Configurazione di ISE Self Registered Guest Portal

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Topologia e flusso

Configurazione

- WLC
- ISE

Verifica

Risoluzione dei problemi

Configurazione opzionale

- Impostazioni registrazione automatica
- Impostazioni guest di accesso
- Impostazioni registrazione dispositivo
- Impostazioni di conformità del dispositivo guest
- Impostazioni BYOD

Account approvati dallo sponsor

Consegna credenziali tramite SMS

Registrazione dispositivo

Postura

BYOD

Modifica della VLAN

Informazioni correlate

Introduzione

Questo documento descrive come configurare e risolvere i problemi relativi alla funzionalità ISE Self Registered Guest Portal.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione ISE e delle conoscenze base sui seguenti argomenti:

- Implementazioni ISE e flussi guest
- Configurazione dei Wireless LAN Controller (WLC)

Componenti usati

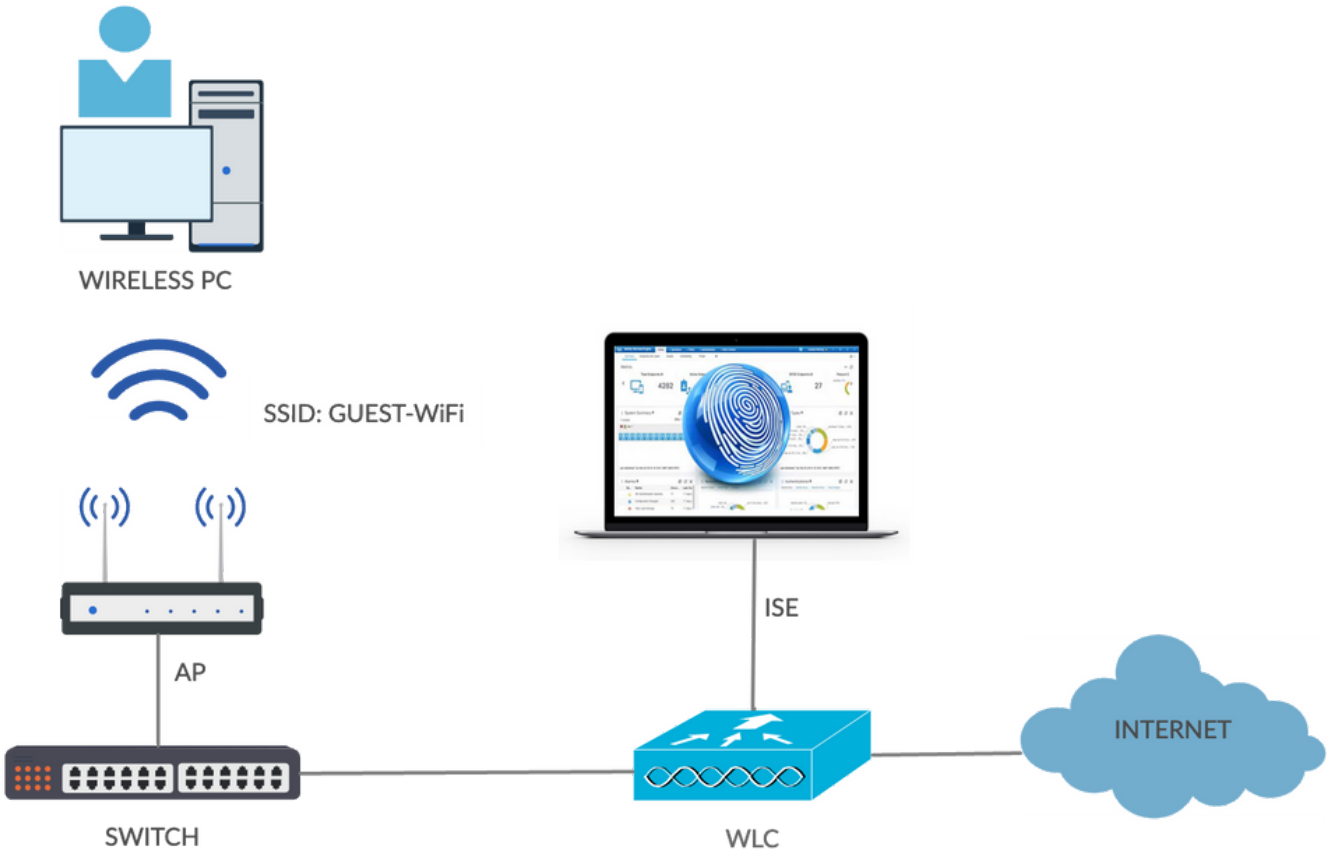
Self Registered Guest Portal, consente agli utenti guest di eseguire la registrazione automatica insieme ai dipendenti per utilizzare le credenziali AD per accedere alle risorse di rete. Questo portale consente di configurare e personalizzare più funzionalità.

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 10 Pro
- Cisco WLC 5508 con versione 8.5.135.0
- Software ISE, versione 3.0

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.

Topologia e flusso



In questo scenario vengono presentate diverse opzioni disponibili per gli utenti guest quando

eseguono la registrazione automatica.

Di seguito è riportato il flusso generale:

Passaggio 1. Utente guest associato a SSID (Service Set Identifier): Guest-WiFi. Questa è una rete aperta con filtro MAC e ISE per l'autenticazione. Questa autenticazione corrisponde alla seconda regola di autorizzazione su ISE e il profilo di autorizzazione reindirizza al portale Guest Self Registered. ISE restituisce un elemento RADIUS Access-Accept con due coppie cisco-av:

- url-redirect-acl (il traffico deve essere reindirizzato e il nome dell'Access Control List (ACL) è definito localmente sul WLC)
- url-redirect (dove reindirizzare il traffico all'ISE)

Passaggio 2. L'utente guest viene reindirizzato ad ISE. Anziché fornire le credenziali per l'accesso, l'utente fa clic su Registra per accesso guest. L'utente viene reindirizzato a una pagina in cui è possibile creare l'account. È possibile attivare un codice di registrazione segreto facoltativo per limitare il privilegio di autoregistrazione agli utenti che conoscono tale valore segreto. Dopo la creazione dell'account, all'utente vengono fornite le credenziali (nome utente e password) e consente di eseguire l'accesso con tali credenziali.

Passaggio 3. L'ISE invia al WLC un messaggio CoA (Change of Authorization) RADIUS autenticato nuovamente. Il WLC autentica nuovamente l'utente quando invia la richiesta di accesso RADIUS con l'attributo Authorize-Only. ISE risponde con ACL Access-Accept e Airespace definiti localmente sul WLC, che fornisce accesso solo a Internet (l'accesso finale per gli utenti guest dipende dalla policy di autorizzazione).

Nota: nelle sessioni EAP (Extensible Authentication Protocol), ISE deve inviare un messaggio CoA Terminate per avviare la riautenticazione perché la sessione EAP è stabilita tra il richiedente e l'ISE. Ma per MAB (filtro MAC), la riautenticazione CoA è sufficiente; non è necessario dissociare/deautenticare il client wireless.

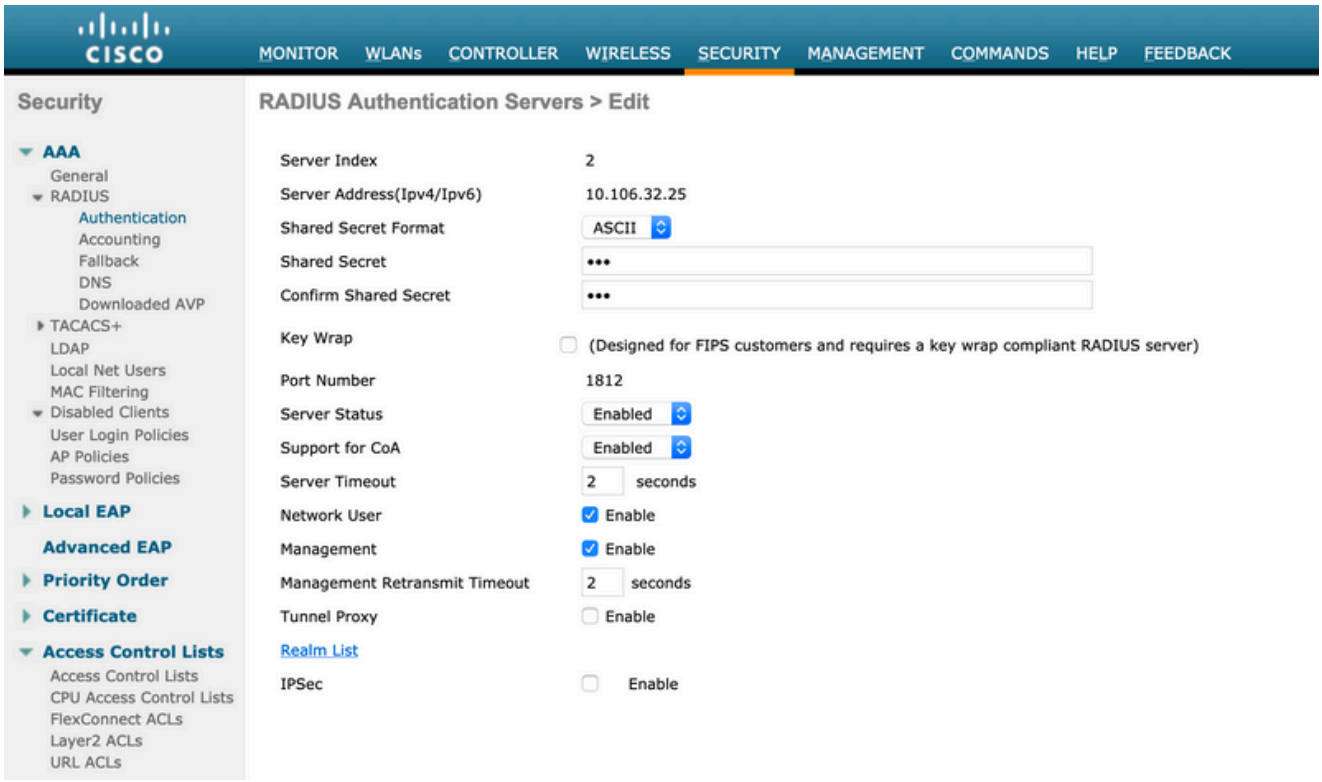
Passaggio 4. L'utente guest ha desiderato accedere alla rete.

È possibile abilitare diverse funzioni aggiuntive, ad esempio la postura e il BYOD (Bring Your Own Device) (illustrate più avanti).

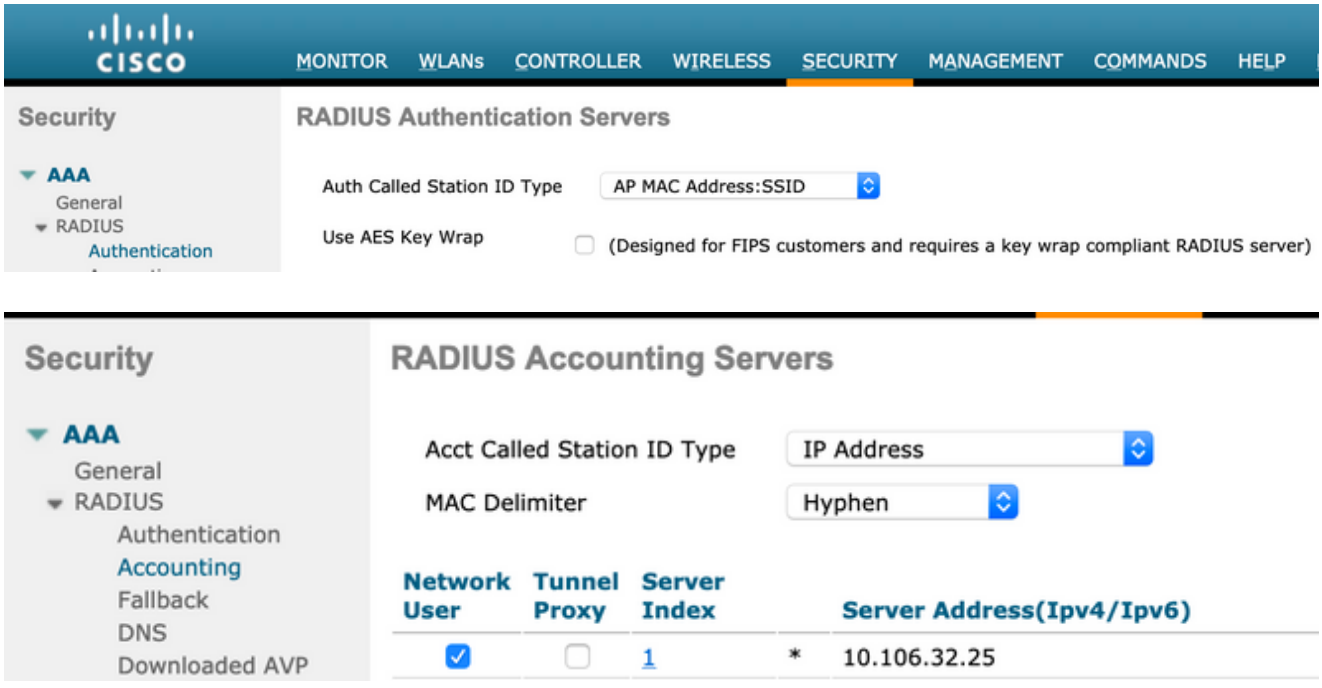
Configurazione

WLC

1. Aggiungere il nuovo server RADIUS per Authentication and Accounting. Selezionare Security > AAA > Radius > Authentication (Sicurezza > AAA > Radius > Autenticazione) per abilitare RADIUS CoA (RFC 3576).



Esiste una configurazione simile per l'accounting. Si consiglia inoltre di configurare il WLC in modo che invii un SSID nell'attributo ID della stazione chiamata, che consente all'ISE di configurare regole flessibili basate su SSID:



2. Nella scheda WLAN, creare la scheda Wireless LAN (WLAN) Guest-WiFi e configurare l'interfaccia corretta. Impostare la sicurezza di layer 2 su None con il filtro MAC. In Server di sicurezza/autenticazione, autorizzazione e accounting (AAA), selezionare l'indirizzo IP ISE per l'autenticazione e l'accounting. Nella scheda Advanced (Avanzate), abilitare AAA Override e impostare lo stato di Network Admission Control (NAC) su ISE NAC (supporto CoA).

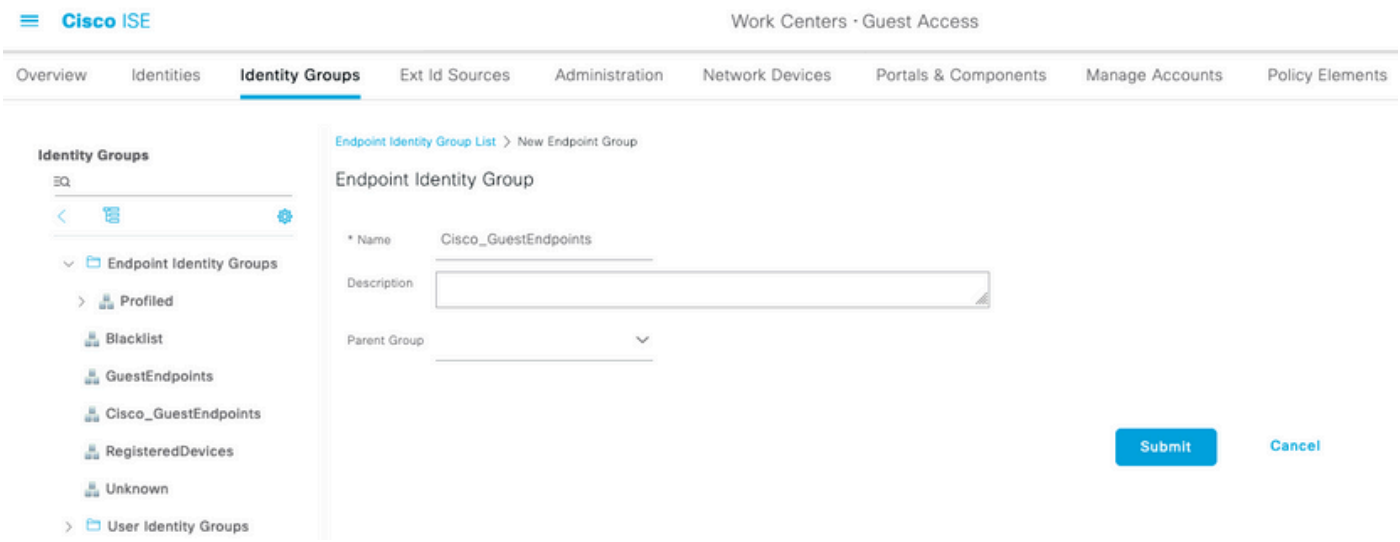
3. Passare a Sicurezza > Liste di controllo dell'accesso > Liste di controllo dell'accesso e creare due elenchi di accesso:

   - GuestRedirect, che consente il traffico che non deve essere reindirizzato e reindirizza tutto il resto del traffico
   - Internet, negata per le reti aziendali e permessa per tutte le altre

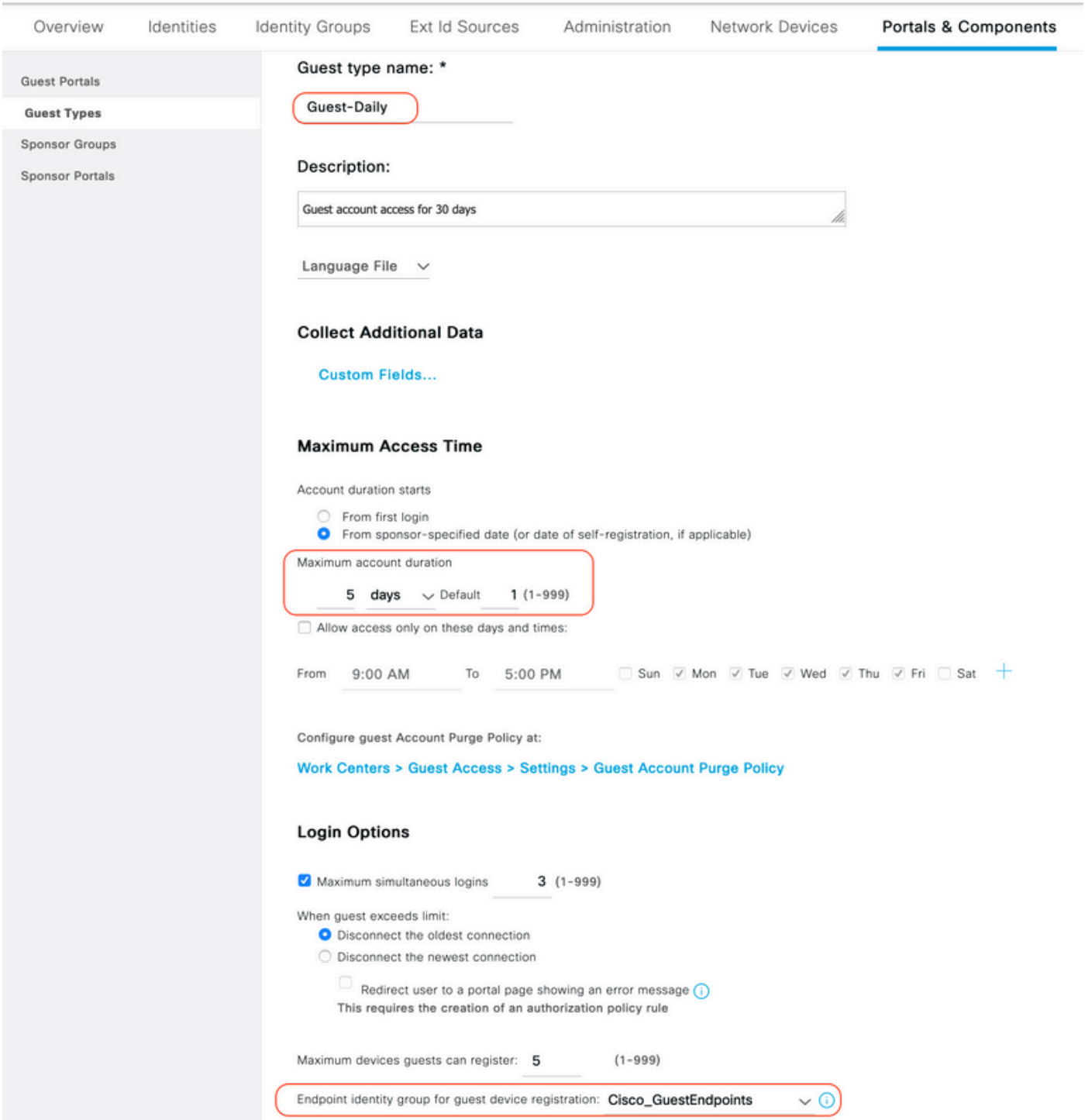
   Di seguito è riportato un esempio di ACL GuestRedirect (è necessario escludere il traffico da/verso ISE dal reindirizzamento):

ISE

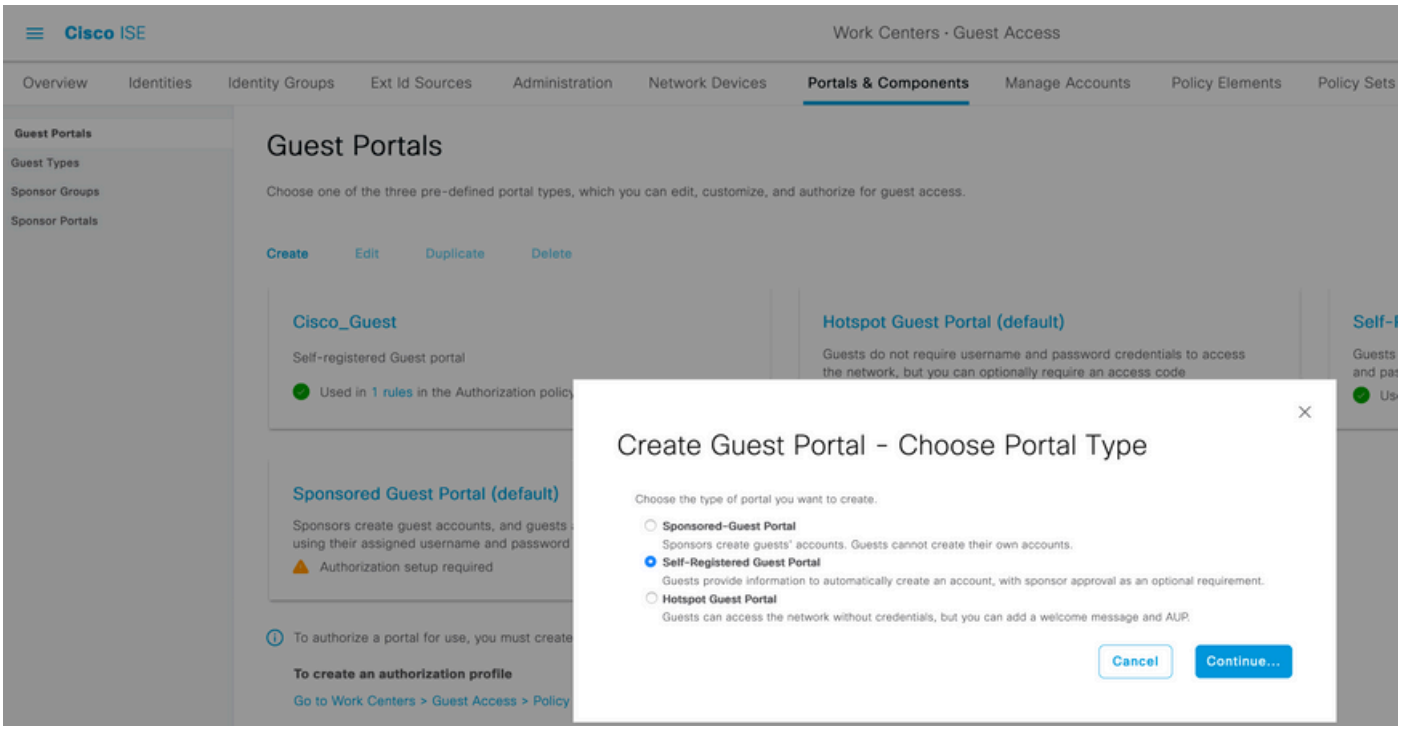
1. Aggiungere il WLC come dispositivo di accesso alla rete dai centri di lavoro > Accesso guest > Dispositivi di rete.
2. Crea gruppo di identità dell'endpoint. Passare a Centri di lavoro > Accesso guest > Gruppi di identità > Gruppi di identità degli endpoint.



3. Creare un tipo di ospite passando a Centri di lavoro > Accesso ospite > Portale e componenti > Tipi di ospite. Fare riferimento al gruppo di identità dell'endpoint creato in precedenza in questo nuovo tipo di ospite e salvataggio.



4. Creare un nuovo tipo di portale guest: Portale guest con registrazione automatica. Passare a Centri di lavoro > Accesso guest > Portali guest.

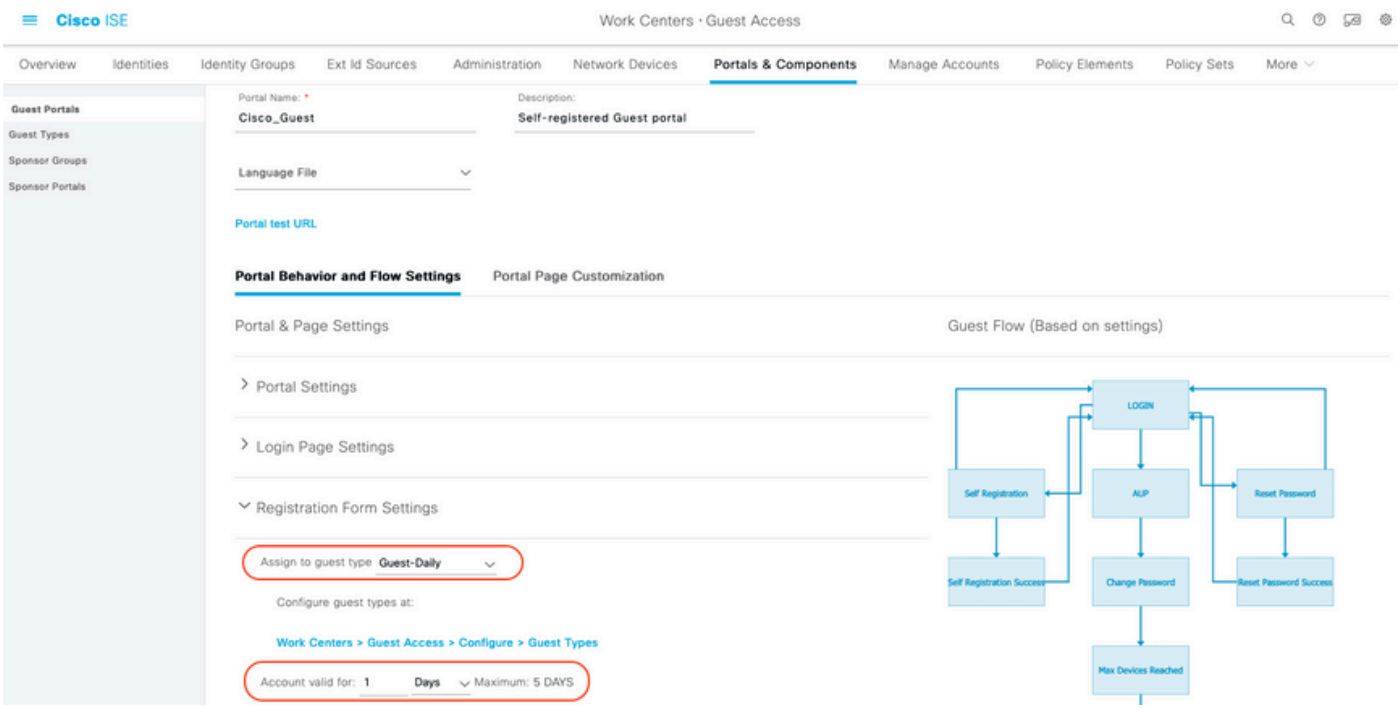


5. Scegliere il nome del portale, fare riferimento al tipo di ospite creato in precedenza e inviare le impostazioni di notifica delle credenziali in Impostazioni modulo di registrazione per inviare le credenziali tramite e-mail.

Per informazioni su come configurare il server SMTP su ISE, consultare il documento:

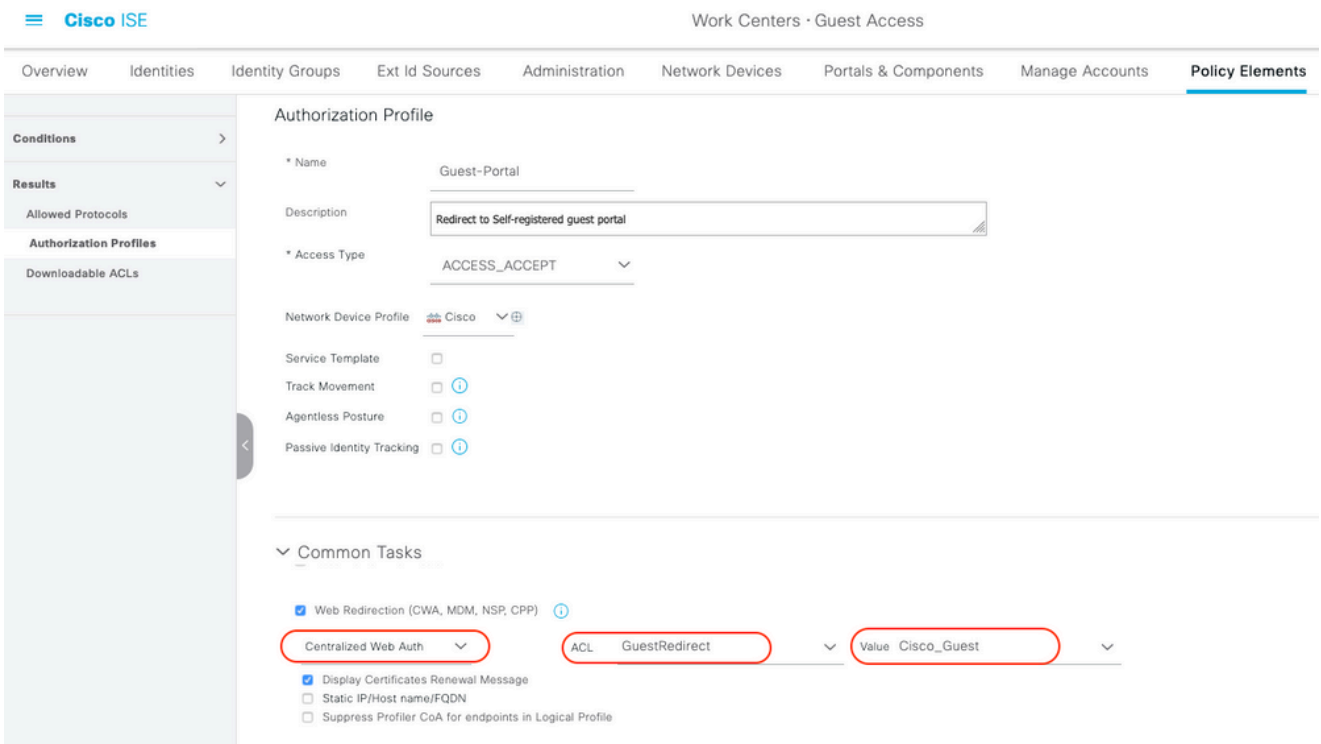
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html

Lasciare tutte le altre impostazioni predefinite. In Personalizzazione pagine portale è possibile personalizzare tutte le pagine presentate. Per impostazione predefinita, l'account Guest è valido per 1 giorno e può essere esteso al numero di giorni configurato in base al tipo di Guest specifico.

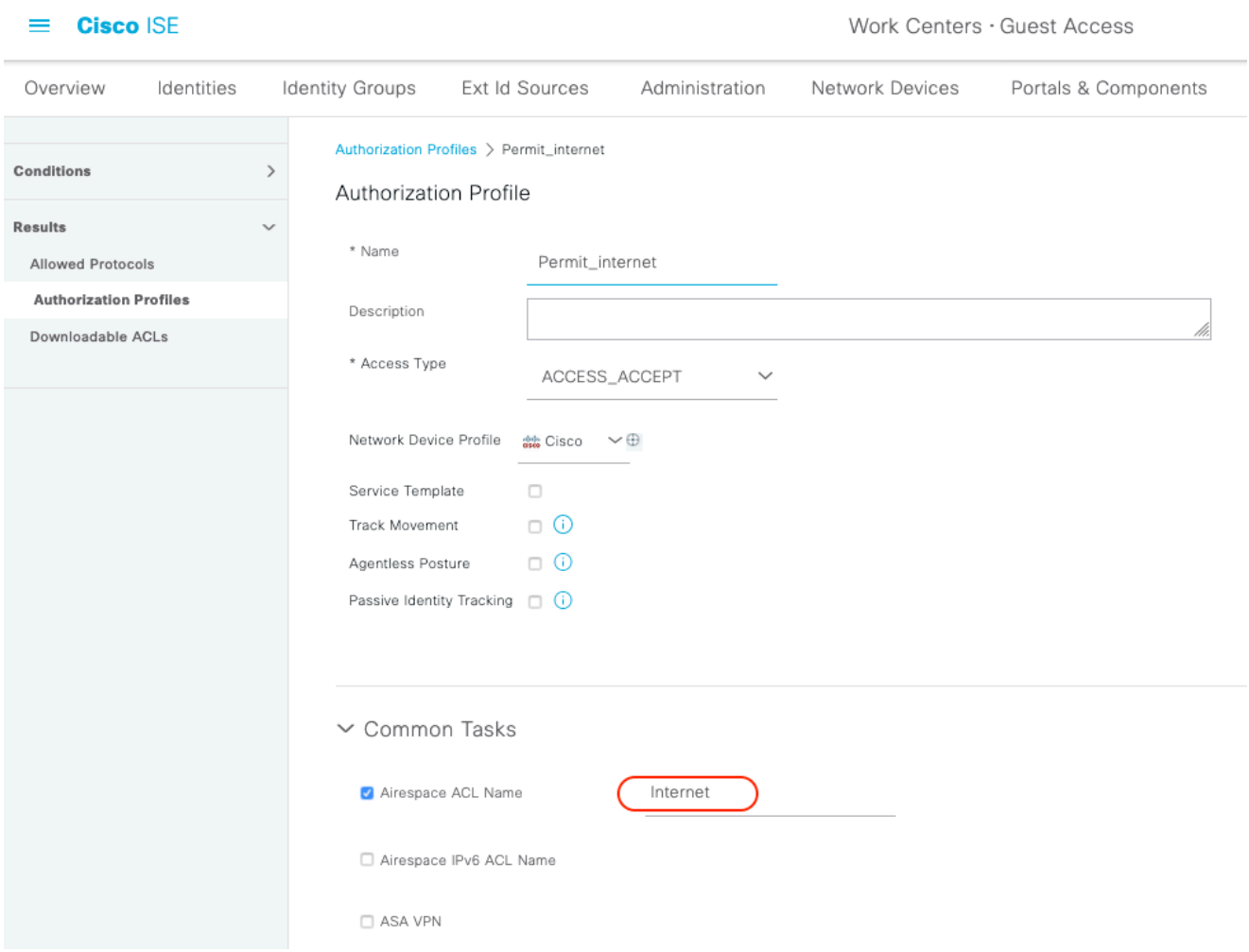


6. Configurare questi due profili di autorizzazione passando a Centri di lavoro > Accesso guest > Elementi criteri > Risultati > Profili di autorizzazione.

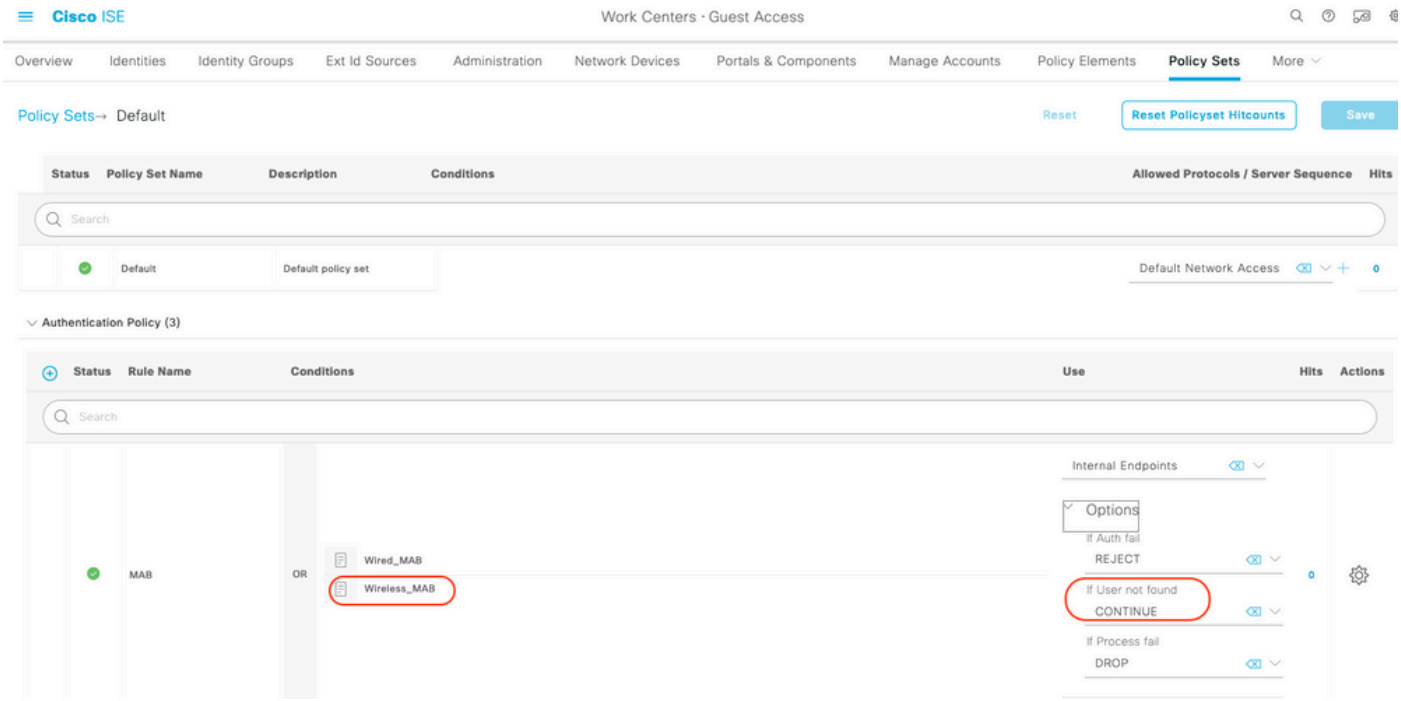
- Guest-Portal (con il reindirizzamento al portale Guest Cisco_Guest e a un ACL di reindirizzamento denominato GuestRedirect). Questo ACL GuestRedirect è stato creato in precedenza sul WLC.



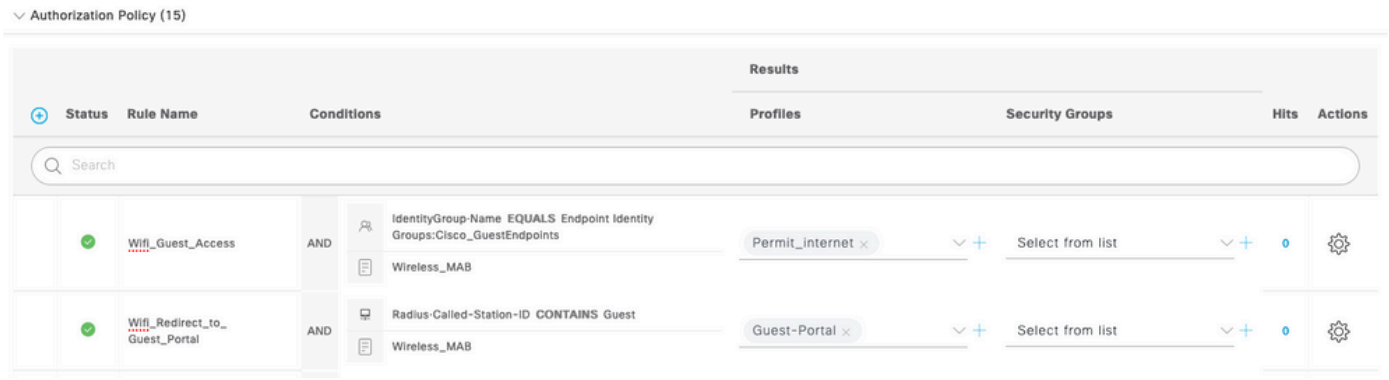
- Permit_Internet (con ACL Airespace uguale a Internet)



7. Modificare il set di criteri denominato Predefinito. Il set di criteri predefinito è preconfigurato per l'accesso al portale guest. È presente un criterio di autenticazione denominato MAB che consente all'autenticazione MAC Authentication Bypass (MAB) di continuare (non rifiutare) per un indirizzo Mac sconosciuto.



8. Passare al criterio di autorizzazione nella stessa pagina. Creare le regole di autorizzazione, come illustrato nell'immagine.



I nuovi utenti associati all'SSID guest non fanno ancora parte di alcun gruppo di identità e pertanto soddisfano la seconda regola e vengono reindirizzati al portale guest.

Dopo che l'utente ha effettuato l'accesso, ISE invia una richiesta RADIUS CoA e il WLC esegue la riautenticazione. In questo caso, viene stabilita una corrispondenza con la prima regola di autorizzazione (quando l'endpoint diventa parte del gruppo di identità dell'endpoint definito) e l'utente ottiene il profilo di autorizzazione Permit_internet.

9. Possiamo anche fornire l'accesso temporaneo agli ospiti utilizzando la condizione Guest flow. Questa condizione sta verificando le sessioni attive su ISE ed è stata attribuita. Se nella sessione è presente l'attributo che indica che in precedenza l'utente guest ha eseguito l'autenticazione con successo, la condizione viene soddisfatta. Dopo che ISE ha ricevuto un messaggio di interruzione dell'accounting Radius da NAD (Network Access Device), la sessione viene terminata e successivamente rimossa. In questa fase la condizione Accesso alla rete:UseCase = Flusso guest non è più soddisfatta. Di conseguenza, tutte le autenticazioni successive dell'endpoint raggiungono il reindirizzamento delle regole generiche per l'autenticazione guest.

Nota: per volta è possibile utilizzare l'accesso temporaneo come Guest oppure l'accesso permanente come Guest, ma non entrambi.

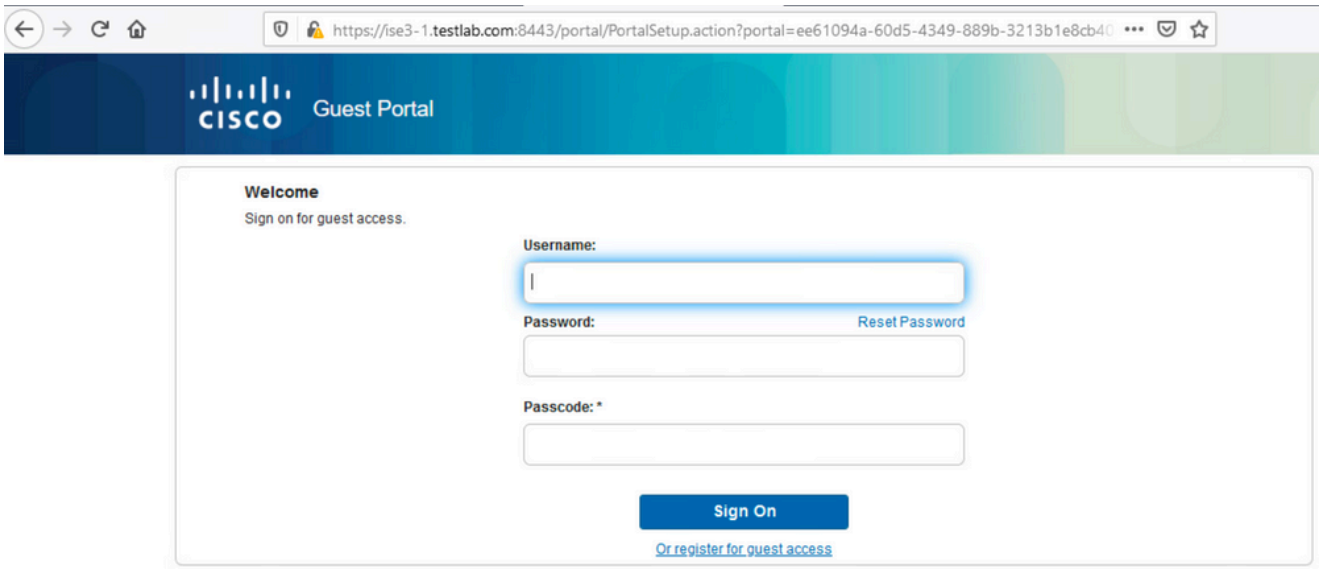
Per la configurazione dell'accesso temporaneo e permanente per i guest ISE, consultare il documento.

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200273-Configure-ISE-Guest-Temporary-and-Perman.html

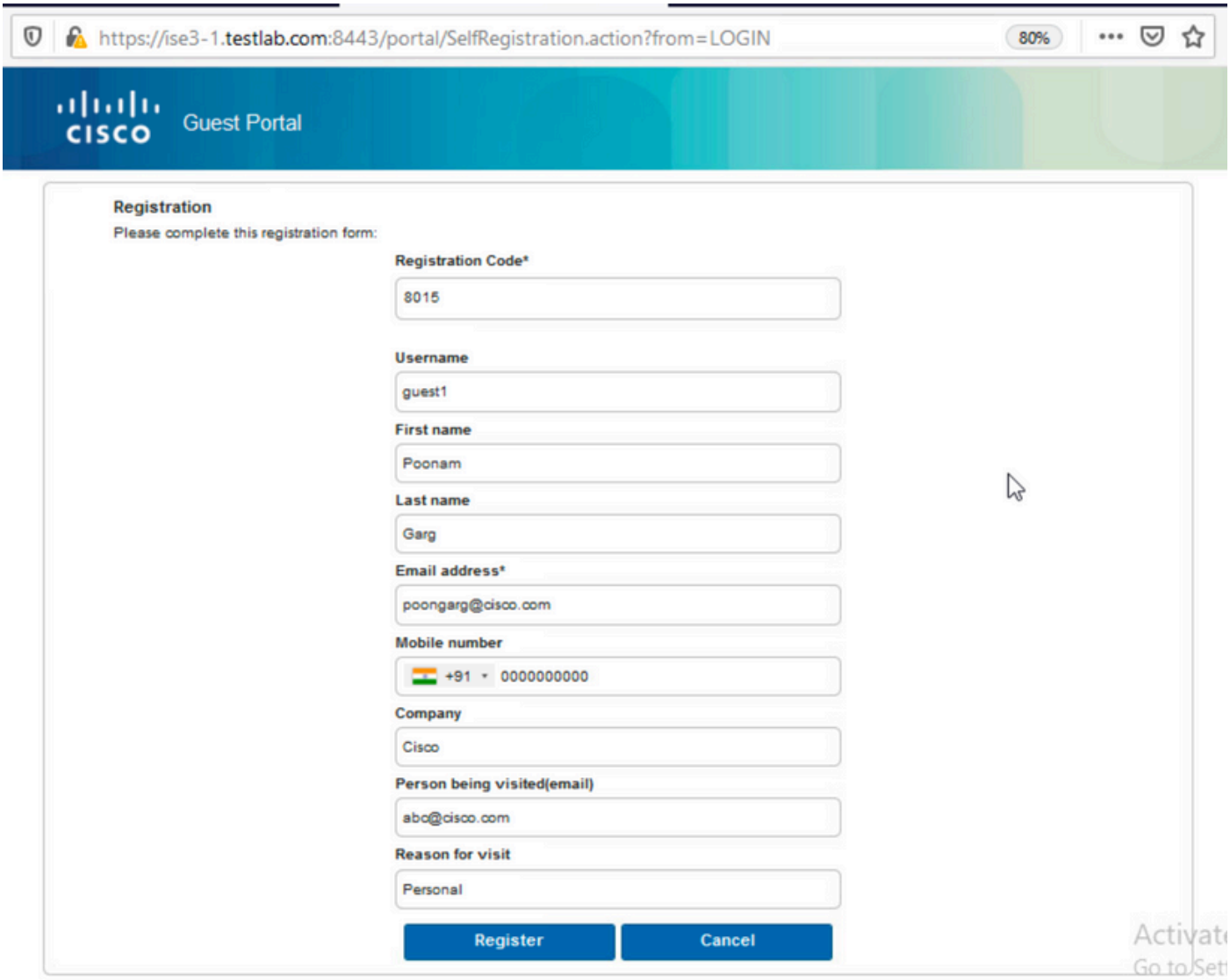
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

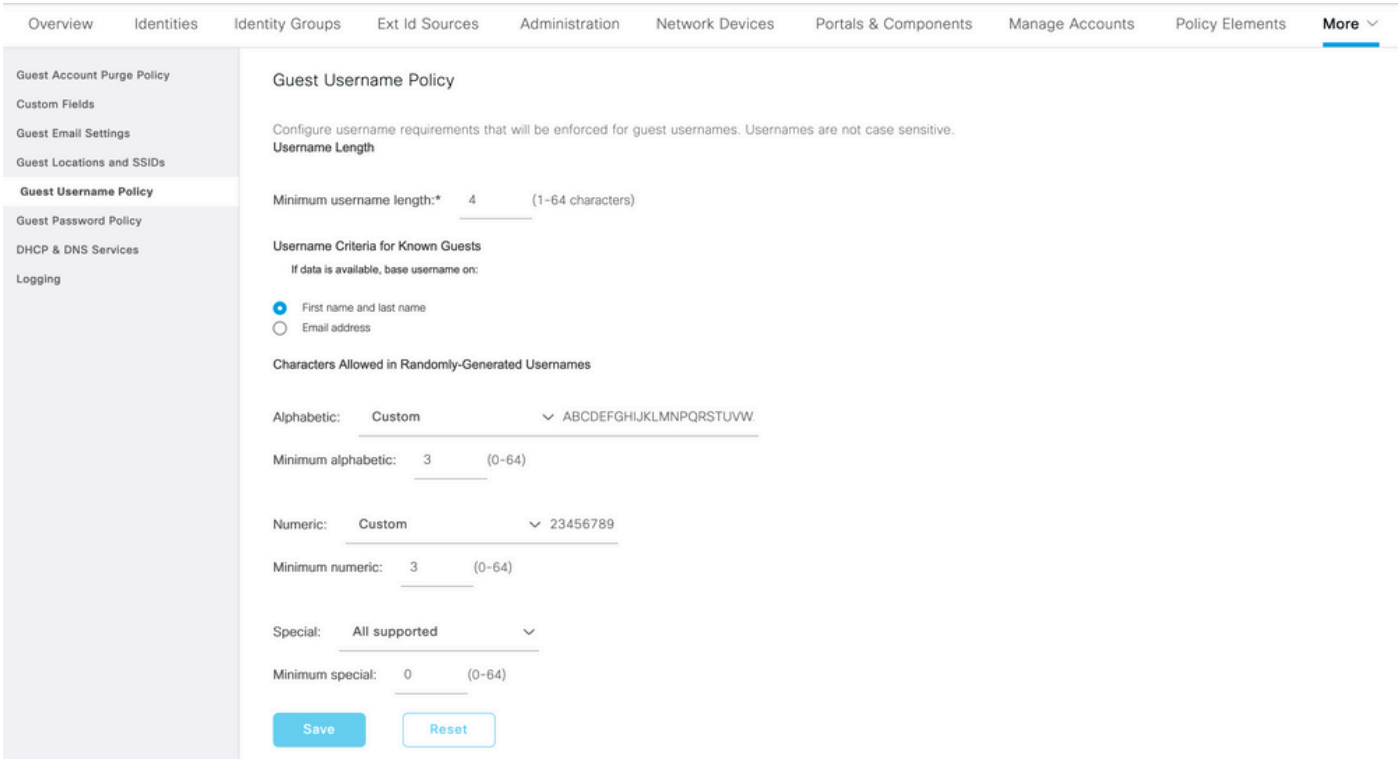
1. Dopo aver eseguito l'associazione con il SSID Guest e aver digitato un URL, si viene reindirizzati alla pagina Guest Portal, come mostrato nell'immagine.



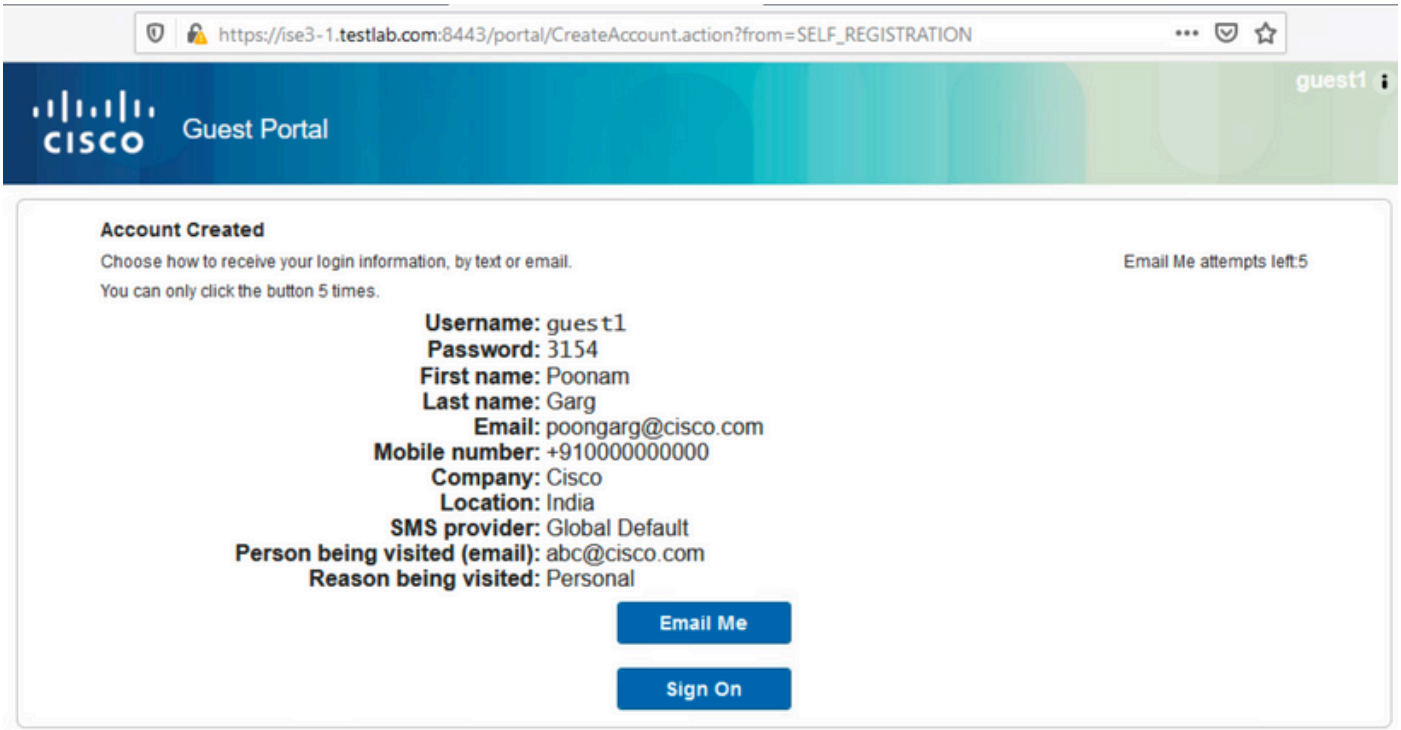
2. Poiché non si dispone ancora di credenziali, è necessario scegliere l'opzione Registra per accesso Guest. Viene visualizzato il modulo di registrazione per creare l'account. Se l'opzione Codice di registrazione è stata attivata nella configurazione del portale guest, il valore segreto è obbligatorio (in questo modo viene garantita la registrazione automatica solo agli utenti con autorizzazioni corrette).

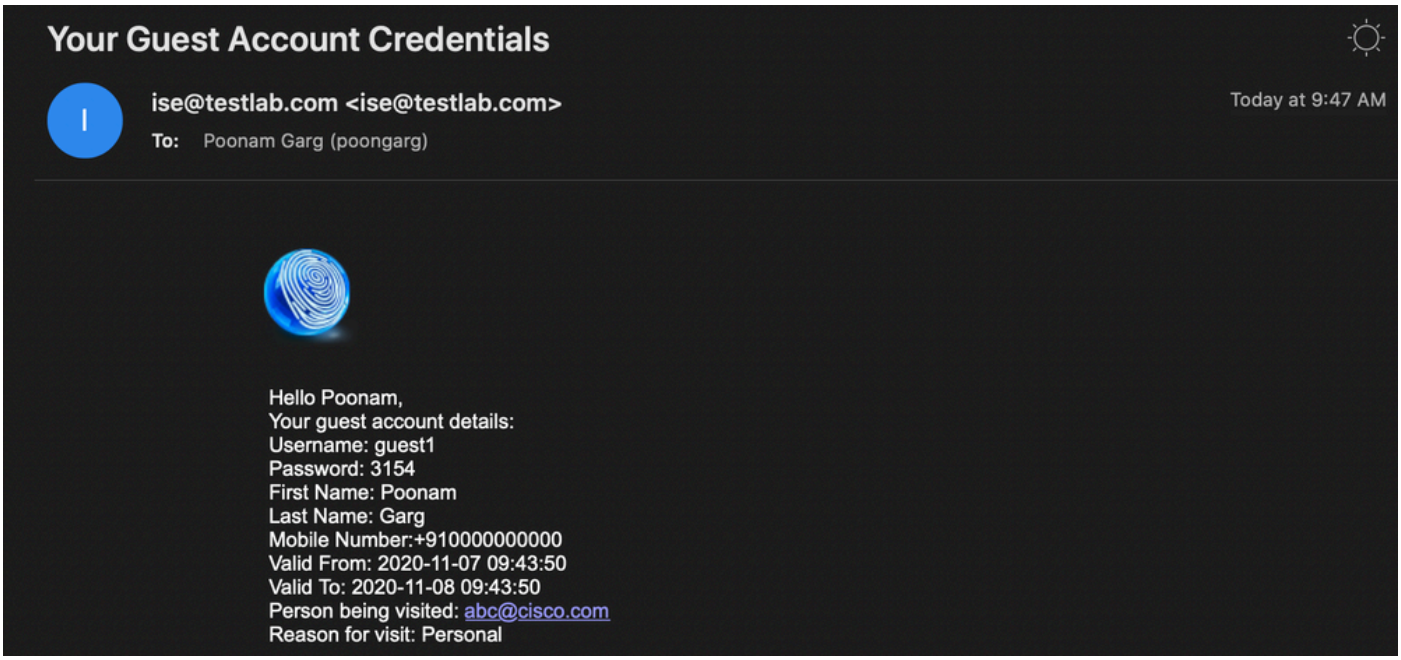


3. In caso di problemi con la password o con la policy utente, passare a Centri di lavoro > Accesso ospite > Impostazioni > Policy nome utente ospite per modificare le impostazioni. Di seguito è riportato un esempio:

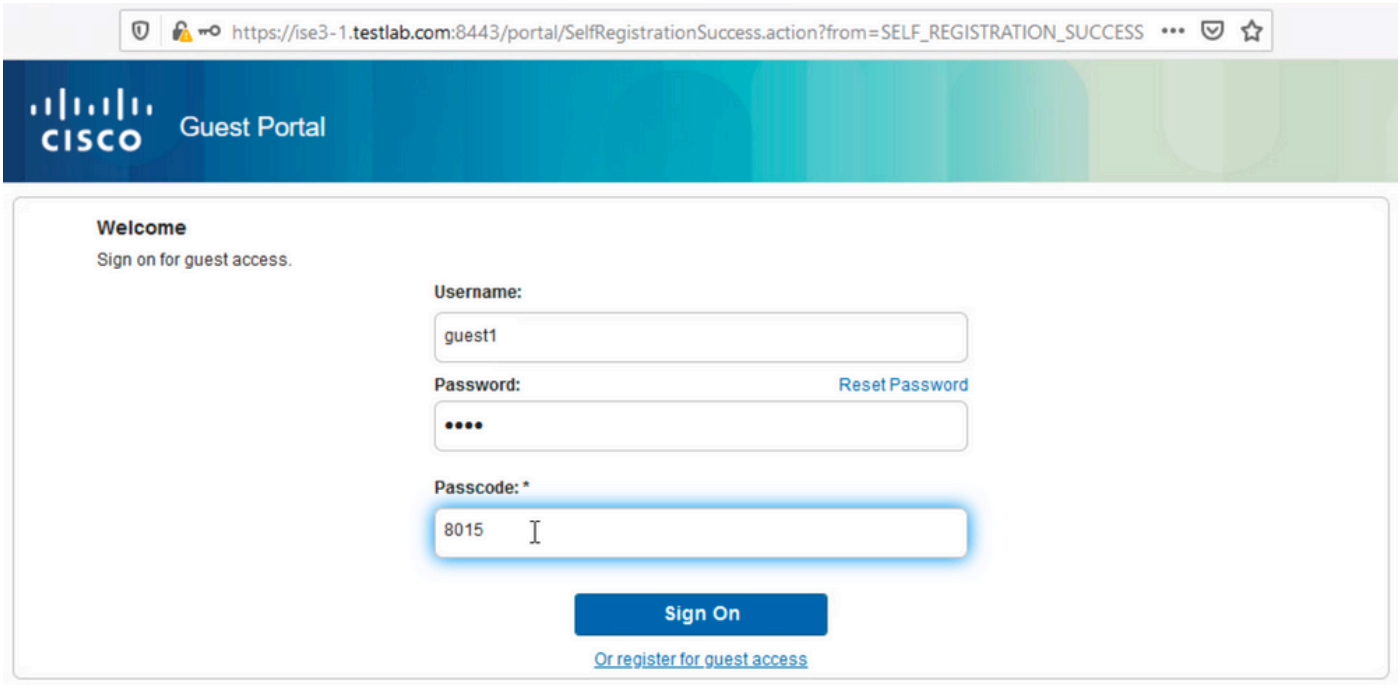


4. Una volta completata la creazione dell'account, all'utente vengono presentate le credenziali (password generata in base ai criteri password guest) e la notifica e-mail all'utente guest se è configurata:

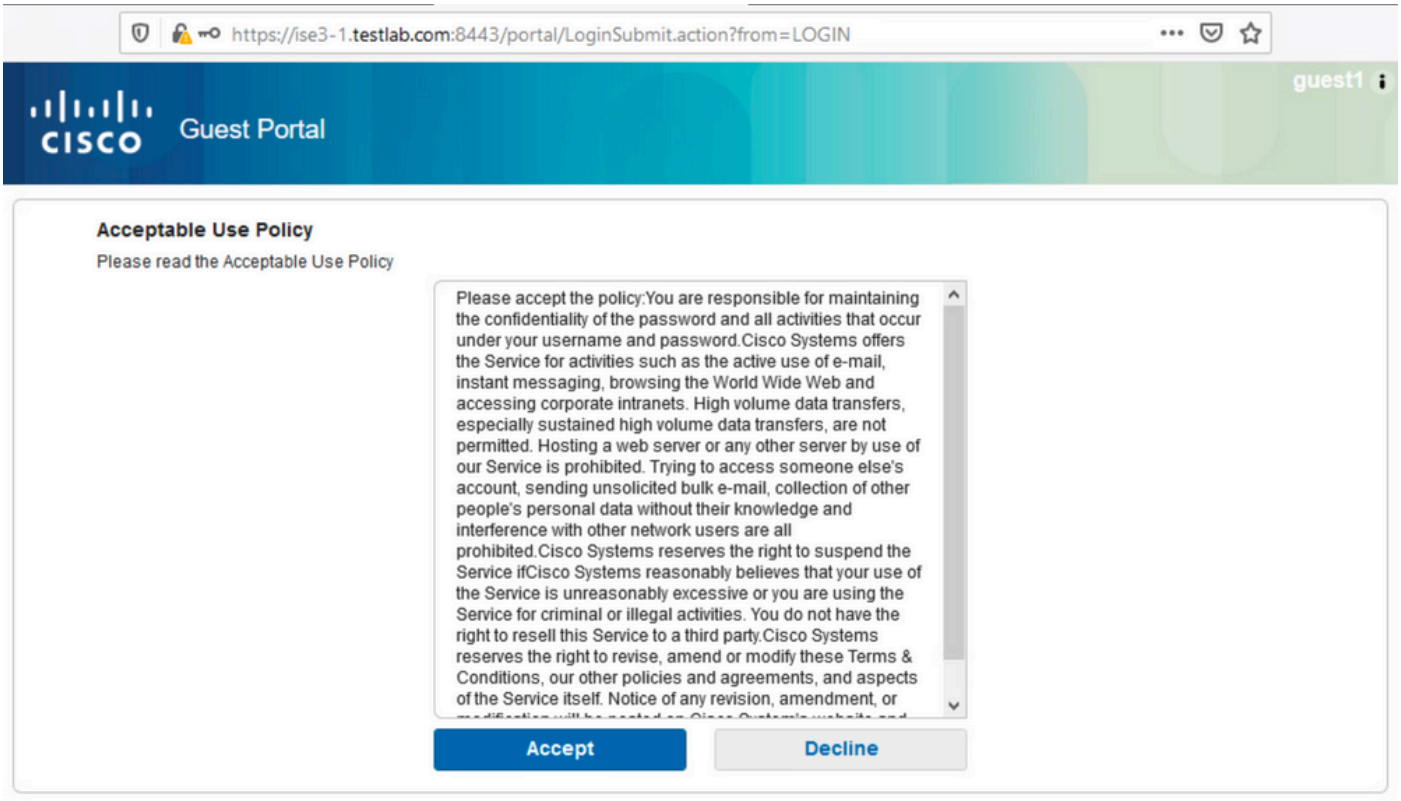


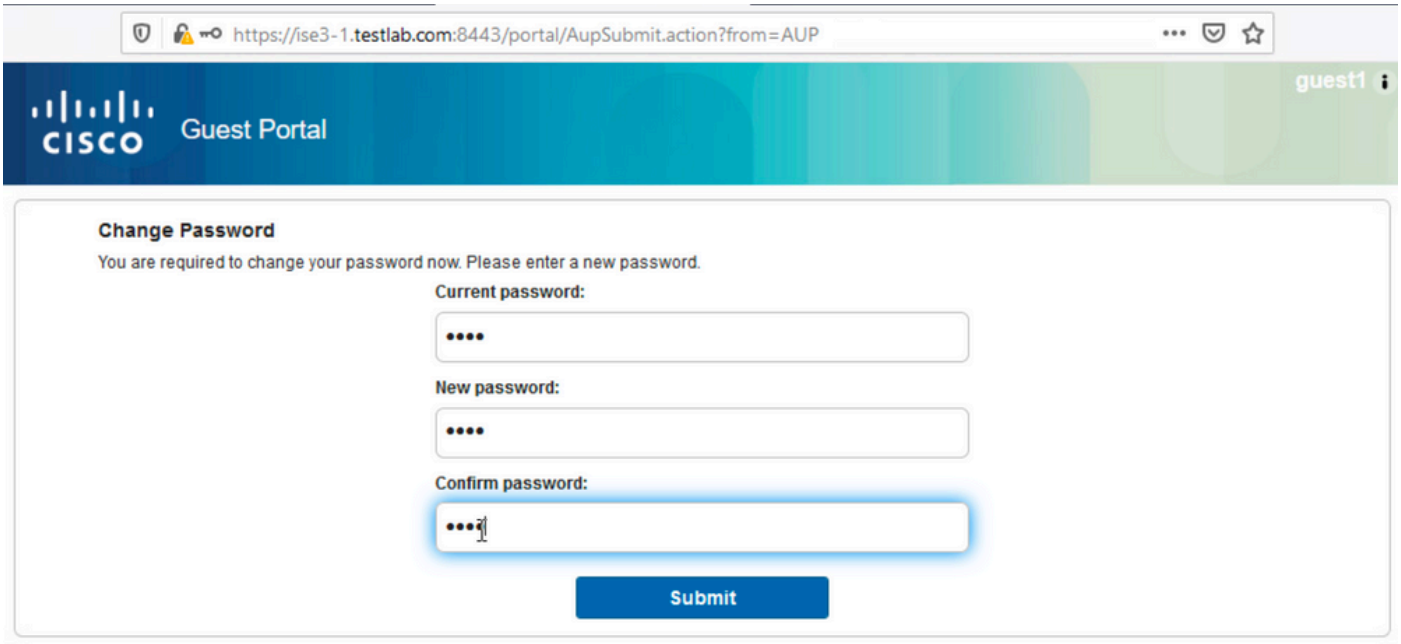


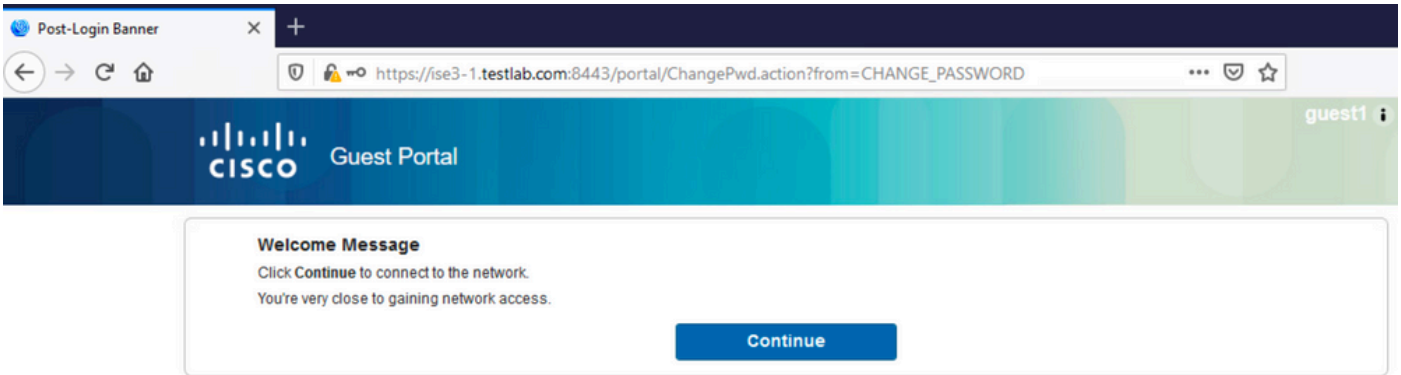
5. Fare clic su Sign On (Accedi) e fornire le credenziali (può essere richiesto un passcode di accesso aggiuntivo se configurato in Guest Portal; si tratta di un altro meccanismo di sicurezza che consente solo a coloro che conoscono la password di accedere).



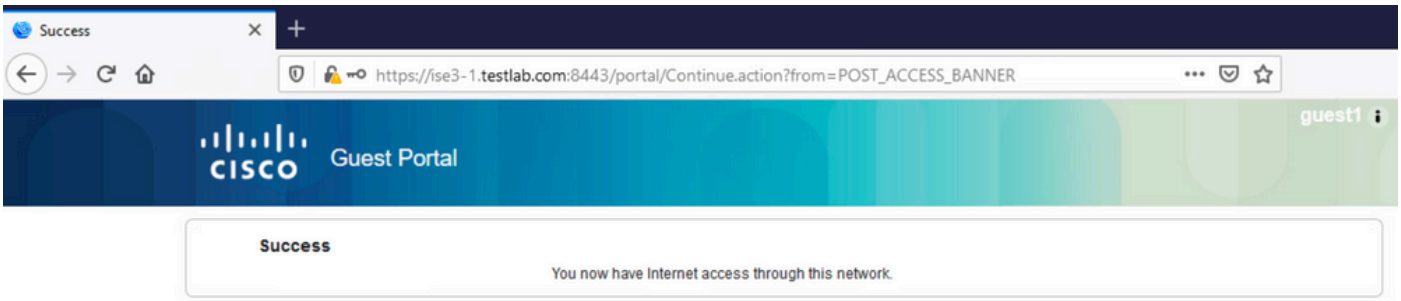
6. Se l'operazione ha esito positivo, è possibile presentare una politica d'uso accettabile (AUP) opzionale (se configurata in Guest Portal). All'utente viene presentata un'opzione di modifica della password ed è possibile visualizzare anche il banner post-login (configurabile anche in Guest Portal).


https://ise3-1.testlab.com:8443/portal/LoginSubmit.action?from=LOGIN
guest1
Guest Portal
Acceptable Use Policy
Please read the Acceptable Use Policy
Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or
Accept
Decline


https://ise3-1.testlab.com:8443/portal/AupSubmit.action?from=AUP
guest1
Guest Portal
Change Password
You are required to change your password now. Please enter a new password.
Current password:
New password:
Confirm password:
Submit


Post-Login Banner
https://ise3-1.testlab.com:8443/portal/ChangePwd.action?from=CHANGE_PASSWORD
guest1
Guest Portal
Welcome Message
Click Continue to connect to the network.
You're very close to gaining network access.
Continue

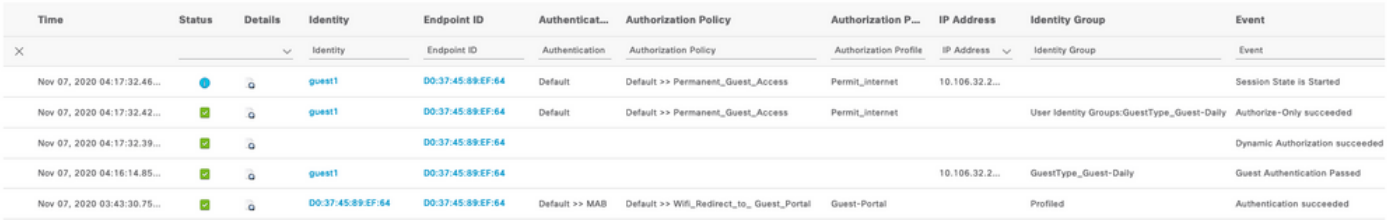
7. L'ultima pagina (Banner post-login) conferma che l'accesso è stato concesso:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

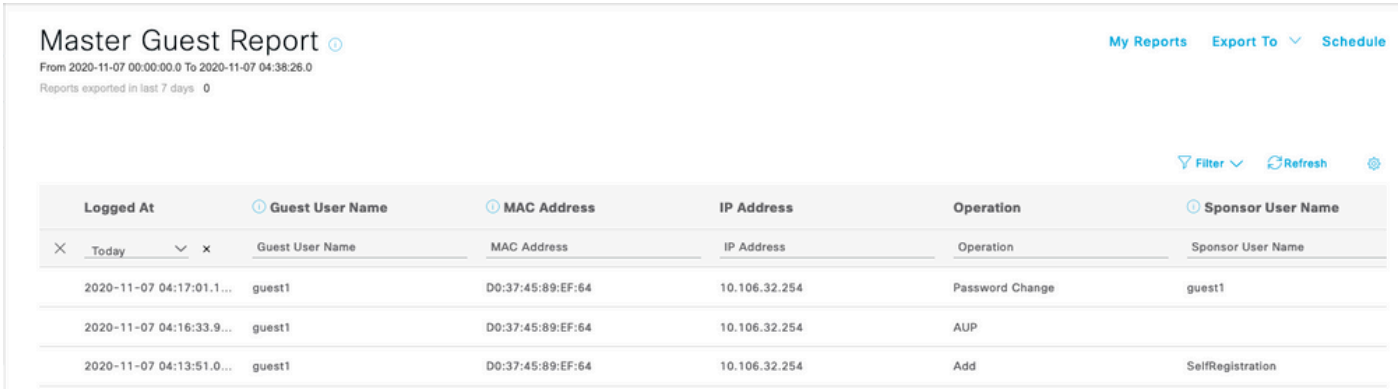
In questa fase, ISE presenta questi log in Operations > RADIUS > Live Log, come mostrato nell'immagine.



Ecco il flusso:

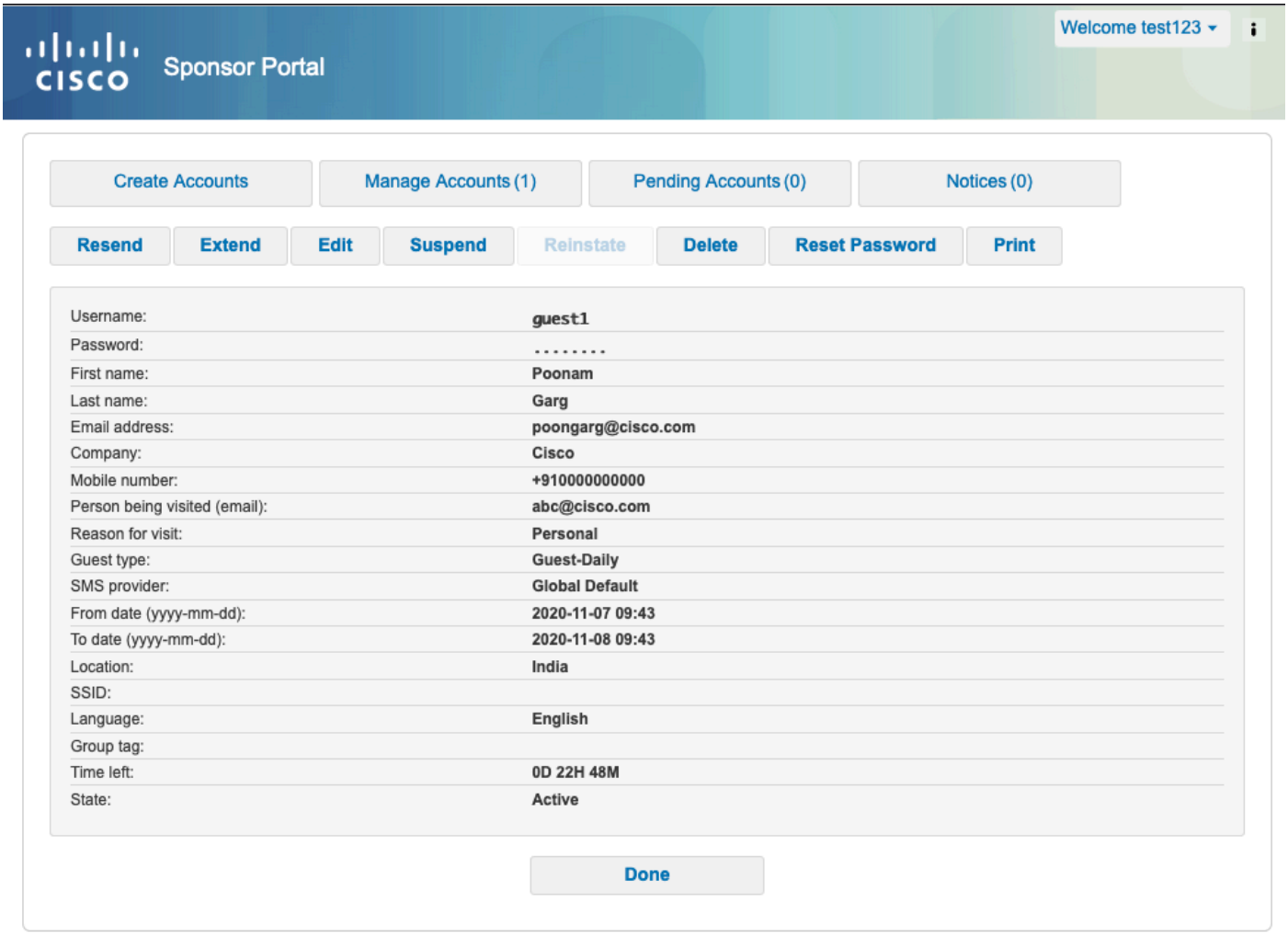
- L'utente guest incontra la seconda regola di autorizzazione (Wifi_Redirect_to_Guest_Portal) e viene reindirizzato a Guest-Portal (Autenticazione completata).
- L'ospite viene reindirizzato per la registrazione automatica. Dopo aver eseguito correttamente il login (con l'account appena creato), ISE invia il messaggio di autenticazione CoA, che viene confermato dal WLC (autorizzazione dinamica riuscita).
- Il WLC esegue la riautenticazione con l'attributo Authorize-Only e viene restituito il nome ACL (Authorize-Only riuscito). Al guest viene fornito l'accesso alla rete corretto.

Rapporti (Operazioni > Rapporti > Guest > Rapporto Guest principale) conferma inoltre che:



Un utente sponsor (con privilegi corretti) è in grado di verificare lo stato corrente di un utente guest.

In questo esempio viene confermato che l'account è stato creato e che l'utente ha eseguito l'accesso al portale:



Configurazione opzionale

Per ogni fase del flusso è possibile configurare diverse opzioni. Tutto questo è configurato per il portale guest nei centri di lavoro > Accesso guest > Portali e componenti > Portali guest > Nome portale > Modifica > Comportamento del portale e impostazioni di flusso. Le impostazioni più

importanti includono:

Impostazioni registrazione automatica

- Tipo di ospite: descrive il periodo di tempo di attività dell'account, le opzioni di scadenza della password, le ore di accesso e le opzioni (combinazione di profilo temporale e ruolo di ospite).
- Codice di registrazione: se questa opzione è abilitata, solo gli utenti che conoscono il codice segreto possono eseguire la registrazione automatica (devono fornire la password al momento della creazione dell'account)
- AUP - Accetta criteri d'uso durante la registrazione automatica
- Obbligo per lo sponsor di approvare/attivare l'account guest.

Impostazioni guest di accesso

- Codice di accesso: se abilitato, l'accesso è consentito solo agli utenti guest che conoscono il codice segreto.
- AUP - Accetta criteri d'uso durante la registrazione automatica.
- Opzione di modifica della password.

Impostazioni registrazione dispositivo

- Per impostazione predefinita, il dispositivo viene registrato automaticamente.

Impostazioni di conformità del dispositivo guest

- Consente una postura all'interno del flusso.

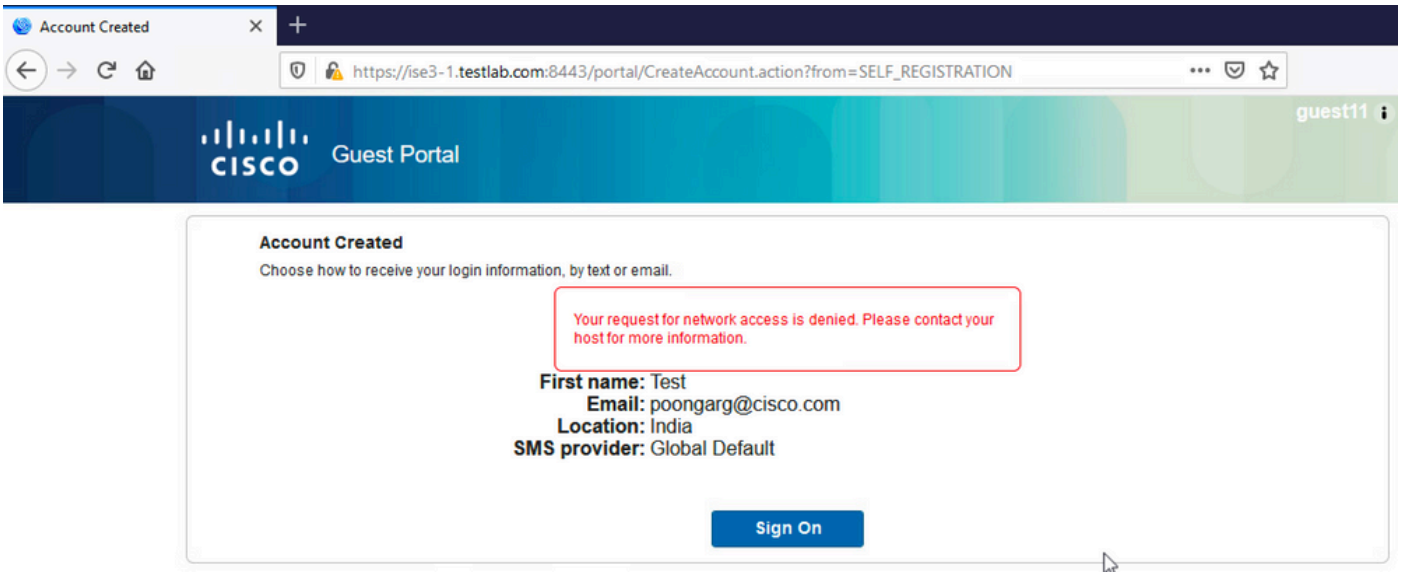
Impostazioni BYOD

- Consente agli utenti aziendali che utilizzano il portale come utenti guest di registrare i propri dispositivi personali.

Account approvati dallo sponsor

Se l'opzione Richiedi approvazione ospiti è selezionata in Impostazioni modulo di registrazione, l'account creato dall'ospite deve essere approvato da uno sponsor. Questa funzionalità può utilizzare l'e-mail per inviare una notifica allo sponsor (per l'approvazione dell'account guest):

Se il server SMTP (Simple Mail Transfer Protocol) non è configurato correttamente, l'account non viene creato:



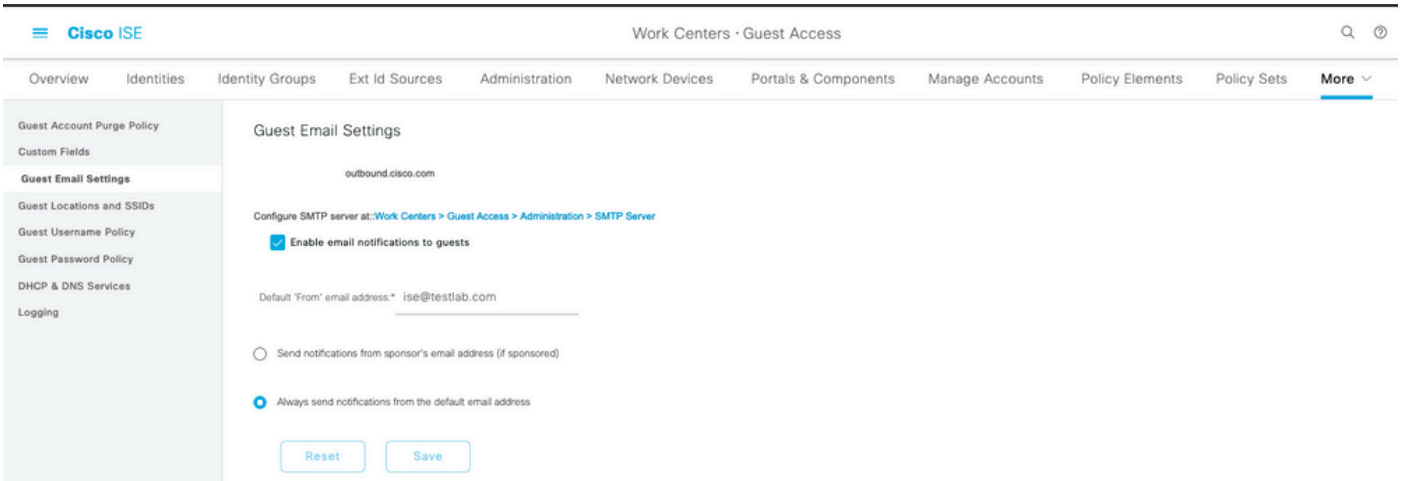
Il log di guest.log conferma che si è verificato un problema con l'invio della notifica di approvazione all'e-mail dello sponsor poiché il server SMTP non è configurato correttamente:

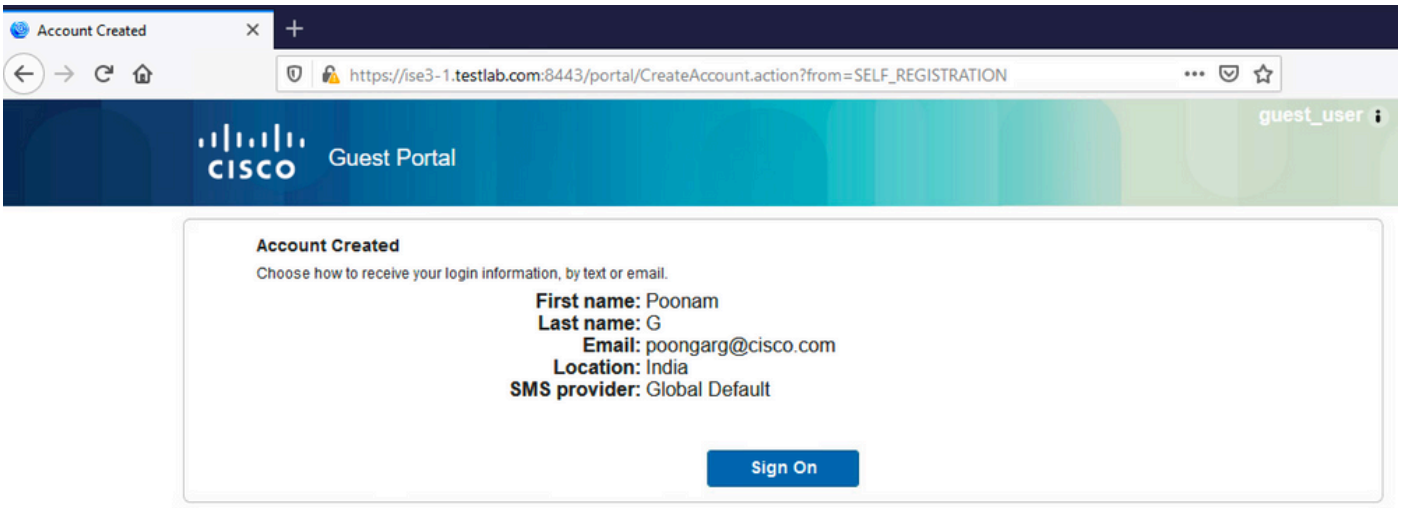
<#root>

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD][] cpm.guestaccess.apiservices.util.SmtpMs
javax.mail.MessagingException: Could not connect to SMTP host: outbound.cicso.com, port: 25, response: 4

2020-11-07 07:16:38,547 ERROR [https-jsse-nio-10.106.32.25-8443-exec-1][] cpm.guestaccess.apiservices.no
com.cisco.cpm.guestaccess.exception.GuestAccessSystemException: com.cisco.cpm.guestaccess.exception.Gues
```

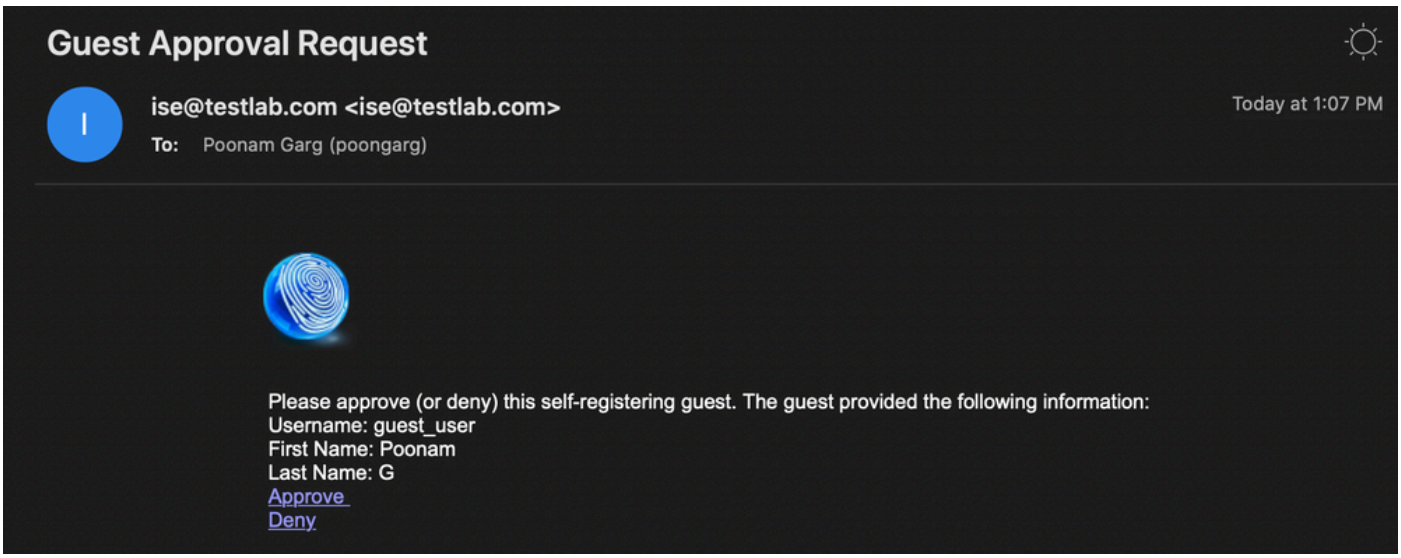
Quando si dispone della configurazione corretta del server di posta elettronica e SMTP, viene creato l'account:





Dopo aver abilitato l'opzione Richiedi approvazione utenti guest, i campi nome utente e password vengono automaticamente rimossi dalla sezione Includi queste informazioni nella pagina Registrazione automatica riuscita. Per questo motivo, quando è necessaria l'approvazione dello sponsor, le credenziali per gli utenti guest non vengono visualizzate per impostazione predefinita nella pagina Web che presenta informazioni che mostrano che l'account è stato creato. Devono invece essere recapitati tramite SMS (Short Message Service) o posta elettronica. Questa opzione deve essere abilitata nella sezione Invia notifica credenziali all'approvazione tramite (contrassegna e-mail/SMS).

Allo sponsor viene inviato un messaggio di posta elettronica di notifica:



Lo sponsor fa clic sul collegamento Approvazione e accede al portale dello sponsor e l'account viene approvato:

Da questo momento in poi, l'utente guest può eseguire l'accesso (con le credenziali ricevute tramite e-mail o SMS).

In sintesi, in questo flusso vengono utilizzati tre indirizzi e-mail:

- Indirizzo di notifica "Da". Viene definito in modo statico o prelevato dall'account sponsor e utilizzato come indirizzo Da sia per la notifica allo sponsor (per l'approvazione) che per i dettagli delle credenziali all'ospite. Questa opzione è configurata in Centri di lavoro > Accesso guest > Impostazioni > Impostazioni e-mail guest.

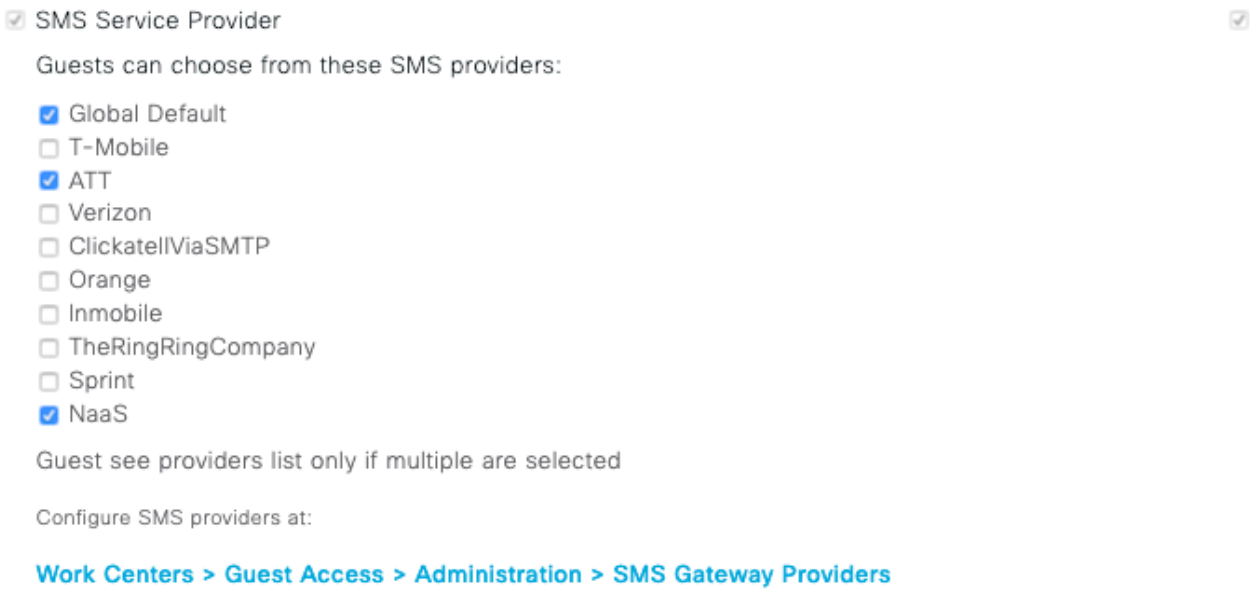
- Indirizzo di notifica "A". Questa opzione viene utilizzata per notificare allo sponsor che ha ricevuto un account per l'approvazione. Questa opzione è configurata nel portale per gli utenti guest in Centri di lavoro > Accesso guest > Portali per gli utenti guest > Portali e componenti > Nome portale > Impostazioni modulo di registrazione > Richiedi approvazione degli utenti guest > Invia richiesta di approvazione tramite posta elettronica a.

- Indirizzo Guest "To". Questo viene fornito dall'utente guest durante la registrazione. Se è selezionata l'opzione Invia notifica delle credenziali all'approvazione tramite posta elettronica, l'e-mail con i dettagli delle credenziali (nome utente e password) viene recapitata al guest.

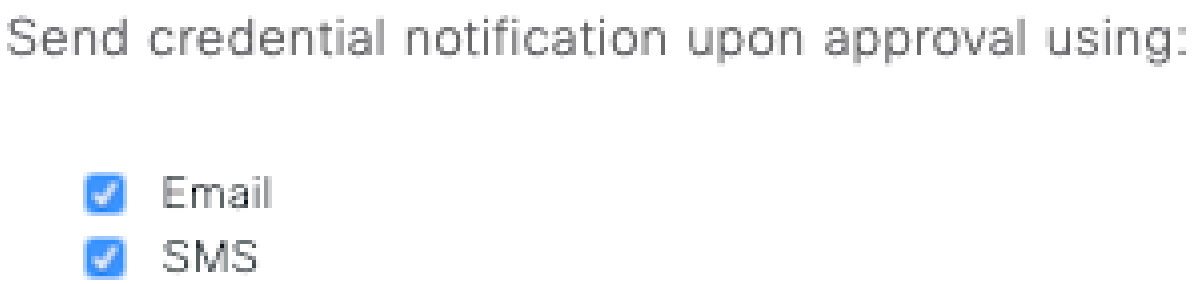
Consegna credenziali tramite SMS

Le credenziali degli utenti guest possono essere recapitate anche tramite SMS. È necessario configurare le seguenti opzioni:

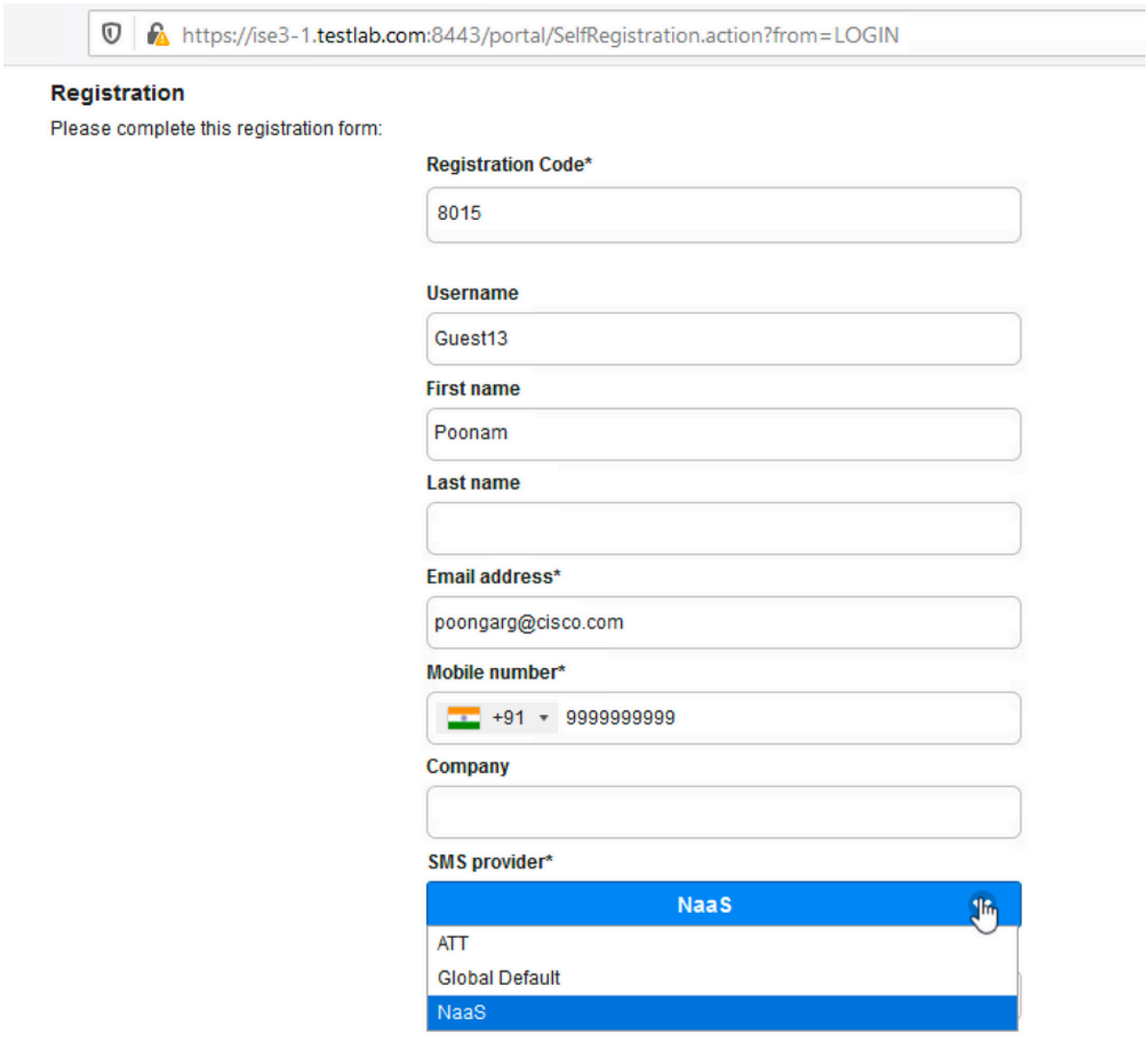
1. Scegliere il provider di servizi SMS in Impostazioni modulo di registrazione:



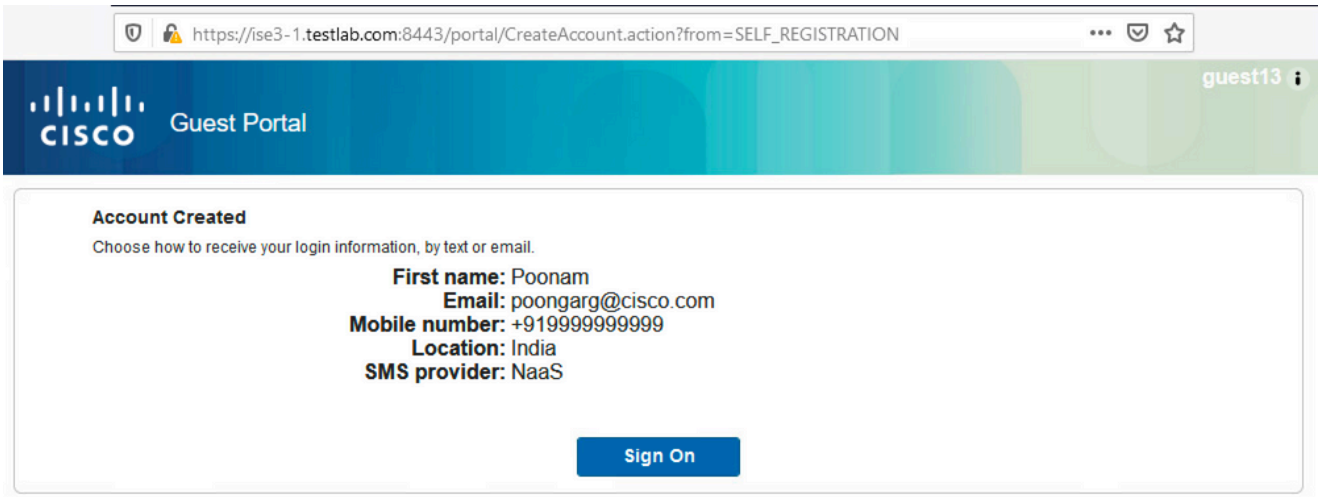
2. Selezionare la casella di controllo Invia notifica credenziali all'approvazione utilizzando: SMS.



3. Quindi, all'utente guest viene chiesto di scegliere il provider disponibile quando crea un account:



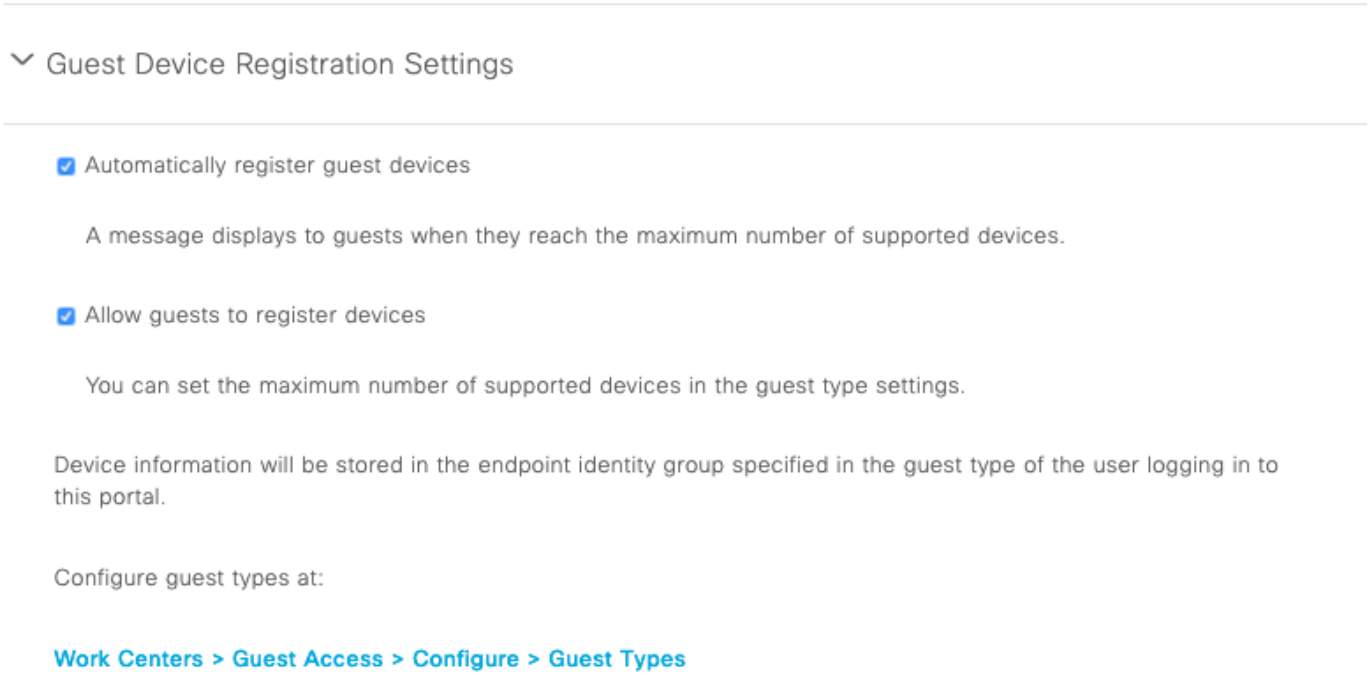
4. Viene inviato un SMS con il provider e il numero di telefono scelti:

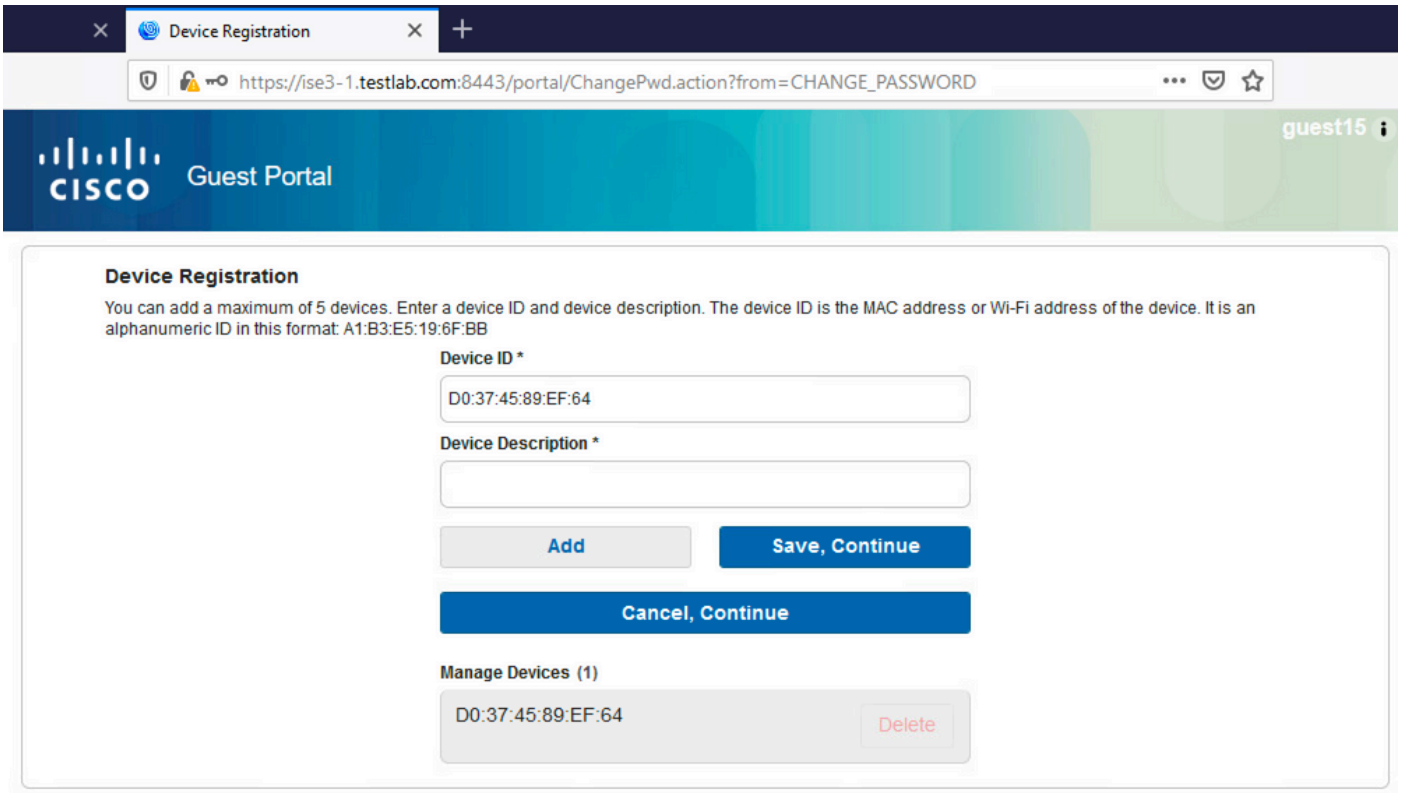


5. È possibile configurare i provider SMS in Amministrazione > Sistema > Impostazioni > Gateway SMS.

Registrazione dispositivo

Se l'opzione Consenti agli utenti guest di registrare i dispositivi è selezionata dopo che un utente guest ha eseguito l'accesso e ha accettato le CDS, è possibile registrare i dispositivi:



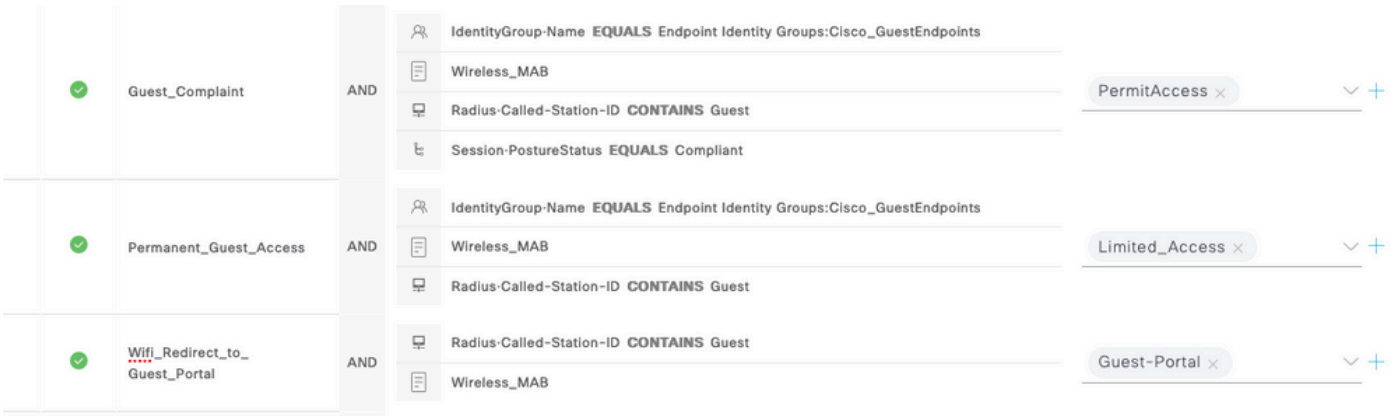


Si noti che il dispositivo è già stato aggiunto automaticamente (si trova nell'elenco Gestione dispositivi). Ciò è dovuto al fatto che è stata selezionata la registrazione automatica dei dispositivi guest.

Postura

Se l'opzione Richiedi conformità dispositivo guest è selezionata, agli utenti guest viene assegnato un agente che esegue la postura (NAC/Web Agent) dopo l'accesso e l'accettazione dell'AUP (e facoltativamente la registrazione del dispositivo). ISE elabora le regole di provisioning client per decidere quale agente deve essere sottoposto a provisioning. L'agente in esecuzione sulla stazione esegue quindi la postura (in base alle regole di postura) e invia i risultati all'ISE, che invia la nuova autenticazione CoA per modificare lo stato di autorizzazione, se necessario.

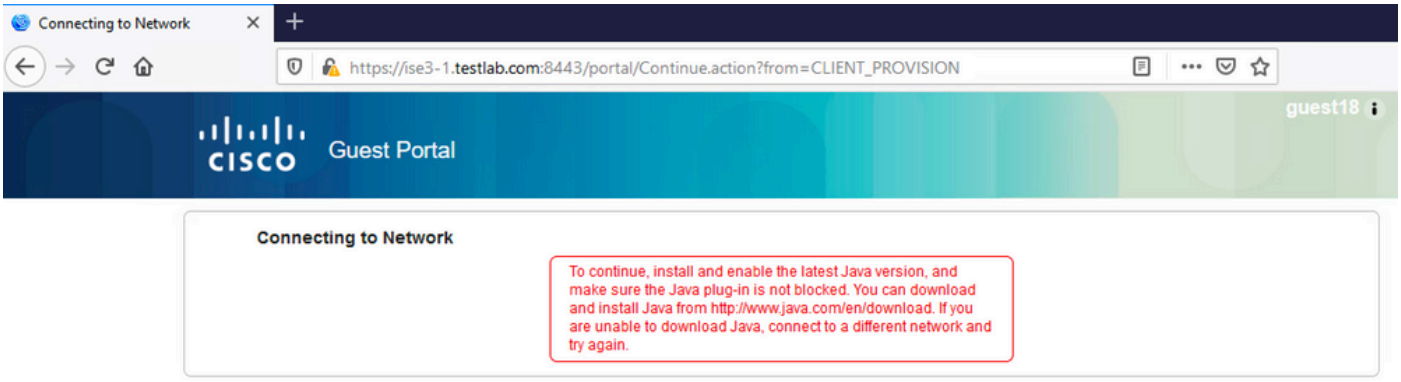
Le regole di autorizzazione possibili sono simili alle seguenti:



I primi nuovi utenti che incontrano la regola Guest_Authenticate reindirizzano al portale Guest con

registrazione automatica. Dopo che l'utente si è registrato e ha effettuato l'accesso, la CoA cambia lo stato di autorizzazione e l'utente dispone di accesso limitato per eseguire la postura e la correzione. Solo dopo il provisioning dell'agente NAC e la conformità della stazione, CoA cambia nuovamente lo stato di autorizzazione per fornire l'accesso a Internet.

I problemi tipici della postura includono la mancanza di regole di provisioning client corrette:



Questa condizione può essere confermata anche se si esamina il file guest.log:

<#root>

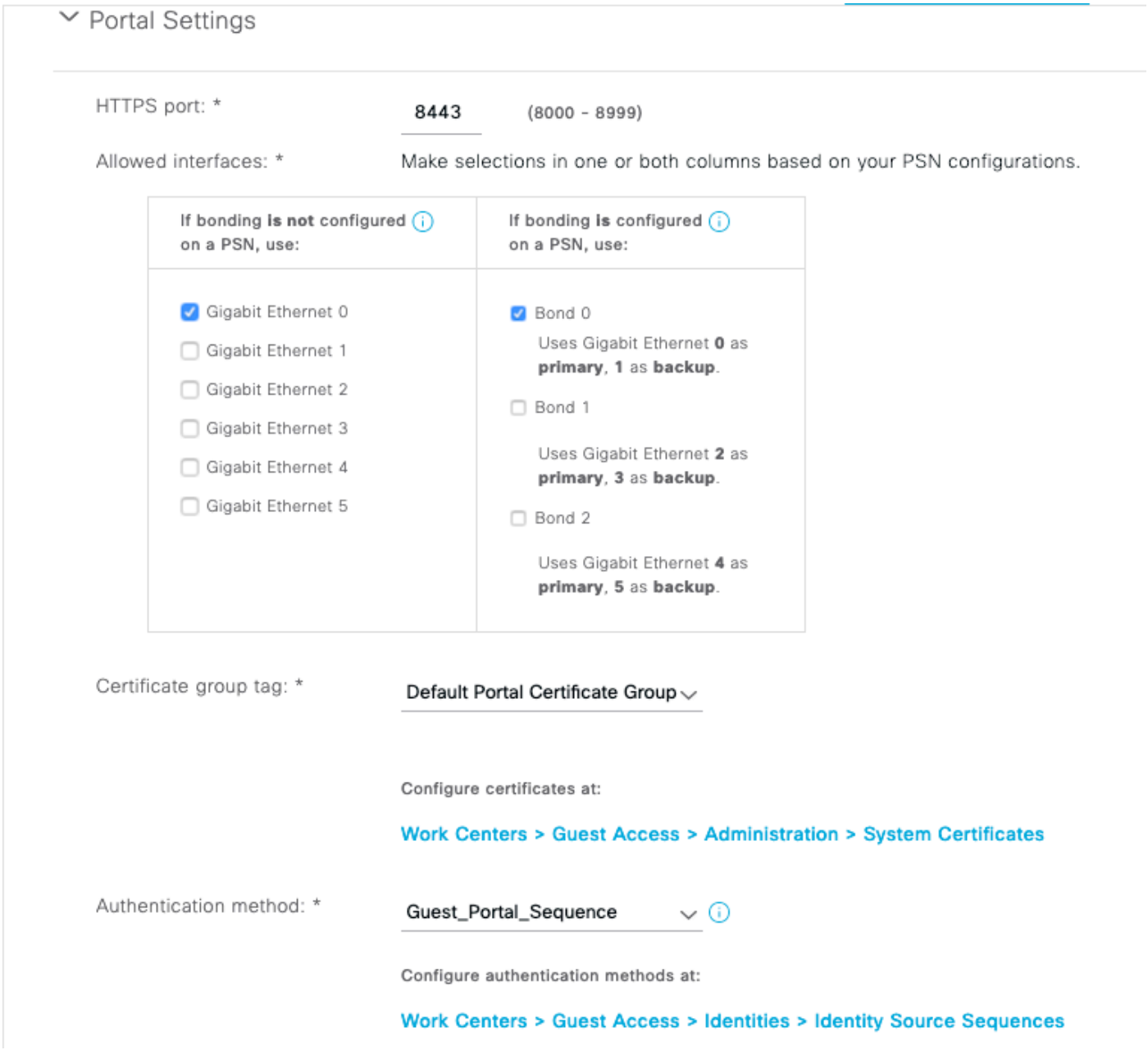
```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7][] guestaccess.flowmanager.step.g
```

BYOD

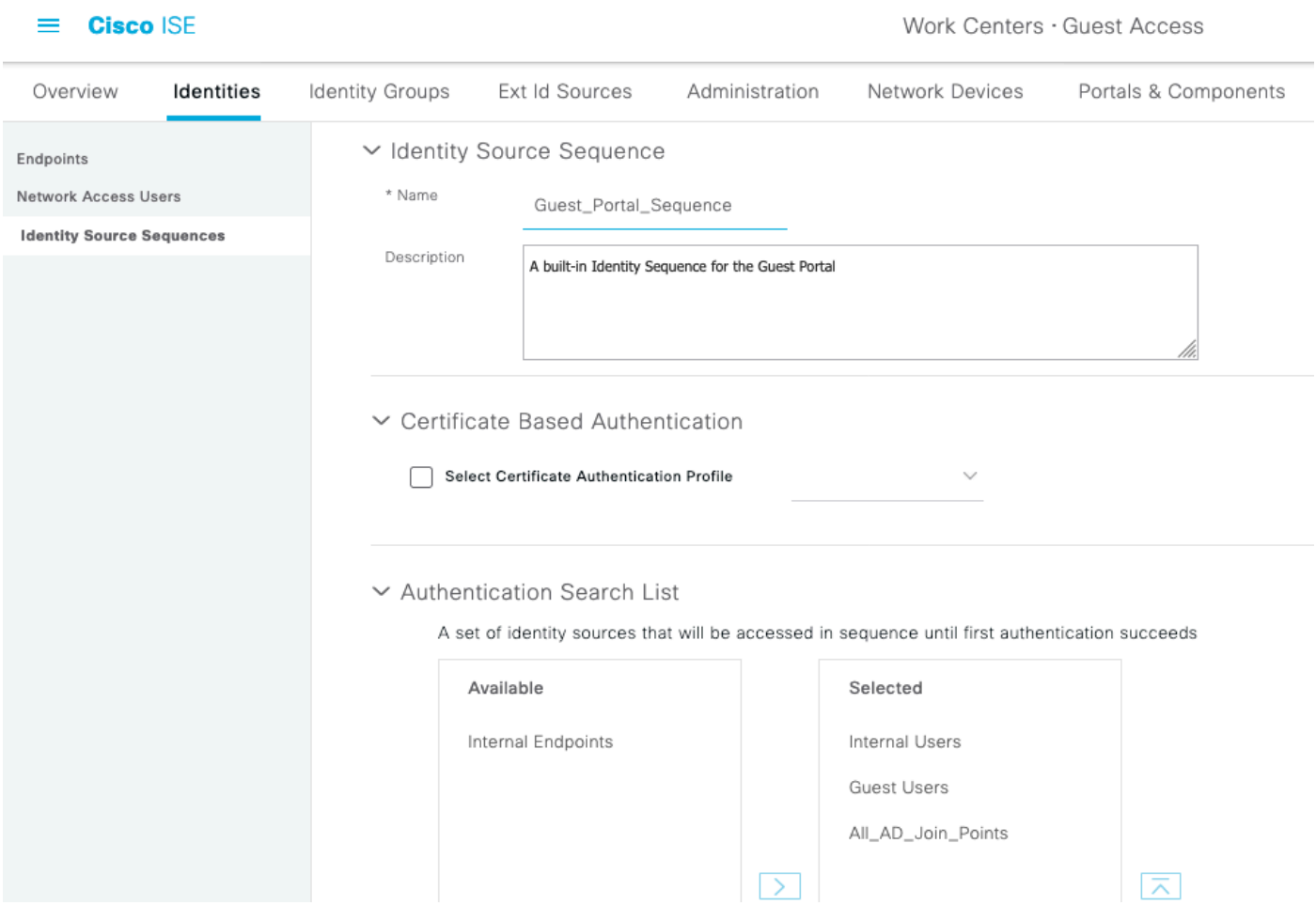
Se è selezionata l'opzione Consenti ai dipendenti di utilizzare i dispositivi personali in rete, gli utenti aziendali che utilizzano questo portale possono passare attraverso il flusso BYOD e registrare i dispositivi personali. Per gli utenti guest, questa impostazione non modifica nulla.

Cosa significa "dipendenti che utilizzano il portale come guest"?

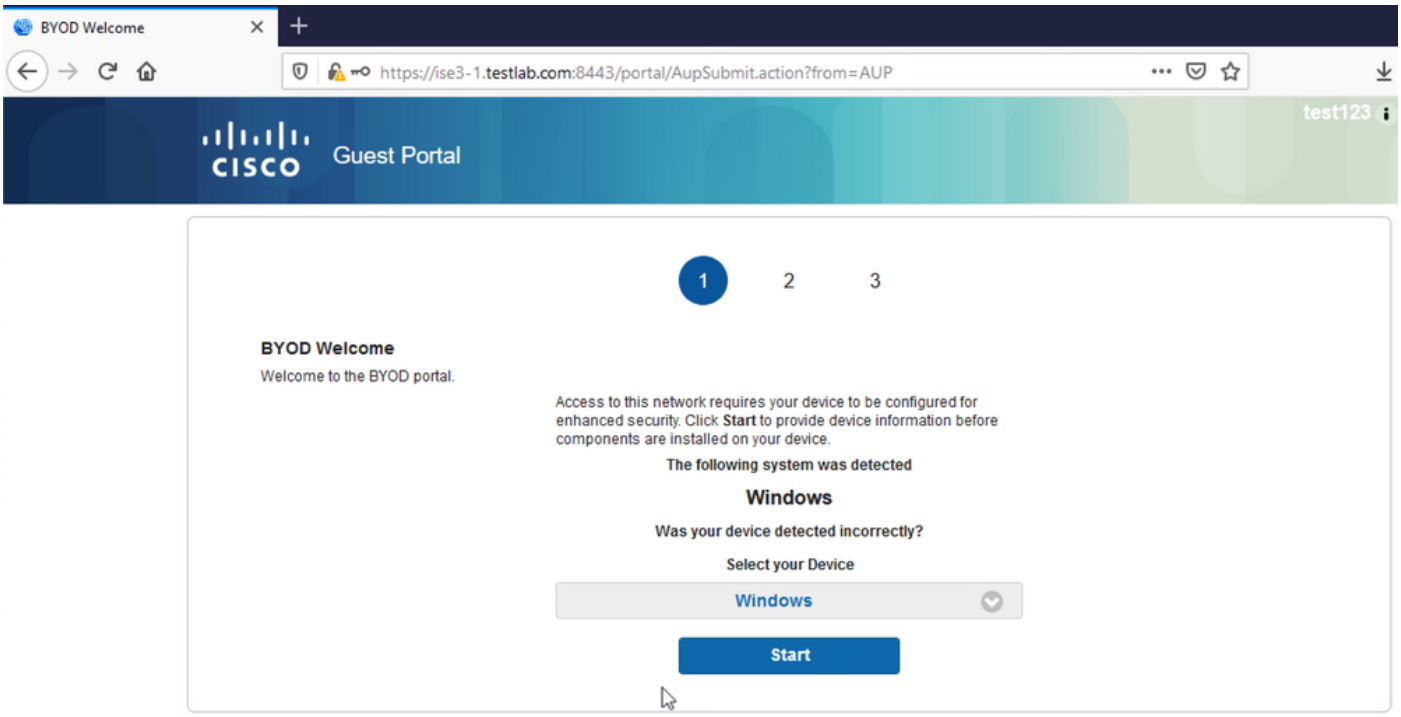
Per impostazione predefinita, i portali guest sono configurati con l'archivio identità Guest_Portal_Sequence:



Si tratta della sequenza di archiviazione interna che tenta prima gli utenti interni (prima degli utenti guest) e quindi le credenziali di Active Directory. Poiché le impostazioni avanzate prevedono di passare all'archivio successivo nella sequenza quando non è possibile accedere a un archivio identità selezionato per l'autenticazione, un dipendente con credenziali interne o credenziali di Active Directory può accedere al portale.



In questa fase del portale guest l'utente fornisce le credenziali definite nell'archivio Utenti interni o in Active Directory e si verifica il reindirizzamento BYOD:



In questo modo gli utenti aziendali possono eseguire BYOD per i dispositivi personali.

Quando invece delle credenziali Internal Users/AD, vengono fornite le credenziali Guest Users, il flusso normale viene proseguito (senza BYOD).

Modifica della VLAN

Consente di eseguire activeX o un'applet Java, che attiva DHCP per il rilascio e il rinnovo. Questa operazione è necessaria quando la funzione CoA attiva la modifica della VLAN per l'endpoint. Quando si usa il protocollo MAB, l'endpoint non rileva una modifica della VLAN. Una soluzione possibile è modificare la VLAN (rilascio/rinnovo DHCP) con l'agente NAC. In alternativa è possibile richiedere un nuovo indirizzo IP tramite l'applet restituito sulla pagina Web. È possibile configurare un ritardo tra rilascio/CoA/rinnovo. Questa opzione non è supportata per i dispositivi mobili.

Informazioni correlate

- Guida alla configurazione dei servizi di postura di Cisco ISE
- BYOD wireless con Identity Services Engine
- Esempio di configurazione del supporto ISE SCEP per BYOD
- Esempio di autenticazione Web centralizzata su WLC e ISE
- Esempio di autenticazione Web centrale con punti di accesso FlexConnect su un WLC con configurazione ISE
- Documentazione e supporto tecnico – Cisco Systems

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).