ISE訪客帳戶管理

簡介

本文檔介紹發起人或ISE管理員可以對ISE上存在的訪客資料執行的常用操作。思科身份服務引擎(ISE)訪客服務為訪客（如訪客、承包商、顧問和客戶）提供安全的網路訪問。

作者：Shivam Kumar，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- ISE
- ISE訪客服務

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本2.6

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

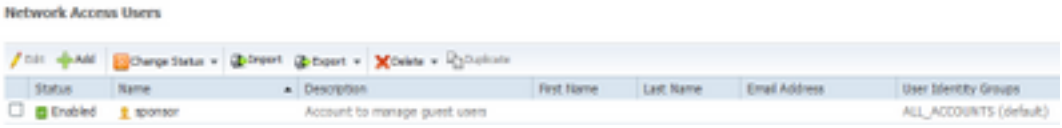
> **附註**：其他ISE版本的過程相似或相同。除非另有說明，否則可以在所有2.x ISE軟體版本上使用這些步驟。

設定

使用發起人管理訪客帳戶

保證人是ISE上有權登入到保證人門戶的使用者帳戶，他們可以在其中為授權訪問者建立臨時訪客帳戶並對其進行管理。發起人可以是內部使用者或外部身份庫（例如Active Directory）上的帳戶。

在本示例中，發起人帳戶在ISE內部定義並新增到預定義組中：ALL_ACCOUNTS。



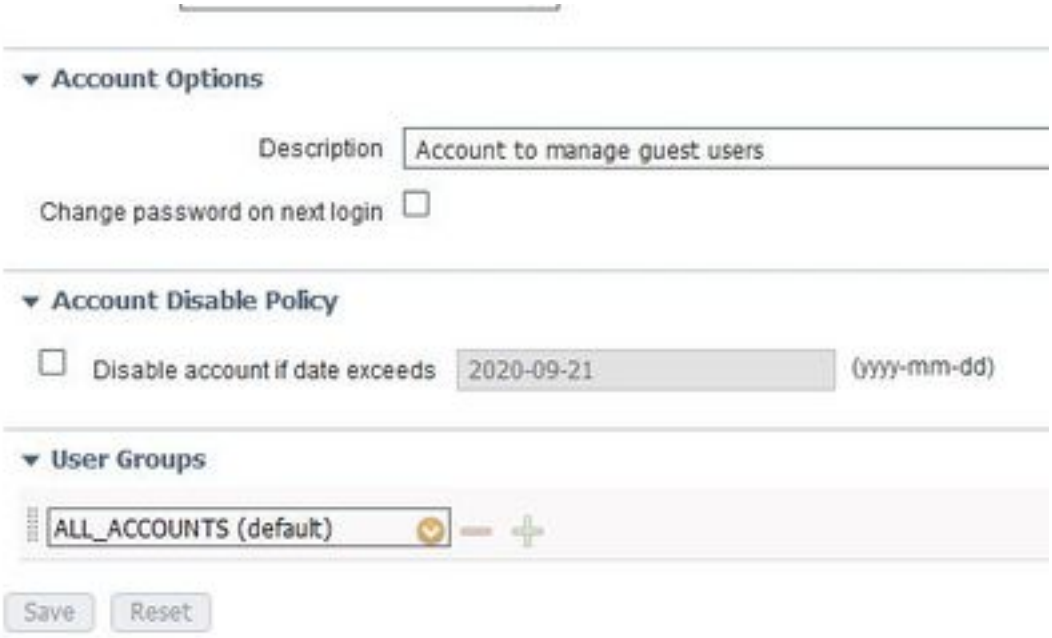
預設情況下，ISE有三個發起人組，發起人可以對映到：

ALL_ACCOUNTS（預設）：分配給此組的發起人可以管理所有訪客使用者帳戶。預設情況下，ALL_ACCOUNTS使用者身份組中的使用者是此發起人組的成員。

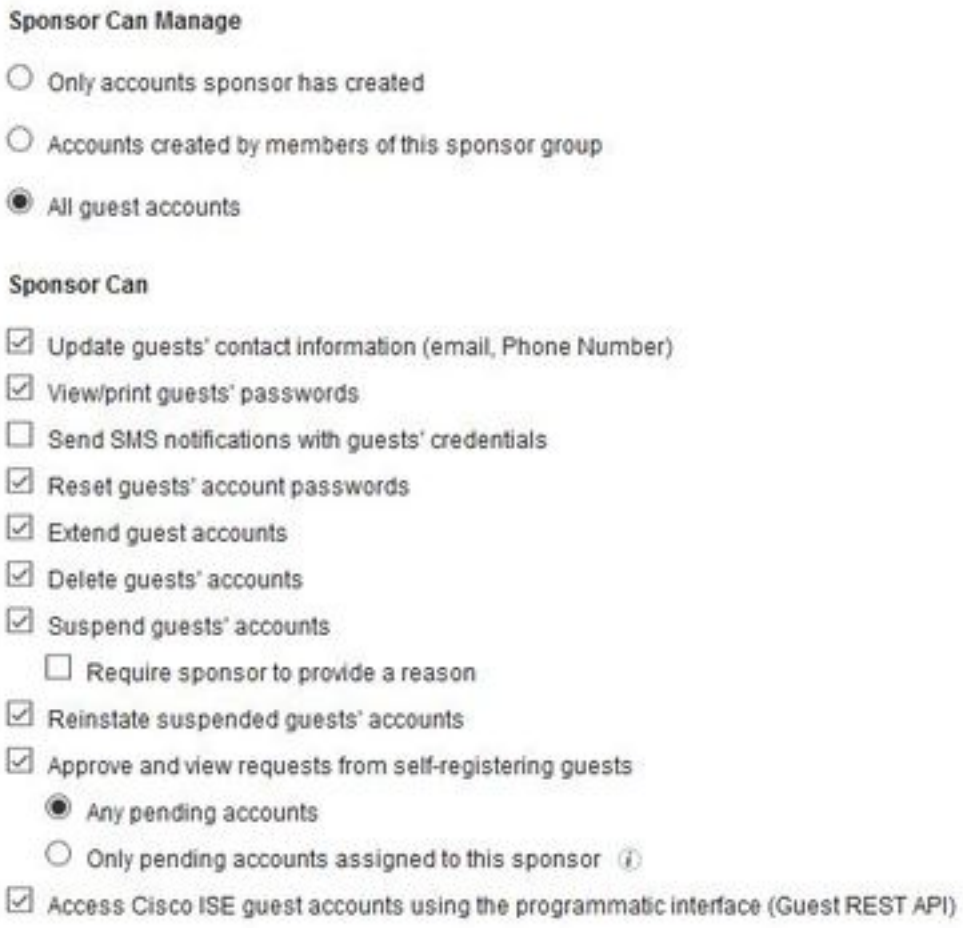
GROUP_ACCOUNTS（預設值）： 分配給此組的發起人只能管理由同一發起人組的發起人建立的訪客帳戶。預設情況下，GROUP_ACCOUNTS使用者身份組中的使用者是此發起人組的成員。

OWN_ACCOUNTS（預設）：分配給此組的發起人只能管理他們建立的訪客帳戶。預設情況下，OWN_ACCOUNTS使用者身份組中的使用者是此發起人組的成員。

此示例中使用的發起人帳戶對映到ALL_ACCOUNTS:



此發起人組的許可權和許可權位於**工作中心>訪客訪問>門戶和元件>發起人組**:



為了允許發起人通過ERS REST API訪問訪客管理，會在發起人的組中新增許可權，如圖所示。

使用Active Directory帳戶作為發起人

除了定義為發起人的內部使用者帳戶之外，外部身份源(如Active Directory(AD)或LDAP)上的帳戶還可以用作發起人來管理訪客帳戶。

導航到**管理>身份>外部身份源> Active Directory**，確保ISE已加入AD。如果尚未加入，請加入一個可用的AD域。

從包含帳戶的AD中檢索組：

此示例演示將AD使用者新增到ALL_ACCOUNTS發起人組。

導覽至 **Work Centers> Guest Access > Portal & Components > Sponsor Groups> ALL_ACCOUNTS**，然後按一下 **Members**，如下圖所示。

成員顯示所有可供選擇的組；選擇AD組並將其移動到右側，以將其新增到發起人組。

儲存更改。發起人門戶登入現在可與屬於選定AD組的AD使用者帳戶一起使用。

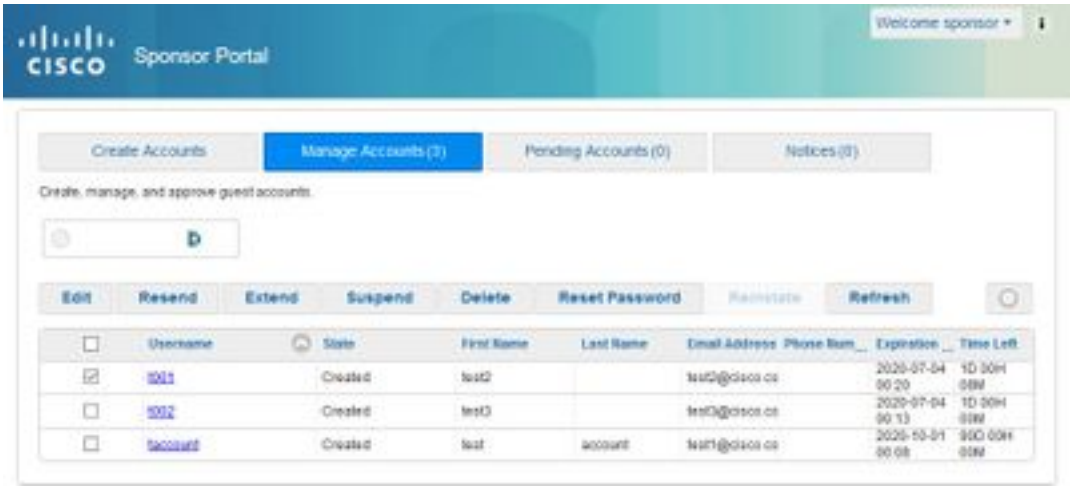
可以按照上述步驟通過LDAP新增使用者。內部定義的使用者身份組也可作為新增到發起人組的選項。

使用一個此類發起人帳戶登入發起人門戶。發起人門戶可用於：

- 編輯和刪除訪客帳戶
- 延長訪客帳戶持續時間
- 暫停訪客帳戶
- 恢復過期的訪客帳戶
- 重新傳送和重置訪客密碼

- 批准暫掛訪客帳戶

在發起人門戶上，選擇**Manage Accounts**頁籤以檢視此發起人有權管理的所有訪客帳戶，如下圖所示。

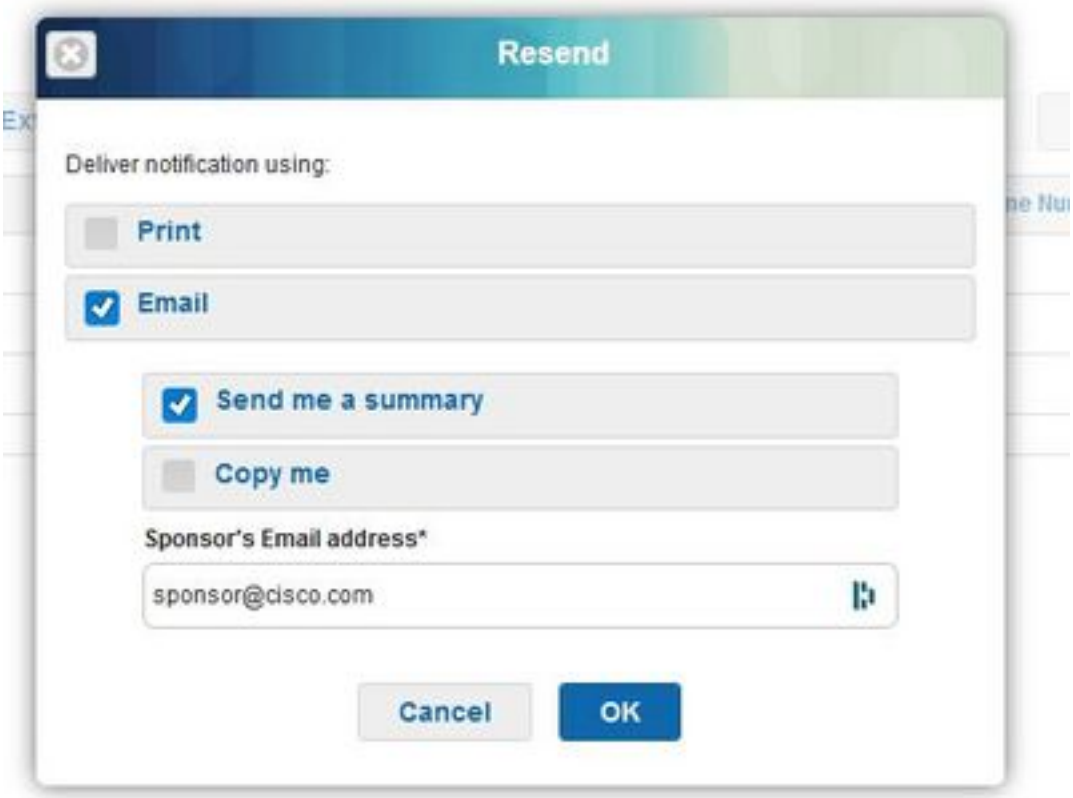


無論訪客帳戶處於何種狀態，都可以對其進行編輯。

如果帳戶擁有者忘記或丟失了訪客帳戶密碼，可以選擇重新傳送訪客帳戶密碼。僅當訪客帳戶的密碼處於**Active**或**Created**狀態時，才能重新傳送密碼。

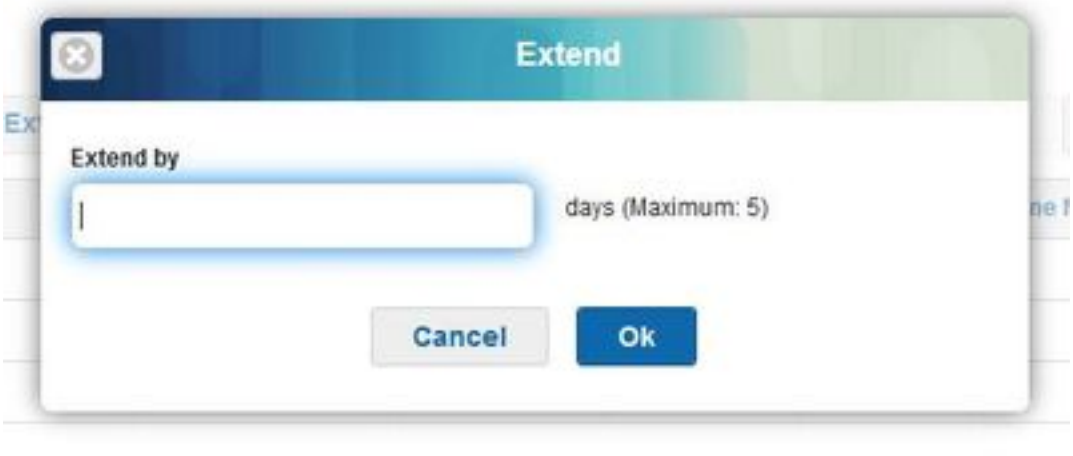
不能為已更改密碼的訪客重新傳送密碼。在這種情況下，必須首先使用reset password選項。無法傳送等待批准、已掛起、已過期或已拒絕的帳戶的密碼。

保證人可以選擇接收更改密碼副本的選項：



如果需要允許訪客訪問網路的時間長於最初允許的時間，請使用擴展選項增加持續時間。處於「已建立」、「活動」或「已過期」狀態的帳戶可以擴展。

已暫停或拒絕的帳戶無法擴展；改用reinstate選項。



允許的最大擴展期限由帳戶的訪客型別控制。

訪客帳戶在達到帳戶持續時間結束時自行過期，無論其處於何種狀態。已暫停或到期的訪客帳戶根據系統中定義的清除策略自動清除。預設情況下，每15天清除一次。

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

訪客帳戶狀態及其含義：

活動：擁有這些帳戶的訪客已通過認證的訪客門戶成功登入，或者繞過認證的訪客強制門戶。在後一種情況下，帳戶屬於配置為繞過憑證型訪客強制門戶的訪客型別。這些訪客可以通過向其裝置上的本地請求方提供其登入憑證來訪問網路。

建立時間：帳戶已建立，但訪客尚未登入到憑證的訪客門戶。在這種情況下，帳戶將分配給訪客型別，這些型別未配置為繞過憑證型訪客強制網路門戶。訪客必須先通過具有憑證的訪客強制網路門戶登入，然後才能訪問網路的其它部分。

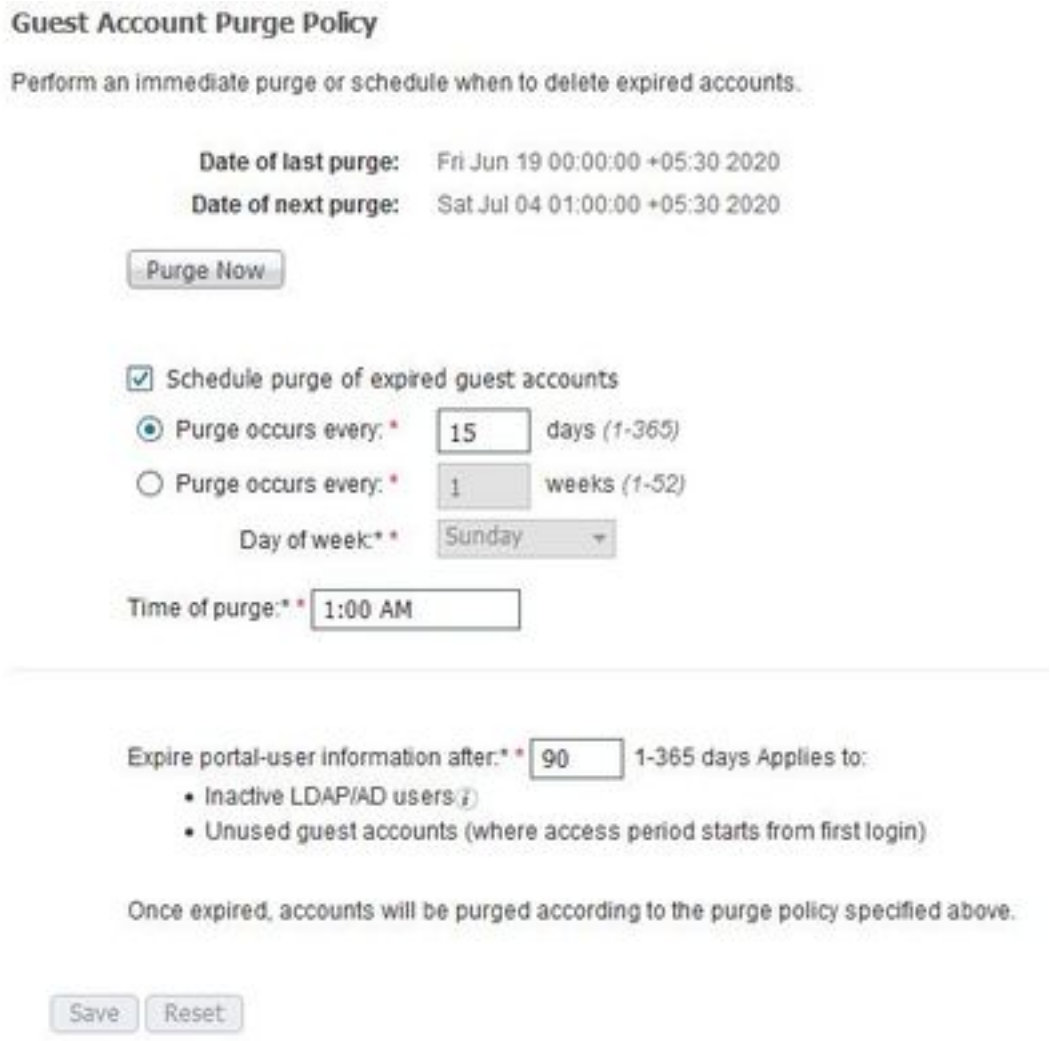
已拒絕:拒絕帳戶訪問網路。處於拒絕狀態時過期的帳戶仍保留為已拒絕。

待審批：帳戶正在等待批准以訪問網路。

已掛起：帳戶由有權這樣做的發起人暫停。

訪客清除策略

預設情況下，ISE每15天自動清除過期的訪客帳戶。此資訊可在**工作中心>訪客接入>設定>訪客帳戶清除策略**下檢視。



下一次清除的日期指明下一次清除的時間。ISE管理員可以：

- 計畫每X天執行一次清除。**清除時間**指定第一次清除在X天內發生的時間。然後，每X天執行一次清除。
- 在每週的某一天計劃清除，每X周。
- 使用選項「立即清除」強制執行**按需清除。**

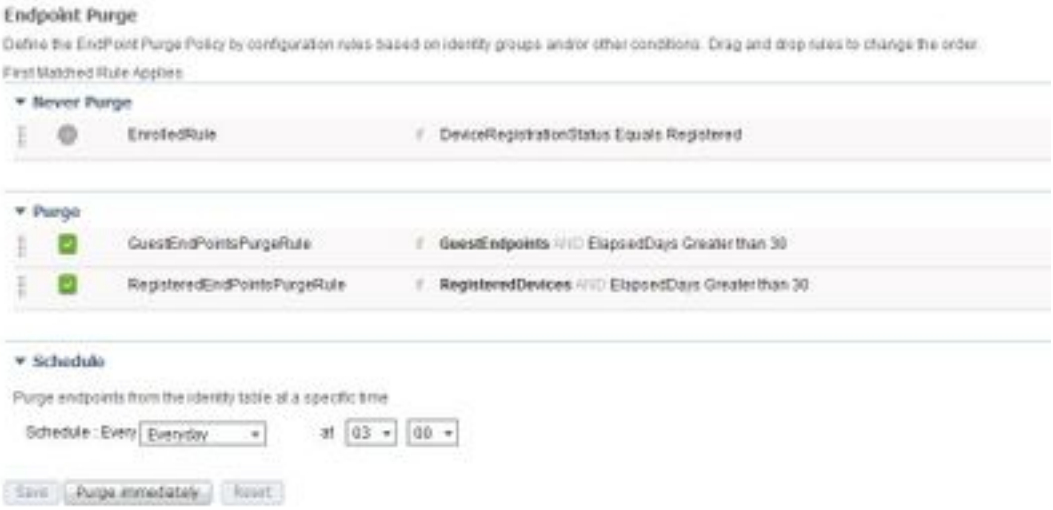
清除過期的訪客帳戶後，將保留關聯的端點、報告和日誌記錄資訊。

終端清除：終端的非活動天數和已用天數

預設情況下，訪客用於訪問網路的終端將成為GuestEndpoints的一部分。ISE具有刪除超過30天的訪客終端和註冊裝置的策略。根據主管理節點(PAN)上配置的時區，此預設清除作業每天凌晨1點運行。 此預設策略使用ElapsedDays**條件**。其它可用選項有**InactiveDays**和**PurgeDate**。

> **附註**：終端清除功能獨立於訪客帳戶清除策略和訪客帳戶過期。

策略在**Administration > Identity Management > Settings > Endpoint Purge**下定義。



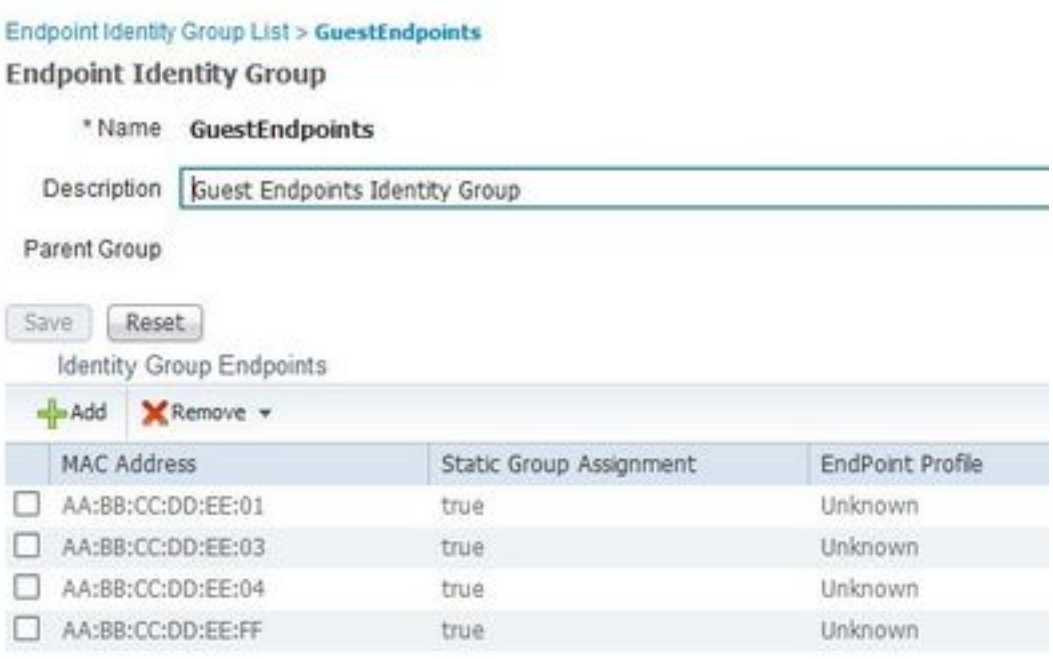
已用天數：這表示自對象建立以來的天數。此條件可用於在設定時間內被授予未經驗證或條件式存取許可權的端點（例如訪客或承包商端點），或是使用webauth進行網路存取的員工。在允許的連線寬限期之後，必須對其進行完全重新驗證和註冊。

非活動天數：表示自終結點上上次分析活動或更新後的天數。此條件會清除隨時間累積的陳舊裝置、通常是臨時訪客或個人裝置，或者已停用的裝置。這些端點在多數部署中往往代表噪音，因為它們不再在網路上處於活動狀態，或者在不久的將來可能會被看到。如果碰巧再次連線，則系統會根據需要重新發現、分析、註冊等。

如果終端有更新，則只有在啟用分析時，InactivityDays才會重置為0。

清除日期：清除終結點的日期。此選項可用於在特定時間授予訪問許可權的特殊事件或組，無論其建立或開始時間如何。這樣可同時清除所有端點。例如，每週有新成員的貿易展、會議或每週培訓課，其中授予特定周或月份訪問許可權，而不是絕對的天/周/月。

此示例profiler.log檔案顯示屬於GuestEndpoints且已運行30天的終結點被清除的時間：



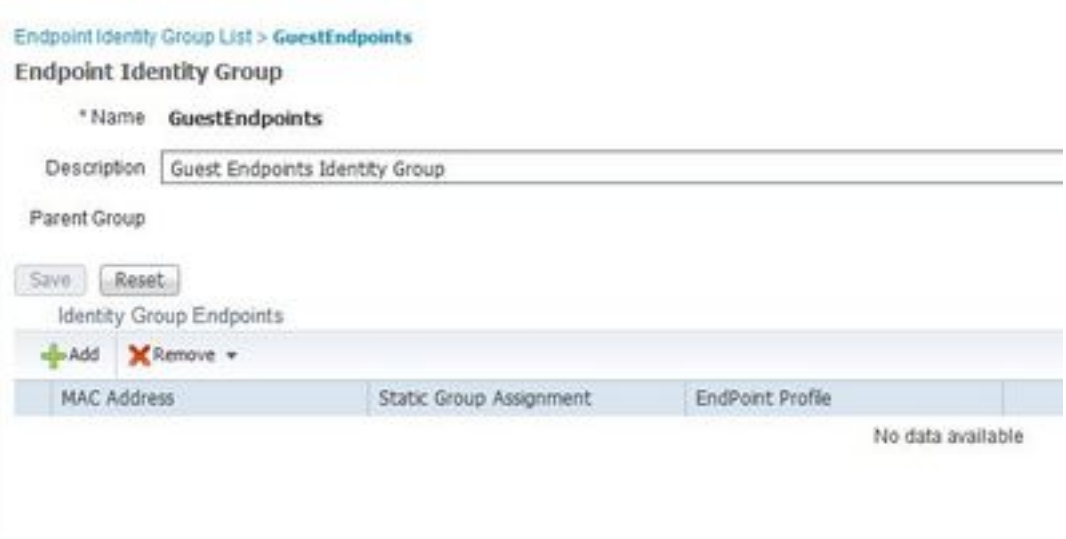

```
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
```

```
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
```

清除完成後：



排解訪客和清除問題

為了捕獲與訪客和清除問題相關的日誌，可以將這些元件設定為調試。要啟用調試，請導航到**管理>系統>調試日誌配置>選擇節點**。

對於訪客/發起人帳戶和終端清除相關的故障排除，請將這些元件設定為調試：

- 訪客接入
- guest-admin
- guest-access-admin
- 探查器
- 運行時AAA

對於與門戶相關的問題，請將這些元件設定為調試：

- 贊助商門戶
- 門戶
- portal-session-manager
- 訪客接入

相關資訊

- **ISE訪客訪問規範部署指南**
- **在ISE上排除故障並啟用調試**