# Gestion des comptes d'invités ISE

## Introduction

Ce document décrit les actions fréquemment utilisées qu'un sponsor ou un administrateur ISE peut effectuer sur les données d'invité présentes sur ISE. Les services d'invité Cisco Identity Services Engine (ISE) fournissent un accès réseau sécurisé aux invités tels que les visiteurs, les sous-traitants, les consultants et les clients.

Contribué par Shivam Kumar, ingénieur TAC Cisco.

## Conditions préalables

### Conditions requises

Cisco vous recommande de connaître ces sujets :

- ISE
- Services d'invité ISE

### Components Used

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

- Cisco ISE, version 2.6

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.

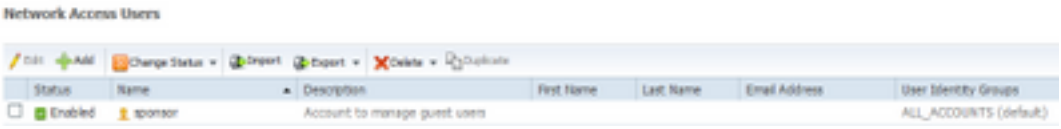
> **Note**: La procédure est similaire ou identique pour d'autres versions ISE. Sauf indication contraire, vous pouvez utiliser ces étapes sur toutes les versions du logiciel ISE 2.x.

## Configuration

### Utiliser un sponsor pour gérer les comptes d'invités

Les sponsors sont des comptes d'utilisateurs sur ISE qui ont le privilège de se connecter au portail de sponsor où ils peuvent créer des comptes d'invités temporaires pour les visiteurs autorisés et les gérer. Un sponsor peut être un utilisateur interne ou un compte présent dans un magasin d'identité externe tel qu'un répertoire actif.

Dans cet exemple, le compte de sponsor est défini en interne sur ISE et ajouté au groupe prédéfini : TOUS_COMPTES.



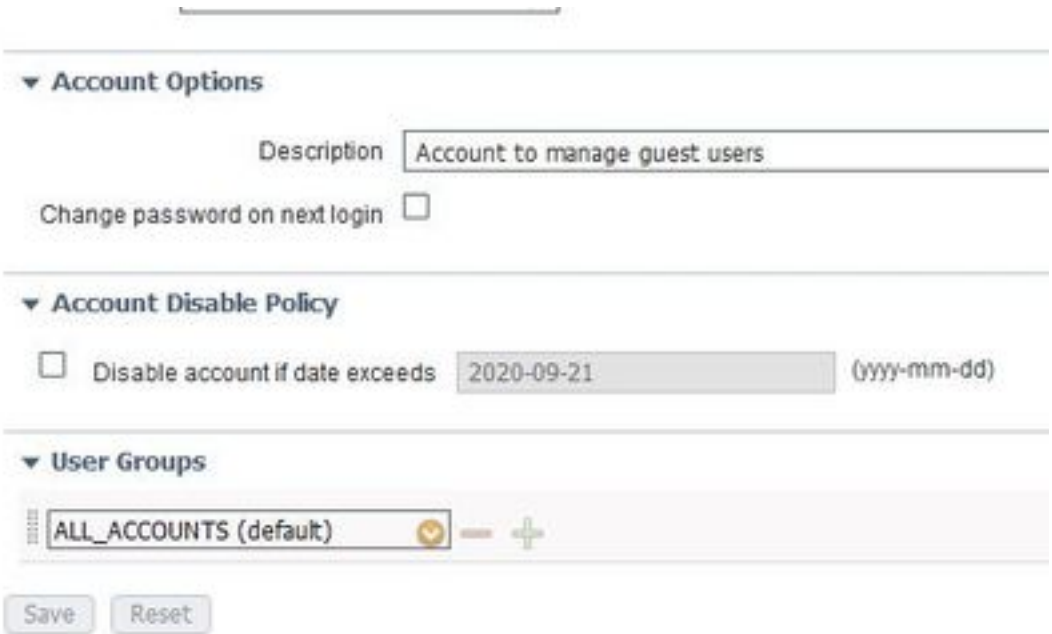

Par défaut, ISE a trois groupes de sponsors auxquels les sponsors peuvent être mappés :


ALL_ACCOUNTS (valeur par défaut) : les sponsors affectés à ce groupe peuvent gérer tous les comptes d'utilisateurs invités. Par défaut, les utilisateurs du groupe d'identité utilisateur ALL_ACCOUNTS sont membres de ce groupe de sponsor.

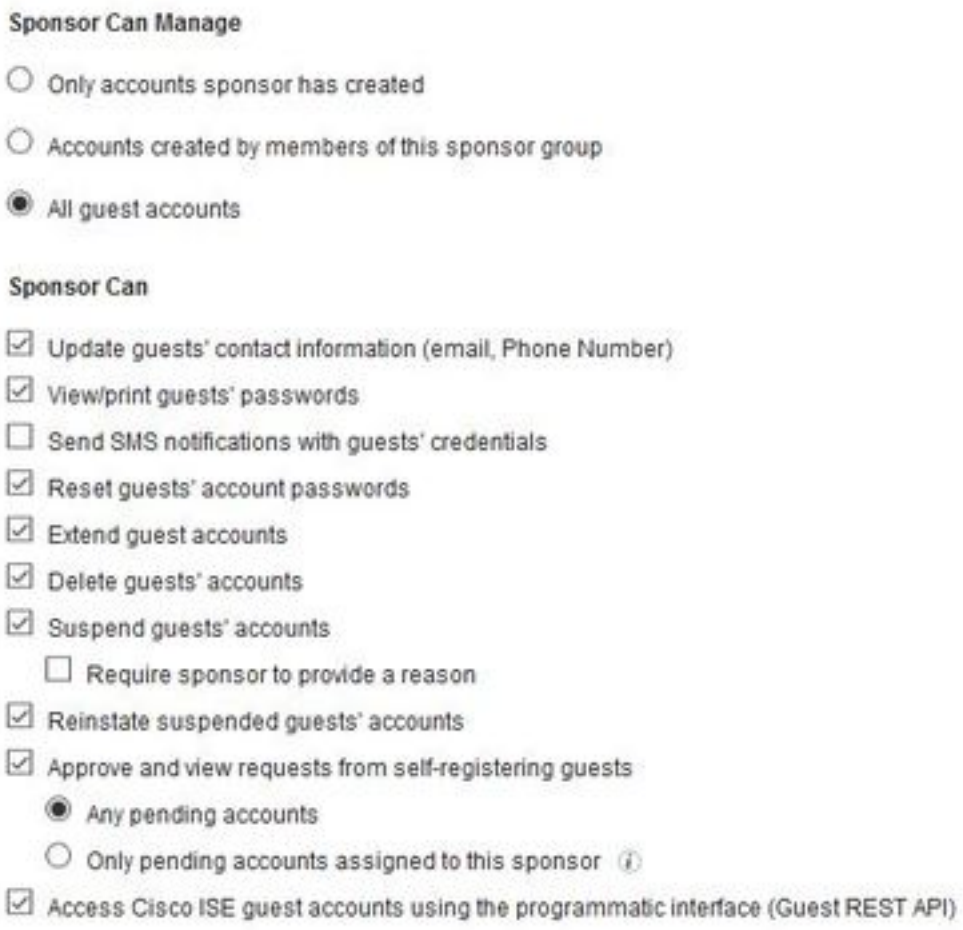
GROUP_ACCOUNTS (valeur par défaut) : les sponsors affectés à ce groupe peuvent gérer uniquement les comptes invités créés par les sponsors du même groupe de sponsors. Par défaut, les utilisateurs du groupe d'identité utilisateur GROUP_ACCOUNTS sont membres de ce groupe de sponsor.

OWN_ACCOUNTS (valeur par défaut) : les sponsors affectés à ce groupe peuvent gérer uniquement les comptes invités qu'ils ont créés. Par défaut, les utilisateurs du groupe d'identité d'utilisateur OWN_ACCOUNTS sont membres de ce groupe de sponsor.

Le compte de sponsor utilisé dans cet exemple est mappé à ALL_ACCOUNTS :




Les autorisations et privilèges de ce groupe de sponsors sont disponibles sur **Work Centers > Guest Access > Portal & Components > Sponsor Groups** :




Afin de permettre à un sponsor d'accéder à la gestion des invités via l'API ERS REST, l'autorisation est ajoutée dans le groupe du sponsor comme le montre l'image.

## Utiliser le compte Active Directory comme sponsor

Outre les comptes d'utilisateurs internes définis comme des sponsors, les comptes présents sur des sources d'identité externes telles qu'Active Directory (AD) ou LDAP peuvent également être utilisés comme sponsor pour gérer les comptes d'invités.

Assurez-vous que l'ISE est joint à AD en naviguant vers **Administration> Identités > Sources d'identité externes > Active Directory**. Si ce n'est déjà fait, joignez l'un des domaines AD disponibles.

Récupérer les groupes à partir d'AD qui contient les comptes :

Cet exemple montre comment ajouter un utilisateur AD au groupe de sponsors ALL_ACCOUNTS. Accédez à **Centres de travail > Accès invité > Portail et composants > Groupes de parrainage> ALL_ACCOUNTS**, puis cliquez sur **Membres**, comme illustré dans cette image.


Les membres affichent tous les groupes disponibles parmi lesquels choisir ; sélectionnez le groupe AD et déplacez-le vers la droite pour l'ajouter au groupe sponsor.


Enregistrez les modifications. La connexion au portail du sponsor fonctionne désormais avec les comptes d'utilisateurs AD qui font partie du groupe AD sélectionné.

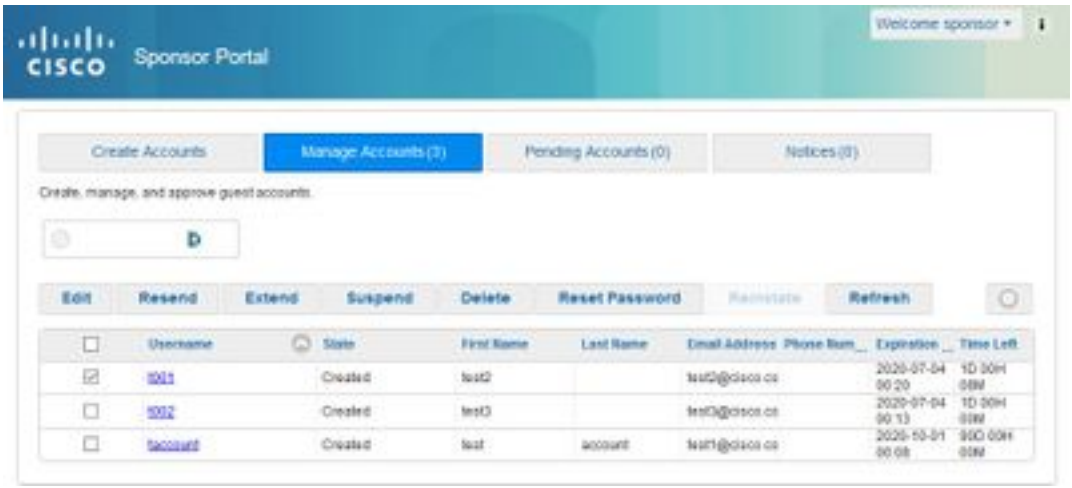
Les mêmes étapes peuvent être suivies pour ajouter des utilisateurs via LDAP. Des groupes d'identité utilisateur définis en interne sont également disponibles en tant qu'option à ajouter aux groupes de sponsor.

Utilisez un de ces comptes de sponsor pour vous connecter au portail de sponsor. Le portail du sponsor peut être utilisé pour :

- Modifier et supprimer des comptes invités

- Prolonger la durée du compte invité
- Suspendre le compte invité
- Rétablir les comptes d'invité expirés
- Réinitialiser et réinitialiser les mots de passe des invités
- Approuver les comptes d'invité en attente

Sur le portail du sponsor, sélectionnez l'onglet **Gérer les comptes** pour afficher tous les comptes invités que ce sponsor est autorisé à gérer, comme illustré dans cette image.

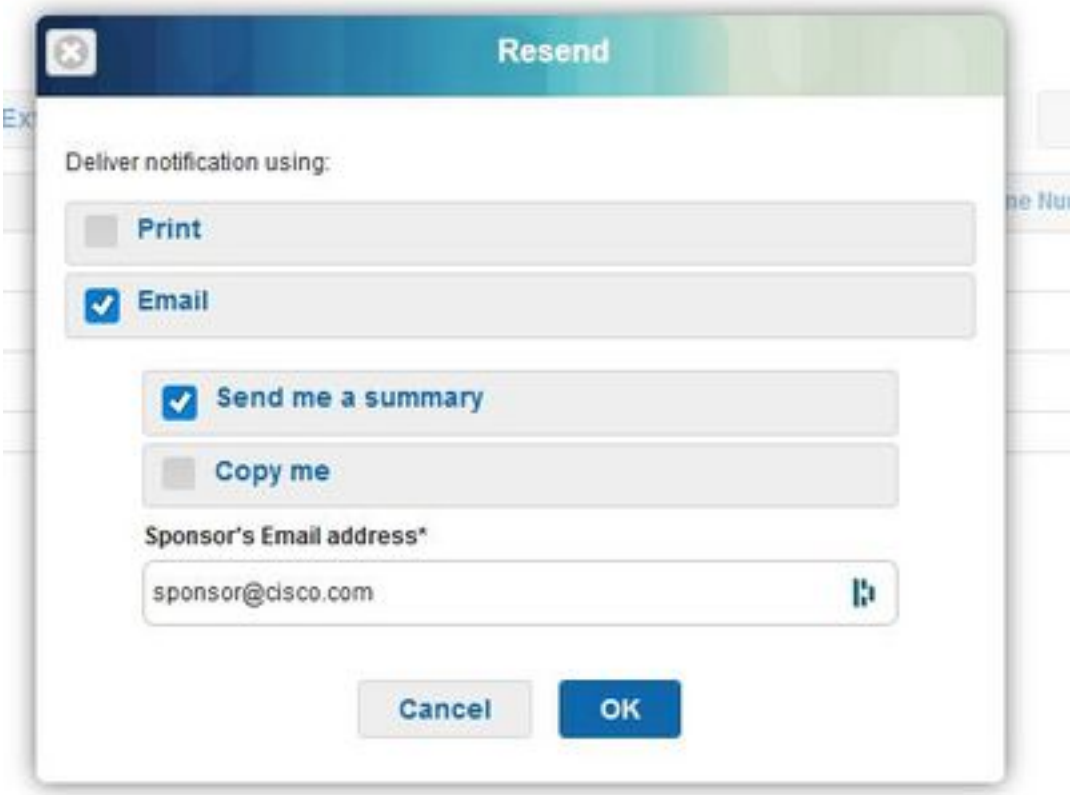



Un compte invité peut être modifié quel que soit l'état dans lequel il se trouve.

Il est possible de renvoyer le mot de passe du compte invité au cas où le titulaire du compte les oublierait ou les perdrait. Le mot de passe d'un compte invité ne peut être renvoyé que s'il est à l'état **Actif** ou **Créé**.

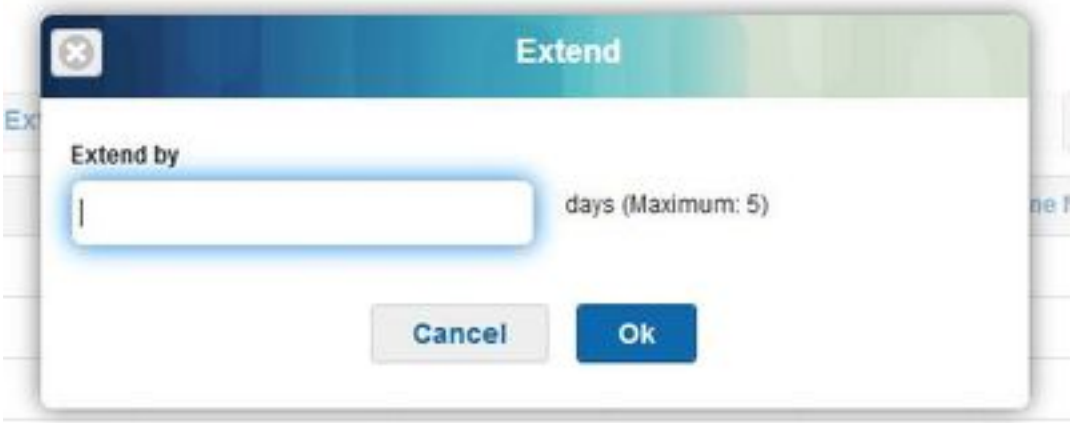
Les mots de passe ne peuvent pas être renvoyés pour les invités qui les ont modifiés. Dans ce cas, l'option de réinitialisation du mot de passe doit être utilisée en premier. Impossible d'envoyer le mot de passe pour les comptes en attente d'approbation, suspendus, expirés ou refusés.

Un sponsor peut choisir l'option de recevoir une copie du mot de passe modifié :




Si vous devez autoriser l'accès invité au réseau pendant une période plus longue que celle autorisée à l'origine, utilisez l'option étendue pour augmenter la durée. Les comptes à l'état Créé, Actif ou Expiré peuvent être étendus.

Un compte suspendu ou refusé ne peut pas être prolongé ; utilisez plutôt l'option de rétablissement.




La période de prolongation maximale autorisée est régie par le type d'invité du compte.

Les comptes d'invité expirent seuls lorsqu'ils atteignent la fin de la durée du compte, quel que soit leur état. Les comptes invités suspendus ou expirés sont automatiquement purgés en fonction de la stratégie de purge définie sur le système. Par défaut, ils sont purgés tous les 15 jours.

| Action | Usage Guidelines | Eligible Account States |
|---|---|---|
| Edit | Make changes to a selected account. | All, except Suspended, Denied. |
| Resend | Email, text, or print account details for the selected guests. | Active, Created |
| Extend | Adjust the access time period or reactivate the selected expired guest accounts. | Active, Created, Expired |
| Suspend | Disable the selected guest accounts without deleting them from the system.<br>You may be prompted to provide reasons for suspending an account. | Active, Created |
| Delete | Remove the selected guest accounts from the Cisco ISE database. | All |
| Reset Password | Reset the selected guest passwords to random passwords and notify the guests of the account details. | Active, Created |
| Reinstate | Enable the selected suspended guest accounts and approve previously denied accounts. | Suspended, Denied |
| Refresh | View any changes to the displayed accounts. | Not applicable |

Le compte d'invité indique et leur signification :

Actif : Les invités disposant de ces comptes se sont correctement connectés via un portail invité accrédité ou ont contourné le portail captif invité accrédité. Dans ce dernier cas, les comptes appartiennent à des types d'invités configurés pour contourner le portail captif invité accrédité. Ces invités peuvent accéder au réseau en fournissant leurs identifiants de connexion au demandeur natif sur leur périphérique.

Créé : Les comptes ont été créés, mais les invités ne se sont pas encore connectés à un portail invité accrédité. Dans ce cas, les comptes sont affectés aux types d'invités qui ne sont pas configurés pour contourner le portail captif invité accrédité. Les invités doivent d'abord se connecter via le portail dédié aux invités accrédités avant de pouvoir accéder à d'autres parties du réseau.

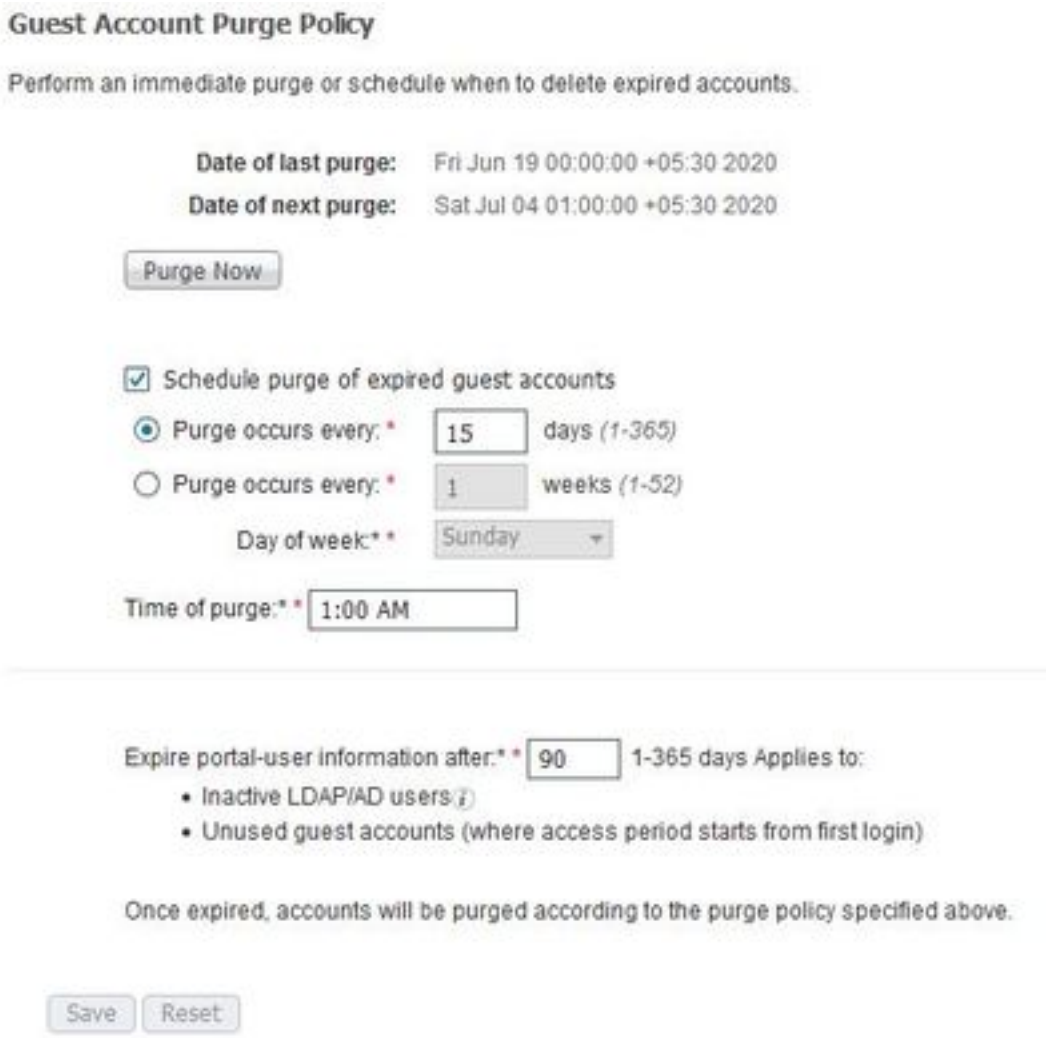
Refusé : L'accès au réseau est refusé aux comptes. Les comptes qui ont expiré alors qu'ils étaient dans un état refusé restent comme refusés.

En attente d'approbation : Les comptes sont en attente d'approbation pour accéder au réseau.

Suspendu : Les comptes sont suspendus par un parrain qui a le privilège de le faire.

## Stratégies de purge des invités

Par défaut, ISE purge automatiquement les comptes d'invité expirés tous les 15 jours. Ces informations peuvent être affichées sous **Centres de travail > Accès invité > Paramètres > Stratégie de purge de compte invité**.




**Date de la purge suivante** indique quand la purge suivante aura lieu. L'administrateur ISE peut :

- Programmez une purge tous les X jours. La **durée de la purge** spécifie quand la première purge se produit en X jours. Après cela, la purge se produit tous les X jours.
- Programmez une purge un jour donné de la semaine, toutes les X semaines.
- Forcer une purge à la demande à l'aide de l'option **Purger maintenant.**

Lorsque des comptes d'invité expirés sont purgés, les informations de terminal, de rapport et de journalisation associées sont conservées.

## Purger le point de terminaison : Jours inactifs par rapport aux jours écoulés pour les terminaux

Les points d'extrémité que les invités utilisent pour accéder au réseau deviennent par défaut partie de GuestEndpoints. ISE a pour politique de supprimer les terminaux invités et les périphériques enregistrés qui ont plus de 30 jours. Ce travail de purge par défaut s'exécute à 1 heure par jour en fonction du fuseau horaire configuré sur le noeud d'administration principal (PAN). Cette stratégie par défaut utilise la condition **ElapsedDays**. Les autres options disponibles sont **InactiveDays** et **PurgeDate**.

> **Note**: La fonctionnalité de purge du point de terminaison est indépendante de la stratégie de purge du compte invité et de l'expiration du compte invité.

La stratégie est définie sous **Administration > Identity Management > Settings > Endpoint Purge**.

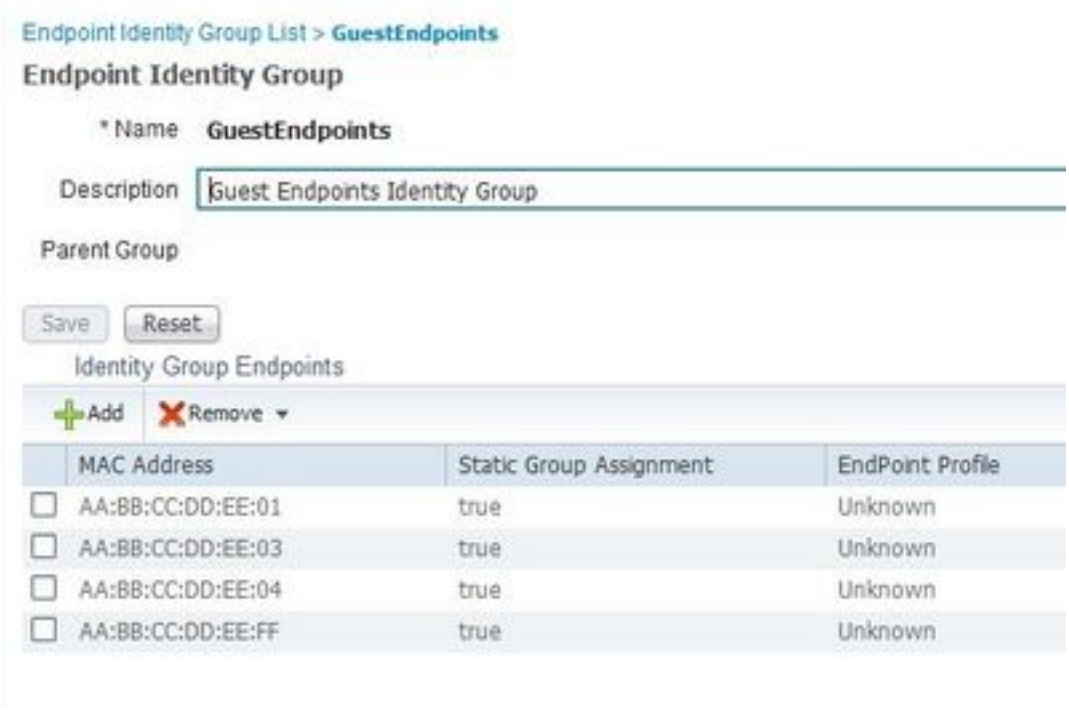

Jours écoulés : Cela se rapporte au nombre de jours depuis la création de l'objet. Cette condition peut être utilisée pour les points de terminaison auxquels un accès non authentifié ou conditionnel a été accordé pendant une période définie, par exemple un point de terminaison invité ou sous-traitant, ou pour les employés qui utilisent l'authentification Web pour accéder au réseau. Après la période de grâce de connexion autorisée, ils doivent être entièrement réauthentifiés et enregistrés.

Jours inactifs : Indique le nombre de jours écoulés depuis la dernière activité de profilage ou la dernière mise à jour du point de terminaison. Cette condition purge les périphériques obsolètes qui se sont accumulés au fil du temps, les invités ou les périphériques personnels généralement temporaires ou les périphériques retirés. Ces terminaux ont tendance à représenter du bruit dans la plupart des déploiements car ils ne sont plus actifs sur le réseau ou risquent d'être détectés dans un avenir proche. S'ils se connectent à nouveau, ils seront redécouverts, profilés, enregistrés, etc. selon les besoins.

Lorsqu'il y a des mises à jour à partir du point de terminaison, InactivityDays sera réinitialisé à 0 uniquement si le profilage est activé.

Date de purge : Date de suppression du point de terminaison. Cette option peut être utilisée pour des événements spéciaux ou des groupes où l'accès est accordé pour une heure spécifique, indépendamment de l'heure de création ou de début. Cela permet de purger tous les terminaux en même temps. Par exemple, un salon professionnel, une conférence ou un cours de formation hebdomadaire avec de nouveaux membres chaque semaine, où l'accès est accordé pour une semaine ou un mois spécifique plutôt que pour des jours/semaines/mois absolus.

Cet exemple de fichier profiler.log montre quand les points de terminaison qui faisaient partie de GuestEndpoints et qui avaient expiré 30 jours ont été purgés :

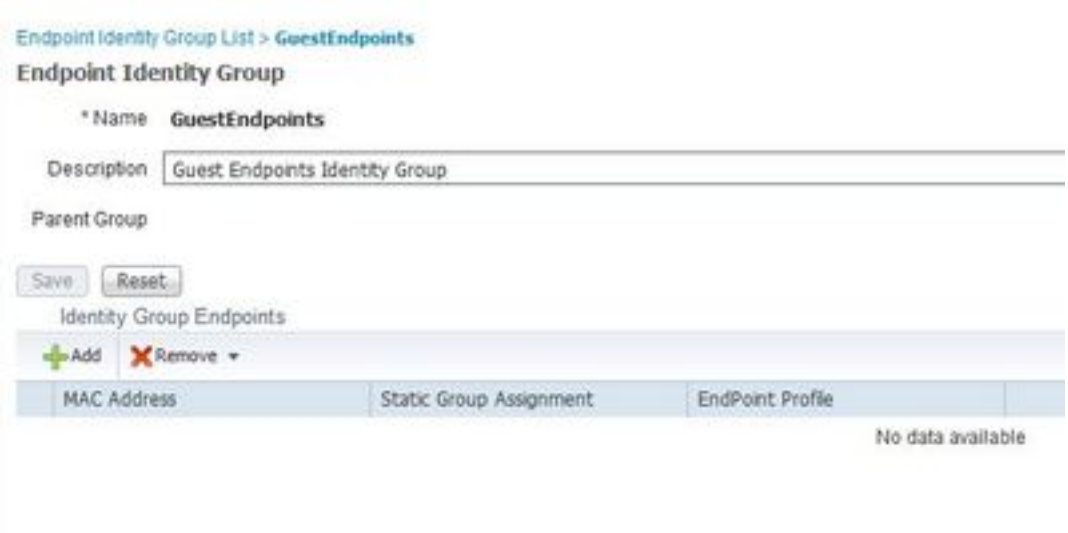



```
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- the rule type is :REGULAR
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- epPurgeRuleID is :3bfaffe0-8c01-
11e6-996c-525400b48521
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- purging description:
ENDPOINTPURGE:ElapsedDays EQUALS 30
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- purging expression:
GuestInactivityCheck & GuestEndPointsPurgeRuleCheck5651c592-cbdb-4e60-aba1-cf415e2d4808
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- EPCondition name is :
GuestInactivityCheck
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- the condLabel are :ENDPOINTPURGE
ElapsedDays EQUALS 30
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- rulename is : 3c119520-8c01-11e6-
996c-525400b48521
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- the rule type is :EXCLUSION
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- rulename is : 3c2ac270-8c01-11e6-
996c-525400b48521
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- the rule type is :REGULAR
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- epPurgeRuleID is :3c2ac270-8c01-
11e6-996c-525400b48521
2

2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- EPCondition name is :
RegisteredInactivityCheck
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- the condLabel are :ElapsedDays
Greater than 30
2020-07-09 09:35:26,407 INFO [admin-http-pool13][]
```

```
cisco.profiler.infrastructure.profiling.EPPurgeRuleEvaluator -::- Started to Update the
ChildParentMappingMap
2020-07-09 09:35:26,408 INFO [admin-http-pool13][]
cisco.profiler.infrastructure.profiling.EPPurgeRuleEvaluator -::- Completed to Update the
ChildParentMappingMap
2020-07-09 09:35:26,512 INFO [admin-http-pool13][]
cisco.profiler.infrastructure.notifications.ProfilerEDFNotificationAdapter -::- EPPurge policy
notification.
2020-07-09 09:35:26,514 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- Requesting purging.
2020-07-09 09:35:26,524 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- New TASK is running : 07-09-
202009:35
2020-07-09 09:35:26,524 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- Read
profiler.endPointNumDaysOwnershipToPan from platform properties: null
2020-07-09 09:35:26,524 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- Value of number days after which
ownership of inactive end points change to PAN: 14
2020-07-09 09:35:26,525 INFO [PurgeImmediateOrphanEPOwnerThread][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- Updating Orphan Endpoint
Ownership to PAN.
2020-07-09 09:35:26,530 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- Purge Endpoints for PurgeID 07-
09-202009:35
2020-07-09 09:35:26,532 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- hostname of the node ise26-
1.shivamk.local
2020-07-09 09:35:26,537 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- Search Query page1 lastEpGUID.
EndpointCount4
2020-07-09 09:35:26,538 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- EndpointAA:BB:CC:DD:EE:FF
IdentityGroupIDaa178bd0-8bff-11e6-996c-525400b48521 identityGroupGuestEndpoints elapsedTime30
inactivityTime0 PurgeDeleteStatustrue CalledStationIDnull EndpointFetchedFromCachetrue
2020-07-09 09:35:26,539 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- EndpointAA:BB:CC:DD:EE:01
IdentityGroupIDaa178bd0-8bff-11e6-996c-525400b48521 identityGroupGuestEndpoints elapsedTime30
inactivityTime0 PurgeDeleteStatustrue CalledStationIDnull EndpointFetchedFromCachetrue
2020-07-09 09:35:26,540 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- EndpointAA:BB:CC:DD:EE:03
IdentityGroupIDaa178bd0-8bff-11e6-996c-525400b48521 identityGroupGuestEndpoints elapsedTime30
inactivityTime0 PurgeDeleteStatustrue CalledStationIDnull EndpointFetchedFromCachetrue
2020-07-09 09:35:26,540 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- EndpointAA:BB:CC:DD:EE:04
IdentityGroupIDaa178bd0-8bff-11e6-996c-525400b48521 identityGroupGuestEndpoints elapsedTime30
inactivityTime0 PurgeDeleteStatustrue CalledStationIDnull EndpointFetchedFromCachetrue
2020-07-09 09:35:27,033 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- Endpoints PurgeID '07-09-
202009:35' purged 4
2020-07-09 09:35:27,034 INFO [EPPurgeEventHandler-20-thread-1][]
profiler.infrastructure.probemgr.event.EPPurgeEventHandler -::- Endpoints PurgeID '07-09-
202009:35' purged 4 in 504 millisec numberofEndpointsRead4
```

Une fois la purge terminée :




### Dépanner les problèmes d'invité et de purge

Afin de capturer les journaux liés aux problèmes d'invité et de purge, ces composants peuvent être définis sur debug. Pour activer les débogages, accédez à **Administration > System > Debug Log Configuration > Select node**.

Pour les comptes invité/sponsor et le dépannage lié à la purge des points d'extrémité, définissez ces composants sur debug :

- accès invité
- guest-admin
- guest-access-admin
- profileur
- runtime-AAA

Pour les problèmes liés au portail, définissez ces composants sur debug :

- portail de parrainage
- portail
- portal-session-manager
- accès invité

## Informations connexes

- Guide de déploiement des conditions d'accès invité ISE
- Dépannage et activation des débogages sur ISE