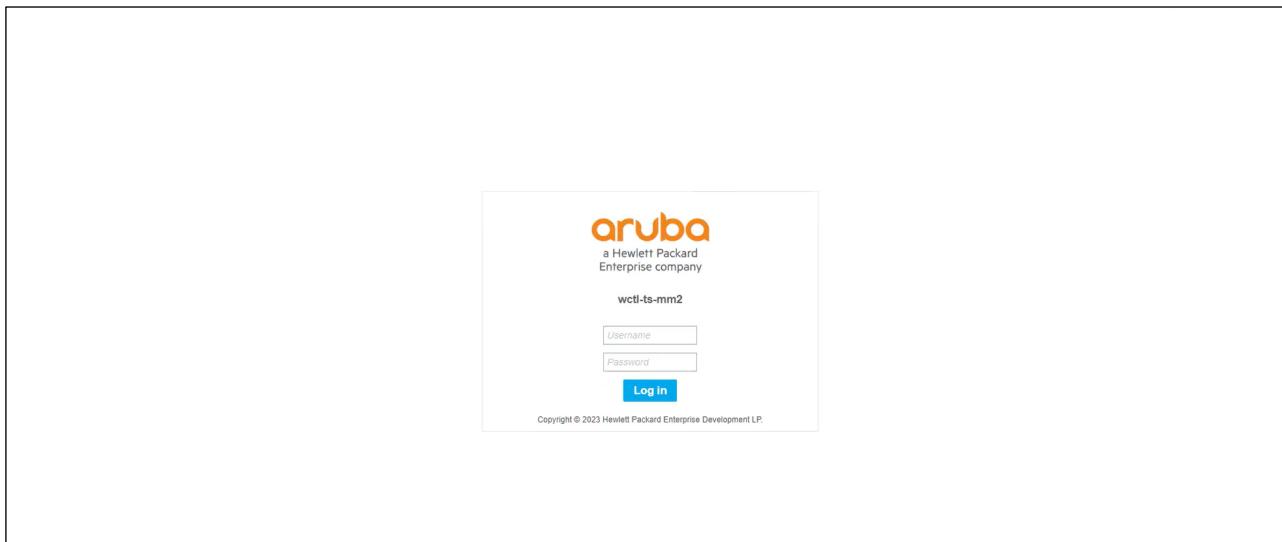


**Figura 1 - Diagramma logico infrastruttura WI-FI**

### 5.1.2. ACCESSO AL MOBILITY CONDUCTOR

Il ‘Mobility Conductor’ è accessibile all’indirizzo:

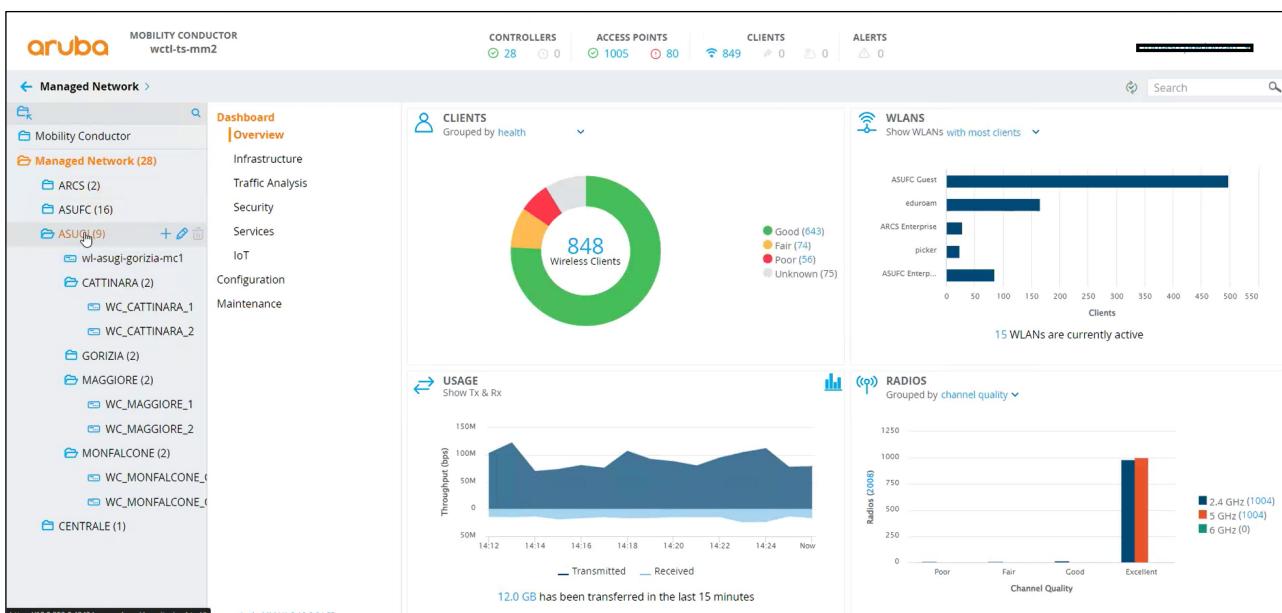
<HTTPS://10.0.253.8:4343/LOGIN.HTM>



**Figura 2 - Accesso al 'Mobility Conductor'**

Le credenziali da utilizzare saranno quelle fornite da INSIEL per il personale con ruolo di ‘Network Administrator’ per l’area isontina.

Si accede in tal modo alla schermata principale del ‘Mobility Conductor’:



**Figura 3 - Schermata principale del 'Mobility Conductor'**

access point e terminali

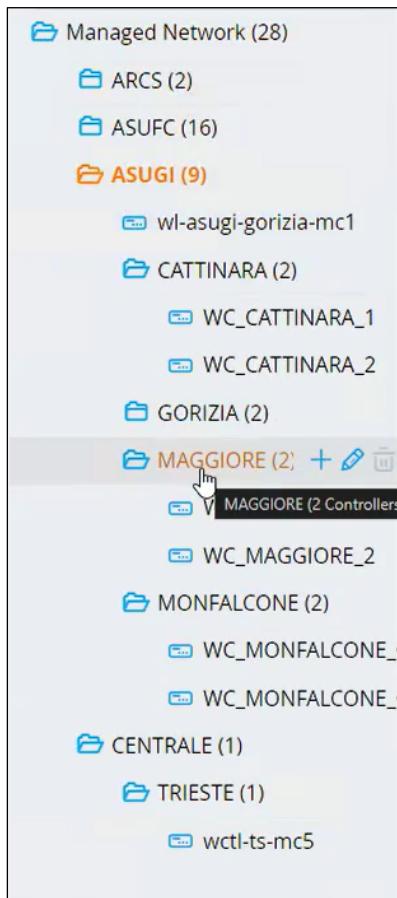
**IO\_XX\_00\_XX**

Pagina 8 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

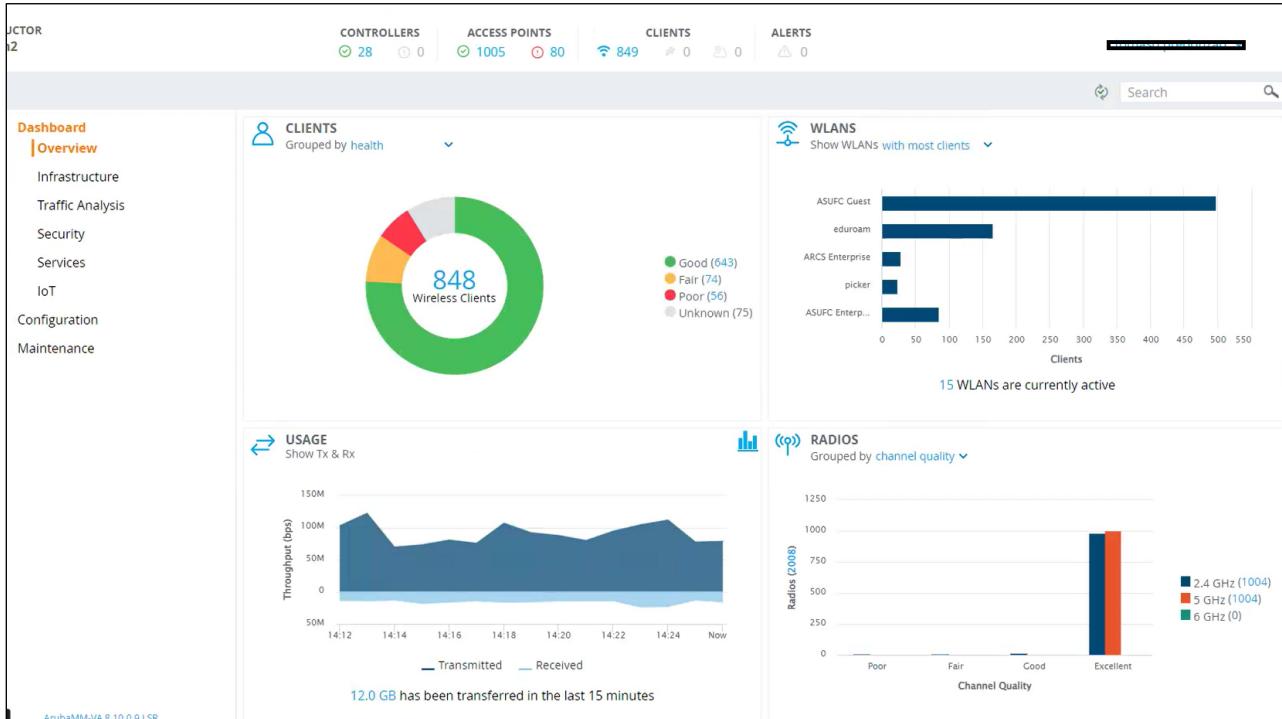
Si ricordi come il ‘Mobility Conductor’ sia di pertinenza di INSIEL; pertanto, sulla sinistra saranno visualizzate tutte le reti WI-FI gestite da INSIEL nella Regione Friuli-Venezia Giulia.



**Figura 4 - Reti gestite**

Saranno di pertinenza di ASUGI, unicamente le reti presenti sotto il nodo ‘ASUGI’, suddivise per collocazione geografica, come indicato nel paragrafo precedente. È possibile inoltre osservare che relativamente ad ogni nodo viene mostrato il numero di ‘Aruba Wireless Controller’ afferenti a quel nodo.

Nel riquadro principale vengono mostrate varie informazioni statistiche inerenti al funzionamento degli apparati sempre relativamente a tutte quanto sia di pertinenza di INSIEL.


**Figura 5 - Statistiche infrastruttura**

Ad esempio nell'header vengono mostrati:

- **CONTROLLERS:** il numero complessivo di WI-FI Controllers.
- **ACCESS POINTS:** il numero complessivo di Access points.
- **CLIENTS:** il numero complessivo di client collegati.
- **ALERTS:** eventuali allarmi di sistema.



access point e terminali

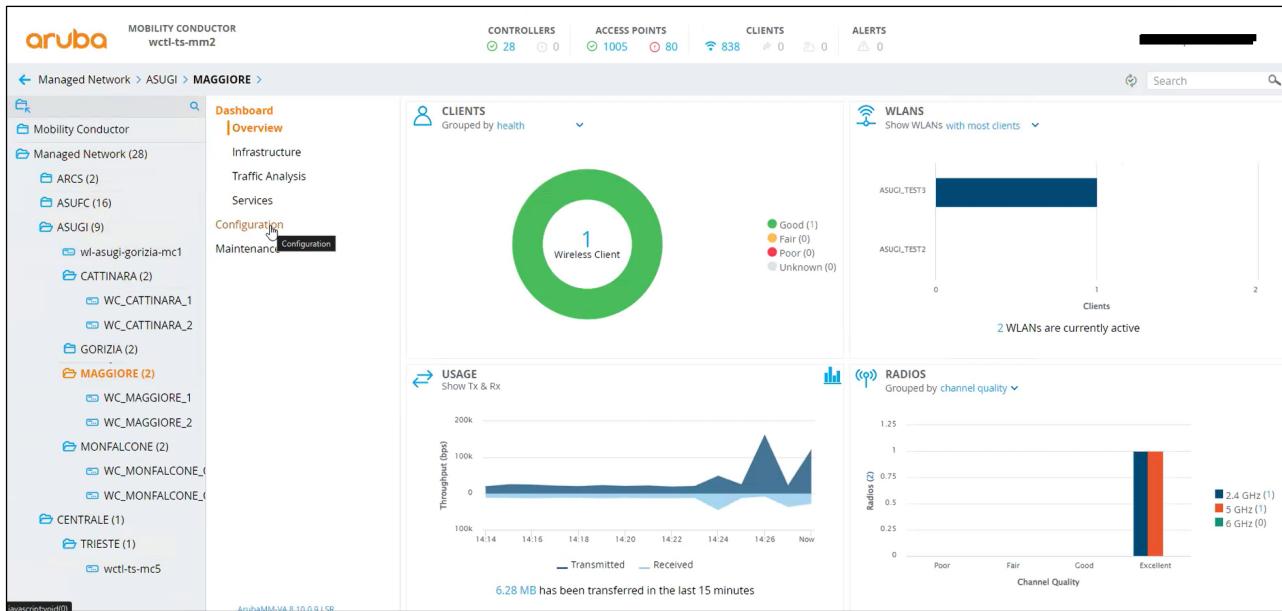
**IO\_XX\_00\_XX**

Pagina 10 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

Andando a selezionare sulla sinistra uno specifico sito, ad esempio 'ASUGI>MAGGIORE' verranno visualizzati nella schermata principale unicamente i dati statistici relativi al sito selezionato:



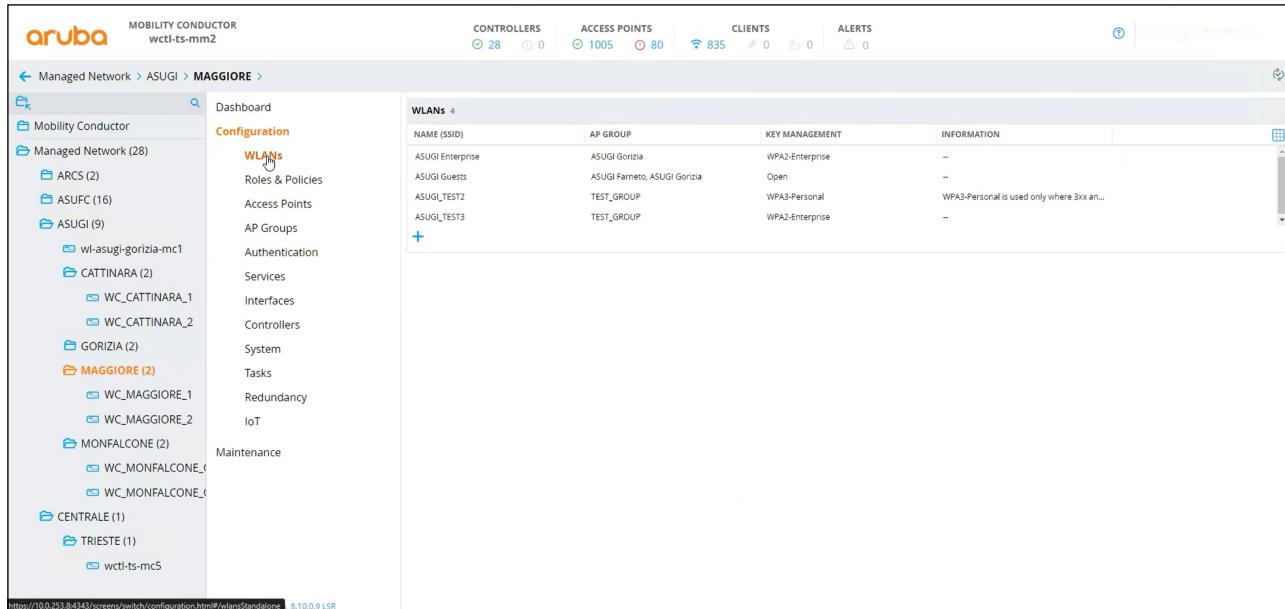
**Figura 6 - Dati statistici relativi ad uno specifico sito**

Nell'header saranno sempre visibili i dati complessivi dell'infrastruttura.

### 5.1.3. CONFIGURAZIONE ACCESS POINT

#### 5.1.3.1. WLAN

Dopo aver cliccato su ‘Configuration’ (vedi Fig.5) si avrà accesso al dettaglio della schermata di configurazione:



NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
ASUGI Enterprise	ASUGI Gorizia	WPA2-Enterprise	--
ASUGI Guests	ASUGI Farinetto, ASUGI Gorizia	Open	--
ASUGI_TEST2	TEST_GROUP	WPA3-Personal	WPA3-Personal is used only where xxx an...
ASUGI_TEST3	TEST_GROUP	WPA2-Enterprise	--

**Figura 7 – Configuration - Dettaglio**

Sotto il nodo ‘Configuration’ verranno mostrati una serie di sotto nodi contenenti i dettagli della configurazione stessa. Come default verrà mostrato il nodo WLAN che riporta l’elenco delle WLAN al momento disponibili relativamente ad ‘ASUGI’ (WLAN propagate in tutta l’infrastruttura), e specificamente a ‘MAGGIORE’ (WLAN presenti solo su questo sito) con alcuni dettagli:

- **NAME (SSID)**: nome della WLAN coincidente con lo SSID propagato.
- **AP GROUP**: gruppo di access point utilizzato.
- **KEY MANAGEMENT**: metodo crittografico utilizzato.
- **INFORMATION**: altre informazioni.

Selezionando una specifica WLAN si avrà accesso ai dettagli della stessa, selezionando gli appositi tab nella parte inferiore della griglia:

- **General**
- **VLANs**
- **Security**
- **Access**

Cliccando sul tasto  sarà possibile creare una nuova WLAN.



access point e terminali

**IO\_XX\_00\_XX**

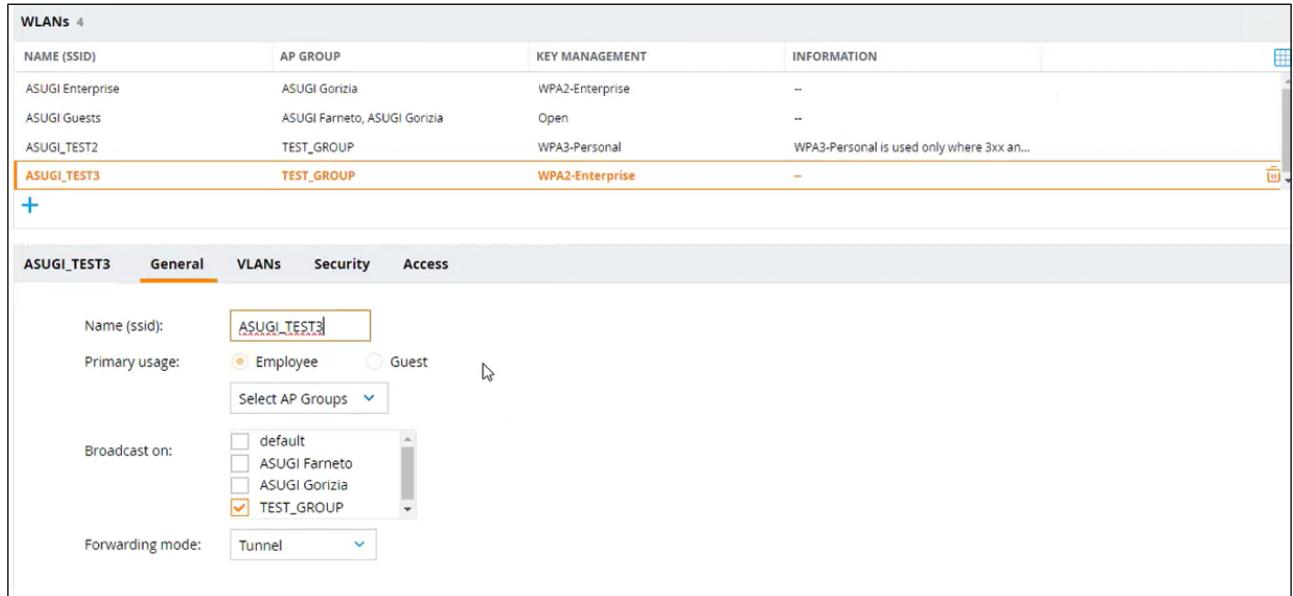
Pagina 12 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.1.1. DETTAGLIO WLAN - GENERAL

Selezionando il tab ‘General’ si avrà accesso a quanto segue:



WLANS 4			
NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
ASUGI Enterprise	ASUGI Gorizia	WPA2-Enterprise	--
ASUGI Guests	ASUGI Farneto, ASUGI Gorizia	Open	--
ASUGI_TEST2	TEST_GROUP	WPA3-Personal	WPA3-Personal is used only where 3xx an...
ASUGI_TEST3	TEST_GROUP	WPA2-Enterprise	--

**Figura 8 - Dettaglio WLAN**

Nello specifico:

- **Name (SSID):** ovvero lo SSID propagato dalla WLAN impostabile liberamente.
- **Primary usage:**
  - Employee.
  - Guest.
- **Broadcast on:** selettore gruppi access point (dettagliato in seguito), ovvero i gruppi di access point che genereranno la WLAN con lo SSID definito sopra.
- **Forwarding mode:** modalità di inoltro con tunnel per garantire la sicurezza ‘by design’ sulla VLAN dedicata per poi raggiungere i ‘Mobility Controller’.

access point e terminali

**IO\_XX\_00\_XX**

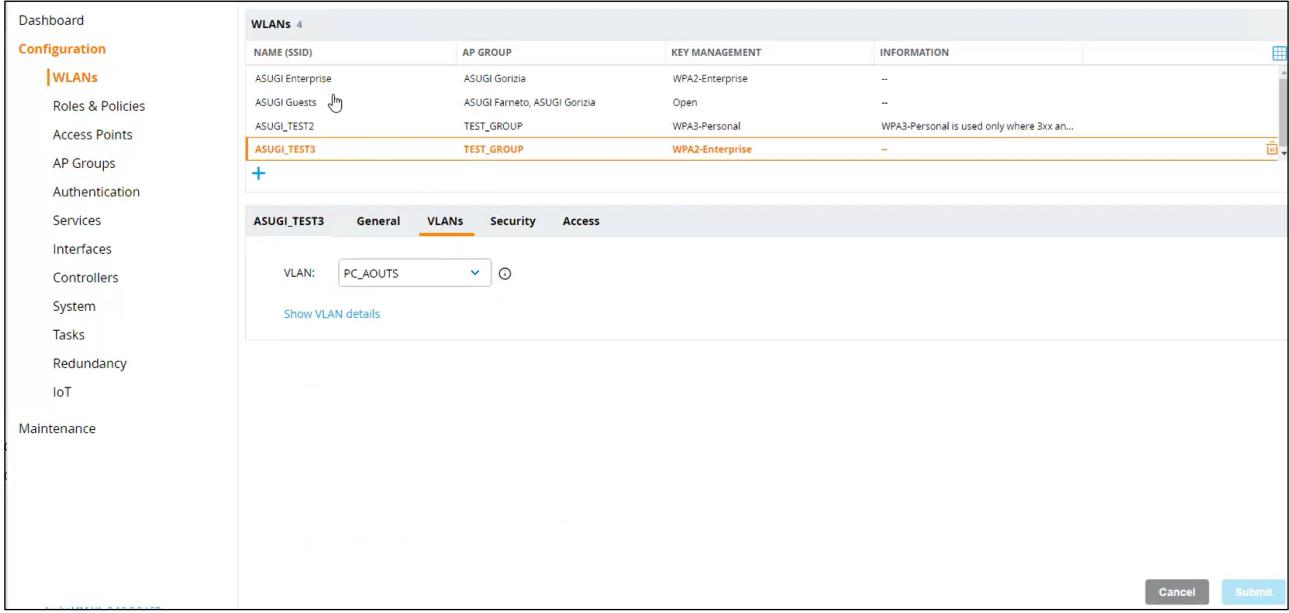
Pagina 13 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.1.2. DETTAGLIO WLAN – VLANS

Selezionando il tab ‘VLANS’ sarà possibile selezionare la VLAN cui afferiranno i client che si collegheranno alla WLAN selezionata:



NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
ASUGI Enterprise	ASUGI Gorizia	WPA2-Enterprise	--
ASUGI Guests	ASUGI Farneto, ASUGI Gorizia	Open	--
ASUGI_TEST2	TEST_GROUP	WPA3-Personal	WPA3-Personal is used only where 3xx an...
<b>ASUGI_TEST3</b>	<b>TEST_GROUP</b>	<b>WPA2-Enterprise</b>	--

**Figura 9 – Dettaglio VLANS**

Gli utenti collegati alla WLAN ‘ASUGI\_TEST3’, utilizzeranno quindi la VLAN ‘PC\_AOUTS’



access point e terminali

**IO\_XX\_00\_XX**

Pagina 14 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.1.3. DETTAGLIO WLAN – SECURITY

Selezionando il tab ‘Security’ si potrà accedere ai criteri di sicurezza per l’accesso alla WLAN:

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
ASUGI Enterprise	ASUGI Gorizia	WPA2-Enterprise	..
ASUGI Guests	ASUGI Farneto, ASUGI Gorizia	Open	..
ASUGI_TEST2	TEST_GROUP	WPA3-Personal	WPA3-Personal is used only where 3xx a...
ASUGI_TEST3	TEST_GROUP	WPA2-Enterprise	..

**Figura 10 - Dettaglio Security**

Dalla slide sulla destra sarà possibile selezionare le macrocategorie di sicurezza:

- **Enterprise**
- **Personal**
- **Open** (nessuna restrizione)

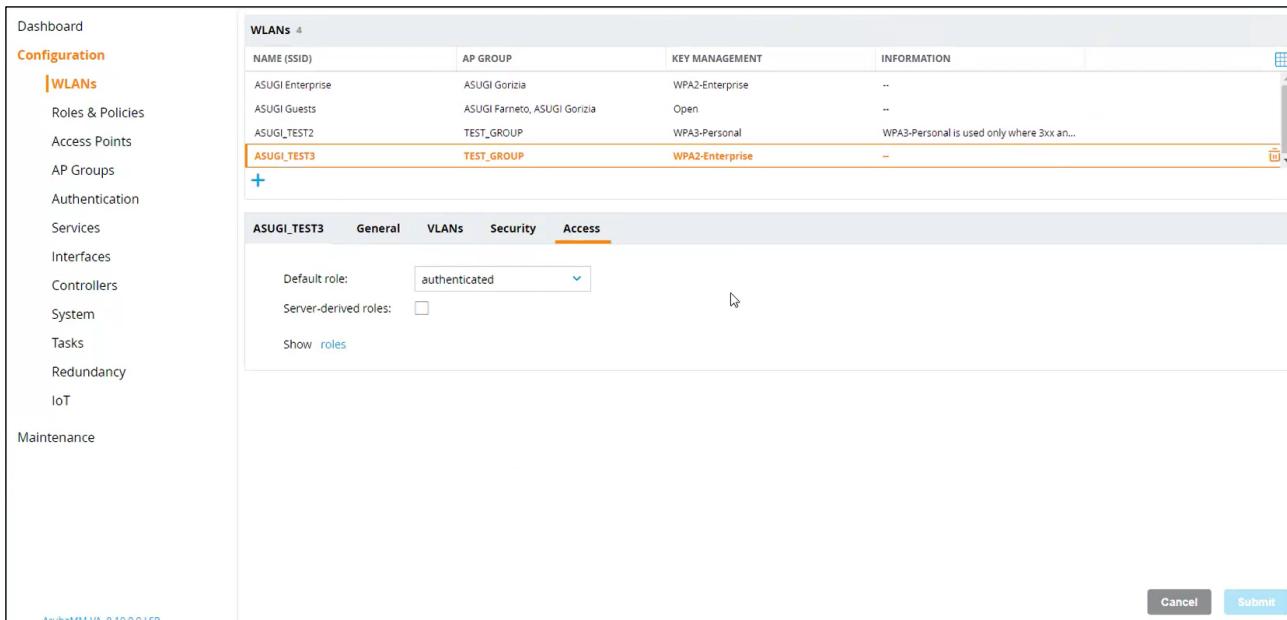
È stato ovviamente selezionato: ‘Enterprise’ ed i parametri disponibili saranno:

- **Key management:** il meccanismo di autenticazione, attualmente impostato su: ‘WPA2-Enterprise’
- **Auth servers:** l’elenco dei server RADIUS su cui effettuare l’autenticazione, attualmente è impostato un unico server: ‘0M0022’ (server RADIUS dell’Ospedale Maggiore). È possibile impostare più server di autenticazione.
- **Reauth interval:** l’intervallo di tempo entro il quale è richiesta una nuova autenticazione di un client già collegato, in questo caso impostato su 86400 sec.
- **Machine authentication:** impostato su ‘Disabled’. Se impostato su ‘Enabled’ può creare anomalie.
- **Denylisting:** la black list dei client, cui viene impedito il collegamento alla WLAN, funzionalità al momento disabilitata.



#### 5.1.3.1.4. DETTAGLIO WLAN – ACCESS

Selezionando il tab ‘Access’, si potrà accedere all’elenco dei ruoli da assegnare agli utenti autenticati:



WLANS 4				
NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION	
ASUGI Enterprise	ASUGI Gorizia	WPA2-Enterprise	--	
ASUGI Guests	ASUGI Farneto, ASUGI Gorizia	Open	--	
ASUGI_TEST2	TEST_GROUP	WPA3-Personal	WPA3-Personal is used only where 3xx an...	
<b>ASUGI_TEST3</b>	<b>TEST_GROUP</b>	<b>WPA2-Enterprise</b>	--	

**ASUGI\_TEST3** General VLANs Security **Access**

Default role: **authenticated**

Server-derived roles:

Show [roles](#)

Cancel Submit

**Figura 11 – Dettaglio Access**

Nello specifico agli utenti autenticati verrà attribuito il ruolo ‘Authenticated’, ovvero dopo aver effettuato l’autenticazione sul server RADIUS all’utente verrà attribuito tale ruolo che è gestito dal firewall interno del Wireless Controller.

#### NOTA BENE:

- Il ruolo ‘Authenticated’ permette una operatività abbastanza completa all’utente.



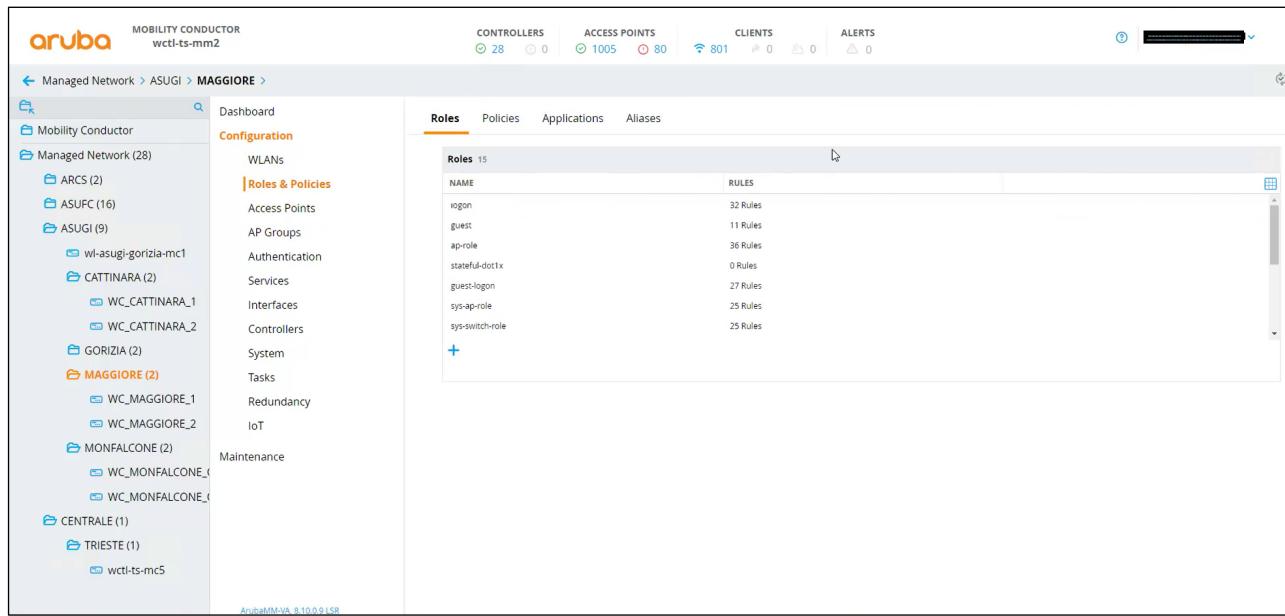
access point e terminali

**IO\_XX\_00\_XX**

Pagina 16 di 51

## ISTRUZIONE OPERATIVA

14/10/2024



The screenshot shows the Aruba Mobility Conductor interface with the following details:

- Top Bar:** MOBILITY CONDUCTOR wctl-ts-mm2
- Header:** Configurazione
- Metrics:** CONTROLLERS (28), ACCESS POINTS (1005), CLIENTS (801), ALERTS (0)
- Breadcrumbs:** Managed Network > ASUGI > MAGGIORE >
- Left Sidebar:**
  - Mobility Conductor
  - Managed Network (28)
    - ARCS (2)
    - ASUFC (16)
    - ASUGI (9)**
      - wl-asugi-gorizia-mc1
      - CATTINARA (2)
        - WC\_CATTINARA\_1
        - WC\_CATTINARA\_2
      - GORIZIA (2)
      - MAGGIORE (2)**
        - WC\_MAGGIRORE\_1
        - WC\_MAGGIRORE\_2
      - MONFALCONE (2)
        - WC\_MONFALCONE\_1
        - WC\_MONFALCONE\_2
      - CENTRALE (1)
      - TRIESTE (1)
        - wctl-ts-mc5
- Right Panel:**
  - Roles** tab (selected): Shows 15 roles with their respective rule counts:
 

NAME	RULES
logon	32 Rules
guest	11 Rules
ap-role	36 Rules
stateful-dot1x	0 Rules
guest-logon	27 Rules
sys-ap-role	25 Rules
sys-switch-role	25 Rules
  - Policies
  - Applications
  - Aliases

**Figura 12 - Roles & Policies**

Sono disponibili quattro tab:

- **Roles**
- **Policies**
- **Applications**
- **Aliases**

### NOTA BENE:

- In questi pannelli non deve essere applicata nessuna modifica.



access point e terminali

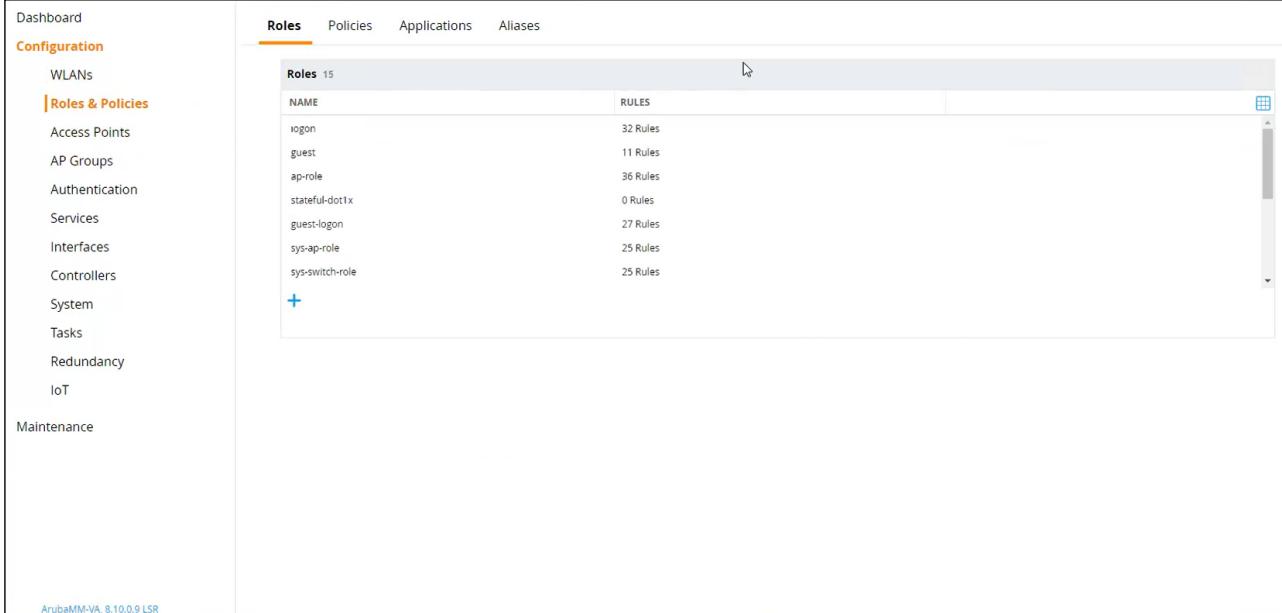
**IO\_XX\_00\_XX**

Pagina 17 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

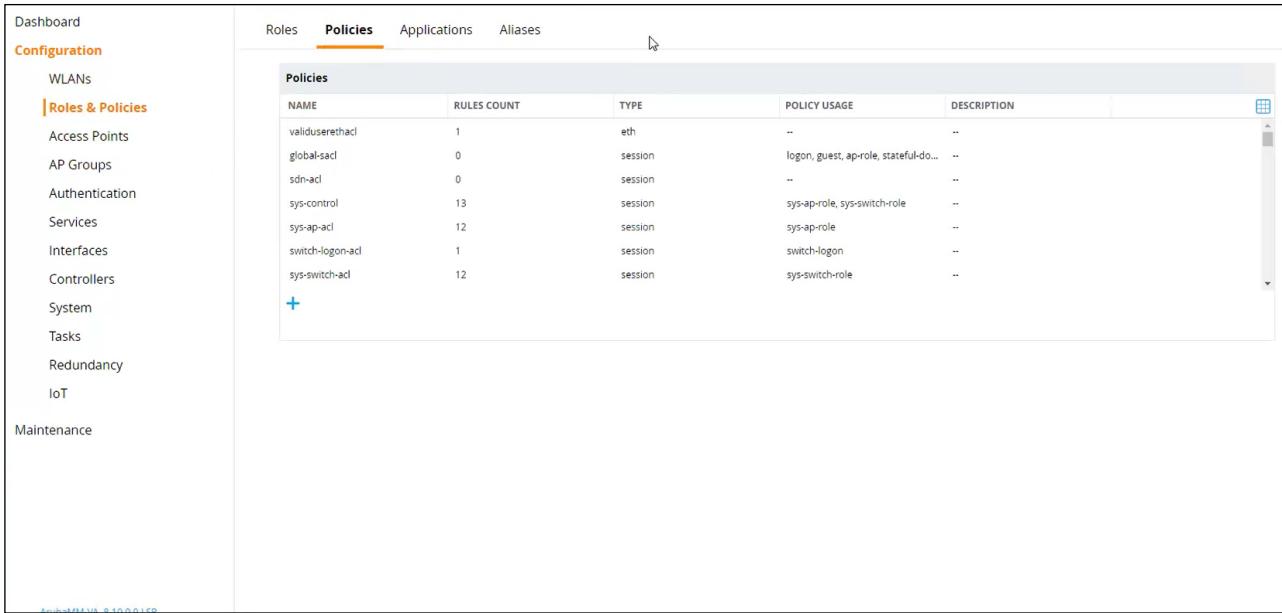
### 5.1.3.2.1. DETTAGLIO ROLES & POLICIES - ROLES



NAME	RULES
logon	32 Rules
guest	11 Rules
ap-role	36 Rules
stateful-dot1x	0 Rules
guest-logon	27 Rules
sys-ap-role	25 Rules
sys-switch-role	25 Rules

**Figura 13 – Dettaglio Roles**

### 5.1.3.2.2. DETTAGLIO ROLES & POLICIES - POLICIES



NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
validuserethacl	1	eth	..	..
global-sadl	0	session	logon, guest, ap-role, stateful-dot1x	..
sdrn-acl	0	session	..	..
sys-control	13	session	sys-ap-role, sys-switch-role	..
sys-ap-acl	12	session	sys-ap-role	..
switch-logon-acl	1	session	switch-logon	..
sys-switch-acl	12	session	sys-switch-role	..

**Figura 14 – Dettaglio Policies**



access point e terminali

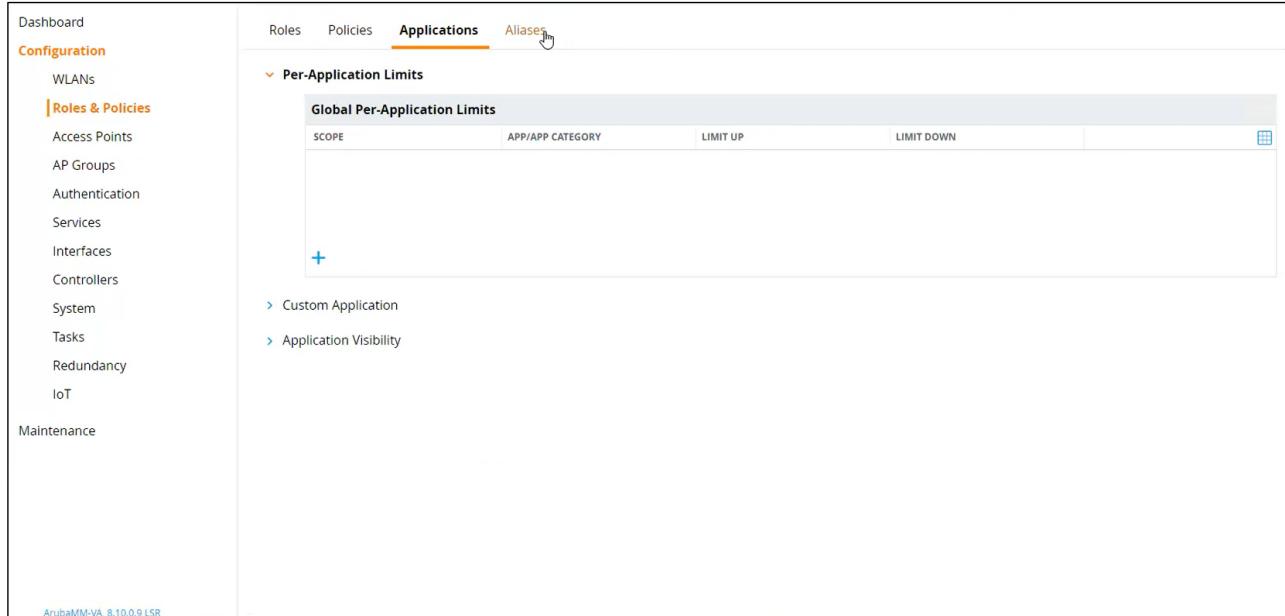
**IO\_XX\_00\_XX**

Pagina 18 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.2.3. DETTAGLIO ROLES & POLICIES - APPLICATIONS



Dashboard

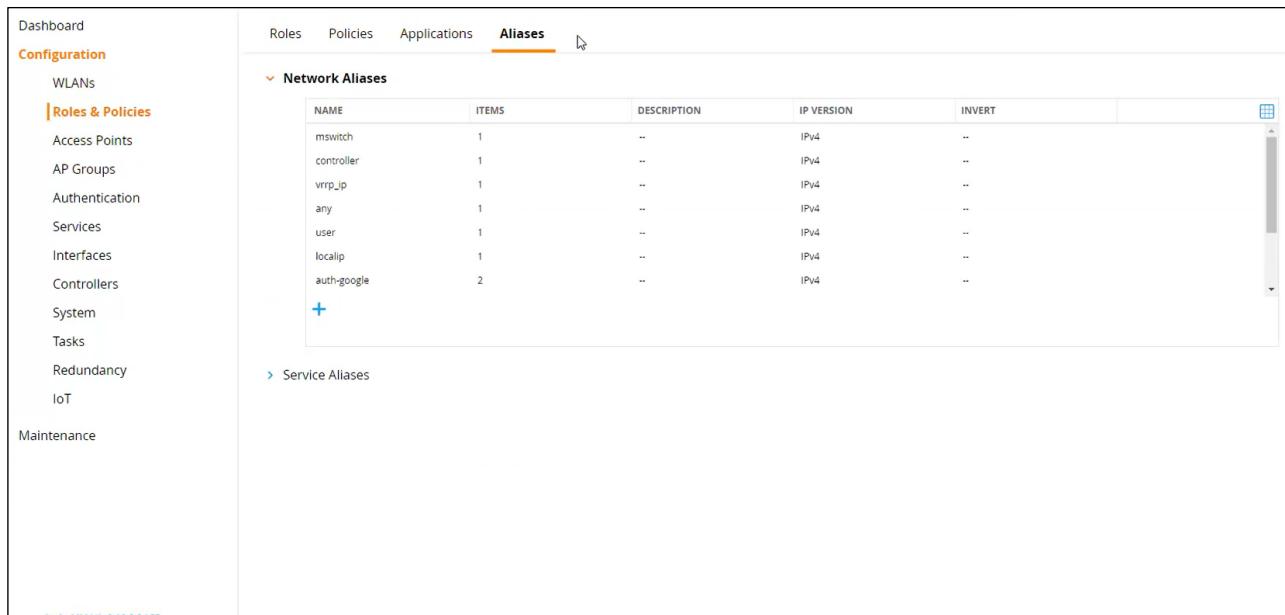
**Configuration**

- WLANs
- Roles & Policies**
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks
- Redundancy
- IoT
- Maintenance

AnubisMMVA\_8.10.0.9\_LCR

**Figura 15 – Dettaglio Applications**

### 5.1.3.2.4. DETTAGLIO ROLES & POLICIES - ALIASES



Dashboard

**Configuration**

- WLANs
- Roles & Policies**
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks
- Redundancy
- IoT
- Maintenance

AnubisMMVA\_8.10.0.9\_LCR

**Figura 16 - Dettaglio Aliases**



access point e terminali

**IO\_XX\_00\_XX**

Pagina 19 di 51

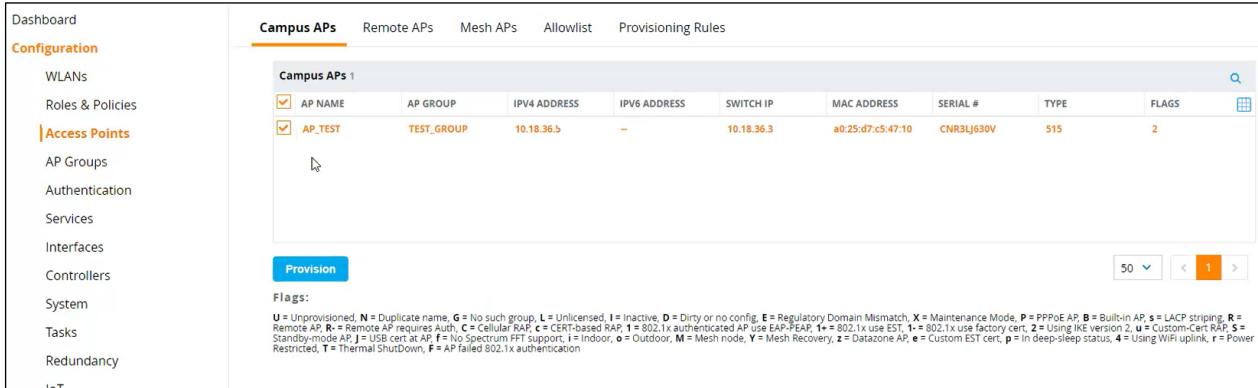
## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.3. ACCESS POINTS

Selezionando ‘Configuration>Access Points’ si avrà accesso all’elenco degli access point disponibili nell’infrastruttura, in pratica sono gli access point a presentarsi.

Verrà visualizzata la seguente schermata:



The screenshot shows the 'Campus APs' configuration page. On the left, there's a sidebar with various options like WLANs, Roles & Policies, Access Points (which is selected and highlighted in orange), AP Groups, Authentication, Services, Interfaces, Controllers, System, Tasks, Redundancy, and IoT. The main area has tabs for Campus APs, Remote APs, Mesh APs, Allowlist, and Provisioning Rules. Under 'Campus APs', there's a table titled 'Campus APs 1' with one row for 'AP\_TEST'. The columns in the table are: AP NAME, AP GROUP, IPV4 ADDRESS, IPV6 ADDRESS, SWITCH IP, MAC ADDRESS, SERIAL #, TYPE, and FLAGS. The data for 'AP\_TEST' is: AP\_NAME (AP\_TEST), AP\_GROUP (TEST\_GROUP), IPV4\_ADDRESS (10.18.36.5), IPV6\_ADDRESS (none), SWITCH\_IP (10.18.36.3), MAC\_ADDRESS (a0:25:d7:c5:47:10), SERIAL\_# (CNR3LJ630V), TYPE (515), and FLAGS (2). Below the table is a 'Provision' button. At the bottom of the page, there's a 'Flags:' section with a detailed legend explaining various abbreviations used in the table.

**Figura 17 - Elenco access point**

L’elenco mostra gli access point configurati, per ogni access point saranno disponibili le seguenti informazioni:

- **AP NAME:** nome access point: AP\_TEST
- **AP GROUP:** nome gruppo access point (se assegnato): TEST\_GROUP
- **IPV4 ADDRESS:** indirizzo IPv4: 10.18.36.5 (ottenuto tramite DHCP)
- **IPV6 ADDRESS:** indirizzo IPv6: nessuno
- **SWITCH IP:** 10.18.36.3, VIP del cluster di wireless Controller di riferimento.
- **MAC ADDRESS:** indirizzo fisico: a0:25:d7:c5:47:10
- **TYPE:** 515, ovvero il modello dell’apparato
- **SERIAL NUMBER:** CNR3LJ630V, ovvero il seriale dell’apparato
- **FLAGS:** fornisce varie informazioni dettagliate sotto la griglia.

Selezionando un access point si avrà accesso ad una serie di tab che forniranno informazioni di dettaglio sullo stesso, ovvero:

- **Campus APs**
- **Remote APs**
- **Mesh APs**
- **Allowlist**
- **Provisioning Rules**

Cliccando sul tasto **Provision** si potrà configurare l’access selezionato, che si è annunciato, pertanto è visualizzato, ma non ancora configurato.

#### 5.1.3.3.1. DETTAGLIO ACCES POINTS – CAMPUS APs

Il tab ‘Campus APs’ consente la configurazione del singolo access point dopo il provisioning dello stesso:



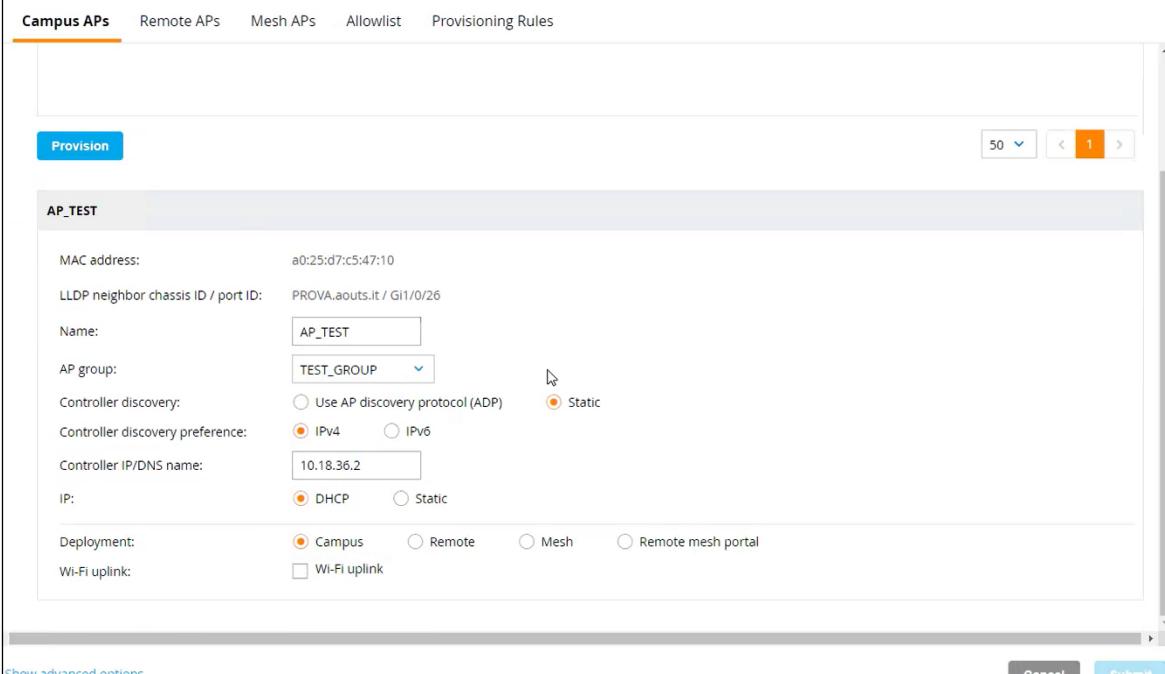
access point e terminali

**IO\_XX\_00\_XX**

Pagina 20 di 51

### ISTRUZIONE OPERATIVA

14/10/2024



**Campus APs**    Remote APs    Mesh APs    Allowlist    Provisioning Rules

**AP\_TEST**

MAC address: a0:25:d7:c5:47:10

LLDP neighbor chassis ID / port ID: PROVA.aouts.it / Gi1/0/26

Name:

AP group:  ▼

Controller discovery:  Use AP discovery protocol (ADP)  Static

Controller discovery preference:  IPv4  IPv6

Controller IP/DNS name:

IP:  DHCP  Static

Deployment:  Campus  Remote  Mesh  Remote mesh portal

Wi-Fi uplink:

Show advanced options

**Cancel** **Submit**

**Figura 18 - Dettaglio access point**

Sono disponibili varie informazioni:

- **MAC address:** indirizzo fisico dell'access point.
- **LLDP neighbor chassis IP / port ID:** protocollo per la gestione di varie funzionalità di rete.
- **Name:** nome dell'access point.
- **AP Group:** gruppo di access point di appartenenza.
- **Controller discovery:** modalità di accesso al 'Wireless Controller':
  - AP Discovery Protocol (ADP).
  - Static.
- **Controller discovery preference:** modalità di indirizzamento per il 'Wireless Controller':
  - IPv4.
  - IPv6.
- **Controller IP/DNS name:** indirizzo del 'Wireless Controller'.
- **IP:** indirizzo dell'access point:
  - DHCP.
  - Static.
- **Deployment:** modalità di utilizzo:
  - Campus.
  - Remote.
  - Mesh.
  - Remote mesh portal.
- **Wi-Fi uplink:**
  - Yes.
  - No.

Oltre alle varie opzioni di configurazione disponibili, è da notare come ivi sia possibile assegnare uno specifico access point ad uno specifico AP Group.

access point e terminali

**IO\_XX\_00\_XX**

Pagina 21 di 51

ISTRUZIONE OPERATIVA

14/10/2024

**NOTA BENE:**

- Gli access point devono essere sulla VLAN 11 dedicata al management degli stessi.
- Sulla VLAN 11 nell'Ospedale Maggiore, è stato creato uno scope DHCP che rilascia l'indirizzo IP del wireless Controller di appartenenza e gli IP degli access point.
- L'IP 10.18.36.2 del wireless Controller, è in realtà un VIP, poiché i wireless Controller sono due, configurati in modalità 'alta affidabilità'.



access point e terminali

**IO\_XX\_00\_XX**

Pagina 22 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.4. AP GROUPS

Selezionando ‘Configuration>AP Groups’ si avrà accesso all’elenco dei gruppi di access point, verrà visualizzata la seguente schermata:



NAME	APs
ASUGI Gorizia	..
default	..
NoAuthApGroup	..
<b>TEST_GROUP</b>	1
<b>+ </b>	

AP Groups > TEST_GROUP	APs	WLANs	Radio	Mesh	LMS	MultiZone	IoT
NAME	IPV4 ADDRESS	IPV6 ADDRESS	MAC ADDRESS	TYPE	SERIAL #	PER AP OVERRIDE	
AP_TEST	10.18.36.5	..	a0:25:d7:c5:47:10	515	CNR3LJ630V	No	

**Figura 19 – Elenco AP Groups**

Nella parte superiore della griglia verranno mostrate le seguenti informazioni:

- **NAME:** denominazione del gruppo di access point.
- **APs:** numero di access point configurati per lo specifico gruppo di access point.

Selezionando un singolo ‘AP Group’ si avrà accesso ad una serie di tab che forniranno informazioni di dettaglio sullo stesso, ovvero:

- **APs**
- **WLANs**
- **Radio**
- **Mesh**
- **LMS**
- **MultiZone**
- **IoT**

Cliccando sul tasto sarà possibile creare un nuovo ‘AP Group’.

#### 5.1.3.4.1. DETTAGLIO AP GROUPS - APS

Selezionando ad esempio ‘TEST\_GROUP’ si avrà accesso ai dettagli di uno specifico ‘AP Group’, ovvero ad un gruppo di singoli access point, nel caso specifico di tale gruppo fa parte un unico access point.

Nella griglia sottostante verranno mostrate le seguenti informazioni:

- **NAME:** il nome dell’access point, in questo caso: AP\_TEST.
- **IPV4 ADDRESS:** l’indirizzo IPv4, in questo caso: 10.18.36.5 (ottenuto tramite DHCP).
- **IPV6 ADDRESS:** l’indirizzo IPv6, in tal caso non assegnato.
- **MAC ADDRESS:** l’indirizzo fisico dell’access point, in tal caso: a0:25:d7:c5:47:10
- **TYPE:** il modello dell’access point, in questo caso 515
- **SERIAL NUMBER:** il numero seriale dell’access point, in tal caso: CNR3LJ630V
- **PER AP OVERRIDE:** No

access point e terminali

**IO\_XX\_00\_XX**

Pagina 23 di 51

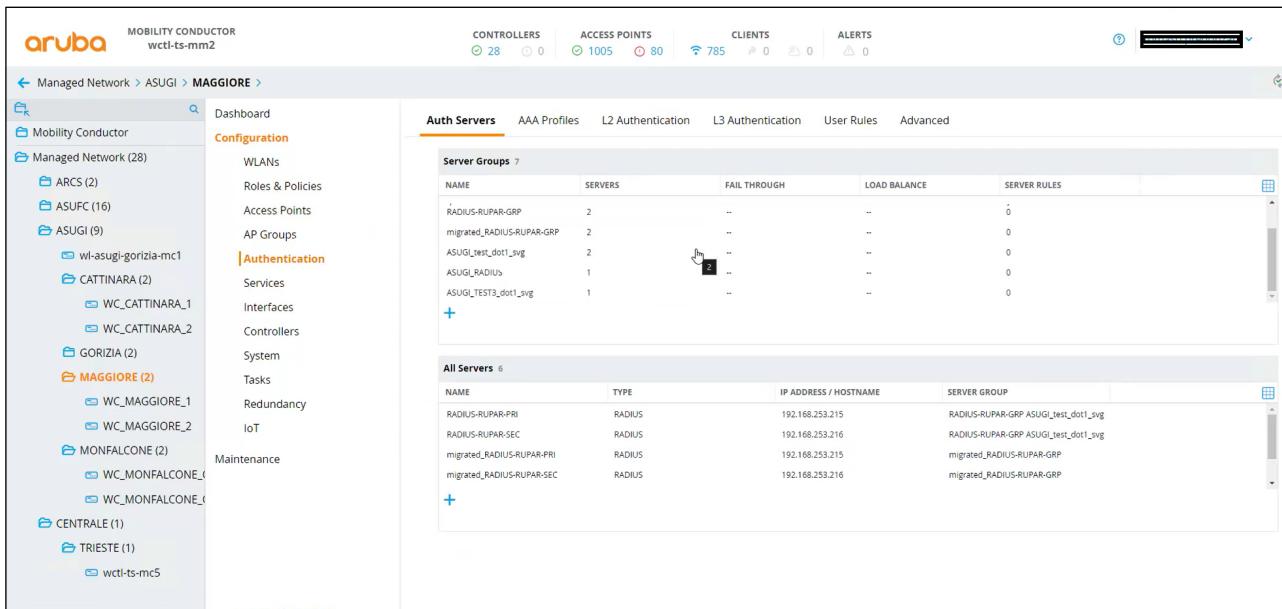
**ISTRUZIONE OPERATIVA**

14/10/2024

In teoria non ci sono vincoli specifici nell'associazione di access point ad uno specifico gruppo; tuttavia, per quanto possibile è preferibile raggrupparli secondo criteri geografici.

**5.1.3.5. AUTHENTICATION**

Selezionando il nodo 'Configuration > Authentication' si avrà accesso alle funzionalità di gestione dei server di autenticazione (RADIUS):



NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
RADIUS-RUPAR-GRP	2	--	--	0
migrated_RADIUS-RUPAR-GRP	2	--	--	0
ASUGI_test_dot1_svg	2	--	--	0
ASUGI_RADIUS	1	--	--	0
ASUGI_TEST3_dot1_svg	1	--	--	0

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
RADIUS-RUPAR-PRI	RADIUS	192.168.253.215	RADIUS-RUPAR-GRP ASUGI_test_dot1_svg
RADIUS-RUPAR-SEC	RADIUS	192.168.253.216	RADIUS-RUPAR-GRP ASUGI_test_dot1_svg
migrated_RADIUS-RUPAR-PRI	RADIUS	192.168.253.215	migrated_RADIUS-RUPAR-GRP
migrated_RADIUS-RUPAR-SEC	RADIUS	192.168.253.216	migrated_RADIUS-RUPAR-GRP

**Figura 20 – Authentication**

Sono disponibili i seguenti tab:

- **Auth Servers**
- **AAA Profiles**
- **L2 Authentication**
- **L3 Authentication**
- **User Rules**
- **Advanced**



access point e terminali

**IO\_XX\_00\_XX**

Pagina 24 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.5.1. DETTAGLIO AUTH SERVERS

Selezionando il tab ‘Auth Servers’ si accede alla configurazione dei server di autenticazione:

Server Groups 7				
NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
RADIUS-RUPAR-GRP	2	--	--	0
migrated_RADIUS-RUPAR-GRP	2	--	--	0
ASUGI_test_dot1_svg	2	--	--	0
ASUGI_RADIUS	1	--	--	0
ASUGI_TEST3_dot1_svg	1	--	--	0

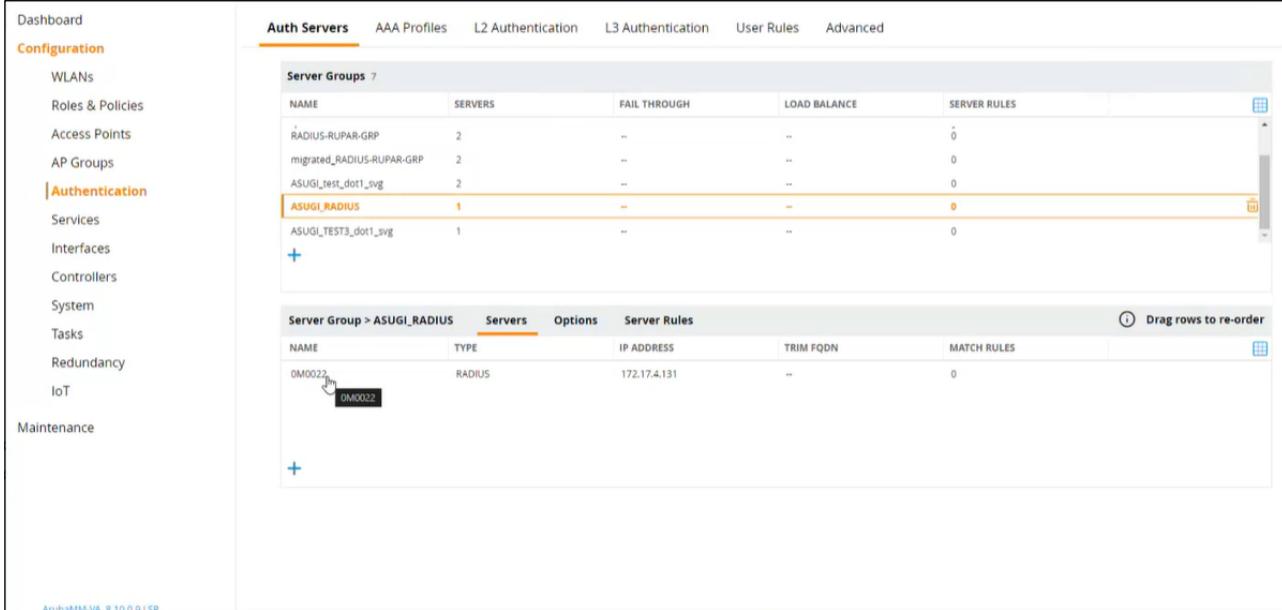
All Servers 6			
NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
RADIUS-RUPAR-PRI	RADIUS	192.168.253.215	RADIUS-RUPAR-GRP ASUGI_test_dot1_svg
RADIUS-RUPAR-SEC	RADIUS	192.168.253.216	RADIUS-RUPAR-GRP ASUGI_test_dot1_svg
migrated_RADIUS-RUPAR-PRI	RADIUS	192.168.253.215	migrated_RADIUS-RUPAR-GRP
migrated_RADIUS-RUPAR-SEC	RADIUS	192.168.253.216	migrated_RADIUS-RUPAR-GRP

**Figura 21 - Dettaglio Auth Servers**

Nella griglia inferiore sono visualizzati tutti i server di autenticazione di ASUGI, è possibile aggiungere un nuovo server cliccando sul tasto (inferiore).

Nella griglia superiore sono visualizzati i gruppi di server di autenticazione, ottenuti associando i singoli server di autenticazione riportati nella griglia inferiore. Per creare un nuovo gruppo è necessario cliccare sul tasto (superiore).

Selezionando un gruppo di server nella griglia superiore, sarà possibile, nella griglia inferiore, visualizzare i server RADIUS afferenti a quel gruppo:



NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
RADIUS-RUPAR-GRP	2	--	--	0
migrated_RADIUS-RUPAR-GRP	2	--	--	0
ASUGI_test_dot1_svg	2	--	--	0
<b>ASUGI_RADIUS</b>	<b>1</b>	<b>--</b>	<b>--</b>	<b>0</b>
ASUGI_TEST3_dot1_svg	1	--	--	0

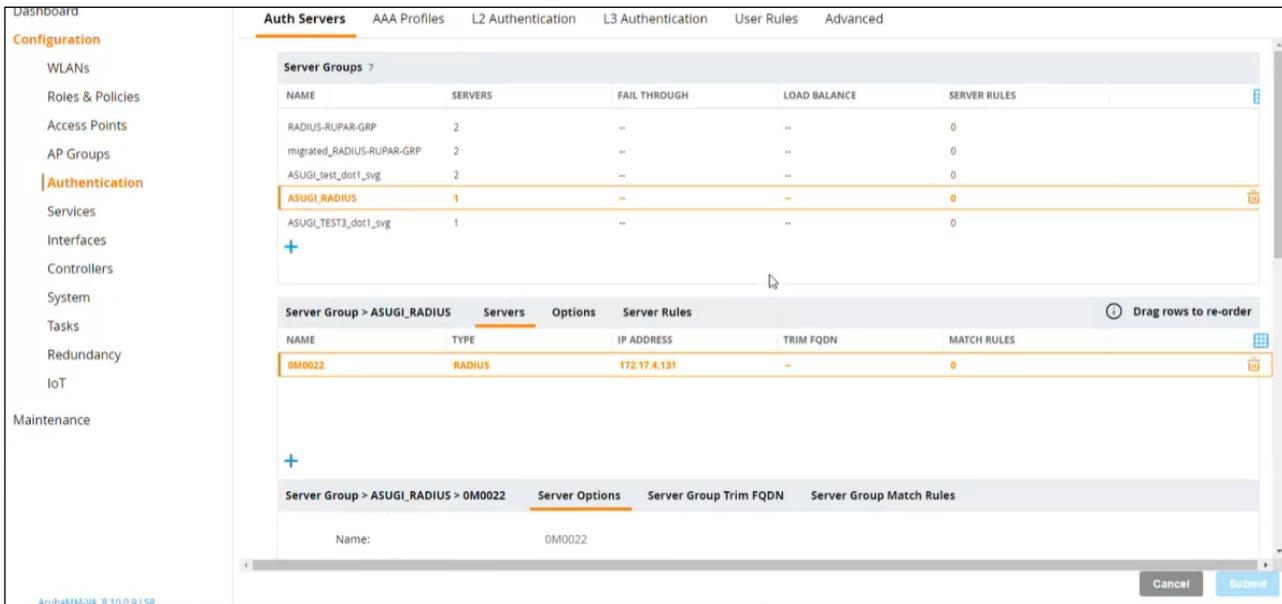
NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
OM0022	RADIUS	172.17.4.131	--	0

**Figura 22 - Dettagli server group – Tab servers**

Nella griglia inferiore sono presenti tre tab:

- **Servers** (mostrato di default)
- **Options**
- **Server rules**

Cliccando sul nome del server nella griglia inferiore, sia avrà accesso al dettaglio dello stesso:



NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
OM0022	RADIUS	172.17.4.131	--	0

Server Group > ASUGI_RADIUS > OM0022		Server Options	Server Group Trim FQDN	Server Group Match Rules
Name:	OM0022			

**Figura 23 - Dettaglio server RADIUS - 1**

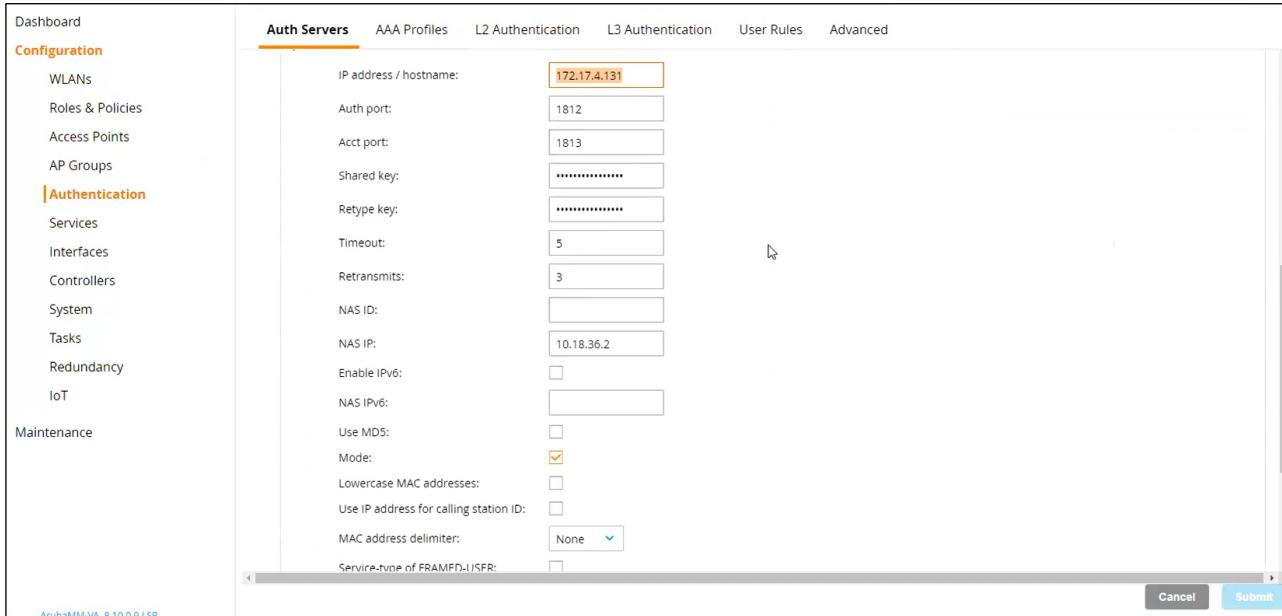
access point e terminali

**IO\_XX\_00\_XX**

Pagina 26 di 51

**ISTRUZIONE OPERATIVA**

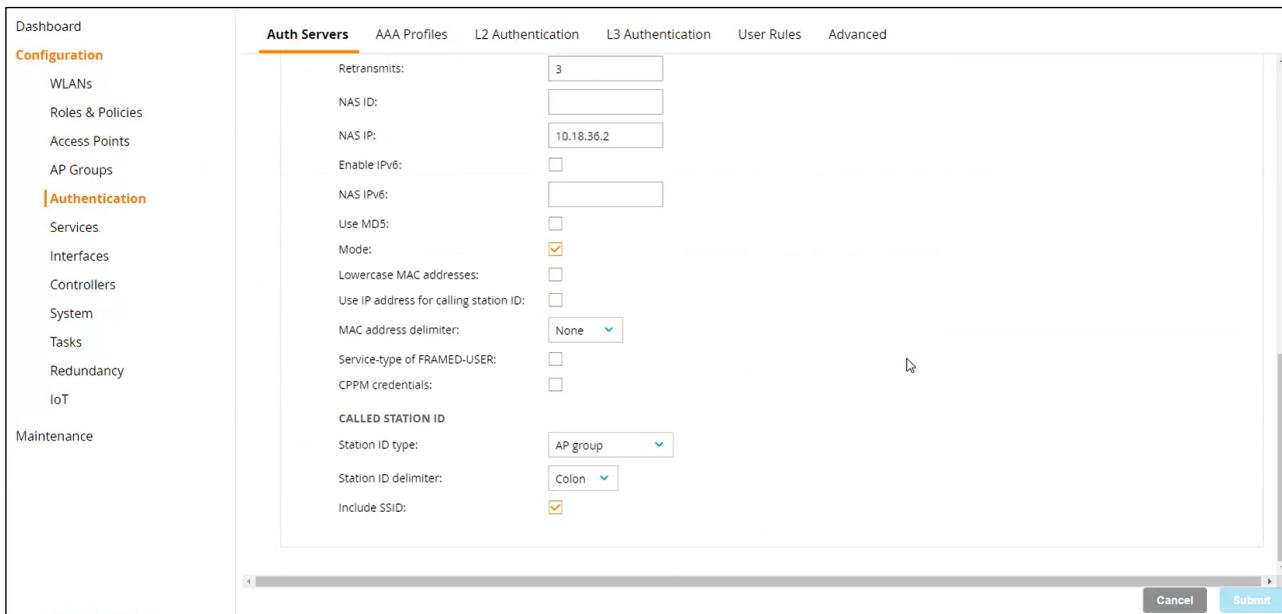
14/10/2024



The screenshot shows the Aruba configuration interface with the 'Auth Servers' tab selected under the 'Configuration' section. The 'Radius' tab is active. The configuration includes:

- IP address / hostname: 172.17.4.131
- Auth port: 1812
- Acct port: 1813
- Shared key: (redacted)
- Retype key: (redacted)
- Timeout: 5
- Retransmits: 3
- NAS ID: (redacted)
- NAS IP: 10.18.36.2
- Enable IPv6:
- NAS IPv6: (redacted)
- Use MD5:
- Mode:
- Lowercase MAC addresses:
- Use IP address for calling station ID:
- MAC address delimiter: None
- Service-type of FRAMED-USER: (redacted)

At the bottom right are 'Cancel' and 'Submit' buttons.

**Figura 24 - Dettaglio server RADIUS - 2**


The screenshot shows the Aruba configuration interface with the 'Auth Servers' tab selected under the 'Configuration' section. The 'Radius' tab is active. The configuration includes:

- Retransmits: 3
- NAS ID: (redacted)
- NAS IP: 10.18.36.2
- Enable IPv6:
- NAS IPv6: (redacted)
- Use MD5:
- Mode:
- Lowercase MAC addresses:
- Use IP address for calling station ID:
- MAC address delimiter: None
- Service-type of FRAMED-USER: (redacted)
- CPPM credentials: (redacted)
- CALLED STATION ID**
- Station ID type: AP group
- Station ID delimiter: Colon
- Include SSID:

At the bottom right are 'Cancel' and 'Submit' buttons.

**Figura 25 - Dettaglio server RADIUS - 3**

Si osservi come in questa griglia siano riportati tutti i riferimenti del server RADIUS, tra cui

- Indirizzo IP / Hostname
- Shared key
- Ecc.

access point e terminali

**IO\_XX\_00\_XX**

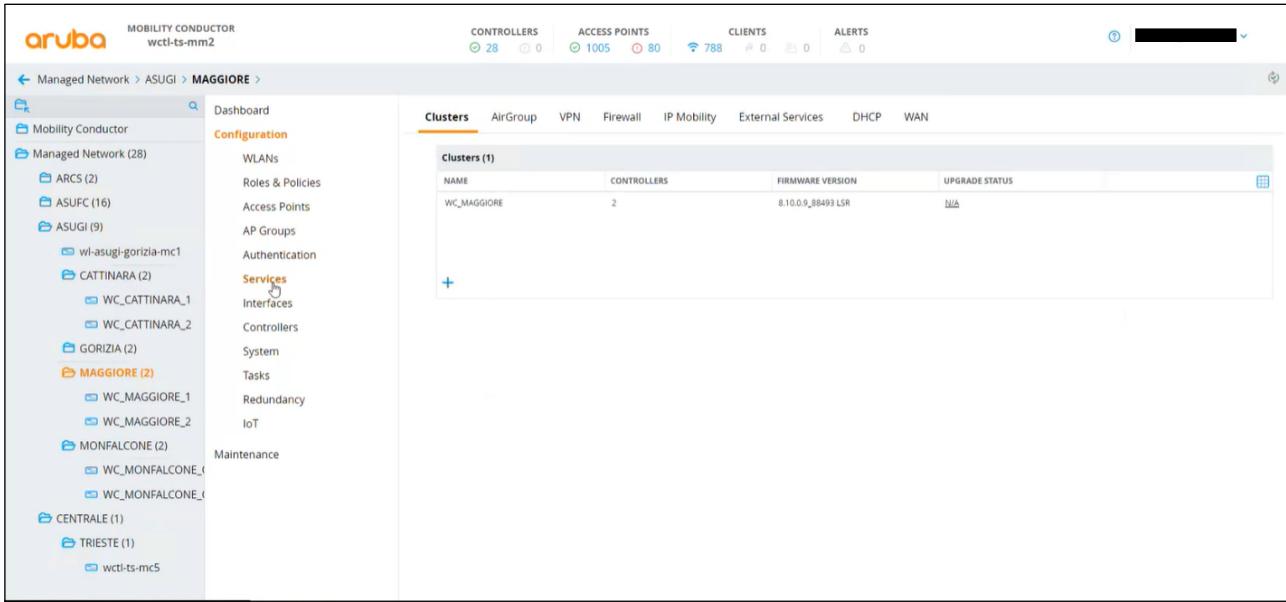
Pagina 27 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.6. SERVICES

Selezionando ‘Configuration>Service’ si avrà accesso ad ulteriori servizi del wireless Controller:



NAME	CONTROLLERS	FIRMWARE VERSION	UPGRADE STATUS
WC_MAGGIORE	2	8.10.0.9_88493 LSR	N/A

**Figura 26 – Services**

Nel dettaglio saranno disponibili i tab:

- **Clusters**
- **AirGroup**
- **VPN**
- **Firewall**
- **IP Mobility**
- **External Services**
- **DHCP**
- **WAN**

Il primo tab ‘Clusters’ fa riferimento ai cluster di wireless Controller, quello visibile nell’immagine si riferisce al wireless Controller dell’Ospedale Maggiore, strutturato, come si è già detto su due apparati configurati in alta affidabilità.



access point e terminali

**IO\_XX\_00\_XX**

Pagina 28 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

**Figura 27 - Interfaces**

Nel dettaglio saranno disponibili i tab:

- **Ports**
- **VLANs**
- **IP Routes**
- **GRE Tunnels**
- **Pool Management**
- **OSPF**
- **Multicast**

### NOTA BENE:

- Si osservi come in questi pannelli non è stata apportata alcuna modifica.

access point e terminali

**IO\_XX\_00\_XX**

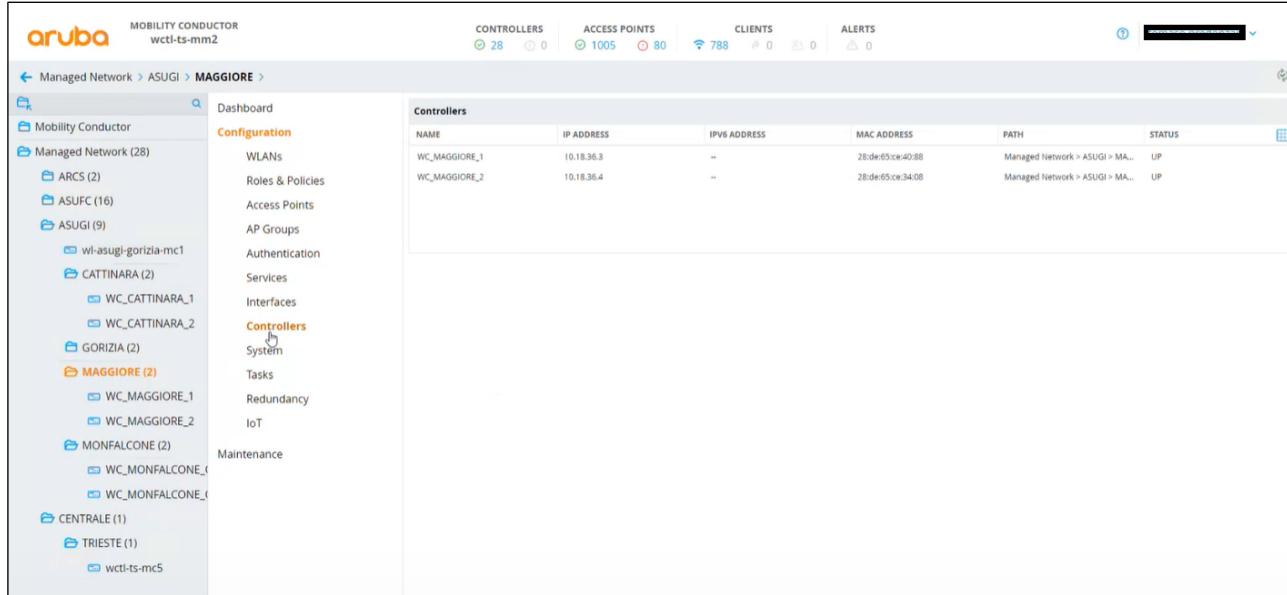
Pagina 29 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.8. CONTROLLERS

Selezionando ‘Configuration>Controllers’ si avrà accesso alle configurazioni dei wireless Controller per il nodo selezionato.

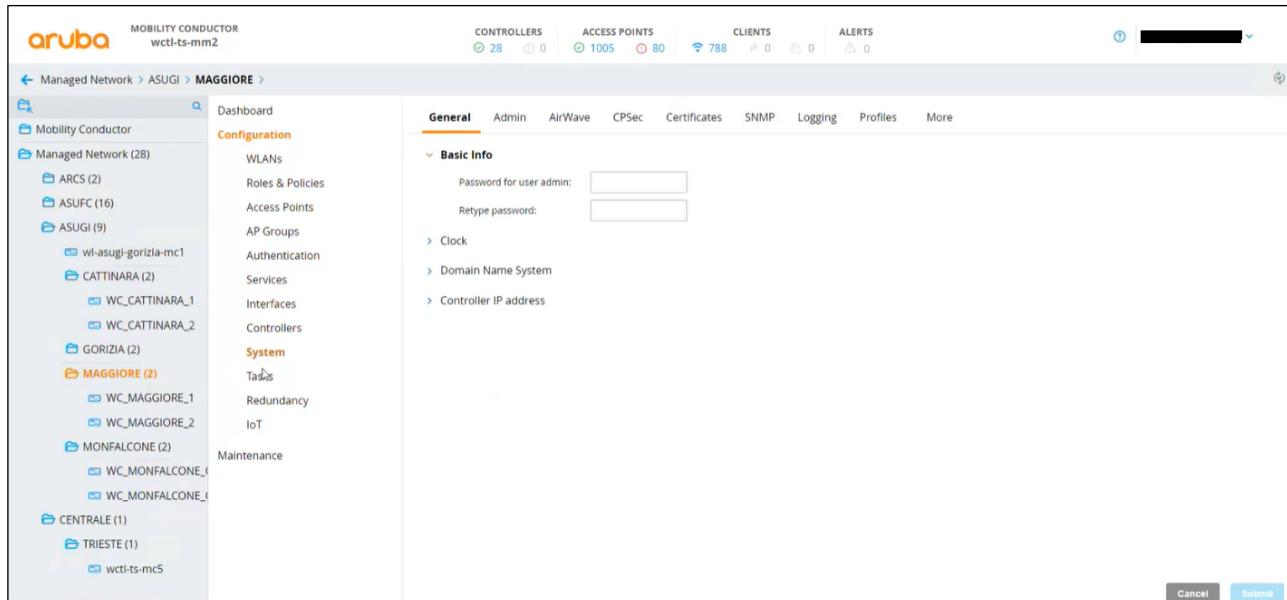


NAME	IP ADDRESS	IPV6 ADDRESS	MAC ADDRESS	PATH	STATUS
WC_MAGGIORE_1	10.18.36.3	--	28:de:65:ce:40:88	Managed Network > ASUGI > MA...	UP
WC_MAGGIORE_2	10.18.36.4	--	28:de:65:ce:34:08	Managed Network > ASUGI > MA...	UP

**Figura 28 - Controllers**

### 5.1.3.9. SYSTEM

Selezionando ‘Configuration>System’ si avrà accesso alle configurazioni di sistema.



**Figura 29 – System**

Saranno disponibili i seguenti tab:

- **General**
- **Admin**

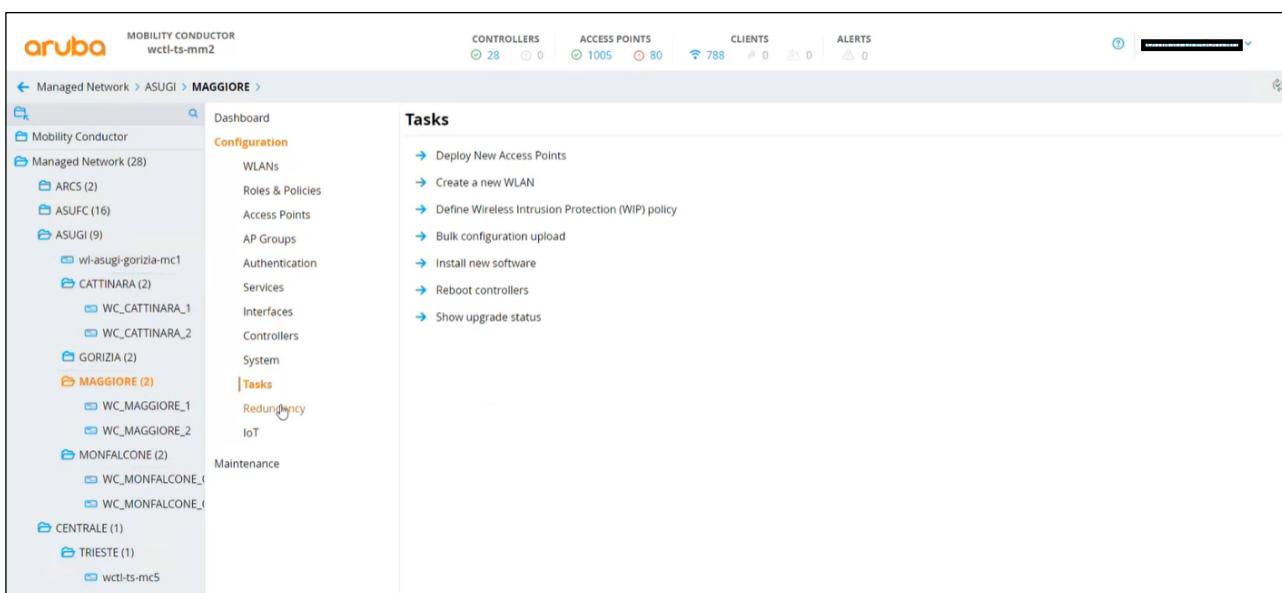
- **AirWave**
- **CPsec**
- **Certificates**
- **SNMP**
- **Logging**
- **Profiles**
- **More**

### NOTA BENE:

- A questi pannelli non deve essere apportata alcuna modifica.

#### 5.1.3.10. TASKS

Selezionando ‘Configuration>Tasks’ si avrà accesso ad una serie di wizard che consentono varie attività sul sistema:



The screenshot shows the Aruba Mobility Conductor interface. At the top, it displays 'MOBILITY CONDUCTOR wctl-ts-mm2' and various system statistics: CONTROLLERS (28), ACCESS POINTS (1005), CLIENTS (788), and ALERTS (0). The left sidebar shows a tree view of managed networks: ARCS (2), ASUFC (16), ASUGI (9), CATTINARA (2), GORIZIA (2), MAGGIORE (2), MONFALCONE (2), CENTRALE (1), and TRIESTE (1). The 'wctl-ts-mm2' controller is selected. The main content area is titled 'Tasks' and lists several configuration options:

- Deploy New Access Points
- Create a new WLAN
- Define Wireless Intrusion Protection (WIP) policy
- Bulk configuration upload
- Install new software
- Reboot controllers
- Show upgrade status

Figura 30 – Tasks

access point e terminali

**IO\_XX\_00\_XX**

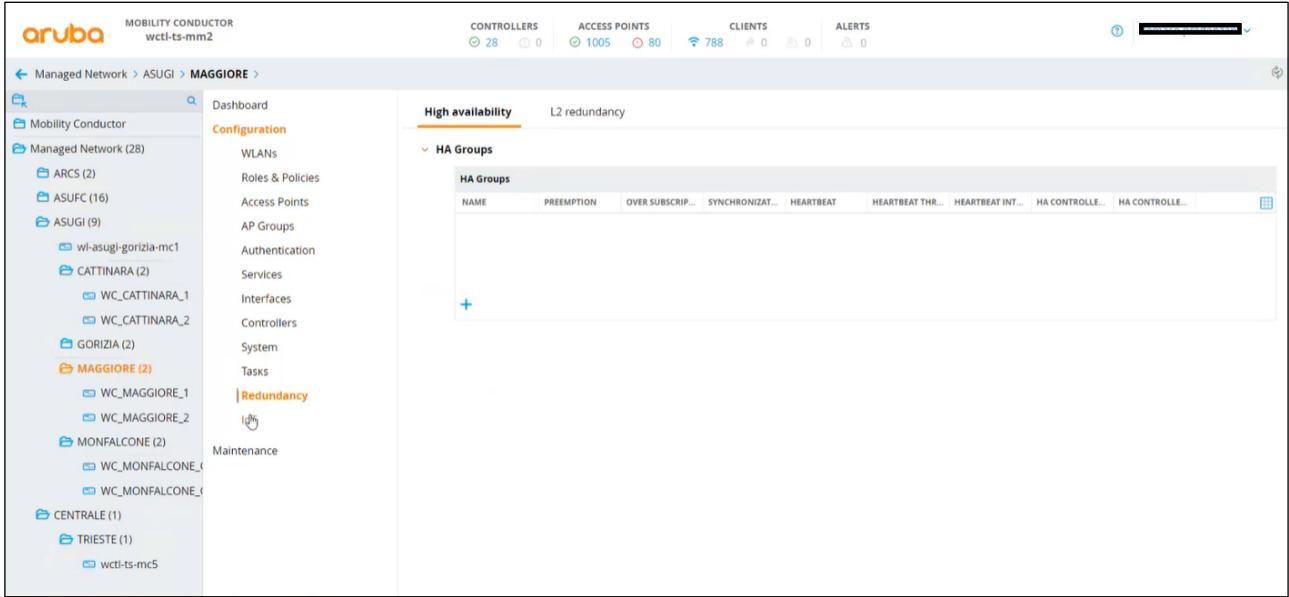
Pagina 31 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.1.3.11. REDUNDANCY

Selezionando ‘Configuration>Redundancy’ si avrà accesso alle funzionalità relative all’alta affidabilità:



**Figura 31 - Redundancy**

Sono disponibili due tab:

- **High availability**
- **L2 Redundancy**

### NOTA BENE:

- Si osservi come in questi pannelli non è stata apportata alcuna modifica.

access point e terminali

**IO\_XX\_00\_XX**

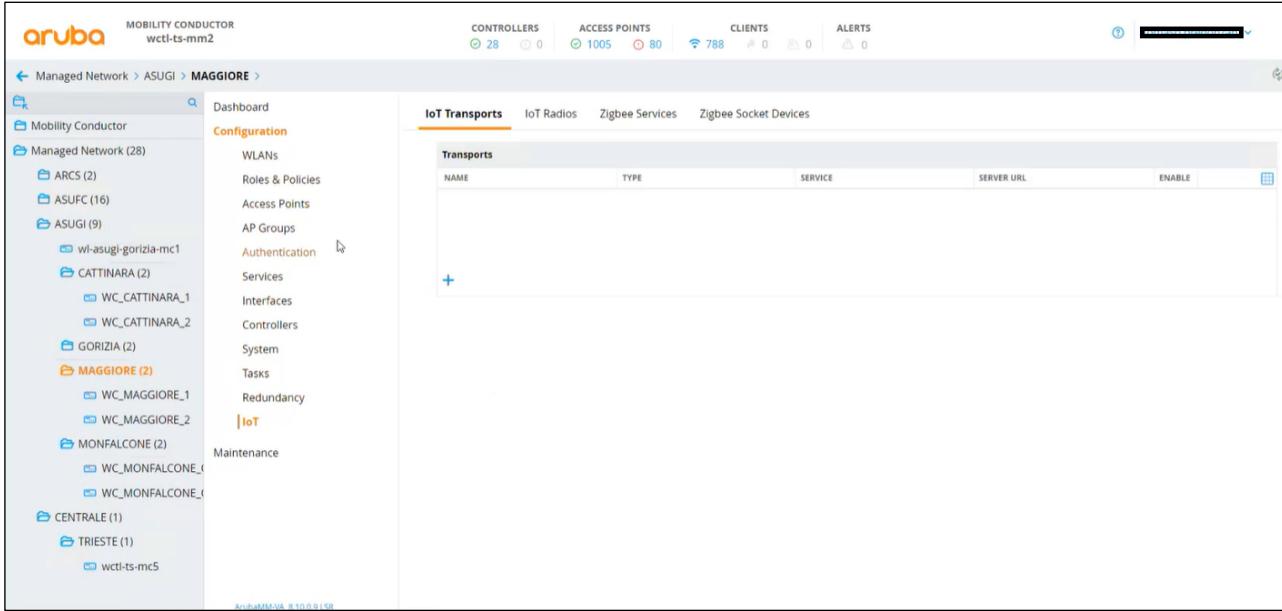
Pagina 32 di 51

ISTRUZIONE OPERATIVA

14/10/2024

#### 5.1.3.12.IOT

Selezionando ‘Configuration>IoT’ si avrà accesso alle funzionalità relative all’IoT che non vengono al momento utilizzate:



The screenshot shows the Aruba Mobility Conductor interface with the following details:

- Top Bar:** MOBILITY CONDUCTOR wctl-ts-mm2
- Header:** CONTROLLERS (28), ACCESS POINTS (1005), CLIENTS (788), ALERTS (0)
- Breadcrumbs:** Managed Network > ASUGI > MAGGIORE >
- Left Sidebar:**
  - Dashboard
  - Configuration** (selected)
  - WLANS
  - Roles & Policies
  - Access Points
  - AP Groups
  - Authentication
  - Services
  - Interfaces
  - Controllers
  - System
  - Tasks
  - Redundancy
  - IoT** (selected)
  - Maintenance
  - wctl-ts-mc5
- Right Panel - IoT Transports:**
  - Sub-tabs: IoT Radios, Zigbee Services, Zigbee Socket Devices
  - Table: Transportes

NAME	TYPE	SERVICE	SERVER URL	ENABLE
(empty)				

**Figura 32 - IoT**

Sono disponibili i seguenti tab:

- **IoT Transports**
- **IoT Radios**
- **Zigbee Services**
- **Zigbee Socket Devices**

#### NOTA BENE:

- Si osservi come in questi pannelli non è stata apportata alcuna modifica.

#### 5.1.4. AGGIUNTA DI UN NUOVO ACCESS POINT

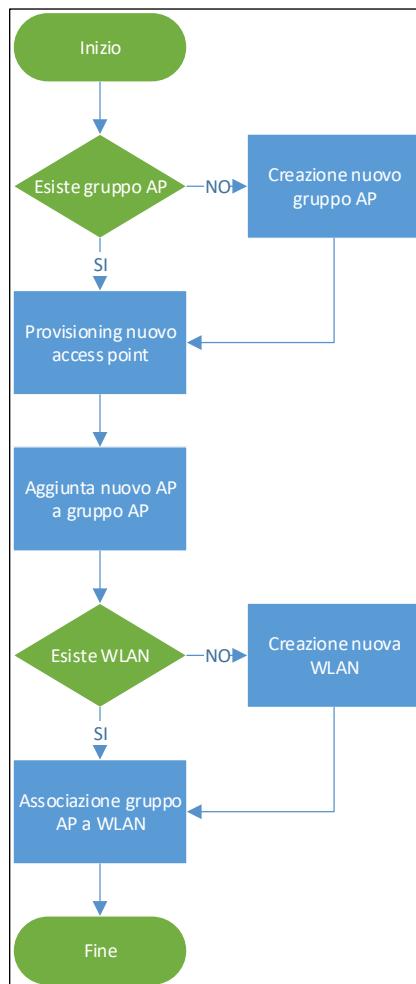
Per la procedura di configurazione sono rilevanti i soli pannelli

- **WLAN** ([PAR 5.1.3.1](#))
- **Access Points** ([PAR 5.1.3.3](#))
- **AP Groups** ([PAR 5.1.3.4](#))
- **Authentication** ([PAR 5.1.3.5](#))

Seguendo i dettagli illustrati nei paragrafi precedenti si potrà procedere come segue:

1. Provisioning nuovo access point
2. Creazione gruppo AP (se non esistente)
3. Aggiunta access point a gruppo AP
4. Creazione WLAN (se non esistente)
5. Associazione gruppo AP a WLAN

Di seguito un diagramma esemplificativo:



**Figura 33 - Aggiunta nuovo access point**



access point e terminali

**IO\_XX\_00\_XX**

Pagina 34 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.2. CONFIGURAZIONE DEI TERMINALI

#### 5.2.1. PROCEDURA CONFIGURAZIONE TERMINALE

Di seguito verrà dettagliata la procedura di configurazione di un terminale per l'accesso al WI-FI



1. Selezionare 'Pannello di controllo':

2. Aprire il 'Pannello di controllo':

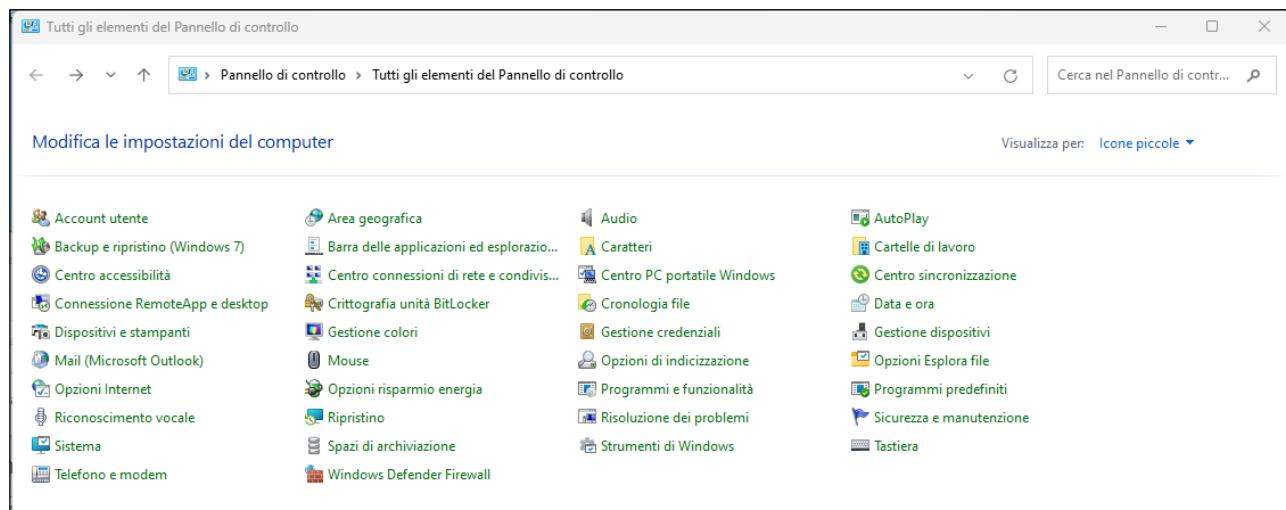


Figura 34 - Pannello di controllo

3. Selezionare 'Centro connessioni di rete e condivisione':

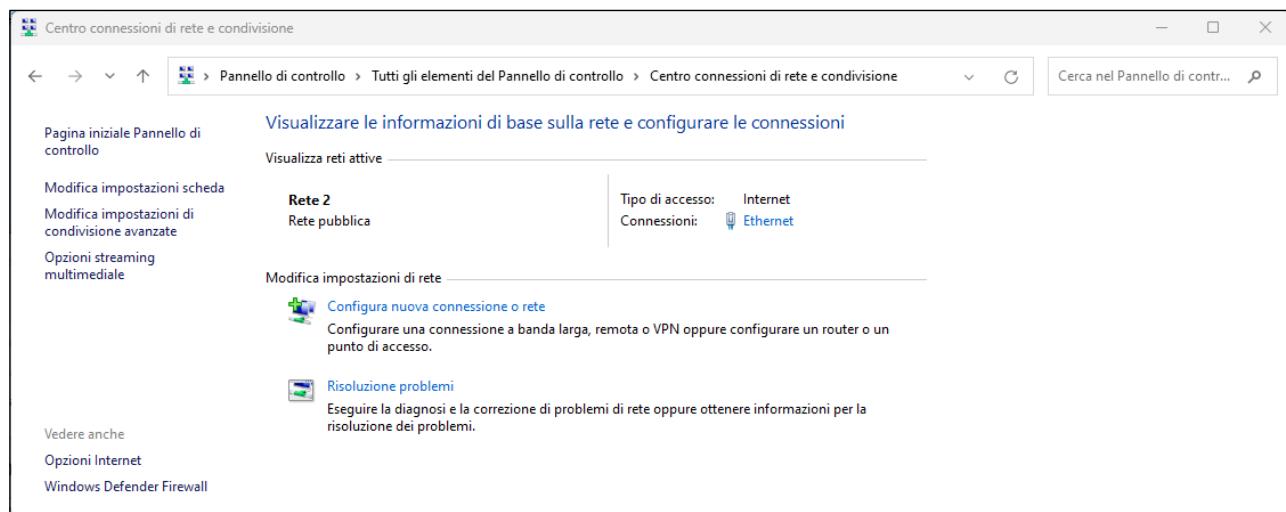


Figura 35 - Centro connessioni di rete e condivisione

Configurazione Wi-Fi Aruba:

access point e terminali

**IO\_XX\_00\_XX**

Pagina 35 di 51

ISTRUZIONE OPERATIVA

14/10/2024



access point e terminali

**IO\_XX\_00\_XX**

Pagina 36 di 51

ISTRUZIONE OPERATIVA

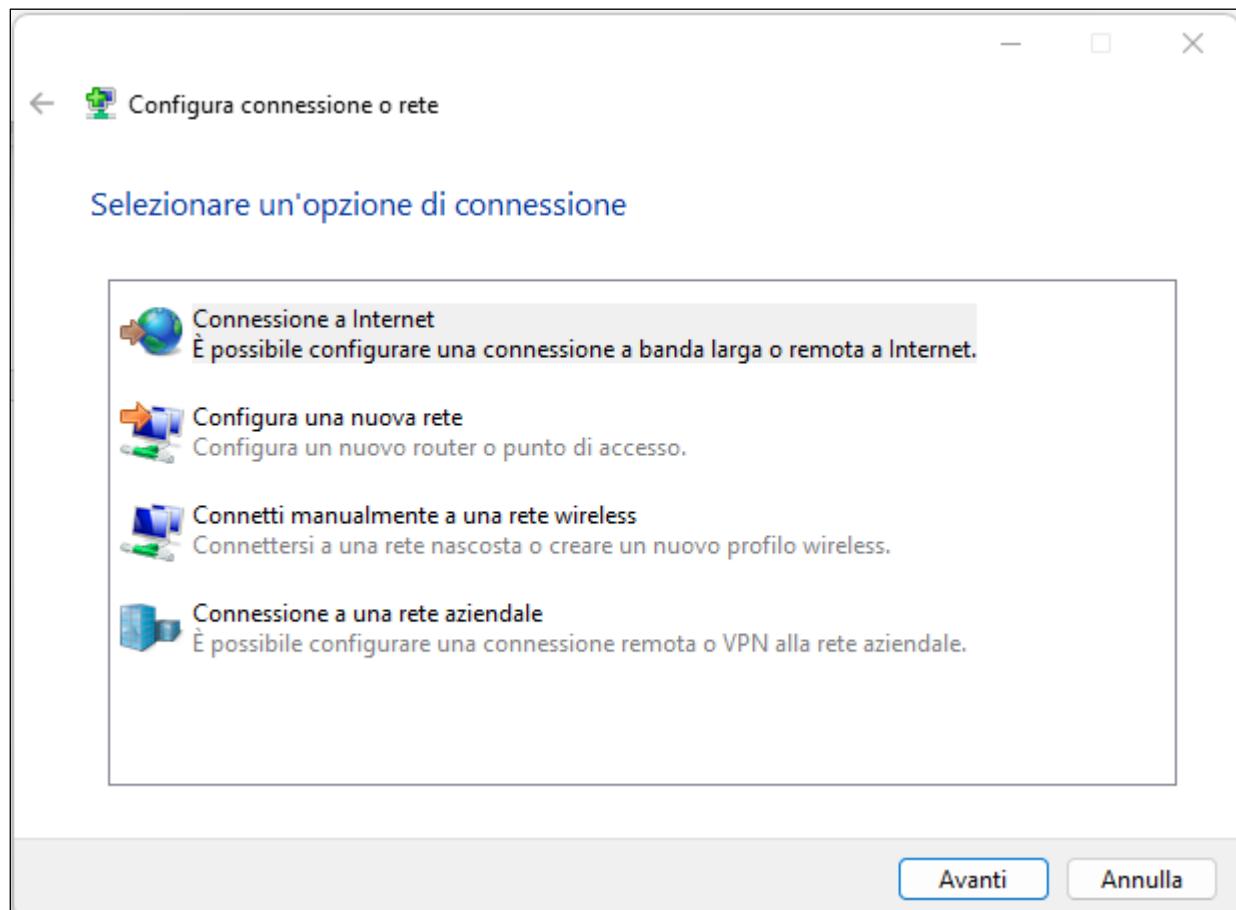
14/10/2024

4. Selezionare 'Configura nuova connessione o rete':



[Configura nuova connessione o rete](#)

Configurare una connessione a banda larga, remota o VPN oppure configurare un router o un punto di accesso.



**Figura 36 - Configura connessione o rete**

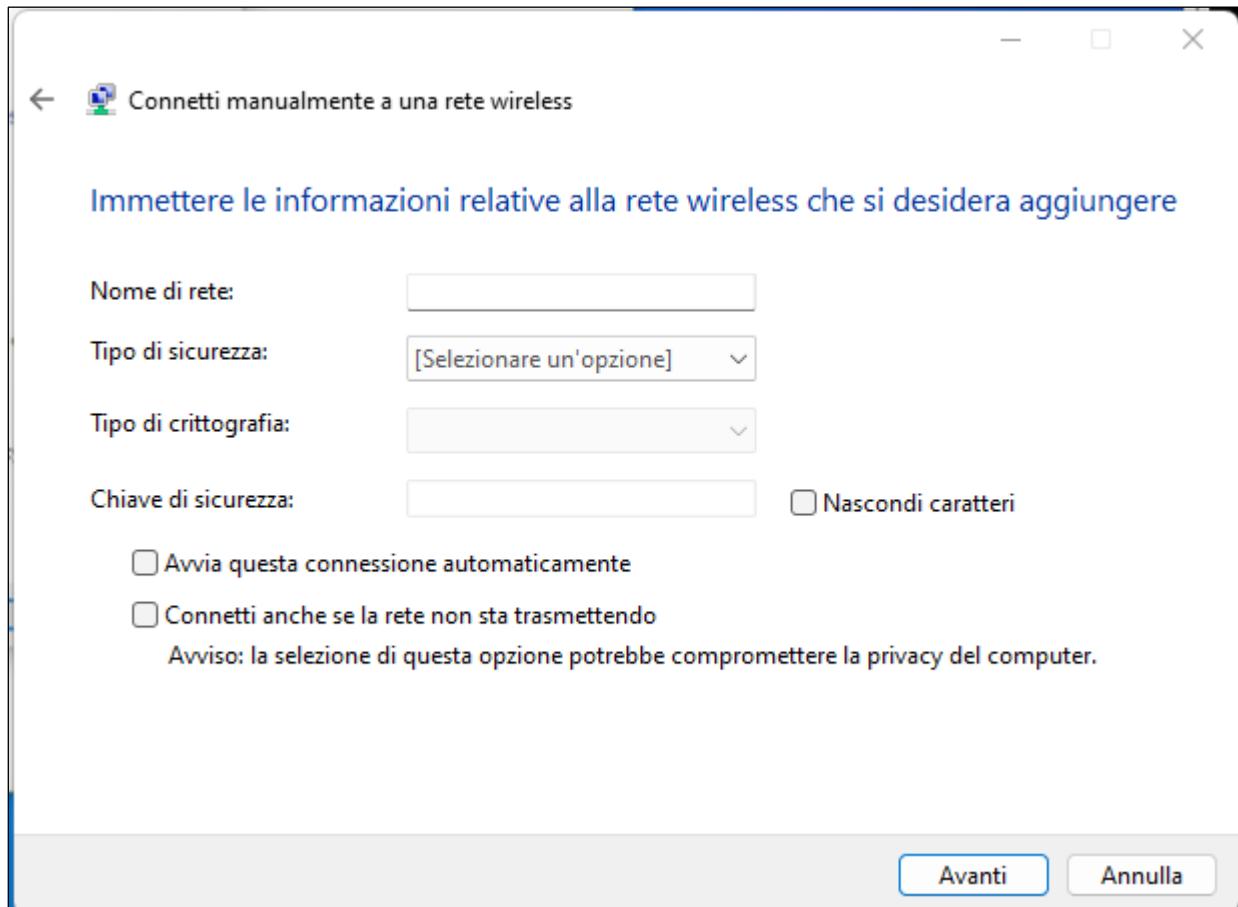
5. Selezionare ‘Connetti manualmente a una rete wireless’:



Connetti manualmente a una rete wireless

Connettersi a una rete nascosta o creare un nuovo profilo wireless.

e cliccare su ‘Avanti’.



**Figura 37 - Connotti manualmente a una rete wireless**

access point e terminali

**IO\_XX\_00\_XX**

Pagina 38 di 51

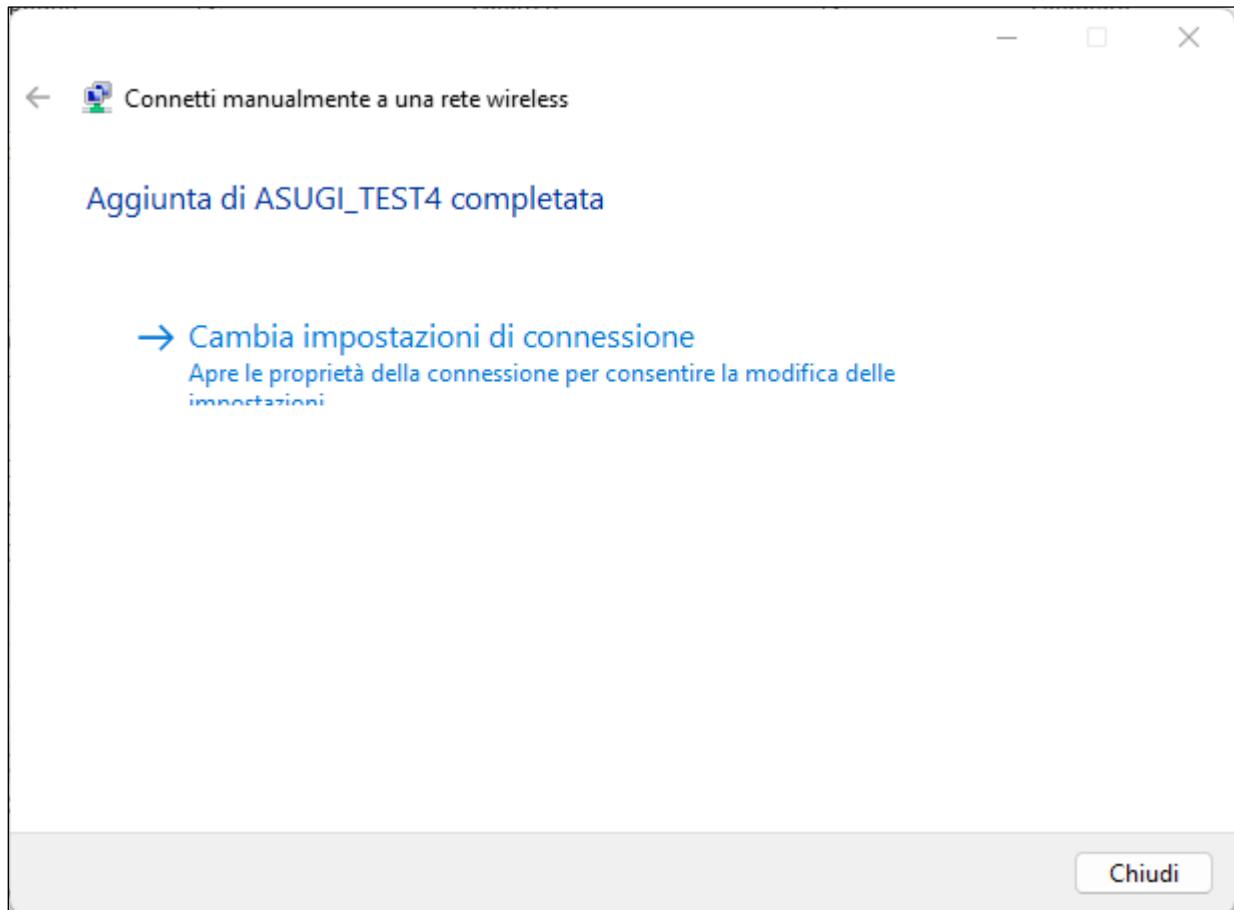
ISTRUZIONE OPERATIVA

14/10/2024

6. Il pannello andrà configurato come segue:

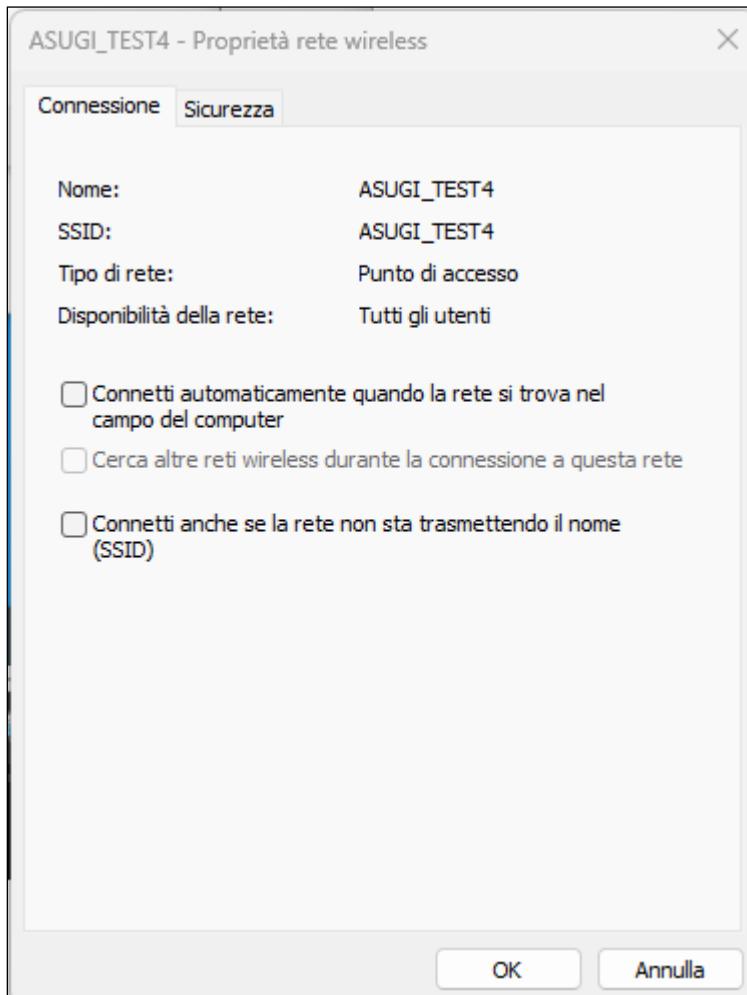
- Nome di rete: ASUGI\_TEST (in relazione a quanto visto nei paragrafi precedenti)
- Tipo di sicurezza: WPA2-Enterprise
- Tipo di crittografia: AES (automatico)
- Chiave di sicurezza:
- Avvia questa connessione automaticamente: disabilitare

Cliccare su 'Avanti':



**Figura 38 - Aggiunta di ASUGI\_TEST4 completata**

7. Selezionare ‘Cambia impostazioni di connessione’, verrà mostrato:



**Figura 39 - Proprietà rete wireless - Connessione**

8. Selezionare: ‘Connetti automaticamente quando la rete si trova nel campo del computer’.

access point e terminali

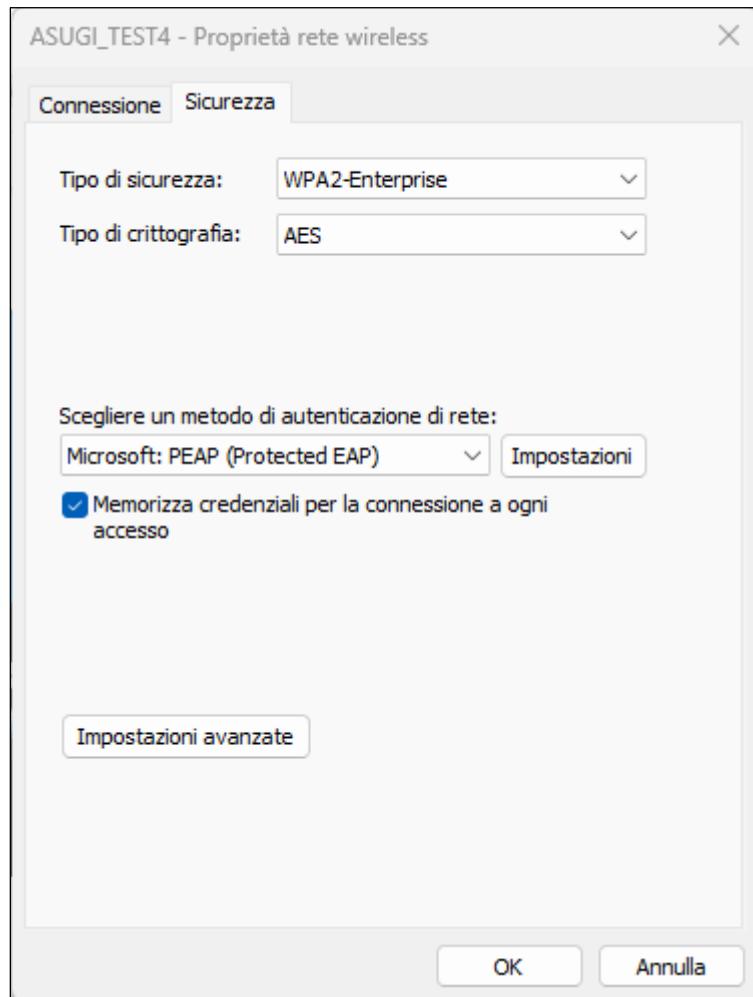
**IO\_XX\_00\_XX**

Pagina 40 di 51

ISTRUZIONE OPERATIVA

14/10/2024

9. Selezionare il tab: 'Sicurezza':



**Figura 40 - Proprietà rete wireless - Sicurezza**



access point e terminali

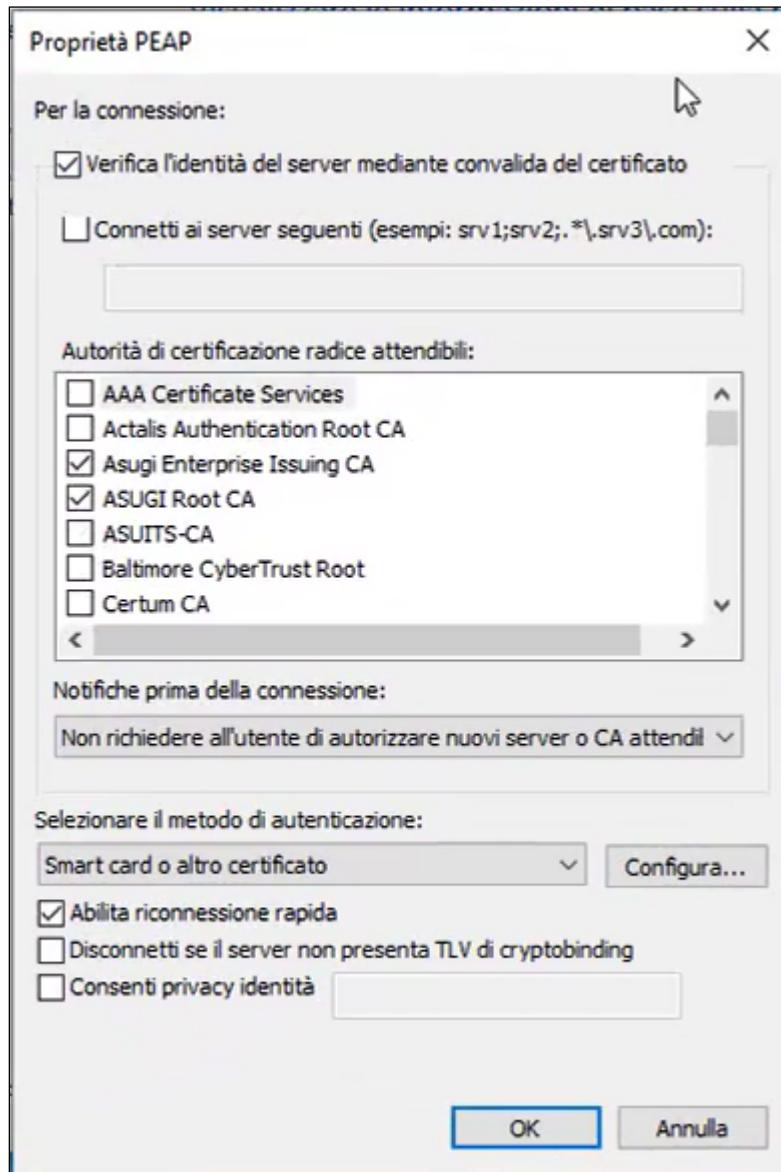
**IO\_XX\_00\_XX**

Pagina 41 di 51

### ISTRUZIONE OPERATIVA

14/10/2024

10. Selezionare ‘Impostazioni’:



**Figura 41 - Proprietà PEAP**

Devono essere selezionate:

- Verifica l'identità del server mediante convalida certificato
- Autorità di certificazione radice attendibili:
  - Asugi Enterprise Issuing CA
  - Asugi Root CA
- Notifiche prima della connessione:
  - Non richiedere all'utente di autorizzare nuovi server o CA...
- Selezionare il metodo di autenticazione:
  - Smart card o altro certificato
- Abilita connessione rapida



access point e terminali

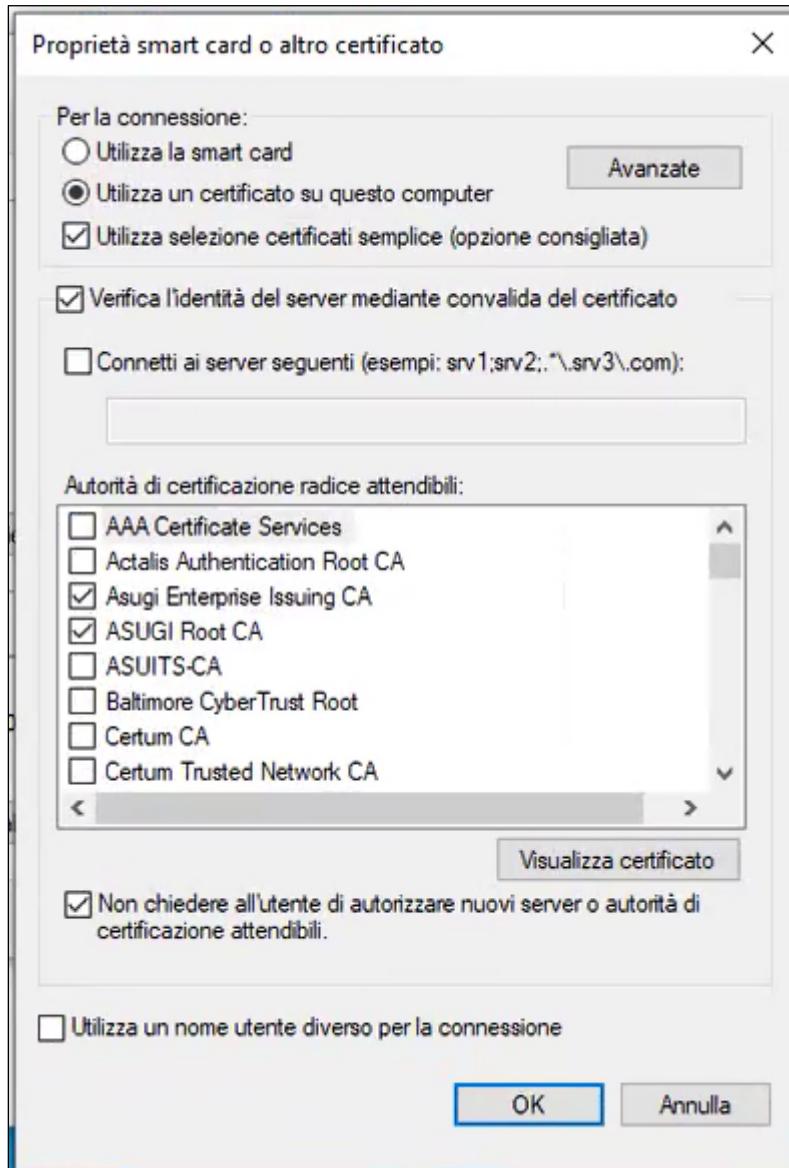
**IO\_XX\_00\_XX**

Pagina 42 di 51

**ISTRUZIONE OPERATIVA**

14/10/2024

11. Cliccare su 'Configura':


**Figura 42 - Proprietà smart card o altro certificato**

Selezionare:

- Per la connessione:
  - Utilizza un certificato su questo computer
  - Utilizza selezione certificati semplice
- Verifica l'identità del server mediante convalida del certificato
- Autorità di certificazione radice attendibili:
  - Asugi Enterprise Issuing CA
  - ASUGI Root CA



access point e terminali

**IO\_XX\_00\_XX**

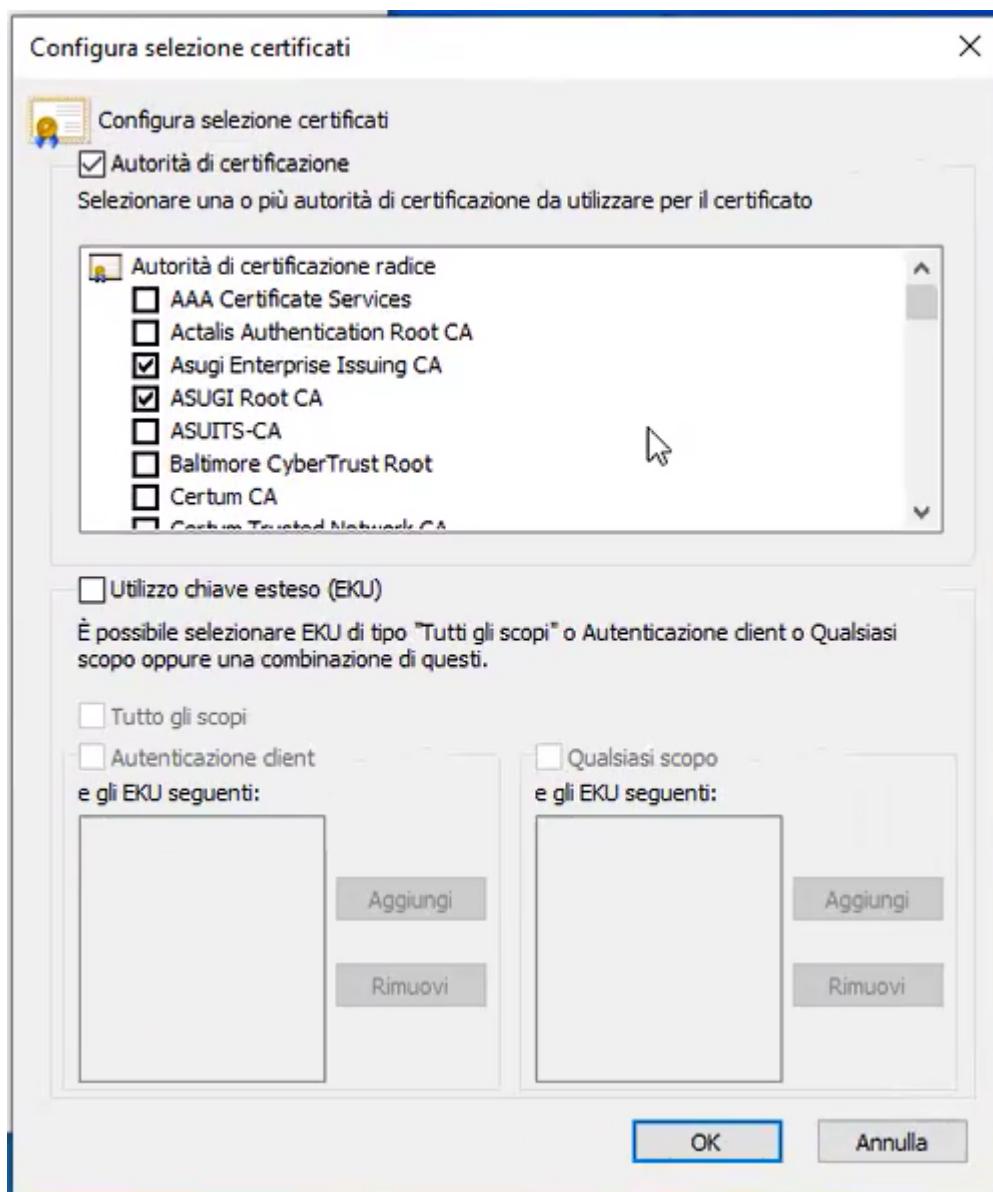
Pagina 43 di 51

### ISTRUZIONE OPERATIVA

14/10/2024

- Non chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili.

12. Cliccare su 'Avanzate':



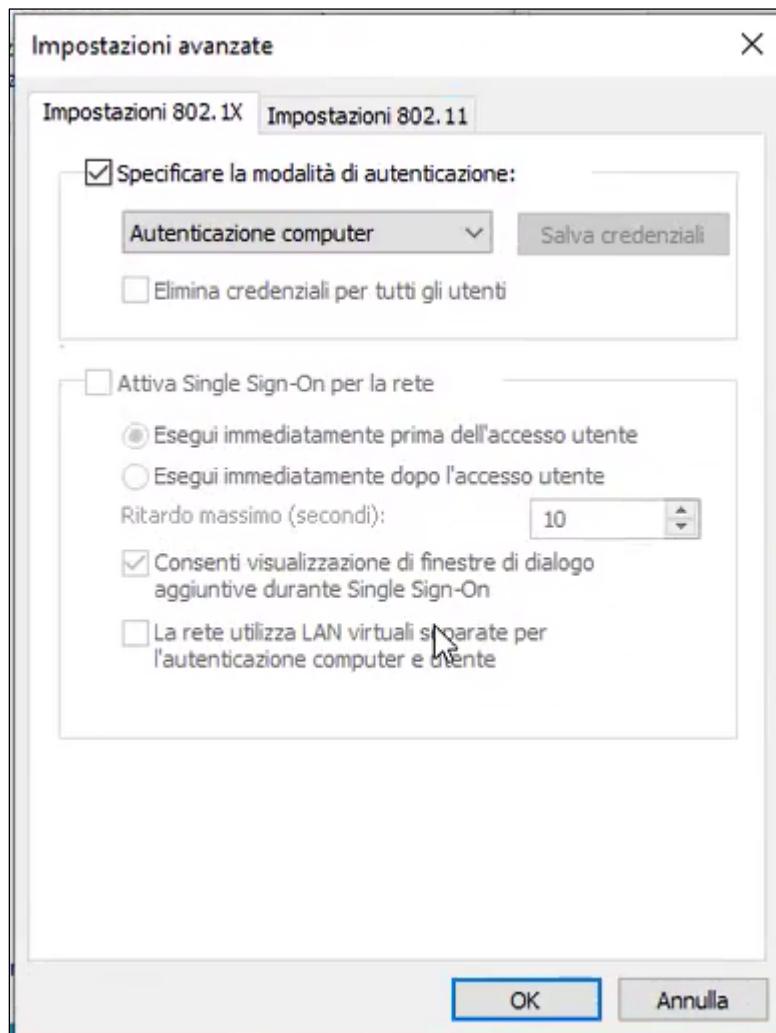
**Figura 43 - Configurazione selezione certificati**

Selezionare:

- Autorità di certificazione:
  - Asugi Enterprise Issuing CA
  - ASUGI Root CA

Cliccare su 'OK' e chiudere a ritroso la finestra in Fig.43, in Fig.42 ed in Fig.41.

13. Sulla finestra in Fig.40 cliccare: ‘Impostazioni avanzate’:



**Figura 44 - Impostazioni avanzate – 802.1X**

Selezionare:

- Specificare la modalità di autenticazione:
  - Autenticazione computer

access point e terminali

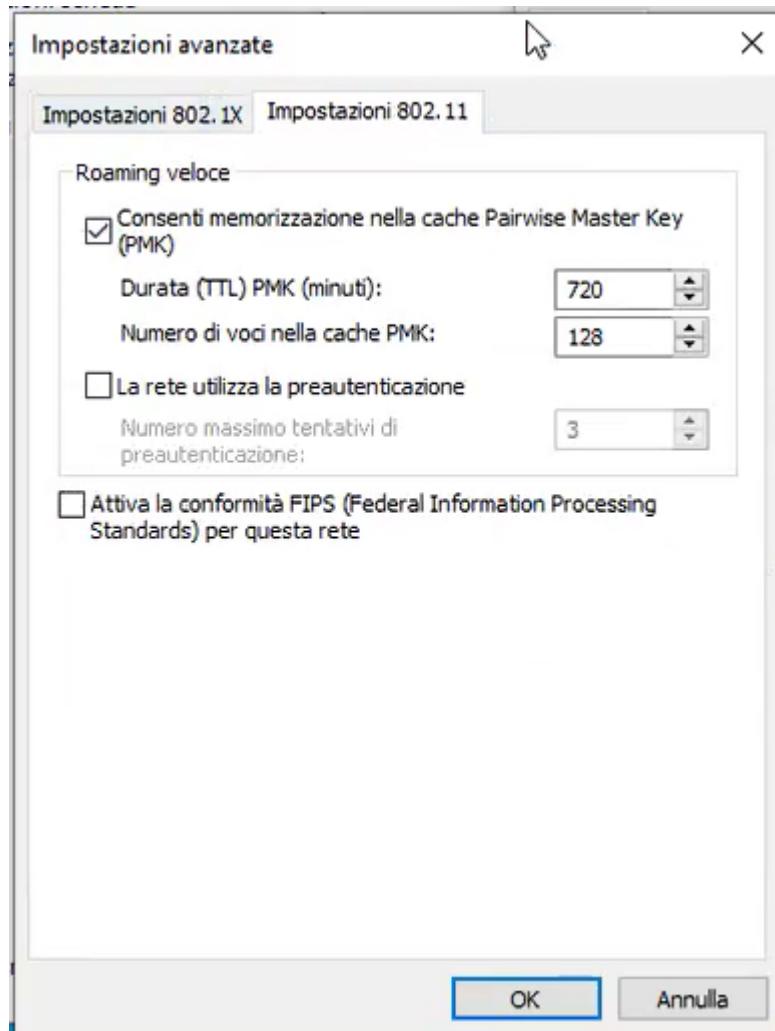
**IO\_XX\_00\_XX**

Pagina 45 di 51

ISTRUZIONE OPERATIVA

14/10/2024

14. Selezionare il tab ‘Impostazioni 802.11’



**Figura 45 - Impostazioni avanzate – 802.11**

Selezionare:

- Roaming veloce:
  - Consenti memorizzazione nella cache Pairwise Master Key (PMK)
    - Durata (TTL) PMK (minuti): 720
    - Numero di voci nella cache PMK: 128

15. A conclusione della procedura, si potrà cliccare su  **Internet**  **Wi-Fi (ASUGI\_TEST3)** e collegarsi alla rete



access point e terminali

**IO\_XX\_00\_XX**

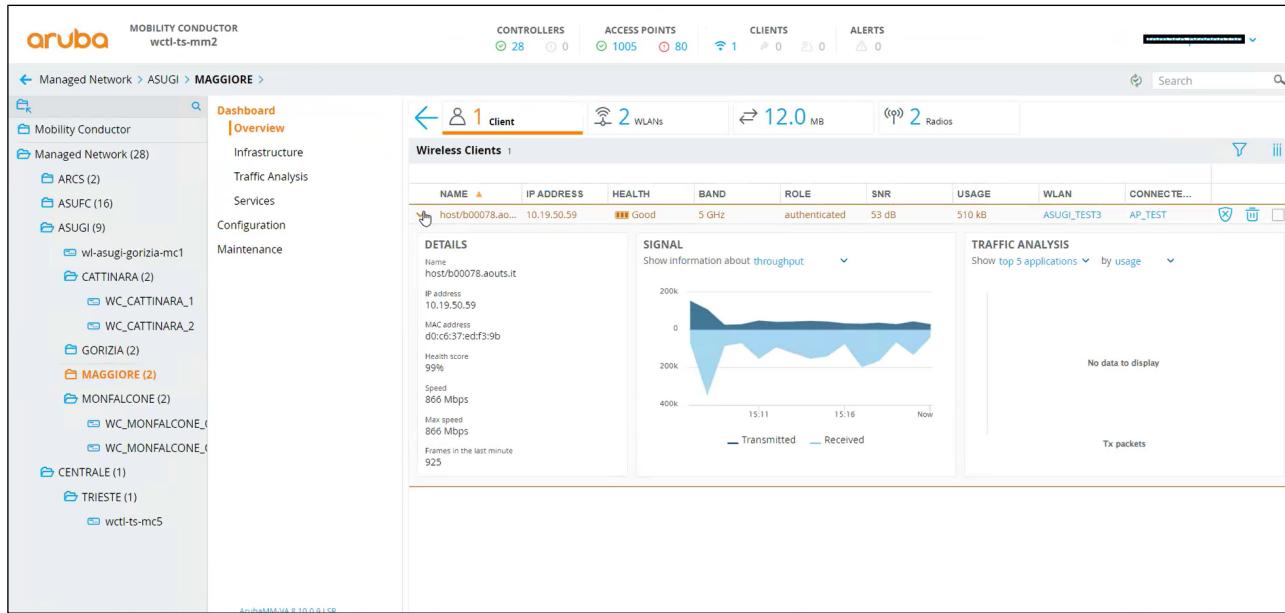
Pagina 46 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.2.2. VERIFICA CONNESSIONE TERMINALE

La correttezza della connessione si potrà verificare accedendo alla pagina principale del mobility Conductor:

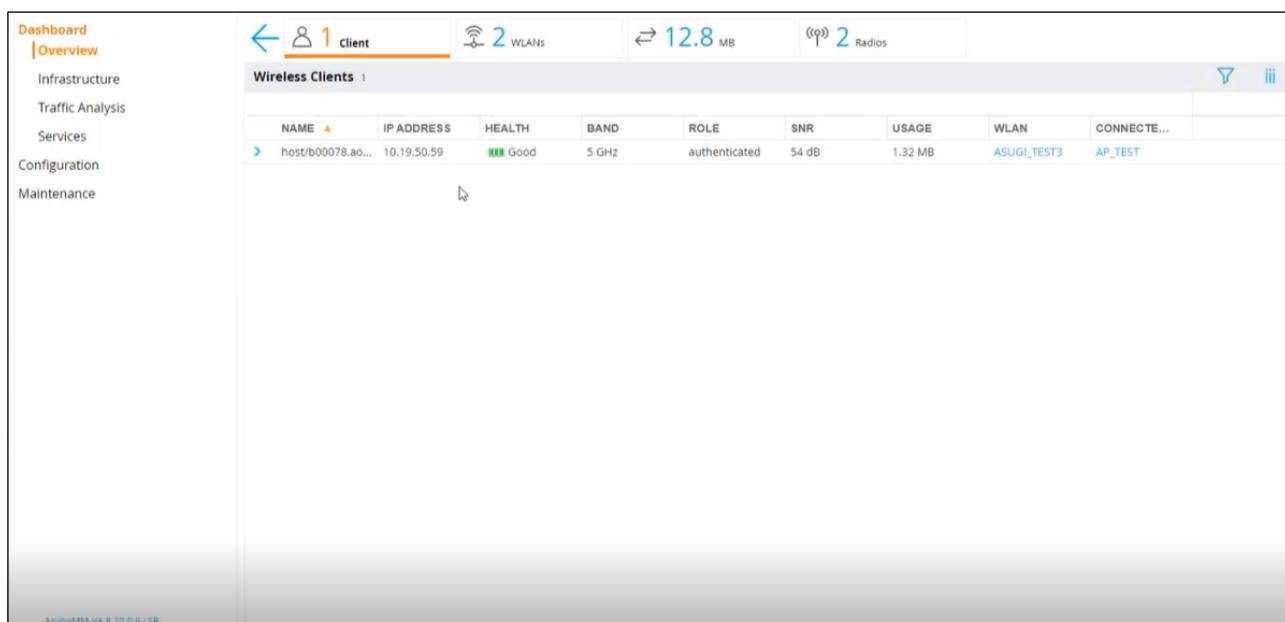


**Figura 46 - Dashboard - Overview**

Selezionando: 'DASHBOARD>OVERVIEW' sarà possibile verificare lo stato delle connessioni.

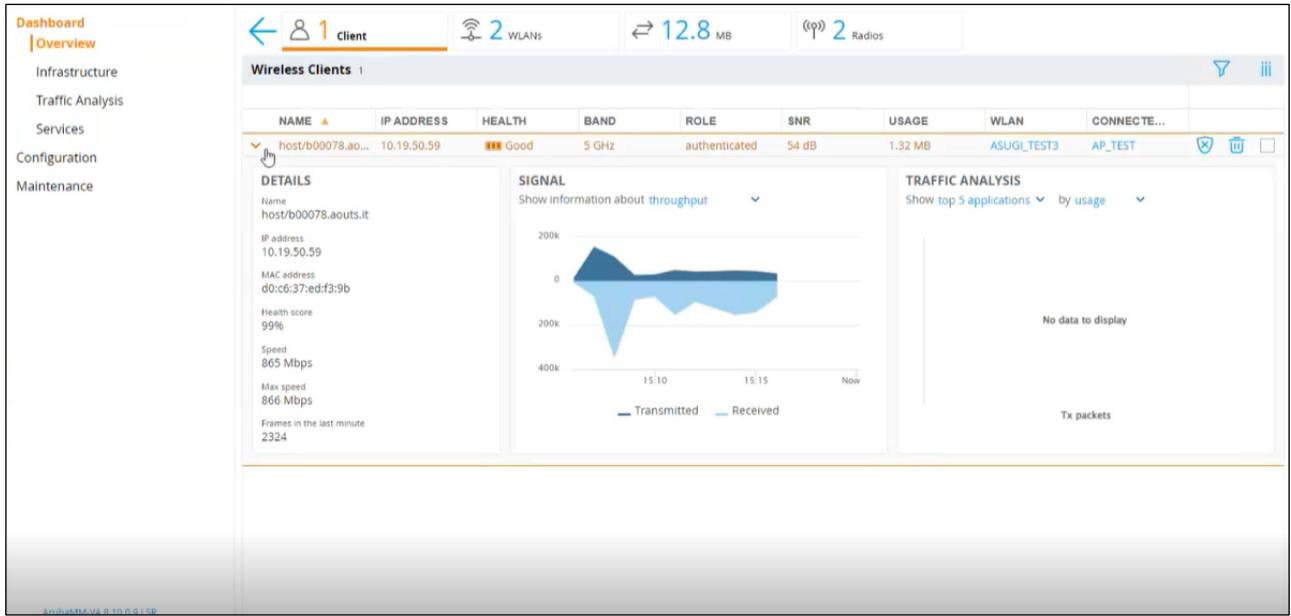
#### 5.2.2.1. CLIENT

Selezionando il tab 'Client':



**Figura 47 - Dashboard - Overview - Client**

Si avrà l'elenco dei client connessi. Cliccando sulla freccia sulla sinistra del client desiderato si avranno i dettagli dello stesso:



**Figura 48 - Dashboard - Overview - Client - Dettaglio**

Si potranno visualizzare:

- Nome dispositivo
- Indirizzo IP
- Qualità della connessione
- Banda utilizzata
- Ruolo dell'utente connesso (nel contesto del mobility Conductor)
- Rapporto Segnale Rumore
- Traffico dati
- WLAN utilizzata
- Gruppo AP utilizzato



access point e terminali

**IO\_XX\_00\_XX**

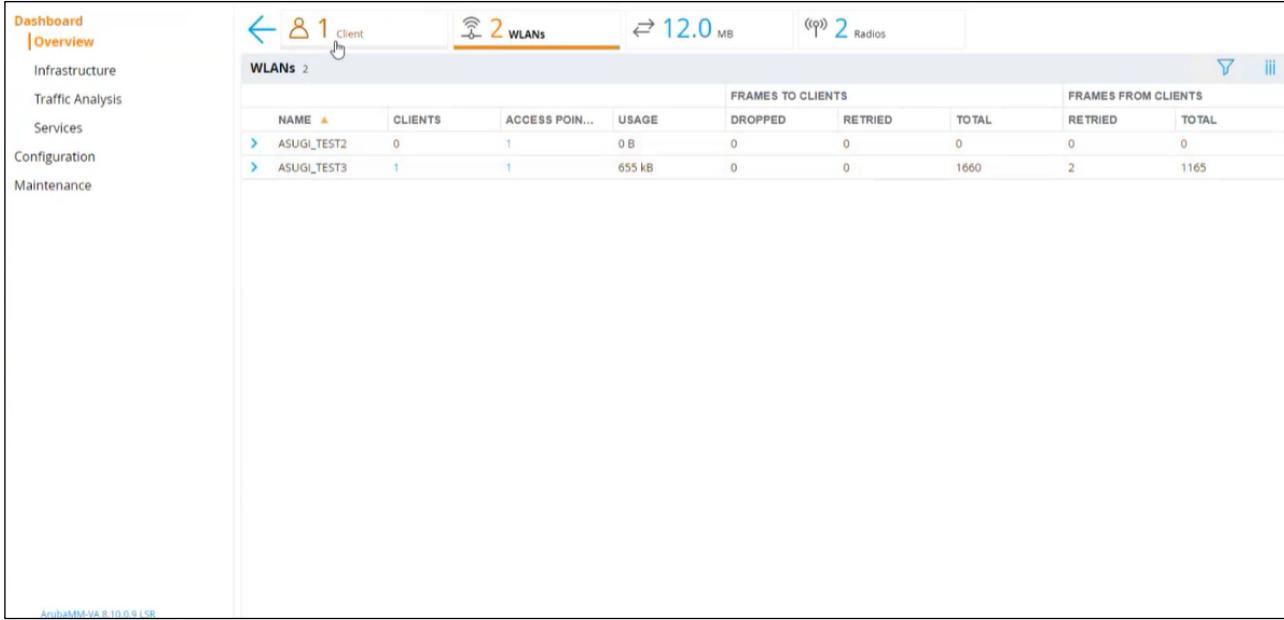
Pagina 48 di 51

## ISTRUZIONE OPERATIVA

14/10/2024

### 5.2.2.2. WLAN

Selezionando il tab 'WLANs':



NAME	CLIENTS	ACCESS POIN...	USAGE	FRAMES TO CLIENTS			FRAMES FROM CLIENTS	
				DROPPED	RETRIED	TOTAL	RETRIED	TOTAL
ASUGI_TEST2	0	1	0 B	0	0	0	0	0
ASUGI_TEST3	1	1	655 kB	0	0	1660	2	1165

**Figura 49 - Dashboard - Overview - WLANs**

Si avrà accesso all'elenco delle WLAN disponibili per il nodo selezionato (MAGGIORE) con varie informazioni.

Le più rilevanti sono:

- Nome WLAN
- Numero di client connessi
- Numero di access point utilizzati
- Traffico dati

access point e terminali

**IO\_XX\_00\_XX**

Pagina 49 di 51

ISTRUZIONE OPERATIVA

14/10/2024

## 6. GESTIONE DELLA DOCUMENTAZIONE

Nel presente documento andranno aggiornati al variare degli stessi i seguenti dati:

- Le versioni degli apparati utilizzati.
- La documentazione esterna relativa agli apparati utilizzati.
- I riferimenti alle persone da contattare in caso di problemi ed anomalie.
- Ogni altro elemento dovesse essere modificato nel tempo.

## 7. RIFERIMENTI (NORMATIVI E BIBLIOGRAFICI)

### 7.1. ARUBAOS

- [HTTPS://WWW.ARUBANETWORKS.COM/TECHDOCS/ARUBAOS-8.X-BOOKS/810/ARUBAOS-8.10.0.0-GETTING-STARTED-GUIDE.PDF](https://www.arubanetworks.com/techdocs/arubaos-8.x-books/810/arubaos-8.10.0.0-getting-started-guide.pdf)
- [HTTPS://WWW.ARUBANETWORKS.COM/TECHDOCS/ARUBAOS-8.X-BOOKS/810/ARUBAOS-8.10.0.0-USER-GUIDE.PDF](https://www.arubanetworks.com/techdocs/arubaos-8.x-books/810/arubaos-8.10.0.0-user-guide.pdf)

### 7.2. WI-FI CONTROLLER

- [HTTPS://WWW.HPE.COM/PSNOW/DOC/C05315623](https://www.hpe.com/psnow/doc/c05315623)

### 7.3. ACCESS POINT

- [HTTPS://WWW.ARUBANETWORKS.COM/TECHDOCS/HARDWARE/APS/AP500/IG/AP-500\\_INSTALL\\_GUIDE\\_IT.PDF](https://www.arubanetworks.com/techdocs/hardware/aps/ap500/ig/ap-500_install_guide_it.pdf)

## 8. DOCUMENTI COLLEGATI

- [HTTP://WIKI.AOUTS.IT/DOKU.PHP?ID=DOCUMENTAZIONE:WIRELESS:WIRELESS\\_CONTROLLER\\_9240:START&S\[\]](https://wiki.aouts.it/doku.php?id=documentazione:wireless:wireless_controller_9240:start&s[])=ARUBA
- [HTTP://WIKI.AOUTS.IT/DOKU.PHP?ID=DOCUMENTAZIONE:WIRELESS:NO\\_LLDP:START&S\[\]](https://wiki.aouts.it/doku.php?id=documentazione:wireless:no_lldp:start&s[])=ARUBA
- [HTTP://WIKI.AOUTS.IT/DOKU.PHP?ID=DOCUMENTAZIONE:WIRELESS:MOBILITY\\_CONDUCTOR:START&S\[\]](https://wiki.aouts.it/doku.php?id=documentazione:wireless:mobility_conductor:start&s[])=ARUBA
- [HTTP://WIKI.AOUTS.IT/DOKU.PHP?ID=DOCUMENTAZIONE:WIRELESS:RESET\\_ARUBA\\_9240:START&S\[\]](https://wiki.aouts.it/doku.php?id=documentazione:wireless:reset_aruba_9240:start&s[])=ARUBA
- [HTTP://WIKI.AOUTS.IT/DOKU.PHP?ID=DOCUMENTAZIONE:WIRELESS:START&S\[\]](https://wiki.aouts.it/doku.php?id=documentazione:wireless:start&s[])=ARUBA

## 9. ALLEGATI (SE PRESENTI)

- Nessuno

## 10. INDICE DELLE FIGURE

<a href="#"><u>FIGURA 1 - DIAGRAMMA LOGICO INFRASTRUTTURA WI-FI</u></a>	6
<a href="#"><u>FIGURA 2 - ACCESSO AL 'MOBILITY CONDUCTOR'</u></a>	7
<a href="#"><u>FIGURA 3 - SCHERMATA PRINCIPALE DEL 'MOBILITY CONDUCTOR'</u></a>	7
<a href="#"><u>FIGURA 4 - RETI GESTITE</u></a>	8
<a href="#"><u>FIGURA 5 - STATISTICHE INFRASTRUTTURA</u></a>	9
<a href="#"><u>FIGURA 6 - DATI STATISTICI RELATIVI AD UNO SPECIFICO SITO</u></a>	10
<a href="#"><u>FIGURA 7 – CONFIGURATION - DETTAGLIO</u></a>	11
<a href="#"><u>FIGURA 8 - DETTAGLIO WLAN</u></a>	12
<a href="#"><u>FIGURA 9 – DETTAGLIO VLANS</u></a>	13
<a href="#"><u>FIGURA 10 - DETTAGLIO SECURITY</u></a>	14
<a href="#"><u>FIGURA 11 – DETTAGLIO ACCESS</u></a>	15
<a href="#"><u>FIGURA 12 - ROLES &amp; POLICIES</u></a>	16
<a href="#"><u>FIGURA 13 – DETTAGLIO ROLES</u></a>	17
<a href="#"><u>FIGURA 14 – DETTAGLIO POLICIES</u></a>	17
<a href="#"><u>FIGURA 15 – DETTAGLIO APPLICATIONS</u></a>	18
<a href="#"><u>FIGURA 16 - DETTAGLIO ALIASES</u></a>	18
<a href="#"><u>FIGURA 17 - ELENCO ACCESS POINT</u></a>	19
<a href="#"><u>FIGURA 18 - DETTAGLIO ACCESS POINT</u></a>	20
<a href="#"><u>FIGURA 19 – ELENCO AP GROUPS</u></a>	22
<a href="#"><u>FIGURA 20 – AUTHENTICATION</u></a>	23
<a href="#"><u>FIGURA 21 - DETTAGLIO AUTH SERVERS</u></a>	24
<a href="#"><u>FIGURA 22 - DETTAGLI SERVER GROUP – TAB SERVERS</u></a>	25
<a href="#"><u>FIGURA 23 - DETTAGLIO SERVER RADIUS - 1</u></a>	25
<a href="#"><u>FIGURA 24 - DETTAGLIO SERVER RADIUS - 2</u></a>	26
<a href="#"><u>FIGURA 25 - DETTAGLIO SERVER RADIUS - 3</u></a>	26
<a href="#"><u>FIGURA 26 – SERVICES</u></a>	27
<a href="#"><u>FIGURA 27 - INTERFACES</u></a>	28
<a href="#"><u>FIGURA 28 - CONTROLLERS</u></a>	29
<a href="#"><u>FIGURA 29 – SYSTEM</u></a>	29
<a href="#"><u>FIGURA 30 – TASKS</u></a>	30
<a href="#"><u>FIGURA 31 - REDUNDANCY</u></a>	31
<a href="#"><u>FIGURA 32 - IOT</u></a>	32
<a href="#"><u>FIGURA 33 - AGGIUNTA NUOVO ACCESS POINT</u></a>	33
<a href="#"><u>FIGURA 34 - PANNELLO DI CONTROLLO</u></a>	34
<a href="#"><u>FIGURA 35 - CENTRO CONNESSIONI DI RETE E CONDIVISIONE</u></a>	34
<a href="#"><u>FIGURA 36 - CONFIGURA CONNESSIONE O RETE</u></a>	35
<a href="#"><u>FIGURA 37 - CONNETTI MANUALMENTE A UNA RETE WIRELESS</u></a>	36
<a href="#"><u>FIGURA 38 - AGGIUNTA DI ASUGI_TEST4 COMPLETATA</u></a>	37
<a href="#"><u>FIGURA 39 - PROPRIETÀ RETE WIRELESS - CONNESSIONE</u></a>	38
<a href="#"><u>FIGURA 40 - PROPRIETÀ RETE WIRELESS - SICUREZZA</u></a>	39
<a href="#"><u>FIGURA 41 - PROPRIETÀ PEAP</u></a>	40
<a href="#"><u>FIGURA 42 - PROPRIETÀ SMART CARD O ALTRO CERTIFICATO</u></a>	41
<a href="#"><u>FIGURA 43 - CONFIGURAZIONE SELEZIONE CERTIFICATI</u></a>	42
<a href="#"><u>FIGURA 44 - IMPOSTAZIONI AVANZATE – 802.1X</u></a>	43
<a href="#"><u>FIGURA 45 - IMPOSTAZIONI AVANZATE – 802.11</u></a>	44

access point e terminali

**IO\_XX\_00\_XX**

Pagina 51 di 51

ISTRUZIONE OPERATIVA

14/10/2024

<a href="#"><u>FIGURA 46 - DASHBOARD - OVERVIEW</u></a>	45
<a href="#"><u>FIGURA 47 - DASHBOARD - OVERVIEW - CLIENT</u></a>	45
<a href="#"><u>FIGURA 48 - DASHBOARD - OVERVIEW - CLIENT - DETTAGLIO</u></a>	46
<a href="#"><u>FIGURA 49 - DASHBOARD - OVERVIEW - WLANS</u></a>	47