Gestione account guest ISE

Introduzione

Questo documento descrive le azioni utilizzate di frequente che uno sponsor o un amministratore ISE può intraprendere sui dati dei clienti presenti su ISE. I servizi guest di Cisco Identity Services Engine (ISE) offrono accesso sicuro alla rete agli ospiti, come visitatori, appaltatori, consulenti e clienti.

Contributo di Shivam Kumar, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE
- Servizi guest ISE

Componenti usati

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

- Cisco ISE, release 2.6

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.

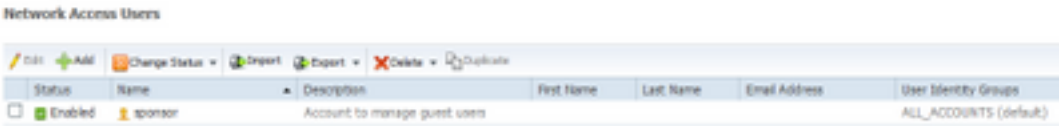
> **Nota:** La procedura è simile o identica per altre versioni ISE. Ove non diversamente specificato, è possibile eseguire la procedura seguente su tutte le versioni software ISE 2.x.

Configurazione

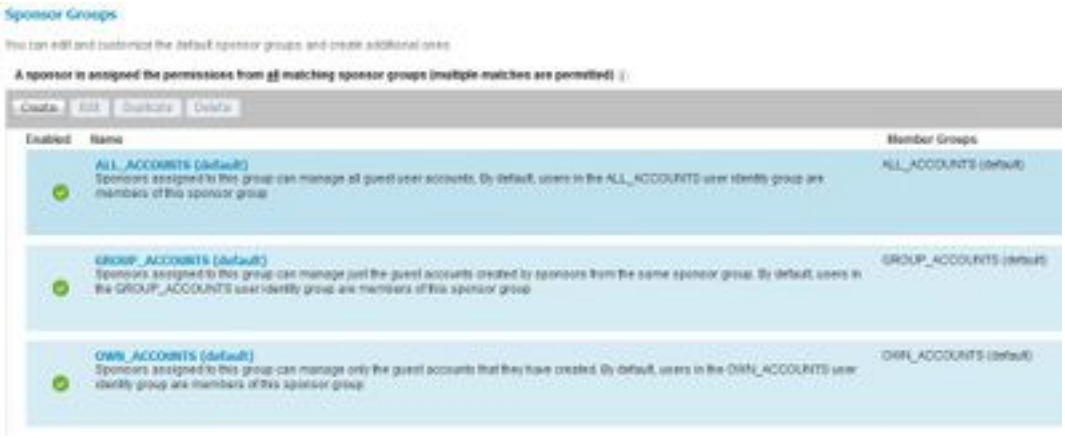
Usa uno sponsor per gestire gli account guest

Gli sponsor sono account utente ISE che hanno il privilegio di accedere al portale degli sponsor per creare account guest temporanei per i visitatori autorizzati e gestirli. Uno sponsor può essere un utente interno o un account presente in un archivio di identità esterno, ad esempio Active Directory.

Nell'esempio, l'account sponsor viene definito internamente su ISE e aggiunto al gruppo predefinito: ALL_ACCOUNTS



Per impostazione predefinita, ISE dispone di tre gruppi di sponsor a cui è possibile associare gli sponsor:

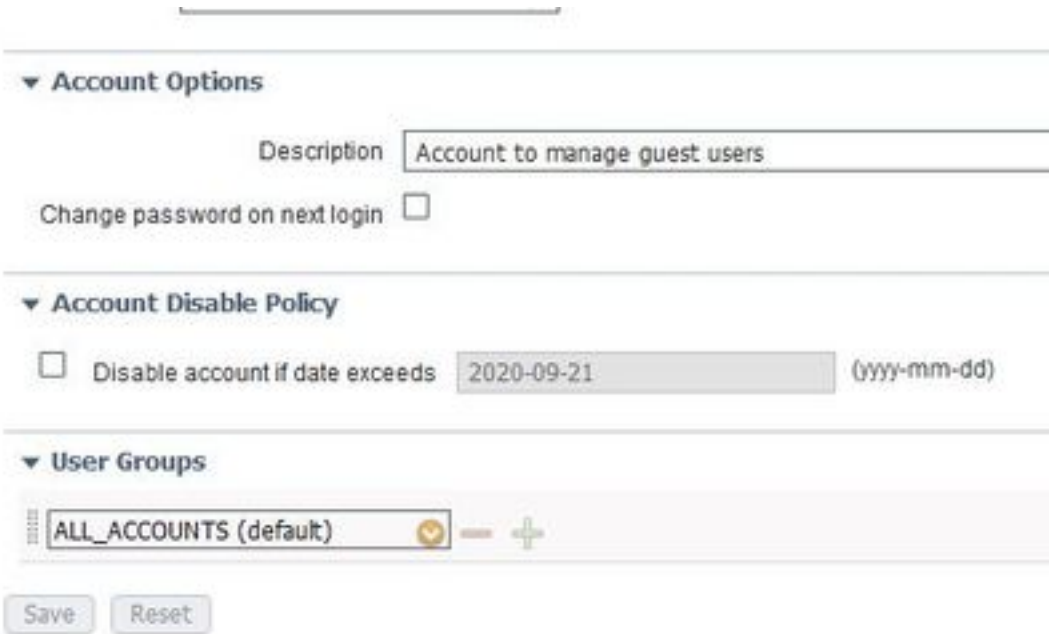


ALL_ACCOUNTS (predefinito): gli sponsor assegnati a questo gruppo possono gestire tutti gli account utente guest. Per impostazione predefinita, gli utenti del gruppo di identità utenti ALL_ACCOUNTS sono membri di questo gruppo sponsor.

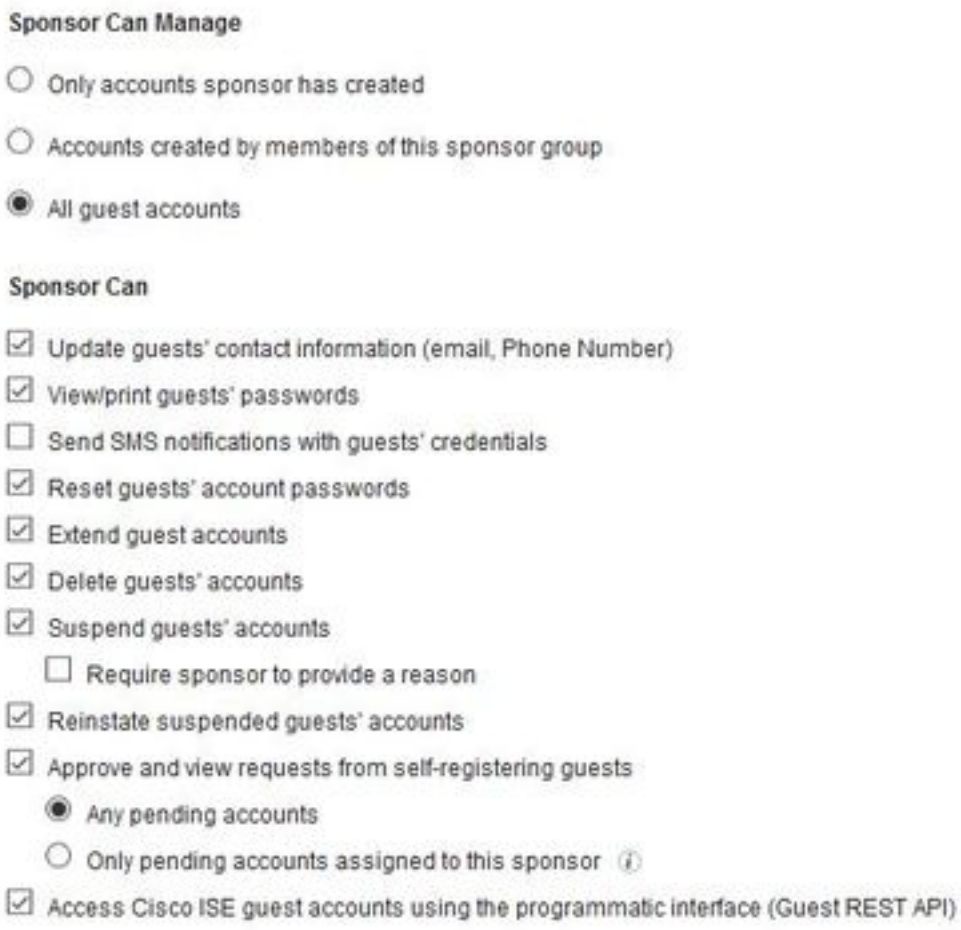
GROUP_ACCOUNTS (predefinito): Gli sponsor assegnati a questo gruppo possono gestire solo gli account guest creati dagli sponsor dello stesso gruppo. Per impostazione predefinita, gli utenti del gruppo di identità utenti GROUP_ACCOUNTS sono membri di questo gruppo sponsor.

OWN_ACCOUNTS (impostazione predefinita): gli sponsor assegnati a questo gruppo possono gestire solo gli account guest che hanno creato. Per impostazione predefinita, gli utenti del gruppo di identità utenti OWN_ACCOUNTS sono membri di questo gruppo sponsor.

L'account sponsor utilizzato in questo esempio è mappato a ALL_ACCOUNTS:



Le autorizzazioni e i privilegi di questo gruppo sponsor sono disponibili in **Centri di lavoro > Accesso guest > Portale e componenti > Gruppi sponsor**:



Per consentire a uno sponsor di accedere alla gestione guest tramite l'API REST ERS, l'autorizzazione viene aggiunta nel gruppo dello sponsor come mostrato nell'immagine.

Usa account di Active Directory come sponsor

Oltre agli account utente interni definiti come sponsor, è possibile utilizzare come sponsor per gestire gli account guest anche gli account presenti in origini di identità esterne quali Active Directory (AD) o LDAP.

Verificare che l'ISE sia unita ad AD selezionando **Amministrazione > Identità > Origini identità esterne > Active Directory**. Se non è già stato aggiunto, aggiungere il computer a uno dei domini AD disponibili.

Recuperare i gruppi da AD che contengono gli account:

In questo esempio viene illustrato come aggiungere un utente AD al gruppo Sponsor ALL_ACCOUNTS.

Passare a **Centri di lavoro> Accesso guest > Portale e componenti > Gruppi sponsor > ALL_ACCOUNTS** e fare clic su **Membri**, come mostrato nell'immagine.

I membri mostrano tutti i gruppi disponibili tra cui scegliere; selezionare il gruppo AD e spostarlo a destra per aggiungerlo al gruppo sponsor.

Salvare le modifiche. L'accesso al portale sponsor ora funziona con gli account utente di Active Directory che fanno parte del gruppo AD selezionato.

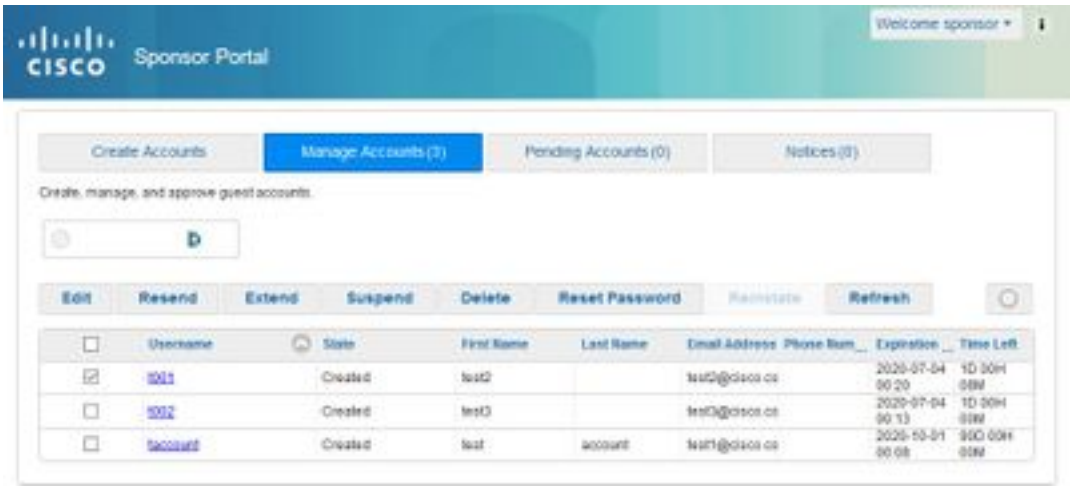
Per aggiungere utenti tramite LDAP, seguire la stessa procedura descritta in precedenza. Sono inoltre disponibili gruppi di identità utente definiti internamente come opzione da aggiungere ai gruppi sponsor.

Utilizzare un account sponsor di questo tipo per accedere al portale sponsor. Il portale degli sponsor può essere utilizzato per:

- Modifica ed elimina account guest

- Estendi durata account guest
- Sospendi account guest
- Reintegra account guest scaduti
- Invia e reimposta le password per gli utenti guest
- Approva account guest in sospeso

Sul portale degli sponsor, selezionare la scheda **Gestisci account** per visualizzare tutti gli account guest che lo sponsor è autorizzato a gestire, come mostrato in questa immagine.

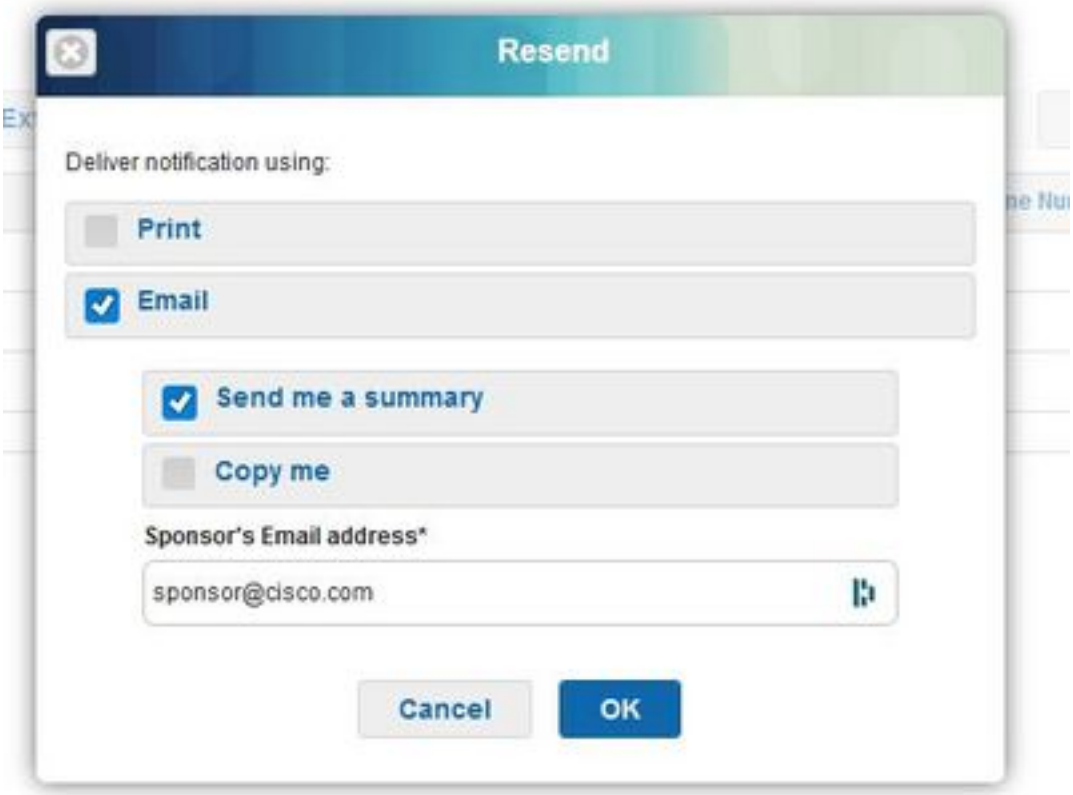


Un account Guest può essere modificato indipendentemente dallo stato in cui si trova.

Èpossibile inviare nuovamente la password dell'account guest nel caso in cui il titolare dell'account la dimentichi o la perda. La password di un account guest può essere inviata solo se si trova nello stato **Attivo** o **Creato**.

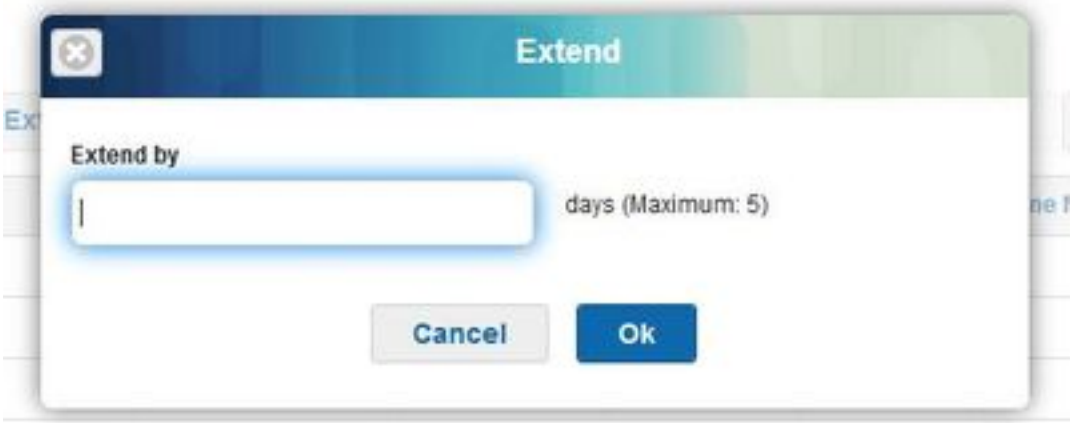
Le password non possono essere reinviate per gli ospiti che le hanno modificate. In tal caso, è necessario utilizzare prima l'opzione di reimpostazione della password. Impossibile inviare la password per gli account in attesa di approvazione, sospesi, scaduti o negati.

Lo sponsor può scegliere l'opzione per ricevere una copia della password modificata:



Se è necessario consentire l'accesso guest alla rete per un periodo superiore a quello originariamente consentito, utilizzare l'opzione estesa per aumentare la durata. Gli account con stato Creato, Attivo o Scaduto possono essere estesi.

Un account sospeso o rifiutato non può essere esteso; utilizzate invece l'opzione reintegra (reinstate).



Il periodo di estensione massimo consentito è determinato dal tipo guest dell'account.

Gli account Guest scadono da soli quando raggiungono la fine della durata dell'account, indipendentemente dallo stato. Gli account guest sospesi o scaduti vengono automaticamente eliminati in base ai criteri di eliminazione definiti nel sistema. Per impostazione predefinita, vengono eliminati ogni 15 giorni.

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. 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

Stati dell'account Guest e relativo significato:

Attiva: Gli utenti guest con questi account hanno eseguito l'accesso tramite un portale Guest con credenziali oppure hanno ignorato il portale Guest con credenziali. Nel secondo caso, gli account appartengono a tipi guest configurati per ignorare il portale per utenti guest con credenziali. Questi guest possono accedere alla rete fornendo le proprie credenziali di accesso al richiedente nativo sul proprio dispositivo.

Creato: Gli account sono stati creati, ma gli utenti guest non hanno ancora eseguito l'accesso a un portale Guest con credenziali. In questo caso, gli account vengono assegnati a tipi di guest non configurati per ignorare il portale per utenti guest con credenziali. Gli utenti guest devono prima accedere tramite il portale attendibile Guest Captive prima di poter accedere ad altre parti della rete.

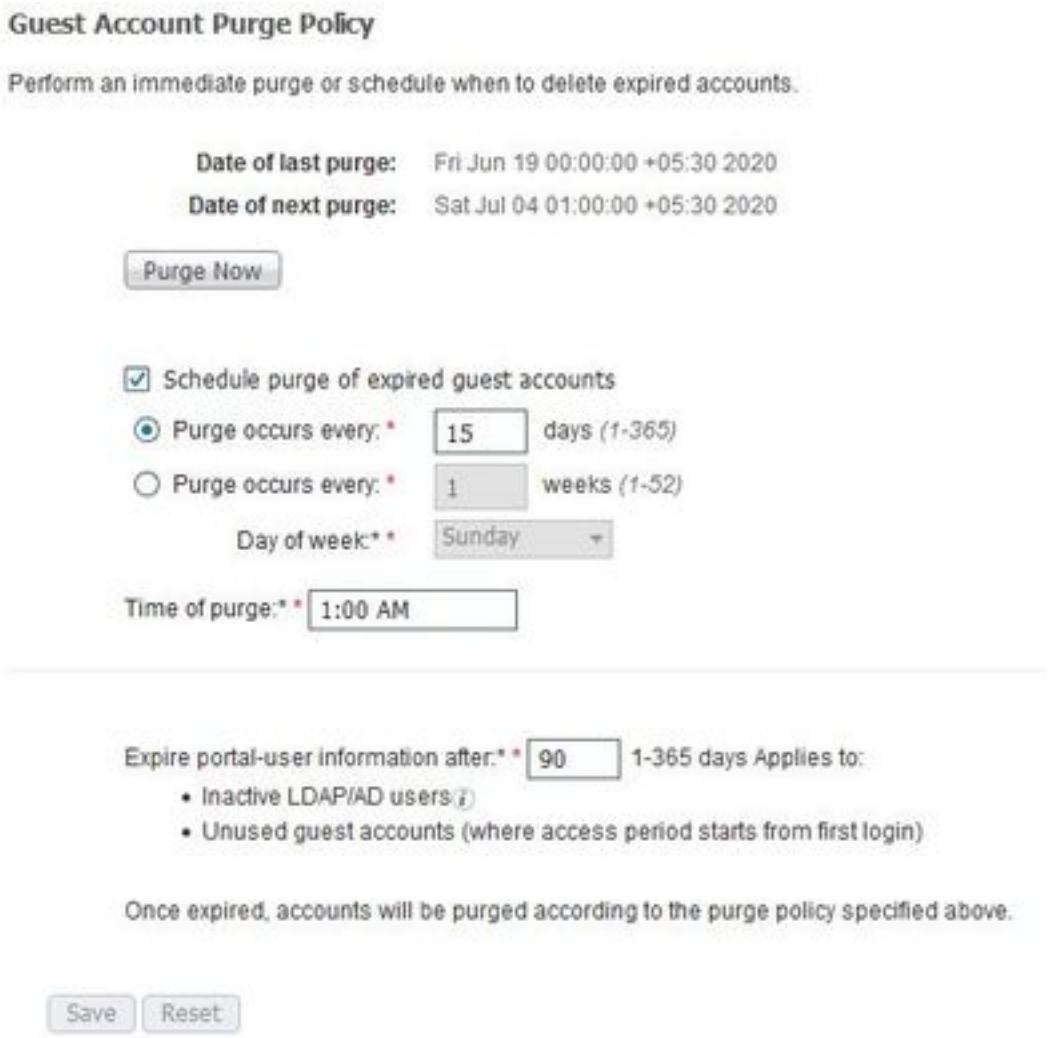
Negato: Agli account viene negato l'accesso alla rete. Gli account scaduti in stato negato rimangono tali.

In attesa di approvazione: Gli account sono in attesa di approvazione per accedere alla rete.

Sospeso: Gli account vengono sospesi da uno sponsor che ha il privilegio di farlo.

Criteri di rimozione guest

Per impostazione predefinita, ISE rimuove automaticamente gli account guest scaduti ogni 15 giorni. Queste informazioni sono disponibili in **Centri di lavoro > Accesso guest > Impostazioni > Criteri di rimozione account guest**.



Data prossima rimozione indica quando verrà eseguita la rimozione successiva. L'amministratore ISE può:

- Pianificare un'eliminazione ogni X giorni. L'opzione **Ora eliminazione** specifica quando la prima eliminazione viene eseguita in X giorni. Dopo di che, l'eliminazione avviene ogni X giorni.
- Pianificare un'eliminazione in un determinato giorno della settimana, ogni X settimane.
- Imporre un'eliminazione a richiesta utilizzando l'opzione **Rimuovi ora.**

Quando gli account guest scaduti vengono eliminati, gli endpoint, i report e le informazioni di registrazione associati vengono mantenuti.

Rimozione endpoint: Giorni inattivi rispetto ai giorni trascorsi per gli endpoint

Gli endpoint utilizzati dagli utenti guest per accedere alla rete diventano parte di GuestEndpoints per impostazione predefinita. ISE prevede l'eliminazione degli endpoint guest e dei dispositivi registrati più vecchi di 30 giorni. Questo processo di eliminazione predefinito viene eseguito ogni giorno alle 1 del mattino in base al fuso orario configurato nel nodo di amministrazione primario (PAN). Questo criterio predefinito utilizza la condizione **ElapsedDays**. Altre opzioni disponibili sono **InactiveDays** e **PurgeDate**.

> **Nota:** La funzionalità di rimozione degli endpoint è indipendente dai criteri di rimozione degli account guest e dalla scadenza degli account guest.

I criteri sono definiti in **Amministrazione > Gestione identità > Impostazioni > Rimozione endpoint**.

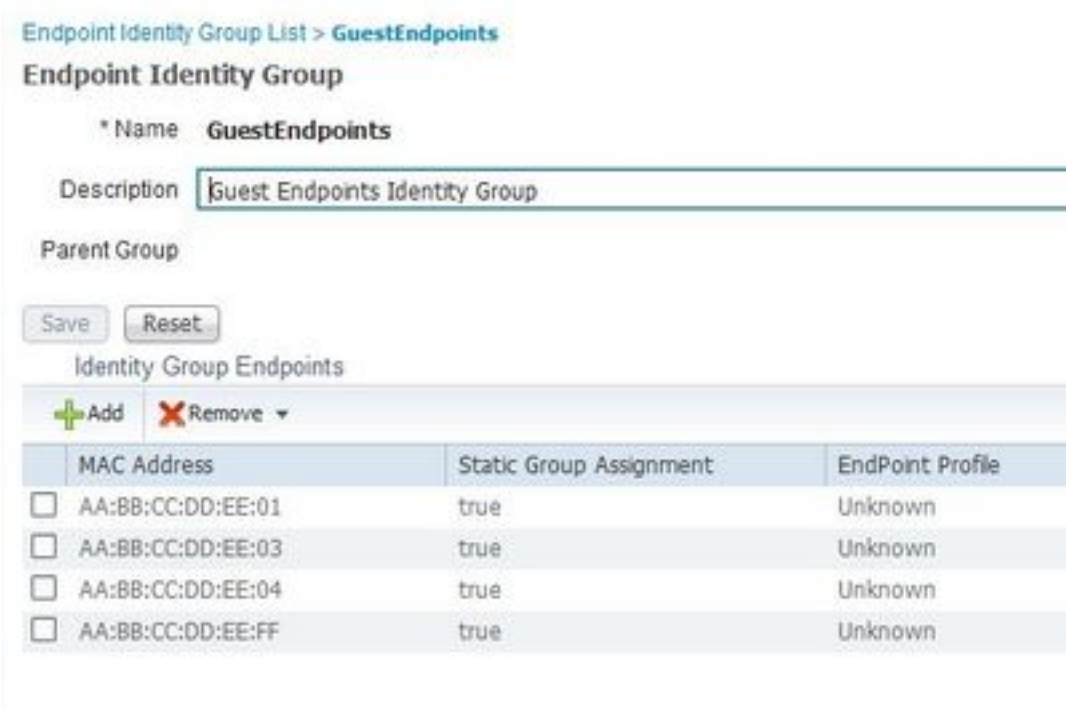
Giorni trascorsi: Indica il numero di giorni trascorsi dalla creazione dell'oggetto. Questa condizione può essere utilizzata per gli endpoint a cui è stato concesso l'accesso non autenticato o condizionale per un determinato periodo di tempo, ad esempio un endpoint guest o di un collaboratore esterno oppure per i dipendenti che utilizzano webauth per l'accesso alla rete. Al termine del periodo di prova consentito per la connessione, è necessario che le connessioni vengano riautenticate e registrate.

Giorni inattivi: Indica il numero di giorni trascorsi dall'ultima attività di profiling o dall'ultimo aggiornamento sull'endpoint. Questa condizione elimina i dispositivi obsoleti che si sono accumulati nel tempo, solitamente ospiti transitori o dispositivi personali o dispositivi ritirati. Nella maggior parte delle distribuzioni questi endpoint tendono a rappresentare un rumore in quanto non sono più attivi sulla rete o potrebbero essere rilevati nel prossimo futuro. In caso di riconnessione, verranno individuati, analizzati, registrati e così via in base alle esigenze.

Se sono presenti aggiornamenti dall'endpoint, InactivityDays verrà reimpostato su 0 solo se la profilatura è abilitata.

Data rimozione: Data di rimozione dell'endpoint. Questa opzione può essere utilizzata per eventi o gruppi speciali in cui l'accesso viene concesso per un periodo di tempo specifico, indipendentemente dall'ora di creazione o di inizio. In questo modo, è possibile eliminare tutti gli endpoint contemporaneamente. Ad esempio, una fiera, una conferenza o una classe di formazione settimanale con nuovi membri ogni settimana, in cui l'accesso viene concesso per una settimana o un mese specifico anziché per giorni/settimane/mesi assoluti.

In questo file profiler.log di esempio viene mostrato quando sono stati eliminati gli endpoint che facevano parte di GuestEndpoints e che erano trascorsi 30 giorni:

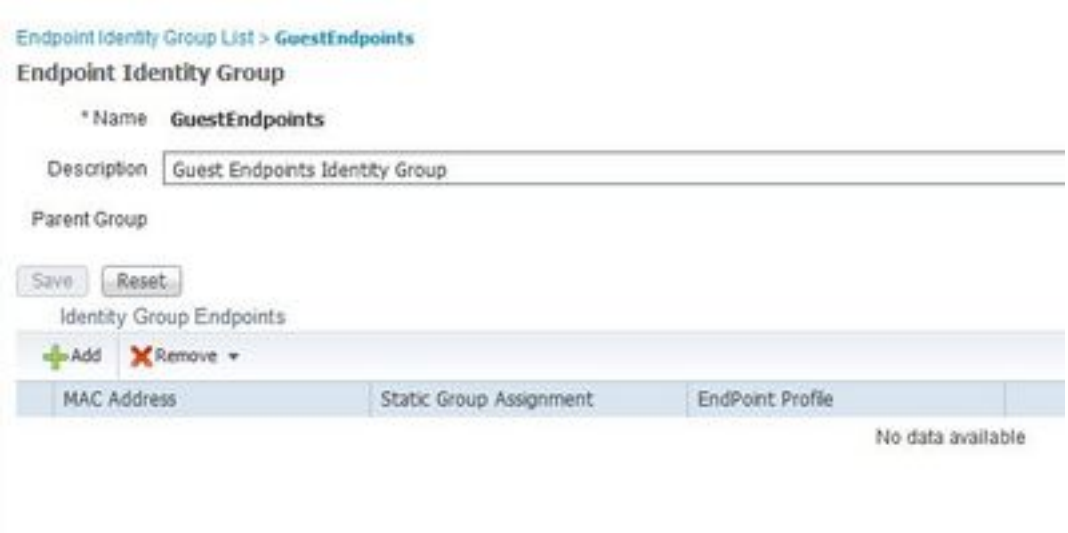



```
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- the rule type is :REGULAR
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- epPurgeRuleID is :3bfaffe0-8c01-
11e6-996c-525400b48521
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
```

Al termine dell'eliminazione:



Risoluzione dei problemi relativi a Guest ed Elimina

Per acquisire i log relativi ai problemi di guest ed eliminazione, questi componenti possono essere impostati per il debug. Per abilitare i debug, selezionare **Amministrazione > Sistema > Configurazione registro di debug > Seleziona nodo**.

Per la risoluzione dei problemi relativi agli account guest/sponsor e all'eliminazione degli endpoint, impostare questi componenti su debug:

- guestaccess
- guest-admin
- guest-access-admin
- profiler
- runtime-AAA

Per i problemi relativi al portale, impostare il debug dei seguenti componenti:

- sponsor
- portale
- portal-session-manager
- guestaccess

Informazioni correlate

- Guida all'installazione prescrittiva di ISE Guest Access
- Risoluzione dei problemi e abilitazione dei debug su ISE