ISE Gastkontenmanagement

Einführung

In diesem Dokument werden die häufig verwendeten Aktionen beschrieben, die ein Sponsor oder ein ISE-Administrator in Bezug auf Gastdaten in der ISE durchführen kann. Die Cisco Identity Services Engine (ISE)-Gastservices bieten sicheren Netzwerkzugriff für Gäste wie Besucher, Auftragnehmer, Berater und Kunden.

Unterstützt von Shivam Kumar, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über die folgenden Themen zu verfügen:

- ISE
- ISE-Gastservices

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ISE, Version 2.6

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

> **Hinweis**: Die Vorgehensweise ist für andere ISE-Versionen ähnlich oder identisch. Sofern nicht anders angegeben, können Sie diese Schritte für alle 2.x ISE-Softwareversionen ausführen.

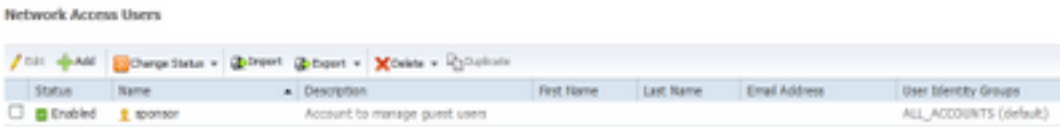
Konfigurieren

Verwenden eines Sponsors zum Verwalten von Gastkonten

Sponsoren sind Benutzerkonten auf der ISE, die die Berechtigung haben, sich beim Sponsorportal anzumelden, wo sie temporäre Gastkonten für autorisierte Besucher erstellen und verwalten können. Ein Sponsor kann ein interner Benutzer oder ein Konto sein, das in einem externen Identitätsspeicher wie einem Active Directory vorhanden ist.

In diesem Beispiel wird das Sponsor-Konto intern auf der ISE definiert und der vordefinierten

Gruppe hinzugefügt: ALL_ACCOUNTS.



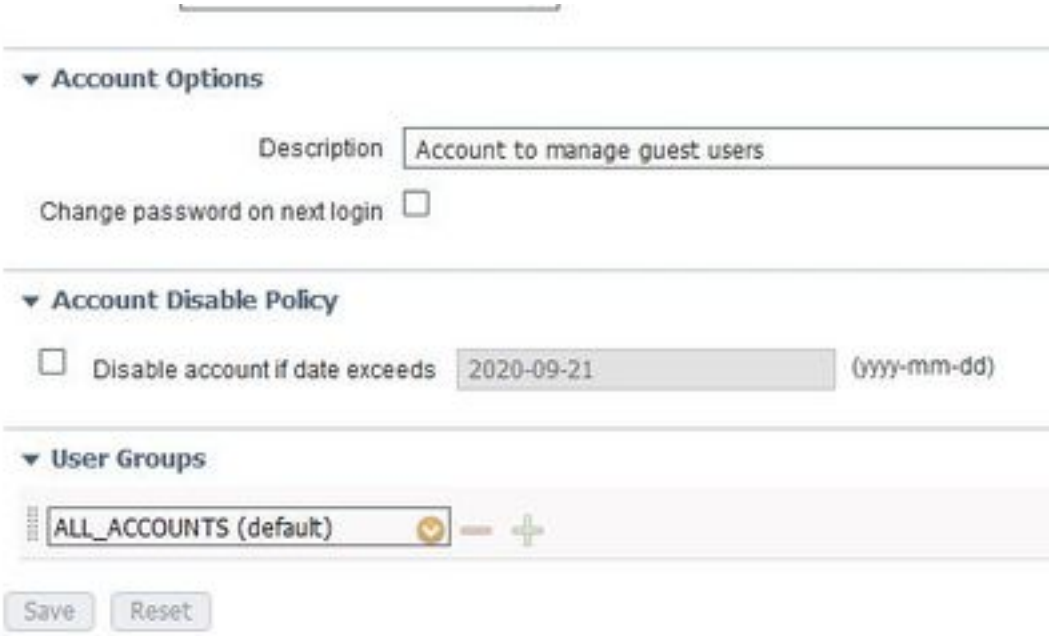
Standardmäßig verfügt die ISE über drei Sponsorengruppen, die den folgenden Personen zugeordnet werden können:

ALL_ACCOUNTS (Standard): Die dieser Gruppe zugewiesenen Sponsoren können alle Gastbenutzerkonten verwalten. Standardmäßig sind Benutzer in der Benutzeridentitätsgruppe ALL_ACCOUNTS Mitglieder dieser Sponsorengruppe.

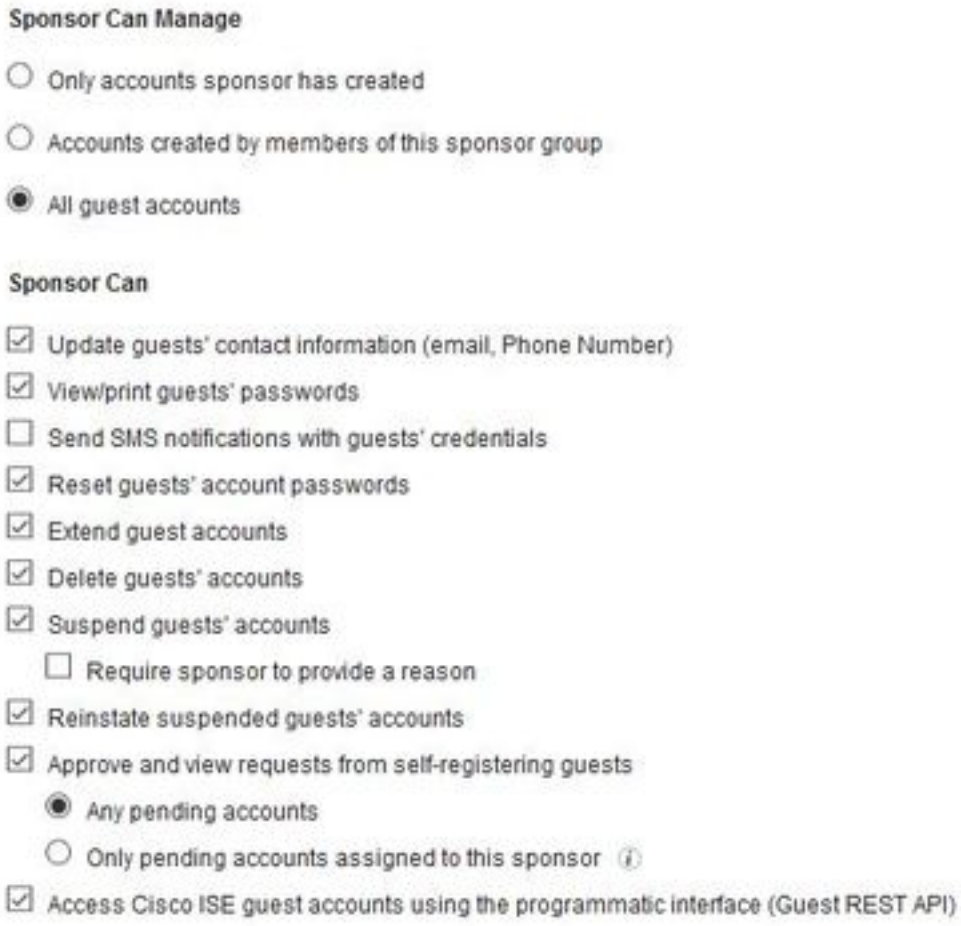
GROUP_ACCOUNTS (Standard): Sponsoren, die dieser Gruppe zugewiesen sind, können nur die Gastkonten verwalten, die von Sponsoren derselben Sponsorengruppe erstellt wurden. Standardmäßig sind Benutzer in der Benutzeridentitätsgruppe GROUP_ACCOUNTS Mitglieder dieser Sponsorengruppe.

OWN_ACCOUNTS (Standard): Sponsoren, die dieser Gruppe zugewiesen sind, können nur die von ihnen erstellten Gastkonten verwalten. Standardmäßig sind Benutzer in der Benutzeridentitätsgruppe OWN_ACCOUNTS Mitglieder dieser Sponsorgruppe.

Das in diesem Beispiel verwendete Sponsorkonto ist ALL_ACCOUNTS zugeordnet:



Die Berechtigungen und Berechtigungen dieser Sponsor-Gruppe sind unter **Work Center > Guest Access > Portal & Components > Sponsor Groups** verfügbar:



Um einem Sponsor den Zugriff auf die Gastverwaltung über ERS REST API zu ermöglichen, wird die Berechtigung in der Gruppe des Sponsors hinzugefügt, wie im Bild gezeigt.

Active Directory-Konto als Programmpate verwenden

Neben internen Benutzerkonten, die als Sponsoren definiert sind, können auch Konten, die auf externen Identitätsquellen wie Active Directory (AD) oder LDAP vorhanden sind, als Sponsor für

die Verwaltung von Gastkonten verwendet werden.

Stellen Sie sicher, dass die ISE AD zugeordnet ist, indem Sie zu **Administration > Identities > External Identity Sources > Active Directory** navigieren. Wenn Sie noch nicht Mitglied sind, treten Sie einer der verfügbaren AD-Domänen bei.

Rufen Sie die Gruppen aus AD ab, die die Konten enthalten:

In diesem Beispiel wird das Hinzufügen eines AD-Benutzers zur ALL_ACCOUNTS-Sponsorengruppe veranschaulicht.

Navigieren Sie zu **Work Center > Guest Access > Portal & Components > Sponsor Groups> ALL_ACCOUNTS** und klicken Sie dann auf **Members** (Mitglieder), wie in diesem Bild gezeigt.

Die Mitglieder zeigen alle verfügbaren Gruppen, aus denen sie auswählen können. Wählen Sie die AD-Gruppe aus, und verschieben Sie sie nach rechts, um sie der Sponsorengruppe hinzuzufügen.

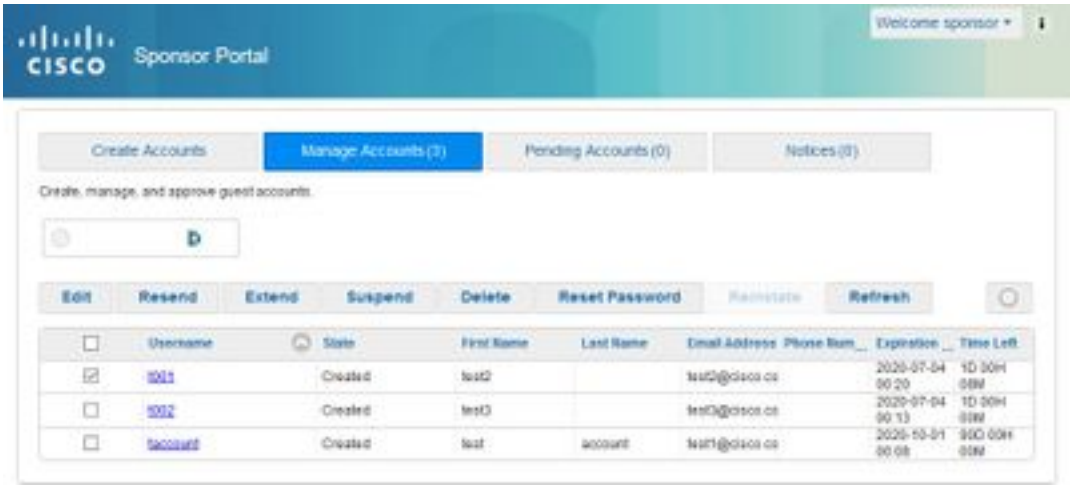
Speichern Sie die Änderungen. Die Anmeldung beim Sponsor-Portal funktioniert jetzt mit AD-Benutzerkonten, die zur ausgewählten AD-Gruppe gehören.

Zum Hinzufügen von Benutzern über LDAP können die oben beschriebenen Schritte ausgeführt werden. Interne Benutzeridentitätsgruppen sind auch als Option zum Hinzufügen zu Sponsorgruppen verfügbar.

Verwenden Sie ein solches Sponsorkonto, um sich beim Sponsorportal anzumelden. Das Sponsorportal kann verwendet werden, um:

- Bearbeiten und Löschen von Gastkonten
- Verlängerung der Dauer von Gastkonten
- Gastkonto aussetzen
- Abgelaufene Gastkonten wieder einrichten
- Kennwörter für Gäste erneut senden und zurücksetzen
- Genehmigen ausstehender Gastkonten

Wählen Sie im Sponsorportal die Registerkarte **Konten verwalten** aus, um alle Gastkonten anzuzeigen, die dieser Sponsor verwalten darf, wie in diesem Bild gezeigt.

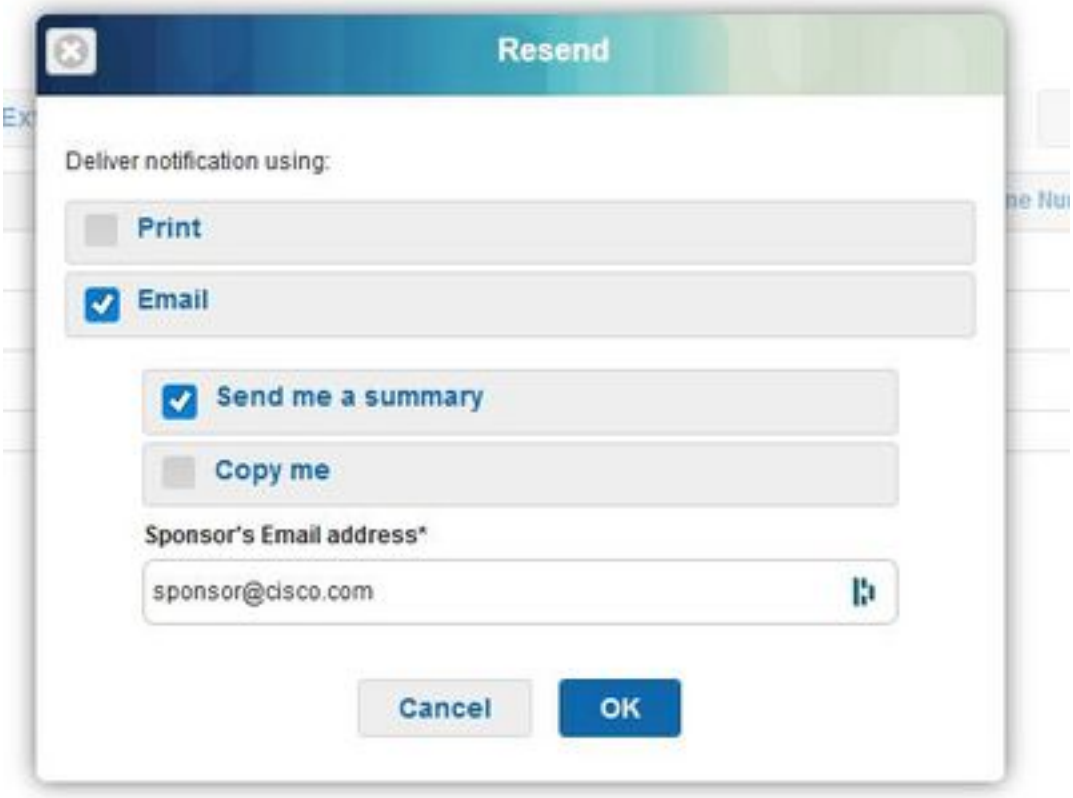


Ein Gastkonto kann unabhängig vom Status bearbeitet werden.

Es besteht die Möglichkeit, das Kennwort des Gastkontos erneut zu senden, falls der Kontoinhaber es vergisst oder verliert. Das Kennwort eines Gastkontos kann nur dann erneut gesendet werden, wenn es sich entweder im Status **Aktiv** oder **Erstellt** befindet.

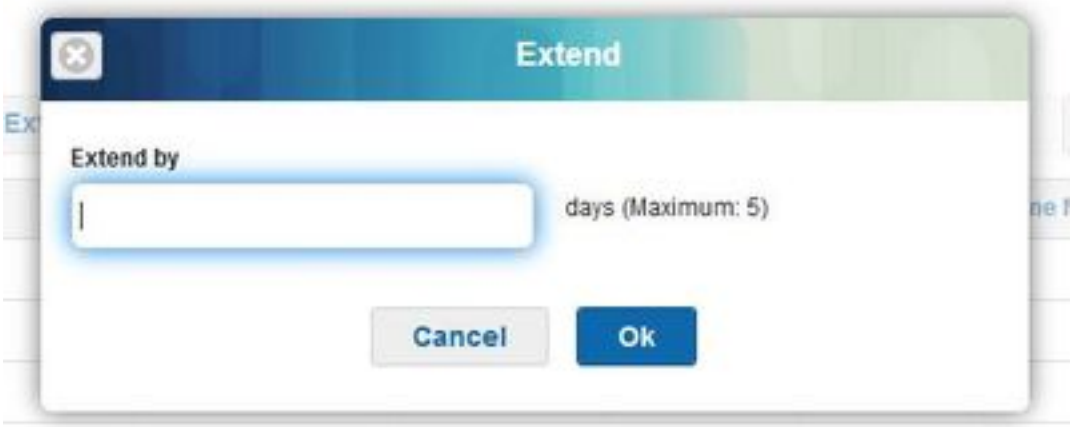
Passwörter können nicht an Gäste gesendet werden, die sie geändert haben. In diesem Fall muss zuerst die Kennwortrücksetzoption verwendet werden. Für Konten, die noch nicht genehmigt, ausgesetzt, abgelaufen oder abgelehnt wurden, kann kein Kennwort gesendet werden.

Ein Sponsor kann die Option wählen, eine Kopie des geänderten Kennworts zu erhalten:



Falls der Gastzugriff auf das Netzwerk für einen längeren Zeitraum als ursprünglich zulässig zugelassen zugelassen werden muss, können Sie die verlängerte Option verwenden, um die Dauer zu erhöhen. Konten im Status "Erstellt", "Aktiv" oder "Abgelaufen" können erweitert werden.

Ein Konto, das ausgesetzt oder verweigert wurde, kann nicht verlängert werden. verwenden Sie stattdessen die Option zum Wiederherstellen.



Der maximal zulässige Verlängerungszeitraum richtet sich nach dem Gasttyp des Kontos.

Gastkonten verfallen auf eigene Faust, wenn sie das Ende des Kontos erreichen, unabhängig von ihrem Status. Ausgesetzte oder abgelaufene Gastkonten werden gemäß einer im System definierten Richtlinie zum Löschen des Kontos automatisch gelöscht. Standardmäßig werden sie alle 15 Tage gelöscht.

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

Gastkontenstatus und deren Bedeutung:

Aktiv: Gäste mit diesen Konten haben sich erfolgreich über ein als "Credential Guest Portal" (Portal für berechtigte Gäste) angemeldet oder das als "Guest Captive" bezeichnete Portal umgangen. Im letzteren Fall gehören die Konten zu Gasttypen, die so konfiguriert sind, dass sie das als "Guest Captive" bezeichnete Portal umgehen. Diese Gäste können auf das Netzwerk zugreifen, indem sie ihre Anmeldedaten der nativen Komponente auf ihrem Gerät übermitteln.

Erstellt: Die Konten wurden erstellt, aber die Gäste haben sich noch nicht bei einem als "Credential Guest Portal" bezeichneten Gastportal angemeldet. In diesem Fall werden die Konten Gasttypen zugewiesen, die nicht so konfiguriert sind, dass sie das als "Guest Captive" bezeichnete Portal umgehen. Die Gäste müssen sich zuerst über das Captive Portal für Gäste anmelden, bevor sie auf andere Teile des Netzwerks zugreifen können.

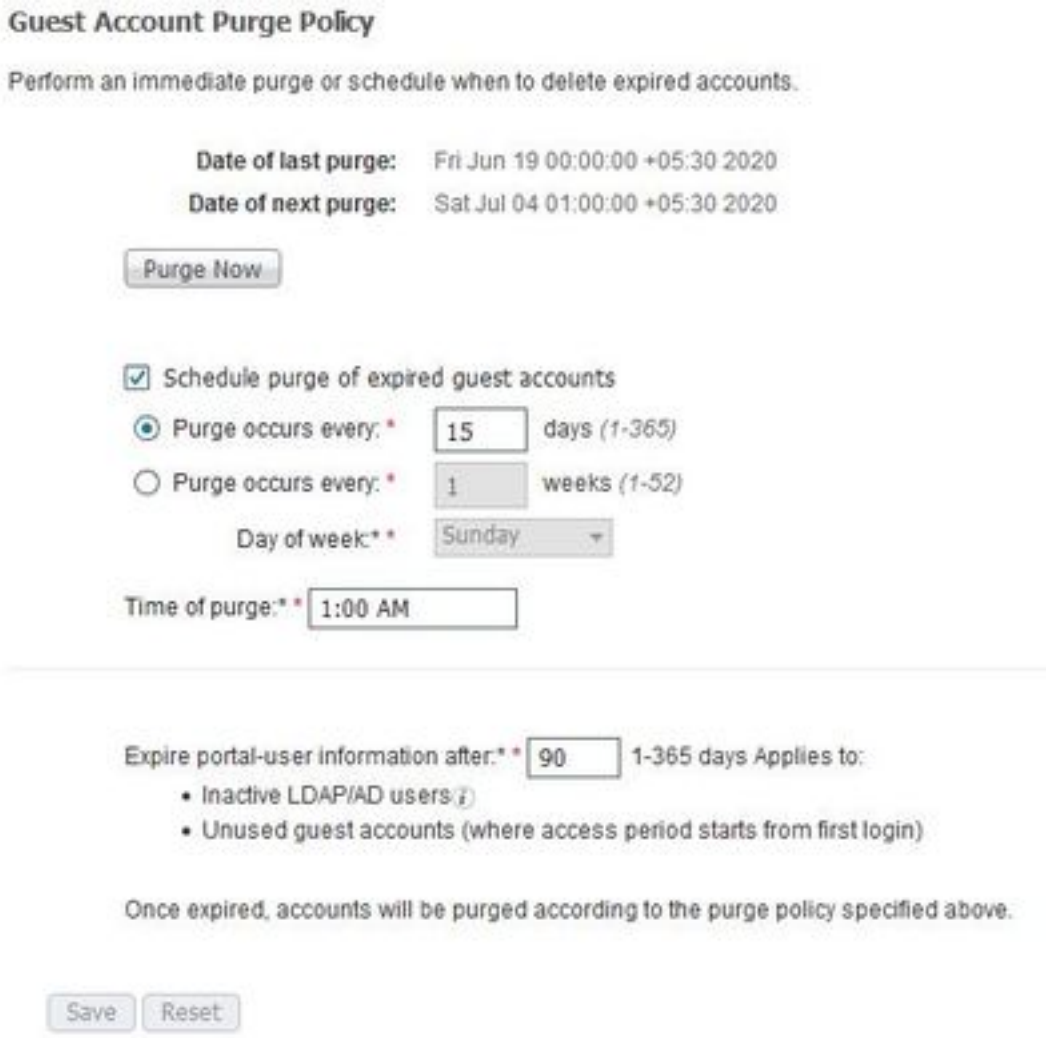
Abgelehnt: Den Konten wird der Zugriff auf das Netzwerk verweigert. Konten, die abgelaufen sind, während sie sich im Status "Abgelehnt" befinden, bleiben abgelehnt.

Zur Genehmigung ausstehend: Die Konten warten auf Genehmigung für den Zugriff auf das Netzwerk.

Ausgesetzt: Die Konten werden von einem Sponsor gesperrt, der dazu berechtigt ist.

Richtlinien für die Löschung von Gastgeräten

Standardmäßig löscht die ISE abgelaufene Gastkonten alle 15 Tage automatisch. Diese Informationen finden Sie unter **Work Centers > Guest Access > Settings > Guest Account Purge Policy**.



Das Datum der nächsten Säuberung gibt an, wann die nächste Säuberung erfolgt. Der ISE-Administrator kann:

- Planen Sie eine Säuberung alle X Tage ein. Der **Zeitpunkt der Löschung** bestimmt, wann die erste Löschung innerhalb von X Tagen erfolgt. Danach erfolgt die Säuberung alle X Tage.
- Planen Sie eine Säuberung an einem bestimmten Wochentag, alle X Wochen.
- Erzwingen Sie eine bedarfsgesteuerte Säuberung mit der Option **Jetzt entfernen.**

Wenn abgelaufene Gastkonten gelöscht werden, werden die zugehörigen Endpunkte, die zugehörigen Berichts- und Protokollierungsinformationen beibehalten.

Zurücksetzen von Endpunkten: Inaktive Tage und vergangene Tage für Endgeräte

Die Endpunkte, die Gäste für den Zugriff auf das Netzwerk verwenden, werden standardmäßig zum Teil von GuestEndpoints. Die ISE hat die Richtlinie, Gast-Endpunkte und registrierte Geräte zu löschen, die älter als 30 Tage sind. Dieser Standard-Bereinigungsauftrag wird täglich um 1 Uhr ausgeführt, basierend auf der Zeitzone, die auf dem primären Admin-Knoten (PAN) konfiguriert wurde. Diese Standardrichtlinie verwendet die Bedingung von **ElapsedDays**. Weitere verfügbare Optionen sind **InactiveDays** und **PurgeDate**.

> **Hinweis**: Die Funktion zum Zurücksetzen von Endpunkten ist unabhängig von der Richtlinie zum Zurücksetzen von Gastkonten und dem Ablauf von Gastkonten.

Die Richtlinie wird unter **Administration > Identity Management > Settings > Endpoint Purge** definiert.

Vergangene Tage: Dies bezieht sich auf die Anzahl der Tage seit der Erstellung des Objekts. Diese Bedingung kann für Endpunkte verwendet werden, die für einen bestimmten Zeitraum nicht authentifiziert oder bedingt zugänglich sind, z. B. ein Gast- oder Auftragnehmer-Endpunkt, oder für Mitarbeiter, die Webauth für den Netzwerkzugriff nutzen. Nach dem zulässigen Verbindungs-Kulanzzeitraum müssen sie vollständig neu authentifiziert und registriert werden.

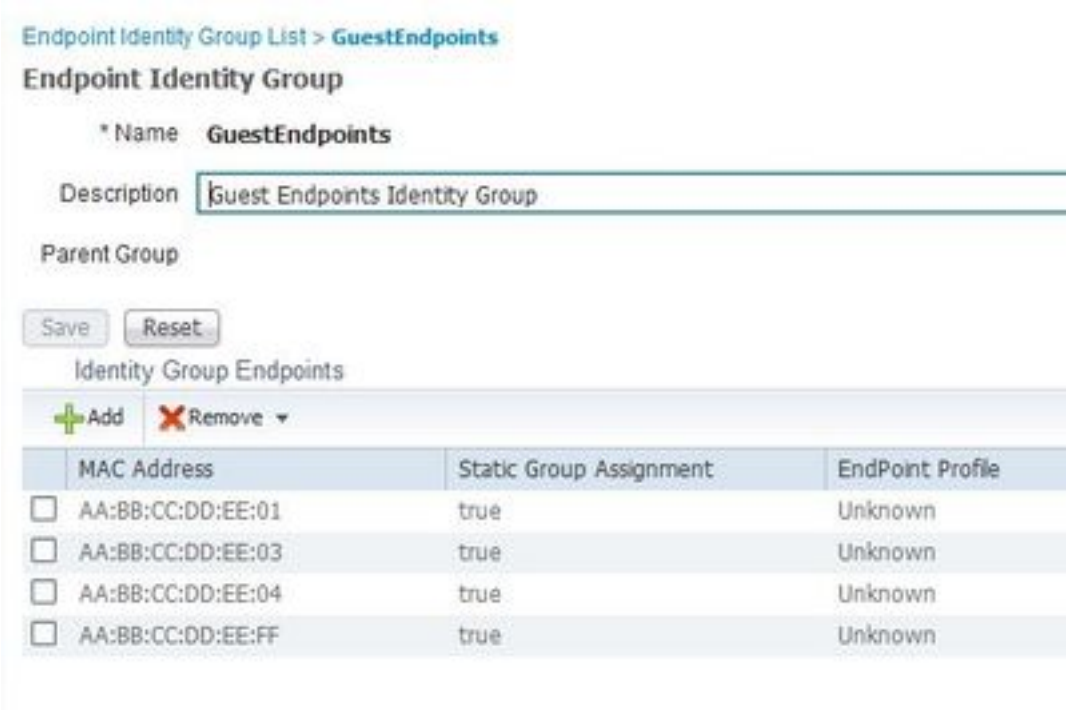
Inaktive Tage: Bezieht sich auf die Anzahl der Tage seit der letzten Profilerstellungsaktivität oder -aktualisierung für den Endpunkt. Bei diesem Zustand werden veraltete Geräte, die sich im Laufe der Zeit angesammelt haben, in der Regel vorübergehend besuchte Gäste oder private Geräte oder Geräte im Ruhestand entfernt. Diese Endgeräte stellen in den meisten Bereitstellungen ein Geräusch dar, da sie nicht mehr im Netzwerk aktiv sind oder in naher Zukunft nicht mehr sichtbar sein werden. Wenn der Kunde erneut eine Verbindung herstellt, wird er nach Bedarf erneut entdeckt, einem Profil zugeordnet, registriert usw.

Wenn Updates vom Endpunkt vorhanden sind, wird InactivityDays nur dann auf 0 zurückgesetzt, wenn die Profilerstellung aktiviert ist.

Löschdatum: Datum zum Löschen des Endpunkts. Diese Option kann für besondere Ereignisse oder Gruppen verwendet werden, bei denen der Zugriff für eine bestimmte Zeit gewährt wird, unabhängig von der Erstellungs- oder Startzeit. Dadurch können alle Endpunkte gleichzeitig gelöscht werden. Beispielsweise eine Messe, eine Konferenz oder eine wöchentliche Schulung mit neuen Mitgliedern pro Woche, bei der der Zugang für eine bestimmte Woche oder einen

bestimmten Monat statt für absolute Tage/Wochen/Monate gewährt wird.

Diese Beispielprofiler.log-Datei zeigt, wann Endpunkte, die Teil von GuestEndpoints waren und 30 Tage verstrichen waren, gelöscht wurden:

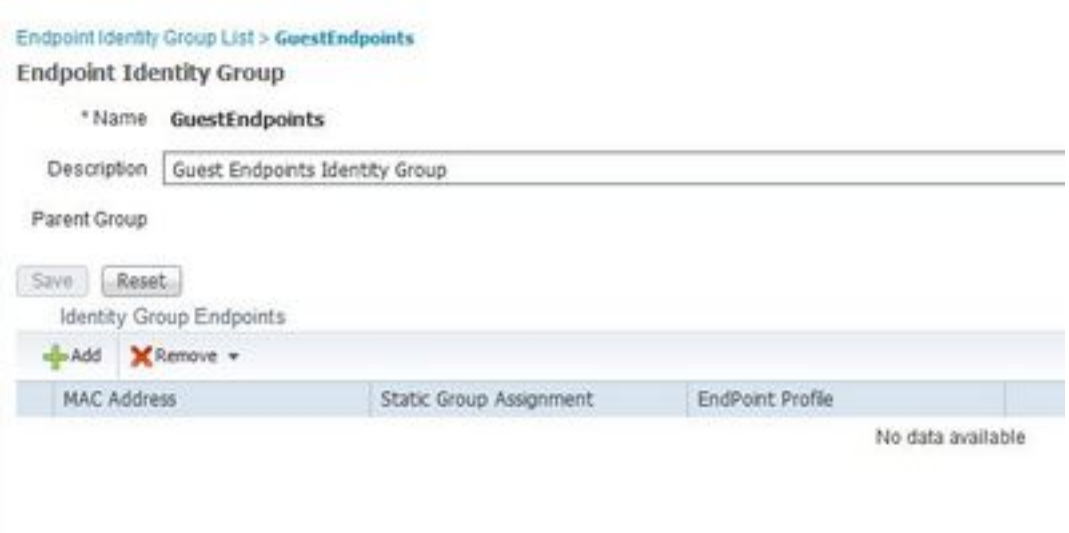



```
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- the rule type is :REGULAR
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- epPurgeRuleID is :3bfaffe0-8c01-
11e6-996c-525400b48521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

Nach Abschluss der Säuberung:



Beheben von Gast- und Löschproblemen

Um Protokolle zu Gast- und Löschproblemen zu erfassen, können diese Komponenten auf Debuggen eingestellt werden. Um das Debuggen zu aktivieren, navigieren Sie zu **Administration > System > Debug Log Configuration > Select node (Verwaltung > System > Debugprotokollkonfiguration > Knoten auswählen)**.

Legen Sie für Gast-/Sponsorkonten und für die Fehlerbehebung bei Endpunktlöschungen folgende Komponenten fest:

- Gastzugriff
- Gast-Administrator
- Gastzugriff-Admin
- Profiler
- Runtime-AAA

Legen Sie bei portalbezogenen Problemen die folgenden Komponenten zum Debuggen fest:

- Sponsorportal
- Portal
- Portal-Session-Manager
- Gastzugriff

Zugehörige Informationen

- ISE Guest Access - Leitfaden zur Bereitstellung
- Fehlerbehebung und Debugging auf der ISE aktivieren