ISE访客帐户管理

简介

本文档介绍保证人或ISE管理员可对ISE上存在的访客数据执行的常用操作。思科身份服务引擎(ISE)访客服务为访客（如访客、承包商、顾问和客户）提供安全的网络访问。

作者：思科TAC工程师Shivam Kumar。

先决条件

要求

思科建议您了解以下主题：

- ISE
- ISE访客服务

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本2.6

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

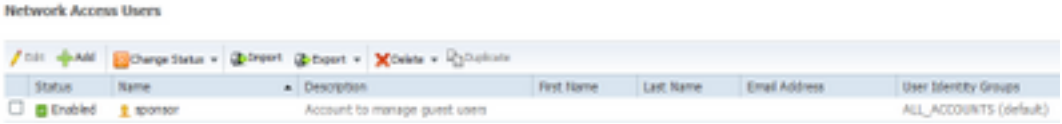
> **注意：**其他ISE版本的过程类似或相同。除非另有说明，否则可在所有2.x ISE软件版本上使用这些步骤。

配置

使用发起人管理访客帐户

保证人是ISE上有权登录保证人门户的用户帐户，在该门户中，他们可以为授权访问者创建临时访客帐户并管理这些帐户。发起人可以是内部用户或外部身份库（如活动目录）上的帐户。

在本示例中，保证人帐户在ISE内部定义并添加到预定义组：ALL_ACCOUNTS。



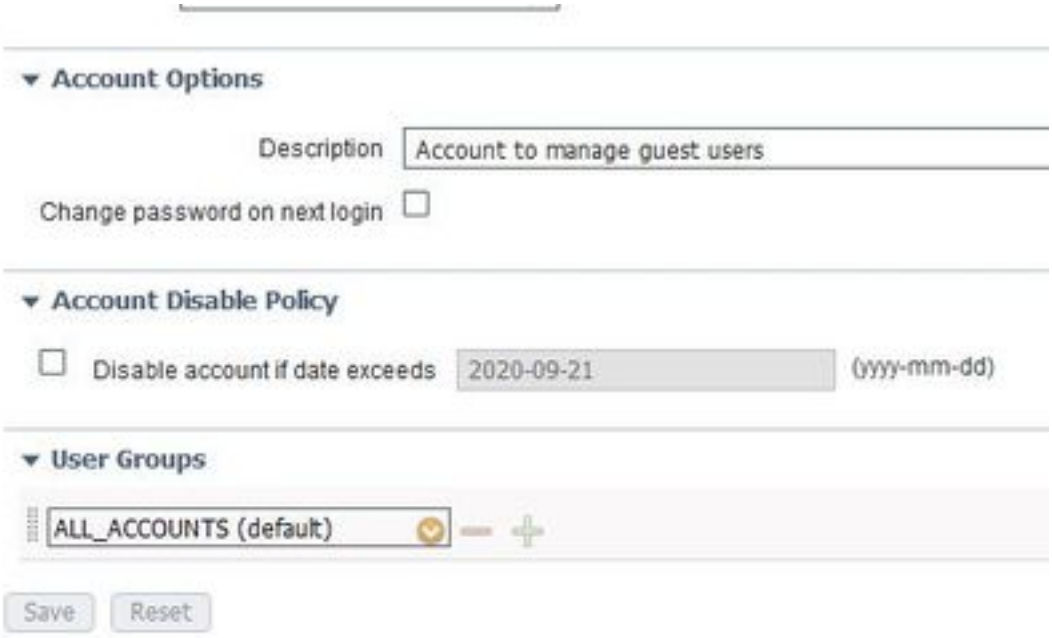
默认情况下，ISE有三个发起人组，发起人可以映射到：

ALL_ACCOUNTS（默认）：分配给此组的发起人可以管理所有访客用户帐户。默认情况下，ALL_ACCOUNTS用户身份组中的用户是此发起人组的成员。

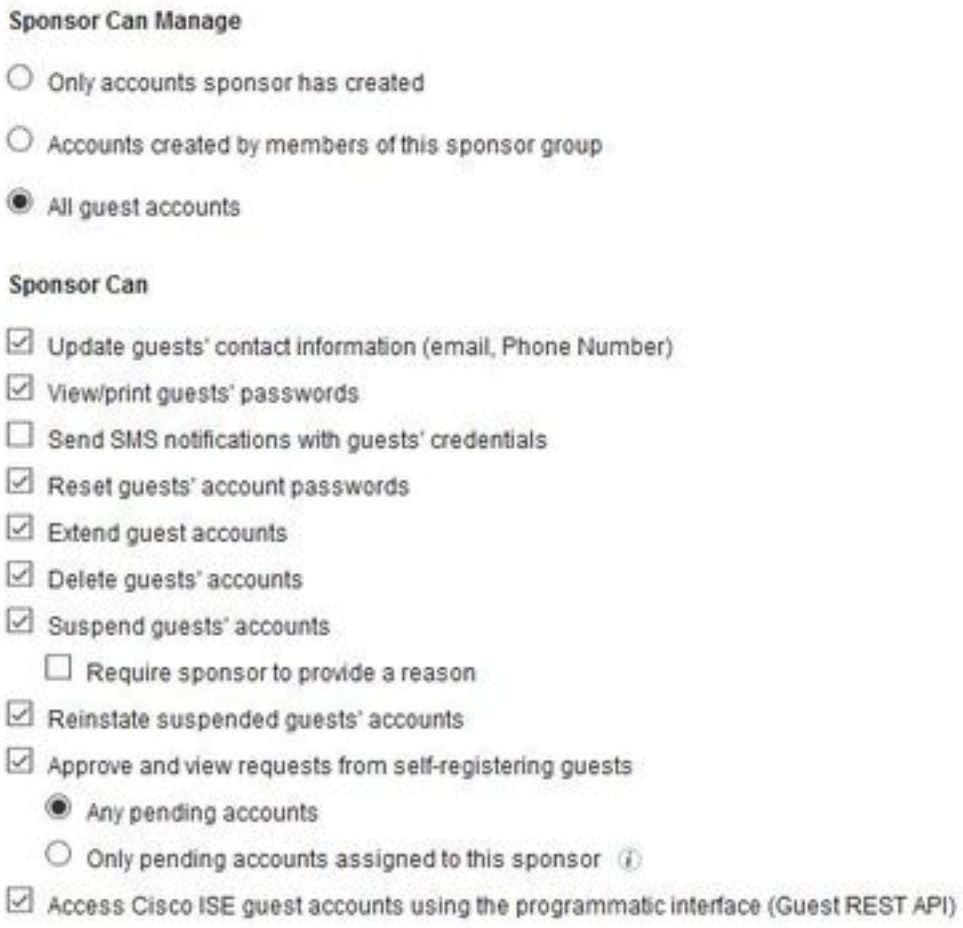
GROUP_ACCOUNTS（默认）： 分配给此组的发起人只能管理由同一发起人组的发起人创建的访客帐户。默认情况下，GROUP_ACCOUNTS用户身份组中的用户是此发起人组的成员。

OWN_ACCOUNTS（默认）：分配给此组的发起人只能管理他们创建的访客帐户。默认情况下，OWN_ACCOUNTS用户身份组中的用户是此发起人组的成员。

本示例中使用的保证人帐户映射到ALL_ACCOUNTS:



此发起人组的权限和权限可在工作中心>访**客访问>门户和组件>发起人组**:



为了允许发起人通过ERS REST API访问访客管理，会在发起人的组中添加权限，如图所示。

使用Active Directory帐户作为发起人

与定义为发起人的内部用户帐户一起，外部身份源(如Active Directory(AD)或LDAP)上的帐户也可用作发起人来管理访客帐户。

通过导航至Administration > Identities > External Identity Sources > Active Directory，确保ISE已加入AD。如果尚未加入，请加入其中一个可用AD域。

从包含帐户的AD检索组：

此示例演示将AD用户添加到ALL_ACCOUNTS发起人组。

导航到工 **作中心>访客访问>门户和组件>发起人组> ALL_ACCOUNTS，然**后单击成 **员**，如下图所示。

成员显示所有可供选择的组；选择AD组并将其向右移动，以将其添加到发起人组。

保存更改。保证人门户登录现在与属于所选AD组的AD用户帐户配合使用。

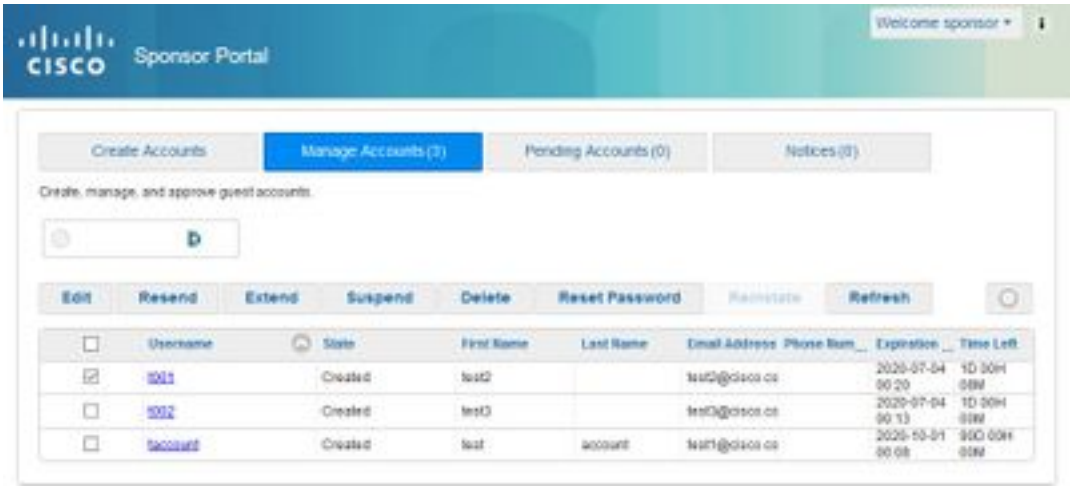
通过LDAP添加用户时，可遵循上述相同步骤。内部定义的用户身份组也可作为添加到发起人组的选项。

使用此类发起人帐户登录发起人门户。发起人门户可用于：

- 编辑和删除访客帐户
- 延长访客帐户持续时间
- 暂停访客帐户
- 恢复过期的访客帐户
- 重新发送和重置访客密码

- 批准待处理访客帐户

在发起人门户上，选择**Manage Accounts** 选项卡，查看此发起人有权管理的所有访客帐户，如此图所示。

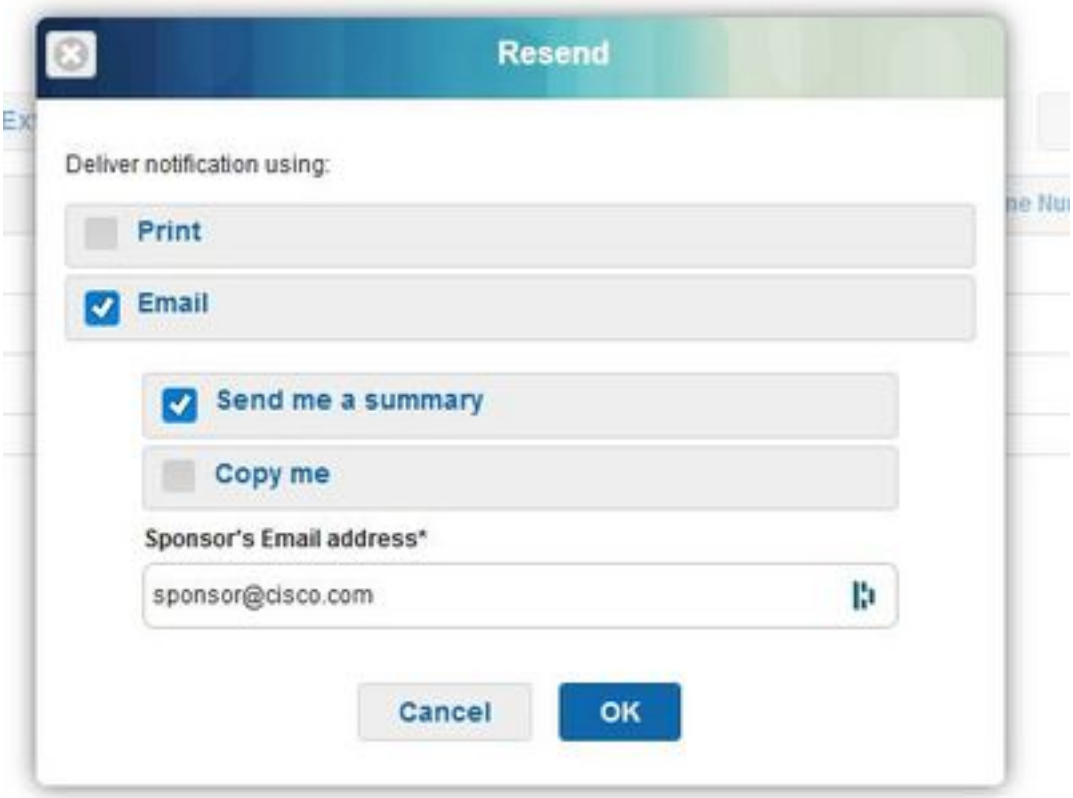


无论访客帐户处于何种状态，都可以编辑访客帐户。

可以选择重新发送访客帐户密码，以防帐户持有者忘记或丢失密码。仅当访客帐户的密码处于“活动”或“已创建”状态时，才**能重新**发送**该密**码。

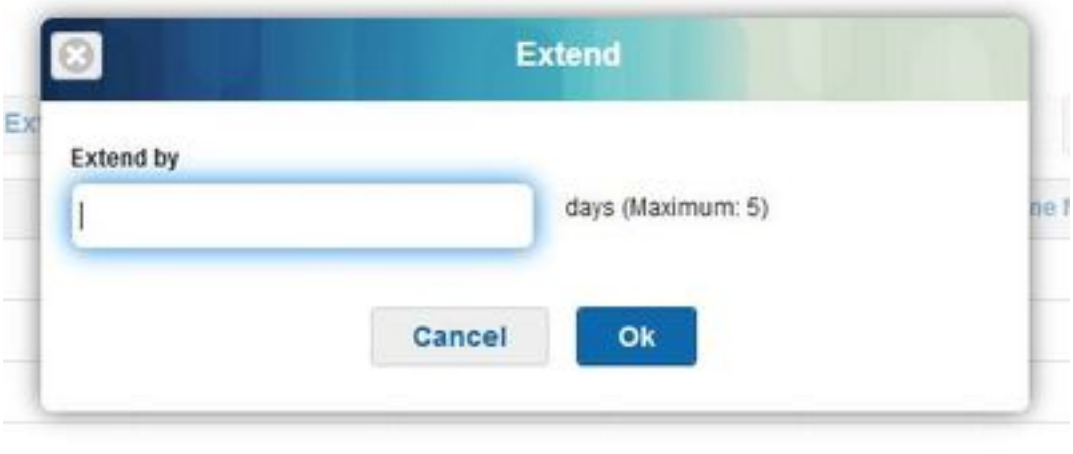
密码不能重新发送给已更改密码的访客。在这种情况下，必须首先使用重置密码选项。无法为等待审批、暂停、过期或拒绝的帐户发送密码。

保证人可以选择接收更改密码副本的选项：



如果需要允许访客访问网络的时间超过最初允许的时间，请使用扩展选项延长持续时间。处于“已创建”、“活动”或“已过期”状态的帐户可以扩展。

已暂停或拒绝的帐户不能延期；请改用reintate选项。



允许的最长延长期由帐户的访客类型管理。

访客帐户在达到帐户持续时间结束时自行过期，无论其状态如何。系统将根据系统上定义的清除策略自动清除已暂停或过期的访客帐户。默认情况下，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

访客帐户状态及其含义：

活动：拥有这些帐户的访客已通过需要提供凭证的访客门户成功登录，或绕过需要提供凭证的访客强制门户。在后一种情况下，帐户属于配置为绕过需要提供凭证的访客强制网络门户的访客类型。这些访客可以通过向其设备上的本地请求方提供登录凭证来访问网络。

已创建：帐户已创建，但访客尚未登录需要提供凭证的访客门户。在这种情况下，帐户将分配给未配置为绕过需要提供凭证的访客强制网络门户的访客类型。访客必须先通过需要提供凭证的访客强制网络门户登录，然后才能访问网络的其他部分。

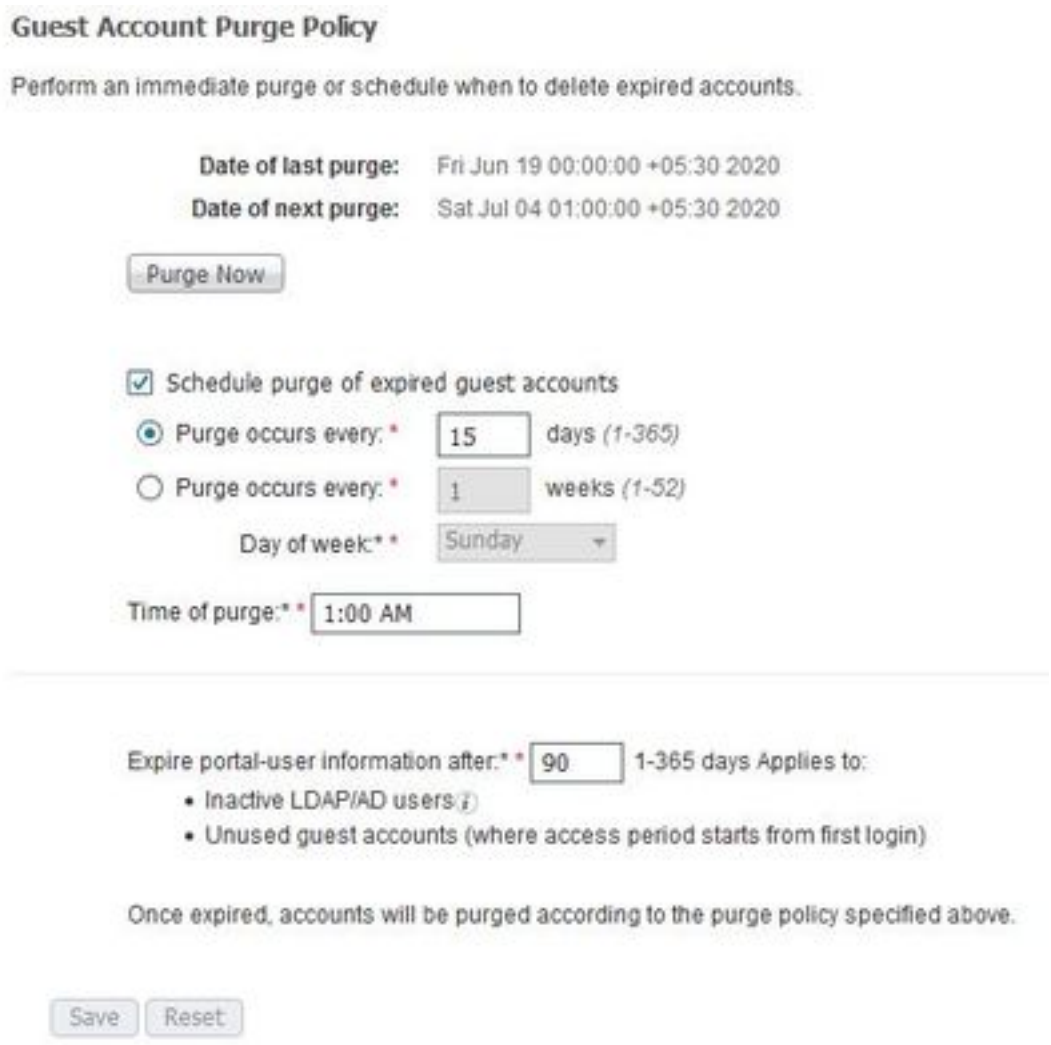
拒绝：拒绝帐户访问网络。处于拒绝状态时过期的帐户将保持为拒绝状态。

等待审批:这些帐户正在等待批准访问网络。

暂停：帐户由有权暂停的发起人暂停。

访客清除策略

默认情况下，ISE每15天自动清除过期的访客帐户。此信息可在工作中心(**Work Centers)>访客访问(Guest Access)>设置(Settings)>访客帐户清除策略(Guest Account Purge Policy)下查看**。



下次清除的日期指示下次清除的时间。ISE管理员可以：

- 计划每X天执行一次清除。清除**时间指**定第一次清除的时间（X天）。之后，清除每X天发生一次。
- 安排在一周中的某一天，每X周执行一次清除。
- 使用“立即清除”选项强制按需**清除。**

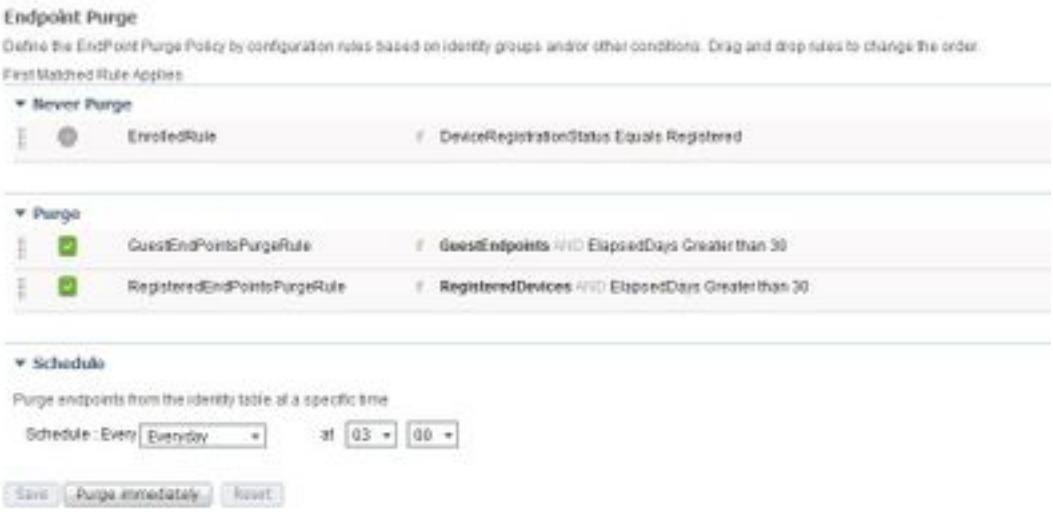
清除过期的访客帐户后，会保留关联的终端、报告和日志记录信息。

终端清除：终端的非活动天数与已用天数

默认情况下，访客用于访问网络的终端将成为访客终端的一部分。ISE具有删除访客终端和30天以前的注册设备的策略。此默认清除作业根据在主管理节点(PAN)上配置的时区每天上午1点运行。 此默认策略使用ElapsedDays**条件**。其他可用选项**为InactiveDays**和**PurgeDate**。

> **注意**：终端清除功能独立于访客帐户清除策略和访客帐户过期。

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



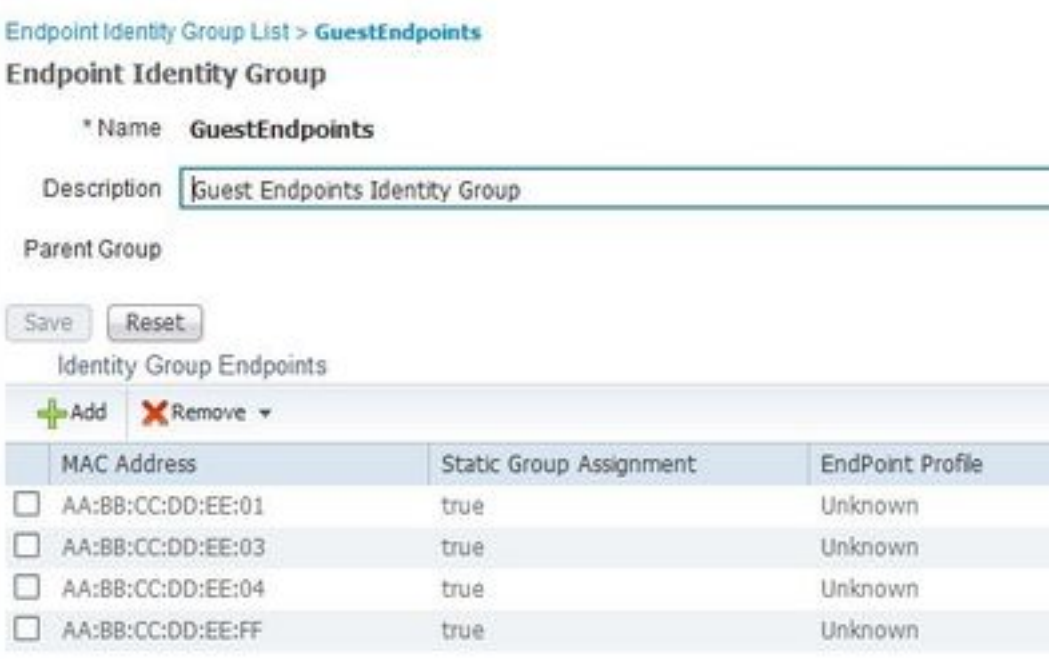
已用天数：这表示自创建对象以来的天数。此条件可用于在指定时间段内被授予未经身份验证或有条件访问权限的终端，例如访客或承包商终端，或使用webauth进行网络访问的员工。在允许的连接宽限期后，必须对它们进行完全重新身份验证和注册。

非活动天数：表示自上次分析活动或终端更新以来的天数。此条件清除随时间积累的过时设备、通常为临时访客或个人设备或已停用设备。由于这些终端在网络中不再处于活动状态或在不久的将来可能出现，因此在大多数部署中，这些终端往往代表噪音。如果它们碰巧再次连接，则会根据需要重新发现、分析、注册等。

当终端有更新时，仅当启用分析时，InactivityDays才会重置为0。

清除日期:清除终端的日期。此选项可用于授予特定时间访问权限的特殊事件或组，无论创建时间或开始时间如何。这允许同时清除所有终端。例如，每周有新成员参加的贸易展、会议或每周培训课程，其中授予访问权限的是特定周或月，而不是绝对的天/周/月。

此示例profiler.log文件显示属于GuestEndpoints且已过30天的终端何时被清除：



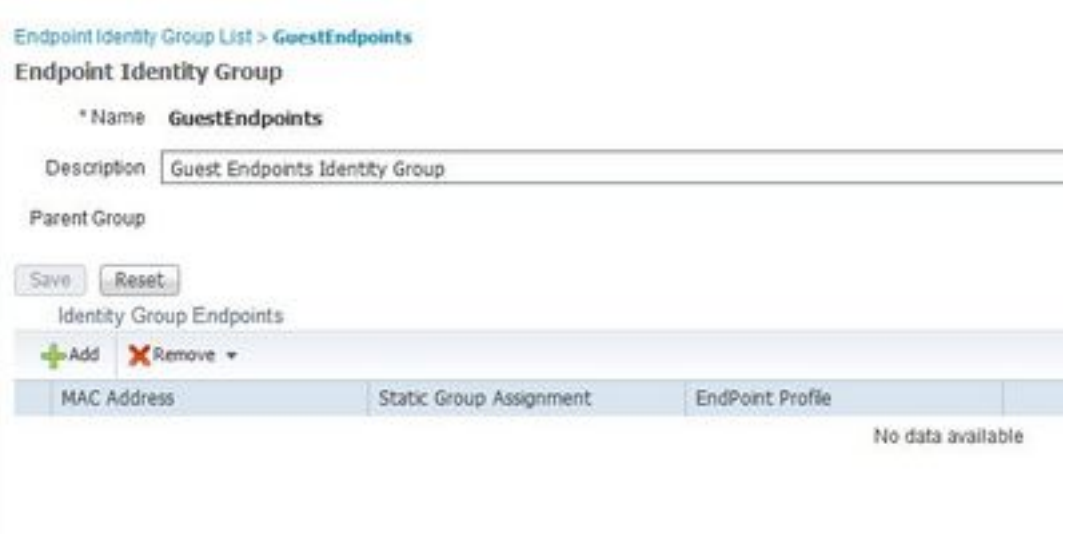

```
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
```

```
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
```

清除完成后：



排除访客和清除问题

为了捕获与访客和清除问题相关的日志，这些组件可设置为调试。要启用调试，请导航至 **Administration > System > Debug Log Configuration > Select node**。

对于访客/发起人帐户和终端清除相关故障排除，请将以下组件设置为调试：

- 访客访问
- guest-admin
- guest-access-admin
- 分析器
- 运行时AAA

对于与门户相关的问题，请将以下组件设置为调试：

- 响应门户
- 门户
- portal-session-manager
- 访客访问

相关信息

- ISE访客接入规范部署指南
- ISE上的故障排除和启用调试