Configurer le portail invité auto-inscrit ISE

Table des matières

Introduction

Ce document décrit comment configurer et dépanner la fonctionnalité ISE Self Registered Guest Portal.

Conditions préalables

Exigences

Cisco vous recommande d'avoir de l'expérience en matière de configuration ISE et des connaissances de base sur les sujets suivants :

- Déploiements ISE et flux d'invités
- Configuration des contrôleurs LAN sans fil (WLC)

Composants utilisés

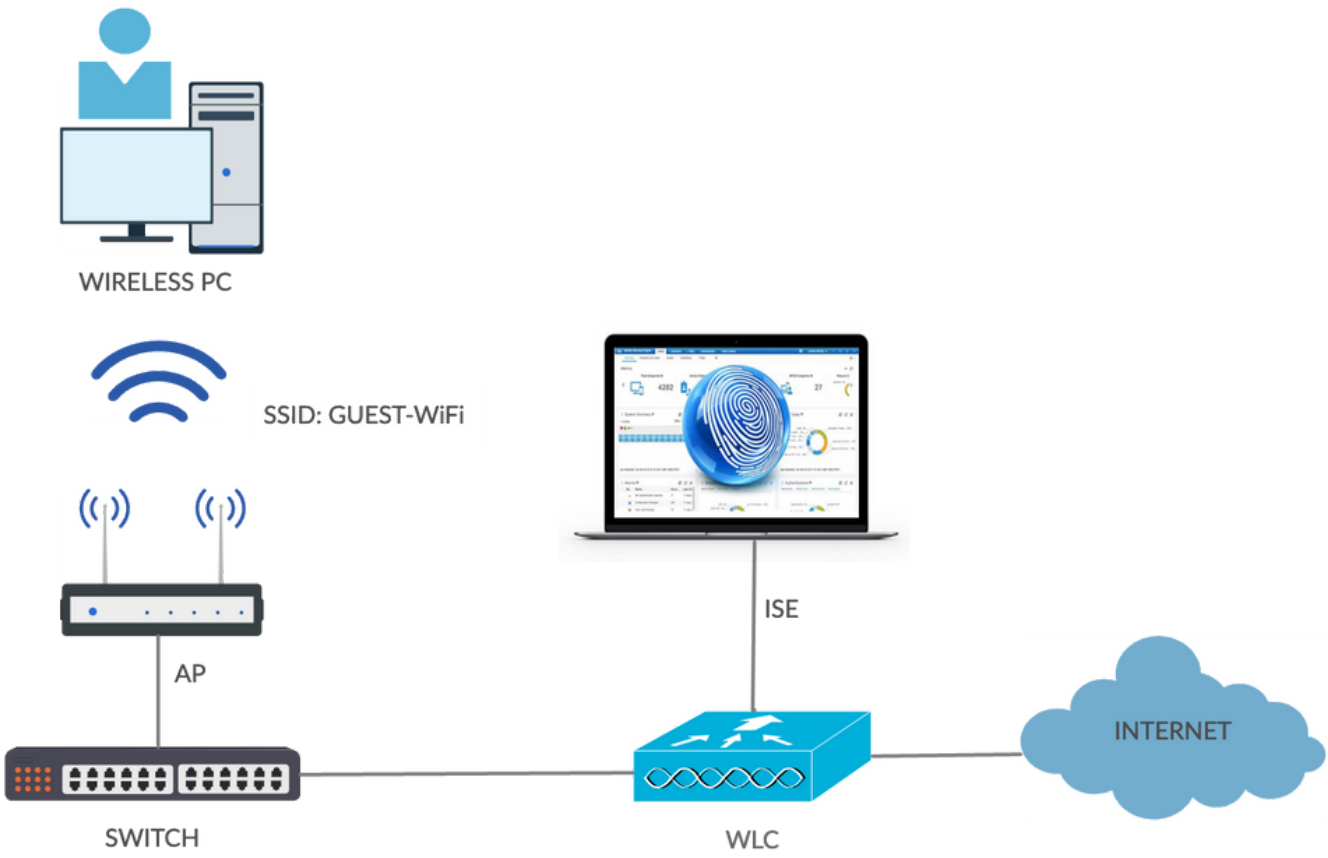
Self Registered Guest Portal, permet aux utilisateurs invités de s'inscrire eux-mêmes avec les employés pour utiliser leurs identifiants AD afin d'accéder aux ressources réseau. Ce portail vous permet de configurer et de personnaliser plusieurs fonctionnalités.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 10 Professionnel
- Cisco WLC 5508 avec version 8.5.135.0
- Logiciel ISE, version 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Topologie et flux



Ce scénario présente plusieurs options disponibles pour les utilisateurs invités lors de l'auto-inscription.

Voici le flux général :

Étape 1. L'utilisateur invité s'associe au SSID (Service Set Identifier) : Guest-WiFi. Il s'agit d'un réseau ouvert avec filtrage MAC avec ISE pour l'authentification. Cette authentification correspond à la deuxième règle d'autorisation sur l'ISE et le profil d'autorisation redirige vers le portail invité auto-enregistré. ISE renvoie un message d'acceptation d'accès RADIUS avec deux paires cisco-av :

- url-redirect-acl (le trafic qui doit être redirigé et le nom de la liste de contrôle d'accès (ACL) définie localement sur le WLC)
- url-redirect (où rediriger ce trafic vers ISE)

Étape 2. L'utilisateur invité est redirigé vers ISE. Plutôt que de fournir des informations d'identification pour se connecter, l'utilisateur clique sur S'inscrire pour accéder aux invités. L'utilisateur est redirigé vers une page où ce compte peut être créé. Un code d'enregistrement secret facultatif peut être activé afin de limiter le privilège d'auto-enregistrement aux personnes qui connaissent cette valeur secrète. Une fois le compte créé, l'utilisateur reçoit des informations d'identification (nom d'utilisateur et mot de passe) et se connecte avec ces informations d'identification.

Étape 3. ISE envoie une nouvelle authentification de changement d'autorisation (CoA) RADIUS au WLC. Le WLC authentifie à nouveau l'utilisateur lorsqu'il envoie la requête d'accès RADIUS avec l'attribut Authorize-Only. ISE répond avec les listes de contrôle d'accès Access-Accept et Airespace définies localement sur le WLC, qui fournit un accès à Internet uniquement (l'accès final pour l'utilisateur invité dépend de la stratégie d'autorisation).

Remarque : dans le cas des sessions EAP (Extensible Authentication Protocol), ISE doit envoyer un message CoA Terminate afin de déclencher une nouvelle authentification, car la session EAP se trouve entre le demandeur et l'ISE. Mais pour le MAB (filtrage MAC), la réauthentification CoA suffit ; il n'est pas nécessaire de dissocier/désauthentifier le client sans fil.

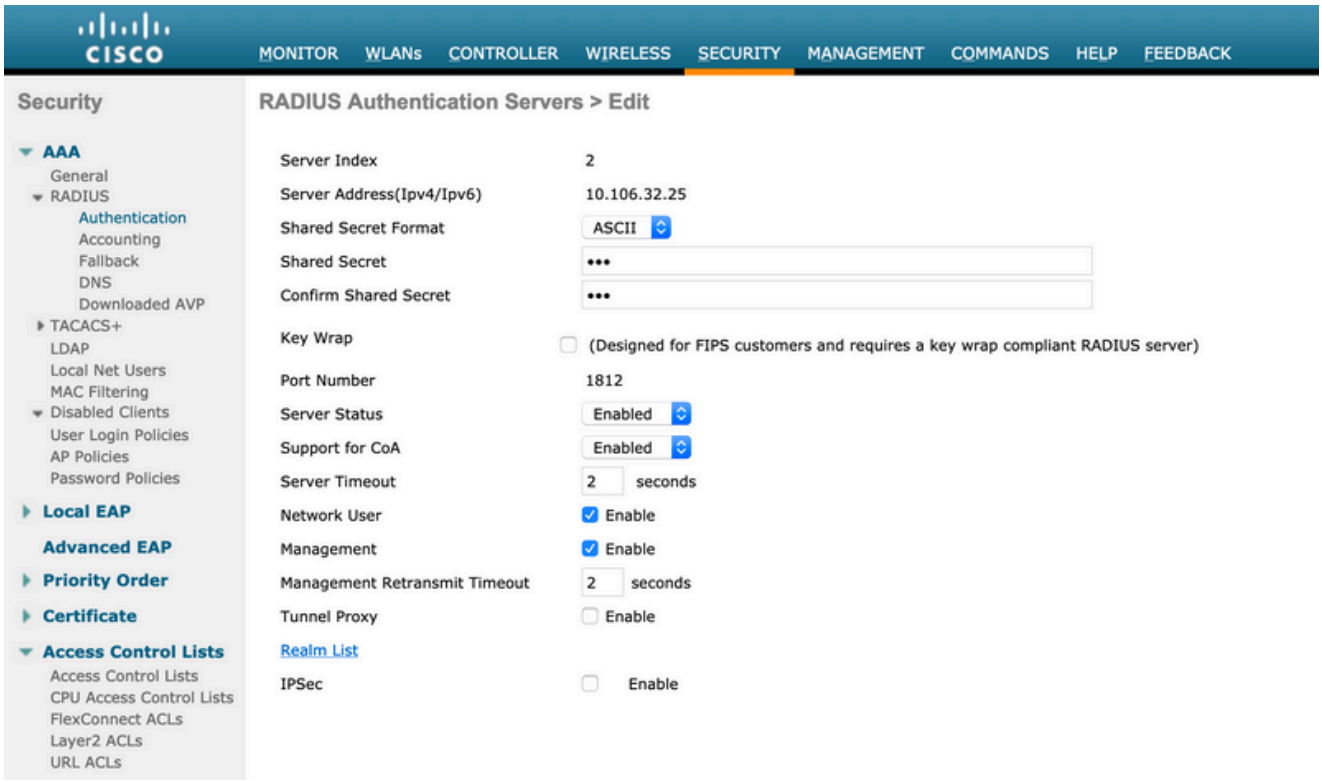
Étape 4. L'utilisateur invité a souhaité accéder au réseau.

Plusieurs fonctionnalités supplémentaires, telles que la posture et le BYOD (Bring Your Own Device), peuvent être activées (voir plus loin).

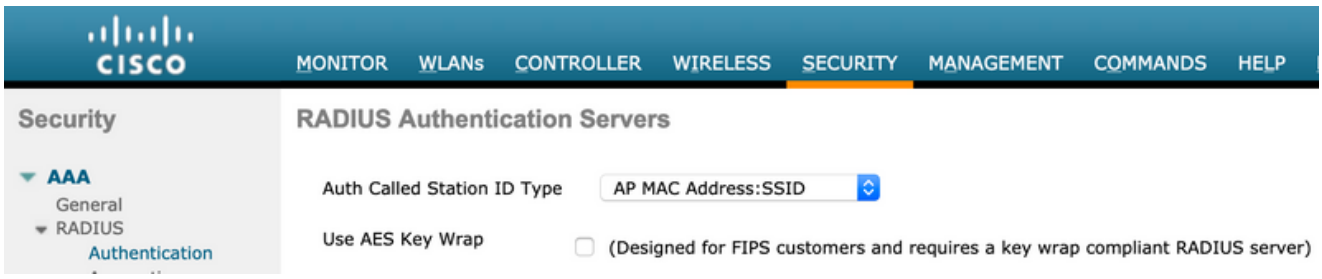
Configurer

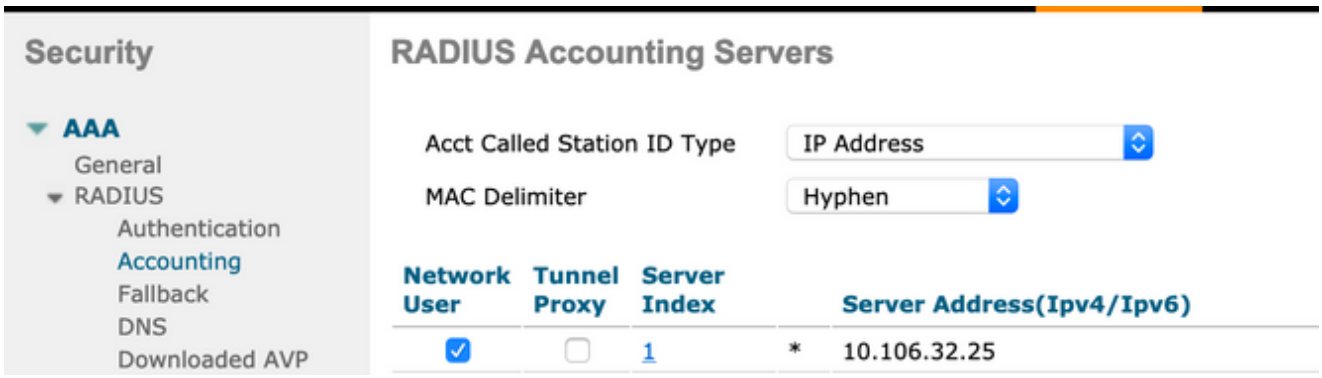
WLC

1. Ajoutez le nouveau serveur RADIUS pour l'authentification et la comptabilité. Accédez à Security > AAA > Radius > Authentication afin d'activer RADIUS CoA (RFC 3576).



Il existe une configuration similaire pour la comptabilité. Il est également conseillé de configurer le WLC pour envoyer le SSID dans l'attribut ID de la station appelée, ce qui permet à l'ISE de configurer des règles flexibles basées sur le SSID :





2. Sous l'onglet WLANs (Réseaux locaux sans fil), créez le WLAN Guest-WiFi et configurez l'interface appropriée. Définissez la sécurité de la couche 2 sur None avec le filtrage MAC. Dans Serveurs AAA (Security/Authentication, Authorization, and Accounting), sélectionnez l'adresse IP ISE pour l'authentification et la comptabilité. Dans l'onglet Advanced, activez AAA Override et définissez l'état Network Admission Control (NAC) sur ISE NAC (prise en charge CoA).

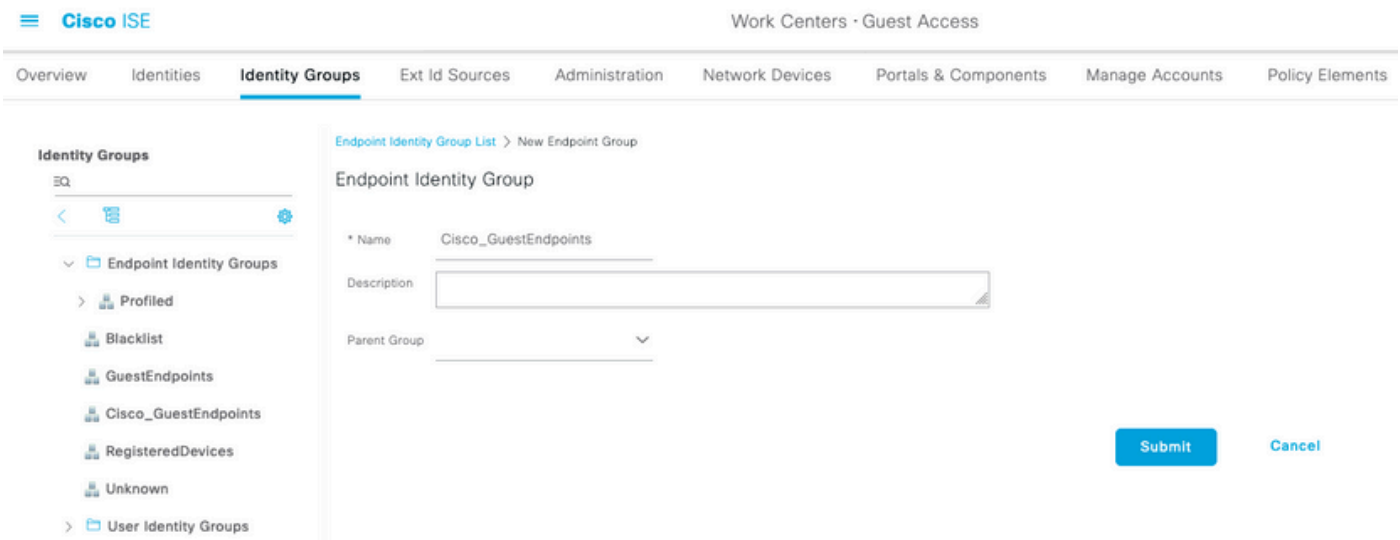
3. Accédez à Sécurité > Listes de contrôle d'accès > Listes de contrôle d'accès et créez deux listes d'accès :

    - GuestRedirect, qui autorise le trafic qui ne doit pas être redirigé et redirige tout autre trafic
    - Internet, qui est refusé pour les réseaux d'entreprise et autorisé pour tous les autres

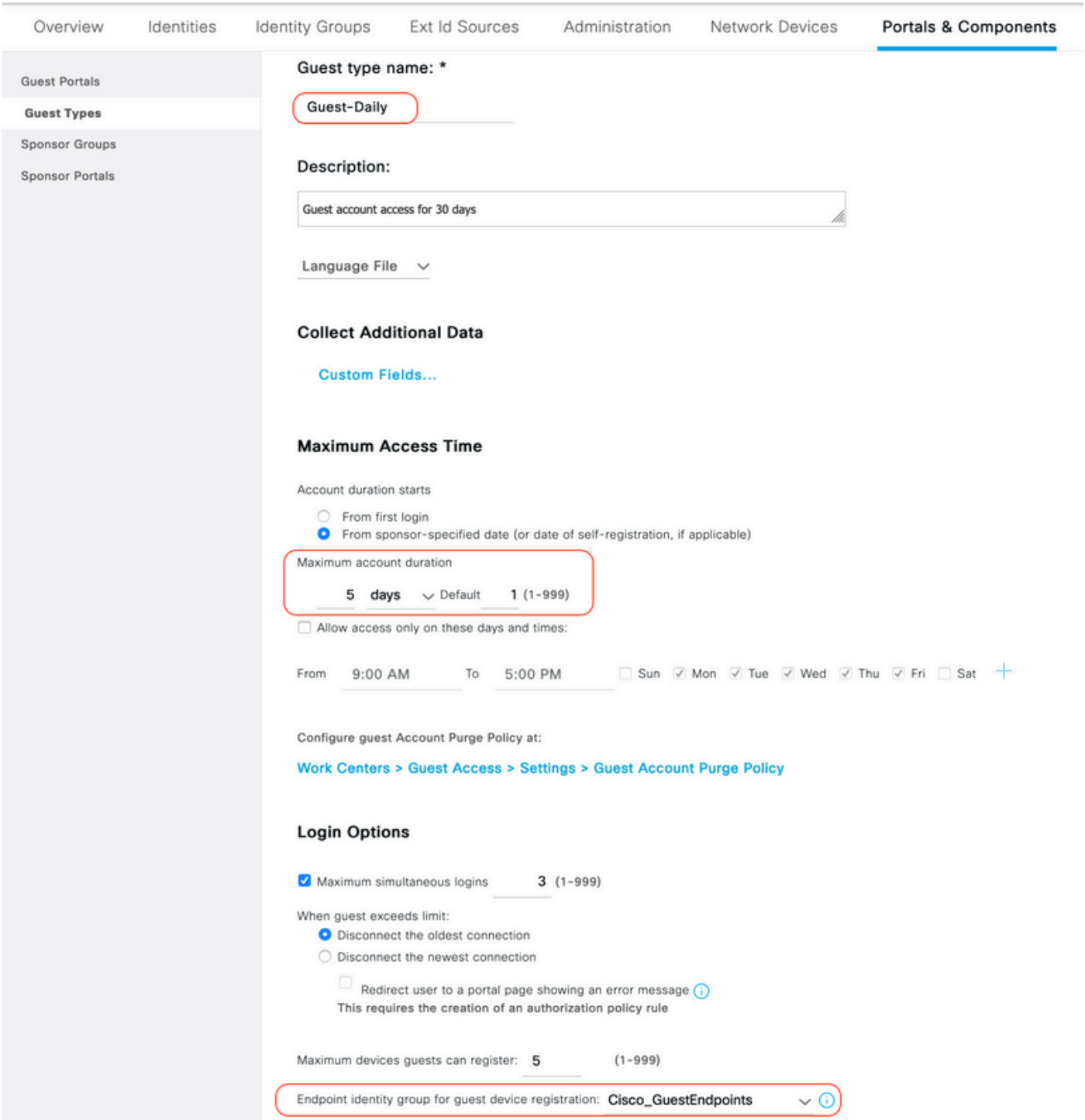
    Voici un exemple pour la liste de contrôle d'accès GuestRedirect (besoin d'exclure le trafic vers/depuis ISE de la redirection) :

ISE

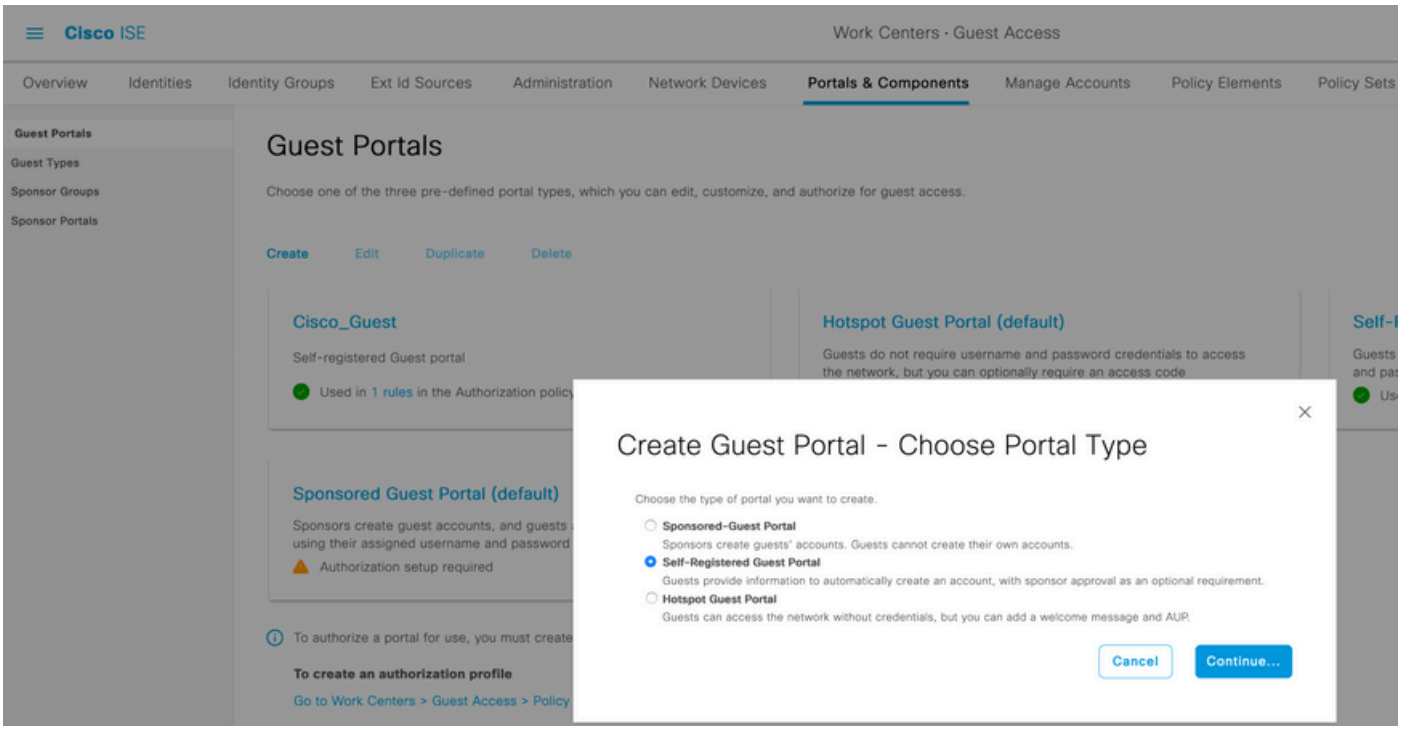
1. Ajoutez le WLC en tant que périphérique d'accès réseau à partir de Work Centers > Guest Access > Network Devices.
2. Créez un groupe d'identités de point de terminaison. Accédez à Work Centers > Guest Access > Identity Groups > Endpoint Identity Groups.



3. Créez un type d'invité en accédant à Centres de travail > Accès invité > Portail et composants > Types d'invité. Reportez-vous au groupe d'identités de point de terminaison précédemment créé sous ce nouveau type d'invité et cet enregistrement.



4. Créez un nouveau type de portail d'invité : portail d'invité auto-inscrit. Accédez à Work Centers > Guest Access > Guest Portals.

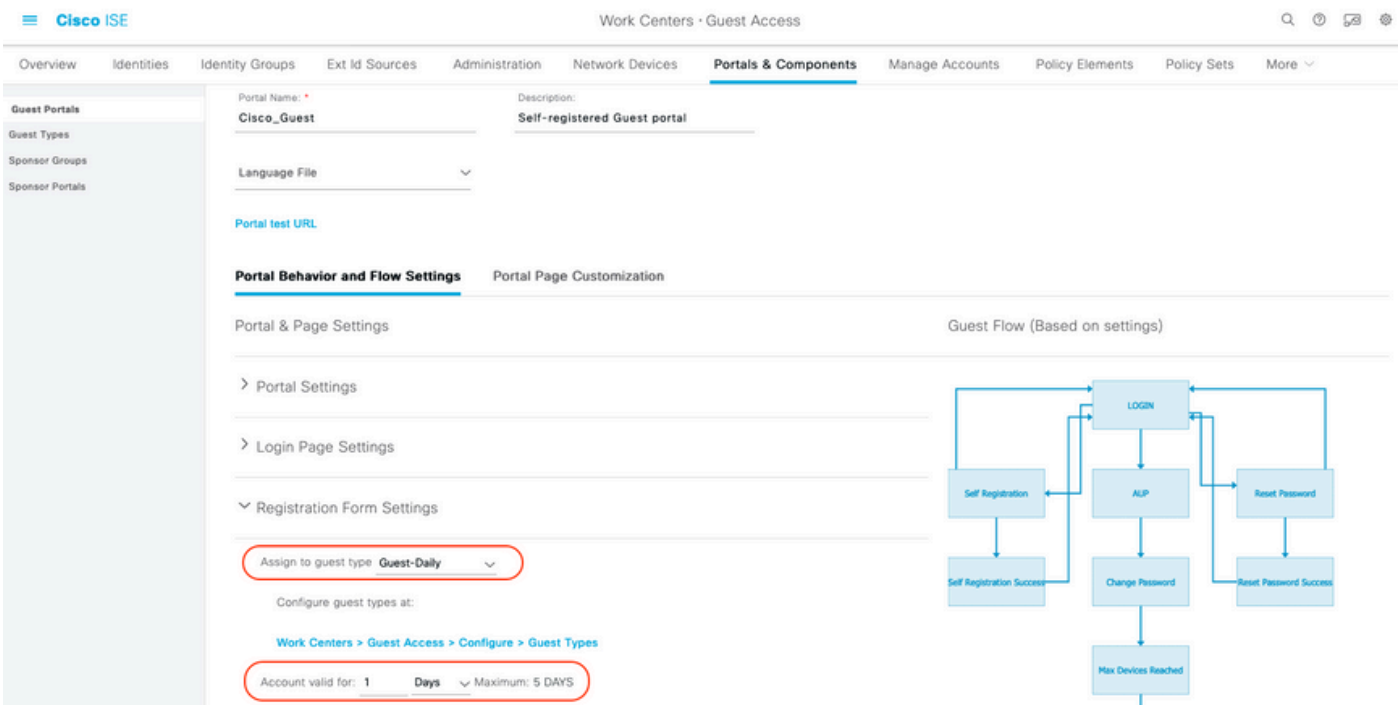


5. Choisissez le nom du portail, reportez-vous au type d'invité créé précédemment et envoyez les paramètres de notification d'informations d'identification sous Paramètres du formulaire d'inscription pour envoyer les informations d'identification par e-mail.

Reportez-vous à ce document pour savoir comment configurer le serveur SMTP sur ISE :

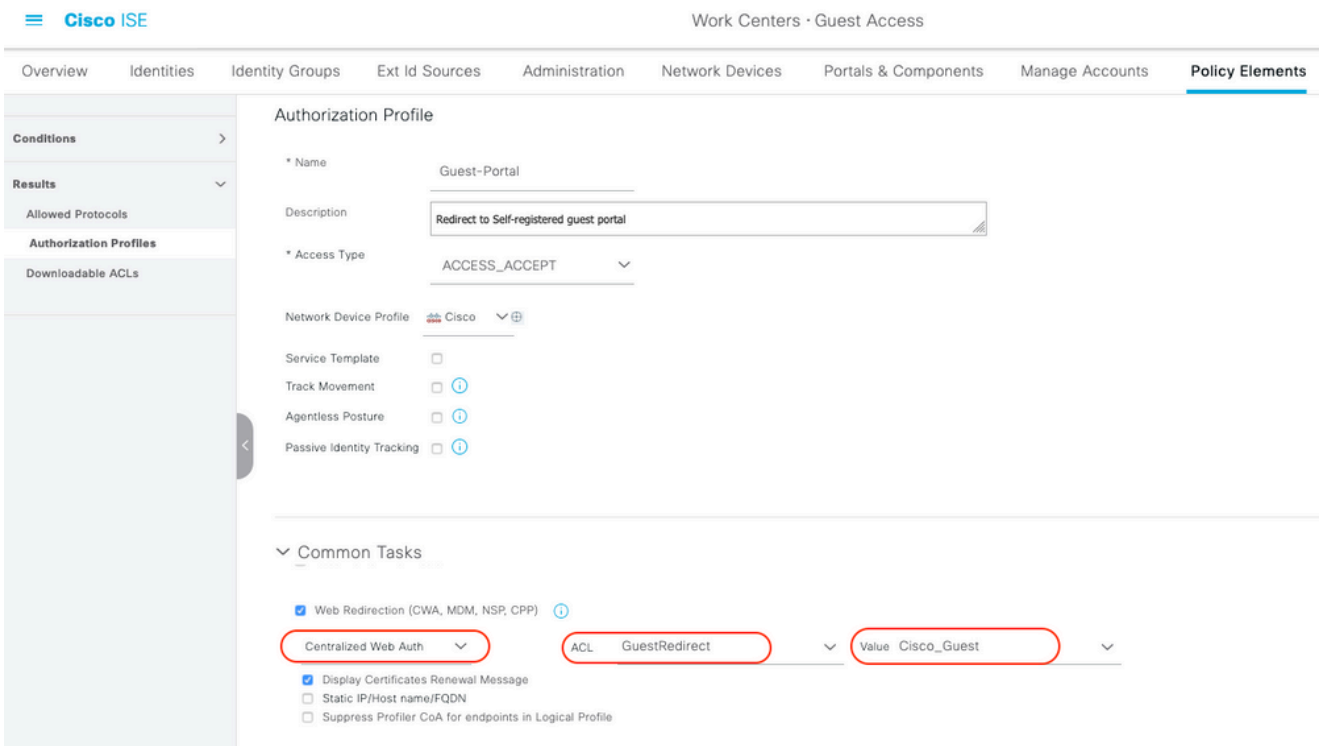
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html

Conservez tous les autres paramètres par défaut. Sous Personnalisation des pages du portail, toutes les pages présentées peuvent être personnalisées. Par défaut, le compte Invité est valide pendant 1 jour et peut être étendu au nombre de jours configuré sous le type d'invité spécifique.

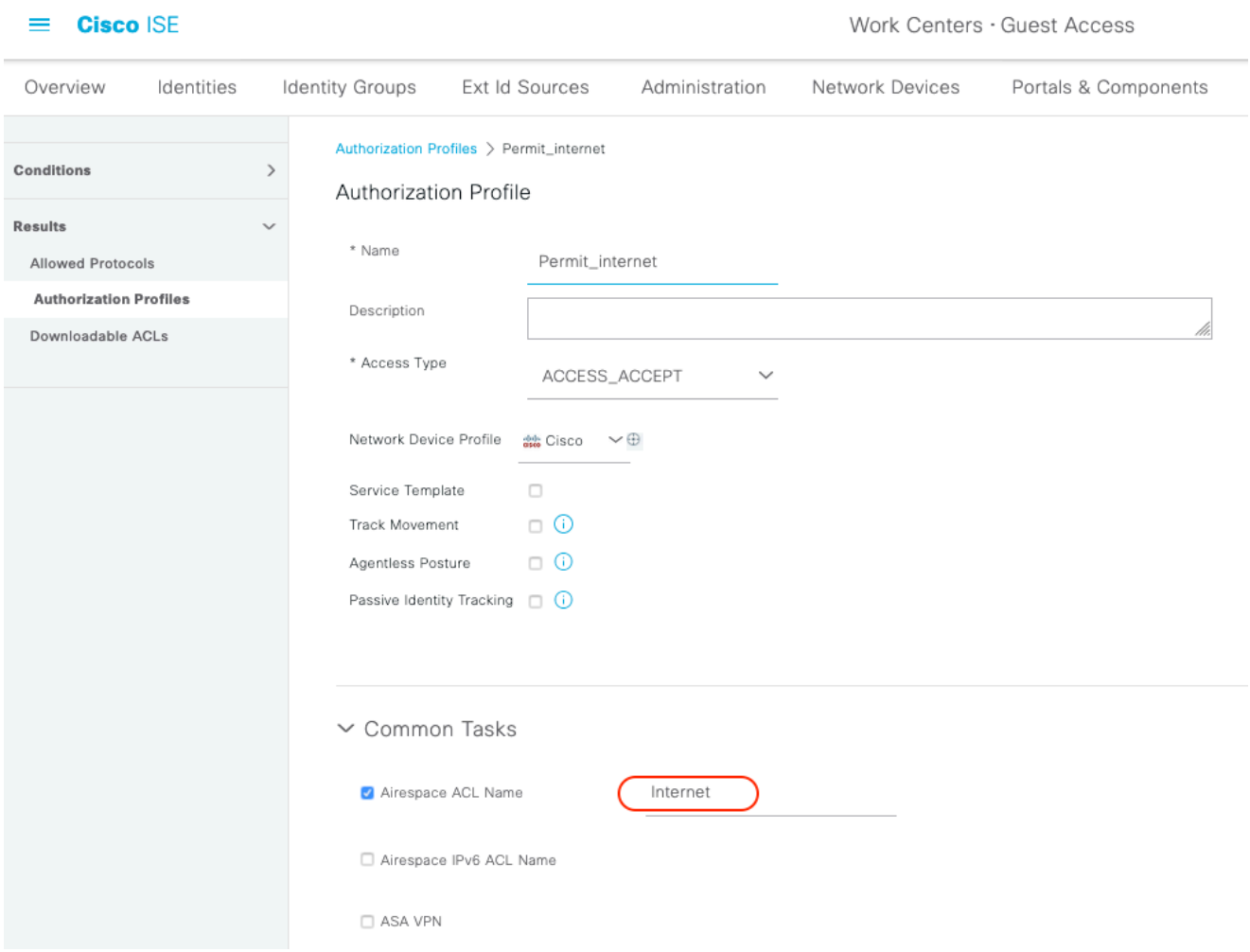


6. Configurez ces deux profils d'autorisation en accédant à Centres de travail > Accès invité > Éléments de stratégie > Résultats > Profils d'autorisation.

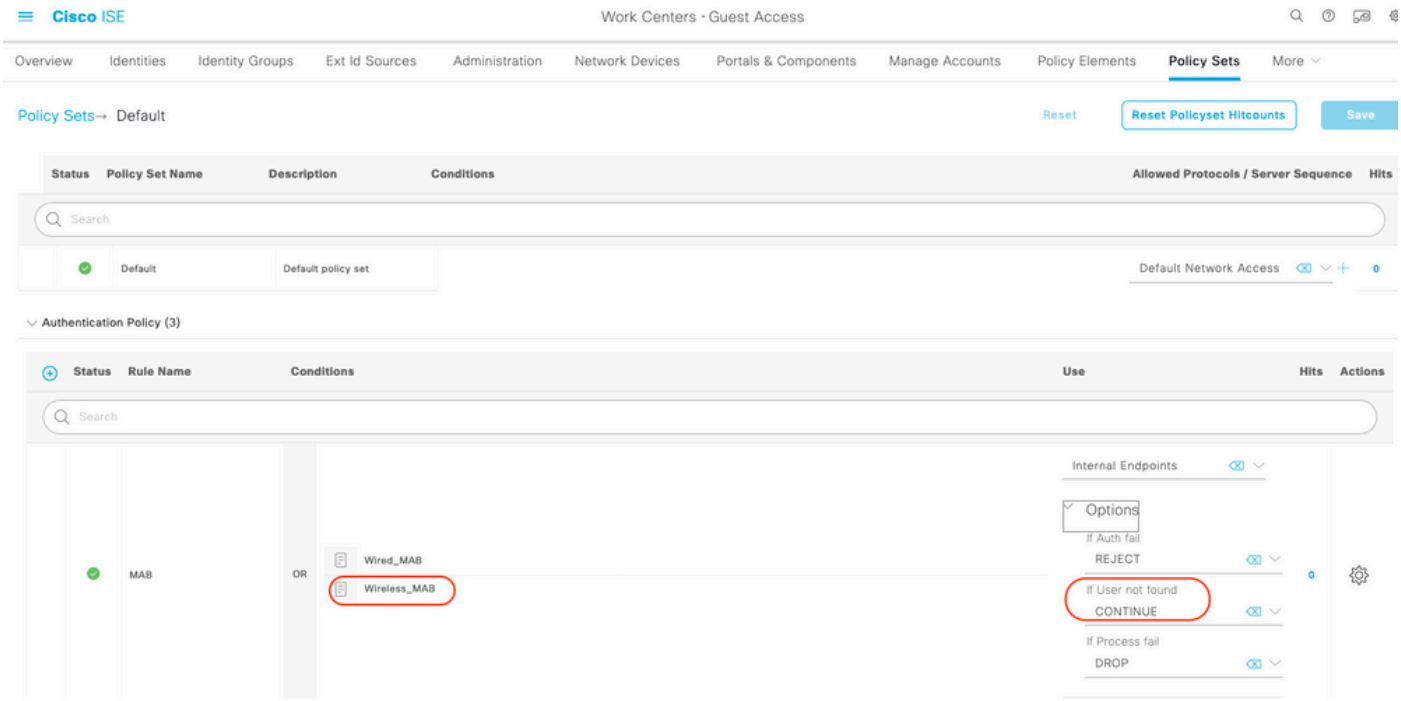
- Guest-Portal (avec redirection vers Guest Portal Cisco_Guest et une ACL de redirection nommée GuestRedirect). Cette ACL GuestRedirect a été créée précédemment sur WLC.



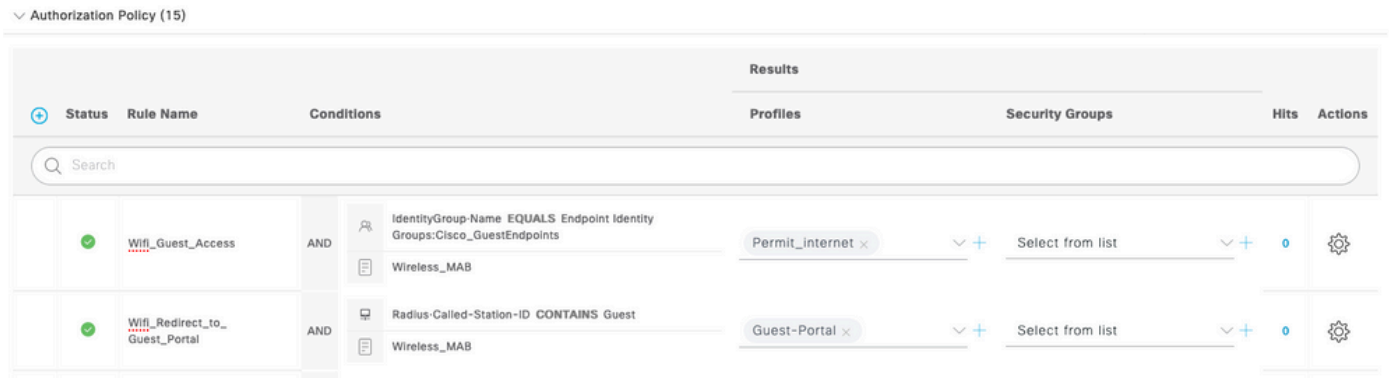
- Permit_Internet (avec la liste de contrôle d'accès Airespace égale Internet)



7. Modifiez le jeu de stratégies nommé Default. Le jeu de stratégies par défaut est préconfiguré pour l'accès au portail Invité. Une stratégie d'authentification nommée MAB est présente, ce qui permet à l'authentification MAC Authentication Bypass (MAB) de continuer (et non de rejeter) pour les adresses Mac inconnues.



8. Accédez à la stratégie d'autorisation sur la même page. Créez ces règles d'autorisation, comme illustré dans cette image.



Les nouveaux utilisateurs associés au SSID Invité ne font pas encore partie d'un groupe d'identité et correspondent donc à la deuxième règle et sont redirigés vers Guest Portal.

Une fois que l'utilisateur s'est connecté avec succès, ISE envoie un RADIUS CoA et le WLC effectue une nouvelle authentification. Cette fois, la première règle d'autorisation est mise en correspondance (lorsque le point de terminaison fait partie du groupe d'identité de point de terminaison défini) et l'utilisateur obtient le profil d'autorisation Permit_internet.

9. Nous pouvons également fournir un accès temporaire aux invités en utilisant la condition Guest flow. Cette condition vérifie les sessions actives sur ISE et elle est attribuée. Si cette session a l'attribut indiquant que l'utilisateur précédemment invité s'est authentifié avec succès, la condition est satisfaite. Une fois qu'ISE a reçu le message d'arrêt de comptabilité Radius de la part du périphérique d'accès réseau (NAD), la session est interrompue et supprimée ultérieurement. À ce stade, la condition Network Access:UseCase = Guest Flow n'est plus satisfaite. Par conséquent, toutes les authentifications suivantes de ce point de terminaison accèdent à la redirection de règle générique pour l'authentification d'invité.

Remarque : vous pouvez utiliser à la fois l'accès Invité temporaire ou l'accès Invité permanent, mais pas les deux.

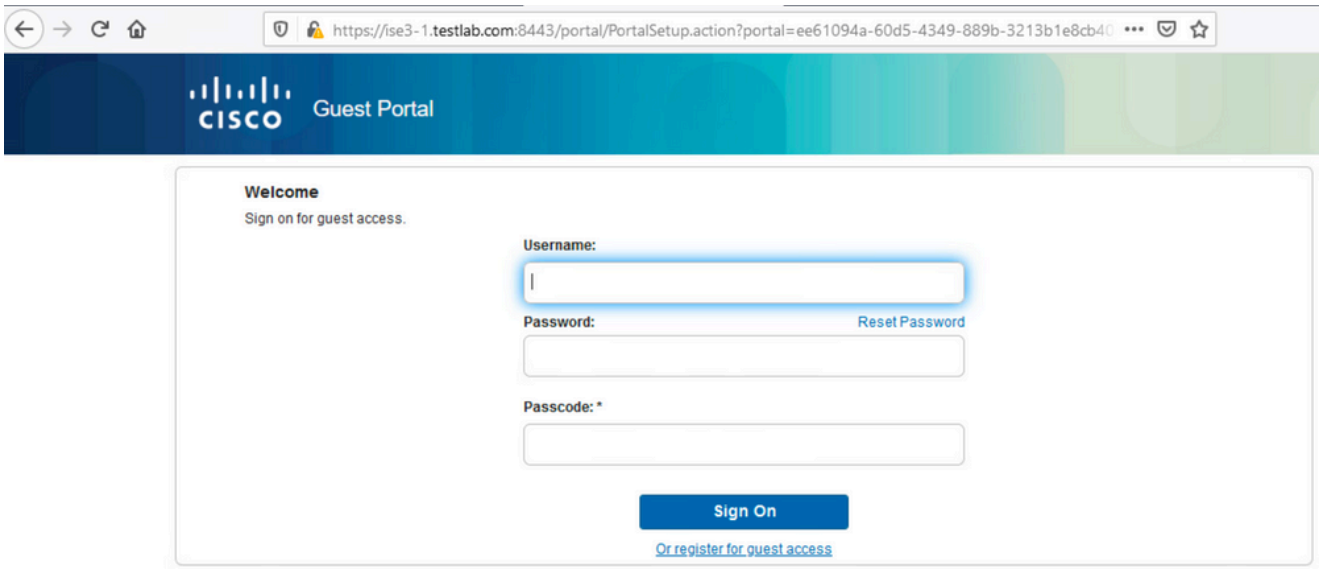
Reportez-vous à ce document pour une configuration détaillée de l'accès temporaire et permanent des invités ISE.

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

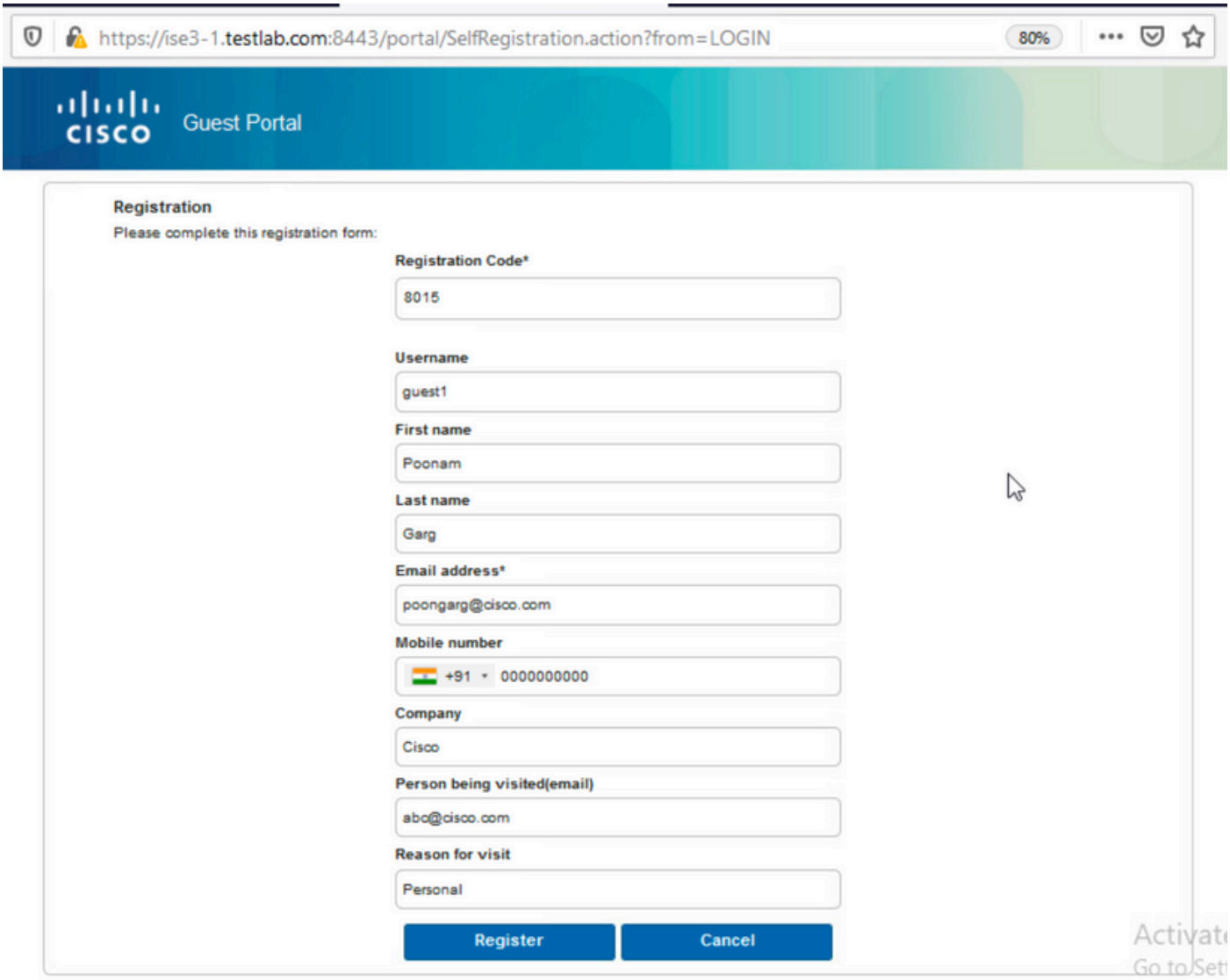
Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

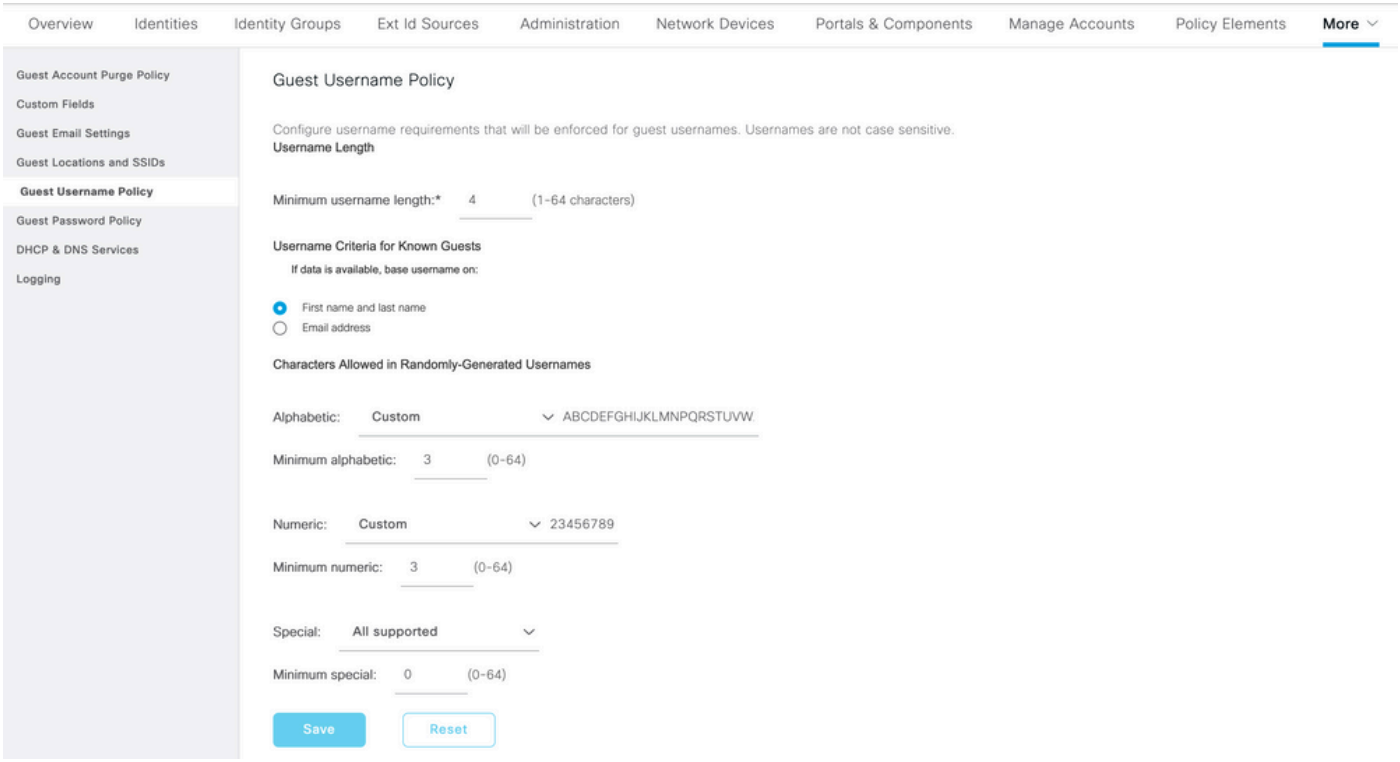
1. Une fois que vous vous êtes associé au SSID invité et que vous avez tapé une URL, vous êtes redirigé vers la page Guest Portal, comme illustré dans l'image.



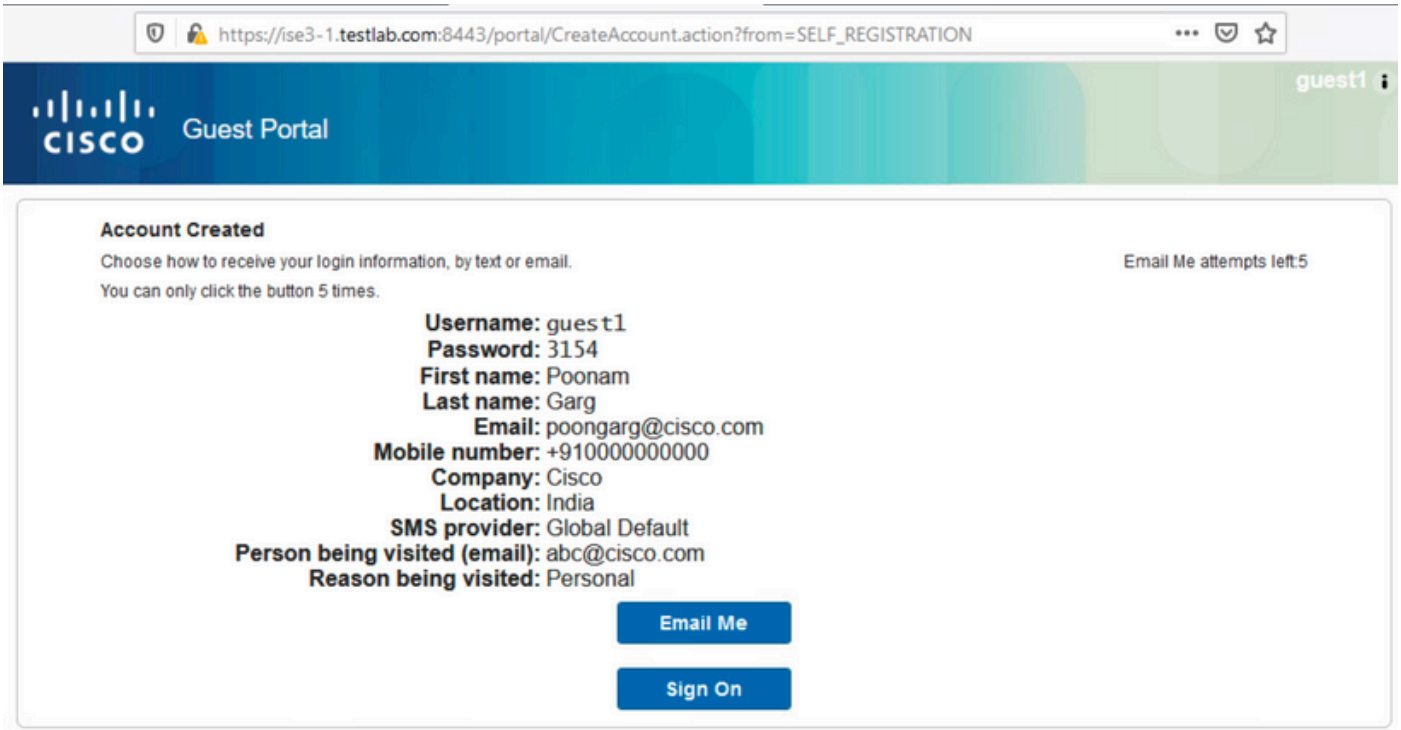
2. Comme vous ne disposez pas encore d'informations d'identification, vous devez choisir l'option Register for Guest access. Le formulaire d'inscription vous est présenté pour créer le compte. Si l'option Code d'enregistrement a été activée dans la configuration du portail invité, cette valeur secrète est requise (ce qui garantit que seules les personnes disposant des autorisations correctes sont autorisées à s'enregistrer elles-mêmes).

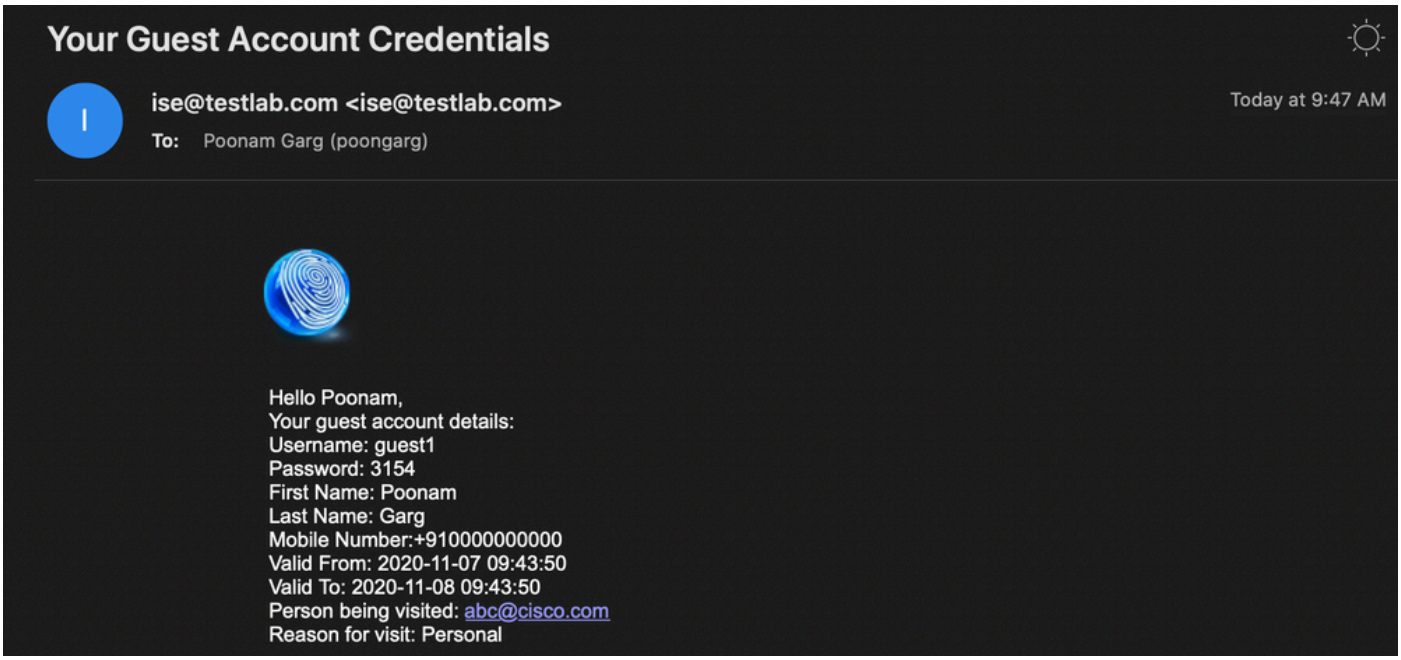


3. Si vous rencontrez des problèmes avec le mot de passe ou la stratégie utilisateur, accédez à Work Centers > Guest Access > Settings > Guest Username Policy afin de modifier les paramètres. Voici un exemple :

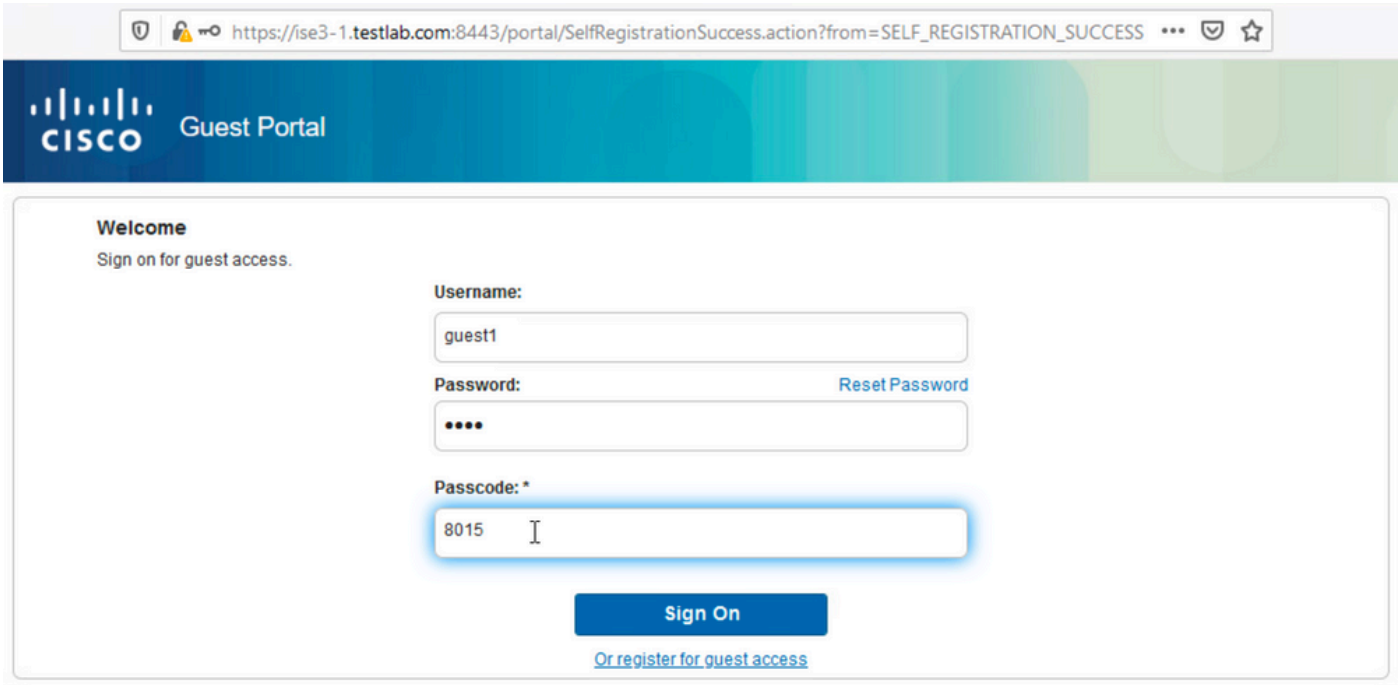


4. Après la création réussie du compte, vous êtes présenté avec les informations d'identification (mot de passe généré selon les stratégies de mot de passe invité) également l'utilisateur invité obtient la notification par e-mail si elle est configurée :

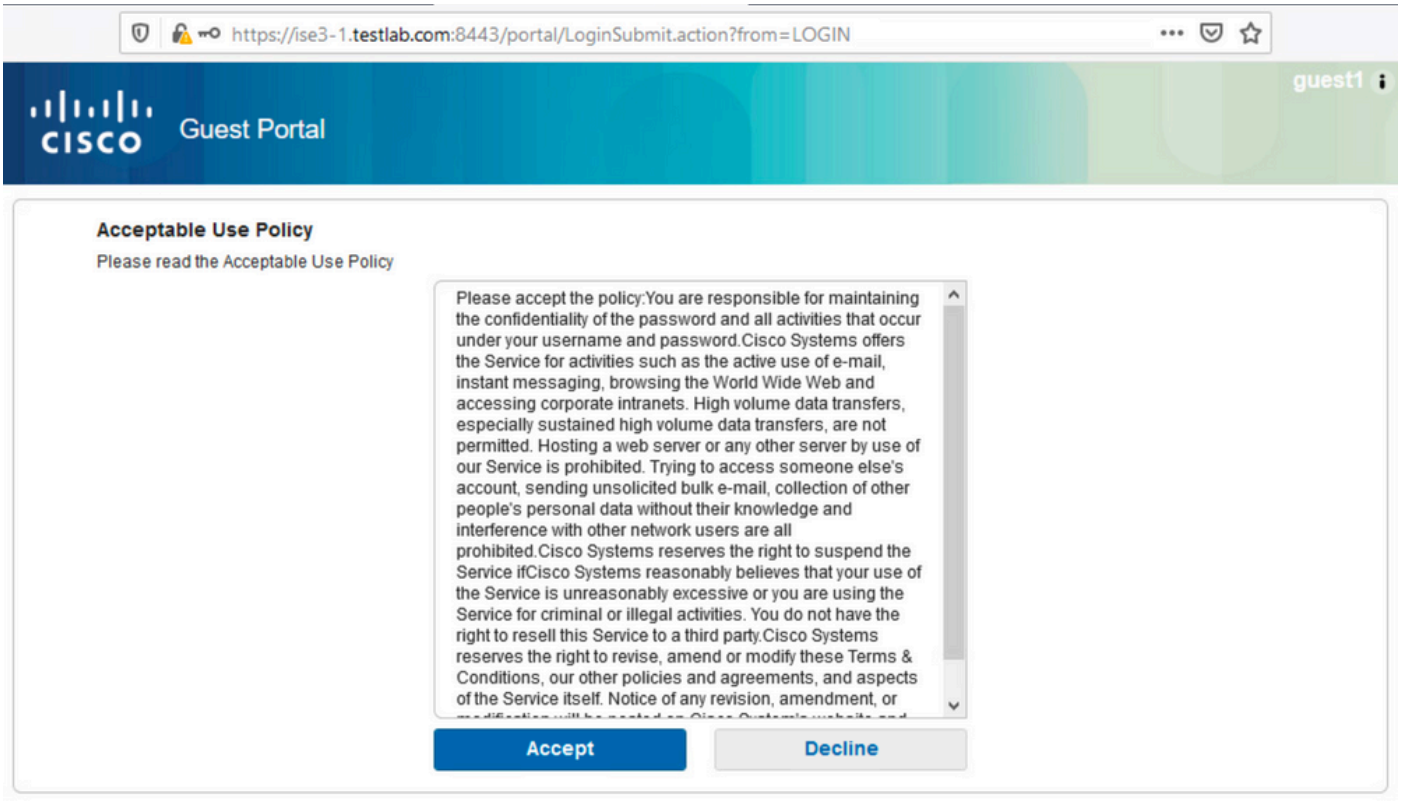


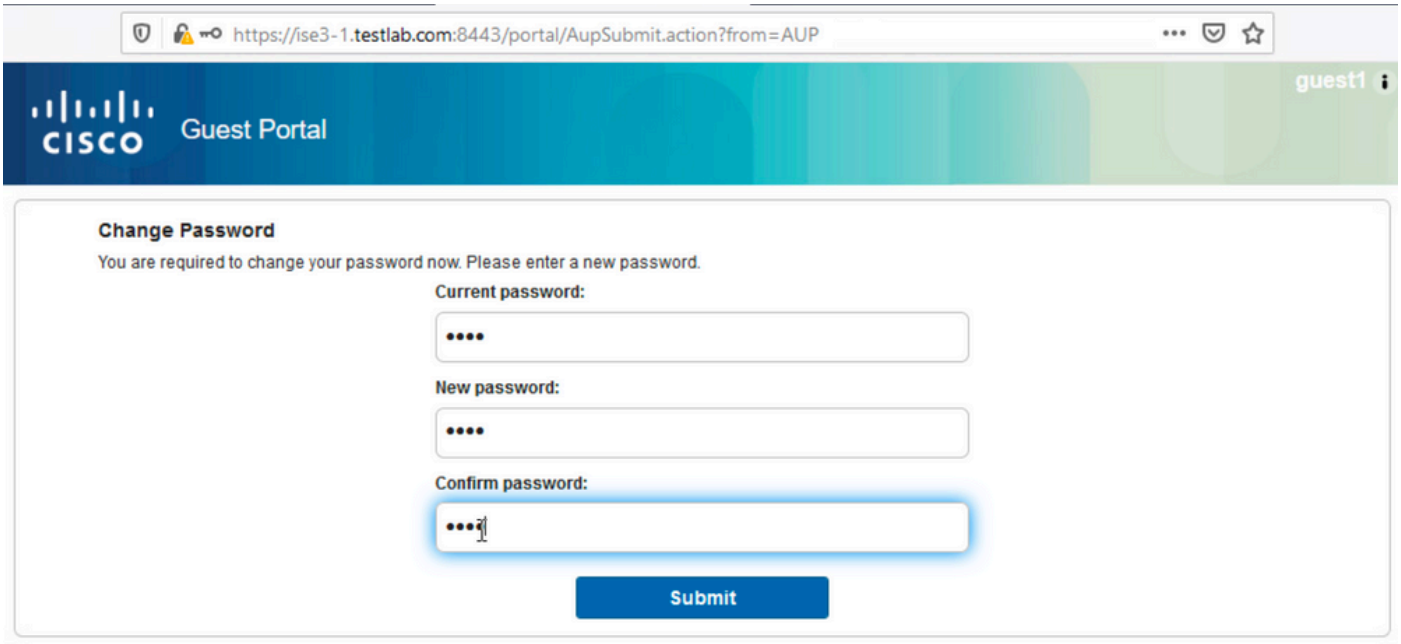


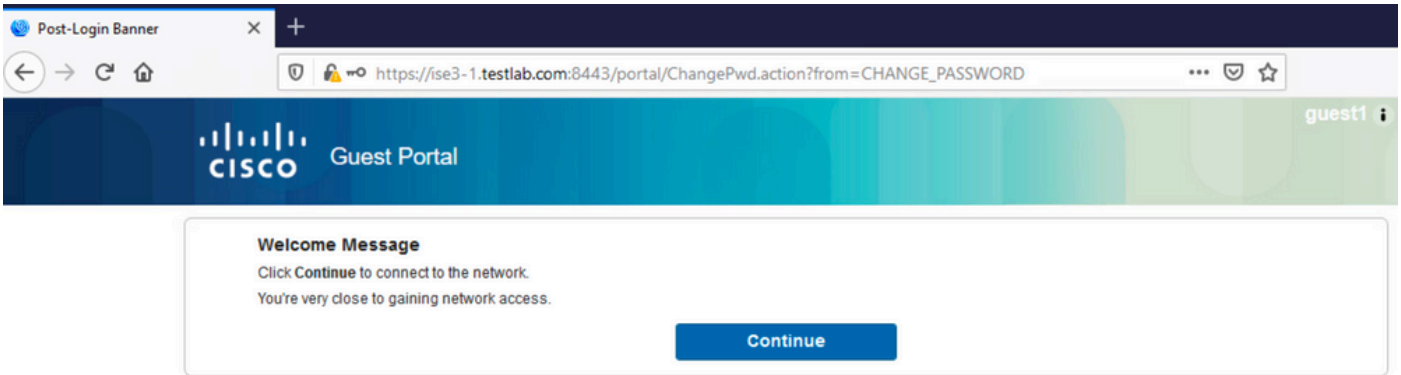
5. Cliquez sur Sign On et fournissez des informations d'identification (un code d'accès supplémentaire peut être requis s'il est configuré sous le portail invité ; il s'agit d'un autre mécanisme de sécurité qui permet uniquement à ceux qui connaissent le mot de passe de se connecter).



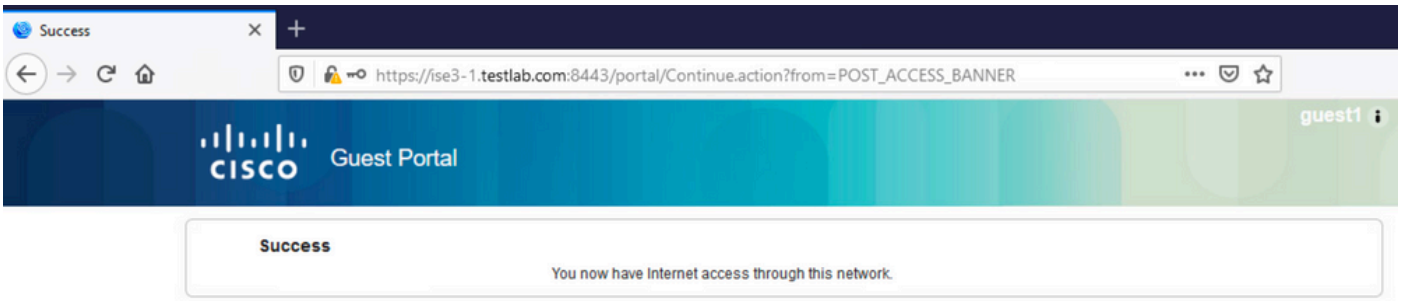
6. Une fois l'opération terminée, une politique d'utilisation acceptable (AUP) facultative peut être présentée (si elle est configurée dans le portail invité). L'utilisateur reçoit une option de modification de mot de passe et la bannière post-connexion (également configurable sous Guest Portal) peut également s'afficher.


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

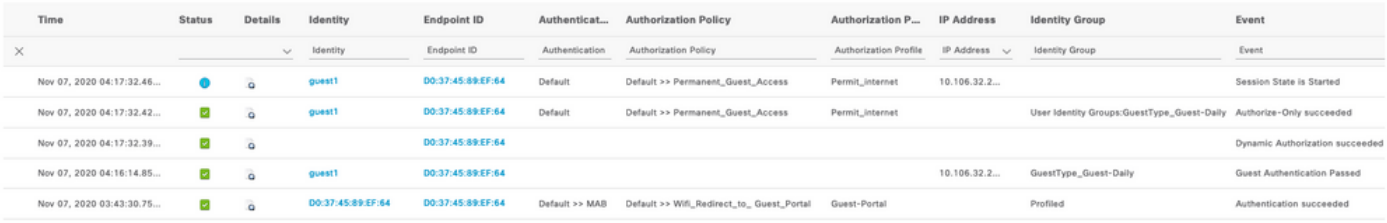
7. La dernière page (Bannière post-connexion) confirme que l'accès a été accordé :



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

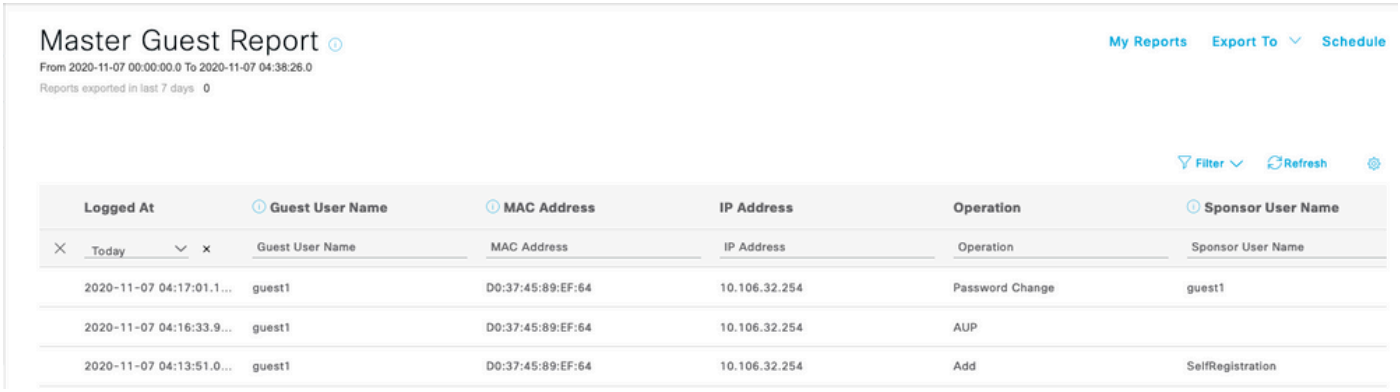
À ce stade, ISE présente ces journaux sous Operations > RADIUS > Live Logs, comme illustré dans l'image.



Voici le flux :

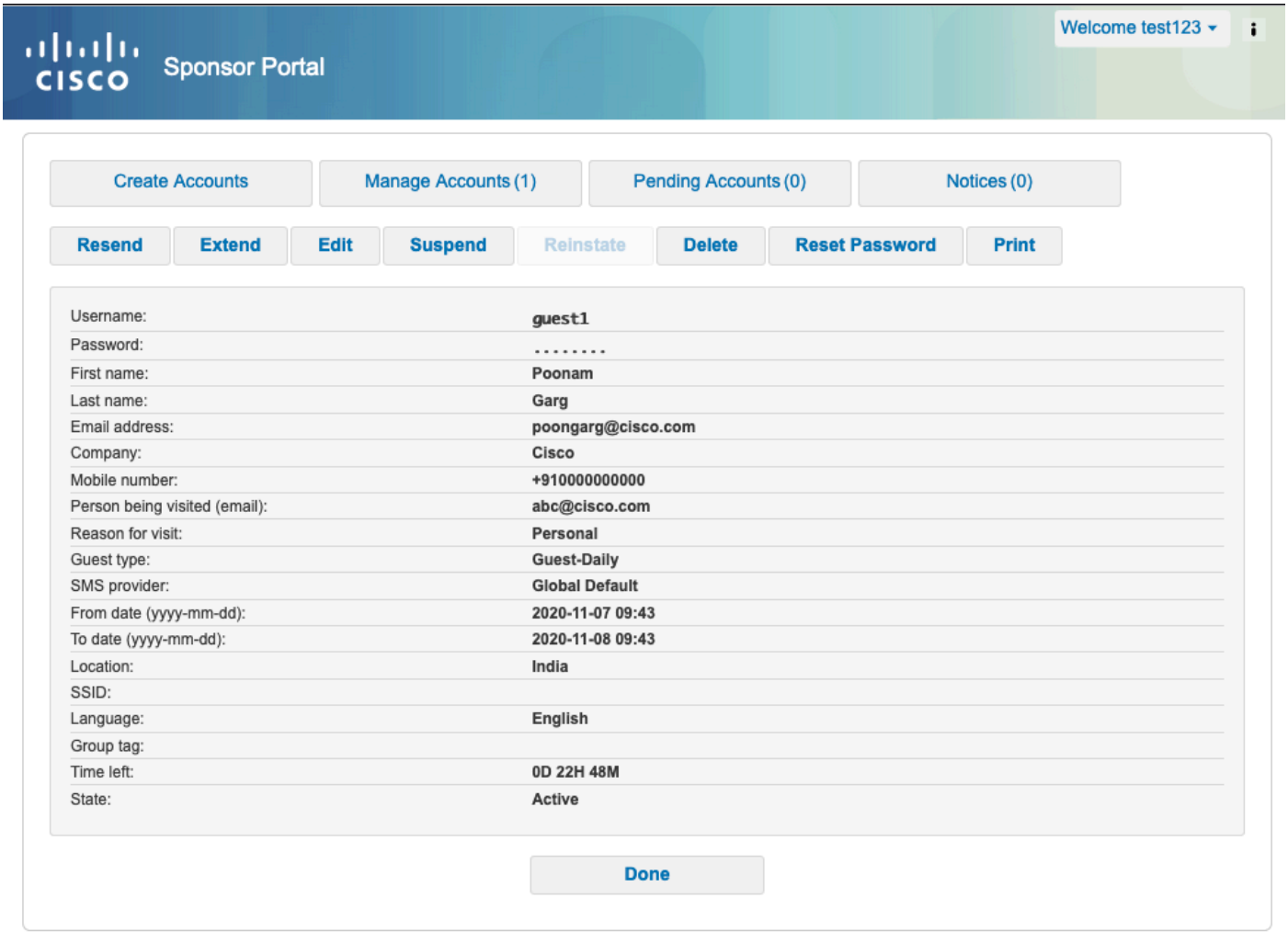
- L'utilisateur invité rencontre la deuxième règle d'autorisation (Wifi_Redirect_to_Guest_Portal) et est redirigé vers Guest-Portal (authentification réussie).
- L'invité est redirigé pour l'auto-inscription. Après une connexion réussie (avec le compte nouvellement créé), ISE envoie la réauthentification CoA, qui est confirmée par le WLC (Dynamic Authorization successful).
- Le WLC effectue une nouvelle authentification avec l'attribut Authorize-Only et le nom de la liste de contrôle d'accès est retourné (Authorize-Only a réussi). L'accès réseau correct est fourni à l'invité.

Les rapports (Opérations > Rapports > Invité > Rapport invité principal) confirment également que :



Un utilisateur parrain (disposant des privilèges appropriés) peut vérifier l'état actuel d'un utilisateur invité.

Cet exemple confirme que le compte est créé et que l'utilisateur est connecté au portail :



Configuration facultative

Pour chaque étape de ce flux, différentes options peuvent être configurées. Toutes ces options sont configurées dans le portail Invité de Work Centers > Guest Access > Portals & Components > Guest Portals > Portal Name > Edit > Portal Behavior and Flow Settings. Les paramètres les plus importants sont les suivants :

Paramètres d'auto-inscription

- Type d'invité : décrit la durée d'activité du compte, les options d'expiration du mot de passe, les heures d'ouverture de session et les options (il s'agit d'un mélange de profil de temps et de rôle d'invité)
- Code d'enregistrement : si cette option est activée, seuls les utilisateurs qui connaissent le code secret sont autorisés à s'enregistrer (ils doivent fournir le mot de passe lors de la création du compte)
- AUP - Accepter la politique d'utilisation lors de l'auto-inscription
- L'exigence pour le sponsor d'approuver/activer le compte invité.

Paramètres de connexion invité

- Code d'accès : si cette option est activée, seuls les utilisateurs invités qui connaissent le code secret sont autorisés à se connecter.
- AUP - Accepter la politique d'utilisation lors de l'auto-inscription.
- Option de modification du mot de passe.

Paramètres d'enregistrement des périphériques

- Par défaut, le périphérique est enregistré automatiquement.

Paramètres de conformité des périphériques invités

- Permet une posture dans le flux.

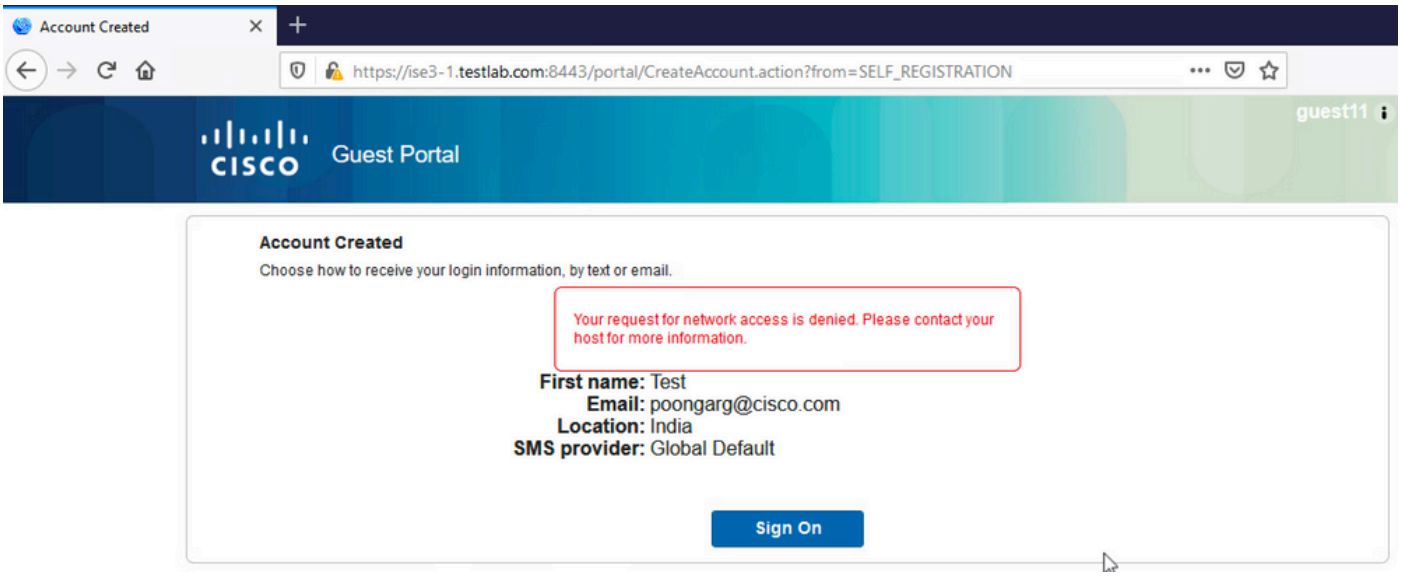
Paramètres BYOD

- Permet aux utilisateurs professionnels qui utilisent le portail en tant qu'invités d'enregistrer leurs appareils personnels.

Comptes approuvés par le sponsor

Si l'option Exiger que les invités soient approuvés est sélectionnée sous Paramètres du formulaire d'inscription, alors le compte créé par l'invité doit être approuvé par un sponsor. Cette fonctionnalité peut utiliser l'e-mail afin d'envoyer une notification au sponsor (pour l'approbation du compte invité) :

Si le serveur SMTP (Simple Mail Transfer Protocol) est mal configuré, le compte n'est pas créé :



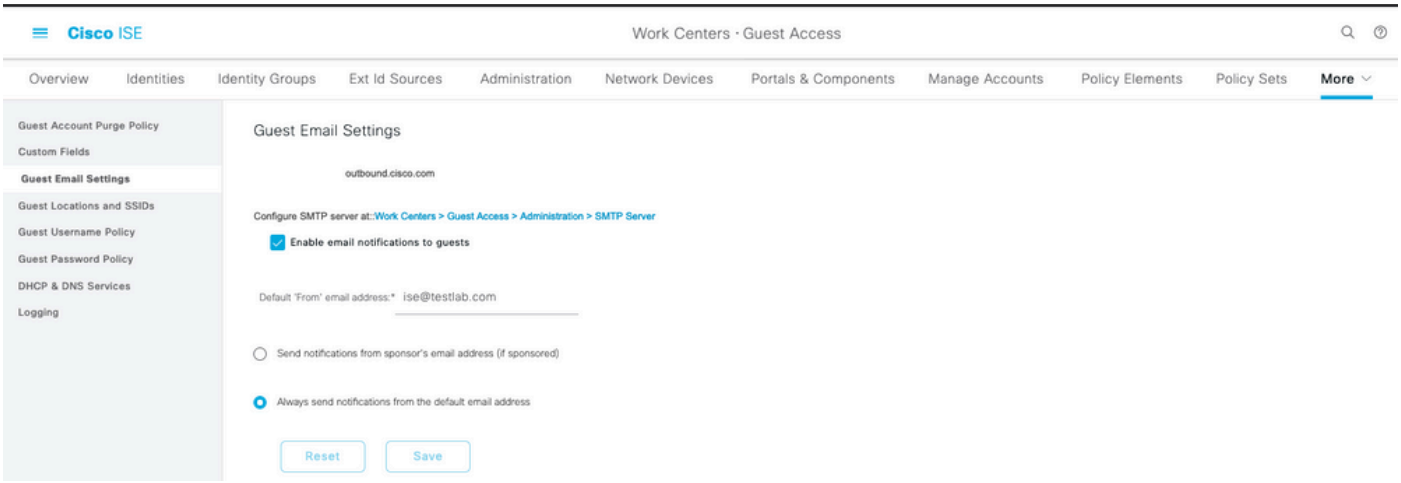
Le journal du fichier guest.log confirme qu'un problème est survenu lors de l'envoi de la notification d'approbation au courrier électronique du sponsor, car le serveur SMTP est mal configuré :

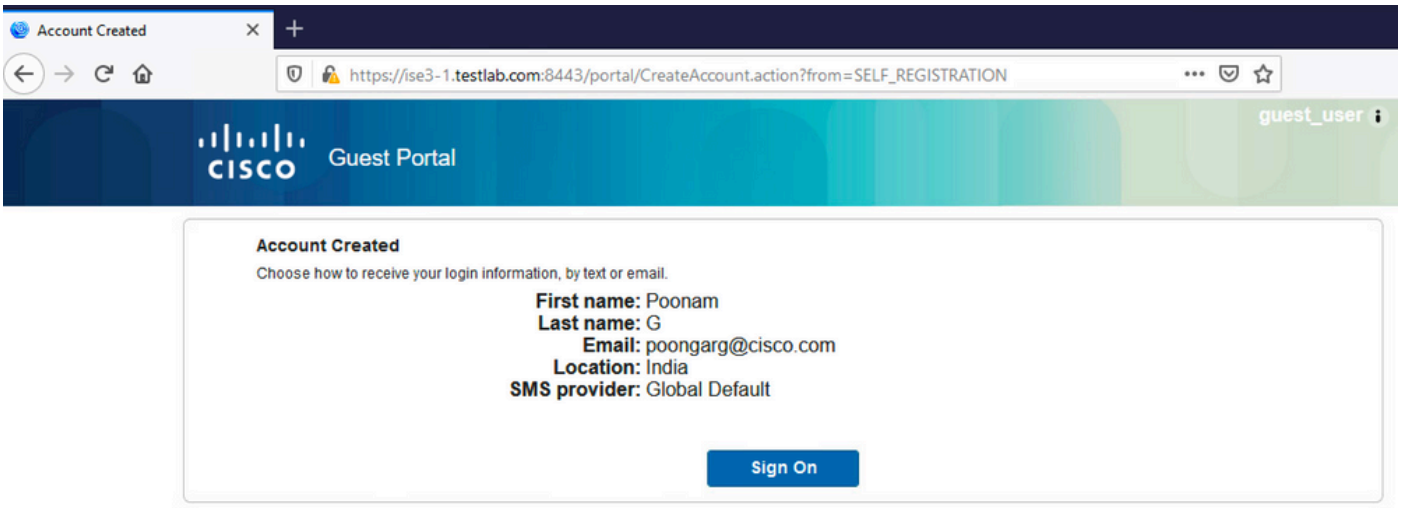
<#root>

```
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
```

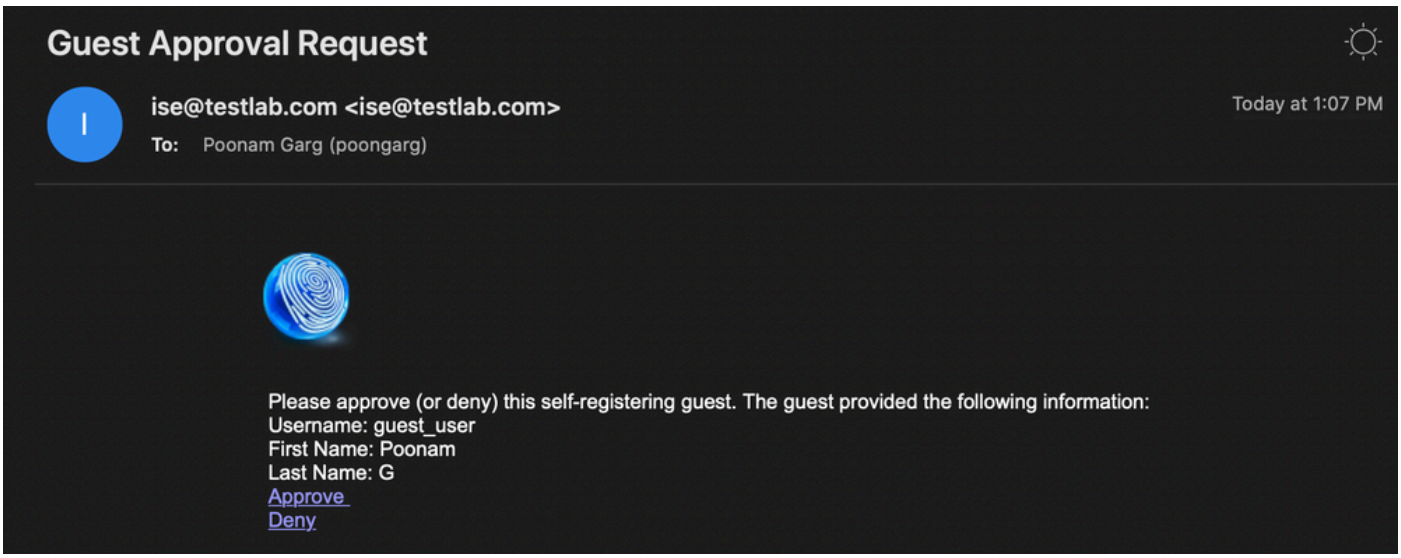
Lorsque vous disposez de la configuration de serveur SMTP et de messagerie appropriée, le compte est créé :





Une fois que vous avez activé l'option Exiger que les invités soient approuvés, les champs de nom d'utilisateur et de mot de passe sont automatiquement supprimés de la section Inclure ces informations dans la page Réussite de l'auto-inscription. C'est pourquoi, lorsque l'approbation d'un sponsor est nécessaire, les informations d'identification des utilisateurs invités ne sont pas affichées par défaut sur la page Web qui présente les informations indiquant que le compte a été créé. Elles doivent être fournies par SMS (Short Message Services) ou par e-mail. Cette option doit être activée dans la section Envoyer la notification d'informations d'identification lors de l'approbation à l'aide de (marquer e-mail/SMS).

Un e-mail de notification est envoyé au sponsor :



Le sponsor clique sur le lien Approbation et se connecte au portail du sponsor et le compte est approuvé :

À partir de ce moment, l'utilisateur invité est autorisé à se connecter (avec les informations d'identification reçues par e-mail ou SMS).

En résumé, trois adresses e-mail sont utilisées dans ce flux :

- Adresse de notification « De ». Cette adresse est définie de manière statique ou est prise à partir du compte du sponsor et utilisée comme adresse d'expéditeur pour la notification au sponsor (pour approbation) et les informations d'identification à l'invité. Cette option est configurée sous Work Centers > Guest Access > Settings > Guest Email Settings.

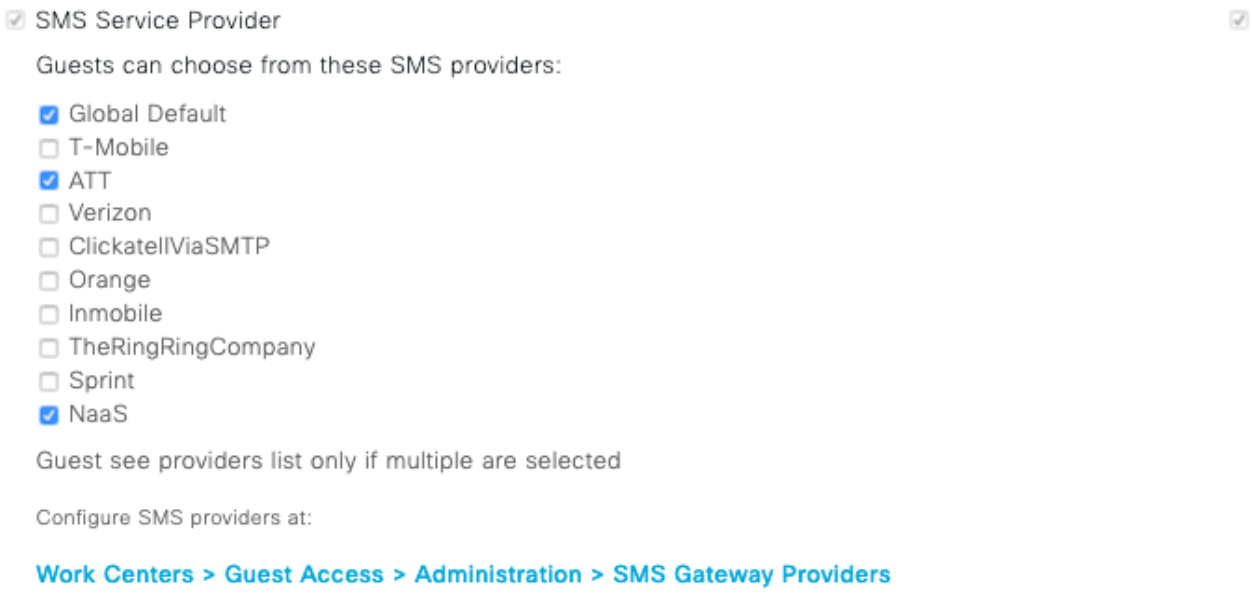
- Adresse de destination de la notification. Cette information est utilisée afin d'aviser le promoteur qu'il a reçu un compte pour approbation. Elle est configurée dans le portail Invité sous Centres de travail > Accès invité > Portails Invité > Portails et composants > Nom du portail > Paramètres du formulaire d'inscription > Exiger l'approbation des invités > Envoyer une demande d'approbation par e-mail à.

- Adresse de destination de l'invité. Cette information est fournie par l'utilisateur invité lors de l'inscription. Si Envoyer une notification d'informations d'identification lors de l'approbation par e-mail est sélectionné, l'e-mail avec les détails d'informations d'identification (nom d'utilisateur et mot de passe) est remis à l'invité.

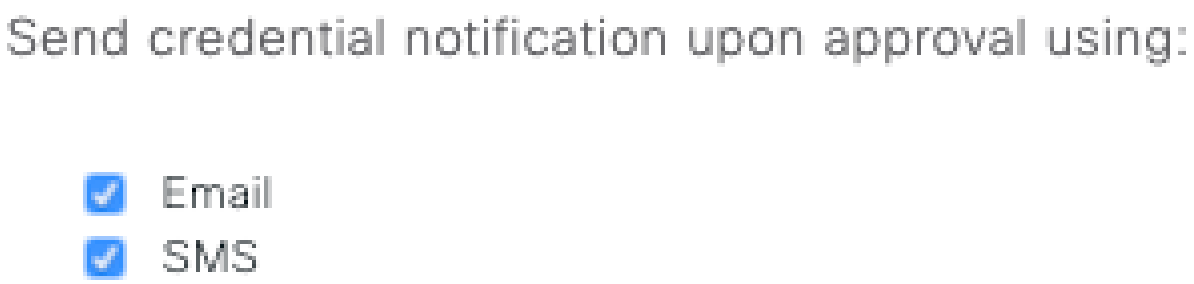
Remettre les informations d'identification par SMS

Les informations d'identification des invités peuvent également être envoyées par SMS. Ces options doivent être configurées :

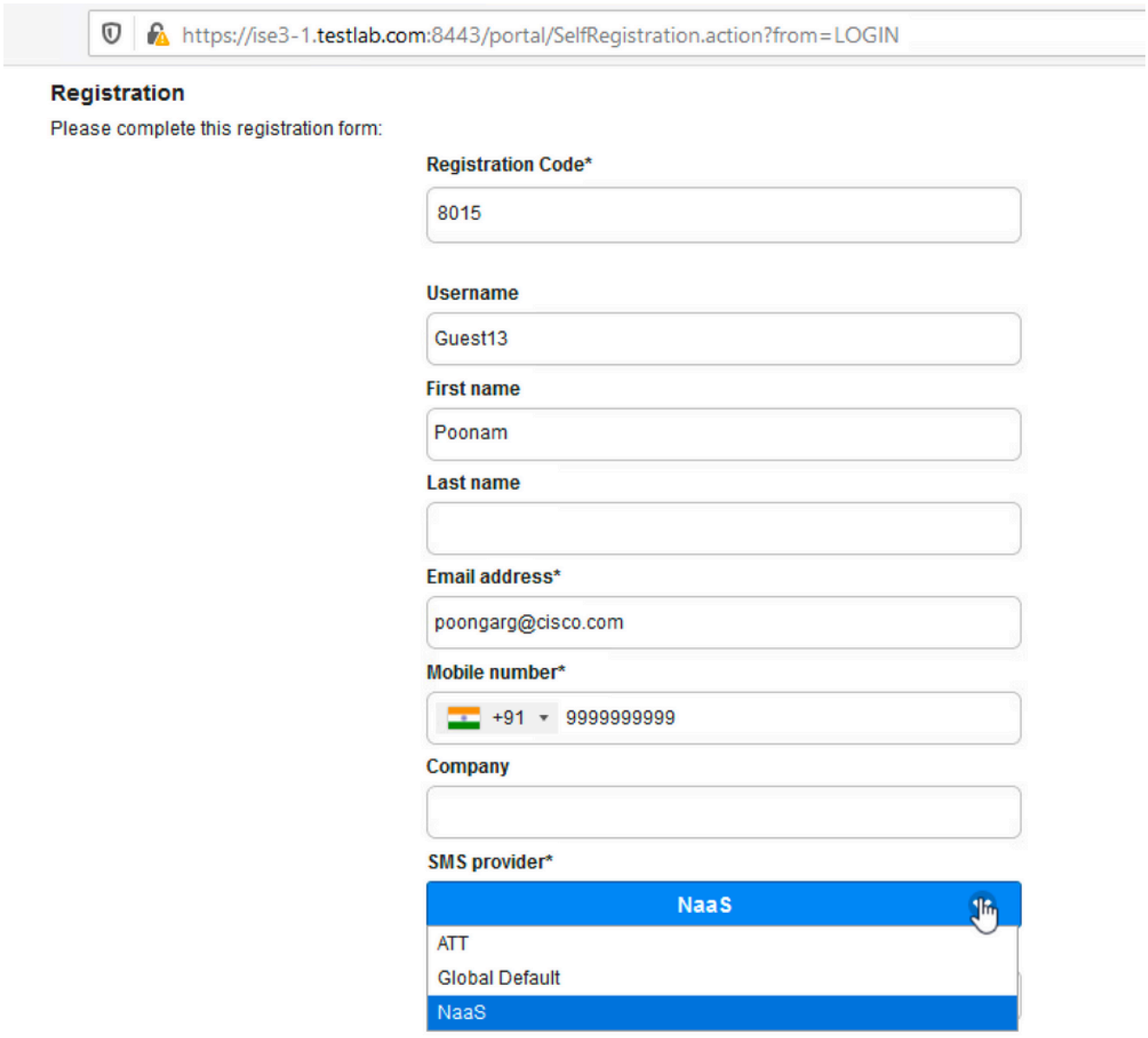
1. Sélectionnez le fournisseur de services SMS sous Paramètres du formulaire d'inscription :



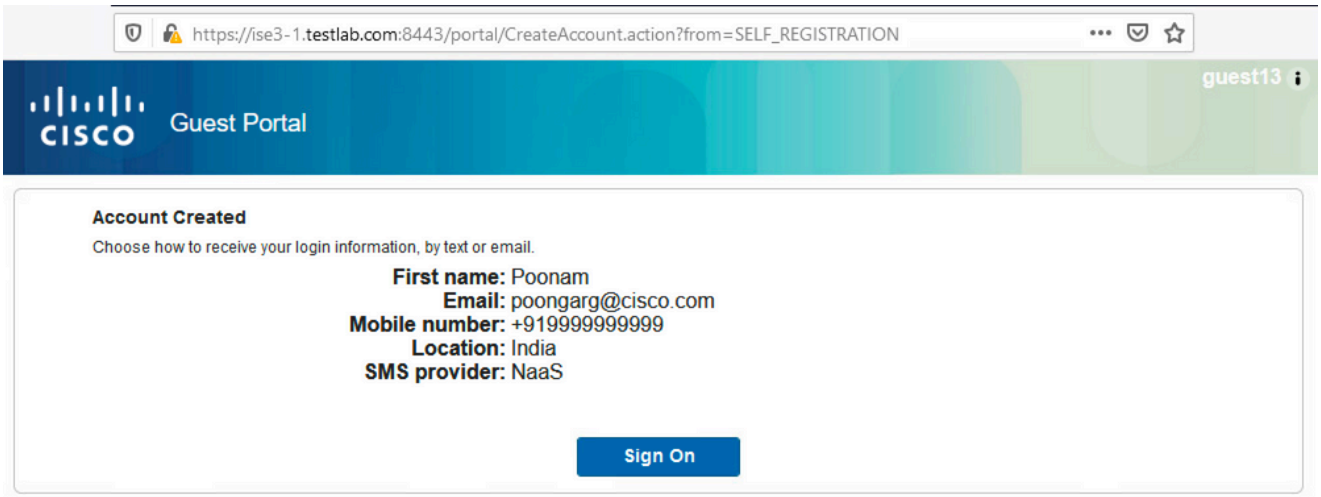
2. Cochez la case Envoyer la notification d'informations d'identification après approbation en utilisant : SMS.



3. Ensuite, l'utilisateur invité est invité à choisir le fournisseur disponible lorsqu'il crée un compte :



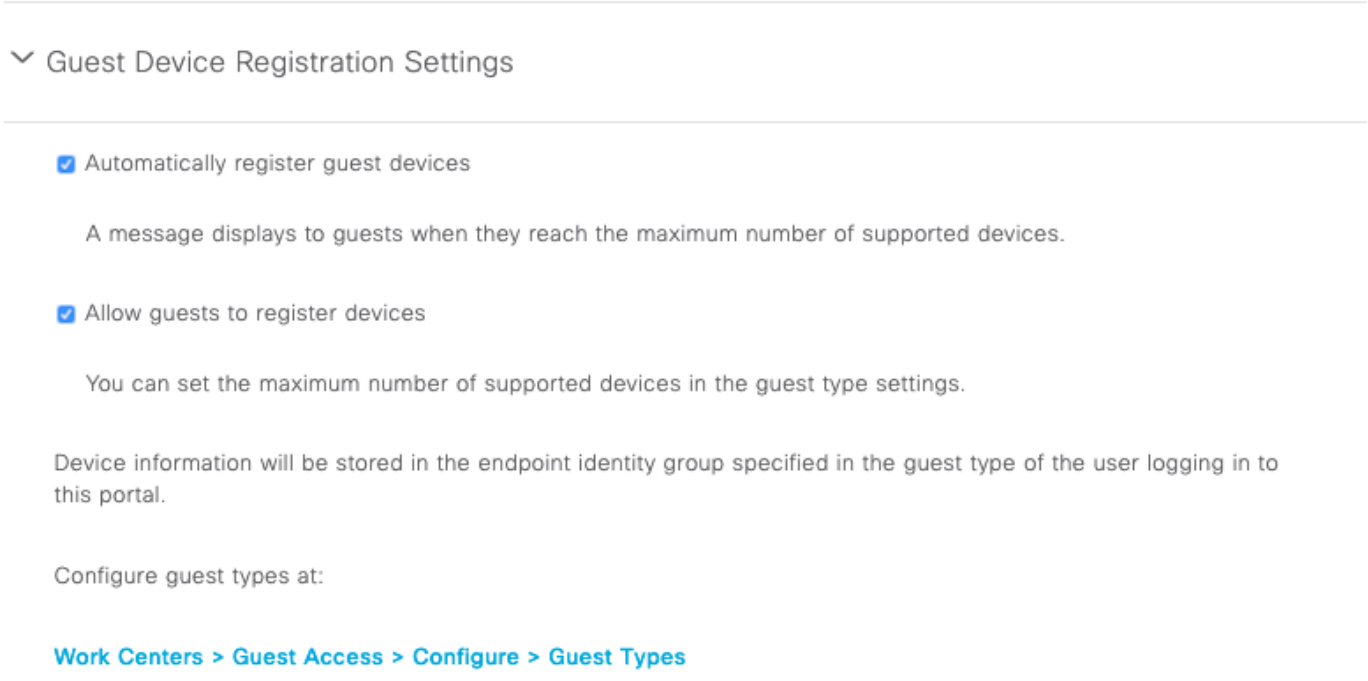
4. Un SMS est envoyé avec le fournisseur et le numéro de téléphone choisis :

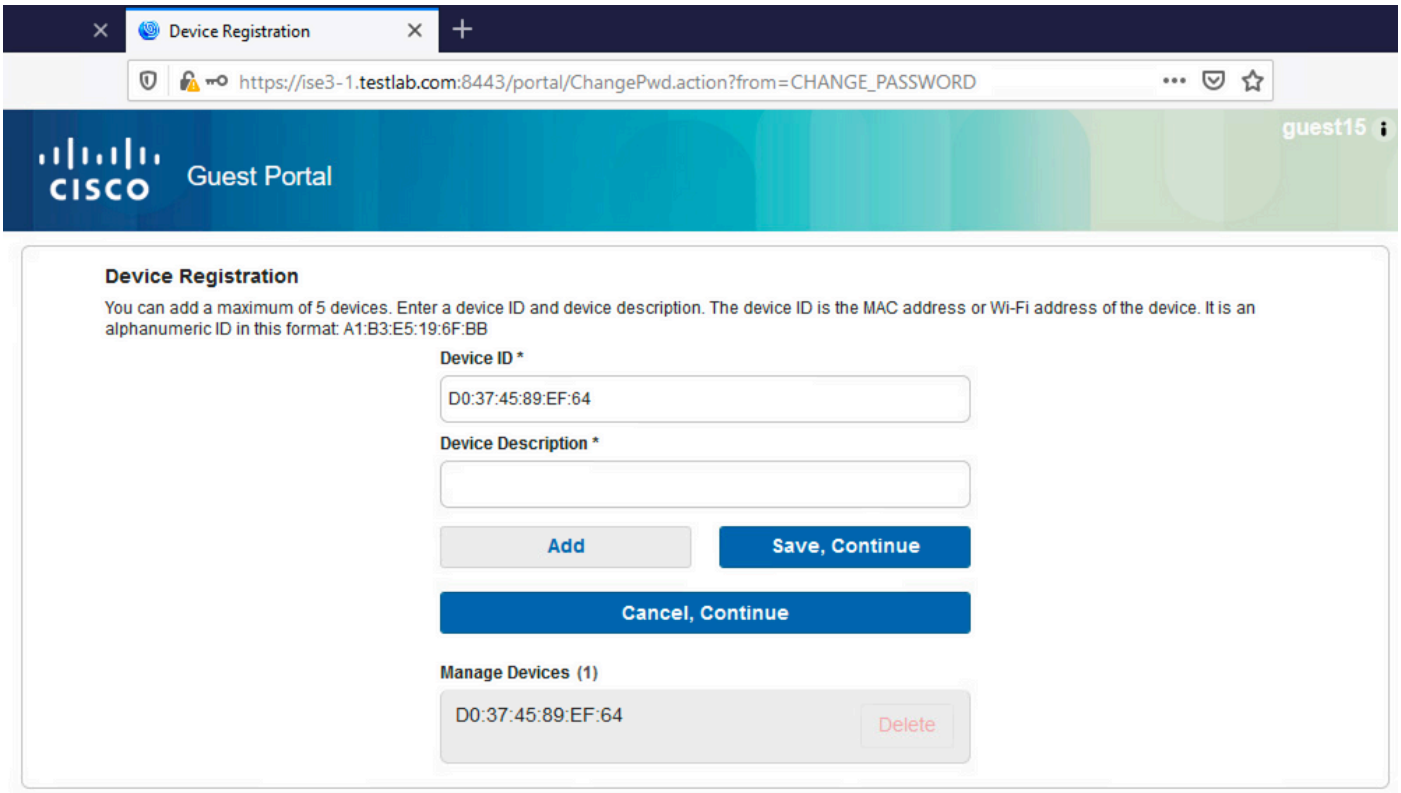


5. Vous pouvez configurer les fournisseurs SMS sous Administration > System > Settings > SMS Gateway.

Enregistrement des périphériques

Si l'option Autoriser les invités à enregistrer des périphériques est sélectionnée après qu'un utilisateur invité se connecte et accepte le protocole AUP, vous pouvez enregistrer des périphériques :



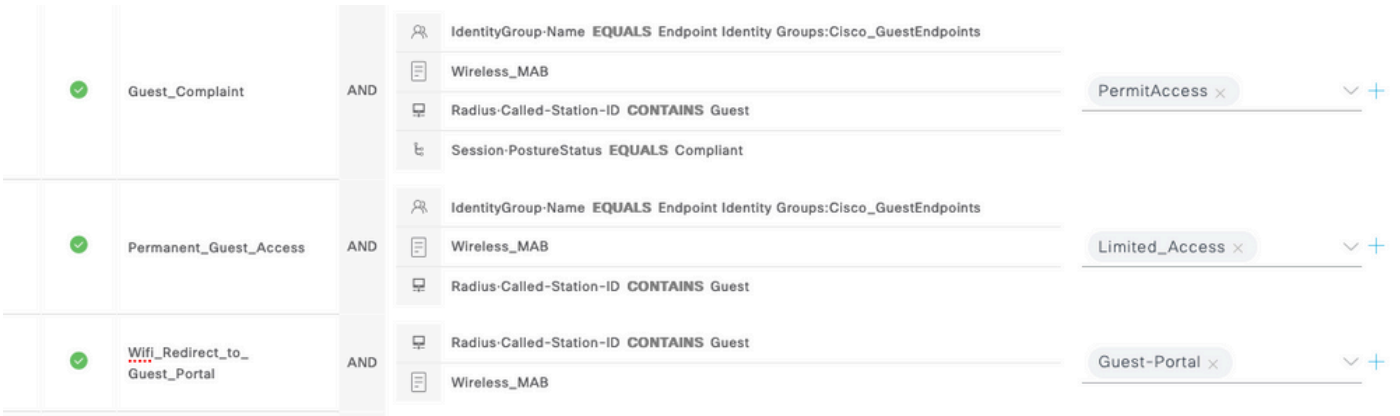


Notez que le périphérique a déjà été ajouté automatiquement (il figure dans la liste Gérer les périphériques). En effet, les périphériques invités inscrits automatiquement ont été sélectionnés.

Posture

Si l'option Require guest device compliance est sélectionnée, alors les utilisateurs invités sont approvisionnés avec un agent qui effectue la posture (NAC/Web Agent) après qu'ils se soient connectés et ont accepté l'AUP (et éventuellement effectuer l'enregistrement du périphérique). ISE traite les règles de provisionnement du client pour décider quel agent doit être provisionné. Ensuite, l'agent qui s'exécute sur la station effectue la posture (conformément aux règles de posture) et envoie les résultats à l'ISE, qui envoie la réauthentification CoA pour modifier l'état d'autorisation si nécessaire.

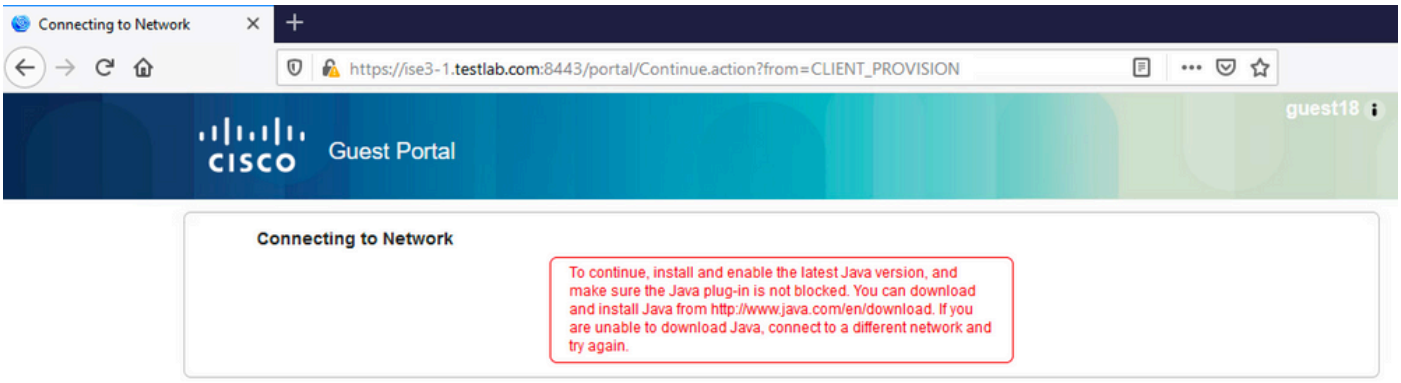
Les règles d'autorisation possibles peuvent ressembler à ceci :



Les premiers nouveaux utilisateurs qui rencontrent la règle Guest_Authenticate redirigent vers le

portail d'inscription automatique des invités. Une fois que l'utilisateur s'enregistre et se connecte lui-même, CoA change d'état d'autorisation et l'utilisateur bénéficie d'un accès limité pour effectuer la posture et la correction. Ce n'est qu'une fois que l'agent NAC est configuré et que la station est conforme que la CoA modifie à nouveau l'état d'autorisation afin de fournir un accès à Internet.

Les problèmes typiques de posture incluent l'absence de règles de provisionnement client correctes :



Cela peut également être confirmé si vous examinez le fichier guest.log :

<#root>

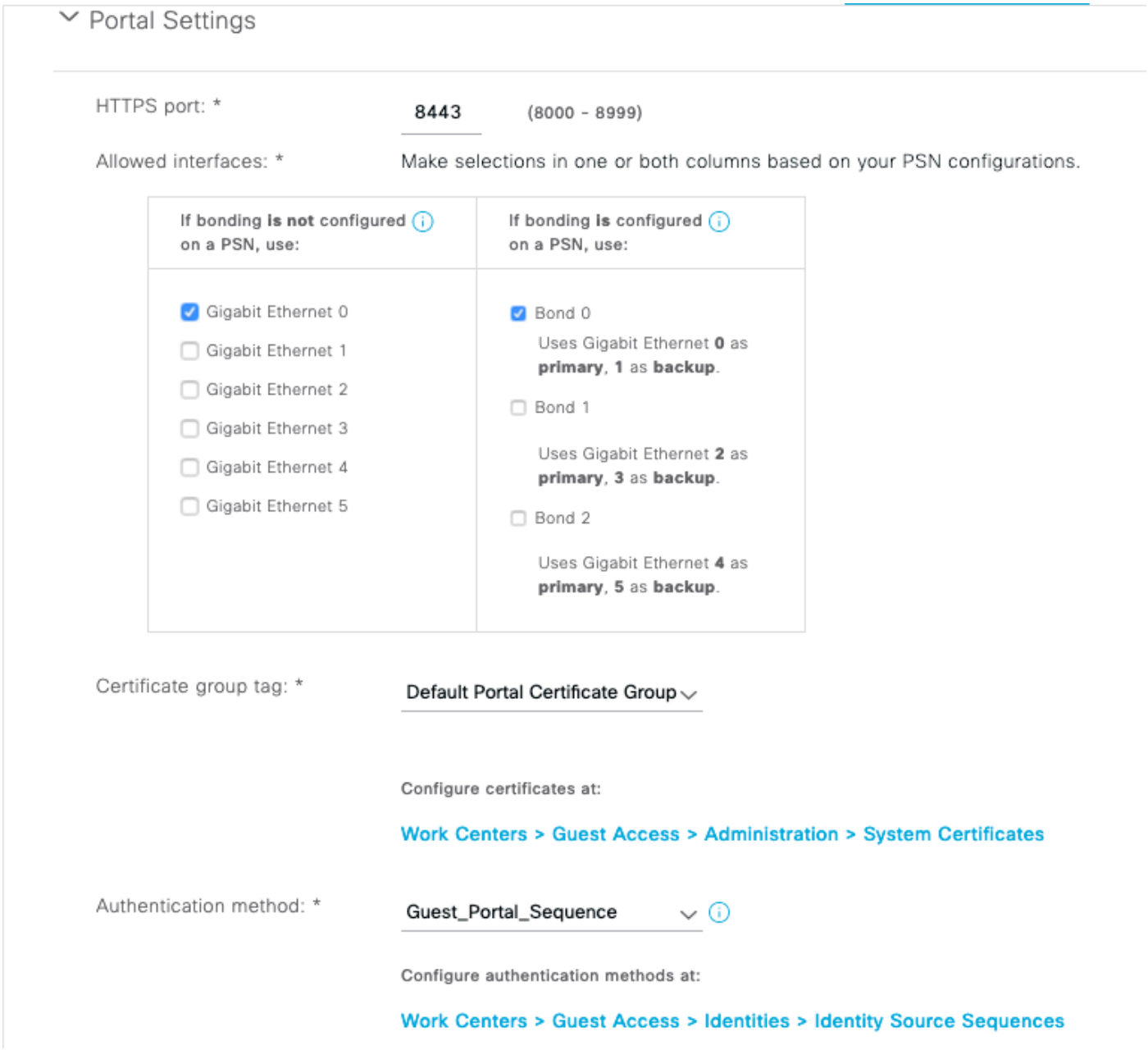
```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7][] guestaccess.flowmanager.step.g
```

BYOD

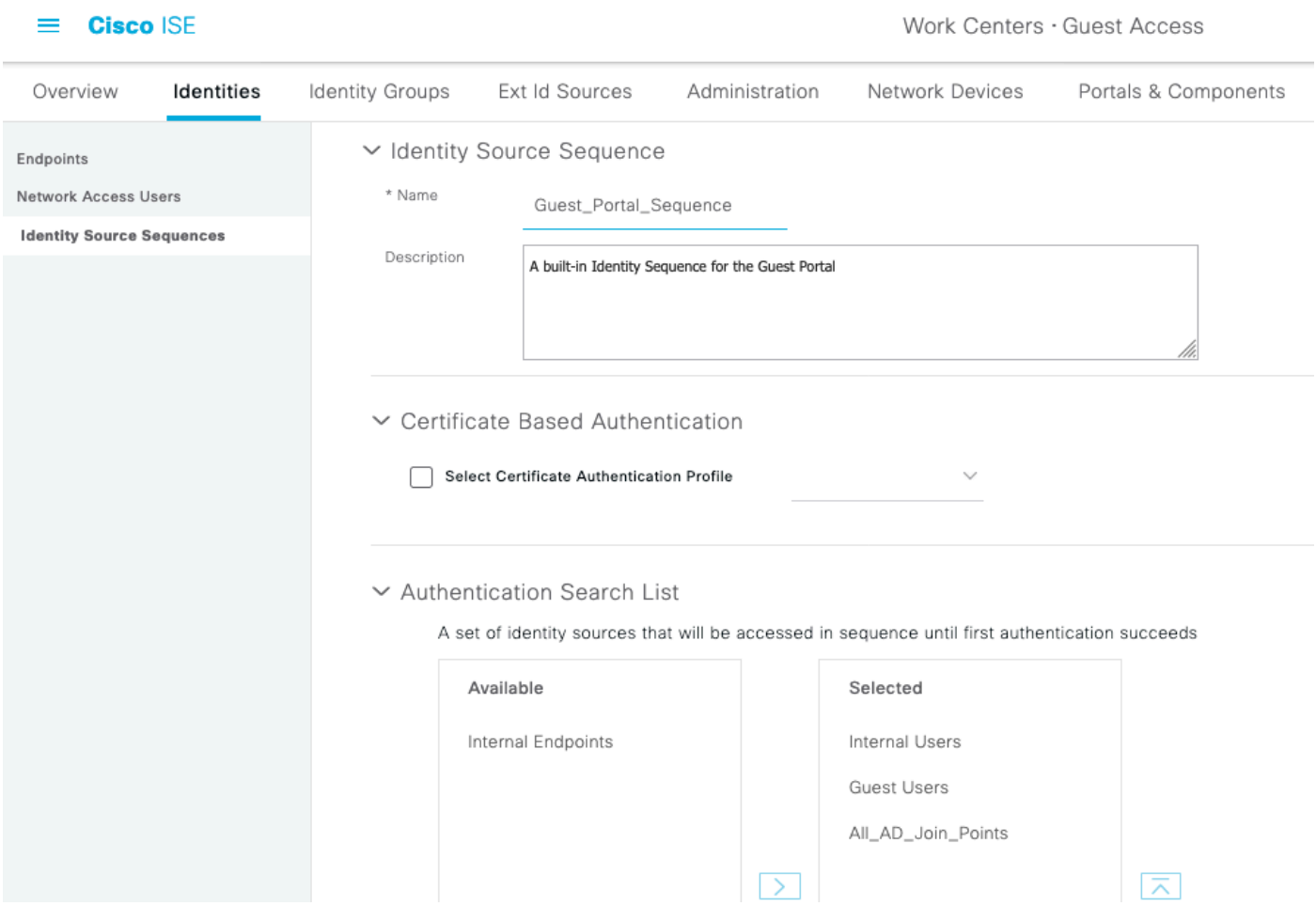
Si l'option Autoriser les employés à utiliser des appareils personnels sur le réseau est sélectionnée, alors les utilisateurs d'entreprise qui utilisent ce portail peuvent passer par le flux BYOD et enregistrer des appareils personnels. Pour les utilisateurs invités, ce paramètre ne change rien.

Que signifie « employés utilisant le portail en tant qu'invité » ?

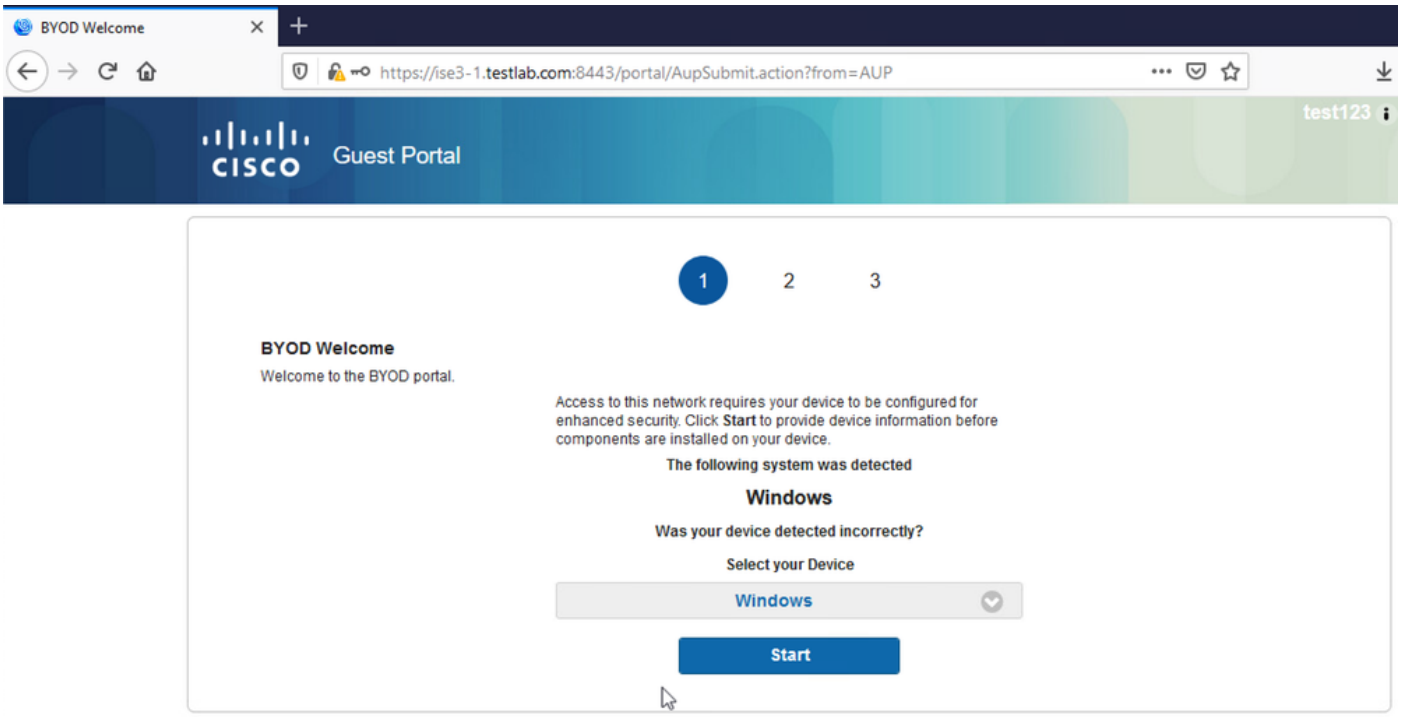
Par défaut, les portails invités sont configurés avec le magasin d'identités Guest_Portal_Sequence :



Il s'agit de la séquence de stockage interne qui essaie d'abord les utilisateurs internes (avant les utilisateurs invités), puis les informations d'identification Active Directory. Comme les paramètres avancés doivent passer au magasin suivant de la séquence lorsqu'un magasin d'identités sélectionné n'est pas accessible pour l'authentification, un employé avec des informations d'identification internes ou des informations d'identification Active Directory peut se connecter au portail.



À ce stade du portail invité, l'utilisateur fournit des informations d'identification définies dans le magasin Utilisateurs internes ou Active Directory et la redirection BYOD se produit :



Les utilisateurs d'entreprise peuvent ainsi effectuer des opérations BYOD sur leurs appareils personnels.

Lorsque les informations d'identification des utilisateurs internes/AD sont remplacées par celles des utilisateurs invités, le flux normal se poursuit (pas de BYOD).

Modification VLAN

Il vous permet d'exécuter activeX ou une applet Java, ce qui déclenche la libération et le renouvellement de DHCP. Cela est nécessaire lorsque CoA déclenche la modification du VLAN pour le terminal. Lorsque MAB est utilisé, le point d'extrémité n'est pas conscient d'un changement de VLAN. Une solution possible consiste à modifier le VLAN (version/renouvellement DHCP) avec l'agent NAC. Une autre option consiste à demander une nouvelle adresse IP via l'applet renvoyée sur la page Web. Un délai peut être configuré entre la libération, la CoA et le renouvellement. Cette option n'est pas prise en charge pour les appareils mobiles.

Informations connexes

- Services de posture sur le guide de configuration Cisco ISE
- BYOD sans fil avec Identity Services Engine
- Exemple de configuration de la prise en charge ISE SCEP pour BYOD
- Authentification Web centralisée (CWA, pour Central Web Authentification) sur le WLC et exemple de configuration ISE
- Exemple de configuration d'authentification Web centrale avec des points d'accès FlexConnect sur un WLC avec ISE
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.