Gerenciamento de contas de convidado do ISE

Introduction

Este documento descreve as ações usadas com frequência que um patrocinador ou um administrador do ISE pode executar nos dados de convidado presentes no ISE. Os serviços de convidados do Cisco Identity Services Engine (ISE) fornecem acesso seguro à rede para convidados, como visitantes, contratados, consultores e clientes.

Contribuído por Shivam Kumar, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- ISE
- Serviços para convidados do ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE, versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

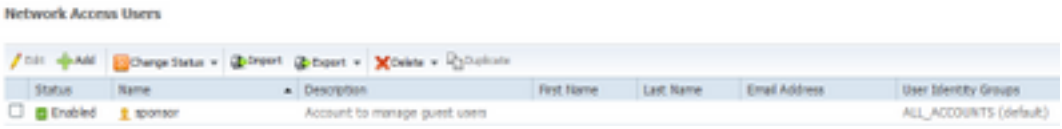
> **Note**: O procedimento é semelhante ou idêntico para outras versões do ISE. É possível usar essas etapas em todas as versões 2.x do software ISE, a menos que declarado de outra forma.

Configurar

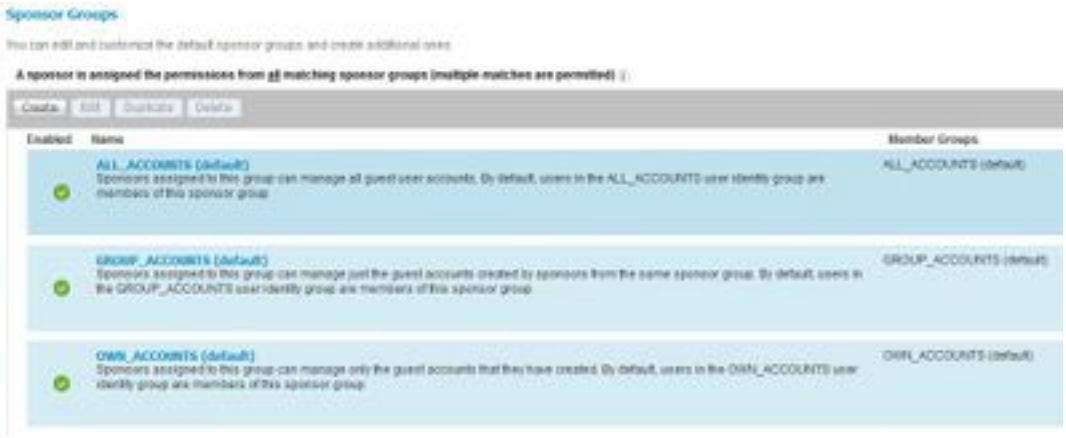
Usar um patrocinador para gerenciar contas de convidado

Os patrocinadores são contas de usuário no ISE que têm o privilégio de fazer login no portal do patrocinador, onde podem criar contas de convidado temporárias para visitantes autorizados e gerenciá-las. Um patrocinador pode ser um usuário interno ou uma conta presente em um repositório de identidade externo, como um diretório ativo.

Neste exemplo, a conta do patrocinador é definida internamente no ISE e adicionada ao grupo predefinido: ALL_ACCOUNTS.



Por padrão, o ISE tem três grupos de patrocinadores para os quais os patrocinadores podem ser mapeados:

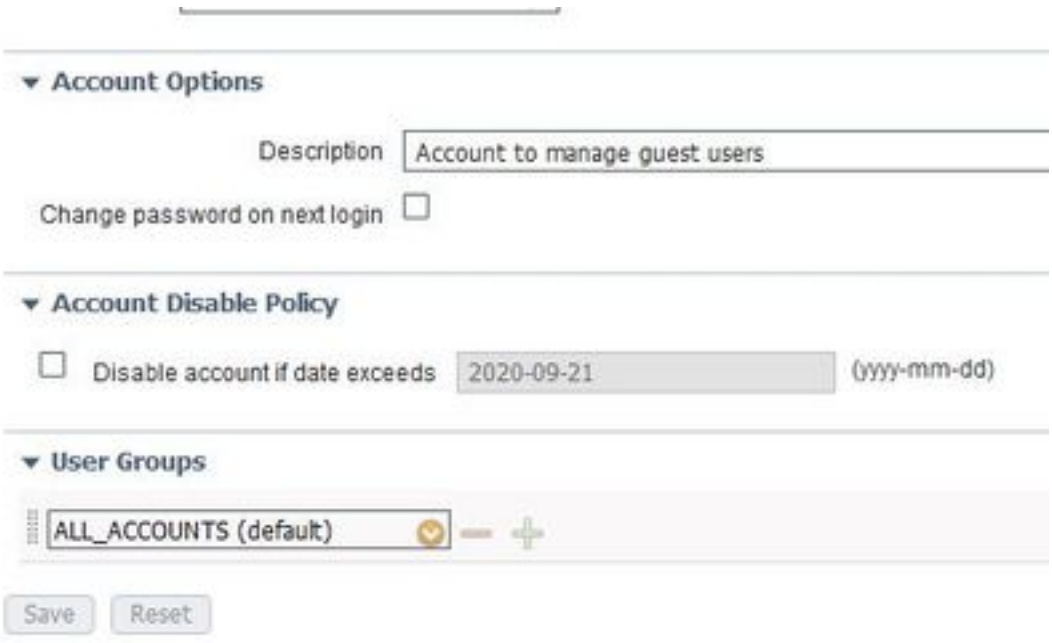


ALL_ACCOUNTS (padrão): os patrocinadores atribuídos a este grupo podem gerenciar todas as contas de usuário convidado. Por padrão, os usuários do grupo de identidade de usuário ALL_ACCOUNTS são membros desse grupo de patrocinadores.

GROUP_ACCOUNTS (padrão): Os patrocinadores atribuídos a este grupo podem gerenciar apenas as contas de convidado criadas por patrocinadores do mesmo grupo de patrocinadores. Por padrão, os usuários do grupo de identidade de usuário GROUP_ACCOUNTS são membros desse grupo de patrocinadores.

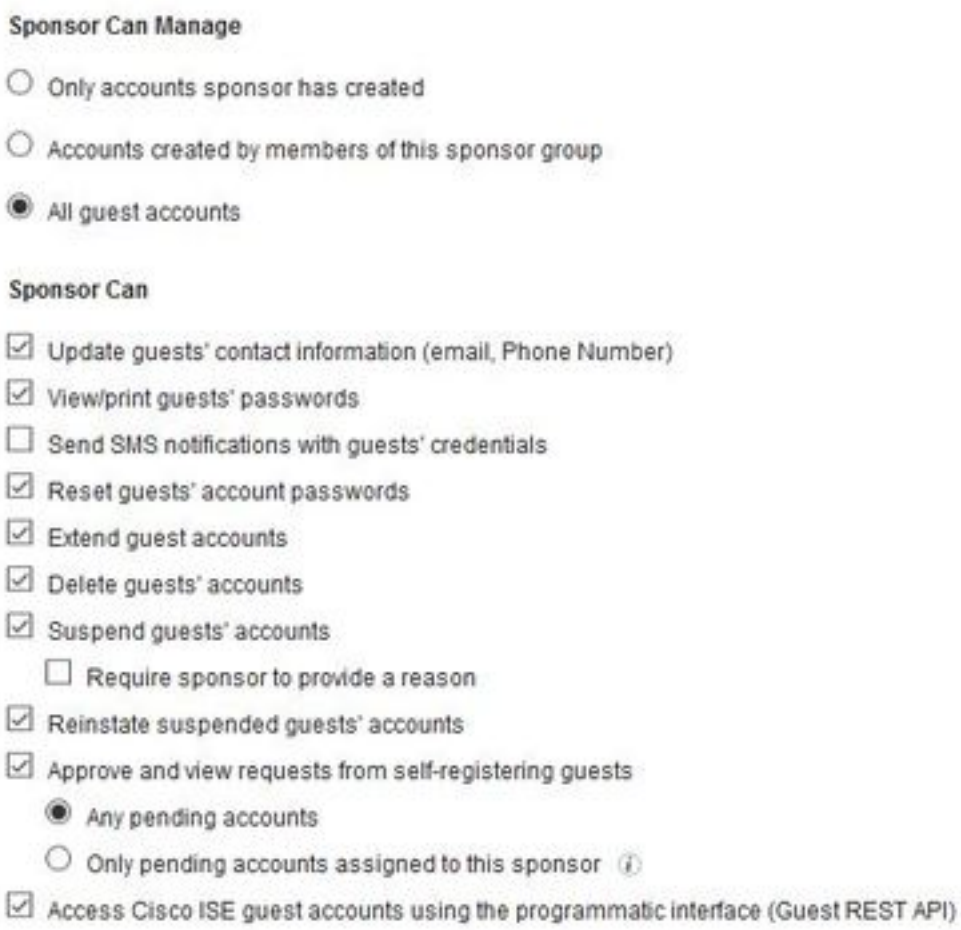
OWN_ACCOUNTS (padrão): os patrocinadores atribuídos a este grupo podem gerenciar somente as contas de convidado que criaram. Por padrão, os usuários do grupo de identidade de usuário OWN_ACCOUNTS são membros desse grupo de patrocinadores.

A conta do patrocinador usada neste exemplo é mapeada para ALL_ACCOUNTS:



As permissões e os privilégios desse grupo de patrocinadores estão disponíveis em **Centros de**

Trabalho> Acesso para Convidado > Portal e Componentes > Grupos de Patrocinadores:



Para permitir que um patrocinador acesse o gerenciamento de convidados via API REST do ERS, a permissão é adicionada ao grupo do patrocinador, como visto na imagem.

Usar conta do Ative Diretory como patrocinador

Juntamente com contas de usuário internas definidas como patrocinadores, contas presentes em fontes de identidade externas como Ative Diretory (AD) ou LDAP também podem ser usadas como patrocinadores para gerenciar contas de convidado.

Certifique-se de que o ISE esteja associado ao AD navegando para **Administração> Identidades > Fontes de identidade externas > Ative Diretory**. Se ainda não tiver ingressado, ingresse em um dos domínios do AD disponíveis.

Recuperar os grupos do AD que contêm as contas:

Este exemplo demonstra a adição de usuário do AD ao grupo de patrocinadores ALL_ACCOUNTS.

Navegue até **Centros de trabalho> Acesso de convidado > Portal & Components > Sponsor Groups> ALL_ACCOUNTS** e clique em **Member**, como mostrado nesta imagem.

Os membros mostram todos os grupos disponíveis a escolher; selecione o grupo do AD e mova-o para a direita para adicioná-lo ao grupo de patrocinadores.

Salve as alterações. O login do portal do patrocinador agora funciona com contas de usuário do AD que fazem parte do grupo do AD selecionado.

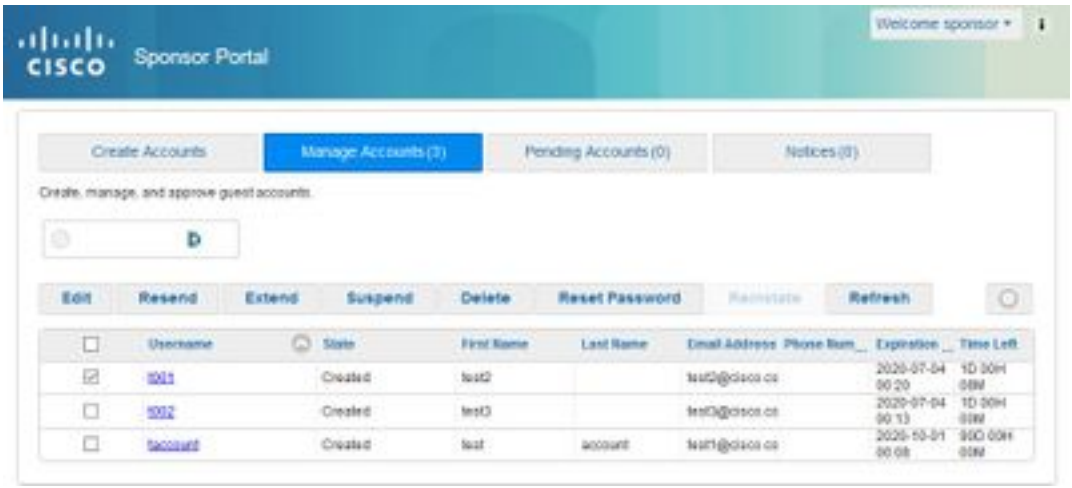
As mesmas etapas acima podem ser seguidas para adicionar usuários via LDAP. Grupos de identidade de usuário definidos internamente também estão disponíveis como uma opção a ser adicionada a grupos de patrocinadores.

Use uma conta desse patrocinador para fazer login no portal do patrocinador. O portal do patrocinador pode ser usado para:

- Editar e excluir contas de convidado

- Estender a duração da conta de convidado
- Suspender conta de convidado
- Reintegrar contas de convidado expiradas
- Reenviar e redefinir senhas para convidados
- Aprovar contas de convidado pendentes

No portal do patrocinador, selecione a guia **Gerenciar contas** para ver todas as contas de convidado que este patrocinador está autorizado a gerenciar, como mostrado nesta imagem.

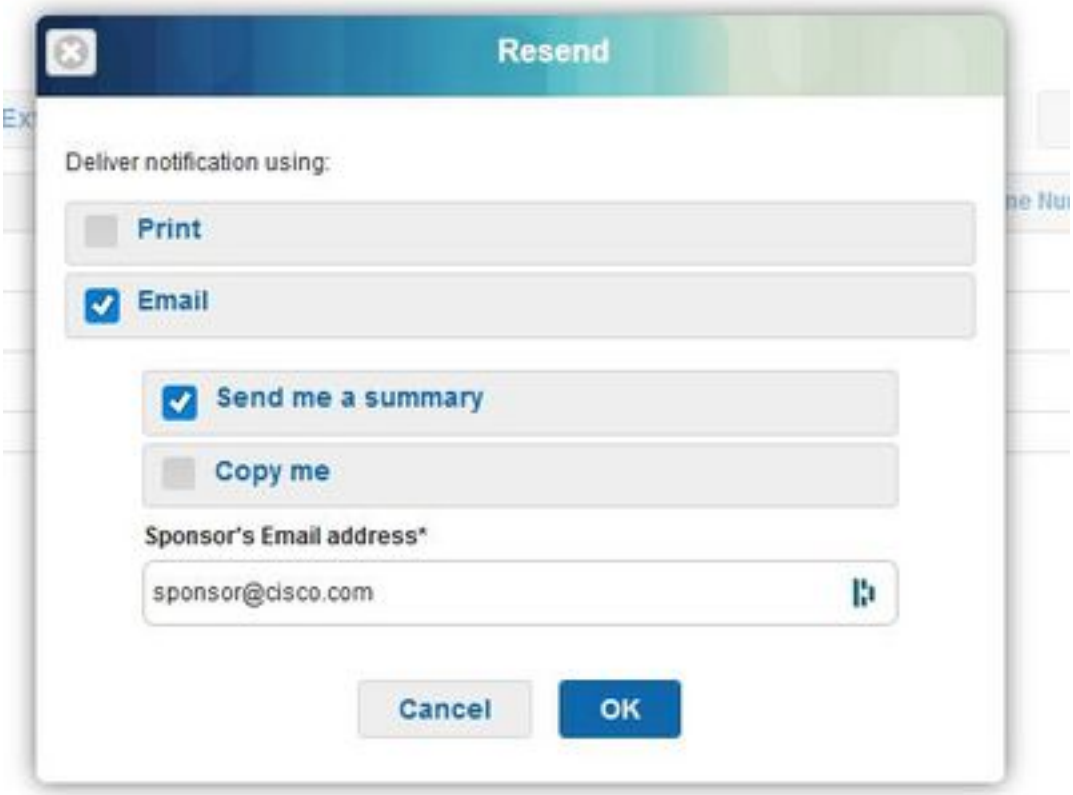


Uma conta de convidado pode ser editada independentemente do estado em que está.

Há uma opção para reenviar a senha da conta de convidado caso o titular da conta a esqueça ou perca. A senha de uma conta de convidado só pode ser enviada novamente se estiver no estado **Ativo** ou **Criado**.

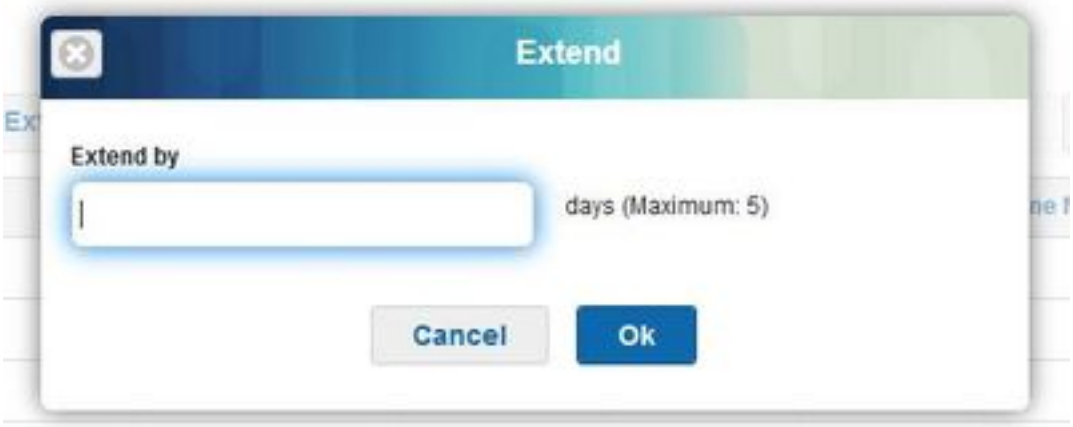
As senhas não podem ser enviadas para convidados que as alteraram. Nesse caso, a opção de redefinição de senha deve ser usada primeiro. A senha não pode ser enviada para contas com aprovação pendente, suspensas, expiradas ou negadas.

Um patrocinador pode escolher a opção de receber uma cópia da senha alterada:



Caso haja necessidade de permitir o acesso de convidado à rede por um período maior do que o permitido originalmente, use a opção estendida para aumentar a duração. As contas no estado Criado, Ativo ou Expirado podem ser estendidas.

Uma conta que tenha sido suspensa ou negada não pode ser prolongada; use a opção reinstalar.



O período de extensão máximo permitido é regido pelo tipo de convidado da conta.

As contas de convidado expiram por conta própria quando atingem o fim da duração da conta, independentemente de seu estado. As contas de convidado suspensas ou expiradas são limpas automaticamente com base na política de limpeza definida no sistema. Por padrão, eles são limpos a cada 15 dias.

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

Estados da conta de convidado e seu significado:

Ativo: Convidados com essas contas entraram com êxito por meio de um portal de Convidado credenciado ou ignoraram o portal cativo de Convidado credenciado. Neste último caso, as contas pertencem a tipos de convidados configurados para ignorar o portal cativo de convidado. Esses convidados podem acessar a rede fornecendo suas credenciais de login ao requerente nativo em seu dispositivo.

Criado: As contas foram criadas, mas os convidados ainda não efetuaram login em um portal de convidado credenciado. Nesse caso, as contas são atribuídas a tipos de convidado que não estão configurados para ignorar o portal cativo de convidado credenciado. Os convidados devem primeiro entrar através do portal cativo Convidado credenciado antes de poderem acessar outras partes da rede.

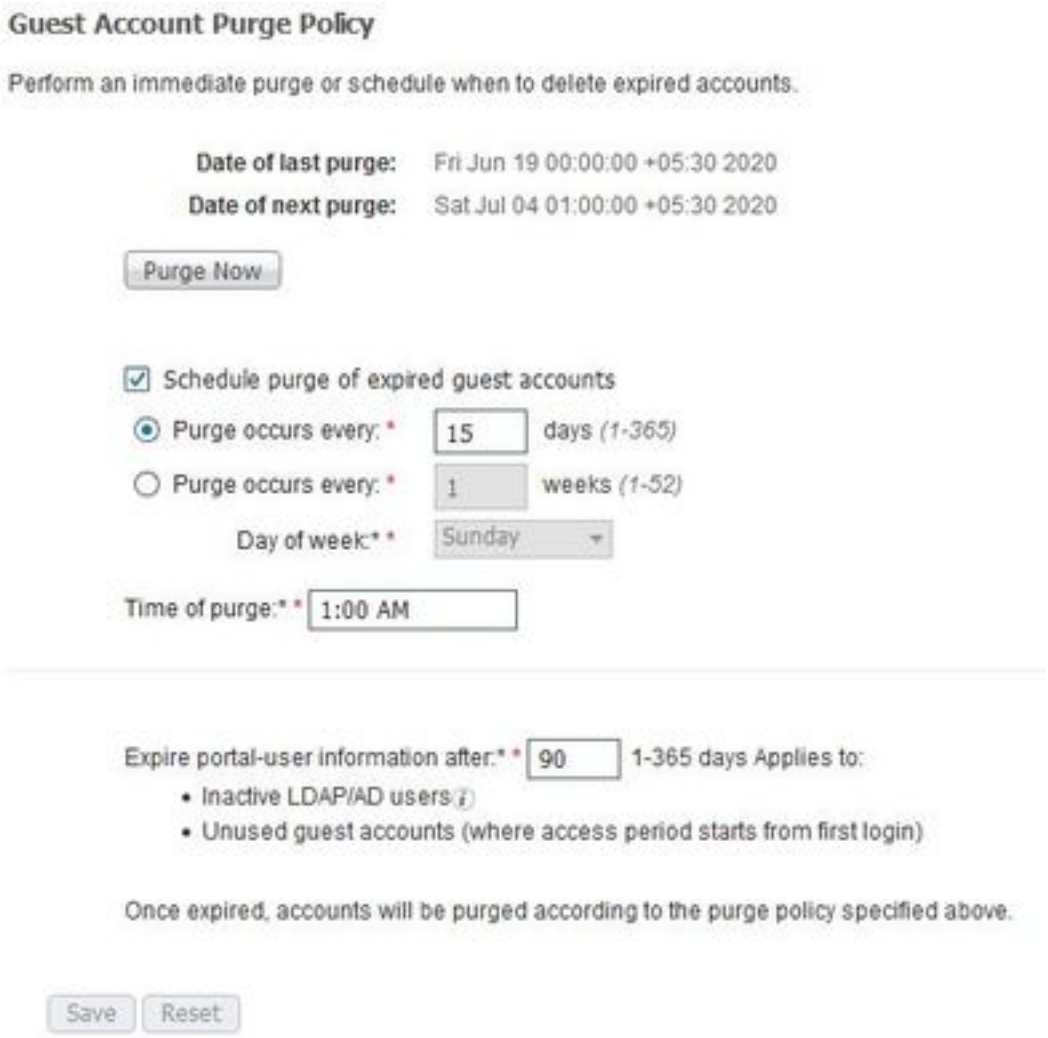
Negado: O acesso à rede foi negado às contas. As contas que expiraram enquanto estavam em um estado negado permanecem como negadas.

Aprovação pendente: As contas estão aguardando aprovação para acessar a rede.

Suspenso: As contas são suspensas por um patrocinador que tem o privilégio de o fazer.

Políticas de limpeza de convidado

Por padrão, o ISE limpa automaticamente contas de convidado expiradas a cada 15 dias. Essas informações podem ser vistas em **Centros de trabalho > Acesso de convidado > Configurações > Política de limpeza de conta de convidado**.



A data da próxima limpeza indica quando a próxima limpeza ocorrerá. O administrador do ISE pode:

- Agende uma limpeza a cada X dias. A **hora da limpeza** especifica quando a primeira limpeza acontece em X dias. Depois disso, a limpeza ocorre a cada X dias.
- Agende uma limpeza em um determinado dia da semana, a cada X semanas.
- Force uma limpeza sob demanda usando a opção **Limpar agora.**

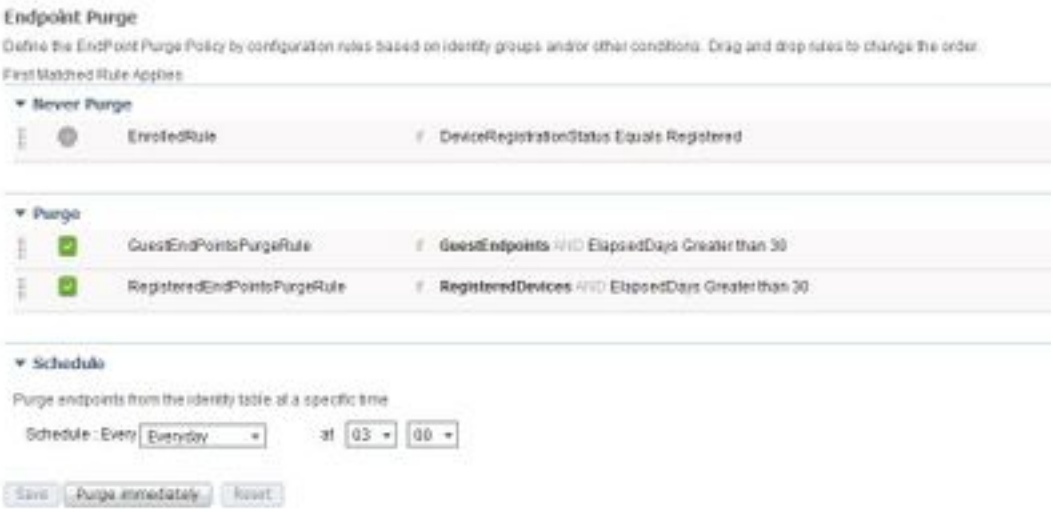
Quando as contas de convidado expiradas são limpas, os endpoints associados, os relatórios e as informações de registro são retidos.

Limpeza do ponto final: Dias Inativos versus Dias Decorrido para Endpoints

Os endpoints que os convidados usam para acessar a rede tornam-se parte dos GuestEndpoints por padrão. O ISE tem a política de excluir endpoints convidados e dispositivos registrados com mais de 30 dias. Este trabalho de limpeza padrão é executado a 1 da manhã do dia com base no fuso horário configurado no nó administrativo principal (PAN). Esta política predefinida utiliza a condição de **ElapsedDays**. Outras opções disponíveis são **InativeDays** e **PurgeDate**.

> **Note**: A funcionalidade de limpeza de endpoint é independente da Política de limpeza de conta de convidado e do vencimento da conta de convidado.

A política é definida em **Administration > Identity Management > Settings > Endpoint Purge**.



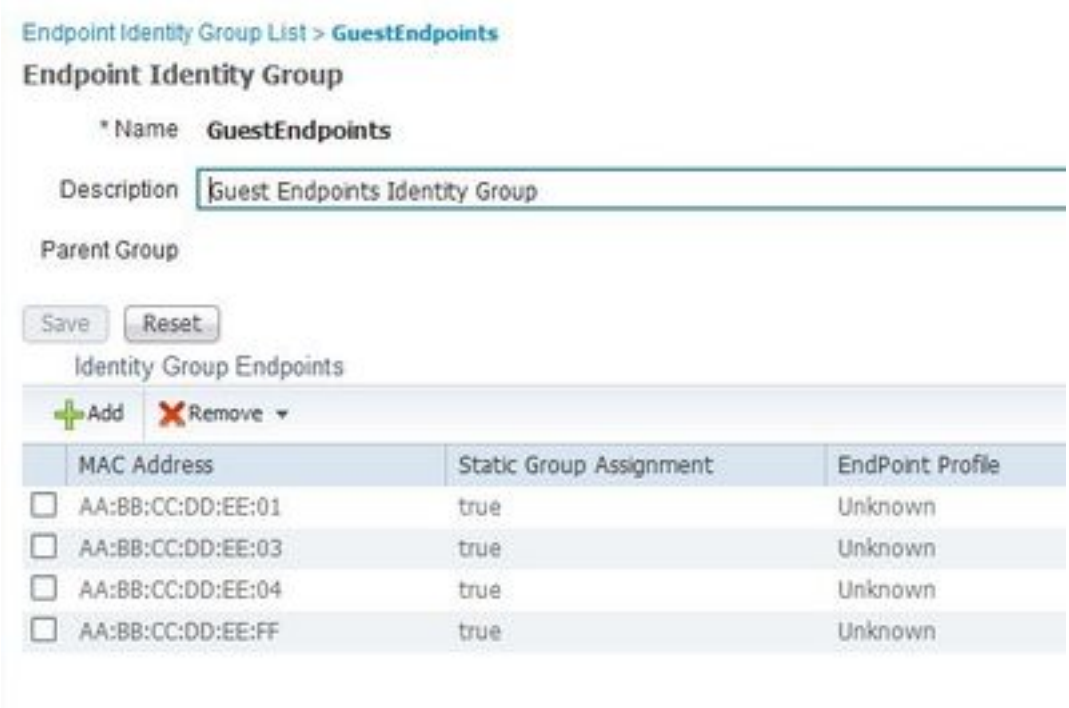
Dias decorrido: Refere-se ao número de dias desde que o objeto foi criado. Essa condição pode ser usada para endpoints aos quais foi concedido acesso inautenticado ou condicional por um período definido, como um endpoint de convidado ou contratante ou funcionários que utilizam a webauth para acessar a rede. Após o período de tolerância de conexão permitido, eles devem ser totalmente reautenticados e registrados.

Dias inativos: Refere-se ao número de dias desde a última atividade de criação de perfil ou atualização no endpoint. Essa condição elimina dispositivos obsoletos que se acumularam ao longo do tempo, geralmente convidados temporários ou dispositivos pessoais ou dispositivos descontinuados. Esses endpoints tendem a representar ruído na maioria das implantações, pois não estão mais ativos na rede ou provavelmente serão vistos em um futuro próximo. Se eles se conectarem novamente, serão redescobertos, com perfil, registrados, etc., conforme necessário.

Quando há atualizações do ponto final, InactivityDays será redefinido para 0 somente se o perfil estiver ativado.

Data de limpeza: Data para limpar o ponto final. Essa opção pode ser usada para eventos ou grupos especiais em que o acesso é concedido para um horário específico, independentemente da criação ou da hora de início. Isso permite que todos os endpoints sejam eliminados ao mesmo tempo. Por exemplo, uma feira de negócios, uma conferência ou uma aula de treinamento semanal com novos membros a cada semana, em que o acesso é concedido para uma semana ou mês específico em vez de dias/semanas/meses absolutos.

Este arquivo de exemplo profiler.log mostra quando os endpoints que faziam parte de GuestEndpoints e tinham transcorrido 30 dias foram removidos:

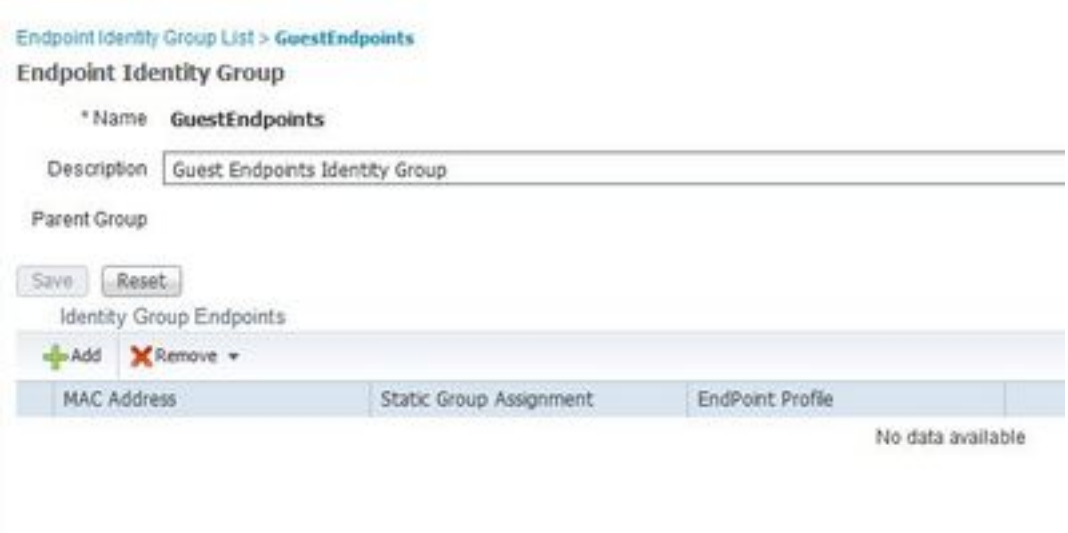



```
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- the rule type is :REGULAR
2020-07-09 09:35:21,983 INFO [admin-http-pool20][]
cpm.admin.profiler.action.ProfilerEndpointsPurgingAction -::- epPurgeRuleID is :3bfaffe0-8c01-
11e6-996c-525400b48521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

Após a limpeza:



Solucionar problemas de convidado e limpeza

Para capturar registros relacionados a problemas de convidado e limpeza, esses componentes podem ser definidos como debug. Para ativar depurações, navegue até **Administration> System > Debug Log Configuration> Select node**.

Para contas de convidado/patrocinador e solução de problemas relacionados à limpeza de endpoints, defina estes componentes como debug:

- acesso de convidado
- guest-admin
- guest-access-admin
- profiler
- runtime-AAA

Para problemas relacionados ao portal, defina estes componentes como debug:

- portal patrocinado
- portal
- gerenciador de sessão de portal
- acesso de convidado

Informações Relacionadas

- Guia de implantação prescritiva do ISE Guest Access
- Solucionar problemas e ativar depurações no ISE