Configurare Guest Flow con ISE 2.0 e Aruba WLC

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Flusso guest](#)
[Configurazione](#)
[Passaggio 1. Aggiungere Aruba WLC come AND in ISE.](#)
[Passaggio 2. Configurare I Profili Di Autorizzazione.](#)
[Passaggio 3. Configurare i criteri di autorizzazione.](#)
[Passaggio 4. Configurare il server Radius su Aruba.](#)
[Passaggio 5. Creare un SSID guest su Aruba.](#)
[Passaggio 6. Configurare Captive Portal.](#)
[Passaggio 7. Configurazione dei ruoli utente.](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Errore COA](#)
[Reindirizza problema](#)
[Nessun URL di reindirizzamento presente nel browser](#)
[Timer di unione sessioni scaduto](#)

Introduzione

In questo documento viene descritto come configurare i portali guest con Aruba Wireless LAN Controller (WLC). Da Identity Services Engine (ISE) versione 2.0 è introdotto il supporto per dispositivi di accesso alla rete (NAD) di terze parti. ISE supporta attualmente l'integrazione con Aruba Wireless per i flussi BYOD (Guest, Posture and Bring Your Own Device).

> **Nota:** Cisco non è responsabile della configurazione o del supporto di dispositivi di altri fornitori.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Aruba IAP

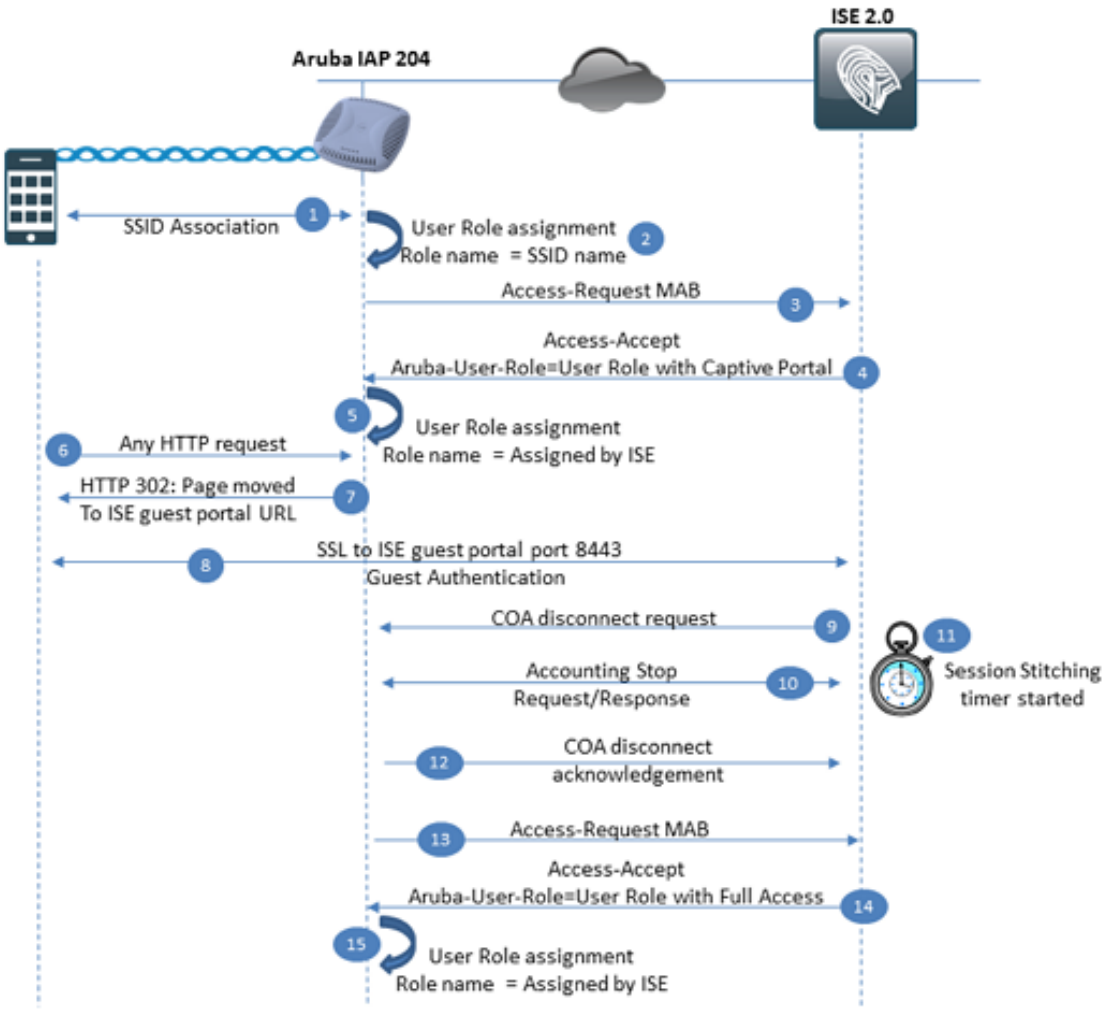
- OB flow su ISE

Componenti usati

- Software Aruba IAP 204 6.4.2.3
- Cisco Identity Services Engine 2.0

Premesse

Flusso guest



Passaggio 1. L'utente è associato all'identificatore del set di servizi (SSID). SSID può essere configurato come aperto o con l'autenticazione a chiave già condivisa.

Passaggio 2. Aruba applica User-Role a questa connessione. Il primo ruolo utente è sempre SSID stesso. User-role contiene impostazioni diverse, ad esempio VLAN, restrizione del controllo di accesso, impostazione di Captive-Portal e altro ancora. Nell'esempio corrente, il ruolo utente predefinito assegnato a SSID ha solo l'istruzione Permit-All.

Passaggio 3. SSID è configurato per fornire il filtro MAC sul server RADIUS esterno. La richiesta di accesso Radius MAB (MAC Authentication Bypass) viene inviata ad ISE.

Passaggio 4. Al momento della valutazione della policy, ISE seleziona il profilo di autorizzazione

per il guest. Questo profilo di autorizzazione contiene un tipo di accesso uguale ad ACCESS_ACCEPT e un ruolo utente-Aruba uguale al nome del ruolo utente configurato localmente su Aruba WLC (Wireless LAN Controller). Questo ruolo utente è configurato per Captive-Portal e il traffico viene reindirizzato verso ISE.

Ruoli utente di Aruba

Il componente principale utilizzato da Aruba WLC è User-Role. User-Role definisce la restrizione di accesso applicabile all'utente al momento della connessione. Le restrizioni di accesso possono includere: reindirizzamento Captive Portal, lista di controllo dell'accesso, VLAN (Virtual Local Area Network), limitazione della larghezza di banda e altre ancora. Ogni SSID esistente in Aruba WLC ha il ruolo utente predefinito in cui il ruolo utente è uguale al nome SSID. Tutti gli utenti connessi a SSID specifico inizialmente ricevono le restrizioni dal ruolo predefinito. User-Role può essere sovrascritto dal server Radius, in questo caso Access-Accept deve contenere l'attributo Aruba-User-Role specifico del fornitore Aruba. Il valore di questo attributo viene utilizzato dal WLC per trovare il ruolo utente locale.

Passaggio 5. Con l'attributo Aruba-User-Role WLC verifica localmente la presenza di ruoli utente configurati e ne applica uno richiesto.

Passaggio 6. L'utente avvia la richiesta HTTP nel browser.

Passaggio 7. Aruba WLC intercetta la richiesta a causa del ruolo utente configurato per Captive Portal. In risposta a questa richiesta, WLC restituisce il codice HTTP 302 Pagina spostata con il portale guest ISE come nuova posizione.

Passaggio 8. L'utente stabilisce una connessione SSL a ISE sulla porta 8443 e fornisce un nome utente/password nel portale guest.

Passaggio 9. ISE invia un messaggio di richiesta di disconnessione del certificato di autenticità (COA) al WLC di Aruba.

Passaggio 10. Dopo la disconnessione del certificato di autenticità (COA), il WLC interrompe la connessione con l'utente e informa ISE che la connessione deve essere terminata utilizzando il messaggio Radius Accounting-Request (Stop). ISE deve confermare che questo messaggio è stato ricevuto da Accounting.

Passaggio 11. ISE avvia il timer di unione sessioni. Questo timer viene utilizzato per associare la sessione prima e dopo il certificato di autenticità (COA). Durante questo periodo ISE ricorda tutti i parametri della sessione, come il nome utente, ecc. Prima della scadenza del timer è necessario eseguire un secondo tentativo di autenticazione per selezionare i criteri di autorizzazione corretti per il client. Se il timer scade, la nuova richiesta di accesso verrà interpretata come una sessione completamente nuova e i criteri di autorizzazione con il reindirizzamento guest verranno applicati di nuovo.

Passaggio 12. Aruba WLC conferma la richiesta di disconnessione del certificato di autenticità ricevuta in precedenza con la conferma della disconnessione del certificato di autenticità.

Passaggio 13. Aruba WLC invia una nuova richiesta di accesso Radius MAB.

Passaggio 14. Al momento della valutazione della policy, ISE seleziona il profilo di autorizzazione per il guest dopo l'autenticazione. Questo profilo di autorizzazione contiene un tipo di accesso uguale ad ACCESS_ACCEPT e un ruolo utente-Aruba uguale al nome del ruolo utente

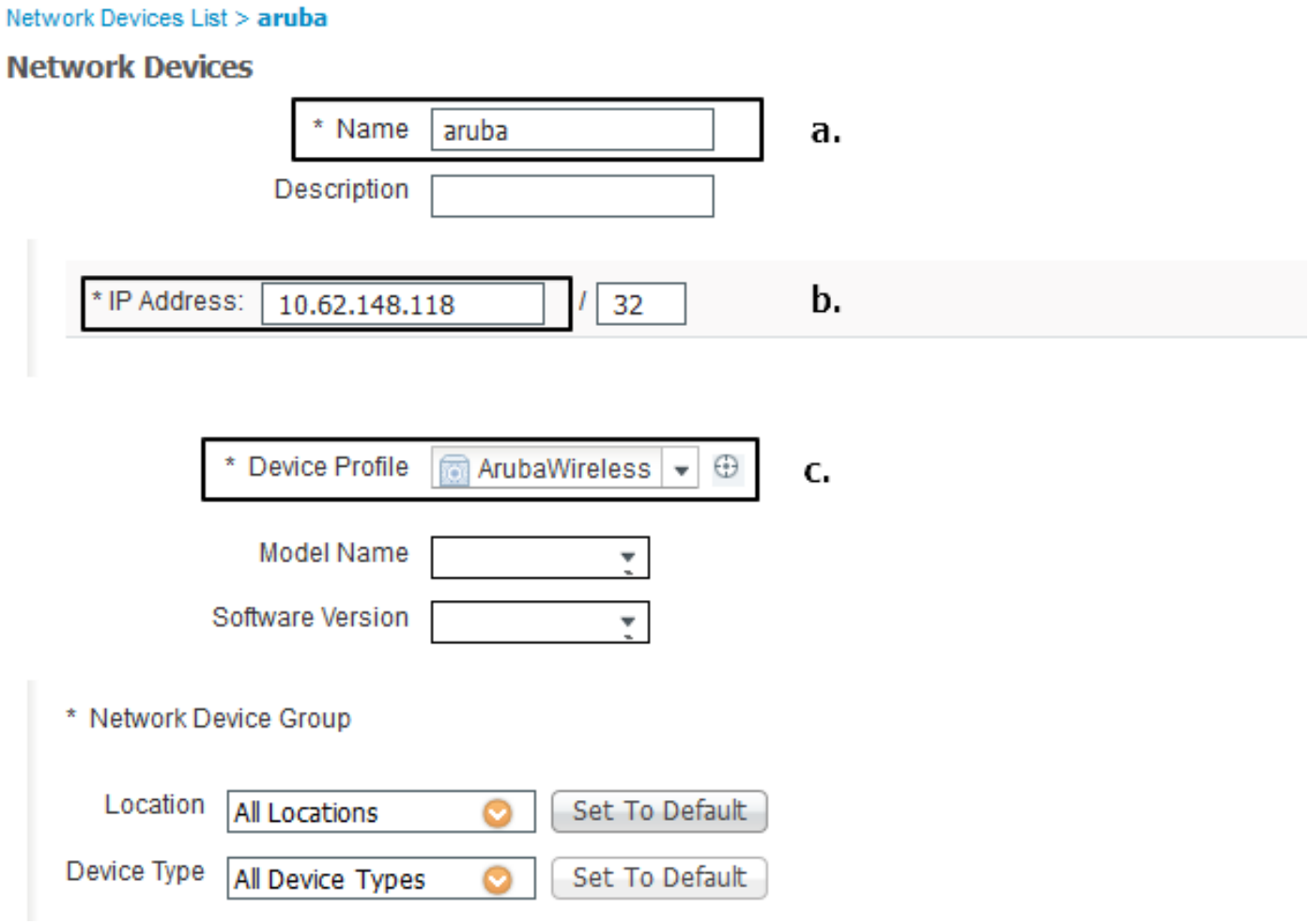
configurato localmente sul WLC di Aruba. Questo ruolo utente è configurato per consentire tutto il traffico.

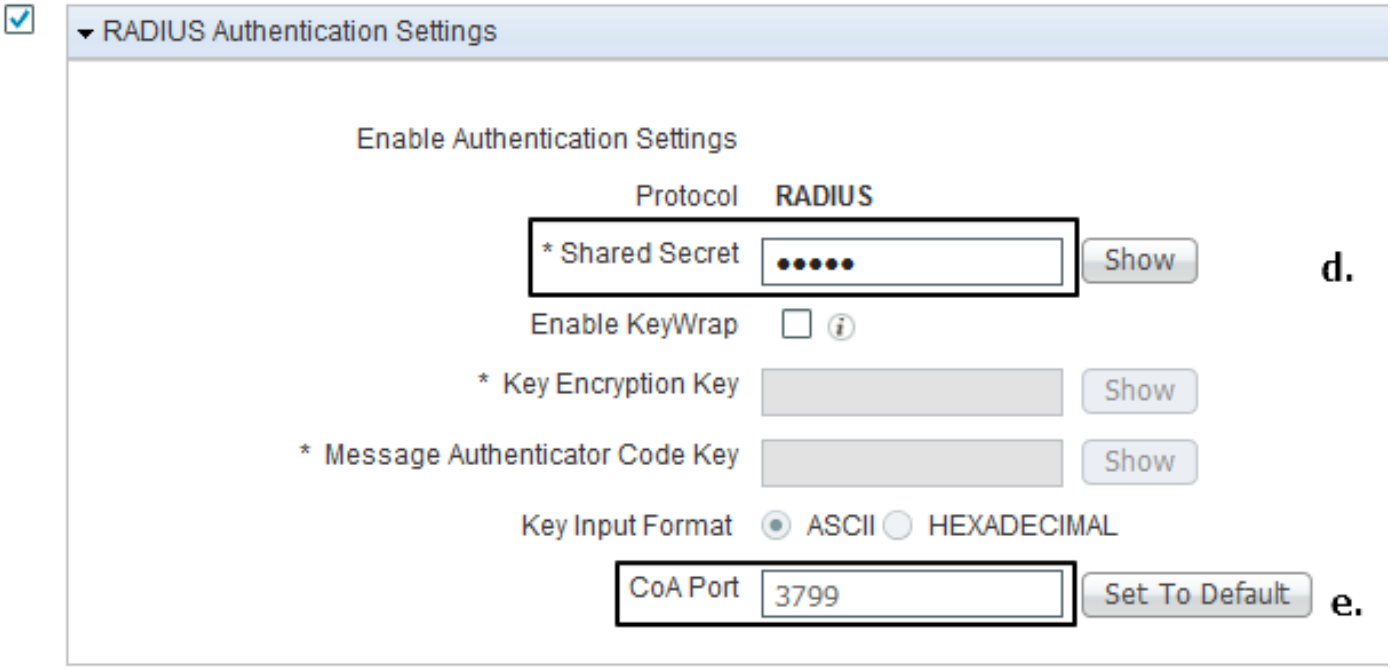
Passaggio 15. Con l'attributo Aruba-User-Role WLC controlla i ruoli utente configurati localmente e ne applica uno richiesto.

Configurazione

Passaggio 1. Aggiungere Aruba WLC come AND in ISE.

Selezionare **Amministrazione > Risorse di rete > Dispositivi di rete** e fare clic su **Aggiungi**

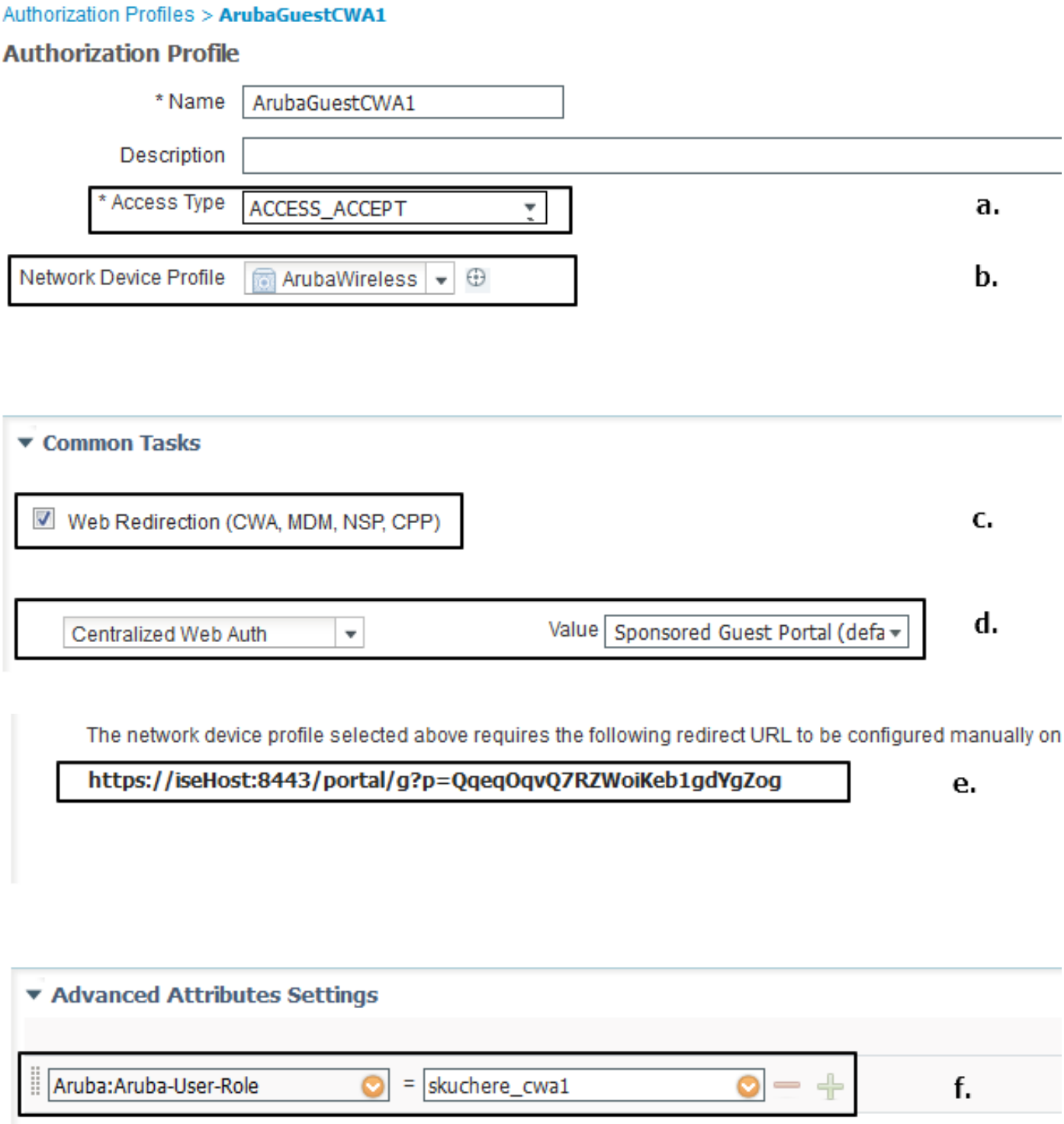




1. Specificare il nome del dispositivo di accesso alla rete (NAD).
2. Specificare l'indirizzo IP AND.
3. Scegliere Profilo dispositivo di rete. Per Aruba WLC, è possibile usare il profilo incorporato ArubaWireless.
4. Fornire una chiave già condivisa.
5. Definire la porta COA, il dispositivo dall'esempio corrente utilizzare la porta UDP 3799 per il COA.

Passaggio 2. Configurare I Profili Di Autorizzazione.

Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profilo autorizzazione** e fare clic su **Aggiungi.** È innanzitutto necessario creare un profilo di autorizzazione per il reindirizzamento dell'autenticazione Web centrale (CWA, Central Web Authentication), come illustrato nell'immagine.

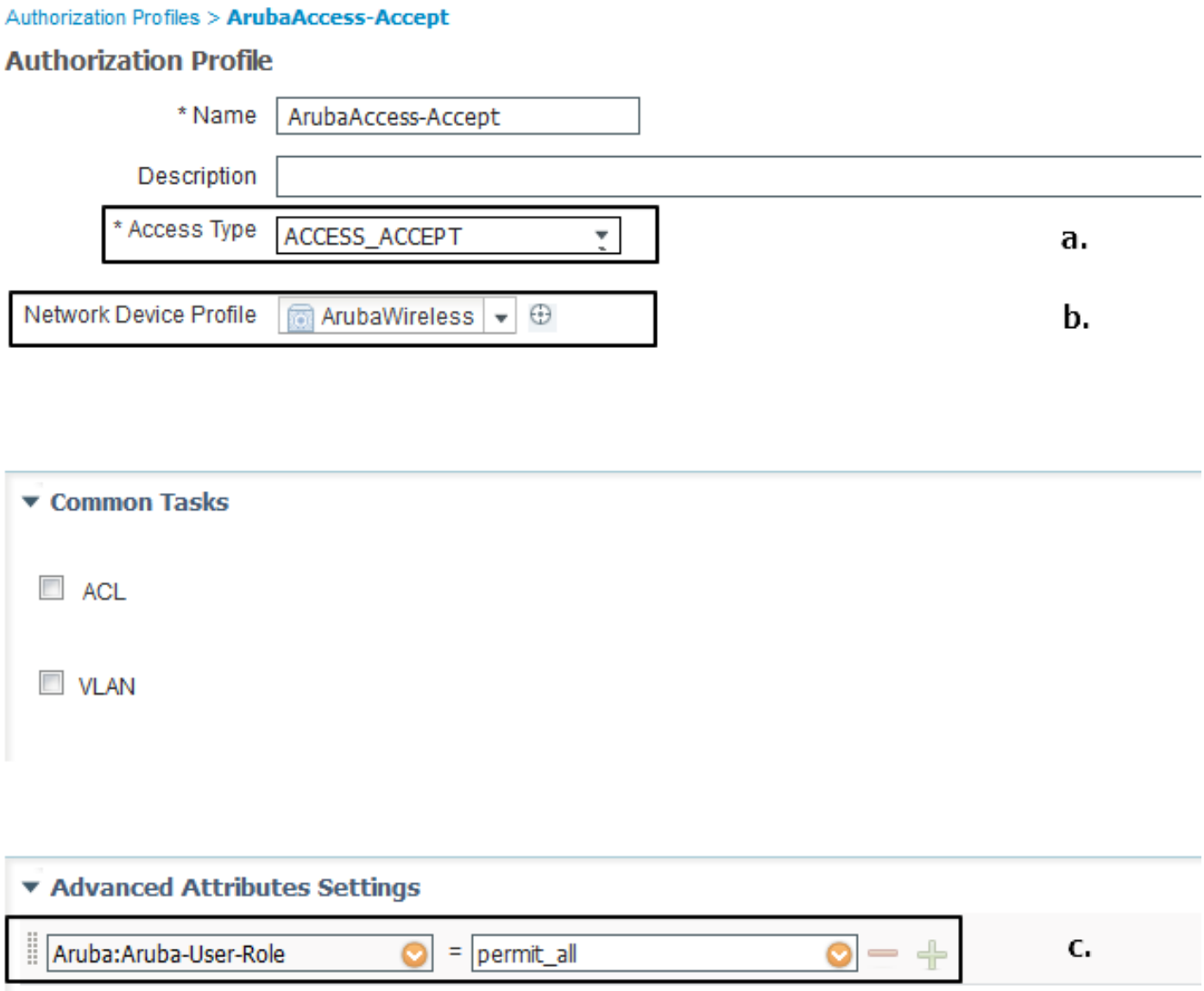


Nota: Per impostazione predefinita, tutti i profili di autorizzazione hanno un tipo di dispositivo di rete uguale a Cisco. Se NAD è configurato come ArubaWireless e viene creato un profilo di autorizzazione per un altro tipo di dispositivo, questo profilo non viene mai associato a questo dispositivo.

1. Definire **Access-Type** come **Access-Accept**.
2. In **Profilo dispositivo di rete** selezionare **ArubaWireless**.
3. Nella sezione Attività comuni abilitare l'opzione **Reindirizzamento Web**.
4. Come tipo di reindirizzamento selezionare **Autenticazione Web centralizzata** e selezionare il portale guest che si desidera utilizzare per il reindirizzamento.
5. L'URL presentato da ISE deve essere definito sul WLC di Aruba come URL del portale Captive esterno.

6. Nella sezione **Impostazioni avanzate attributi** definire il valore dell'attributo User-Role di Aruba.

Ènecessario creare un secondo profilo di autorizzazione per consentire l'accesso agli utenti guest dopo l'autenticazione del portale:



1. Definire **Access-Type** come **Access-Accept**.
2. In **Profilo dispositivo di rete** selezionare **ArubaWireless**.
3. Nella sezione **Impostazioni avanzate attributi** definire il valore dell'attributo User-Role di Aruba. In seguito, sarà possibile configurare il ruolo utente locale sul WLC di Aruba con lo stesso nome.

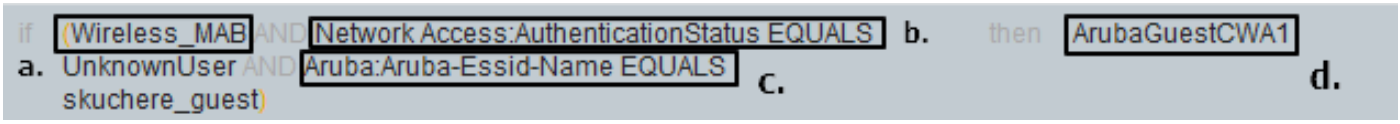
Passaggio 3. Configurare i criteri di autorizzazione.

Il primo criterio di autorizzazione è responsabile del reindirizzamento dell'utente al portale guest. Nel caso più semplice, è possibile utilizzare la condizione composta

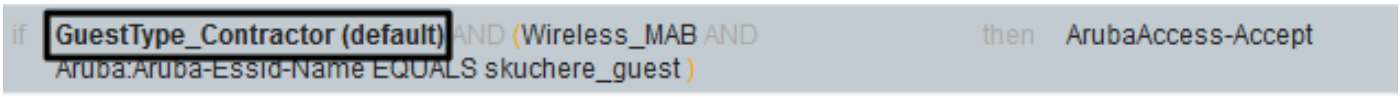
- Wireless_MAB (a.) e
- Autenticazione di accesso alla reteStatus uguale a Unknown user (b.) e
- Aruba Aruba-Essid-Name è uguale al nome SSID dell'ospite (c.).

Per questo criterio, configurare il profilo di autorizzazione con il conseguente reindirizzamento al

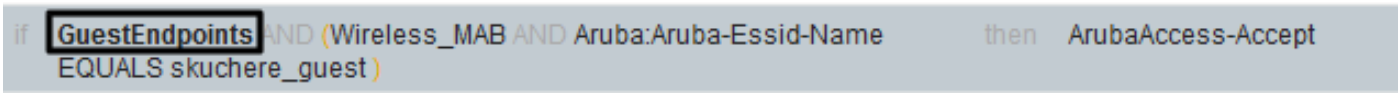
portale guest (d.)



I criteri di seconda autorizzazione devono consentire l'accesso per gli utenti guest dopo l'autenticazione tramite il portale. Questo criterio può basarsi sui dati della sessione (gruppo di identità utente/flusso guest Use Case e così via). In questo scenario è necessario riconnettersi prima della scadenza del timer di unione sessioni:



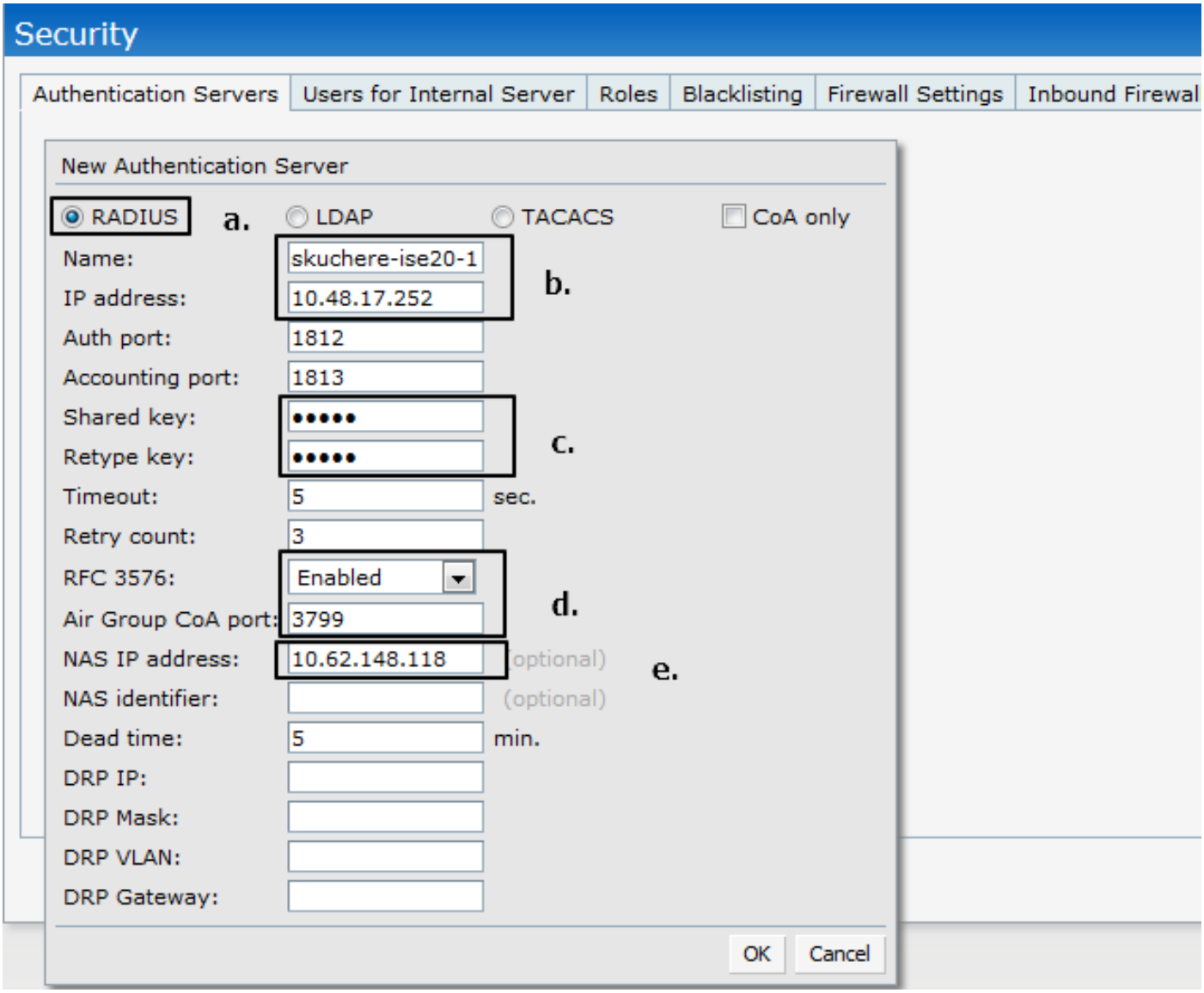
Per proteggersi dalla scadenza del timer di unione sessioni, è possibile fare affidamento sui dati dell'endpoint anziché sui dati della sessione. Per impostazione predefinita, il portale guest sponsorizzato in ISE 2.0 è configurato per la registrazione automatica dei dispositivi guest (il dispositivo guest viene inserito automaticamente nel gruppo di identità endpoint Guest_Endpoints). Questo gruppo può essere utilizzato come condizione:



Criteri di autorizzazione nell'ordine corretto:

Passaggio 4. Configurare il server Radius su Aruba.

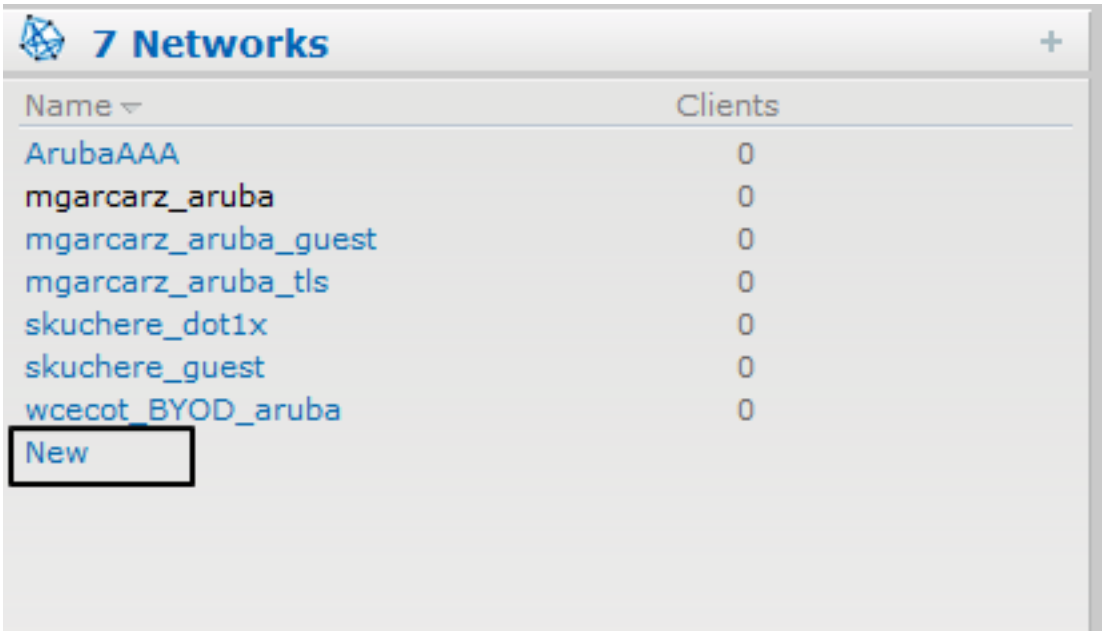
Selezionare **Protezione > Server di autenticazione** e fare clic su **Nuovo:**



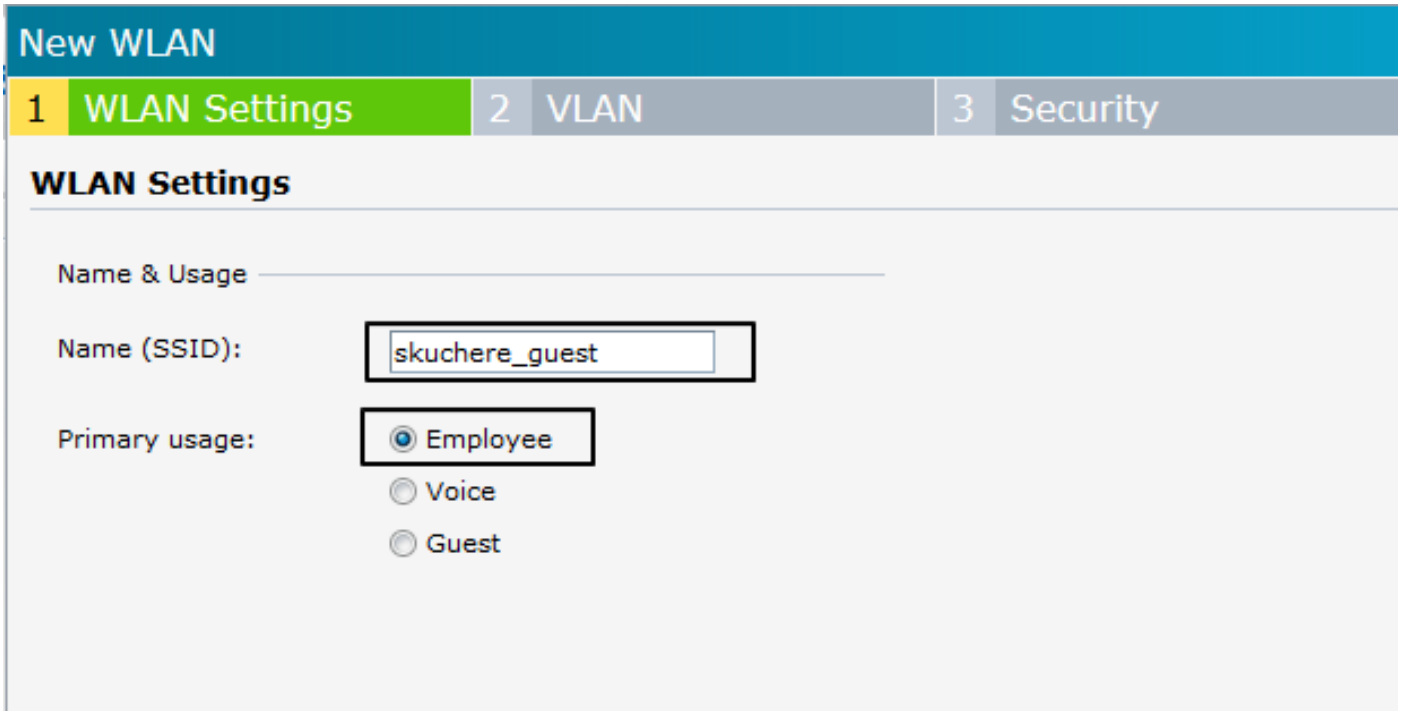
1. Scegliere RADIUS come protocollo AAA.
2. Definire il nome e l'indirizzo IP del server AAA.
3. Specificare una chiave già condivisa.
4. Abilitare il supporto della RFC 3576 e definire la porta COA.
5. Specificare l'indirizzo IP dell'interfaccia di gestione WLC Aruba come indirizzo IP NAS.

Passaggio 5. Creare un SSID guest su Aruba.

Nella pagina del dashboard selezionare **Nuovo** alla fine dell'elenco della rete. Avviare la creazione guidata SSID. Seguire i passaggi della procedura guidata.

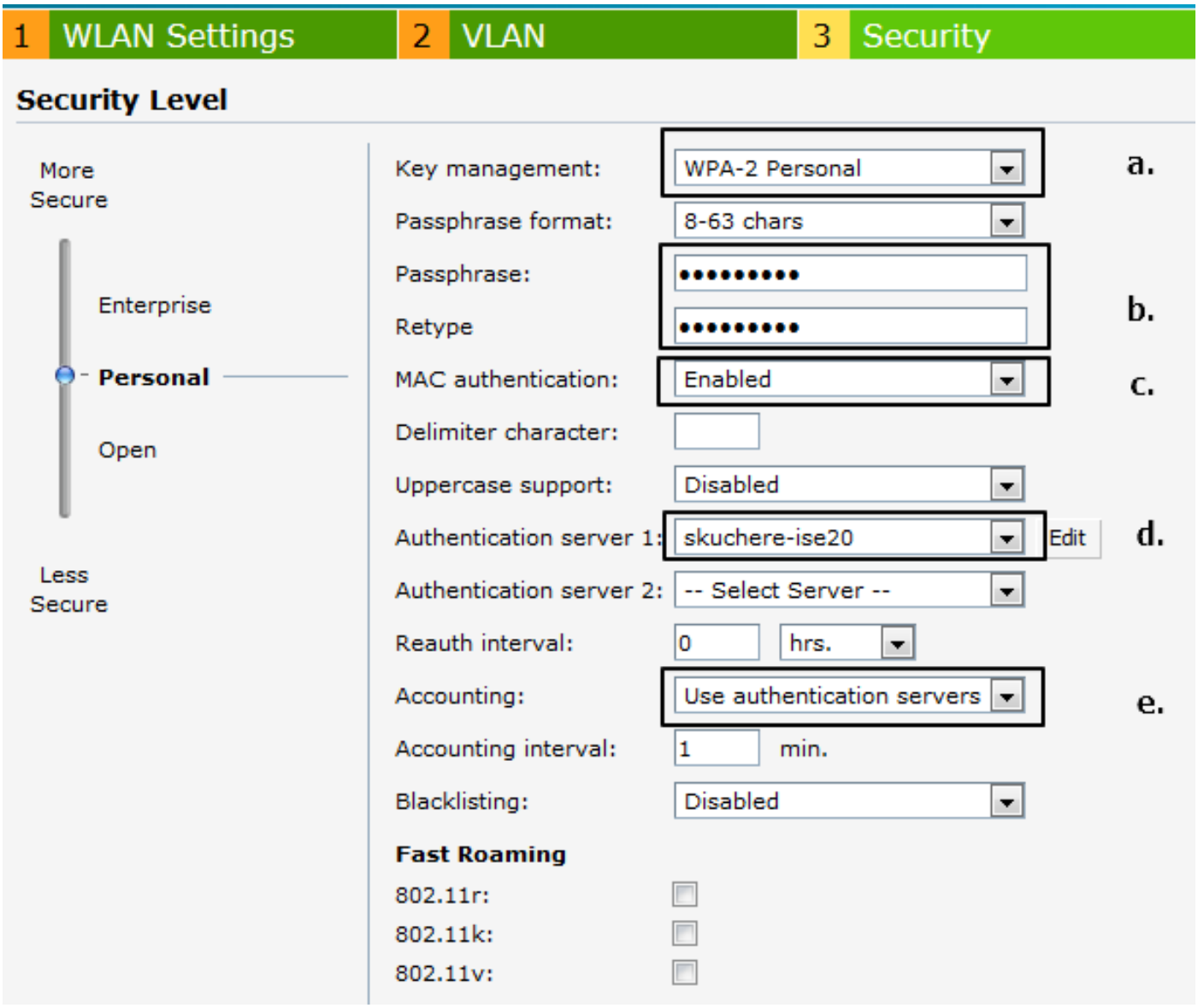


Passaggio 1. Definire il nome SSID e selezionare il tipo SSID. In questo caso, viene utilizzato il tipo SSID Dipendente. Questo tipo di SSID dispone del ruolo predefinito con l'applicazione di tutti i diritti consentiti e nessuna applicazione di portale vincolato. È inoltre possibile scegliere il tipo Guest. In questo scenario è necessario definire le impostazioni del portale vincolato durante la configurazione SSID.



Passaggio 2. Assegnazione di VLAN e indirizzi IP. Qui le impostazioni sono lasciate come predefinite, come mostrato nell'immagine.

Passaggio 3. Impostazioni di protezione. Per SSID guest è possibile selezionare Aperto o Personale. La chiave personale richiede una chiave già condivisa.



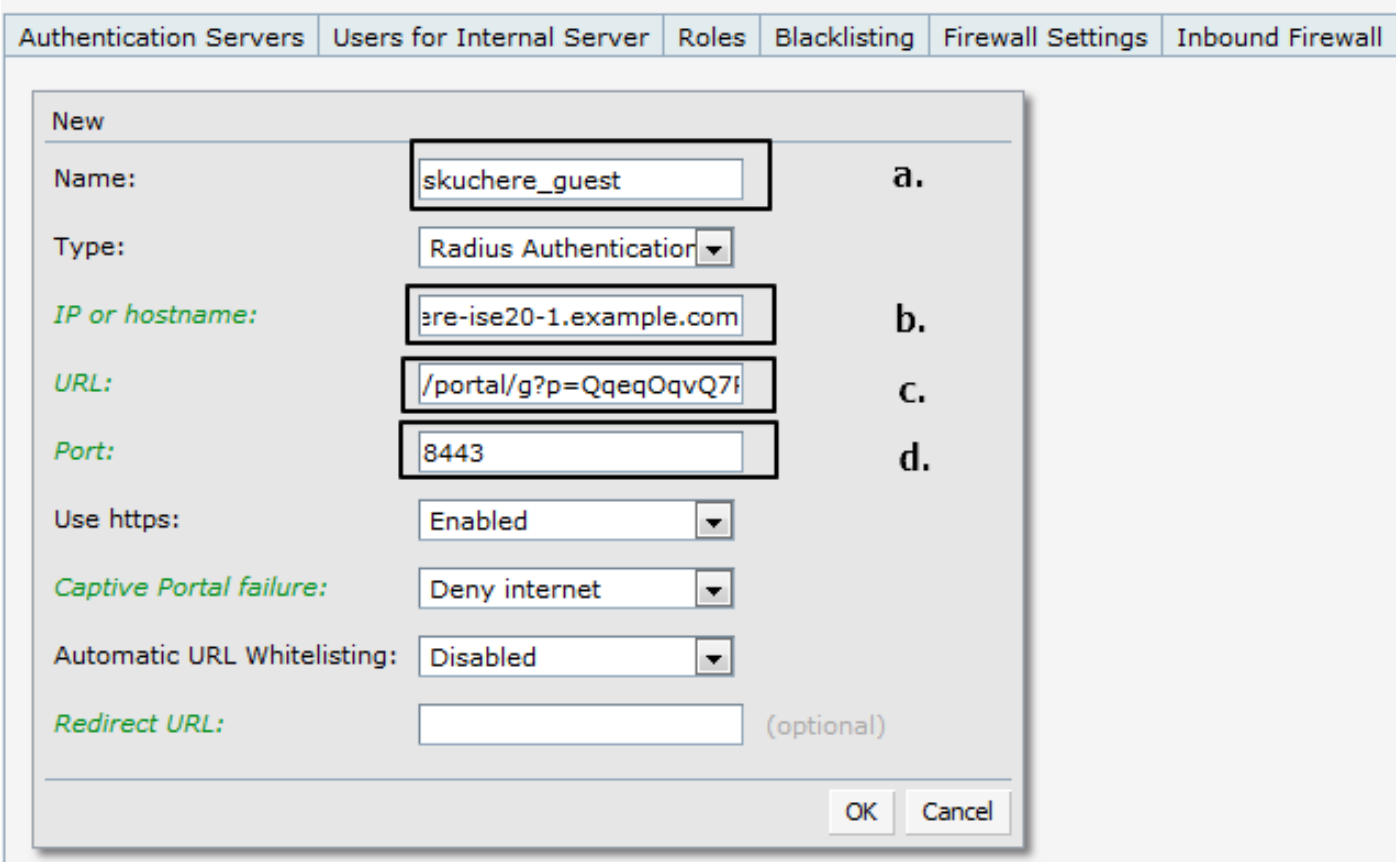
1. Scegliere il meccanismo di gestione delle chiavi.
2. Definire la chiave già condivisa.
3. Per autenticare l'utente ad ISE usando il filtro MAC MAB, occorre abilitarlo.
4. Nell'elenco dei server di autenticazione scegliere il server AAA.
5. Per abilitare l'accounting verso un server AAA definito in precedenza, scegliere Usa server di

autenticazione nell'elenco a discesa.

Nota: La contabilità è fondamentale con i NAD di terza parte. Se Policy Service Node (PSN) non riceve Accounting-Stop per l'utente da NAD, la sessione potrebbe rimanere bloccata nello stato Avviato.

Passaggio 6. Configurare Captive Portal.

Passare a **Sicurezza > Portali esterni in cattività** e creare un nuovo portale, come mostrato nell'immagine:



Passaggio 1. Specificare il nome del portale vincolato.

Steo 2. Definire il FQDN o l'indirizzo IP di ISE. Se si utilizza un indirizzo IP, verificare che tale indirizzo IP sia definito nel campo Nome alternativo soggetto (SAN) del certificato del portale guest.

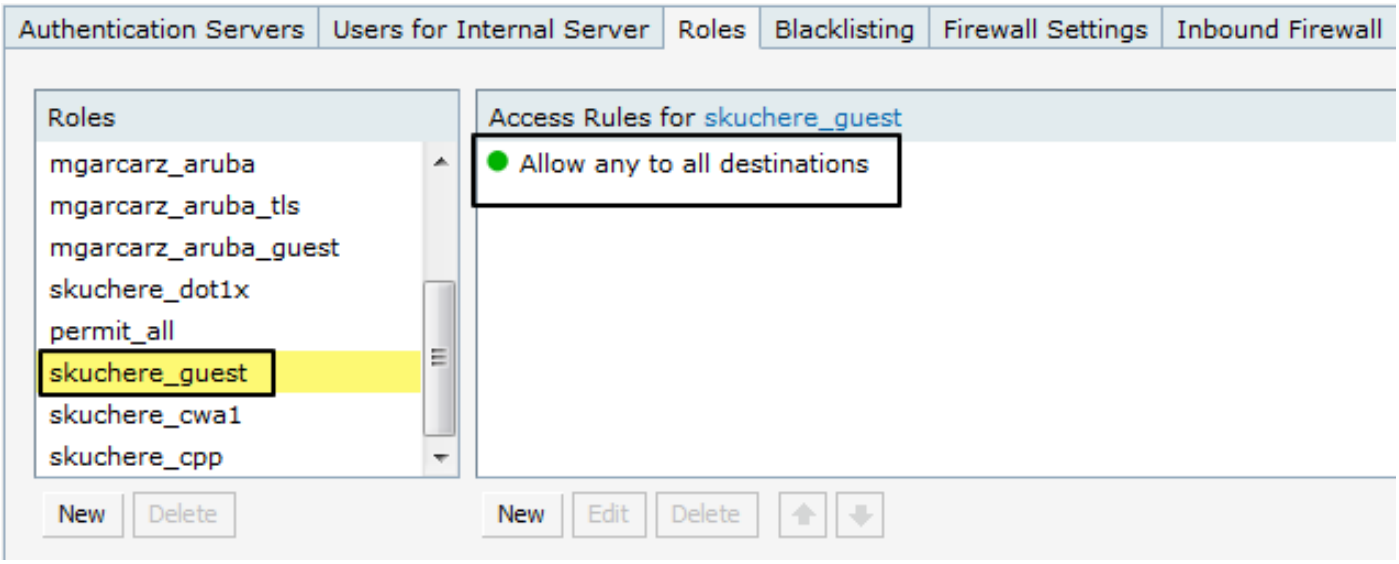
Nota: È possibile utilizzare qualsiasi server PSN, ma l'utente deve essere sempre reindirizzato al server in cui si è verificato il MAB. In genere è necessario definire il nome di dominio completo (FQDN) del server Radius configurato su SSID.

Passaggio 3. Fornire il reindirizzamento dal profilo di autorizzazione ISE. Inserire qui la parte dopo il numero di porta,

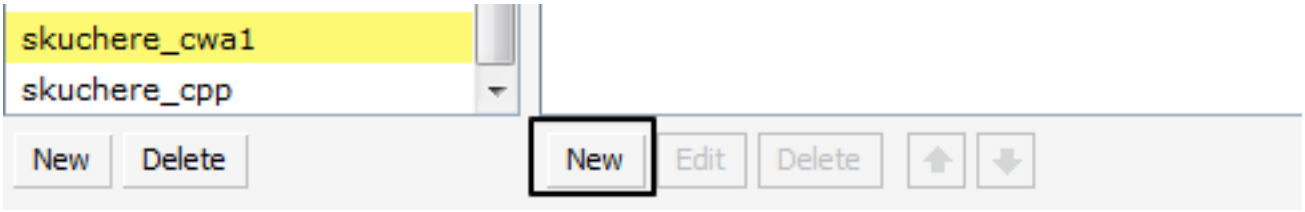
Passaggio 4. Definire la porta del portale guest ISE.

Passaggio 7. Configurazione dei ruoli utente.

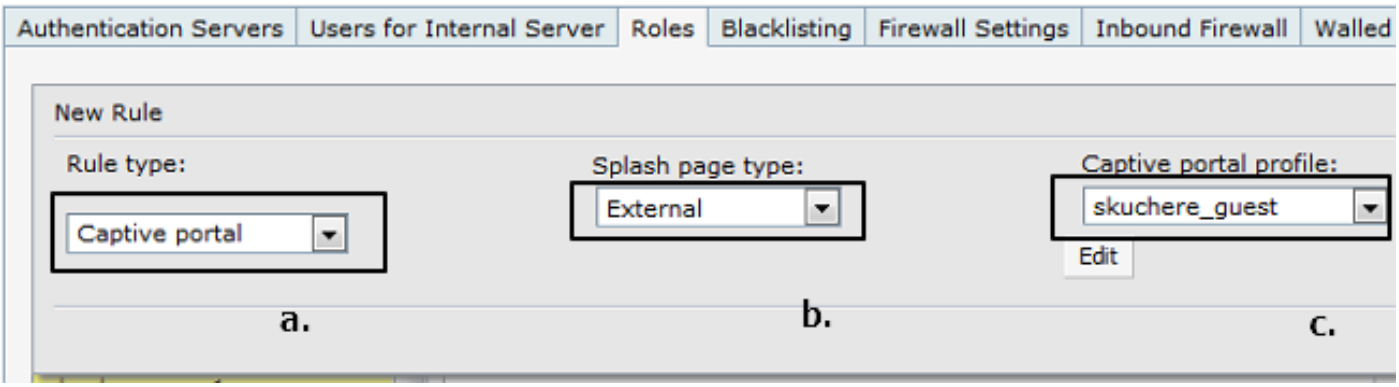
Passare a **Sicurezza > Ruoli.** Dopo la creazione di SSID, verificare che nell'elenco sia presente un nuovo ruolo con lo stesso nome con la regola di accesso che consente qualsiasi a tutte le destinazioni. Inoltre, creare due ruoli: una per il reindirizzamento di CWA e una seconda per consentire l'accesso dopo l'autenticazione sui portali guest. I nomi di questi ruoli devono essere identici al ruolo utente Aruba definito nei profili di autorizzazione ISE.



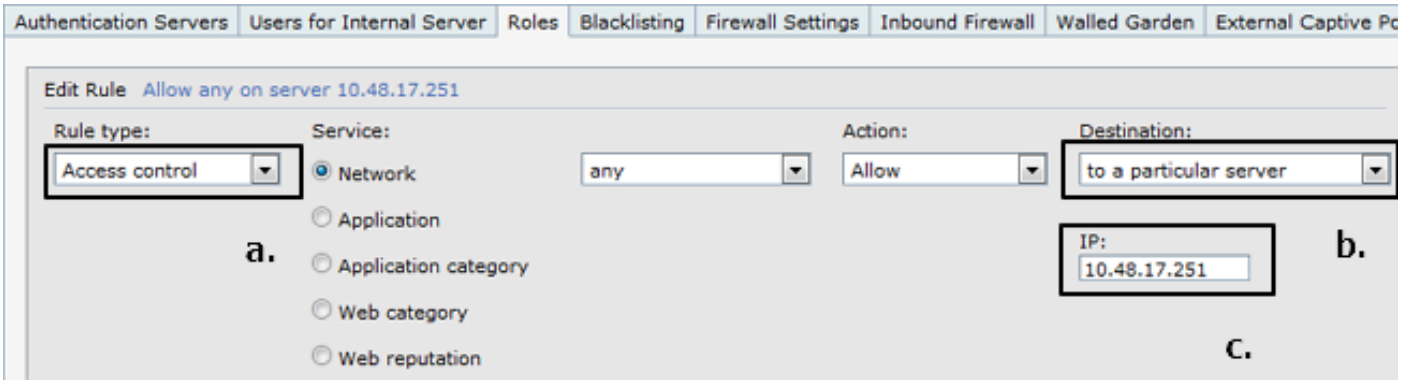
Come mostrato nell'immagine, creare un nuovo ruolo utente per il reindirizzamento e aggiungere la restrizione di protezione.



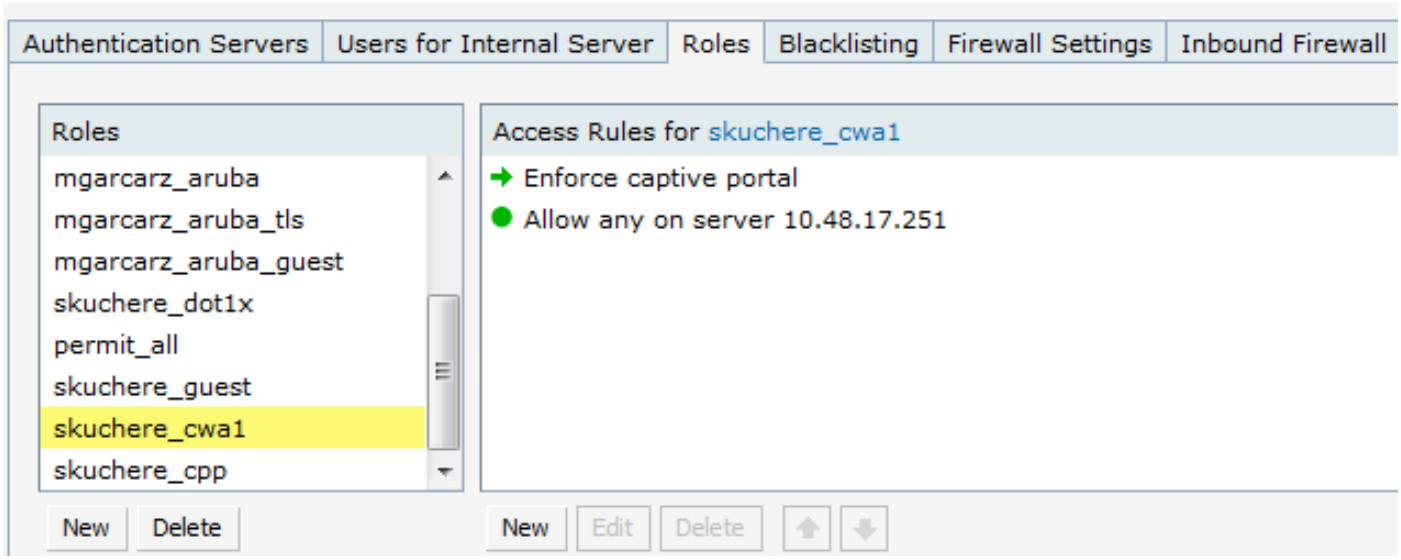
Per la prima restrizione è necessario definire:



Per la seconda restrizione è necessario definire:

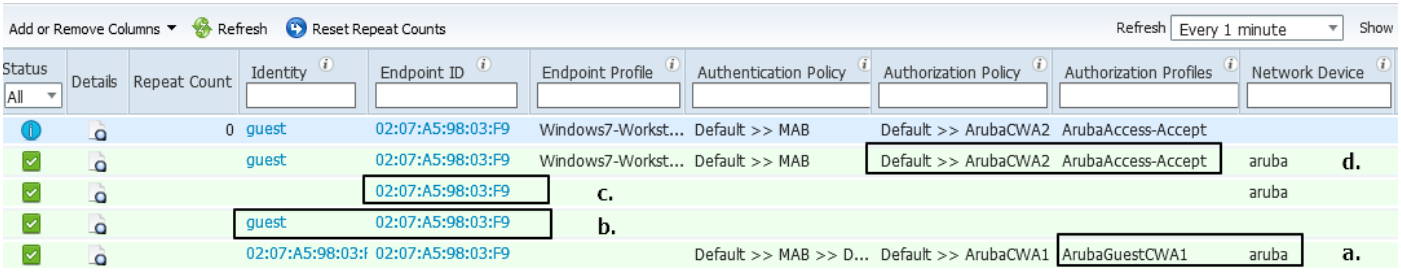


Come mostrato nell'immagine, la regola predefinita Consenti a tutte le destinazioni può essere eliminata. Questo è il risultato del riepilogo della configurazione del ruolo.



Verifica

Esempio di flusso guest in ISE **Operations > Radius Livelog**.



1. Primo MAB e, di conseguenza, un profilo di autorizzazione con reindirizzamento CWA e ruolo utente con portale vincolato configurato sul lato Aruba.
2. Autenticazione Guest.
3. Modifica di autorizzazione (CoA) completata.
4. Secondo MAB e, di conseguenza, un profilo di autorizzazione con permesso di accesso e ruolo utente che ha permesso tutte le regole sul lato Aruba.

Sul lato Aruba è possibile usare il comando **show clients** per assicurarsi che l'utente sia connesso, che l'indirizzo IP sia assegnato e che il ruolo utente corretto sia assegnato come risultato dell'autenticazione:

```
04:bd:88:c3:88:14# show clients

Client List
-----------
Name              IP Address    MAC Address        OS     Network        Access Point       Channel  Type  Role
----              ----------    -----------        --     -------        ------------       -------  ----  ----
02-07-A5-98-03-F9  10.62.148.77  02:07:a5:98:03:f9  Win 7  skuchere_guest  04:bd:88:c3:88:14  11       GN    skuchere_cwa1
Number of Clients   :1
Info timestamp      :92552
```

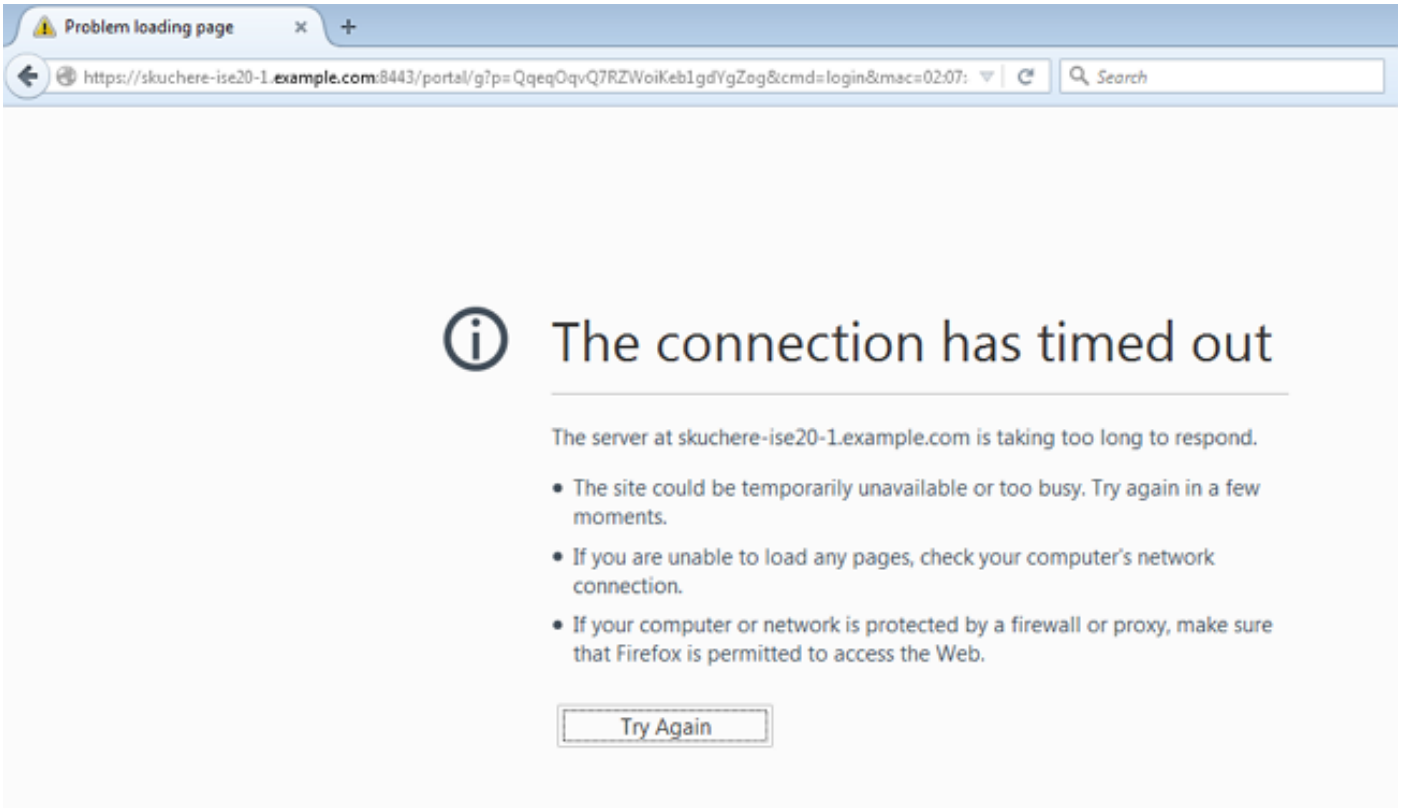
Risoluzione dei problemi

Errore COA

Nelle impostazioni ISE, verificare che Aruba NAD sia configurato con il tipo di dispositivo di rete corretto sul lato ISE e che la porta COA sia definita correttamente nelle impostazioni NAD. Sul lato Aruba, verificare che la RFC 3576 sia abilitata nelle impostazioni del server di autenticazione e che la porta COA sia definita correttamente. Dal punto di vista della rete, verificare che la porta UDP 3799 sia consentita tra ISE e Aruba WLC.

Reindirizza problema

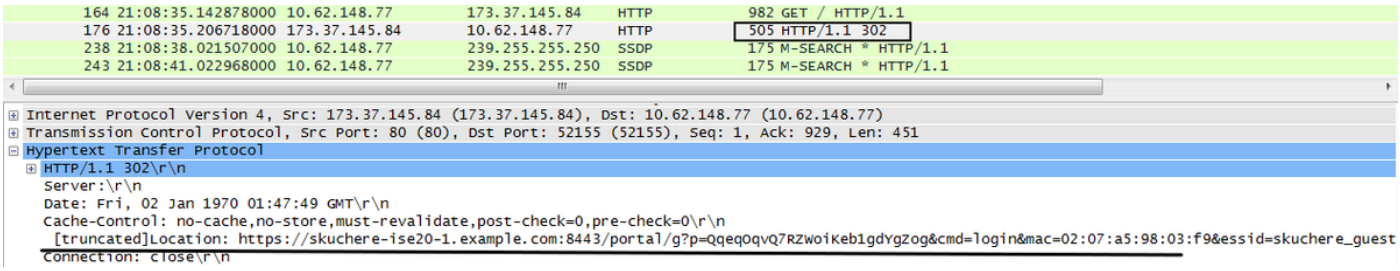
L'utente vede l'URL ISE nel browser, ma la pagina ISE non viene visualizzata, come mostrato nell'immagine:



Sul lato utente, verificare che l'FQDN ISE possa essere risolto correttamente per correggere l'IP. Su Aruba, verificare che l'URL ISE sia definito correttamente nelle impostazioni del portale riservato e che il traffico verso ISE sia consentito nelle restrizioni di accesso al ruolo utente. Verificare inoltre che il server Radius su SSID e il PSN ISE nelle impostazioni del portale captive siano sullo stesso dispositivo. Dal punto di vista della rete, verificare che la porta TCP 8443 sia consentita dal segmento utente a ISE.

Nessun URL di reindirizzamento presente nel browser

Sul lato utente, verificare che, come risultato di ogni richiesta HTTP, Aruba WLC restituisca il codice HTTP 302 pagina spostata con l'URL ISE.



Timer di unione sessioni scaduto

In genere, questo problema si verifica quando l'utente viene reindirizzato per la seconda volta al portale guest. In questo caso, in ISE Radius Livelog dovrebbe essere visualizzato che dopo il COA per la seconda autenticazione il profilo di autorizzazione con CWA è stato selezionato di nuovo. Sul lato Aruba, controllare il ruolo utente effettivo con l'aiuto del comando **show clients**.

Per risolvere questo problema, è possibile utilizzare i criteri di autorizzazione basati sull'endpoint in ISE per le connessioni dopo l'autenticazione guest.