Risoluzione dei problemi comuni di accesso guest ad ISE

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi comuni dei guest nella distribuzione, come isolare e controllare il problema e come provare soluzioni semplici.

Prerequisito

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione guest ISE
- Configurazione CoA su dispositivi di accesso alla rete (NAD)
- Sono necessari strumenti di acquisizione sulle workstation.

Componenti usati

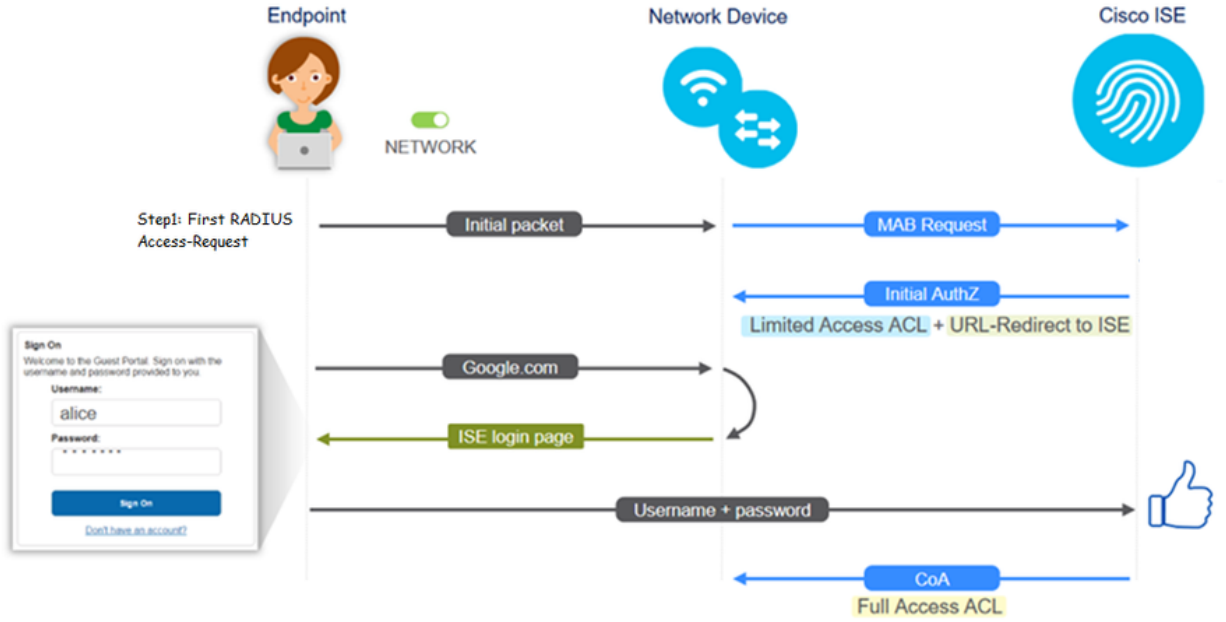
Le informazioni di questo documento si basano Cisco ISE, release 2.6, e:

- WLC 5500
- Catalyst switch 3850 versione 15.x
- Workstation Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Flusso guest

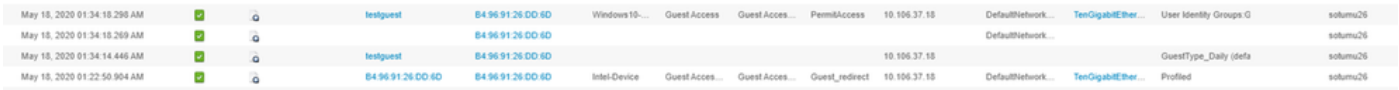
La panoramica del flusso guest è simile alle impostazioni cablate o wireless. Questa immagine del diagramma di flusso può essere utilizzata come riferimento in tutto il documento. Consente di visualizzare il passo e l'entità.



Il flusso può essere seguito anche sui log ISE live [**Operations > RADIUS Live Log**] filtrando l'ID dell'endpoint:

- Autenticazione MAB riuscita - il campo username contiene l'indirizzo MAC - URL è stato inviato al NAD - L'utente ottiene il portale
- Autenticazione guest riuscita: il campo username contiene il nome utente guest, è stato identificato come GuestType_Daily (o il tipo configurato per l'utente guest)
- Avvio CoA - Il campo username è vuoto. Nel report dettagliato è indicato che l'autorizzazione dinamica è stata completata
- Accesso guest fornito

Sequenza di eventi nell'immagine (dal basso in alto)



Guide comuni alla distribuzione

Di seguito sono riportati alcuni collegamenti per l'assistenza alla configurazione. Per la risoluzione dei problemi relativi a casi di utilizzo specifici, è utile conoscere la configurazione ideale o prevista.

- Configurazione guest cablato
- Configurazione guest wireless
- Wireless Guest CWA con punti di accesso FlexAuth

Problemi riscontrati frequentemente

Questo documento tratta principalmente i seguenti argomenti:

Il reindirizzamento al portale guest non funziona

Dopo aver rimosso l'URL di reindirizzamento e l'ACL da ISE, verificare quanto segue:

1. Lo stato del client sullo switch (in caso di accesso guest via cavo) con il comando **show authentication session int <interface> restituisce i dettagli**:

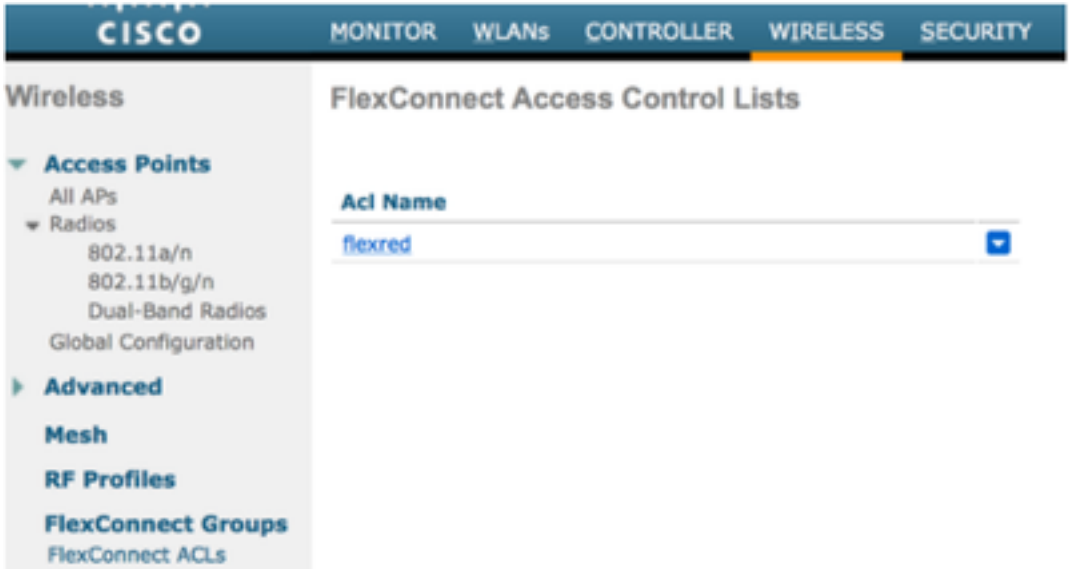
```
guestlab#sh auth sess int T1/0/48 de
            Interface:  TenGigabitEthernet1/0/48
              IIF-ID:  0x1096380000001DC
         MAC Address:  b496.9126.dd6d
        IPv6 Address:  Unknown
        IPv4 Address:  10.106.37.18
           User-Name:  B4-96-91-26-DD-6D
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
     Restart timeout:  N/A
   Common Session ID:  0A6A25110000012652C64B014
     Acct Session ID:  0x0000124F
              Handle:  0x5E00014D
      Current Policy:  POLICY_Te1/0/48

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:

        URL Redirect:  https://10.127.197.212:8443/portal/gateway?sessionId=0A6
A25110000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
     URL Redirect ACL:  REDIRECT_ACL

Method status list:
      Method           State
      mab              Authc Success
```

2. Stato del client sul controller LAN wireless (se l'accesso guest wireless): **Monitor > Client > Indirizzo MAC**

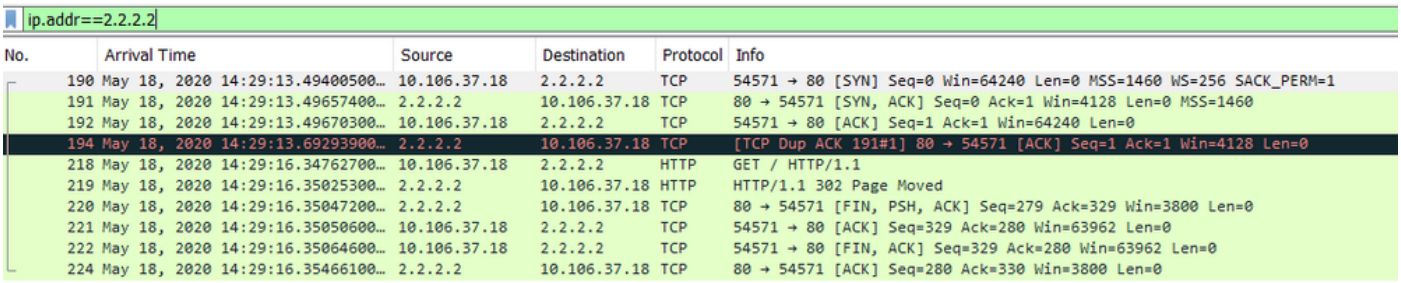
3. La raggiungibilità dall'endpoint all'ISE sulla porta TCP 8443 con l'aiuto del prompt dei comandi: **C:\Users\user>telnet <ISE-IP> 8443**

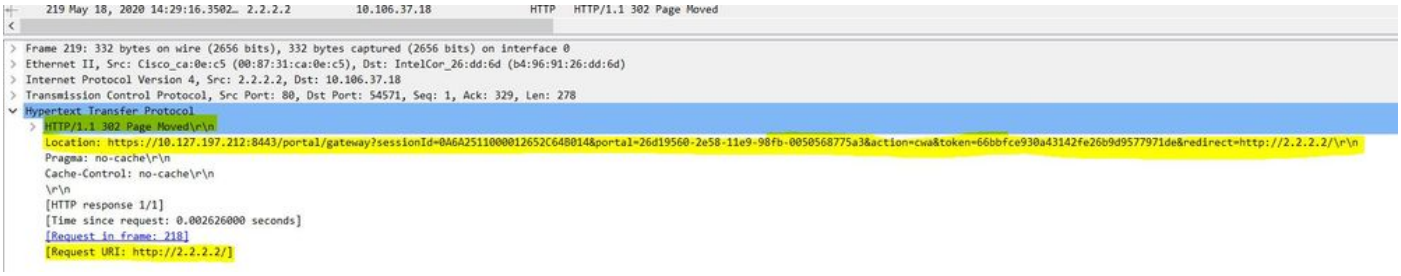
4. Se l'URL di reindirizzamento del portale dispone di un FQDN, verificare se il client è in grado di risolvere dal prompt dei comandi: **C:\Users\user>nslookup guest.ise.com**

5. Nella configurazione della connessione flessibile, verificare che lo stesso nome ACL sia configurato in ACL e ACL flessibili. Verificare inoltre che l'ACL sia mappato agli access point. Per ulteriori informazioni, consultare la guida alla configurazione della sezione precedente - Fasi 7 b e c.



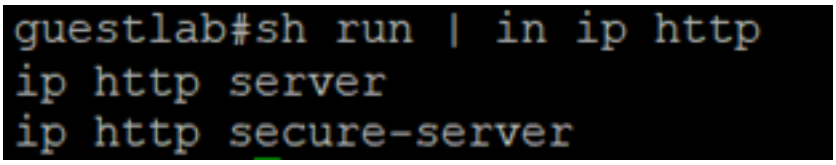
6. Acquisire un pacchetto dal client e verificare se è presente il reindirizzamento. La pagina HTTP/1.1 302 del pacchetto spostato indica che il WLC/switch ha reindirizzato il sito visitato al portale guest ISE (URL reindirizzato):





7. Il motore HTTP(s) è abilitato sui dispositivi di accesso alla rete:

Sullo switch:



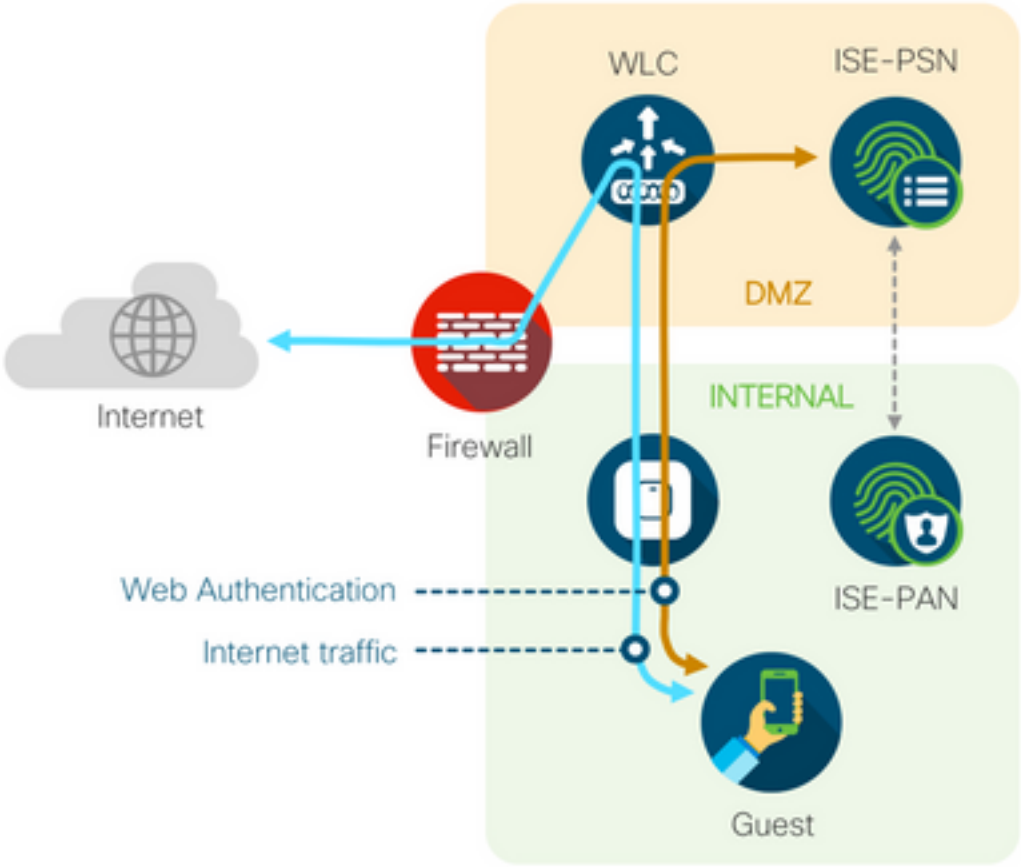
Sul WLC:

8. Se il WLC si trova in una configurazione con un ancoraggio esterno, verificare quanto segue:

Passaggio 1. Lo stato del client deve essere lo stesso su entrambi i WLC.

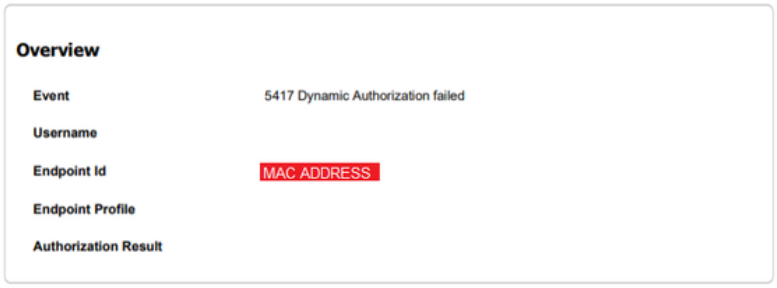
Passaggio 2. L'URL di reindirizzamento deve essere visualizzato su entrambi i WLC.

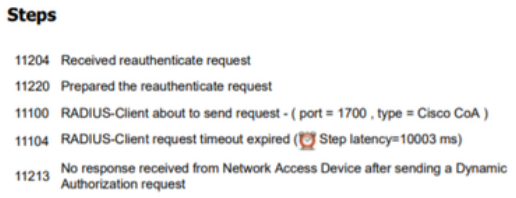
Passaggio 3. L'accounting RADIUS deve essere disabilitato sul WLC di ancoraggio.



Autorizzazione dinamica non riuscita

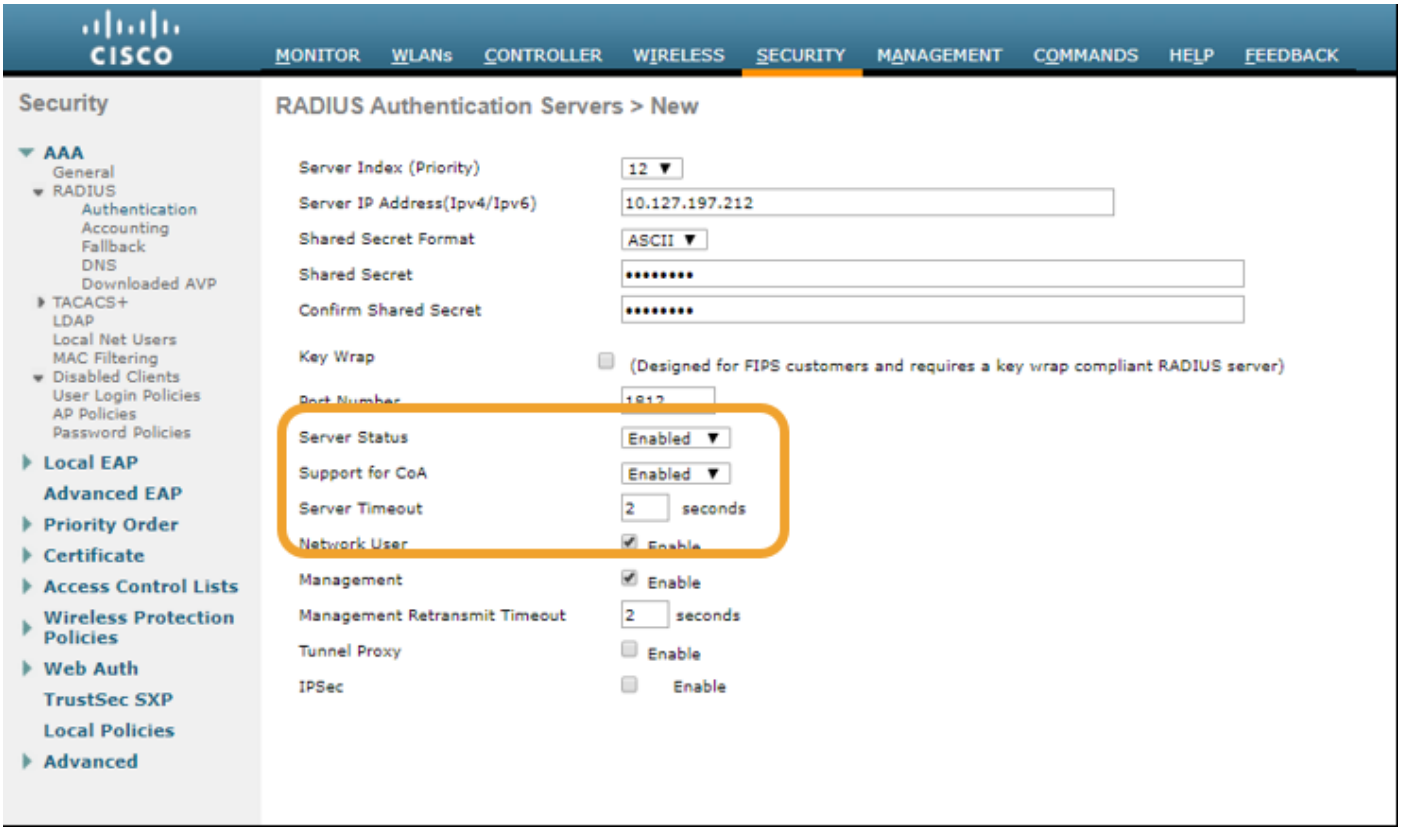
Se l'utente finale è in grado di accedere al portale guest e di eseguire correttamente l'accesso, il passaggio successivo consiste in una modifica dell'autorizzazione per concedere all'utente l'accesso guest completo. Se l'operazione non riesce, sui log live ISE Radius si verifica un errore di autorizzazione dinamica. Per risolvere il problema, verificare quanto segue:





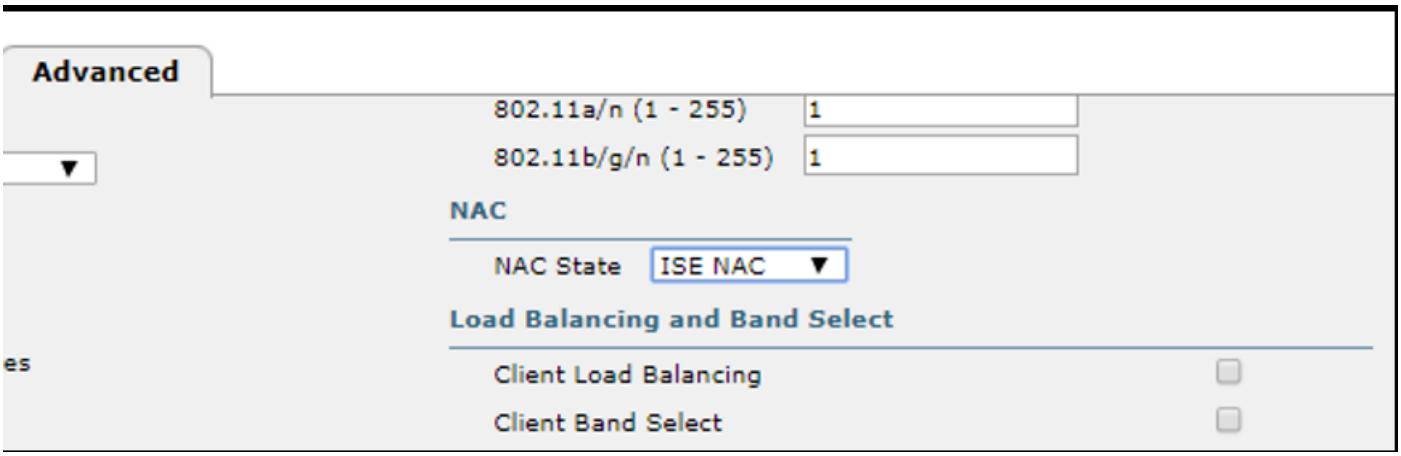
1. Il cambiamento di autorizzazione (CoA) deve essere abilitato/configurato sul NAD:

```
!
aaa server radius dynamic-author
 client 10.127.197.209 server-key cisco123
 client 10.127.197.212 server-key cisco123
!
```



2. La porta UDP 1700 deve essere consentita sul firewall.

3. Lo stato NAC sul WLC non è corretto. In Advanced settings on **WLC GUI > WLAN (**Impostazioni avanzate su **WLC GUI >** WLAN) modificare lo stato del NAC su ISE NAC (ISE NAC).

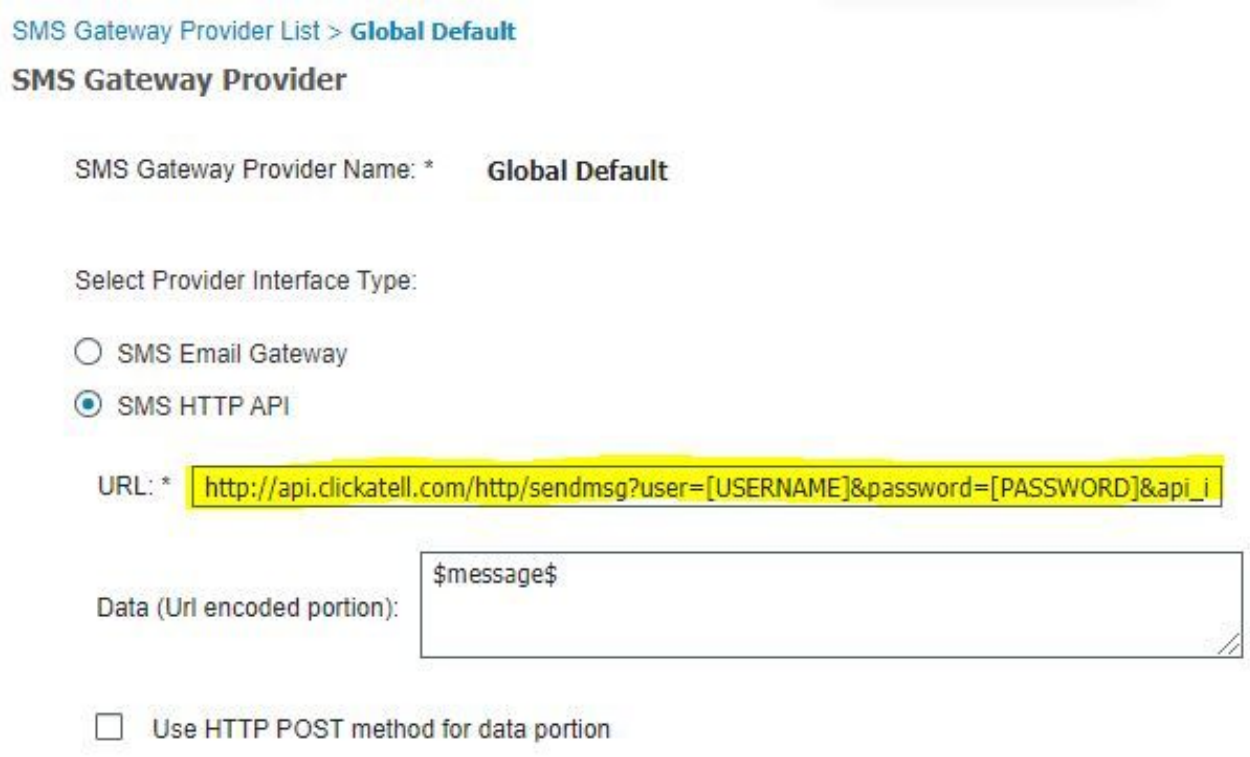


Notifiche via SMS/e-mail non inviate

1. Controllare la configurazione SMTP in **Amministrazione > Sistema > Impostazioni > SMTP**.

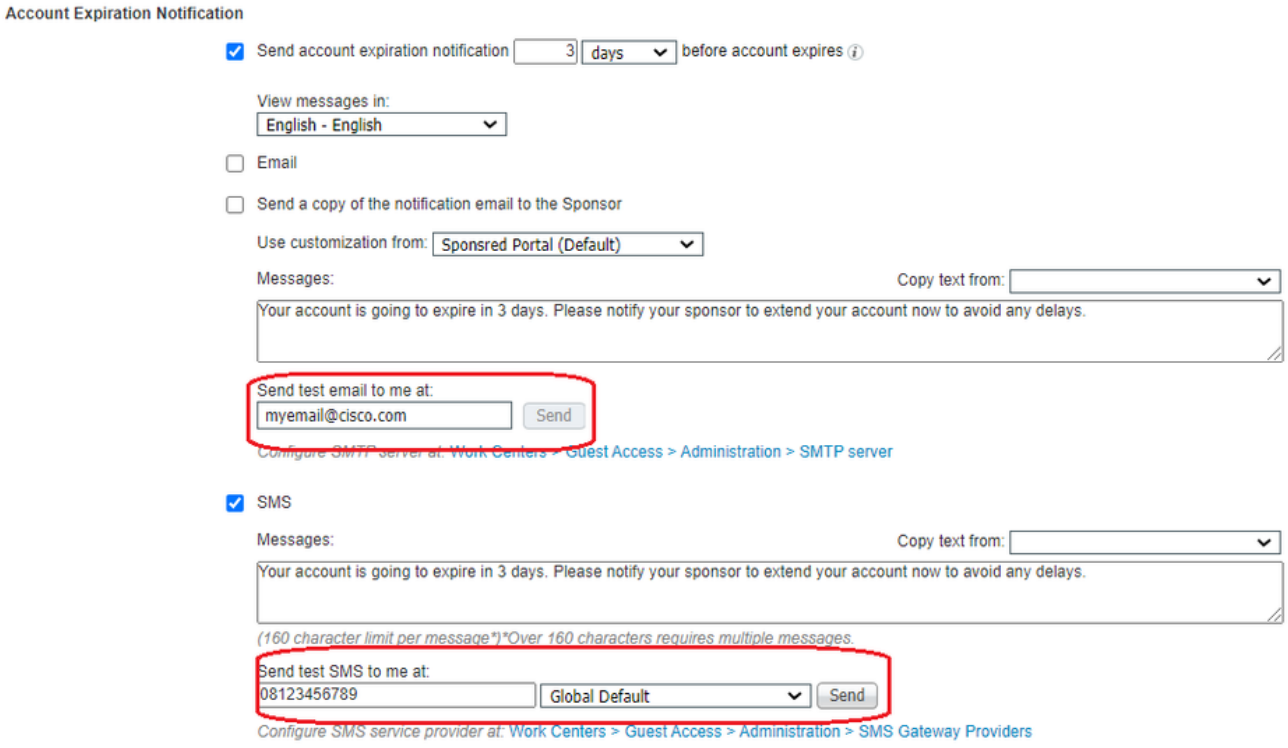
2. Controlla l'API per verificare la presenza di gateway SMS/e-mail all'esterno di ISE:

Verificare gli URL forniti dal fornitore su un client API o un browser, sostituire le variabili come nomi utente, password, numero di cellulare e verificare la raggiungibilità. [**Amministrazione > Sistema > Impostazioni > Gateway SMS**]



In alternativa, se si esegue il test dai gruppi degli sponsor ISE [**Workcenter > Guest Access > Portals and Components > Guest Types**], acquisire un pacchetto su ISE e sul gateway SMS/SMTP per verificare se

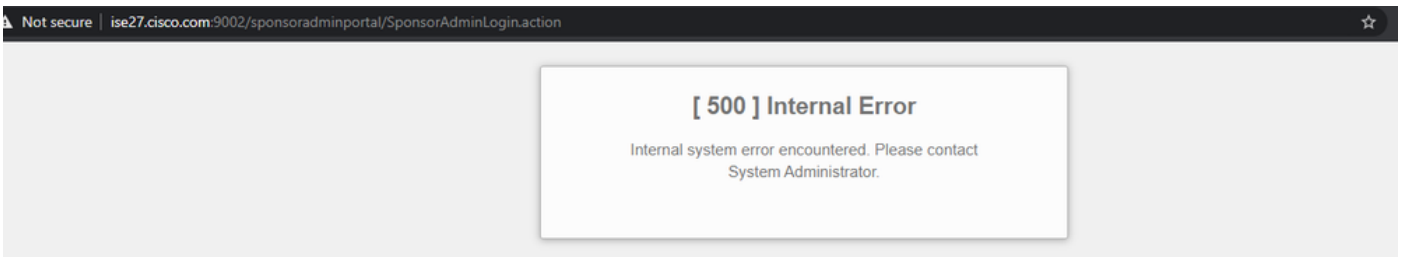
1. Il pacchetto di richiesta raggiunge il server senza errori.
2. Il server ISE dispone delle autorizzazioni/dei privilegi consigliati dal fornitore affinché il gateway possa elaborare la richiesta.



Impossibile raggiungere la pagina Gestisci account

1. Sotto il pulsante **Workcentres > Guest Access > Manage account**, viene reindirizzato all'FQDN

ISE sulla porta 9002, in modo che l'amministratore ISE possa accedere al portale degli sponsor:



2. Verificare se il nome di dominio completo (FQDN) viene risolto dalla workstation da cui si accede al portale sponsor con il comando **nslookup <FQDN of ISE PAN>**.

3. Verificare se la porta TCP 9002 di ISE è aperta dalla CLI di ISE con il comando **show ports | includere 9002**.

Procedure consigliate per i certificati del portale

- Per un'esperienza utente ottimale, il certificato utilizzato per i portali e i ruoli di amministratore deve essere firmato da un'autorità di certificazione pubblica nota (ad esempio: GoDaddy, DigiCert, VeriSign, ecc.), comunemente considerata attendibile dai browser (ad esempio: Google Chrome, Firefox e così via).

- Non è consigliabile utilizzare l'indirizzo IP statico per il reindirizzamento guest, in quanto questo rende l'indirizzo IP privato di ISE visibile a tutti gli utenti. La maggior parte dei fornitori non fornisce certificati di terze parti per l'IP privato.

- Quando si passa da ISE 2.4 p6 a p8 o p9, è presente un bug noto: ID bug Cisco CSCvp75207 dove le caselle **Trust for authentication in ISE** and **Trust for client authentication and Syslog** devono essere selezionate manualmente dopo l'aggiornamento della patch. In questo modo, ISE invia l'intera catena di certificati per il flusso TLS quando si accede al portale guest.

Se queste azioni non risolvono i problemi di accesso dei guest, contattare TAC con un pacchetto di supporto composto dalle istruzioni indicate nel documento Debug da abilitare per ISE.

Informazioni correlate

- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).