ISE Guest Account Management

Introduction

This document describes the frequently used actions that a sponsor or an ISE administrator can take on guest data present on ISE. Cisco Identity Services Engine (ISE) guest services provide secure network access to guests such as visitors, contractors, consultants, and customers.

Contributed by Shivam Kumar, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

- ISE
- ISE guest services

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE, Release 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. If your network is live, ensure that you understand the potential impact of any command.

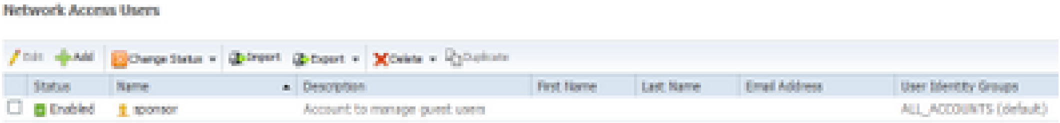
> **Note**: The procedure is similar or identical for other ISE versions. One can use these steps on all 2.x ISE Software Releases unless stated otherwise.

Configure

Use a Sponsor to Manage Guest Accounts

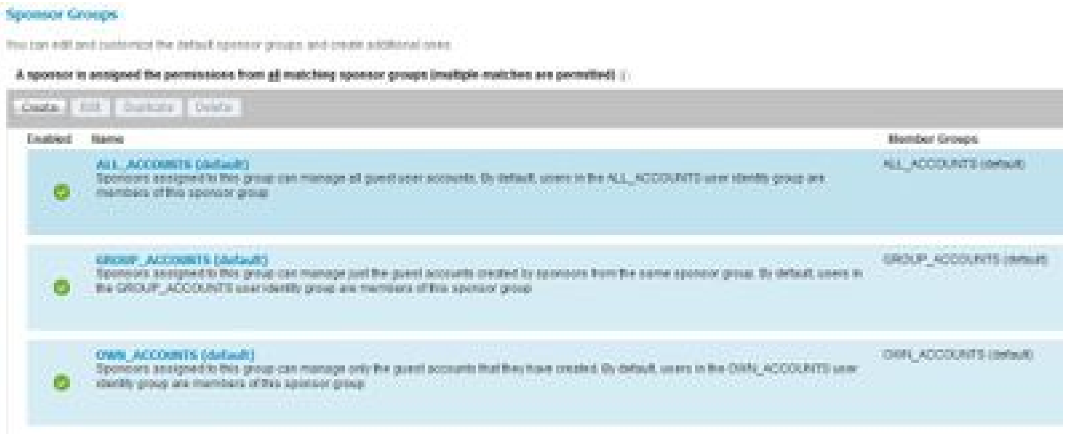
Sponsors are user accounts on ISE that have the privilege to log in to sponsor portal where they can create temporary guest accounts for authorized visitors and manage them. A sponsor can be an internal user or an account present on an external identity store such as an active directory.

In this example, the sponsor account is defined internally on ISE and added to the predefined group: ALL_ACCOUNTS.



	Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups
□	Enabled	sponsor	Account to manage guest users				ALL_ACCOUNTS (default)

By default, ISE has three sponsor groups that sponsors can be mapped to:



Sponsor Groups

You can edit and customize the default sponsor groups and create additional ones

A sponsor is assigned the permissions from all matching sponsor groups (multiple matches are permitted)

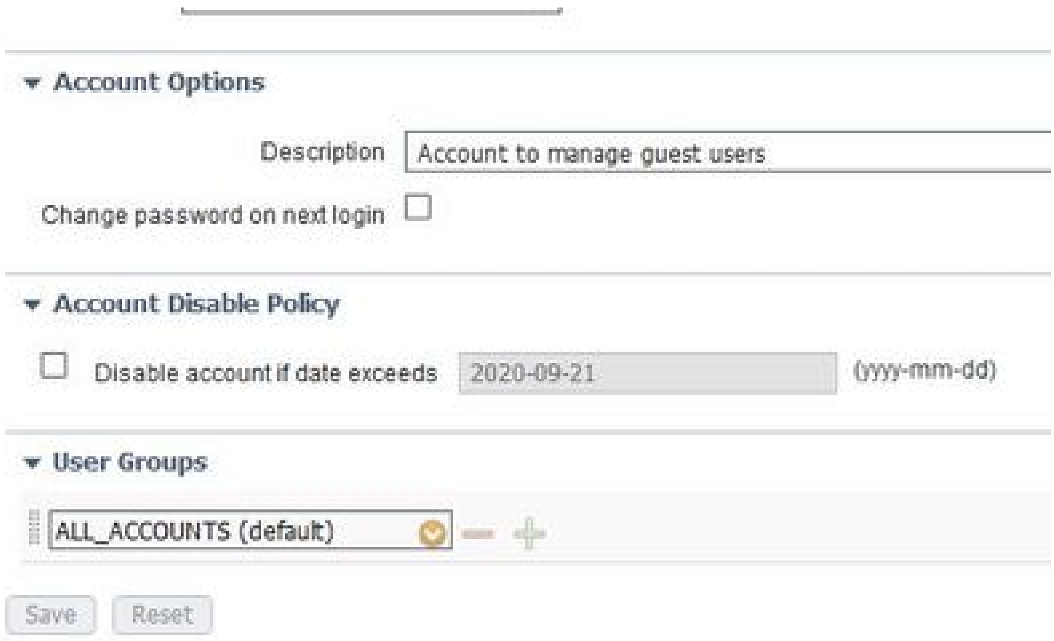
Enabled	Name	Member Groups
✓	ALL_ACCOUNTS (default) Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group	ALL_ACCOUNTS (default)
✓	GROUP_ACCOUNTS (default) Sponsors assigned to this group can manage just the guest accounts created by sponsors from the same sponsor group. By default, users in the GROUP_ACCOUNTS user identity group are members of this sponsor group	GROUP_ACCOUNTS (default)
✓	OWN_ACCOUNTS (default) Sponsors assigned to this group can manage only the guest accounts that they have created. By default, users in the OWN_ACCOUNTS user identity group are members of this sponsor group	OWN_ACCOUNTS (default)

ALL_ACCOUNTS (default): Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group.

GROUP_ACCOUNTS (default): Sponsors assigned to this group can manage just the guest accounts created by sponsors from the same sponsor group. By default, users in the GROUP_ACCOUNTS user identity group are members of this sponsor group.

OWN_ACCOUNTS (default): Sponsors assigned to this group can manage only the guest accounts that they have created. By default, users in the OWN_ACCOUNTS user identity group are members of this sponsor group.

The sponsor account used in this example is mapped to ALL_ACCOUNTS:



▾ Account Options

Description: Account to manage guest users

Change password on next login □

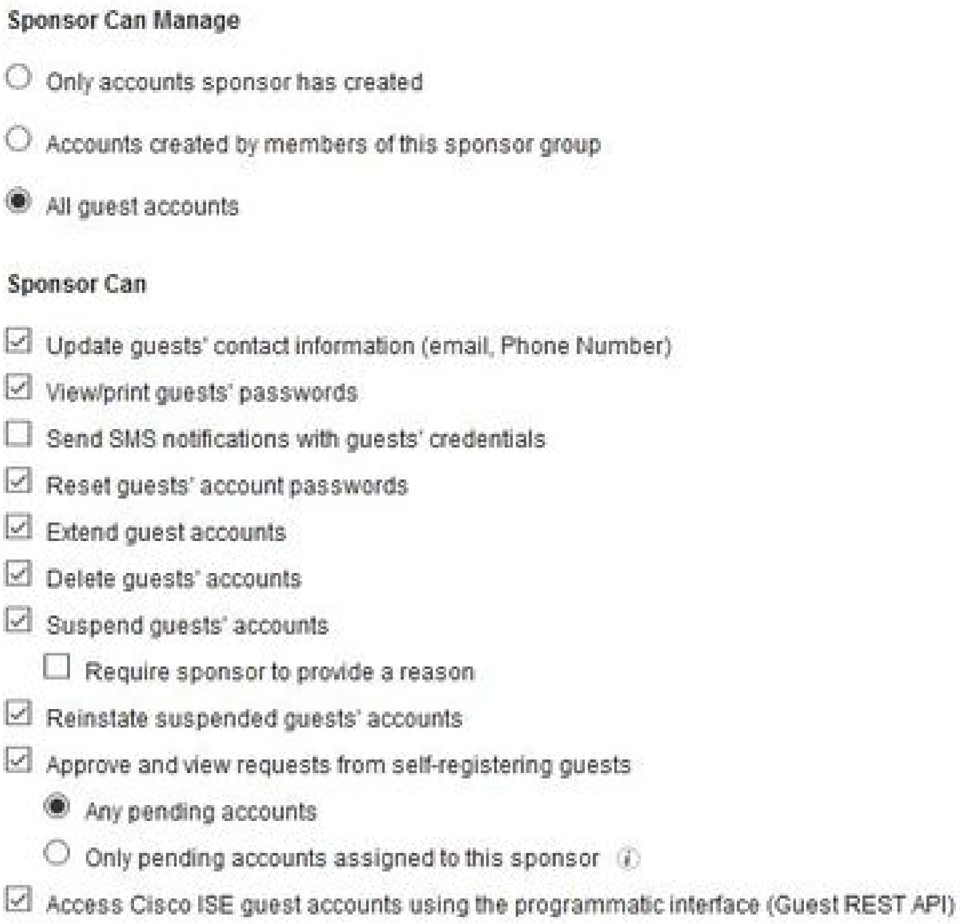
▾ Account Disable Policy

□ Disable account if date exceeds 2020-09-21 (yyyy-mm-dd)

▾ User Groups

ALL_ACCOUNTS (default)

The permissions and privileges of this sponsor group are available at **Work Centres> Guest Access > Portal & Components > Sponsor Groups**:



Sponsor Can Manage

○ Only accounts sponsor has created

○ Accounts created by members of this sponsor group

● All guest accounts

Sponsor Can

☑ Update guests' contact information (email, Phone Number)

☑ View/print guests' passwords

□ Send SMS notifications with guests' credentials

☑ Reset guests' account passwords

☑ Extend guest accounts

☑ Delete guests' accounts

☑ Suspend guests' accounts

  □ Require sponsor to provide a reason

☑ Reinstate suspended guests' accounts

☑ Approve and view requests from self-registering guests

  ● Any pending accounts

  ○ Only pending accounts assigned to this sponsor

☑ Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)

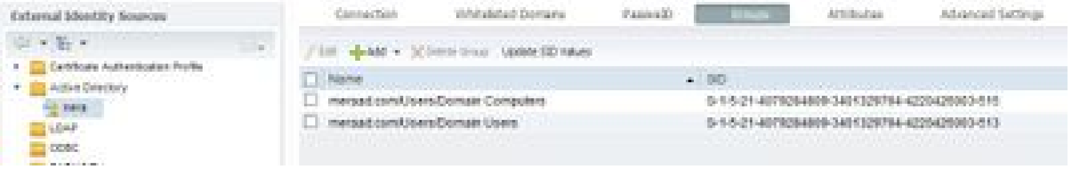
In order to allow a sponsor access to guest management via ERS REST API, permission is added in the sponsor's group as seen in the image.

Use Active Directory Account as Sponsor

Along with internal user accounts defined as sponsors, accounts present on external identity sources such as Active Directory (AD) or LDAP can also be used as sponsor to manage guest accounts.

Ensure that the ISE is joined to AD by navigating to **Administration> Identities > External Identity Sources > Active Directory**. If not already joined, join one of the available AD domains.

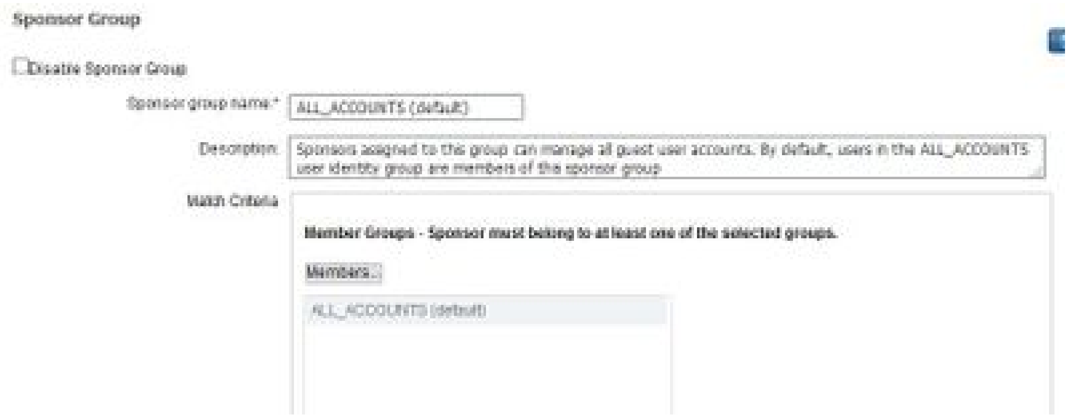
Retrieve the groups from AD that contains the accounts:



Name	SID
mersad.com/Users/Domain Computers	S-1-5-21-4078284809-3401329784-4220426063-515
mersad.com/Users/Domain Users	S-1-5-21-4078284809-3401329784-4220426063-513

This example demonstrates adding AD user to ALL_ACCOUNTS Sponsor group.

Navigate to **Work Centres> Guest Access > Portal & Components > Sponsor Groups> ALL_ACCOUNTS** and then click on **Members**, as shown in this image.



Sponsor Group

□ Disable Sponsor Group

Sponsor group name:* ALL_ACCOUNTS (default)

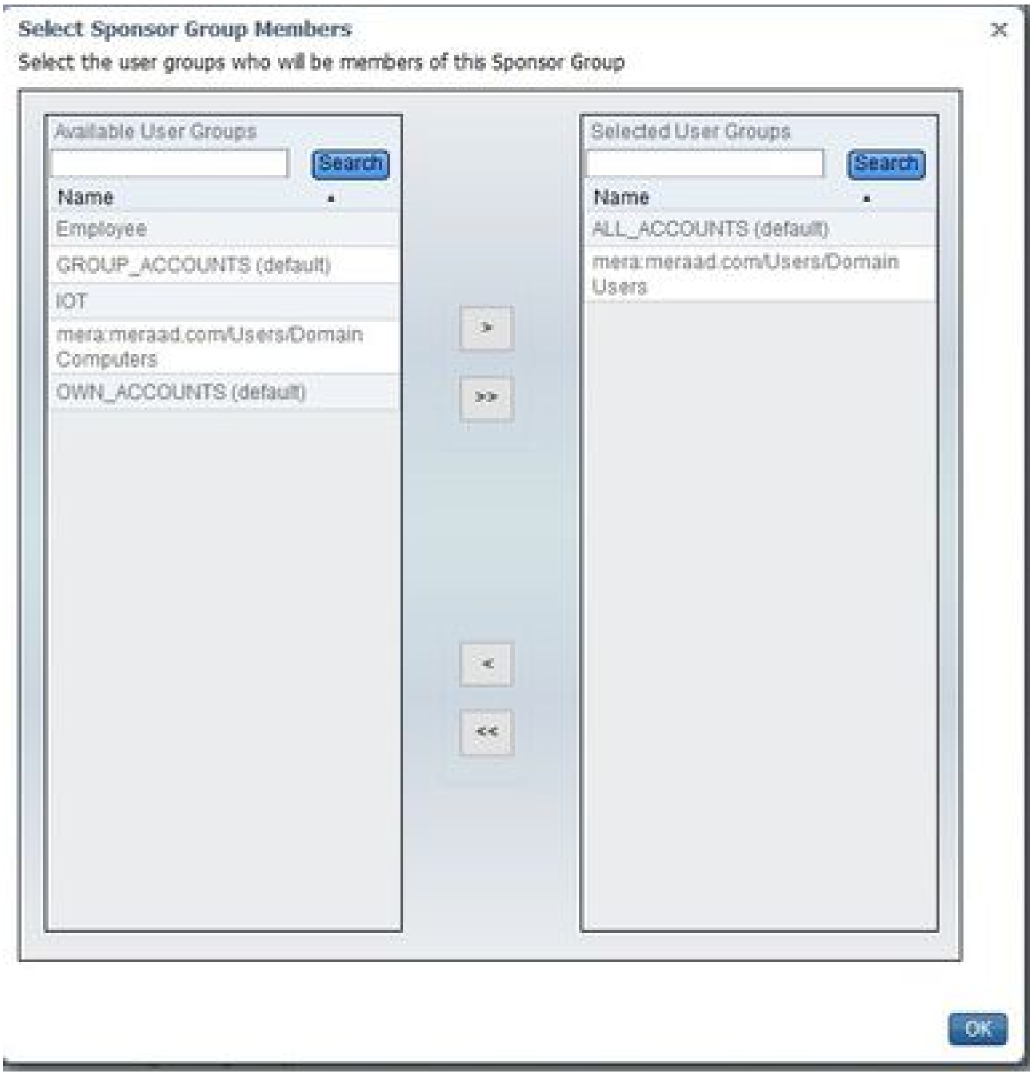
Description: Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group

Match Criteria

Member Groups - Sponsor must belong to at least one of the selected groups.

ALL_ACCOUNTS (default)

The Members show all the available groups to choose from; select the AD group and move it to the right to add it to the sponsor group.



Select Sponsor Group Members

Select the user groups who will be members of this Sponsor Group

Available User Groups
Name
Employee
GROUP_ACCOUNTS (default)
IOT
mera:meraad.com/Users/Domain Computers
OWN_ACCOUNTS (default)

Selected User Groups
Name
ALL_ACCOUNTS (default)
mera:meraad.com/Users/Domain Users

Save the changes. Sponsor portal login now works with AD user accounts that are part of the selected AD group.

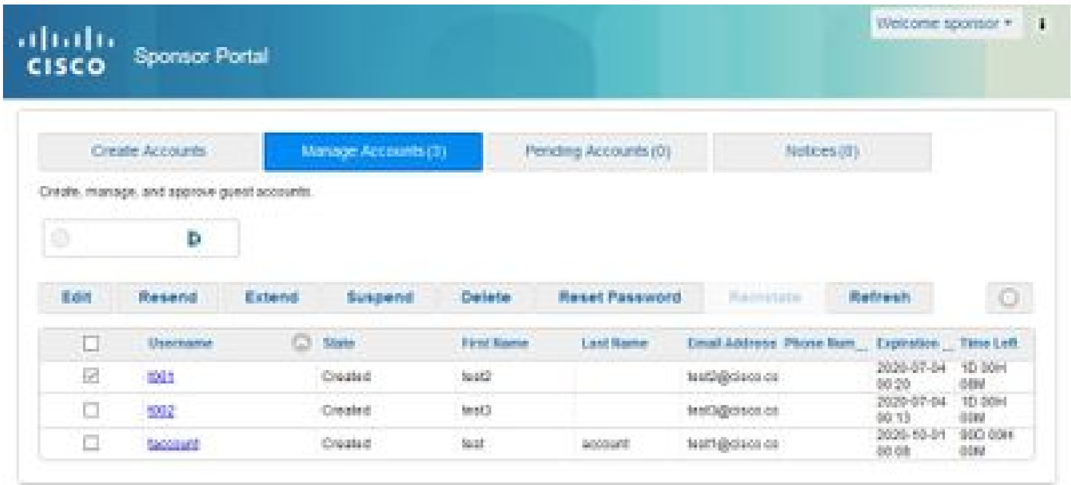
The same steps above can be followed to add users via LDAP. Internally defined user identity groups are also available as an option to add to sponsor groups.

Use one such sponsor account to login to sponsor portal. The sponsor portal can be used to:

- Edit and delete guest accounts
- Extend guest account duration
- Suspend guest account

- Reinstate expired guest accounts
- Resend and reset passwords for guests
- Approve pending guest accounts

On the sponsor portal, select the **Manage Accounts** tab to see all the guest accounts that this sponsor is authorized to manage, as shown in this image.



Create, manage, and approve guest accounts.

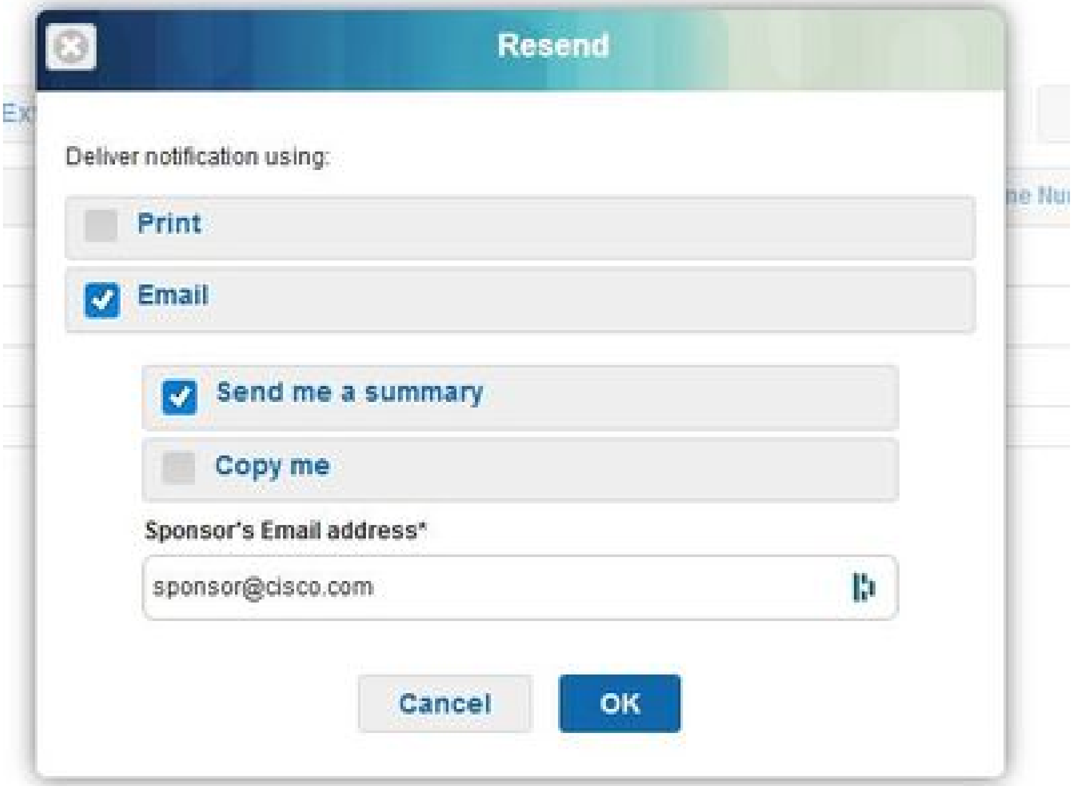
□	Username	State	First Name	Last Name	Email Address	Phone Num...	Expiration	Time Left
☑	t001	Created	test2		test2@cisco.co		2020-07-04 00:20	1D 00H 08M
□	t002	Created	test3		test3@cisco.co		2020-07-04 00:13	1D 00H 00M
□	taccount	Created	test	account	test1@cisco.co		2020-10-01 00:08	90D 00H 00M

A guest account can be edited regardless of the state that they are in.

There is an option to resend the guest account password in case the account holder forgets or loses them. A guest account's password can only be resent if they are either in **Active** or **Created** state.

Passwords cannot be resent for guests who have changed them. For that case, the reset password option must be used first. Password cannot be sent for accounts that are pending approval, suspended, expired or denied.

A sponsor may choose the option to receive a copy of the changed password:



Deliver notification using:

□ Print

☑ Email

☑ Send me a summary

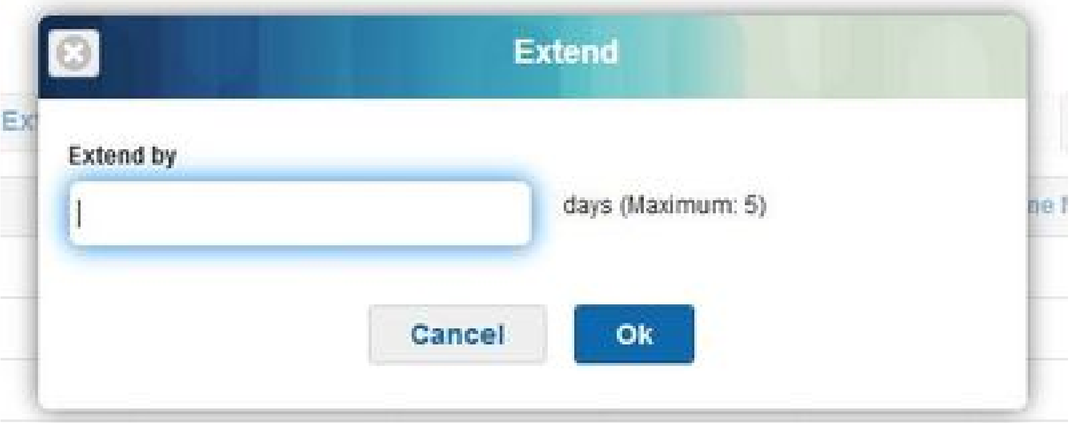
□ Copy me

Sponsor's Email address*

sponsor@cisco.com

In case there is a need to allow guest access to the network for a period longer than originally permitted, use the extended option to increase duration. Accounts in Created, Active or Expired state can be extended.

An account that has been suspended or denied, cannot be extended; use the reinstate option instead.

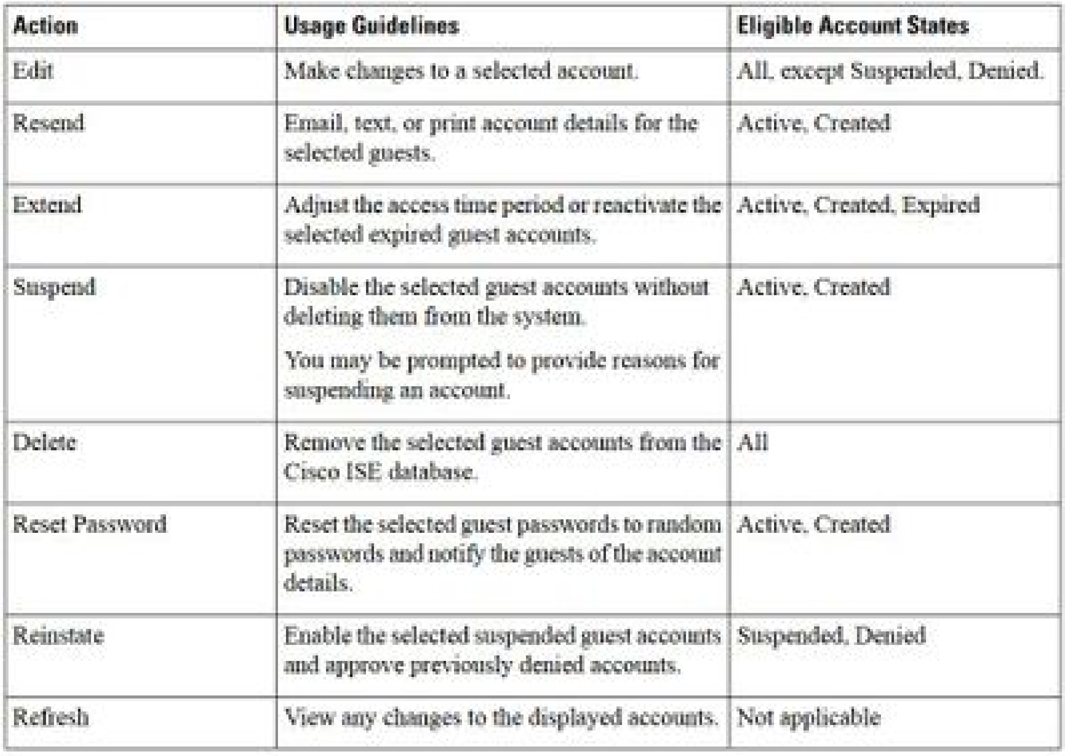


Extend by

days (Maximum: 5)

The maximum allowed extension period is governed by the account's guest type.

Guest accounts expire on their own when they reach the end of account duration, regardless of their state. Suspended or expired guest accounts are automatically purged based on purge policy defined on the system. By default, they are purged every 15 days.



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

Guest account states and their meaning:

Active: Guests with these accounts have successfully signed in through a credentialed Guest portal, or bypassed the credentialed Guest captive portal. In the latter case, the accounts belong to guest types that are configured to bypass the credentialed Guest captive portal. These guests can access the network by providing their login credentials to the native supplicant on their device.

Created: The accounts have been created, but the guests have not yet logged in to a credentialed

Guest portal. In this case, the accounts are assigned to guest types that are not configured to bypass the credentialed Guest captive portal. Guests must first sign in through the credentialed Guest captive portal before they are able to access other parts of the network.

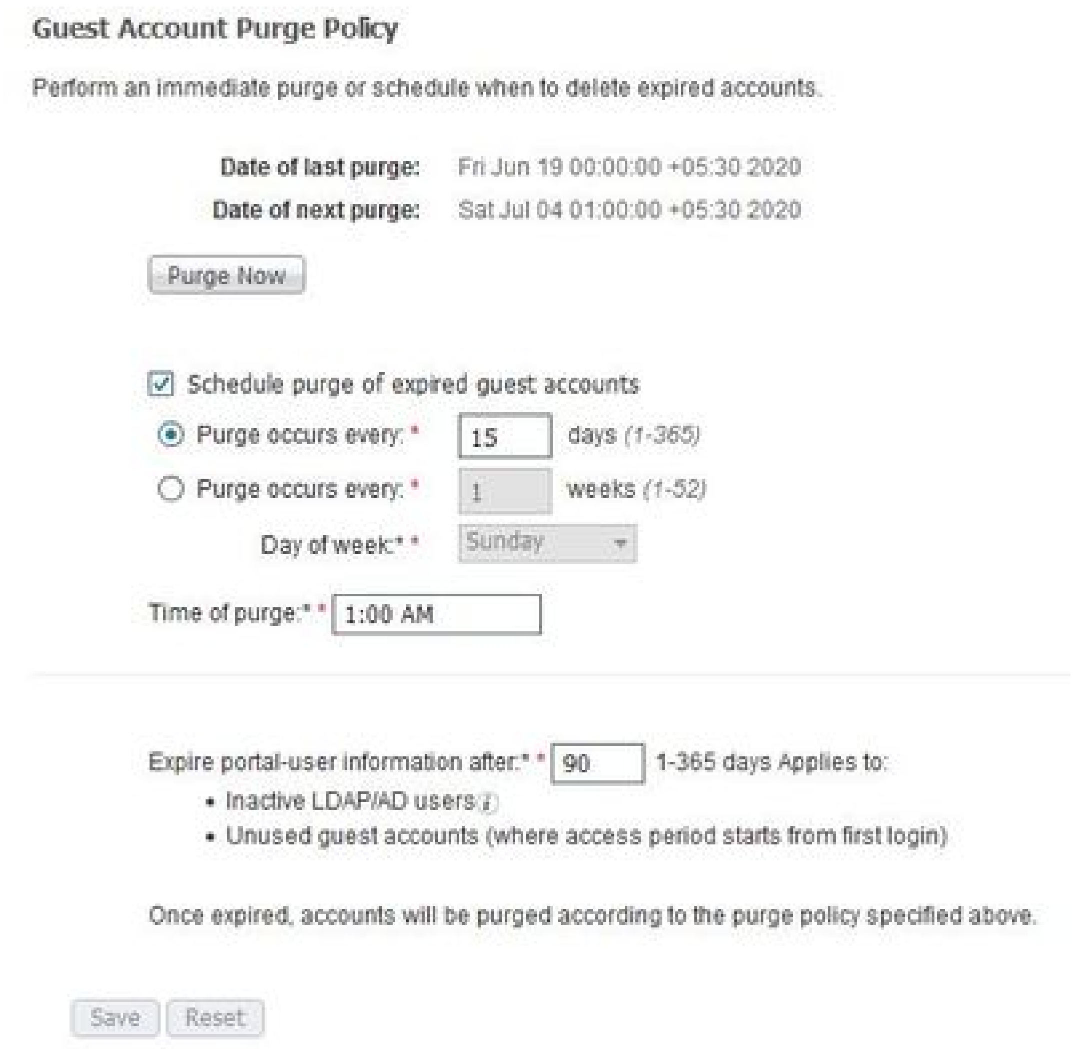
Denied: The accounts are denied access to the network. Accounts that expired while in a denied state remain as denied.

Pending Approval: The accounts are awaiting approval to access the network.

Suspended: The accounts are suspended by a sponsor who has the privilege to do so.

Guest Purge Policies

By default, ISE automatically purges expired guest accounts every 15 days. This information can be seen under **Work Centers > Guest Access > Settings > Guest Account Purge Policy**.



Guest Account Purge Policy

Perform an immediate purge or schedule when to delete expired accounts.

Date of last purge: Fri Jun 19 00:00:00 +05:30 2020
Date of next purge: Sat Jul 04 01:00:00 +05:30 2020

☑ Schedule purge of expired guest accounts
● Purge occurs every: * 15 days (1-365)
○ Purge occurs every: * 1 weeks (1-52)
Day of week:* * Sunday
Time of purge:* * 1:00 AM

Expire portal-user information after:* * 90 1-365 days Applies to:
- Inactive LDAP/AD users
- Unused guest accounts (where access period starts from first login)

Once expired, accounts will be purged according to the purge policy specified above.

Date of Next Purge indicates when the next purge will occur. The ISE administrator can:

- Schedule a purge to occur every X days. The **Time of Purge** specifies when the first purge happens in X days. After that, the purge occurs every X days.
- Schedule a purge on a given day of the week, every X weeks.
- Force an on-demand purge using the option **Purge Now.**

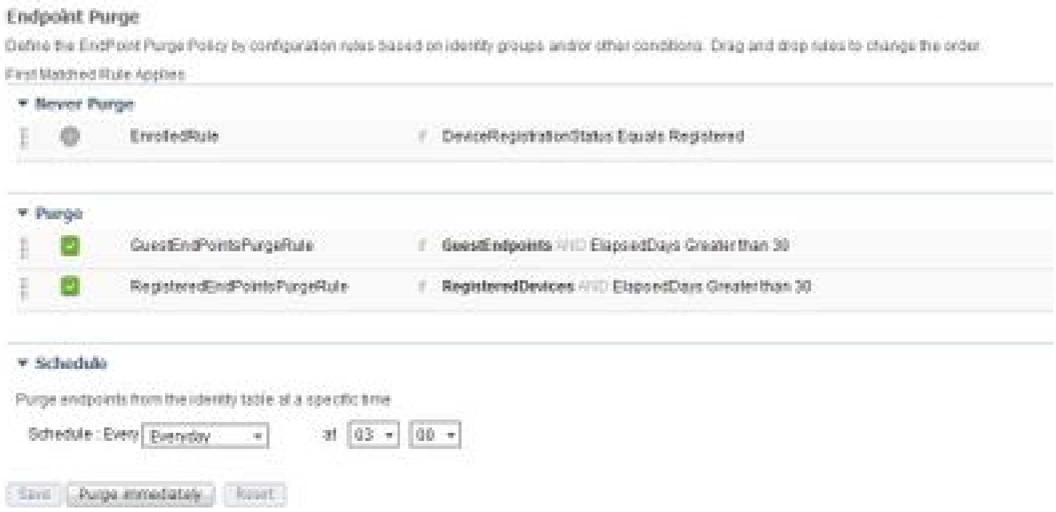
When expired guest accounts are purged, the associated endpoints, reporting, and logging information are retained.

Endpoint Purge: Inactive Days vs Elapsed Days for Endpoints

The endpoints that guests use to access the network become the part of GuestEndpoints by default. ISE has the policy to delete Guest endpoints and registered devices that are older than 30 days. This default purge job runs at 1 AM every day based on the time zone configured on the Primary Admin Node (PAN). This default policy uses the condition of **ElapsedDays**. Other options available are **InactiveDays** and **PurgeDate**.

> **Note**: Endpoint Purge functionality is independent of Guest Account Purge Policy and Guest Account Expiration.

Policy is defined under **Administration > Identity Management > Settings > Endpoint Purge**.



Endpoint Purge

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▾ Never Purge

EnrolledRule   if   DeviceRegistrationStatus Equals Registered

▾ Purge

☑ GuestEndPointsPurgeRule   if   **GuestEndpoints** AND ElapsedDays Greater than 30

☑ RegisteredEndPointsPurgeRule   if   **RegisteredDevices** AND ElapsedDays Greater than 30

▾ Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every Everyday at 03 00

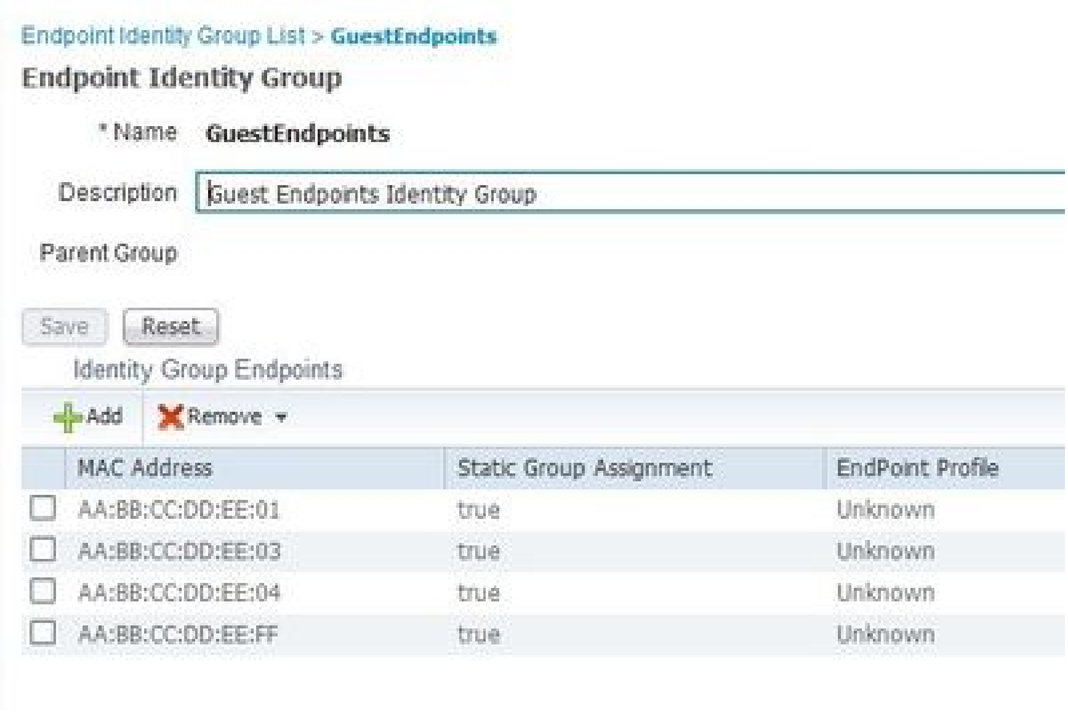
Elapsed Days: This refers to the number of days since the object was created. This condition can be used for endpoints that have been granted unauthenticated or conditional access for a set time period, such as a guest or contractor endpoint, or employees leveraging webauth for network access. After the allowed connect grace period, they must be fully reauthenticated and registered.

Inactive Days: Refers to the number of days since the last profiling activity or update on the endpoint. This condition purges stale devices that have accumulated over time, commonly transient guests or personal devices, or retired devices. These endpoints tend to represent noise in most deployments as they are no longer active on the network or likely to be seen in the near future. If they do happen to connect again, then they will be rediscovered, profiled, registered, etc as needed.

When there are updates from the endpoint, InactivityDays will be reset to 0 only if profiling is enabled.

Purge Date: Date to purge the endpoint. This option can be used for special events or groups where access is granted for a specific time, regardless of creation or start time. This allows all endpoints to be purged at the same time. For example, a trade show, a conference, or a weekly training class with new members each week, where access is granted for a specific week or month rather than absolute days/weeks/months.

This sample profiler.log file shows when endpoints which were part of GuestEndpoints and had elapsed 30 days were purged:



Endpoint Identity Group List > GuestEndpoints

Endpoint Identity Group

* Name GuestEndpoints

Description Guest Endpoints Identity Group

Parent Group

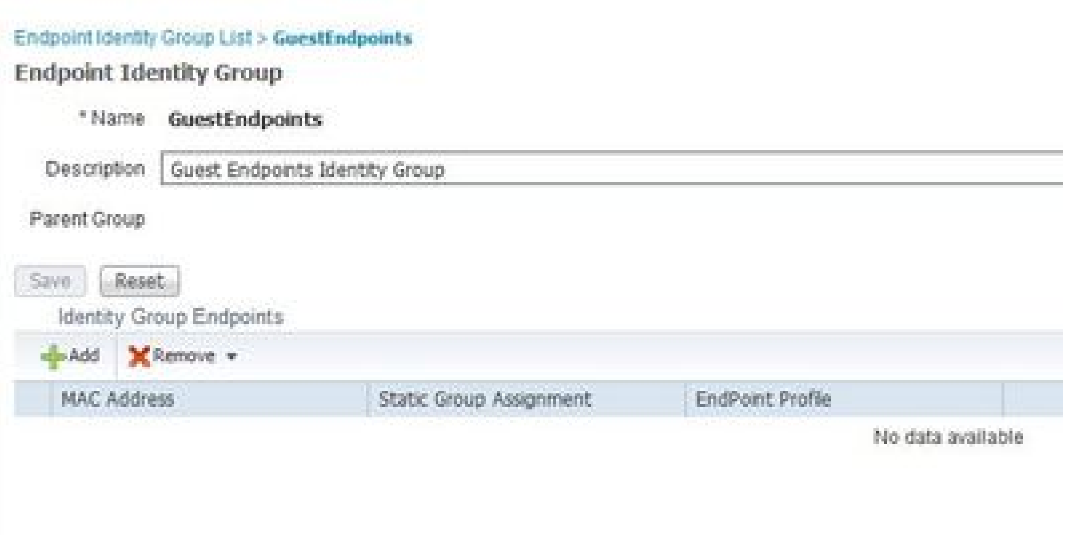
	MAC Address	Static Group Assignment	EndPoint Profile
□	AA:BB:CC:DD:EE:01	true	Unknown
□	AA:BB:CC:DD:EE:03	true	Unknown
□	AA:BB:CC:DD:EE:04	true	Unknown
□	AA:BB:CC:DD:EE:FF	true	Unknown

```
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
```

```
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
```

After the purge is complete:



Endpoint Identity Group List > GuestEndpoints

Endpoint Identity Group

* Name GuestEndpoints

Description Guest Endpoints Identity Group

Parent Group

Save Reset

Identity Group Endpoints

Add Remove

MAC Address	Static Group Assignment	EndPoint Profile

No data available

Troubleshoot Guest and Purge Issues

In order to capture logs related to guest and purge issues, these components can be set to debug. To enable debugs, navigate to **Administration> System > Debug Log Configuration> Select node**.

For guest/sponsor accounts and endpoint purge related troubleshooting, set these components to debug:

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

For portal related issues set these components to debug:

- sponsorportal
- portal
- portal-session-manager
- guestaccess

Related Information

- **ISE Guest Access Prescriptive Deployment Guide**
- **Troubleshoot and Enable Debugs on ISE**