

# Contents

[Documentação do Privileged Identity Management](#)

[Visão geral](#)

[O que é o PIM do Azure AD?](#)

[Conceitos](#)

[Requisitos de licença](#)

[Funções que você não pode gerenciar](#)

[Proteger o acesso privilegiado](#)

[MFA e PIM](#)

[Visão geral dos painéis](#)

[Notificações por email](#)

[APIs do Microsoft Graph](#)

[Guias de instruções](#)

[Implantar o PIM](#)

[Comece a usar o PIM](#)

[Configurar PIM](#)

[Assistente de segurança](#)

[Recursos de descoberta do Azure](#)

[Conceder acesso a outras pessoas para gerenciar o PIM](#)

[Elevar o acesso para gerenciar todas as assinaturas](#)

[Ativar minhas funções](#)

[Ativar minhas funções do Azure AD](#)

[Ativar minhas funções de recurso do Azure](#)

[Gerenciar funções do Azure AD](#)

[Atualização de recursos](#)

[PowerShell para funções do Azure AD](#)

[Atribuir funções](#)

[Aprovar solicitações](#)

[Definir configurações de função](#)

[Configurar alertas](#)

## [Versão prévia das funções personalizadas](#)

- [Ativar uma função personalizada](#)
- [Atribuir uma função personalizada](#)
- [Excluir uma atribuição de função](#)
- [Configurar funções personalizadas](#)

## [Exibir histórico de auditoria](#)

## [Gerenciar funções do Azure](#)

- [Atribuir funções](#)
- [Convidar usuários externos](#)
- [Aprovar solicitações](#)
- [Estender ou renovar funções](#)
- [Definir configurações de função](#)
- [Configurar alertas](#)
- [Exibir histórico de auditoria](#)
- [Usar funções personalizadas](#)

## [Solucionar problemas do PIM](#)

## [Análises de acesso](#)

- [Funções do Azure AD](#)
- [Criar uma análise de acesso](#)
- [Examinar acesso](#)
- [Concluir uma revisão de acesso](#)

## [Funções do Azure](#)

- [Criar uma análise de acesso](#)
- [Examinar acesso](#)
- [Concluir uma revisão de acesso](#)

## [Referência](#)

- [API do Graph](#)
- [CLI do Azure AD](#)
- [PowerShell do Azure AD para Graph](#)
- [Limites de serviço do Azure AD](#)

# O que é o Azure AD Privileged Identity Management?

22/07/2020 • 10 minutes to read • [Edit Online](#)

O PIM (Privileged Identity Management) do Azure AD (Azure Active Directory) é um serviço que permite gerenciar, controlar e monitorar o acesso a importantes recursos em sua organização. Esses recursos incluem os recursos no Azure AD, no Azure e em outros Microsoft Online Services, como o Office 365 ou o Microsoft Intune.

## Motivos para usá-lo

As empresas desejam minimizar o número de pessoas que têm acesso a informações seguras ou recursos, porque isso reduz a chance de um ator mal-intencionado obter esse tipo de acesso ou um usuário autorizado afetar accidentalmente um recurso confidencial. No entanto, os usuários ainda precisam executar operações privilegiadas em aplicativos do Azure AD, Azure, Office 365 ou SaaS. As organizações podem proporcionar aos usuários acesso privilegiado JIT (Just-In-Time) aos recursos do Azure e ao Azure AD. É preciso supervisionar o que esses usuários estão fazendo com seus privilégios de administrador.

## O que ela faz?

O Privileged Identity Management fornece ativação de função baseada em tempo e aprovação para atenuar os riscos de permissões de acesso excessivas, desnecessárias ou que foram indevidamente utilizadas em recursos importantes. Estes são alguns dos principais recursos do Privileged Identity Management:

- Fornecer acesso privilegiado **just-in-time** ao Azure AD e aos recursos do Azure
- Atribua acesso com **limite de tempo** aos recursos usando as datas de início e término
- Exigir **aprovação** para ativar funções com privilégios
- Impor **autenticação multifator** para ativar qualquer função
- Usar **justificativa** para entender por que os usuários ativam
- Obter **notificações** quando as funções privilegiadas forem ativadas
- Realizar **revisões de acesso** para garantir que os usuários ainda precisem de funções
- Baixar o **histórico de auditoria** para auditoria interna ou externa

## O que posso fazer com ele?

Depois de configurar o Privileged Identity Management, você verá as opções **Tarefas**, **Gerenciar** e **Atividade** no menu de navegação à esquerda. Como administrador, você poderá escolher entre gerenciar **funções do Azure AD** e **funções de recursos do Azure**. Quando você escolhe o tipo de funções a ser gerenciado, você vê um conjunto semelhante de opções para esse tipo de função.

The screenshot shows the Microsoft Azure portal with the URL [https://portal.azure.com/#blade/Microsoft\\_Azure\\_PIM/DirectoryRoleManagementBlade](https://portal.azure.com/#blade/Microsoft_Azure_PIM/DirectoryRoleManagementBlade). The page title is "Azure AD Privileged Identity Management". The left sidebar has sections like "Visão geral", "Início Rápido", and "Tarefas" (My Functions, My Requests, Approve Requests, Access Analysis). The main content area is titled "Azure AD Privileged Identity Management" and describes PIM as a Premium resource for managing privileged access. It shows three main actions: "Atribuir" (Assign), "Ativar" (Enable), and "Aprovar" (Approve). Each action has a description and a button: "Atribuir qualificação" (Assign qualification), "Ativar sua função" (Enable your function), and "Aprovar solicitações" (Approve requests).

## Quem pode fazer o quê?

Para as funções do Azure AD no Privileged Identity Management, somente um usuário que está na função de administrador de funções com privilégios ou administrador global pode gerenciar atribuições para outros administradores. Você pode [permitir acesso a outros administradores para gerenciar o Privileged Identity Management](#). Os Administradores globais, os Administradores de segurança, os Leitores globais e os Leitores de segurança também podem exibir as atribuições às funções do Azure AD no Privileged Identity Management.

Para as funções de recurso do Azure no Privileged Identity Management, somente um administrador de assinatura, um proprietário de recurso ou um administrador de acesso de usuário de recurso pode gerenciar atribuições para outros administradores. Por padrão, os usuários que são Administradores de funções com privilégios, Administradores da segurança ou Leitores de segurança não têm acesso para exibir as atribuições às funções de recurso do Azure no Privileged Identity Management.

## Cenários

O PIM dá suporte aos seguintes cenários:

### Permissões do Administrador de funções com privilégios

- Habilitar a aprovação para funções específicas
- Especificar usuários ou grupos aprovadores para aprovar solicitações
- Exibir o histórico de solicitações e aprovações de todas as funções com privilégios

### Permissões do aprovador

- Exibir as aprovações pendentes (solicitações)
- Aprovar ou rejeitar solicitações de elevação de função (única e em massa)
- Fornecer uma justificativa para minha aprovação ou rejeição

### Permissões de usuário de função qualificado

- Solicitar a ativação de uma função que exige aprovação
- Exibir o status de sua solicitação a ser ativada

- Concluir a tarefa no Azure AD caso a ativação tenha sido aprovada

## Terminologia

Para entender melhor o Privileged Identity Management e a documentação dele, examine os termos a seguir.

| TERMOS OU CONCEITOS         | CATEGORIA DE ATRIBUIÇÃO DE FUNÇÃO | DESCRIÇÃO  |
|-----------------------------|-----------------------------------|--|
| qualificado                 | Type                              | Uma atribuição de função que requer que um usuário execute uma ou mais ações para usá-la. Se um usuário se qualificou para uma função, isso significa que ele poderá ativá-la quando precisar executar tarefas privilegiadas. Não há nenhuma diferença no modo de acesso concedido a uma pessoa com uma atribuição de função permanente em comparação com uma qualificada. A única diferença é que algumas pessoas não precisam desse acesso o tempo todo. |
| ativo                       | Type                              | Uma atribuição de função que não requer que um usuário execute nenhuma ação para usar a função. Usuários atribuídos como ativos têm os privilégios atribuídos à função.  |
| ativar                      |                                   | O processo de execução de uma ou mais ações a fim de usar uma função para a qual um usuário está qualificado. As ações podem incluir a execução de uma verificação de MFA (Autenticação Multifator), fornecimento de uma justificativa comercial ou solicitação de aprovação dos aprovadores designados.   |
| atribuída                   | Estado                            | Um usuário que tem uma atribuição de função ativa.   |
| ativada                     | Estado                            | Um usuário que tem uma atribuição de função qualificada, executou as ações para ativar a função e agora está ativo. Depois que a função for ativada, o usuário poderá usar a função por um período pré-configurado antes de precisar ativá-la novamente.   |
| qualificada permanentemente | Duration                          | Uma atribuição de função em que um usuário sempre está qualificado para ativar a função.   |
| permanentemente ativa       | Duration                          | Uma atribuição de função em que um usuário sempre pode usar a função sem executar nenhuma ação.  |

| TERMO OU CONCEITO                          | CATEGORIA DE ATRIBUIÇÃO DE FUNÇÃO | DESCRIÇÃO   |
|--|-----------------------------------|---|
| qualificado com expiração                  | Duration                          | Uma atribuição de função em que um usuário está qualificado para ativar a função dentro de uma data de início e término especificada.   |
| ativo com expiração                        | Duration                          | Uma atribuição de função em que um usuário pode usar a função sem executar nenhuma ação dentro de uma data de início e término especificada.  |
| Acesso JIT (Just-In-Time)                  |                                   | Um modelo no qual os usuários recebem permissões temporárias para executar tarefas privilegiadas, o que impede que usuários mal-intencionados ou não autorizados obtenham acesso após a expiração das permissões. O acesso é concedido somente quando os usuários precisam dele.                              |
| princípio de acesso de privilégios mínimos |                                   | Uma prática de segurança recomendada na qual todos os usuários recebem apenas os privilégios mínimos necessários para realizar as tarefas que estão autorizados a executar. Essa prática minimiza o número de Administradores Globais usando funções de administrador específicas para determinados cenários. |

## Requisitos de licença

Para usar esse recurso, é necessária uma licença do Azure AD Premium P2. Para encontrar a licença certa para seus requisitos, consulte comparando [recursos disponíveis de forma geral dos aplicativos gratuitos, Office 365 e edições Premium](#).

Para obter informações sobre licenças para usuários, confira [Requisitos de licença para usar o Privileged Identity Management](#).

## Próximas etapas

- [Requisitos de licença para usar o Privileged Identity Management](#)
- [Protegendo o acesso privilegiado para implantações de nuvem e híbridos no Azure AD](#)
- [Implantar o Privileged Identity Management](#)

# Requisitos de licença para usar o Privileged Identity Management

22/07/2020 • 5 minutes to read • [Edit Online](#)

Para usar o Azure AD (Azure Active Directory) PIM (Privileged Identity Management), um diretório precisa ter uma licença válida. Além disso, as licenças precisam ser atribuídas aos administradores e aos usuários relevantes. Este artigo descreve os requisitos de licença para usar o Privileged Identity Management.

## Licenças válidas

Para usar esse recurso, é necessária uma licença do Azure AD Premium P2. Para encontrar a licença certa para seus requisitos, consulte comparando [recursos disponíveis de forma geral dos aplicativos gratuitos, Office 365 e edições Premium](#).

## Quantas licenças você precisa ter?

Verifique se o seu diretório tem um número de licenças do Azure AD Premium P2 igual ou superior ao número dos seus funcionários que executarão as seguintes tarefas:

- Usuários atribuídos como qualificados para funções do Azure AD gerenciadas usando o PIM
- Usuários capazes de aprovar ou rejeitar solicitações de ativação no PIM
- Usuários atribuídos a uma função de recurso do Azure com atribuições Just-In-Time ou diretas (por tempo limitado)
- Usuários atribuídos a uma revisão de acesso
- Usuários que executam revisões de acesso

As licenças do Azure AD Premium P2 **não** são necessárias para as seguintes tarefas:

- Nenhuma licença é necessária para usuários com funções de administrador global ou de administrador de função com privilégios que configuram o PIM, configurar políticas, receber alertas e configurar revisões de acesso.

Para obter mais informações sobre licenças, confira [Atribuir ou remover licenças usando o portal do Azure Active Directory](#).

## Cenários de licença de exemplo

Aqui estão alguns exemplos de cenários de licença para ajudá-lo a determinar o número de licenças que você precisa ter.

| CENÁRIO   | CÁLCULO   | NÚMERO DE LICENÇAS |
|---|---|--------------------|
| O Woodgrove Bank tem 10 administradores para diferentes departamentos e 2 administradores globais que configuram e gerenciam o PIM. Eles tornam cinco administradores qualificados. | Cinco licenças para os administradores que estão qualificados | 5                  |

| CENÁRIO  | CÁLCULO   | NÚMERO DE LICENÇAS |
|--|---|--------------------|
| O design gráfico Institute tem 25 administradores dos quais 14 são gerenciados por meio do PIM. A ativação de função requer aprovação e há três usuários diferentes na organização que podem aprovar ativações.  | 14 licenças para as funções qualificadas + três aprovadores                   | 17                 |
| A contoso tem 50 administradores dos quais a 42 é gerenciada por meio do PIM. A ativação de função requer aprovação e há cinco usuários diferentes na organização que podem aprovar ativações. A contoso também faz revisões mensais de usuários atribuídos a revisores e funções de administrador são os gerentes dos usuários dos quais seis não estão em funções de administrador gerenciadas pelo PIM. | 42 licenças para as funções qualificadas + cinco aprovadores + seis revisores | 53                 |

## O que acontece quando uma licença expira?

Se uma licença Azure AD Premium P2, EMS E5 ou de avaliação expirar, Privileged Identity Management recursos não estarão mais disponíveis em seu diretório:

- Atribuições de função permanentes para funções do Azure AD não serão afetadas.
- O serviço de Privileged Identity Management no portal do Azure, bem como os cmdlets do API do Graph e as interfaces do PowerShell do Privileged Identity Management, não estarão mais disponíveis para que os usuários ativem funções privilegiadas, gerenciem o acesso privilegiado ou realizem revisões de acesso de funções privilegiadas.
- Atribuições de funções qualificadas de funções do Azure AD serão removidas, pois os usuários não poderão mais ativar funções privilegiadas.
- Todas as revisões de acesso em andamento das funções do Azure AD serão encerradas e Privileged Identity Management definições de configuração serão removidas.
- Privileged Identity Management não enviará mais emails sobre alterações de atribuição de função.

## Próximas etapas

- [Implantar o Privileged Identity Management](#)
- [Começar usando o Privileged Identity Management](#)
- [Funções que você não pode gerenciar no Privileged Identity Management](#)

# Funções que você não pode gerenciar no Privileged Identity Management

22/07/2020 • 2 minutes to read • [Edit Online](#)

O Azure Active Directory (Azure AD) Privileged Identity Management (PIM) permite que você gerencie todas as [funções do Azure ad](#) e todas as [funções do Azure](#). As funções do Azure também podem incluir suas funções personalizadas anexadas aos grupos de gerenciamento, assinaturas, grupos de recursos e recursos. No entanto, há algumas poucas funções que não podem ser gerenciadas. Este artigo descreve as funções que você não pode gerenciar no Privileged Identity Management.

## Funções de administrador de assinatura Clássico

Você não pode gerenciar as seguintes funções de administrador de assinatura clássica no Privileged Identity Management:

- Administrador de conta
- Administrador de serviços
- Coadministrador

Para saber mais sobre as funções administrador de assinatura clássica, confira o artigo [Funções de administrador de assinatura clássica, funções RBAC do Azure e funções de administrador do Azure AD](#).

## E as funções de administrador do Office 365?

Damos suporte a todas as funções do Office365 na experiência do portal de funções e administradores do Azure AD, como administrador do Exchange e administrador do SharePoint, mas não damos suporte a funções específicas no RBAC do Exchange ou no RBAC do SharePoint. Para saber mais sobre esses serviços do Office 365, confira [Funções de administrador do Office 365](#).

### NOTE

Usuários qualificados para a função de administrador do SharePoint, a função de administrador do dispositivo e todas as funções que tentam acessar o centro de conformidade e segurança da Microsoft podem enfrentar atrasos de até algumas horas após a ativação de sua função. Estamos trabalhando com essas equipes para corrigir os problemas.

## Próximas etapas

- [Atribuir funções do Azure AD no Privileged Identity Management](#)
- [Atribuir funções de recurso do Azure no Privileged Identity Management](#)

# Proteger o acesso privilegiado para implantações de nuvem híbrida no Azure AD

22/07/2020 • 50 minutes to read • [Edit Online](#)

A segurança dos ativos de negócios da organização moderna depende da integridade das contas com privilégios que administram seus sistemas de TI. Os invasores virtuais usam ataques de roubo de credenciais para direcionar contas de administrador e outro acesso privilegiado para tentar obter acesso a dados confidenciais.

Para serviços de nuvem, prevenção e resposta são as responsabilidades conjuntas do provedor de serviços de nuvem e do cliente. Para obter mais informações sobre as ameaças mais recentes aos pontos de extremidade e à nuvem, consulte o [Relatório de Inteligência de Segurança da Microsoft](#). Este artigo pode ajudá-lo a desenvolver um roteiro para fechar as lacunas entre os planos atuais e as diretrizes descritas aqui.

## NOTE

A Microsoft está comprometida com os mais altos níveis de confiança, transparência, conformidade com os padrões e conformidade normativa. Saiba mais sobre como a equipe de resposta a incidentes globais da Microsoft atenua os efeitos de ataques contra serviços de nuvem e como a segurança é criada em produtos comerciais da Microsoft e serviços de nuvem no [Microsoft Trust Center - Segurança](#) e destinos de conformidade da Microsoft em [Microsoft Trust Center - Conformidade](#).

Tradicionalmente, a segurança organizacional se concentrou nos pontos de entrada e saída de uma rede como o perímetro de segurança. No entanto, os aplicativos SaaS e dispositivos pessoais na Internet tornaram essa abordagem menos eficaz. No Azure AD, substituímos o perímetro de segurança de rede pela autenticação na camada de identidade da sua organização, com usuários atribuídos a funções administrativas privilegiadas no controle. Seu acesso deve ser protegido, independentemente de o ambiente estar no local, na nuvem ou em um híbrido.

Proteger acesso privilegiado requer alterações a:

- Processos, práticas administrativas e gerenciamento de conhecimento
- Componentes técnicos, como proteção de host, proteções de conta e gerenciamento de identidade

Proteja seu acesso privilegiado de uma maneira que seja gerenciado e relatado nos serviços da Microsoft que você deseja. Se você tiver contas administrativas locais, confira as diretrizes para acesso privilegiado no local e híbrido no Active Directory em [Proteção de acesso privilegiado](#).

## NOTE

As diretrizes neste artigo referem-se principalmente a recursos do Azure Active Directory que são incluídos em planos de Azure Active Directory Premium P1 e P2. O Azure Active Directory Premium P2 está incluído no conjunto de EMS E5 e Microsoft 365 E5. Este guia pressupõe que sua organização já tem as licenças do Azure AD Premium P2 adquiridas para os usuários. Se você não tiver essas licenças, algumas das orientações podem não se aplicar à sua organização. Além disso, ao longo deste artigo, o termo administrador global significa o mesmo que "administrador da empresa" ou "administrador locatário".

## Desenvolver um roteiro

A Microsoft recomenda que você crie e execute um roteiro para proteger o acesso privilegiado contra invasores virtuais. Você sempre pode ajustar seu roteiro para acomodar seus recursos existentes e os requisitos específicos

dentro da sua organização. Cada estágio de nossos planos deverá aumentar o custo e a dificuldade de adversários de atacar o acesso privilegiado ao seu local, nuvem e ativos híbridos. A Microsoft recomenda os quatro estágios de roteiro a seguir. Agende primeiro as implementações mais eficazes e rápidas. Este artigo pode ser seu guia, com base nas experiências da Microsoft com a implementação de incidente e resposta de ataque cibernético. As linhas do tempo deste roteiro são aproximadas.



- Estágio 1 (24 a 48 horas): Itens críticos, recomendamos que você faça imediatamente
- Estágio 2 (2 a 4 semanas): Reduzir as técnicas de ataque usados com mais frequência
- Estágio 3 (1 a 3 meses): Criar visibilidade e obter controle total da atividade do administrador
- Estágio 4 (seis meses ou mais): Continuar criando defesas para proteger ainda mais sua plataforma de segurança

Essa estrutura de roteiro foi projetada para maximizar o uso de tecnologias da Microsoft que você já tiver implantado. Considere a vincular qualquer ferramenta de segurança de outros fornecedores que você já tenha implantado ou esteja considerando a implantação.

## Etapa 1: Itens críticos para fazer no momento



A etapa 1 do roteiro do destina-se as tarefas críticas que são rápidas e fáceis de implementar. É recomendável que você faça alguns desses itens imediatamente dentro de 24 a 48 horas primeiramente para garantir um nível básico de proteção ao acesso privilegiado. Essa etapa do roteiro de Acesso Privilegiado Seguro inclui as ações a seguir:

### **Preparação geral**

#### **Ative o Azure AD Privileged Identity Management**

Recomendamos que você ative o Azure AD PIM (Privileged Identity Management) em seu ambiente de produção do Azure AD. Depois de ativar o PIM, você receberá mensagens de notificação por email para alterações da função de acesso privilegiado. Notificações fornecem aviso antecipado quando usuários adicionais são adicionados às funções altamente privilegiadas.

O Azure AD Privileged Identity Management está incluído no Azure AD Premium P2 ou EMS E5. Para ajudá-lo a proteger o acesso a aplicativos e recursos locais e na nuvem, inscreva-se na [avaliação gratuita de 90 dias do Enterprise Mobility + Security](#). O Azure AD Privileged Identity Management e o Azure AD Identity Protection monitoram a atividade usando relatório, auditoria e alertas do Azure AD.

Depois de ativar o Azure AD Privileged Identity Management:

1. Entre no [portal do Azure](#) com uma conta que seja um administrador global da organização de produção do Azure AD.
2. Para selecionar a organização do Azure AD em que você deseja usar o Privileged Identity Management, selecione seu nome de usuário no canto superior direito do portal do Azure.
3. No menu do portal do Azure, selecione **Todos os serviços** e filtre a lista para **Azure AD Privileged Identity Management**.
4. Abra o Privileged Identity Management a partir de **Todos os serviços** liste e fixá-o ao seu painel.

Garanta que a primeira pessoa a usar o PIM em sua organização seja atribuída com as funções de **Administrador de segurança** e **Administrador de funções com privilégios**. Somente os administradores com privilégios de função podem gerenciar atribuições de função de usuários do diretório do Azure AD. O assistente de segurança do PIM orienta você durante a experiência inicial de detecção e atribuição. Você pode sair do assistente sem fazer alterações adicionais no momento.

#### **Identifique e categorize as contas que estão em funções altamente privilegiadas**

Depois de ativar Azure AD Privileged Identity Management, visualize os usuários que estão nas seguintes funções do Azure AD:

- Administrador global
- Administrador de função com privilégios
- Administradores do Exchange
- Administrador do SharePoint

Se você não tiver o Azure AD Privileged Identity Management em sua organização, poderá usar a [API do PowerShell](#). Comece com a função de administrador global porque um administrador global tem as mesmas permissões em todos os serviços de nuvem ao quais sua organização tenha assinado. Essas permissões são concedidas independentemente de onde foram atribuídas: no Centro de Administração do Microsoft 365, no portal do Azure ou pelo módulo do Azure AD para Microsoft PowerShell.

Remova todas as contas que não são mais necessárias nessas funções. Em seguida, categorize as contas restantes atribuídas às funções administrativas:

- Atribuídas a usuários administrativos, mas também podem ser usadas para fins não administrativos (por exemplo, email pessoal)
- Atribuídas a usuários administrativos e usadas apenas para fins administrativos
- Compartilhada por vários usuários
- Para cenários de acesso de emergência em situação crítica
- Para scripts automatizados
- Para usuários externos

#### **Defina pelo menos duas contas de acesso de emergência**

É possível que um usuário seja bloqueado acidentalmente de sua função. Por exemplo, se um provedor de identidade local federado não estiver disponível, os usuários não poderão entrar ou ativar uma conta de administrador existente. Você pode se preparar para a falta de acesso acidental armazenando duas ou mais contas de acesso de emergência.

As contas de acesso de emergência ajudam a restringir o acesso privilegiado em uma organização do Azure AD. Essas contas são altamente privilegiadas e não são atribuídas a indivíduos específicos. As contas de acesso de emergência são limitadas a cenários de emergência ou urgência em que as contas administrativas normais não podem ser usadas. Certifique-se de controlar e reduzir o uso da conta de emergência somente pelo tempo necessário.

Avalie as contas que são atribuídas ou qualificadas para a função de administrador global. Se você não vir

nenhuma conta somente em nuvem usando o domínio \*.onmicrosoft.com (para acesso de emergência), crie-as. Para obter mais informações, consulte [Gerenciamento de contas administrativas de acesso de emergência no Azure AD](#).

#### **Ativar autenticação multifator e registrar todas as outras contas de administrador de usuário único, não federadas e altamente privilegiadas**

Exigir a MFA (autenticação multifator) do Azure na entrada para todos os usuários individuais que são atribuídos permanentemente a uma ou mais das funções de administrador do Azure AD: administrador global, administrador de função com privilégios, administrador do Exchange e administrador do SharePoint. Use o guia para habilitar [Multi-factor Authentication \(MFA\) para suas contas de administrador](#) e certifique-se de que todos os usuários se registraram em <https://aka.ms/mfasetup>. Mais informações podem ser encontradas na etapa 2 e 3 do guia [Proteger o acesso a dados e serviços no Office 365](#).

## Etapa 2: Atenuar ataques usados com frequência



O estágio 2 do roteiro se concentra na redução das técnicas de ataque e roubo de credenciais usadas com mais frequência e pode ser implementado em aproximadamente 2 a 4 semanas. Essa etapa do roteiro de Acesso Privilegiado Seguro inclui as ações a seguir.

### **Preparação geral**

#### **Realizar um inventário de serviços, proprietários e administradores**

O aumento de "bring your own device" e políticas de trabalho de casa e o crescimento da conectividade sem fio torna importante monitorar quem está se conectando à sua rede. Uma auditoria de segurança pode revelar dispositivos, aplicativos e programas em sua rede para os quais sua organização não dá suporte e que representam alto risco. Para obter mais informações, veja [visão geral de monitoramento e gerenciamento de segurança do Azure](#). Certifique-se de incluir todas as tarefas a seguir em seu processo de inventário.

- Identifique os usuários que têm os serviços e funções administrativas, onde eles podem gerenciar.
- Use o Azure AD PIM para descobrir quais usuários em sua organização têm acesso de administrador ao Azure AD.
- Além das funções definidas no Azure Ad, o Office 365 vem com um conjunto de funções de administrador que você pode atribuir a usuários em sua organização. Cada função de administrador é mapeada para funções comerciais comuns e concede permissão às pessoas em sua organização para realizar tarefas específicas no [Centro de Administração do Microsoft 365](#). Use o Centro de administração do Microsoft 365 para descobrir quais usuários em sua organização têm acesso de administrador ao Office 365, inclusive por meio de funções não gerenciadas no Azure AD. Para obter mais informações, confira [Sobre funções de administrador do Office 365](#) e [Práticas de segurança para o Office 365](#).
- Execute o inventário em serviços de que sua organização depende, como Azure, Intune ou Dynamics 365.
- Verifique se as contas são usadas para fins de administração:
  - Tenha endereços de email de trabalho anexados a elas

- Registre na Autenticação Multifator do Azure ou use a MFA local
- Pergunte aos usuários sua justificativa de negócios para acesso administrativo.
- Remova o acesso de administrador para as pessoas e serviços que não são necessários.

#### **Identifique as contas da Microsoft em funções administrativas que precisam ser alternadas para contas de trabalho ou escolares**

Se os administradores globais iniciais reutilizarem as credenciais de conta da Microsoft existentes quando começarem a usar o Azure AD, substitua as contas da Microsoft por contas individuais baseadas em nuvem ou sincronizadas.

#### **Garanta contas de usuário separadas e emails de encaminhamento para as contas de administrador global**

Contas de email pessoais são regularmente capturadas por invasores virtuais, um risco que torna os endereços de email pessoais inaceitáveis para contas do administrador global. Para ajudar a separar os riscos de internet de privilégios administrativos, crie contas dedicadas para cada usuário com privilégios administrativos.

- Crie contas separadas para os usuários realizarem tarefas de administração globais
- Certifique-se de que os administradores globais não abram emails ou executem programas acidentalmente com suas contas de administrador
- Certifique-se de que essas contas tenham seu email encaminhado para uma caixa de correio comercial

#### **Certifique-se de que as senhas de contas administrativas foram alteradas recentemente**

Certifique-se de que todos os usuários entraram nas contas administrativas e alteraram as senhas pelo menos uma vez nos últimos 90 dias. Além disso, verifique se todas as contas compartilhadas tiveram as senhas alteradas recentemente.

#### **Ativar a sincronização de hash de senha**

O Azure AD Connect sincroniza um hash do hash da senha do usuário de um Active Directory local para uma organização do Azure AD baseada em nuvem. Você poderá usar a sincronização de hash de senha como um backup se usar a federação com os AD FS (Serviços de Federação do Active Directory). Esse backup poderá ser útil se seus servidores do Active Directory ou AD FS locais estiverem temporariamente indisponíveis.

A sincronização de hash de senha permite que os usuários se conectem ao serviço com a mesma senha usada para entrar em sua instância local do Active Directory. A sincronização de hash de senha permite que a Proteção de Identidade detecte credenciais comprometidas comparando hashes de senha com senhas conhecidamente comprometidas. Para obter mais informações, consulte [Implementar a sincronização de senha com a sincronização do Azure AD Connect](#).

#### **Exigir autenticação multifator para usuários em funções privilegiadas e usuários expostos**

O Azure AD recomenda que você exija a MFA (autenticação multifator) para todos os usuários. Considere os usuários que teriam um impacto significativo se sua conta estivesse comprometida (por exemplo, gerentes financeiros). A MFA reduz o risco de um ataque devido a uma senha comprometida.

Ativar:

- [A MFA usando políticas de acesso condicional](#) para todos os usuários em sua organização.

Se você usar o Windows Hello for Business, o requisito de MFA pode ser atendido usando o logon do Windows Hello. Para obter mais informações, consulte [Windows Hello](#).

#### **Configurar o Identity Protection**

O Azure AD Identity Protection é uma ferramenta de monitoramento e relatório baseada em algoritmos que detecta possíveis vulnerabilidades que afetam as identidades da sua organização. Você pode configurar as respostas automatizadas a essas atividades suspeitas detectadas e tomar as devidas providências para resolvê-las. Para obter mais informações, consulte [Azure Active Directory Identity Protection](#).

#### **Obter o Office 365 Secure Score (se estiver usando o Office 365)**

O Secure Score analisa suas configurações e atividades para os serviços do Office 365 que você está usando e compara com uma linha de base estabelecida pela Microsoft. Você obterá uma pontuação com base em como está

alinhado às práticas de segurança. Qualquer pessoa que tenha permissões de administrador para uma assinatura do Office 365 Business Premium ou Enterprise pode acessar o Secure Score em <https://securescore.office.com>.

#### **Verifique as diretrizes de segurança e conformidade do Office 365 (se estiver usando o Office 365)**

O [plano de segurança e conformidade](#) descreve a abordagem de um cliente do Office 365 para configurar o Office 365 e habilitar outros recursos do EMS. Em seguida, analise as etapas de 3 a 6 de como [proteger o acesso a dados e serviços no Office 365](#) e o guia de como [monitorar segurança e conformidade no Office 365](#).

#### **Configure o Office 365 Activity Monitoring (se estiver usando o Office 365)**

Monitore sua organização para usuários que estão usando o Office 365 para identificar a equipe que tem uma conta de administrador, mas pode não precisar de acesso ao Office 365 porque não entram nesses portais. Para obter mais informações, confira [Relatórios de atividade no Centro de administração do Microsoft 365](#).

#### **Estabelecer os proprietários de plano de resposta de incidente/emergência**

O estabelecimento de uma capacidade de resposta a incidentes bem-sucedida requer planejamento considerável e recursos. Você deve monitorar continuamente os ataques cibernéticos e estabelecer prioridades para o tratamento de incidentes. Colete, analise e relate dados de incidentes para criar relações e estabelecer comunicação com outros grupos internos e proprietários do plano. Para obter mais informações, consulte [Microsoft Security Response Center](#).

#### **Proteja as contas as contas administrativas locais, se ainda não tiver feito isso**

Se a sua organização do Azure Active Directory estiver sincronizada ao Active Directory local, siga as orientações em [Roteiro de acesso privilegiado à segurança](#): Este estágio inclui:

- Criar contas de administrador separadas para usuários que precisam realizar tarefas administrativas locais
- Implantar estações de trabalho com acesso privilegiado para administradores do Active Directory
- Criar senhas de administrador local exclusivas para estações de trabalho e servidores

#### **Etapas adicionais para as organizações a gerenciar o acesso do Azure**

##### **Concluir um inventário de assinaturas**

Use o portal da Enterprise e o portal do Azure para identificar as assinaturas em sua organização que hospedam aplicativos de produção.

##### **Remover as contas da Microsoft de funções de administrador**

As contas da Microsoft de outros programas, como Xbox, Live e Outlook não devem ser usadas como contas de administrador para assinaturas da sua organização. Remova o status administrativo de todas as contas da Microsoft e substitua por contas corporativas ou de estudante do Azure AD (por exemplo, chris@contoso.com). Para fins de administração, dependa de contas que são autenticadas no Azure AD e não em outros serviços.

##### **Monitorar a atividade do Azure**

O Log de Atividades do Azure fornece um histórico de eventos no nível da assinatura no Azure. Oferece informações sobre quem criou, atualizou ou excluiu quais recursos e quando fez isso. Para obter mais informações, consulte [Auditar e receber notificações sobre ações importantes em sua assinatura do Azure](#).

#### **Etapas adicionais para as organizações a gerenciar o acesso do Azure**

##### **Configurar as políticas de acesso condicional**

Prepare as políticas de acesso condicional para o local e os aplicativos hospedados em nuvem. Se você tiver os dispositivos vinculados no local de trabalho dos usuários, obtenha mais informações em [Configurar acesso condicional local usando o registro do dispositivo do Azure Active Directory](#).

## **Etapa 3: Assuma o controle da atividade do administrador**

# *Stage 3*

## 1-3 months

O Estágio 3 amplia as atenuações do Estágio 2 e deve ser implementado em aproximadamente um a três meses. Essa etapa do roteiro de Acesso Privilegiado Seguro inclui as ações a seguir.

### **Preparação geral**

#### **Concluir uma análise de acesso de usuários em funções de administrador**

Mais usuários corporativos estão obtendo acesso privilegiado por meio de serviços de nuvem, o que pode levar a um acesso não gerenciado. Os usuários de hoje podem se tornar administradores globais do Office365, administradores da assinatura do Azure ou ter acesso administrativo para VMs ou via aplicativos SaaS.

Sua organização deve fazer com que todos os funcionários tratem transações de negócios comuns como usuários sem privilégios e conceder direitos de administrador somente quando necessário. Conclua as revisões de acesso para identificar e confirmar os usuários que estão qualificados para ativar os privilégios de administrador.

É recomendável que você:

1. Determine quais usuários são administradores do Azure AD, habilite sob demanda, acesso de administração just-in-time e controles de segurança baseada em função.
2. Converter os usuários que têm sem justificativa clara para acesso de administrador com privilégios para uma função diferente (se não houver função qualificada, remova-o).

#### **Continuar a distribuição de autenticação mais forte para todos os usuários**

Exija que usuários altamente expostos tenham autenticação moderna e forte, como Azure MFA ou Windows Hello. Exemplos de usuários altamente expostos incluem:

- Diretores
- Gerentes de alto nível
- Pessoal de TI e segurança crítica

#### **Use estações de trabalho dedicadas para a administração do Azure AD**

Os invasores podem direcionar para contas com privilégios para interromper a integridade e autenticidade dos dados. Geralmente, eles usam código mal-intencionado que altera a lógica do programa ou espiona o administrador inserindo uma credencial. As Estações de Trabalho com Acesso Privilegiado (PAWs) fornecem um sistema operacional dedicado para as tarefas confidenciais protegidas contra ataques da Internet e vetores de ameaça. Separar essas contas e tarefas confidenciais de dispositivos e estações de trabalho de uso diário proporciona forte proteção contra:

- Ataques de phishing
- Vulnerabilidades do aplicativo e do sistema operacional
- Ataques de usurpação de identidade
- Ataques de roubo de credenciais, como registro de pressionamento de teclas, Pass-the-Hash e Pass-the-Ticket

Com a implantação de estações de trabalho de acesso privilegiado, você pode reduzir o risco de os administradores inserirem credenciais em um ambiente de área de trabalho que não foi protegido. Para saber mais, confira [Privileged Identity Management](#).

## **Analise as recomendações do Instituto Nacional de padrões e tecnologia para lidar com incidentes**

O Instituto Nacional de padrões e tecnologia (NIST) fornece diretrizes para tratamento de incidentes, particularmente para analisar dados relacionados ao incidente e determinar a resposta apropriada a cada incidente. Para obter mais informações, consulte ([NIST](#)) o [Computer Security Incident Handling Guide \(SP 61 800, Revisão 2\)](#).

### **Implementar Privileged Identity Management (PIM) para JIT a funções administrativas adicionais**

Para o Azure Active Directory, use o recurso [Azure AD Privileged Identity Management](#). Ativação de tempo limitado de funções privilegiadas funciona, permitindo que você:

- Ativar os privilégios de administrador para executar uma tarefa específica
- Imponha o MFA durante o processo de ativação
- Use alertas para informar os administradores sobre alterações fora de banda
- Permita que os usuários mantenham os privilégios de acesso por um período de tempo pré-configurado
- Permita que os administradores de segurança:
  - Descubra todas as identidades com privilégios
  - Visualize relatórios de auditoria
  - Crie revisões de acesso para identificar cada usuário que é elegível para ativar privilégios de administrador

Se você já estiver usando o Azure AD Privileged Identity Management, ajuste intervalos de tempo para privilégios de tempo especificado conforme necessário (por exemplo, janelas de manutenção).

### **Determine a exposição a protocolos com senha (se estiver usando o Exchange Online)**

Recomendamos a identificação de todos os usuários potenciais que poderão ser catastróficos para a organização se suas credenciais forem comprometidas. Para esses usuários, coloque em vigor requisitos de autenticação fortes e use o acesso condicional do Azure AD para impedir a entrada em seus emails usando o nome de usuário e a senha. Você pode bloquear a [autenticação herdada usando acesso condicional](#) e pode [bloquear a autenticação básica](#) por meio do Exchange Online.

### **Conclua uma avaliação de revisão de funções para as funções do Office 365 (se estiver usando o Office 365)**

Avalie se todos os usuários administradores estão nas funções corretas (exclua e reatribua de acordo com essa avaliação).

**Examine a abordagem de gerenciamento de incidentes de segurança usada no Office 365 e compare com sua própria organização**  
Você pode fazer o download desse relatório de [gerenciamento de incidentes de segurança no Microsoft Office 365](#).

### **Continuar a proteger as contas administrativas privilegiadas locais**

Se o seu Azure Active Directory estiver conectado ao Active Directory local, siga as orientações em [Roteiro de Acesso Privilegiado à Segurança](#): Estágio 2. Neste estágio, você pode:

- Implantar estações de trabalho com acesso privilegiado para todos os administradores
- Exigir MFA
- Usar apenas o administrador suficiente para a manutenção do controlador de domínio, reduzindo a superfície de ataque de domínios
- Implantar a avaliação avançada de ameaças para detecção de ataque

### **Etapas adicionais para as organizações a gerenciar o acesso do Azure**

#### **Estabelecer monitoramento integrado**

A [Central de Segurança do Azure Security](#):

- Fornece monitoramento de segurança integrado e gerenciamento de políticas em suas assinaturas do Azure
- Ajuda a detectar ameaças que não seriam observadas de outra forma

- Funciona com uma ampla variedade de soluções de segurança

#### **Faça o inventário de contas privilegiadas em Máquinas Virtuais hospedadas**

Você geralmente não precisa fornecer aos usuários permissões irrestritas a todos os recursos ou assinaturas do Azure. Use as funções de administrador do Azure AD para conceder somente o acesso para os usuários que precisam realizar seus trabalhos. Você pode usar as funções do Azure AD para permitir que um administrador gerencie apenas máquinas virtuais em uma assinatura, enquanto outro pode gerenciar banco de dados SQL dentro da mesma assinatura. Para obter mais informações, consulte [Introdução ao Controle de Acesso Baseado em Função no portal do Azure](#).

#### **Implementar o PIM para funções de administrador do Azure AD**

Use o Privileged Identity Management com as funções de administrador do Azure Ad para gerenciar, controlar e monitorar o acesso aos recursos do Azure. Use as proteções de PIM reduzindo o tempo de exposição de privilégios e aumentando sua visibilidade sobre o uso por meio de alertas e relatórios. Para obter mais informações, consulte [Gerenciar o acesso aos recursos do Azure com o Privileged Identity Management](#).

#### **Usar integrações do log do Azure para enviar logs relevantes do Azure para seus sistemas SIEM**

A integração de log do Azure permite que você integre logs brutos de recursos do Azure aos sistemas Security Information and Event Management (SIEM) da sua organização. A [integração de logs do Azure](#) coleta eventos do Windows de logs de Visualizador de Eventos do Windows e recursos do Azure de:

- Logs de atividades do Azure
- Alertas da Central de Segurança do Azure
- Logs de recursos do Azure

#### **Etapas adicionais para as organizações a gerenciar o acesso do Azure**

##### **Implementar o provisionamento do usuário para aplicativos conectados**

O Azure AD permite automatizar a criação e a manutenção de identidades do usuário em aplicativos de nuvem, como Dropbox, Salesforce e ServiceNow. Para saber mais, confira [Automatizar o provisionamento e o desprovisionamento de usuários para aplicativos SaaS com o Azure AD](#).

##### **Integrar proteção de informações**

O Microsoft Cloud App Security permite que você investigue arquivos e defina políticas com base em rótulos de classificação da Proteção de Informações do Azure permitindo maior visibilidade e controle de seus dados na nuvem. Verifique e classifique arquivos na nuvem e aplique rótulos de proteção de informações do Azure. Para obter mais informações, consulte [integração da Proteção de Informações do Microsoft Azure](#).

##### **Configurar acesso condicional**

Configure o acesso condicional com base em grupo, localização e sensibilidade de aplicativo para [aplicativos SaaS](#) e aplicativos conectados ao Azure AD.

##### **Monitorar a atividade de aplicativos de nuvem conectados**

Recomendamos o uso do [Microsoft Cloud App Security](#) para garantir que o acesso do usuário também esteja protegido em aplicativos conectados. Esse recurso protege o acesso corporativo a aplicativos de nuvem, além de proteger suas contas de administrador, permitindo:

- Aumentar a visibilidade e controle para aplicativos em nuvem
- Criar políticas de acesso, atividades e compartilhamento de dados
- Identificar automaticamente as atividades arriscadas, comportamentos anormais e ameaças
- Impedir o vazamento de dados
- Minimizar o risco e prevenção de ameaças automatizado e aplicação de políticas

O agente Cloud App Security SIEM integra Cloud App Security integra o Cloud App Security ao seu servidor SIEM para habilitar o monitoramento centralizado de atividades e alertas do Office 365. Ele é executado no servidor e recebe alertas e atividades de segurança do aplicativo de nuvem e transmite-as no servidor SIEM. Para obter mais informações, consulte [Integração SIEM](#).

## Estágio 4: Continuar criando defesas

### Stage 4 6 months and beyond

O estágio 4 do roteiro deve ser implementado em cerca de seis meses. Conclua seu roteiro para reforçar as proteções de acesso privilegiado de possíveis ataques que são conhecidos hoje. Para as ameaças de segurança do amanhã, é recomendável ver a segurança como um processo contínuo para aumentar os custos e reduzir a taxa de sucesso dos adversários que estão direcionando para o seu ambiente.

Proteger o acesso privilegiado é importante para estabelecer garantias de segurança para seus ativos de negócios. No entanto, ele deve fazer parte de um programa de segurança completo que fornece garantias de segurança contínuas. Este programa deve incluir elementos como:

- Política
- Operações
- Segurança das informações
- Servidores
- Aplicativos
- PCs
- Dispositivos
- Malha da nuvem

Recomendamos as seguintes práticas quando você estiver gerenciando contas de acesso privilegiado:

- Certifique-se de que os administradores estão fazendo seus negócios diários, como usuários sem privilégios
- Conceda acesso privilegiado apenas quando necessário e remova-o posteriormente (just-in-time)
- Mantenha registros de atividades de auditoria relacionadas a contas privilegiadas

Para obter mais informações sobre a criação de um roteiro de segurança completa, consulte [recursos de arquitetura de TI de nuvem da Microsoft](#). Para que os serviços da Microsoft ajudem você a implementar qualquer parte do seu roteiro, entre em contato com seu representante da Microsoft ou confira [Construir defesas cibernéticas essenciais para proteger a sua empresa](#).

Essa etapa final do roteiro Secured Privileged Access inclui os seguintes componentes.

#### Preparação geral

##### Analise as funções de administrador no Azure AD

Determine se as funções de administrador integradas atuais do Azure AD ainda estão atualizadas e garanta que os usuários estão apenas com as funções de que precisam. Com o Azure AD, você pode atribuir administradores separados para realizar diferentes funções. Para saber mais informações, consulte [Atribuindo funções de administrador no Azure Active Directory](#).

##### Analise os usuários que têm administração dos dispositivos unidos do Azure AD

Para obter mais informações, consulte [Como configurar dispositivos híbridos unidos do Azure Active Directory](#).

##### Reveja os membros de funções internas do administrador do Office 365

Ignore esta etapa se você não estiver usando o Office 365.

#### **Validar o plano de resposta a incidentes**

Para melhorar o seu plano, a Microsoft recomenda que você valide regularmente seu que está funcionando conforme o esperado:

- Passe pelo seu roteiro existente para ver o que foi perdido
- Com base na análise post mortem, revise práticas existentes ou defina novas práticas
- Certifique-se de que seu plano de resposta a incidentes está atualizado e que as práticas são distribuídas por toda a organização

#### **Etapas adicionais para as organizações a gerenciar o acesso do Azure**

Determine se você precisa [transferir a propriedade de uma assinatura do Azure para outra conta](#).

### "Vigilância": o que fazer em caso de emergência



1. Notifique os principais gerentes e executivos de segurança com informações sobre o incidente.
2. Analise o guia estratégico de ataque.
3. Acesse sua combinação de nome de usuário e senha da conta de "vigilância"" para entrar no Azure AD.
4. Obtenha ajuda da Microsoft ao [abrir uma solicitação de suporte do Azure](#).
5. Examine os [relatórios de entrada do Azure AD](#). Pode haver um espaço de tempo entre um evento ocorrendo e quando ele é incluído no relatório.
6. Para ambientes híbridos, se a infraestrutura local federada e o seu servidor AD FS não estiverem disponíveis, você poderá alternar temporariamente da autenticação federada para o uso da sincronização de hash de senha. Essa mudança reverterá a federação de domínio para a autenticação gerenciada até que o servidor do AD FS se torne disponível.
7. Monitorar o email quanto a contas com privilégios.
8. Certifique-se de salvar os backups de logs relevantes para investigação forense e investigação jurídica.

Para obter mais informações sobre como o Microsoft Office 365 trata os incidentes de segurança, consulte [gerenciamento de incidentes de segurança no Microsoft Office 365](#).

### Perguntas frequentes: Respostas para proteger o acesso privilegiado

**P:** O que fazer se eu ainda não implementei os componentes de acesso seguro?

**Resposta:** Defina no mínimo duas contas de vigilância, atribua o MFA a suas contas de administrador privilegiado e separe as contas de usuário das contas de administrador Global.

**P:** Após uma violação, qual é o problema superior que precisa ser abordado primeiro?

**Resposta:** Verifique se você está exigindo a autenticação mais forte para indivíduos altamente expostos.

**P:** O que acontecerá se nossos administradores com privilégios forem desativados?

**Resposta:** Crie uma conta do administrador global que está sempre atualizada.

P: O que acontecerá se houver apenas um administrador global e ele não puder ser contatado?

**Resposta:** Use uma de suas contas de vigilância para obter acesso privilegiado imediato.

P: Como posso proteger administradores dentro da minha organização?

**Resposta:** Dê acesso aos administradores para seus negócios diáários como usuários "não privilegiados" padrão.

P: Quais são as práticas recomendadas para a criação de contas de administrador no Azure AD?

**Resposta:** Reserva com privilégios de acesso para as tarefas administrativas específicas.

P: Quais ferramentas existem para reduzir o acesso de administrador persistentes?

**Resposta:** Funções de administrador Privileged Identity Management (PIM) e Azure AD.

P: Qual é a posição da Microsoft sobre a sincronização de contas de administrador no Azure AD?

**Resposta:** As contas de administrador do Nível 0 são usadas somente para contas do AD local. Essas contas normalmente não são sincronizadas com o Azure AD na nuvem. As contas de administrador do Nível 0 incluem contas, grupos e outros ativos que têm controle administrativo direto ou indireto de floresta, domínios, controladores de domínio e ativos do Active Directory local.

P: Como podemos impedir que os administradores atribuam acesso aleatório de administrador no portal?

**Resposta:** Use contas sem privilégios para todos os usuários e a maioria dos administradores. Inicie desenvolvimento de um volume da organização para determinar quais contas de administrador devem ser privilegiadas. E monitore usuários administrativos recém-criados.

## Próximas etapas

- [Microsoft Trust Center for Product Security](#) - Produtos e serviços de nuvem de recursos de segurança da Microsoft
- [Microsoft Trust Center - Compliance](#) – conjunto abrangente da Microsoft de ofertas de conformidade para serviços de nuvem
- [Orientação sobre como realizar uma avaliação de risco](#) – gerenciar requisitos de conformidade e segurança para serviços de nuvem da Microsoft

## Outros Microsoft Online Services

- [Microsoft Intune Security](#) - O Microsoft Intune oferece recursos de gerenciamento de dispositivo móvel, gerenciamento de aplicativo móvel e gerenciamento de PC na nuvem.
- [Microsoft Dynamics 365 security](#) – O Dynamics 365 é a solução baseada em nuvem da Microsoft que unifica o gerenciamento de relacionamento com clientes (CRM) e recursos de planejamento de recursos empresariais (ERP).

# Autenticação multifator e Privileged Identity Management

22/07/2020 • 4 minutes to read • [Edit Online](#)

É recomendável que você exija MFA (autenticação multifator) a todos os administradores. Isso reduz o risco de um ataque devido a uma senha comprometida.

Você pode exigir que os usuários concluam um desafio de autenticação multifator ao entrarem. Você também pode exigir que os usuários concluam um desafio de autenticação multifator quando ativam uma função no Azure Active Directory (Azure AD) Privileged Identity Management (PIM). Dessa forma, se o usuário não concluiu um desafio de autenticação multifator quando se conectasse, ele será solicitado a fazer isso por Privileged Identity Management.

## IMPORTANT

Agora, a autenticação multifator do Azure funciona apenas com contas corporativas ou de estudante, não com contas pessoais da Microsoft (geralmente uma conta pessoal que é usada para entrar nos serviços da Microsoft, como Skype, Xbox ou Outlook.com). Por isso, qualquer pessoa que usa uma conta pessoal não pode ser um administrador qualificado porque não pode usar a autenticação multifator para ativar suas funções. Se esses usuários precisarem continuar a gerenciar cargas de trabalho usando uma conta da Microsoft, eleve-os a administradores permanentes por enquanto.

## Como o PIM valida MFA

Há duas opções para validar a autenticação multifator quando um usuário ativa uma função.

A opção mais simples é contar com a autenticação multifator do Azure para usuários que estão ativando uma função privilegiada. Para fazer isso, primeiro verifique se os usuários estão licenciados, se necessário, e se foram registrados para a autenticação multifator do Azure. Para obter mais informações sobre como implantar a autenticação multifator do Azure, consulte [implantar a autenticação multifator do Azure baseada em nuvem](#). É recomendável, mas não obrigatório, que você configure o Azure AD para impor a autenticação multifator para esses usuários quando eles entram. Isso ocorre porque as verificações de autenticação multifator serão feitas pelo Privileged Identity Management si mesma.

Como alternativa, se os usuários autenticarem no local, você poderá fazer com que seu provedor de identidade seja responsável pela autenticação multifator. Por exemplo, se você tiver configurado os Serviços de Federação do AD para exigir a autenticação baseada em cartão inteligente antes de acessar o Azure AD, [Protegendo os recursos de nuvem usando a Autenticação Multifator do Azure e o AD FS](#) inclui instruções para configurar o AD FS a fim de enviar solicitações ao Azure AD. Quando um usuário tenta ativar uma função, Privileged Identity Management aceitará que a autenticação multifator já tenha sido validada para o usuário depois de receber as declarações apropriadas.

## Próximas etapas

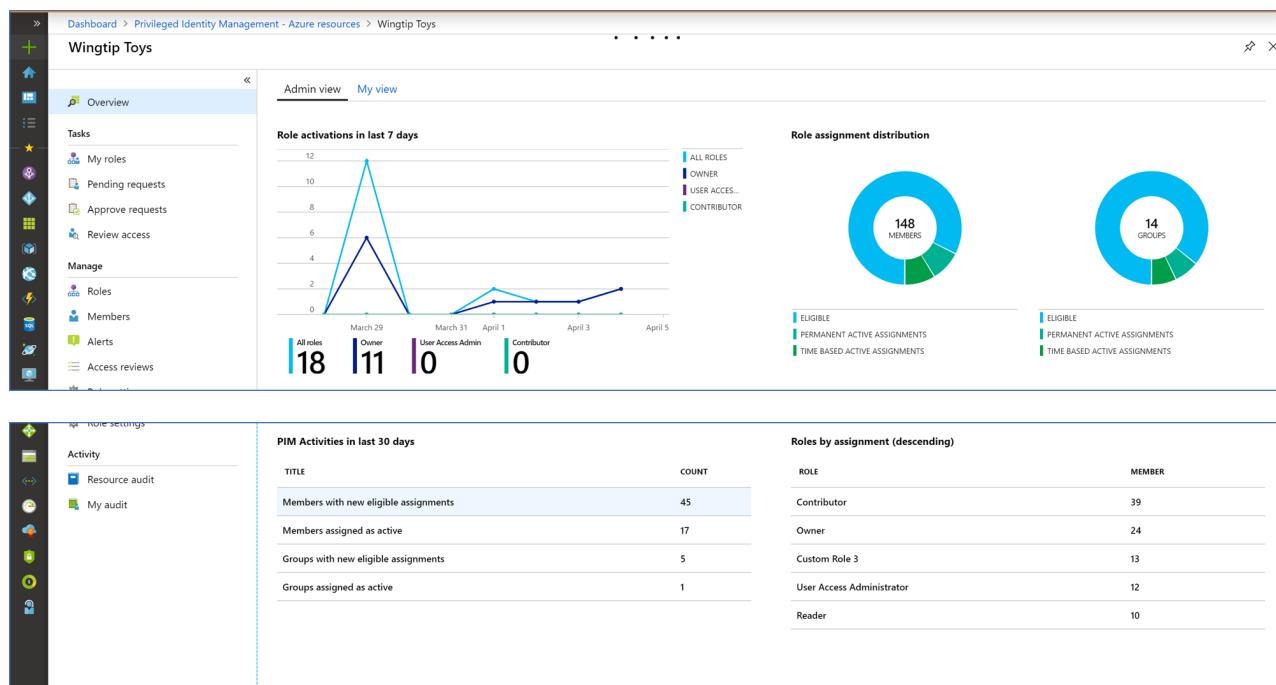
- [Definir as configurações de função do Azure AD no Privileged Identity Management](#)
- [Definir configurações de função de recurso do Azure no Privileged Identity Management](#)

# Use um painel de recursos para executar uma revisão de acesso no Privileged Identity Management

22/07/2020 • 2 minutes to read • [Edit Online](#)

Você pode usar um painel de recursos para executar uma revisão de acesso no Privileged Identity Management (PIM). O painel de exibição do administrador no Azure Active Directory (Azure AD) tem três componentes principais:

- Uma representação gráfica de ativações de função de recurso
- Gráficos que exibem a distribuição de atribuições de função por tipo de atribuição
- Uma área de dados que contém informações para novas atribuições de função



A representação gráfica das ativações de função de recurso abrange os últimos sete dias. Esses dados estão no escopo das ativações de telas e recursos selecionados para as funções mais comuns (Proprietário, Colaborador, Administrador de Acesso do Usuário) e todas as funções combinadas.

Em um lado do gráfico ativações, dois gráficos exibem a distribuição de atribuições de função por tipo de atribuição, para usuários e grupos. Você pode alterar o valor para uma porcentagem (ou vice-versa), selecionando uma fatia do gráfico.

Abaixo dos gráficos estão listados o número de usuários e grupos com novas atribuições de função nos últimos 30 dias e as funções classificadas por atribuições totais em ordem decrescente.

## Próximas etapas

- [Iniciar uma revisão de acesso para funções de recurso do Azure no Privileged Identity Management](#)

# Notificações por email no PIM

22/07/2020 • 8 minutes to read • [Edit Online](#)

Privileged Identity Management (PIM) permite que você saiba quando eventos importantes ocorrem em sua organização do Azure Active Directory (Azure AD), como quando uma função é atribuída ou ativada. Privileged Identity Management mantém você informado enviando-lhe e outros participantes notificações por email. Adicionalmente, esses emails podem incluir links para tarefas relevantes como ativar ou renovar uma função. Este artigo descreve a aparência desses emails, quando são enviados e quem recebe os emails.

## Endereço de email do remetente e linha do assunto

Os emails enviados de Privileged Identity Management para as funções de recurso do Azure AD e do Azure têm o seguinte endereço de email do remetente:

- Endereço de email: **Azure-noresponder @ Microsoft.com**
- Nome de exibição: Microsoft Azure

Esses emails incluem um prefixo **PIM** na linha de assunto. Aqui está um exemplo:

- PIM: Alain Charon atribuiu permanentemente a função de leitor de backup

## Notificações para funções do Azure AD

Privileged Identity Management envia emails quando os seguintes eventos ocorrem para funções do Azure AD:

- Quando uma ativação de função com privilégios está com aprovação pendente
- Quando uma solicitação de ativação de função com privilégios é concluída
- Quando Azure AD Privileged Identity Management está habilitado

Quem recebe esses emails para as funções do Azure AD depende da função, do evento e da configuração de notificações:

| USUÁRIO   | ATIVAÇÃO DE FUNÇÃO ESTÁ PENDENTE DE APROVAÇÃO                   | A SOLICITAÇÃO DE ATIVAÇÃO DE FUNÇÃO ESTÁ CONCLUÍDA | O PIM ESTÁ HABILITADO |
|---|---|--|-----------------------|
| Administrador de função com privilégios (Ativado/Qualificado) | Sim<br>(somente se nenhum aprovador explícito for especificado) | Sim*   | Sim                   |
| Administrador de Segurança (Ativado/Qualificado)              | Não   | Sim*   | Sim                   |
| Administrador global (Ativado/Qualificado)                    | Não   | Sim*   | Sim                   |

\*Se as [configurações de Notificações](#) estiver definida como **Habilitar**.

A seguir, é mostrado um email de exemplo enviado quando um usuário ativa uma função do Azure AD para a organização fictícia Contoso.

Contoso

Your Guest Inviter role was activated in the  
Contoso directory

**Activation details**

| Settings       | Value                    |
|----------------|--------------------------|
| Expiration:    | March 23, 2018 13:26 UTC |
| Justification: | New hire                 |

You can re-activate or cancel your role activation in the Azure Active Directory  
Privileged Identity Management extension on the Azure portal.

[Learn more about Azure AD Privileged Identity Management >](#)



[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



**Email de resumo semanal Privileged Identity Management para funções do Azure AD**

Um email de resumo Privileged Identity Management semanal para funções do Azure AD é enviado para administradores de função com privilégios, administradores de segurança e administradores globais que habilitaram o Privileged Identity Management. Este email semanal fornece um instantâneo de Privileged Identity Management atividades para a semana, bem como atribuições de função com privilégios. Ele só está disponível para organizações do Azure AD na nuvem pública. Aqui está um exemplo de e-mail:

**Subject:** Your weekly PIM digest for Contoso

**Preheader:** Here's a summary of activities over the last seven days.

**Purpose:** Weekly summary email about assignment and activation of privileged roles inside and outside of PIM.



## Your weekly PIM digest for Contoso

Thanks for using Azure Active Directory PIM (privileged identity management). Below is a breakdown of your PIM activities over the last seven days:

Users activated

20 A small gray silhouette of a person.

Users made permanent

6 A small gray silhouette of a person.

Role assignments in PIM

8 A small gray silhouette of a person.

Role assignments outside of PIM

5 A small gray silhouette of a person.

### Overview of your top roles

| Role                   | Permanent | Eligible | Action                           |
|------------------------|-----------|----------|----------------------------------|
| Global Administrator   | 4         | 20       | <a href="#">Take action &gt;</a> |
| Exchange Administrator | 12        | 5        | <a href="#">Take action &gt;</a> |
| Security Administrator | 6         | 2        | <a href="#">Take action &gt;</a> |



[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



O email inclui quatro blocos:

| BLOCO   | DESCRIÇÃO  |
|---|--|
| Usuários ativados                                       | Número de vezes que os usuários ativaram sua função qualificada dentro da organização.                                     |
| Usuários tornados permanentes                           | Número de vezes que usuários com uma atribuição qualificada tornam-se permanentes.   |
| Atribuições de função no Privileged Identity Management | Número de vezes que os usuários recebem uma função qualificada dentro Privileged Identity Management.                      |
| Atribuições de função fora do PIM                       | Número de vezes que os usuários recebem uma função permanente fora do Privileged Identity Management (dentro do Azure AD). |

A visão geral da seção de funções principais lista as cinco principais funções em sua organização com base no número total de administradores permanentes e qualificados para cada função. O link Executar ação abre o assistente do PIM, onde é possível converter administradores permanentes em administradores qualificados em lotes.

## Tempo de email para aprovações de ativação

Quando os usuários ativam sua função e a configuração de função requer aprovação, os aprovadores receberão três emails para cada aprovação:

- Solicitação para aprovar ou negar a solicitação de ativação do usuário (enviada pelo mecanismo de aprovação de solicitação)
- A solicitação do usuário é aprovada (enviada pelo mecanismo de aprovação de solicitação)
- A função do usuário é ativada (enviada por Privileged Identity Management)

Os dois primeiros emails enviados pelo mecanismo de aprovação de solicitação podem ser atrasados. Atualmente, 90% dos emails levam de três a dez minutos, mas para clientes de 1%, pode ser muito mais demorado, até quinze minutos.

Se uma solicitação de aprovação for aprovada no portal do Azure antes de o primeiro email ser enviado, o primeiro email não será disparado e outros Aprovadores não serão notificados por email da solicitação de aprovação. Pode parecer que ele não recebe um email, mas é o comportamento esperado.

## Emails do PIM para funções de recurso do Azure

Privileged Identity Management envia emails aos proprietários e aos administradores de acesso do usuário quando os seguintes eventos ocorrem para as funções de recurso do Azure:

- Quando uma atribuição de função estiver com aprovação pendente
- Quando uma função for atribuída
- Quando uma função estiver prestes a expirar
- Quando uma função for qualificada para estender
- Quando uma função estiver sendo renovada por um usuário final
- Quando uma solicitação de ativação de função for concluída

Privileged Identity Management envia emails aos usuários finais quando os seguintes eventos ocorrem para as funções de recurso do Azure:

- Quando uma função for atribuída ao usuário
- Quando a função de um usuário expirar
- Quando a função do usuário for estendida
- Quando a solicitação de ativação de função de um usuário for concluída

A seguir, é mostrado um email de exemplo enviado quando um usuário recebe uma função de recurso do Azure para a organização fictícia Contoso.

## Contoso

Alain Charon was assigned the Backup Reader role for the Pay-As-You-Go subscription

| Settings         | Value                          |
|------------------|--------------------------------|
| User or Group    | Alan Chairon                   |
| Assigned by      | isabella@example.com           |
| Justification    | New hire                       |
| Approver         | isabella@example.com           |
| Assignment start | September 1, 2018 10:15:00 GMT |
| Assignment end   | October 1, 2018 10:15:00 GMT   |

Privileged Identity Management protects your organization from accidental or malicious activity by reducing persistent access to Azure resources, providing just-in-time or time-limited access when needed.

## Próximas etapas

- Definir as configurações de função do Azure AD no Privileged Identity Management
- Aprovar ou negar solicitações para funções do Azure AD no Privileged Identity Management

# APIs do Microsoft Graph para Privileged Identity Management (versão prévia)

22/07/2020 • 2 minutes to read • [Edit Online](#)

Você pode executar tarefas do Privileged Identity Management usando as [APIs do Microsoft Graph para o Azure Active Directory](#). Este artigo descreve conceitos importantes para uso das APIs do Microsoft Graph para Privileged Identity Management.

Para obter detalhes sobre as APIs do Microsoft Graph, confira a [Referência de API do Azure AD Privileged Identity Management](#).

## IMPORTANT

APIs na versão /beta no Microsoft Graph estão em versão prévia e estão sujeitas a alterações. Não há suporte para o uso dessas APIs em aplicativos de produção.

## Permissões necessárias

Para chamar as APIs do Microsoft Graph para Privileged Identity Management, você precisará ter **uma ou mais** das seguintes permissões:

- `Directory.AccessAsUser.All`
- `Directory.Read.All`
- `Directory.ReadWrite.All`
- `PrivilegedAccess.ReadWrite.AzureAD`

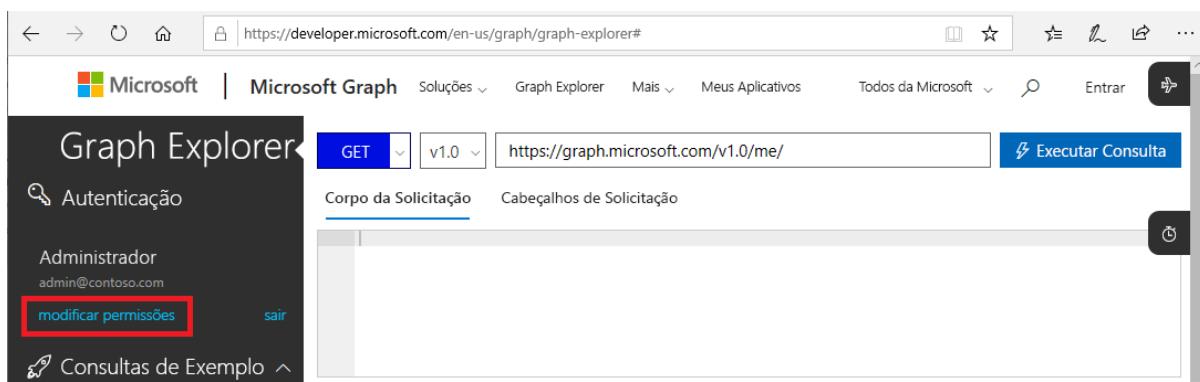
## Definir permissões

Para os aplicativos que chamam as APIs do Microsoft Graph para o Privileged Identity Management, eles precisam ter as permissões necessárias. A forma mais fácil de especificar as permissões necessárias é usando a [estrutura de consentimento do Azure AD](#).

## Definir permissões no Graph Explorer

Caso esteja usando o Graph Explorer para testar suas chamadas, você pode especificar as permissões na ferramenta.

1. Entre no [Graph Explorer](#) como um Administrador Global.
2. Clique em **modificar permissões**.



3. Marque as caixas de seleção ao lado das permissões que deseja incluir. `PrivilegedAccess.ReadWrite.AzureAD` ainda não está disponível no Graph Explorer.

The screenshot shows the Microsoft Graph Explorer interface with a modal dialog titled "Modificar Permissões". The dialog lists various API permissions with checkboxes. Some checkboxes are checked (e.g., Directory.AccessAsUser.All, Directory.Read.All, Directory.ReadWrite.All), while others are not. To the right of each permission, there is a column indicating the required role: "Administrador" (Administrator). Below the list, two informational messages are displayed in yellow boxes:

- Para alterar permissões, é necessário fazer logon novamente.
- Você selecionou permissões que somente um administrador pode conceder. Para obter acesso, um administrador pode conceder [acesso a toda a sua organização](#).

At the bottom right of the dialog are two buttons: "Modificar Permissões" (Change Permissions) and "Fechar" (Close).

4. Clique em **Modificar Permissões** para aplicar as alterações de permissão.

## Próximas etapas

- Referência de API do Azure AD Privileged Identity Management

# Implantar o Azure AD Privileged Identity Management (PIM)

22/07/2020 • 56 minutes to read • [Edit Online](#)

Este guia passo a passo descreve como planejar a implantação do Privileged Identity Management (PIM) em sua organização do Azure Active Directory (AD do Azure).

## TIP

Ao longo deste artigo, você verá itens marcados como:

:heavy\_check\_mark: a **Microsoft recomenda**

Essas são recomendações gerais e você só deverá implementá-las se elas se aplicarem às suas necessidades corporativas específicas.

## Saiba mais sobre o Privileged Identity Management

Azure AD Privileged Identity Management ajuda a gerenciar funções administrativas privilegiadas no Azure AD, recursos do Azure e outros serviços online da Microsoft. Em um mundo em que identidades com privilégios são atribuídas e esquecidas, o Privileged Identity Management fornece soluções como acesso just-in-time, fluxos de trabalho de aprovação de solicitação e revisões de acesso totalmente integradas para que você possa identificar, descobrir e impedir atividades mal-intencionadas de funções privilegiadas em tempo real. A implantação de Privileged Identity Management para gerenciar suas funções privilegiadas em toda a organização reduzirá consideravelmente o risco, ao mesmo tempo que identificando informações valiosas sobre as atividades de suas funções privilegiadas.

### Valor comercial de Privileged Identity Management

**Gerenciar riscos** - proteja sua organização aplicando o princípio do **acesso de privilégios mínimos** e do acesso just-in-time. Ao minimizar o número de atribuições permanentes de usuários para funções com privilégios e impor aprovações e MFA para elevação, você poderá reduzir bastante os riscos de segurança relacionados ao acesso com privilégios em sua organização. A aplicação de privilégios mínimos e acesso just-in-time também permitirá que você visualize um histórico de acesso a funções com privilégios e rastreie problemas de segurança à medida que eles ocorrem.

**Atender à conformidade e governança** - a implantação de Privileged Identity Management cria um ambiente para governança de identidade contínua. A elevação just-in-time de identidades com privilégios fornece uma maneira para Privileged Identity Management manter o controle das atividades de acesso privilegiado em sua organização. Você também poderá exibir e receber notificações de todas as atribuições de funções permanentes e qualificadas dentro de sua organização. Com a revisão de acesso, você pode auditar e remover regularmente identidades com privilégios desnecessários e garantir que sua organização esteja em conformidade com os mais rigorosos padrões de identidade, acesso e segurança.

**Reduza custos**- reduza os custos eliminando ineficiências, erros humanos e problemas de segurança implantando Privileged Identity Management corretamente. O resultado líquido é uma redução de crimes cibernéticos associados a identidades com privilégios que são caras e difíceis de recuperar. Privileged Identity Management também ajudará a sua organização a reduzir o custo associado à auditoria de informações de acesso quando se trata de cumprir normas e padrões.

Para obter mais informações, confira [O que é o Privileged Identity Management do Azure AD?](#).

## Requisitos de licenciamento

Para usar Privileged Identity Management, seu diretório deve ter uma das seguintes licenças pagas ou de avaliação:

- Azure AD Premium P2
- Enterprise Mobility + Security (EMS) E5
- Microsoft 365 Education A5
- Microsoft 365 Enterprise e5

Para obter mais informações, consulte [requisitos de licença para usar Privileged Identity Management](#).

## Terminologia principal

| TERMO OU CONCEITO                          | DESCRIÇÃO  |
|--|--|
| qualificado                                | Uma atribuição de função que requer que um usuário execute uma ou mais ações para usá-la. Se um usuário se qualificou para uma função, isso significa que ele poderá ativá-la quando precisar executar tarefas privilegiadas. Não há nenhuma diferença no modo de acesso concedido a uma pessoa com uma atribuição de função permanente em comparação com uma qualificada. A única diferença é que algumas pessoas não precisam desse acesso o tempo todo. |
| ativar                                     | O processo de execução de uma ou mais ações a fim de usar uma função para a qual um usuário está qualificado. As ações podem incluir a execução de uma verificação de MDA (Autenticação Multifator), fornecimento de uma justificativa comercial ou solicitação de aprovação dos aprovadores designados.   |
| Acesso JIT (Just-In-Time)                  | Um modelo no qual os usuários recebem permissões temporárias para executar tarefas privilegiadas, o que impede que usuários mal-intencionados ou não autorizados obtenham acesso após a expiração das permissões. O acesso é concedido somente quando os usuários precisam dele.   |
| princípio de acesso de privilégios mínimos | Uma prática de segurança recomendada na qual todos os usuários recebem apenas os privilégios mínimos necessários para realizar as tarefas que estão autorizados a executar. Essa prática minimiza o número de Administradores Globais usando funções de administrador específicas para determinados cenários.  |

Para saber mais, confira a [Terminologia](#).

## Visão geral de alto nível de como o Privileged Identity Management funciona

1. Privileged Identity Management é configurado para que os usuários estejam qualificados para funções privilegiadas.
2. Quando um usuário elegível precisa usar sua função privilegiada, ele ativa a função no Privileged Identity Management.
3. Dependendo das configurações de Privileged Identity Management configuradas para a função, o usuário deve concluir determinadas etapas (como executar a autenticação multifator, obter aprovação ou especificar um motivo).
4. Depois que o usuário ativar sua função com sucesso, ele receberá a função por um período de tempo predefinido.
5. Os administradores podem exibir um histórico de todas as atividades de Privileged Identity Management no

log de auditoria. Eles também podem proteger ainda mais suas organizações do Azure AD e cumprir a conformidade usando Privileged Identity Management recursos como revisões de acesso e alertas.

Para obter mais informações, confira [O que é o Privileged Identity Management do Azure AD?](#).

### **Funções que podem ser gerenciadas pelo Privileged Identity Management**

**Funções do Azure ad** – essas funções estão todas em Azure Active Directory (como administrador global, administrador do Exchange e administrador de segurança). Você pode ler mais sobre as funções e suas funcionalidades em [Permissões da função de administrador no Azure Active Directory](#). Para obter ajuda sobre como determinar quais funções devem ser atribuídas aos administradores, confira [funções com menos privilégios por tarefa](#).

**Funções de recurso do Azure** - essas funções são vinculadas a um recurso, grupo de recursos, assinatura ou grupo de gerenciamento do Azure. O Privileged Identity Management fornece acesso just-in-time a funções internas, como proprietário, administrador de acesso do usuário e colaborador, bem como [funções personalizadas](#). Para saber mais sobre funções de recurso do Azure, confira [Controle de acesso baseado em função \(RBAC\)](#).

Para obter mais informações, consulte [funções que você não pode gerenciar em Privileged Identity Management](#).

## **Planejar sua implantação**

Esta seção se concentra no que você precisa fazer antes de implantar Privileged Identity Management em sua organização. É fundamental seguir as instruções e entender os conceitos nesta seção, pois eles orientarão você na criação do melhor plano personalizado para as identidades com privilégios de sua organização.

### **Identificar os participantes**

A seção a seguir ajuda você a identificar todos os participantes envolvidos no projeto e a necessidade de confirmar, revisar ou manter-se informado sobre o projeto. Ele inclui tabelas separadas para a implantação de Privileged Identity Management para funções do Azure AD e Privileged Identity Management para funções de recurso do Azure. Adicione os participantes à tabela a seguir, conforme apropriado para sua organização.

- SO = Confirmar este projeto
- R = Revisar este projeto e fornecer comentários
- I = Informado sobre este projeto

#### **Participantes: Privileged Identity Management para funções do Azure AD**

| NOME         | FUNÇÃO  | AÇÃO   |
|--------------|---|--------|
| Nome e email | Arquiteto de identidade ou de Administrador Global do Azure<br>Um representante da equipe de gerenciamento de identidade encarregado de definir como essa alteração está alinhada com a infraestrutura de gerenciamento de identidade principal em sua organização. | SO/R/I |
| Nome e email | Proprietário do serviço / gerente de linha<br>Um representante dos proprietários de TI de um serviço ou um grupo de serviços. Eles são fundamentais para tomar decisões e ajudar a distribuir Privileged Identity Management para sua equipe.                       | SO/R/I |

| NOME                            | FUNÇÃO   | AÇÃO |
|---------------------------------|--|------|
| Nome e email                    | <b>Proprietário de segurança</b><br>Um representante da equipe de segurança que pode confirmar que o plano atende aos requisitos de segurança da organização.  | SO/R |
| Nome e email                    | <b>Supor te técnico / gerente de suporte de TI</b><br>Um representante da organização de suporte de TI que pode fornecer informações sobre a capacidade de suporte dessa mudança a partir da perspectiva da assistência técnica.                   | R/I  |
| Nome e email de usuários piloto | <b>Usuários de função com privilégios</b><br>O grupo de usuários para o qual o gerenciamento de identidades com privilégios é implementado. Eles precisarão saber como ativar suas funções quando Privileged Identity Management for implementado. | I    |

#### Participantes: Privileged Identity Management para funções de recurso do Azure

| NOME                            | FUNÇÃO  | AÇÃO   |
|---------------------------------|---|--------|
| Nome e email                    | <b>Proprietário da assinatura / recurso</b><br>Um representante dos proprietários de ti de cada assinatura ou recurso que você deseja implantar Privileged Identity Management  | SO/R/I |
| Nome e email                    | <b>Proprietário de segurança</b><br>Um representante da equipe de segurança que pode confirmar que o plano atende aos requisitos de segurança da organização.   | SO/R   |
| Nome e email                    | <b>Supor te técnico / gerente de suporte de TI</b><br>Um representante da organização de suporte de TI que pode fornecer informações sobre a capacidade de suporte dessa mudança a partir da perspectiva da assistência técnica.        | R/I    |
| Nome e email de usuários piloto | <b>Usuários da função RBAC</b><br>O grupo de usuários para o qual o gerenciamento de identidades com privilégios é implementado. Eles precisarão saber como ativar suas funções quando Privileged Identity Management for implementado. | I      |

#### Habilitar Privileged Identity Management

Como parte do processo de planejamento, primeiro você deve consentir e habilitar Privileged Identity

Management seguindo nosso artigo [começar a usar Privileged Identity Management](#). A habilitação de Privileged Identity Management fornece acesso a alguns recursos projetados especificamente para ajudar na implantação.

Se seu objetivo for implantar Privileged Identity Management para recursos do Azure, siga nosso artigo [descobrir recursos do Azure para gerenciar no Privileged Identity Management](#). Somente os proprietários de assinaturas e grupos de gerenciamento podem descobrir e integrar esses recursos no Privileged Identity Management. Depois de ser integrado, a funcionalidade PIM está disponível para proprietários em todos os níveis, incluindo grupo de gerenciamento, assinatura, grupo de recursos e recurso. Se você for um administrador global tentando implantar Privileged Identity Management para seus recursos do Azure, você pode [elevar o acesso para gerenciar todas as assinaturas do Azure](#) para conceder acesso a todos os recursos do Azure no diretório para descoberta. No entanto, aconselhamos que você obtenha aprovação de cada um dos seus proprietários de assinatura antes de gerenciar seus recursos com o Privileged Identity Management.

### Aplicar o princípio de privilégios mínimos

É importante ter certeza de que você aplicou o princípio de privilégios mínimos em sua organização para o Azure AD e suas funções de recurso do Azure.

#### Funções do Azure AD

Para as funções do Azure AD, é comum que as organizações atribuam a função de Administrador Global a um número significativo de administradores, quando a maioria dos administradores precisa apenas de uma ou duas funções de administrador específicas. As atribuições de funções privilegiadas também tendem a ser deixadas sem gerenciamento.

#### NOTE

Problemas comuns da delegação de funções:

- O administrador responsável pelo Exchange recebe a função de Administrador Global, embora precise apenas da função de Administrador do Exchange para executar o trabalho diário.
- A função de Administrador Global é atribuída a um administrador do Office porque o administrador precisa das funções de administrador de Segurança e do SharePoint e é mais fácil delegar apenas uma função.
- O administrador recebeu uma função de Administrador de Segurança para executar uma tarefa há muito tempo, mas ela nunca foi removida.

Siga estas etapas para impor o Princípio de privilégios mínimos para suas funções do Azure AD.

1. Entenda a granularidade das funções lendo e compreendendo as [funções de administrador disponíveis do Azure AD](#). Você e sua equipe também devem fazer referência às [funções de administrador por tarefa de identidade no Azure AD](#), o que explica a função de privilégios mínimos de tarefas específicas.
2. Liste quem tem função com privilégios em sua organização. Você pode usar o [Assistente de Privileged Identity Management](#) para acessar uma página semelhante à seguinte.

Discover privileged roles

Contoso

Review this list of privileged roles that exist in your directory. Select each role to see permanent or eligible users in roles.

[Learn more about privileged roles.](#)

ROLES

| ROLE                          | PERMANENT | ELIGIBLE |   |
|-------------------------------|-----------|----------|---|
| Global Administrator          | 5         | 0        | > |
| Security Administrator        | 1         | 0        | > |
| Privileged Role Administrator | 1         | 0        | > |

PERMANENT

Administrator  
admin@...

**Next**

3. Para todos os Administradores Globais da organização, descubra por que eles precisam da função. Com base na leitura da documentação anterior, se o trabalho da pessoa puder ser executado por uma ou mais funções de administrador granulares, você deverá removê-los da função de administrador global e fazer atribuições adequadamente dentro de Azure Active Directory (como referência: a Microsoft atualmente tem cerca de 10 administradores com a função de administrador global. Saiba mais em [como a Microsoft usa o Privileged Identity Management](#)).
4. Para todas as outras funções do Azure AD, examine a lista de atribuições, identifique os administradores que já não precisam da função e remova-os de suas atribuições.

Para automatizar as duas últimas etapas, você pode usar as revisões de acesso no Privileged Identity Management. Seguindo as etapas em [iniciar uma revisão de acesso para funções do Azure AD no Privileged Identity Management](#), você pode configurar uma revisão de acesso para cada função do Azure AD que tenha um ou mais membros.

**Create an access review**

Access reviews allow reviewers to attest to whether users still need to be in a role. [Learn more about access reviews here.](#)

\* Review name: Review all global administrators in the organization ✓

Description:

\* Start date: 2019-01-17  

Frequency: One time  

Duration (in days):  1  

End: Never End by Occurrences

\* Number of times: 0  

\* End date: 2019-02-17  

**Users**

Scope:  Everyone

---

\* Review role membership >  
Global Administrator

---

**Reviewers**

Reviewers: Members (self)  

Upon completion settings

Advanced settings

**Start**

Os revisores deve ser definidos como **Membros (por conta própria)**. Isso enviará um email para todos os membros na função para que eles confirmem se precisam de acesso. Você também deve ativar **Requer motivo sob aprovação** nas configurações avançadas para que os usuários possam indicar por que precisam da função. Com base nessas informações, você poderá remover usuários de funções desnecessárias e delegar funções de administrador mais granulares no caso de Administradores Globais.

As revisões de acesso dependem de emails para notificar as pessoas sobre o acesso às funções. Se você tiver contas que não têm emails vinculados com privilégios, lembre-se de preencher o campo de email secundário nessas contas. Para saber mais, confira [Atributo proxyAddresses no Azure AD](#).

#### Funções de recurso do Azure

Para assinaturas do Azure e recursos, você pode configurar um processo de revisão de acesso semelhante para revisar as funções em cada assinatura ou recurso. O objetivo desse processo é minimizar as atribuições de Administrador de Acesso do Proprietário e Usuário anexadas a cada assinatura ou recurso e, também, remover atribuições desnecessárias. No entanto, as organizações geralmente delegam essas tarefas ao proprietário de cada assinatura ou recurso porque eles têm um melhor entendimento de funções específicas (especialmente funções

personalizadas).

Se você for um administrador de TI com a função de administrador global tentando implantar Privileged Identity Management para recursos do Azure em sua organização, poderá [elevar o acesso para gerenciar todas as assinaturas do Azure](#) para obter acesso a cada assinatura. Em seguida, é possível localizar o proprietário de cada assinatura e trabalhar com ele para remover atribuições desnecessárias e minimizar a atribuição de funções do proprietário.

Os usuários com a função de proprietário de uma assinatura do Azure também podem utilizar [revisões de acesso para recursos do Azure](#) para realizar a auditoria e remover atribuições de função desnecessárias semelhantes ao processo descrito anteriormente para as funções do Azure AD.

### **Decida quais atribuições de função devem ser protegidas por Privileged Identity Management**

Depois de limpar as atribuições de função com privilégios em sua organização, você precisará decidir quais funções serão protegidas com Privileged Identity Management.

Se uma função for protegida por Privileged Identity Management, os usuários qualificados atribuídos a ela deverão elevar para usar os privilégios concedidos pela função. O processo de elevação também pode incluir a obtenção de aprovação, a execução da autenticação multifator e/ou o motivo pelo qual eles estão sendo ativados. Privileged Identity Management também pode controlar as elevações por meio de notificações e os logs de eventos de auditoria do Privileged Identity Management e do Azure AD.

Escolher quais funções proteger com Privileged Identity Management pode ser difícil e será diferente para cada organização. Esta seção fornece nossos conselhos sobre práticas recomendadas para as funções de recurso do Azure AD e do Azure.

#### **Funções do Azure AD**

É importante priorizar a proteção de funções do Azure AD que têm o maior número de permissões. Com base nos padrões de uso entre todos os clientes Privileged Identity Management, as 10 principais funções do Azure AD gerenciadas pelo Privileged Identity Management são:

1. Administrador global
2. Administrador de segurança
3. Administrador de usuários
4. Administradores do Exchange
5. Administrador do SharePoint
6. Administrador do Intune
7. Leitor de segurança
8. Administrador de serviço
9. Administrador de cobrança
10. Administrador do Skype for Business

#### **TIP**

:heavy\_check\_mark: a **Microsoft recomenda** que você gerencie todos os seus administradores globais e administradores de segurança usando Privileged Identity Management como uma primeira etapa, pois eles são aqueles que podem fazer mais danos quando comprometidos.

É importante considerar quais dados e permissões são mais confidenciais para sua organização. Por exemplo, algumas organizações podem querer proteger sua função de administrador de Power BI ou sua função de administrador de equipes usando Privileged Identity Management, pois têm a capacidade de acessar dados e/ou alterar fluxos de trabalho principais.

Se houver funções com usuários convidados atribuídos, eles estarão particularmente vulneráveis a ataques.

**TIP**

: heavy\_check\_mark: a Microsoft recomenda que você gerencie todas as funções com usuários convidados usando Privileged Identity Management para reduzir o risco associado a contas de usuário convidado comprometidas.

As funções de leitor, como o Leitor de diretório, o Leitor do centro de mensagens e o Leitor de segurança, são, às vezes, consideradas menos importantes em comparação com outras funções, pois não têm permissão de gravação. No entanto, vimos que alguns clientes também protegem essas funções porque os invasores que obtiveram acesso a essas contas podem ser capazes de ler dados confidenciais, como dados pessoais. Você deve levar isso em consideração ao decidir se as funções de leitor em sua organização precisam ser gerenciadas usando Privileged Identity Management.

**Funções de recurso do Azure**

Ao decidir quais atribuições de função devem ser gerenciadas usando Privileged Identity Management para o recurso do Azure, você deve primeiro identificar as assinaturas/recursos que são mais vitais para sua organização. Exemplos dessas assinaturas/recursos são:

- Recursos que hospedam os dados mais confidenciais
- Recursos dos quais os principais aplicativos voltados ao cliente dependem

Se você é Administrador Global e tem problemas para decidir quais assinaturas/recursos são mais importantes, entre em contato com os proprietários da assinatura em sua organização para reunir uma lista de recursos gerenciados por cada assinatura. Em seguida, trabalhe com os proprietários da assinatura para agrupar os recursos com base no nível de gravidade, no caso de eles estarem comprometidos (baixo, médio, alto). Você deve priorizar o gerenciamento de recursos com Privileged Identity Management com base nesse nível de severidade.

**TIP**

: heavy\_check\_mark: a Microsoft recomenda que você trabalhe com os proprietários de assinatura/recurso dos serviços críticos para configurar Privileged Identity Management fluxo de trabalho para todas as funções dentro de assinaturas/recursos confidenciais.

Privileged Identity Management para recursos do Azure dá suporte a contas de serviço com limite de tempo. Você deve tratar as contas de serviço exatamente da mesma forma como você trataria uma conta de usuário normal.

Para assinaturas/recursos que não são tão críticos, você não precisará configurar Privileged Identity Management para todas as funções. No entanto, você ainda deve proteger as funções proprietário e administrador de acesso do usuário com Privileged Identity Management.

**TIP**

: heavy\_check\_mark: a Microsoft recomenda que você gerencie funções de proprietário e funções de administrador de acesso de usuário de todas as assinaturas/recursos usando Privileged Identity Management.

**Decidir quais atribuições de função devem ser permanentes ou qualificáveis**

Depois de decidir a lista de funções a serem gerenciadas pelo Privileged Identity Management, você deve decidir quais usuários devem obter a função qualificada versus a função ativa permanentemente. Funções ativas permanentemente são as funções normais atribuídas por meio de Azure Active Directory e recursos do Azure, enquanto as funções qualificadas só podem ser atribuídas em Privileged Identity Management.

**TIP**

: heavy\_check\_mark: a Microsoft recomenda que você tenha zero atribuições permanentemente ativas para funções do Azure AD e funções de recurso do Azure além das duas contas de acesso de emergência de interrupção recomendadas, que devem ter a função de administrador global permanente.

Apesar de recomendarmos um administrador permanente, às vezes é difícil para as organizações conseguirem isso imediatamente. Veja alguns pontos a considerar ao tomar esta decisão:

- Frequência de elevação - se o usuário precisar da atribuição com privilégios apenas uma vez, ele não deverá ter a atribuição permanente. Por outro lado, se o usuário precisar da função de seu trabalho diário e o uso de Privileged Identity Management reduziria muito sua produtividade, eles poderão ser considerados para a função permanente.
- Casos específicos da organização - se a pessoa que recebe a função qualificada pertencer a uma equipe muito distante ou recebê-la de um executivo de alto escalão, a ponto de a comunicação e o cumprimento do processo de elevação serem difíceis, ela poderá ser considerada para a função permanente.

**TIP**

: heavy\_check\_mark: a Microsoft recomenda que você configure revisões de acesso recorrente para usuários com atribuições de função permanentes (caso você tenha algum). Saiba mais sobre a revisão de acesso recorrente na seção final deste plano de implantação

## Rascunhar suas configurações de Privileged Identity Management

Antes de implementar sua solução de Privileged Identity Management, é uma prática recomendada rascunhar suas configurações de Privileged Identity Management para cada função privilegiada que sua organização usa. Esta seção tem alguns exemplos de configurações de Privileged Identity Management para funções específicas (elas são apenas para referência e podem ser diferentes para sua organização). Cada uma dessas configurações é explicada em detalhes com as recomendações da Microsoft após as tabelas.

### Configurações de Privileged Identity Management para funções do Azure AD

| FUNÇÃO                               | EXIGIR MFA | NOTIFICAÇÃO | TÍQUETE DE INCIDENTE | EXIGIR APROVAÇÃO | APROVADO R                     | DURAÇÃO DA ATIVAÇÃO | ADMINISTRADOR PERMANENTE       |
|--------------------------------------|------------|-------------|----------------------|------------------|--------------------------------|---------------------|--------------------------------|
| Administrador global                 | ✓          | ✓           | ✓                    | ✓                | Outros administradores globais | 1 hora              | Contas de acesso de emergência |
| Administrador do Exchange            | ✓          | ✓           | ✗                    | ✗                | Nenhum                         | 2 horas             | Nenhum                         |
| Administrador de assistência técnica | ✗          | ✗           | ✓                    | ✗                | Nenhum                         | 8 horas             | Nenhum                         |

### Configurações de Privileged Identity Management para funções de recurso do Azure

| FUNÇÃO   | EXIGIR MFA | NOTIFICAÇÃO | EXIGIR APROVAÇÃO | APROVADOR                          | DURAÇÃO DA ATIVAÇÃO | ADMINISTRADORES ATIVOS | EXPIRAÇÃO ATIVA | EXPIRAÇÃO QUALIFICADA |
|--|------------|-------------|------------------|------------------------------------|---------------------|------------------------|-----------------|-----------------------|
| Proprietário de assinaturas críticas                             | ✓          | ✓           | ✓                | Outros proprietários da assinatura | 1 hora              | Nenhum                 | N/D             | 3 meses               |
| Administrador de Acesso do Usuário de assinaturas menos críticas | ✓          | ✓           | ✗                | Nenhum                             | 1 hora              | Nenhum                 | N/D             | 3 meses               |
| Colaborador de Máquina Virtual                                   | ✗          | ✓           | ✗                | Nenhum                             | 3 horas             | Nenhum                 | N/D             | 6 meses               |

A tabela a seguir descreve cada configuração.

| SETTING              | DESCRIÇÃO  |
|----------------------|--|
| Função               | Nome da função para a qual você está definindo as configurações.   |
| Exigir MFA           | <p>Se o usuário qualificado precisa executar a MFA antes de ativar a função.</p> <p>: heavy_check_mark: a Microsoft recomenda que você aplique a MFA para todas as funções de administrador, especialmente se as funções tiverem usuários convidados.</p>  |
| Notificação          | <p>Se configurado como true, o Administrador Global, o Administrador de Função com Privilégios e o Administrador de Segurança da organização receberão uma notificação por email quando um usuário qualificado ativar a função.</p> <p><b>Observação:</b> Algumas organizações não têm um endereço de email vinculado a suas contas de administrador, para obter essas notificações por email, você deve definir um endereço de email alternativo para que os administradores recebam esses emails.</p>              |
| Tíquete de incidente | <p>Se o usuário qualificado precisa registrar um número de tíquete de incidente ao ativar sua função. Essa configuração ajuda uma organização a identificar cada ativação com um número de incidente interno para atenuar ativações indesejadas.</p> <p>: heavy_check_mark: a Microsoft recomenda aproveitar os números de tíquetes de incidentes para vincular Privileged Identity Management ao seu sistema interno. Isso é particularmente útil para os aprovadores que precisam de contexto para a ativação.</p> |

| SETTING                  | DESCRIÇÃO  |
|--------------------------|--|
| Exigir aprovação         | <p>Se o usuário qualificado precisa obter aprovação para ativar a função.</p> <p>: heavy_check_mark: a Microsoft recomenda que você configure a aprovação para funções com a maior permissão. Com base nos padrões de uso de todos os Privileged Identity Management clientes, administrador global, administrador de usuário, administrador do Exchange, administrador de segurança e administrador de senha são as funções mais comuns com a configuração de aprovação.</p>  |
| Aprovador                | <p>Se a aprovação for necessária para ativar a função qualificada, liste as pessoas que deverão aprovar a solicitação. Por padrão, Privileged Identity Management define o aprovador para ser todos os usuários que são um administrador de função com privilégios, sejam eles permanentes ou qualificados.</p> <p><b>Observação:</b> Se um usuário estiver qualificado para uma função do Azure AD e um Aprovador da função, ele não poderá se aprovar.</p> <p>: heavy_check_mark: a Microsoft recomenda que você escolha aprovadores para serem aqueles que são mais especializados sobre a função específica e seus usuários frequentes, em vez de um administrador global.</p> |
| Duração da ativação      | O período de tempo que um usuário será ativado na função antes da expiração.   |
| Administrador permanente | <p>Lista de usuários que serão administradores permanentes da função (nunca precisarão ser ativados).</p> <p>: heavy_check_mark: a Microsoft recomenda que você tenha zero administrador em todas as funções, exceto os administradores globais. Leia mais sobre isso na seção deste plano sobre quem deve ser qualificado e quem deve estar permanentemente ativo.</p>  |
| Administradores ativos   | Para recursos do Azure, o administrador ativo é a lista de usuários que nunca precisarão ser ativados para usar a função. Isso não é chamado de administrador permanente, como nas funções do Azure AD, porque você pode definir um tempo de expiração para quando o usuário perder essa função.   |
| Expiração ativa          | Uma atribuição de função ativa para funções de recurso do Azure expira após esse período de tempo definido. Você pode escolher entre 15 dias, 1 mês, 3 meses, 6 meses, 1 ano ou permanentemente ativa.   |
| Expiração qualificada    | Uma atribuição de função qualificada para funções de recurso do Azure expira após esse período de tempo definido. Você pode escolher entre 15 dias, 1 mês, 3 meses, 6 meses, 1 ano ou permanentemente qualificada.   |

## Implementar sua solução

A base do planejamento adequado é a base sobre a qual você pode implantar um aplicativo com êxito com o

Azure Active Directory. Ele fornece segurança e integração inteligentes que simplificam a integração, reduzindo o tempo para implantações eficazes. Essa combinação garante que seu aplicativo seja integrado com facilidade, ao mesmo tempo que reduz o tempo de inatividade dos usuários finais.

## Identificar usuários de teste

Use esta seção para identificar um conjunto de usuários e/ou grupos de usuários para validar a implementação. Com base nas configurações escolhidas na seção de planejamento, identifique os usuários que você deseja testar para cada função.

### TIP

: heavy\_check\_mark: a **Microsoft recomenda** que você faça com que os proprietários de serviço de cada função do Azure ad sejam os usuários de teste para que possam se familiarizar com o processo e se tornar um defensor interno para a distribuição.

Nesta tabela, identifique os usuários de teste que verificarão se as configurações de cada função estão funcionando.

| NOME DA FUNÇÃO   | USUÁRIOS DE TESTE               |
|------------------|---------------------------------|
| <Nome da função> | <Usuários para testar a função> |
| <Nome da função> | <Usuários para testar a função> |

## Implementação de teste

Agora que você identificou os usuários de teste, use esta etapa para configurar Privileged Identity Management para os usuários de teste. Se sua organização quiser incorporar Privileged Identity Management fluxo de trabalho em seu próprio aplicativo interno, em vez de usar Privileged Identity Management na portal do Azure, todas as operações no Privileged Identity Management também têm suporte por meio da nossa [API do Graph](#).

### Configurar Privileged Identity Management para funções do Azure AD

1. [Defina as configurações de função do Azure ad](#) com base no que você planejou.
2. Navegue até **Funções do Azure AD**, clique em **Funções** e escolha a função que você acabou de configurar.
3. Para o grupo de usuários de teste, se eles já forem administradores permanentes, você poderá torná-los qualificados pesquisando-os e convertendo-os de permanentes em qualificados clicando nas reticências da linha. Se eles ainda não tiverem as atribuições de função, [crie uma nova atribuição qualificada](#).
4. Repita as etapas de 1 a 3 para todas as funções que você deseja testar.
5. Depois de configurar os usuários de teste, você deve enviar o link sobre a [ativação de sua função do Azure AD](#).

### Configurar Privileged Identity Management para funções de recurso do Azure

1. [Defina as configurações da função de recurso do Azure](#) para uma função dentro de uma assinatura ou recurso que você deseja testar.
2. Navegue até **Recursos do Azure** da assinatura e clique em **Funções**, escolha a função que você acabou de configurar.
3. Para o grupo de usuários de teste, se eles já forem administradores ativos, você poderá torná-los qualificados pesquisando-os e [atualize sua atribuição de função](#). Se eles ainda não tiverem a função, você pode [atribuir uma nova função](#).

4. Repita as etapas de 1 a 3 para todas as funções que você deseja testar.
5. Depois de configurar os usuários de teste, você deve enviar o link sobre a [ativação de sua função de recurso do Azure](#).

Você deve usar este estágio para verificar se todas as configurações configuradas para as funções estão funcionando corretamente. Use a tabela a seguir para documentar seus testes. Você também deve usar esse estágio para otimizar a comunicação com os usuários afetados.

| FUNÇÃO                       | COMPORTAMENTO ESPERADO DURANTE A ATIVAÇÃO   | RESULTADOS REAIS |
|------------------------------|---|------------------|
| Administrador global         | (1) Exigir o MFA<br>(2) Exigir aprovação<br>(3) O aprovador recebe a notificação e pode aprovar-a<br>(4) A função expira após o horário predefinido |                  |
| Proprietário da assinatura X | (1) Exigir o MFA<br>(2) A atribuição qualificada expira após o período de tempo configurado   |                  |

### Comunicar Privileged Identity Management com os participantes afetados

A implantação de Privileged Identity Management apresentará etapas adicionais para usuários de funções com privilégios. Embora Privileged Identity Management reduza significativamente os problemas de segurança associados a identidades com privilégios, a alteração precisa ser efetivamente comunicada antes da implantação em toda a organização. Dependendo do número de administradores afetados, as organizações geralmente optam por criar um documento interno, um vídeo ou um email sobre a alteração. Frequentemente incluídos nessas comunicações:

- O que é o PIM
- Qual é o benefício para a organização
- Quem será afetado
- Quando o PIM será implementado
- Quais etapas adicionais serão necessárias para que os usuários ativem suas funções
  - Você deve enviar links para a documentação:
  - [Ativar funções do Azure AD](#)
  - [Ativar funções de recurso do Azure](#)
- Informações de contato ou link do suporte técnico para quaisquer problemas associados ao PIM

#### TIP

:heavy\_check\_mark: a Microsoft recomenda que você configure o tempo com sua equipe de suporte/assistência técnica para orientá-las no fluxo de trabalho de Privileged Identity Management (se sua organização tiver uma equipe de suporte de TI interna). Forneça à equipe as documentações apropriadas e as informações de contato.

### Mover para ambiente de produção

Depois que o teste for concluído e bem-sucedido, move Privileged Identity Management para produção repetindo todas as etapas nas fases de teste para todos os usuários de cada função que você definiu em sua configuração de Privileged Identity Management. Para Privileged Identity Management para funções do Azure AD, as organizações geralmente testam e distribuem Privileged Identity Management para administradores globais antes de testar e distribuir Privileged Identity Management para outras funções. Enquanto isso, para o recurso do Azure, as organizações normalmente testam e distribuem Privileged Identity Management uma assinatura do Azure por vez.

## No caso de uma reversão ser necessária

Se Privileged Identity Management não funcionar conforme desejado no ambiente de produção, as etapas de reversão a seguir podem ajudá-lo a reverter para um estado válido conhecido antes de configurar Privileged Identity Management:

### Funções do Azure AD

1. Entre no [portal do Azure](#).
2. Abra **Azure ad Privileged Identity Management**.
3. Clique em **Funções do Azure AD** e, em seguida, clique em **Funções**.
4. Para cada função configurada, clique nas reticências (...) para todos os usuários com uma atribuição qualificada.
5. Clique na opção **Tornar permanente** para tornar a atribuição de função permanente.

### Funções de recurso do Azure

1. Entre no [portal do Azure](#).
2. Abra **Azure ad Privileged Identity Management**.
3. Clique em **Recursos do Azure** e, em seguida, clique em uma assinatura ou recurso que deseja reverter.
4. Clique em **Funções**.
5. Para cada função configurada, clique nas reticências (...) para todos os usuários com uma atribuição qualificada.
6. Clique na opção **Tornar permanente** para tornar a atribuição de função permanente.

## Próximas etapas após a implantação

A implantação bem-sucedida de Privileged Identity Management em produção é um avanço significativo em termos de proteção das identidades privilegiadas de sua organização. Com a implantação do Privileged Identity Management vem com recursos de Privileged Identity Management adicionais que você deve usar para segurança e conformidade.

### Use Privileged Identity Management alertas para proteger seu acesso privilegiado

Você deve utilizar a funcionalidade interna de alerta do Privileged Identity Management para proteger melhor sua organização. Para saber mais, confira [Alertas de segurança](#). Esses alertas incluem: os administradores não estão usando funções privilegiadas, as funções estão sendo atribuídas fora do Privileged Identity Management, as funções estão sendo ativadas com muita frequência e muito mais. Para proteger totalmente sua organização, confira regularmente sua lista de alertas e corrija os problemas. Você pode exibir e corrigir os alertas da seguinte maneira:

1. Entre no [portal do Azure](#).
2. Abra **Azure ad Privileged Identity Management**.
3. Clique em **Funções do Azure AD** e, em seguida, clique em **Alertas**.

#### TIP

:heavy\_check\_mark: a **Microsoft recomenda** que você lide com todos os alertas marcados com alta gravidade imediatamente. Para alertas de gravidade média e baixa, você deve se manter informado e fazer alterações se achar que existe uma ameaça à segurança.

Se algum dos alertas específicos não for útil ou não se aplicar à sua organização, você poderá descartar o alerta sempre que desejar na página de alertas. Sempre que desejar, você pode reverter esse descarte posteriormente na página de configurações do Azure AD.

### Configurar revisões de acesso recorrentes para auditar regularmente as identidades com privilégios da organização

As revisões de acesso são a melhor maneira de solicitar aos usuários designados com funções com privilégios ou revisores específicos se cada usuário precisa da identidade com privilégios. As revisões de acesso são ótimas se

você quiser reduzir a superfície de ataque e manter a conformidade. Para saber mais sobre como iniciar uma revisão de acesso, confira as [revisões de acesso das funções do Azure AD](#) e as [revisões de acesso de funções de recurso do Azure](#). Para algumas organizações, a revisão periódica do acesso é necessária para manter a conformidade com as leis e regulamentações, enquanto para outras, a revisão de acesso é a melhor maneira de impor o princípio do privilégio mínimo em toda a organização.

**TIP**

:heavy\_check\_mark: a **Microsoft recomenda** que você configure as revisões de acesso trimestral para todas as funções do Azure AD e de recursos do Azure.

Na maioria dos casos, o revisor das funções do Azure AD é o próprio usuário, enquanto o revisor das funções de recurso do Azure é o proprietário da assinatura na qual a função está. No entanto, geralmente é o caso em que as empresas têm contas com privilégios que não estão vinculadas ao endereço de email de uma pessoa em particular. Nesses casos, ninguém lê e analisa o acesso.

**TIP**

:heavy\_check\_mark: a **Microsoft recomenda** que você adicione um endereço de email secundário para todas as contas com atribuições de função com privilégios que não estejam vinculadas a um endereço de email marcado regularmente

### **Obter o máximo proveito de seu log de auditoria para aprimorar a segurança e a conformidade**

O registro de auditoria é o lugar onde você pode se atualizar e estar em conformidade com os regulamentos. O Privileged Identity Management atualmente armazena um histórico de 30 dias de todo o histórico de sua organização dentro de seu log de auditoria, incluindo:

- Ativação/desativação de funções qualificadas
- Atividades de atribuição de função dentro e fora do Privileged Identity Management
- Alterações nas configurações de funções
- Solicitar/aprovar/negar atividades para ativação de funções com configuração de aprovação
- Atualizar para alertas

Se você for um Administrador Global ou um administrador de função com privilégios, poderá acessar esses logs de auditoria. Para saber mais, confira o [histórico de auditoria para funções do Azure AD](#) e o [histórico de auditoria para funções de recurso do Azure](#).

**TIP**

:heavy\_check\_mark: a **Microsoft recomenda** que pelo menos um administrador Leia todos os eventos de auditoria semanalmente e exporte seus eventos de auditoria mensalmente.

Se você quiser armazenar automaticamente seus eventos de auditoria por um período de tempo maior, Privileged Identity Management log de auditoria será sincronizado automaticamente nos [logs de auditoria do Azure ad](#).

**TIP**

:heavy\_check\_mark: a **Microsoft recomenda** que você configure o [monitoramento de log do Azure](#) para arquivar eventos de auditoria em uma conta de armazenamento do Azure para a necessidade de segurança e conformidade.

# Começar usando o Privileged Identity Management

22/07/2020 • 5 minutes to read • [Edit Online](#)

Este artigo descreve como habilitar o PIM (Privileged Identity Management) e começar a usá-lo.

Use o Privileged Identity Management (PIM) para gerenciar, controlar e monitorar o acesso em sua organização do Azure Active Directory (AD do Azure). Com o PIM, você pode fornecer acesso necessário e Just-in-time aos recursos do Azure, aos recursos do Azure AD e a outros serviços online da Microsoft, como o Office 365 ou Microsoft Intune.

## Pré-requisitos

Para usar Privileged Identity Management, você deve ter uma das seguintes licenças:

- Azure AD Premium P2
- Enterprise Mobility + Security (EMS) E5

Para obter mais informações, consulte [requisitos de licença para usar Privileged Identity Management](#).

## Preparar o PIM para funções do Azure AD

Depois de habilitar Privileged Identity Management para seu diretório, você pode preparar Privileged Identity Management para gerenciar funções do Azure AD.

Aqui estão as tarefas que recomendamos para você se preparar para as funções do Azure AD, na ordem:

1. [Defina as configurações de função do Azure ad.](#)
2. [Dê atribuições qualificadas.](#)
3. [Permitir que usuários qualificados ativem sua função do Azure ad just-in-time.](#)

## Preparar o PIM para funções do Azure

Depois de habilitar Privileged Identity Management para seu diretório, você pode preparar Privileged Identity Management para gerenciar funções do Azure para o acesso a recursos do Azure em uma assinatura.

Aqui estão as tarefas que recomendamos para você se preparar para as funções do Azure, na ordem:

1. [Recursos de descoberta do Azure](#)
2. [Defina as configurações de função do Azure.](#)
3. [Dê atribuições qualificadas.](#)
4. [Permitir que usuários qualificados ativem suas funções do Azure just-in-time.](#)

## Navegue até as tarefas

Quando Privileged Identity Management estiver configurado, você pode aprender o seu caminho.

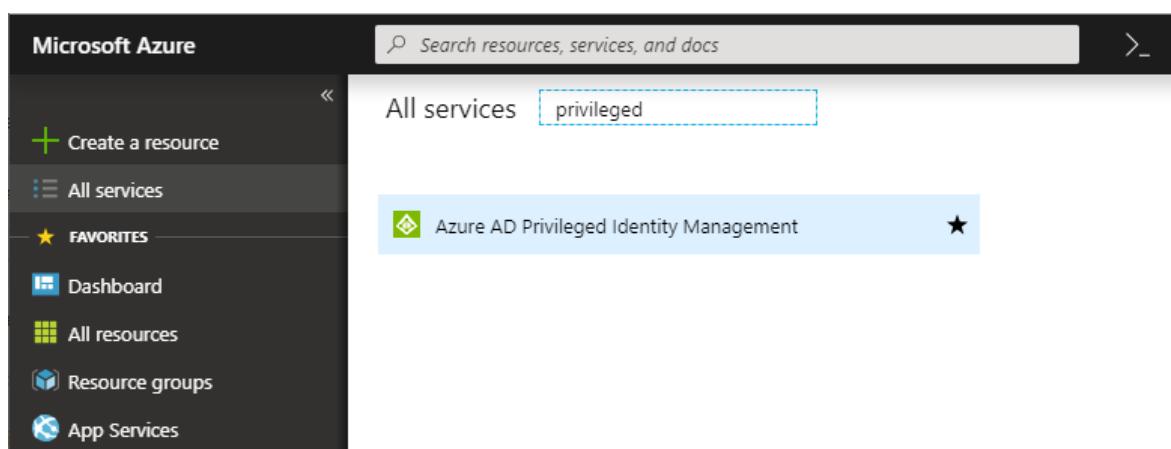
| TAREFA + GERENCIAR          | DESCRIÇÃO   |
|-----------------------------|---|
| <b>Minhas Funções</b>       | Exibe uma lista de funções qualificadas e ativas atribuídas a você. É aqui que você pode ativar as funções qualificadas atribuídas.   |
| <b>Minhas solicitações</b>  | Exibe as solicitações pendentes para ativar atribuições de função qualificadas.   |
| <b>Aprovar solicitações</b> | Exibe uma lista de solicitações de usuários para ativar funções qualificadas em seu diretório, que você pode aprovar.   |
| <b>Examinar acesso</b>      | Lista as revisões de acesso ativas atribuídas a você para completar, esteja você revisando o acesso para si mesmo ou para outra pessoa.   |
| <b>Funções do Azure AD</b>  | Exibe um painel e configurações para administradores de função com privilégios para gerenciar atribuições de função do Azure AD. Esse painel é desabilitado para todos que não forem administradores de função com privilégios. Esses usuários têm acesso a um painel especial denominado Minha exibição. O painel minha exibição exibe apenas informações sobre o usuário que está acessando o painel, e não toda a organização.         |
| <b>Recursos do Azure</b>    | Exibe um painel e configurações para administradores de função com privilégios para gerenciar atribuições de função de recurso do Azure. Esse painel é desabilitado para todos que não forem administradores de função com privilégios. Esses usuários têm acesso a um painel especial denominado Minha exibição. O painel minha exibição exibe apenas informações sobre o usuário que está acessando o painel, e não toda a organização. |

## Adicionar um bloco PIM ao painel

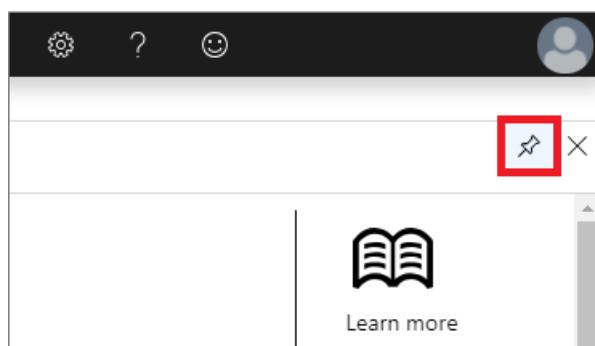
Para facilitar a abertura de Privileged Identity Management, adicione um bloco do PIM ao seu painel de portal do

Azure.

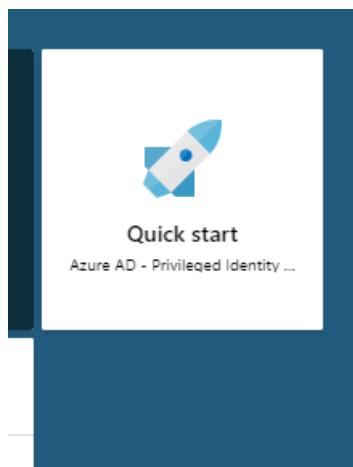
1. Entre no [portal do Azure](#).
2. Selecione todos os serviços e localize o serviço de Azure ad Privileged Identity Management .



3. Selecione o guia de início rápido do Privileged Identity Management.
4. Marque a folha fixar no painel para fixar a folha Privileged Identity Management início rápido no painel.



No painel do Azure, você verá um bloco como este:



## Próximas etapas

- [Atribuir funções do Azure AD no Privileged Identity Management](#)
- [Gerenciar o acesso a recursos do Azure no Privileged Identity Management](#)

# Assistente de segurança de funções do Azure AD no Privileged Identity Management

22/07/2020 • 4 minutes to read • [Edit Online](#)

Se você for a primeira pessoa a usar Privileged Identity Management (PIM) em sua organização do Azure Active Directory (Azure AD), verá um assistente para começar. O assistente ajuda você a entender os riscos de segurança de identidades com privilégios e a usar Privileged Identity Management para reduzir esses riscos. Você não precisará fazer nenhuma alteração nas atribuições de função existentes no assistente, se preferir fazer isso posteriormente.

## IMPORTANT

O assistente de segurança está temporariamente indisponível. Agradecemos sua paciência.

## Visão geral do assistente

Antes que sua organização comece a usar Privileged Identity Management, todas as atribuições de função são permanentes: os usuários sempre estarão nessas funções, mesmo que não precisem atualmente de seus privilégios. A primeira etapa do assistente mostra uma lista de funções com privilégios altos e quantos usuários atualmente estão nessas funções. Você poderá analisar uma função específica para saber mais sobre os usuários se um ou mais não forem familiares.

A segunda etapa do assistente lhe fornece a oportunidade de alterar as atribuições de função do administrador.

## WARNING

É importante que você tenha pelo menos um administrador global e mais de um administrador de função com privilégios com uma conta corporativa ou de estudante (não um conta Microsoft). Se houver apenas um administrador de função com privilégios, a organização não poderá gerenciar Privileged Identity Management se essa conta for excluída. Além disso, mantenha as atribuições de função permanentes se um usuário tiver um conta Microsoft (em outras palavras, uma conta que use para entrar nos serviços da Microsoft, como o Skype e o Outlook.com). Se você planeja exigir a autenticação multifator para ativação para essa função, esse usuário será bloqueado.

## Executar o assistente

1. Entre no [portal do Azure](#).
2. Abra **Azure ad Privileged Identity Management**.
3. Selecione **funções do Azure ad** e, em seguida, selecione **Assistente**.

The screenshot shows the Azure AD roles - Wizard interface. On the left, there's a sidebar with various navigation options like 'Quick start', 'Tasks', 'My roles', 'My requests', etc. Under 'Manage', 'Azure AD roles' and 'Wizard' are highlighted with red boxes. The main pane displays a three-step wizard:

- 1** Discover privileged roles
- 2** Convert members to eligible
- 3** Review the changes to your members in privileged roles

4. Selecione 1 descobrir funções com privilégios.
5. Examine a lista de funções com privilégios para ver quais usuários são permanentes ou qualificados.

The screenshot shows the 'Discover privileged roles' step in the wizard. It displays a list of roles with their respective permanent and eligible user counts:

| ROLE                          | PERMANENT | ELIGIBLE |
|-------------------------------|-----------|----------|
| Global Administrator          | 5         | 0        |
| Security Administrator        | 1         | 0        |
| Privileged Role Administrator | 1         | 0        |

A 'Next' button is located at the bottom of the screen.

6. Selecione Avançar para selecionar os usuários ou grupos que você deseja tornar qualificados.

Select the members you want to make eligible to activate their roles

GLOBAL ADMINISTRATOR

- Administrator admin@
- Isaiah IsaiahL@
- Lidia LidiaH@
- Megan MeganB@
- Nestor NestorW@

PRIVILEGED ROLE ADMINISTRATOR

- Administrator admin@

**Next**

7. Depois de selecionar os usuários ou grupos, selecione Avançar.

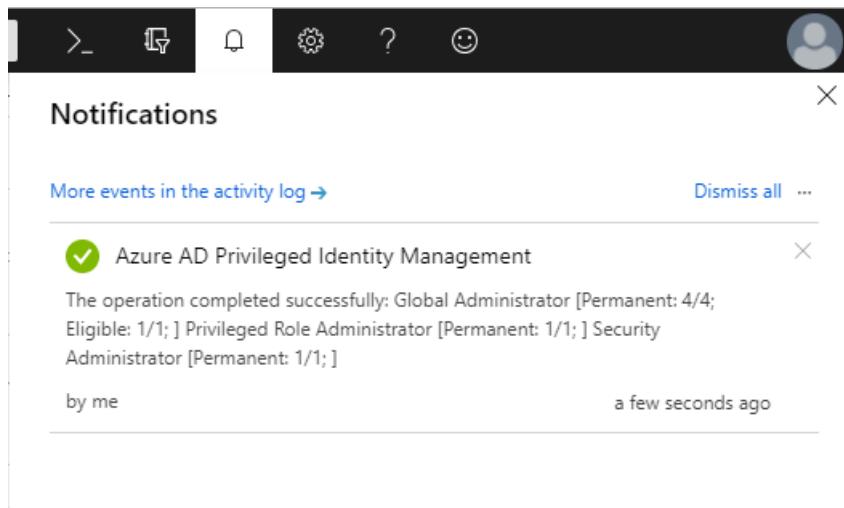
| MEMBER               | ASSIGNMENT |
|----------------------|------------|
| GLOBAL ADMINISTRATOR |            |
| Nestor<br>NestorW@   | Eligible   |

6 assignments will remain permanent, 1 assignments will be able to activate roles as needed.

**OK**

8. Selecione OK para converter as atribuições permanentes para qualificado.

Quando a conversão for concluída, você verá uma notificação.



Se você precisar converter outras atribuições de função com privilégios para qualificados, você pode executar o assistente novamente. Se você quiser usar a interface Privileged Identity Management em vez do assistente, consulte [atribuir funções do Azure AD no Privileged Identity Management](#).

## Próximas etapas

- [Atribuir funções do Azure AD no Privileged Identity Management](#)
- [Conceder acesso a outros administradores para gerenciar Privileged Identity Management](#)

# Descubra os recursos do Azure para gerenciar no Privileged Identity Management

22/07/2020 • 3 minutes to read • [Edit Online](#)

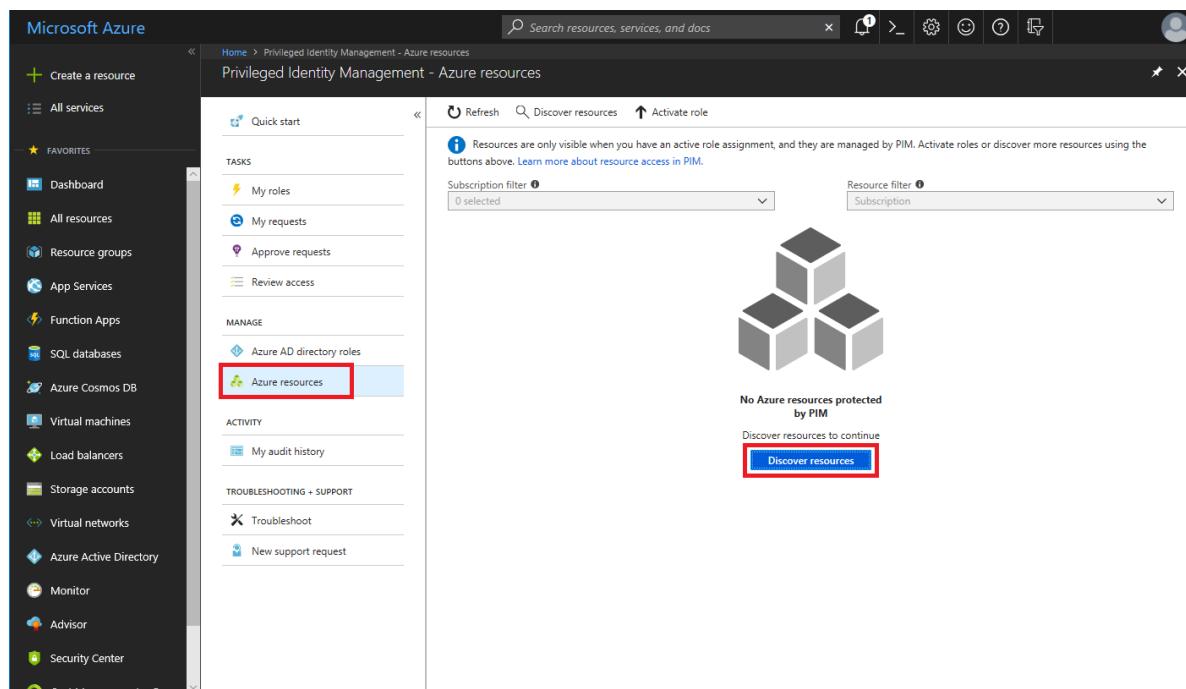
Usando o Azure Active Directory (Azure AD) Privileged Identity Management (PIM), você pode melhorar a proteção dos recursos do Azure. Isso é útil para organizações que já usam Privileged Identity Management para proteger as funções do Azure AD e para os proprietários do grupo de gerenciamento e da assinatura que estão procurando proteger os recursos de produção.

Ao configurar o Privileged Identity Management para recursos do Azure pela primeira vez, você precisa descobrir e selecionar os recursos a serem protegidos com Privileged Identity Management. Não há limite para o número de recursos que você pode gerenciar com Privileged Identity Management. No entanto, é recomendável começar com seus recursos mais importantes (produção).

## Descobrir recursos

1. Entre no [portal do Azure](#).
2. Abra **Azure ad Privileged Identity Management**.
3. Selecione **recursos do Azure**.

Se esta for a primeira vez que você usa Privileged Identity Management para recursos do Azure, você verá uma página **descobrir recursos** .



Se outro administrador em sua organização já estiver gerenciando recursos do Azure no Privileged Identity Management, você verá uma lista dos recursos que estão sendo gerenciados no momento.

The screenshot shows the Azure portal's Privileged Identity Management - Azure resources interface. On the left, there's a sidebar with various icons and links. The 'Azure resources' link under the 'Manage' section is highlighted with a red box. At the top right, there are buttons for 'Refresh', 'Discover resources' (which is also highlighted with a red box), and 'Activate role'. A message box says 'Resources are only visible when you have an active role assignment, and they are not discoverable if you do not have write permission.' Below that is a 'Resource filter' dropdown set to 'Subscription' and a search bar. The main area is titled 'RESOURCE' and shows a single result: 'Wingtip Toys' with a key icon.

4. Selecione **descobrir recursos** para iniciar a experiência de descoberta.

The screenshot shows the 'Azure resources - Discovery' page. It has a header with 'Home > Privileged Identity Management - Azure resources > Azure resources - Discovery'. Below the header are 'Refresh' and 'Manage resource' buttons. A message says 'Discover Azure resources that you have write permission to.' There are two dropdown filters: 'Resource state filter' (set to 'All') and 'Select resource types' (set to 'All'). A search bar is below them. A table lists resources:

| RESOURCE        | RESOURCE TYPE    | MANAGEMENT TYPE | TIME ONBOARDED                    |
|-----------------|------------------|-----------------|-----------------------------------|
| Marketing group | Management group | -               |                                   |
| Pay-As-You-Go   | Subscription     | Direct          | Tuesday, July 10, 2018 5:03:21 PM |

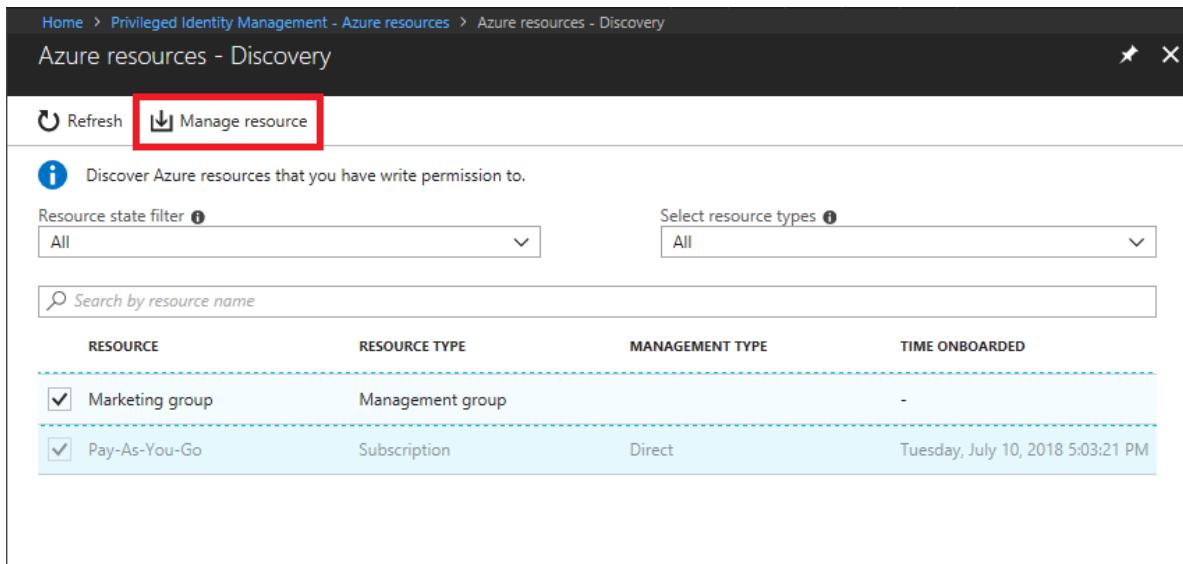
5. Na página **descoberta**, use **filtro de estado do recurso** e **selezione tipo de recurso** para filtrar os grupos de gerenciamento ou assinaturas para os quais você tem permissão de gravação. Ele provavelmente é mais fácil para começar **todos** os inicialmente.

Você só pode procurar e selecionar recursos de assinatura ou grupo de gerenciamento para gerenciar usando Privileged Identity Management. Ao gerenciar um grupo de gerenciamento ou uma assinatura no Privileged Identity Management, você também pode gerenciar seus recursos filhos.

6. Marque a caixa de seleção ao lado de quaisquer recursos não gerenciados que você deseja gerenciar.
7. Selecione **gerenciar recurso** para começar a gerenciar os recursos selecionados.

#### NOTE

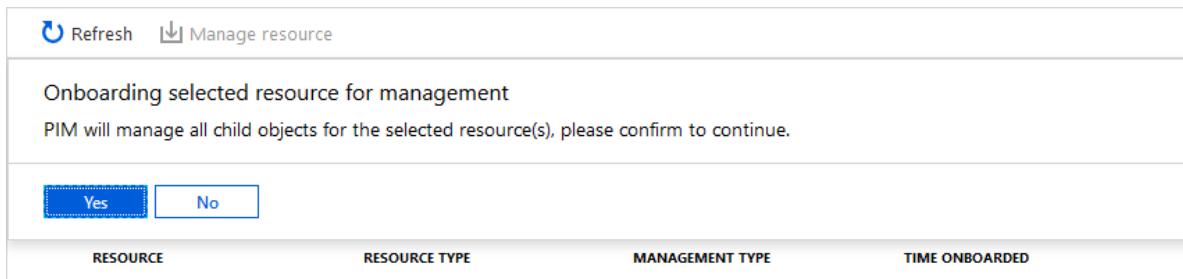
Depois que um grupo de gerenciamento ou assinatura é gerenciado, ele não pode ser não gerenciado. Isso impede que outro administrador de recursos remova Privileged Identity Management configurações.



The screenshot shows the 'Azure resources - Discovery' page. At the top, there are 'Refresh' and 'Manage resource' buttons, with 'Manage resource' being highlighted by a red box. Below them is a message: 'Discover Azure resources that you have write permission to.' There are two dropdown filters: 'Resource state filter' set to 'All' and 'Select resource types' also set to 'All'. A search bar labeled 'Search by resource name' is present. The main area displays a table with four columns: RESOURCE, RESOURCE TYPE, MANAGEMENT TYPE, and TIME ONBOARDED. Two items are listed:

| RESOURCE  | RESOURCE TYPE    | MANAGEMENT TYPE | TIME ONBOARDED                    |
|---|------------------|-----------------|-----------------------------------|
| <input checked="" type="checkbox"/> Marketing group | Management group | -               |                                   |
| <input checked="" type="checkbox"/> Pay-As-You-Go   | Subscription     | Direct          | Tuesday, July 10, 2018 5:03:21 PM |

8. Se você vir uma mensagem para confirmar a integração do recurso selecionado para gerenciamento, selecione **Sim**.



The screenshot shows a confirmation dialog titled 'Onboarding selected resource for management'. It states: 'PIM will manage all child objects for the selected resource(s), please confirm to continue.' Below the message are 'Yes' and 'No' buttons. The 'Yes' button is highlighted with a blue border. At the bottom of the screen, there is a table with the same structure as the previous one, showing the selected resources.

| RESOURCE  | RESOURCE TYPE    | MANAGEMENT TYPE | TIME ONBOARDED                    |
|---|------------------|-----------------|-----------------------------------|
| <input checked="" type="checkbox"/> Marketing group | Management group | -               |                                   |
| <input checked="" type="checkbox"/> Pay-As-You-Go   | Subscription     | Direct          | Tuesday, July 10, 2018 5:03:21 PM |

## Próximas etapas

- Definir configurações de função de recurso do Azure no Privileged Identity Management
- Atribuir funções de recurso do Azure no Privileged Identity Management

# Conceder acesso a outros administradores para gerenciar Privileged Identity Management

22/07/2020 • 3 minutes to read • [Edit Online](#)

O administrador global que habilita Privileged Identity Management (PIM) para uma organização obtém automaticamente atribuições de função e acesso a Privileged Identity Management. Ninguém mais em sua organização do Azure Active Directory (Azure AD) obtém acesso de gravação por padrão, porém, incluindo outros administradores globais. Outros administradores globais, administradores de segurança e leitores de segurança têm acesso somente leitura ao Privileged Identity Management. Para conceder acesso ao Privileged Identity Management, o primeiro usuário pode atribuir outras pessoas à função de **administrador de função com privilégios**.

## NOTE

O gerenciamento de Privileged Identity Management requer a autenticação multifator do Azure. Como as contas da Microsoft não podem se registrar para a autenticação multifator do Azure, um usuário que entra com um conta Microsoft não pode acessar Privileged Identity Management.

Certifique-se de que haja sempre pelo menos dois usuários em uma função de Administrador com Função com Privilégios, no caso de um usuário ser bloqueado ou a conta ser excluída.

## Conceder acesso para gerenciar PIM

1. Entre no [portal do Azure](#).
2. No Azure AD, abra **Privileged Identity Management**.
3. Selecione **funções do Azure ad**.
4. Selecione **funções**.

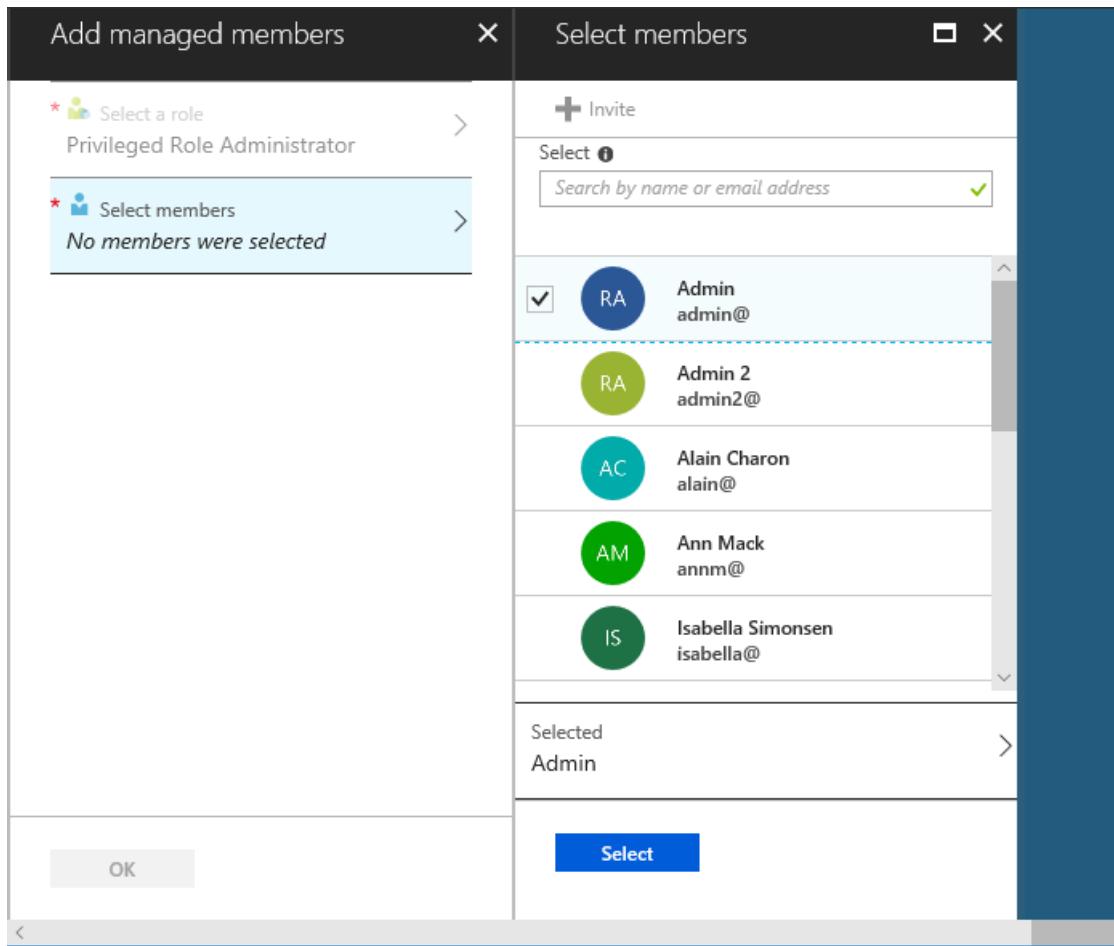
The screenshot shows the 'Azure AD roles - Roles' page under the 'Privileged Identity Management' section. On the left, there's a sidebar with various icons and links. The main area has two columns: 'Overview' and 'Manage'. The 'Manage' column is highlighted with a red box and contains a list of roles: Application Administrator, Application Developer, Authentication Administrator, Billing Administrator, Cloud Application Administrator, Cloud Device Administrator, Compliance Administrator, Conditional Access Administrator, CRM Service Administrator, Customer LockBox Access Approver, Desktop Analytics Administrator, and Device Administrators. The 'Roles' link in the 'Manage' column is also highlighted with a red box.

5. Selecione a função de administrador de função com privilégios para abrir a página Membros.

The screenshot shows the 'Privileged Role Administrator - Members' page. The top navigation bar includes 'Home', 'Privileged Identity Management', 'Azure AD directory roles - Roles', and 'Privileged Role Administrator - Members'. The main area has a 'MANAGE' sidebar with 'Members' selected and a 'TROUBLESHOOTING + SUPPORT' sidebar with 'Troubleshoot' and 'New support request'. The main content area features a header with 'Add member', 'Remove member', 'Access reviews', 'Export', and 'Refresh' buttons. Below this is a search bar labeled 'Search by member's name'. A table lists members with columns: MEMBER, EMAIL, ASSIGNMENT TYPE, and EXPIRATION. One entry is shown: Robert, Permanent, -.

6. Selecione Adicionar membro para abrir o painel Adicionar Membros gerenciados.

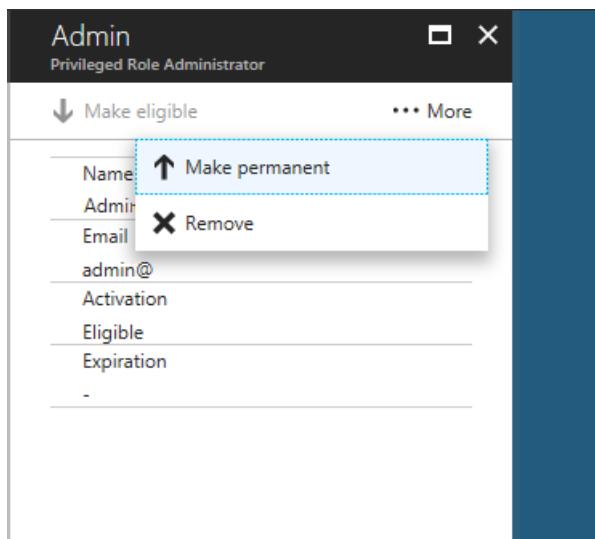
7. Selecione selecionar Membros para abrir o painel Selecionar Membros.



8. Selecione um membro e clique em **Selecionar**.
9. Selecione **OK** para tornar o membro qualificado para a função de **administrador de função com privilégios**.

Quando você atribui uma nova função a alguém em Privileged Identity Management, elas são configuradas automaticamente como **qualificadas** para ativar a função.

10. Para tornar o membro permanente, selecione o usuário na lista de membros de administrador da função com privilégios.
11. Selecione **mais e torne permanente** para tornar a atribuição permanente.

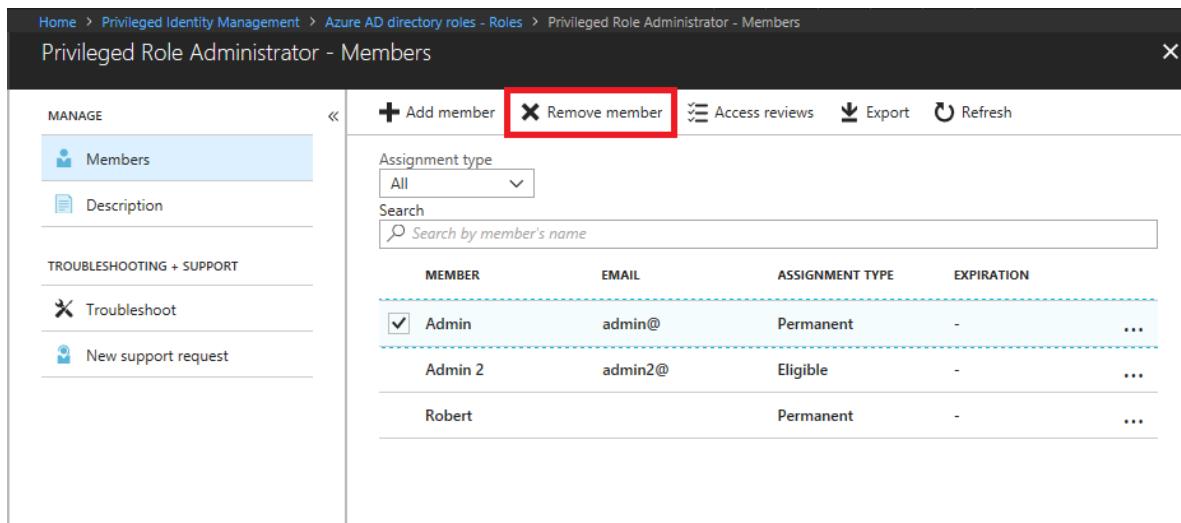


12. Enviar ao usuário um link para [começar a usar Privileged Identity Management](#).

# Remover acesso para gerenciar PIM

Antes de remover alguém da função Administrador com Função com Privilégios, sempre verifique se ainda haverá pelo menos dois usuários atribuídos a ela.

1. Entre no [portal do Azure](#).
2. Abra **Azure ad Privileged Identity Management**.
3. Selecione **funções do Azure ad**.
4. Selecione **funções**.
5. Selecione a função de **administrador de função com privilégios** para abrir a página Membros.
6. Marque a caixa de seleção ao lado do usuário que você deseja remover e, em seguida, selecione **Remover membro**.



The screenshot shows the 'Privileged Role Administrator - Members' page in the Azure portal. On the left, there's a sidebar with 'MANAGE' and 'TROUBLESHOOTING + SUPPORT' sections. The 'MANAGE' section has 'Members' selected, which is highlighted with a blue background. At the top right, there are buttons for 'Add member' (with a plus sign), 'Remove member' (with a minus sign), 'Access reviews', 'Export', and 'Refresh'. The 'Remove member' button is specifically highlighted with a red box. Below these buttons is a dropdown for 'Assignment type' set to 'All' and a search bar. The main area displays a table of members with columns: MEMBER, EMAIL, ASSIGNMENT TYPE, and EXPIRATION. There are three entries: 'Admin' (selected with a checked checkbox), 'Admin 2', and 'Robert'. Each entry has a '...' button to its right.

| MEMBER  | EMAIL   | ASSIGNMENT TYPE | EXPIRATION |
|---------|---------|-----------------|------------|
| Admin   | admin@  | Permanent       | -          |
| Admin 2 | admin2@ | Eligible        | -          |
| Robert  |         | Permanent       | -          |

7. Quando for solicitado que você confirme que deseja remover o membro da função, selecione **Sim**.

## Próximas etapas

- [Começar usando o Privileged Identity Management](#)

# Elevar o acesso para gerenciar todas as assinaturas e grupos de gerenciamento do Azure

22/07/2020 • 17 minutes to read • [Edit Online](#)

Como um Administrador Global no Azure AD (Azure Active Directory), talvez você não tenha acesso a todas as assinaturas e grupos de gerenciamento em seu diretório. Este artigo descreve maneiras de elevar o acesso para todas as assinaturas e grupos de gerenciamento.

## NOTE

Para obter informações sobre como exibir ou excluir dados pessoais, confira [Solicitações do titular dos dados do Azure para RGPD](#). Para obter mais informações sobre RGPD, confira a [seção do RGPD do portal de Confiança do Serviço](#).

## Por que você precisa elevar o acesso?

Se você for um administrador global, pode haver ocasiões em que você deseja executar as seguintes ações:

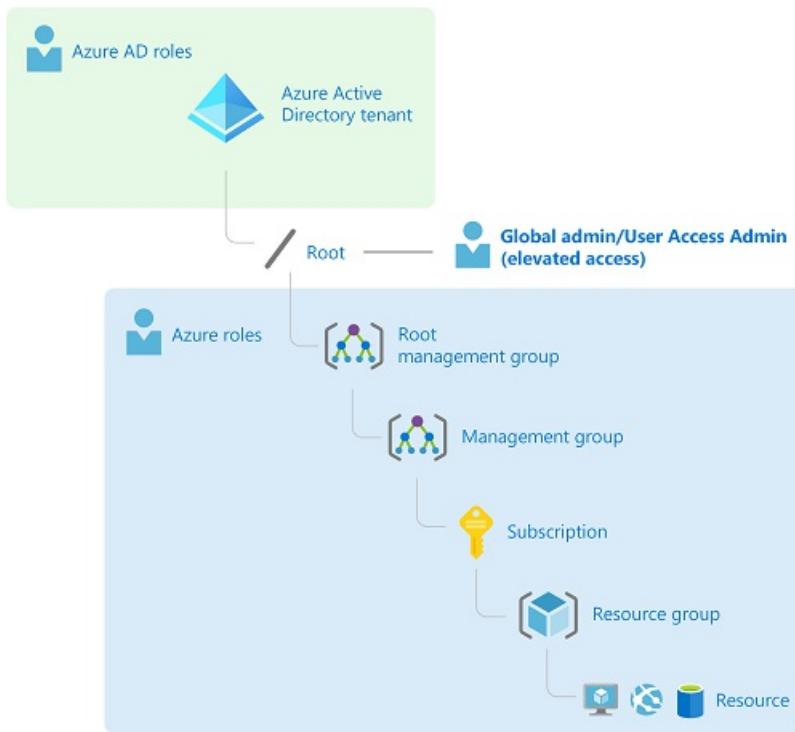
- Recuperar o acesso a um grupo de gerenciamento ou assinatura do Azure quando um usuário tiver perdido o acesso
- Conceder a outro usuário ou a você mesmo acesso a uma assinatura ou grupo de gerenciamento do Azure
- Ver todas as assinaturas ou grupos de gerenciamento do Azure em uma organização
- Permitir o acesso de um aplicativo de automação (como um aplicativo de faturamento ou de auditoria) a todas as assinaturas do Azure ou grupos de gerenciamento

## Como funciona o acesso elevado?

Os recursos do Azure AD e do Azure são protegidos independentemente um do outro. Ou seja, as atribuições de função do Azure AD não concedem acesso aos recursos do Azure, e as atribuições de função do Azure não concedem acesso ao Azure AD. No entanto, se você for um [administrador global](#) no Azure AD, você poderá atribuir a si mesmo acesso a todas as assinaturas e grupos de gerenciamento do Azure em seu diretório. Use esse recurso se você não tiver acesso aos recursos do Azuresubscription, como máquinas virtuais ou contas de armazenamento, e quiser usar o privilégio de administrador global para obter acesso a esses recursos.

Quando você elevar seu acesso, você receberá a função [Administrador de Acesso do Usuário](#) no Azure no escopo da raiz (/). Isso permite que você visualize todos os recursos e atribua acesso a qualquer assinatura ou grupo de gerenciamento no diretório. As atribuições de função de administrador de acesso do usuário podem ser removidas usando Azure PowerShell, CLI do Azure ou a API REST.

Você deve remover esse acesso elevado depois de fazer as alterações necessárias no escopo raiz.



## Portal do Azure

### Elevar o acesso de um administrador global

Siga estas etapas para elevar o acesso de um administrador global usando o portal do Azure.

1. Faça login no [Portal do Azure](#) ou no [centro de administração do Active Directory do Azure](#) como Administrador Global.

Se você estiver usando Azure AD Privileged Identity Management, [Ative sua atribuição de função de administrador global](#).

2. Abra Azure Active Directory.
3. Em gerenciar, selecione Propriedades.

4. Em Gerenciamento de acesso para recursos do Azure, defina a alternância como Sim.

Save Discard

Technical contact

Global privacy contact

Privacy statement URL

Access management for Azure resources

Admin (admin@contoso.com) can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)

Yes  No

[Manage Security defaults](#)

Quando você define a alternância para **Sim**, você recebe a função Administrador de acesso do usuário no RBAC do Azure no escopo raiz (/). Isso concede a você permissão para atribuir funções a todas as assinaturas e grupos de gerenciamento do Azure associados a esse diretório do AD do Azure. Essa alternância está disponível apenas para usuários com a função de administrador global no Azure AD.

Quando você define a alternância como **Não**, a função Administrador de Acesso do Usuário no RBAC do Azure é removida da sua conta de usuário. Você não pode mais atribuir funções a todas as assinaturas e grupos de gerenciamento do Azure associados a esse diretório do AD do Azure. Você pode exibir e gerenciar somente as assinaturas do Azure e os grupos de gerenciamento aos quais você recebeu acesso.

**NOTE**

Se você estiver usando [Privileged Identity Management](#), a desativação de sua atribuição de função não alterará o **Gerenciamento de acesso para recursos do Azure** alternar para **não**. Para manter o acesso com privilégios mínimos, recomendamos que você defina essa alternância como **não** antes de desativar sua atribuição de função.

5. Clique em **Salvar**, para salvar suas configurações.

Essa configuração não é uma propriedade global, aplicando-se somente ao usuário conectado no momento. Você não pode elevar o acesso para todos os membros da função de Administrador Global.

6. Saia e entre novamente para atualizar o seu acesso.

Agora você deve ter acesso a todas as assinaturas e grupos de gerenciamento em seu diretório. Ao exibir o painel de controle de acesso (IAM), você notará que recebeu a função Administrador de acesso do usuário no escopo raiz.

|                          |            | Role                      | Permissions                                  |
|--------------------------|------------|---------------------------|--|
| <input type="checkbox"/> | SA         | Subscription Admins Group | Owner ⓘ This resource                        |
| <input type="checkbox"/> | AM         | User                      | Reader ⓘ This resource                       |
| <input type="checkbox"/> | App2       | App                       | Reader ⓘ This resource                       |
| <input type="checkbox"/> | azure-user | User                      | Reader ⓘ This resource                       |
| <input type="checkbox"/> | Alain      | User                      | Storage Blob Data Reader ⓘ This resource     |
| <input type="checkbox"/> | Admin      | User                      | User Access Administrator ⓘ Root (Inherited) |
| <input type="checkbox"/> | MS-PIM     | App                       | User Access Administrator ⓘ This resource    |

7. Faça as alterações que você precisa fazer em acesso elevado.

Para obter informações sobre como atribuir funções, consulte [Adicionar ou remover atribuições de função do Azure usando o portal do Azure](#). Se você estiver usando Privileged Identity Management, consulte [descobrir recursos do Azure para gerenciar ou atribuir funções de recurso do Azure](#).

8. Execute as etapas na seção a seguir para remover o acesso elevado.

### Remover acesso elevado

Para remover a atribuição de função de administrador de acesso do usuário no escopo raiz (`/`), siga estas etapas.

1. Entre como o mesmo usuário que foi usado para elevar o acesso.
2. Na lista de navegação, clique em **Azure Active Directory**, depois clique em **Propriedades**.
3. Defina a alternância de **Gerenciamento de acesso para recursos do Azure** de volta para **não**. Como essa é uma configuração por usuário, você deve estar conectado como o mesmo usuário que foi usado para elevar o acesso.

Se você tentar remover a atribuição de função de administrador de acesso do usuário no painel controle de acesso (IAM), verá a seguinte mensagem. Para remover a atribuição de função, você deve definir a alternância de volta para **não** ou usar Azure PowerShell, CLI do Azure ou a API REST.

[Add](#) [Edit columns](#) [Refresh](#) | [Remove](#) | [Got feedback?](#)

Remove role assignments  
Role assignments created at root scope must be removed by using the command line. [Learn more](#)

**OK**

| Storage Blob Data Reader            |        |       |  |
|-------------------------------------|--------|-------|--|
| <input type="checkbox"/>            | AC     | Alain | User   |
|                                     |        |       | Storage Blob Data Reader ⓘ This resource     |
| User Access Administrator           |        |       |  |
| <input checked="" type="checkbox"/> | A2     | Admin | User   |
|                                     |        |       | User Access Administrator ⓘ Root (Inherited) |
| <input type="checkbox"/>            | MS-PIM | App   | User Access Administrator ⓘ This resource    |

#### 4. Saia como administrador global.

Se você estiver usando Privileged Identity Management, desative sua atribuição de função de administrador global.

##### NOTE

Se você estiver usando [Privileged Identity Management](#), a desativação de sua atribuição de função não alterará o **Gerenciamento de acesso para recursos do Azure** alternar para **não**. Para manter o acesso com privilégios mínimos, recomendamos que você defina essa alternância como **não** antes de desativar sua atribuição de função.

## Azure PowerShell

##### NOTE

Este artigo foi atualizado para usar o novo módulo Az do Azure PowerShell. Você ainda pode usar o módulo AzureRM, que continuará a receber as correções de bugs até pelo menos dezembro de 2020. Para saber mais sobre o novo módulo Az e a compatibilidade com o AzureRM, confira [Apresentação do novo módulo Az do Azure PowerShell](#). Para obter instruções de instalação do módulo Az, confira [Instalar o Azure PowerShell](#).

### Listar atribuição de função no escopo raiz (/)

Para listar a atribuição de função de administrador de acesso do usuário para um usuário no escopo raiz (`/`), use o comando [Get-AzRoleAssignment](#).

```
Get-AzRoleAssignment | where {$_._RoleDefinitionName -eq "User Access Administrator" `  
-and $_.SignInName -eq "<username@example.com>" -and $_.Scope -eq "/"}  
-
```

|                    |   |   |
|--------------------|---|---|
| RoleAssignmentId   | : | /providers/Microsoft.Authorization/roleAssignments/11111111-1111-1111-1111-111111111111 |
| Scope              | : | /   |
| DisplayName        | : | username  |
| SignInName         | : | username@example.com  |
| RoleDefinitionName | : | User Access Administrator   |
| RoleDefinitionId   | : | 18d7d88d-d35e-4fb5-a5c3-7773c20a72d9  |
| ObjectId           | : | 22222222-2222-2222-2222-222222222222  |
| ObjectType         | : | User  |
| CanDelegate        | : | False   |

## Remover acesso elevado

Para remover a atribuição de função de administrador de acesso do usuário para você mesmo ou outro usuário no escopo raiz ( / ), siga estas etapas.

1. Entre como um usuário que possa remover o acesso com privilégios elevados. Esse pode ser o mesmo usuário que foi usado para elevar o acesso ou outro administrador global com acesso elevado no escopo raiz.
2. Use o comando [Remove-AzRoleAssignment](#) para remover a atribuição de função de Administrador de Acesso do Usuário.

```
Remove-AzRoleAssignment -SignInName <username@example.com> `  
-RoleDefinitionName "User Access Administrator" -Scope "/"
```

## CLI do Azure

### Listar atribuição de função no escopo raiz (/)

Para listar a atribuição de função de administrador de acesso do usuário para um usuário no escopo raiz ( / ), use o comando [AZ role Assignment List](#) .

```
az role assignment list --role "User Access Administrator" --scope "/"
```

```
[  
 {  
   "canDelegate": null,  
   "id": "/providers/Microsoft.Authorization/roleAssignments/11111111-1111-1111-1111-111111111111",  
   "name": "11111111-1111-1111-111111111111",  
   "principalId": "22222222-2222-2222-2222-222222222222",  
   "principalName": "username@example.com",  
   "principalType": "User",  
   "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-  
7773c20a72d9",  
   "roleDefinitionName": "User Access Administrator",  
   "scope": "/",  
   "type": "Microsoft.Authorization/roleAssignments"  
 }  
]
```

## Remover acesso elevado

Para remover a atribuição de função de administrador de acesso do usuário para você mesmo ou outro usuário no escopo raiz ( / ), siga estas etapas.

1. Entre como um usuário que possa remover o acesso com privilégios elevados. Esse pode ser o mesmo usuário que foi usado para elevar o acesso ou outro administrador global com acesso elevado no escopo raiz.
2. Use o comando [AZ role Assignment Delete](#) para remover a atribuição de função de administrador de acesso do usuário.

```
az role assignment delete --assignee username@example.com --role "User Access Administrator" --scope  
"/"
```

## API REST

## Elevar o acesso de um administrador global

Use as etapas básicas a seguir para elevar o acesso de um Administrador global usando a API REST.

1. Usando REST, chame `elevateAccess`, que concede a você a função de administrador de acesso do usuário no escopo raiz (`/`).

```
POST https://management.azure.com/providers/Microsoft.Authorization/elevateAccess?api-version=2016-07-01
```

2. Faça as alterações que você precisa fazer em acesso elevado.

Para obter informações sobre como atribuir funções, consulte [Adicionar ou remover atribuições de função do Azure usando a API REST](#).

3. Execute as etapas em uma seção posterior para remover o acesso elevado.

### Listar atribuições de função no escopo raiz (/)

Você pode listar todas as atribuições de função para um usuário no escopo raiz (`/`).

- Chame `GET roleAssignments`, em que `{objectIdOfUser}` é a ID de objeto do usuário cujas atribuições de função que você deseja recuperar.

```
GET https://management.azure.com/providers/Microsoft.Authorization/roleAssignments?api-version=2015-07-01&$filter=principalId+eq+'{objectIdOfUser}'
```

### Listar atribuições de negação no escopo raiz (/)

Você pode listar todas as atribuições de negação para um usuário no escopo raiz (`/`).

- Chame `GET denyAssignments`, em que `{objectIdOfUser}` é a ID de objeto do usuário cujas atribuições de negação você deseja recuperar.

```
GET https://management.azure.com/providers/Microsoft.Authorization/denyAssignments?api-version=2018-07-01-preview&$filter=gdprExportPrincipalId+eq+'{objectIdOfUser}'
```

## Remover acesso elevado

Quando você chama `elevateAccess`, você cria uma atribuição de função para si mesmo, para revogar esses privilégios, é necessário remover a atribuição de função de administrador de acesso do usuário para você mesmo no escopo raiz (`/`).

1. Chame `GET roleDefinitions`, em que `roleName` é igual a Administrador de Acesso do Usuário, para determinar a ID do nome da função de Administrador de Acesso do Usuário.

```
GET https://management.azure.com/providers/Microsoft.Authorization/roleDefinitions?api-version=2015-07-01&$filter=roleName+eq+'User Access Administrator'
```

```

{
  "value": [
    {
      "properties": {
        "roleName": "User Access Administrator",
        "type": "BuiltInRole",
        "description": "Lets you manage user access to Azure resources.",
        "assignableScopes": [
          "/"
        ],
        "permissions": [
          {
            "actions": [
              "*/*",
              "Microsoft.Authorization/*",
              "Microsoft.Support/*"
            ],
            "notActions": []
          }
        ],
        "createdOn": "2001-01-01T08:00:00.000000Z",
        "updatedOn": "2016-05-31T23:14:04.6964687Z",
        "createdBy": null,
        "updatedBy": null
      },
      "id": "/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
      "type": "Microsoft.Authorization/roleDefinitions",
      "name": "18d7d88d-d35e-4fb5-a5c3-7773c20a72d9"
    }
  ],
  "nextLink": null
}

```

Salve a ID do parâmetro `name`, nesse caso: `18d7d88d-d35e-4fb5-a5c3-7773c20a72d9`.

2. Você também precisa listar a atribuição de função para o administrador de diretório no escopo do diretório. Listar todas as atribuições no escopo de diretório para o `principalId` do administrador de diretório que fez a chamada de acesso elevar. Isso listará todas as atribuições no diretório para o `objectId`.

```
GET https://management.azure.com/providers/Microsoft.Authorization/roleAssignments?api-version=2015-07-01&$filter=principalId+eq+'{objectId}'
```

#### NOTE

Um administrador de diretório não deve ter muitas atribuições, se a consulta anterior retornar muitas atribuições, você também pode consultar todas as atribuições apenas no nível do escopo do diretório e, em seguida, filtrar os resultados:

```
GET https://management.azure.com/providers/Microsoft.Authorization/roleAssignments?api-version=2015-07-01&$filter=atScope()
```

3. As chamadas anteriores retornam uma lista de atribuições de função. Encontre a atribuição de função em que o escopo é `"/"` e o `roleDefinitionId` termina com o ID do nome da função que você encontrou na etapa 1 e `principalId` corresponde ao `objectId` do administrador de diretório.

Atribuição de função de amostra:

```
{  
    "value": [  
        {  
            "properties": {  
                "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",  
                "principalId": "{objectID}",  
                "scope": "/",  
                "createdOn": "2016-08-17T19:21:16.3422480Z",  
                "updatedOn": "2016-08-17T19:21:16.3422480Z",  
                "createdBy": "22222222-2222-2222-2222-222222222222",  
                "updatedBy": "22222222-2222-2222-2222-222222222222"  
            },  
            "id": "/providers/Microsoft.Authorization/roleAssignments/11111111-1111-1111-1111-111111111111",  
            "type": "Microsoft.Authorization/roleAssignments",  
            "name": "11111111-1111-1111-111111111111"  
        }  
    ],  
    "nextLink": null  
}
```

Novamente, salve a ID do `name` parâmetro, neste caso, `11111111-1111-1111-111111111111`.

4. Por fim, use a ID da atribuição de função para remover a atribuição adicionada por `elevateAccess`:

```
DELETE https://management.azure.com/providers/Microsoft.Authorization/roleAssignments/11111111-1111-1111-111111111111?api-version=2015-07-01
```

## Próximas etapas

- [Entender as diferentes funções](#)
- [Adicionar ou remover atribuições de função do Azure usando a API REST](#)

# Ativar minhas funções do Azure AD no PIM

22/07/2020 • 13 minutes to read • [Edit Online](#)

O Azure AD (Azure Active Directory) PIM (Privileged Identity Management) simplifica a forma como as empresas gerenciam o acesso privilegiado a recursos no Azure AD e em outros serviços online da Microsoft, como o Office 365 ou o Microsoft Intune.

Se você tiver se tornado qualificado para uma função administrativa, deverá ativar a atribuição de função quando precisar executar ações privilegiadas. Por exemplo, se você ocasionalmente gerencia recursos do Office 365, administradores de função com privilégios de sua organização podem não o tornar um Administrador Global permanente, pois essa função também afeta outros serviços. Em vez disso, eles o tornam qualificado para funções do Azure AD, como Administrador do Exchange Online. Você pode solicitar a ativação da função quando precisar de seus privilégios e terá controle de administrador por um período predeterminado.

Este artigo é para os administradores que precisam ativar sua função do Azure AD no Privileged Identity Management.

## Determinar sua versão do PIM

A partir de novembro de 2019, a parte das funções do Azure AD da Privileged Identity Management está sendo atualizada para uma nova versão que corresponde às experiências de funções de recurso do Azure. Isso cria recursos adicionais, bem como [as alterações na API existente](#). Enquanto a nova versão está sendo distribuída, os procedimentos que você seguir neste artigo dependem da versão do Privileged Identity Management que você tem atualmente. Siga as etapas nesta seção para determinar qual versão do Privileged Identity Management você tem. Depois de saber sua versão do Privileged Identity Management, você pode selecionar os procedimentos neste artigo que correspondem a essa versão.

1. Entre no [portal do Azure](#) com a função de **administrador de função com privilégios**.
2. Abra **Azure ad Privileged Identity Management**. Se você tiver uma faixa na parte superior da página Visão geral, siga as instruções na **nova guia versão** deste artigo. Caso contrário, siga as instruções na **guia versão anterior**.

- [Nova versão](#)
- [Versão anterior](#)

# Ativar uma função

Quando você precisar assumir uma função do Azure AD, poderá solicitar a ativação abrindo **minhas funções** no Privileged Identity Management.

1. Entre no [portal do Azure](#).
2. Abra **Azure ad Privileged Identity Management**. Para obter informações sobre como adicionar o bloco Privileged Identity Management ao seu painel, consulte [começar a usar o Privileged Identity Management](#).
3. Selecione **minhas funções**, em seguida, selecione **funções do Azure ad** para ver uma lista de suas funções qualificadas do Azure AD.

| Role                         | Scope     | Membership | End time  | Action                            |
|------------------------------|-----------|------------|-----------|-----------------------------------|
| Authentication Administrator | Directory | Direct     | Permanent | <a href="#">Activate   Extend</a> |
| Device Join                  | Directory | Direct     | Permanent | <a href="#">Activate   Extend</a> |

4. Na lista **funções do Azure ad**, localize a função que você deseja ativar.

| Role                         | Scope     | Membership | End time  | Action                            |
|------------------------------|-----------|------------|-----------|-----------------------------------|
| Authentication Administrator | Directory | Direct     | Permanent | <a href="#">Activate   Extend</a> |
| Device Join                  | Directory | Direct     | Permanent | <a href="#">Activate   Extend</a> |

5. Selecione **Ativar** para abrir a página ativar.

Activate - Application Administrator

Privileged Identity Management | Azure AD roles

Roles  Activate Status

Custom activation start time

Duration (hours)

\*Reason (max 500 characters)

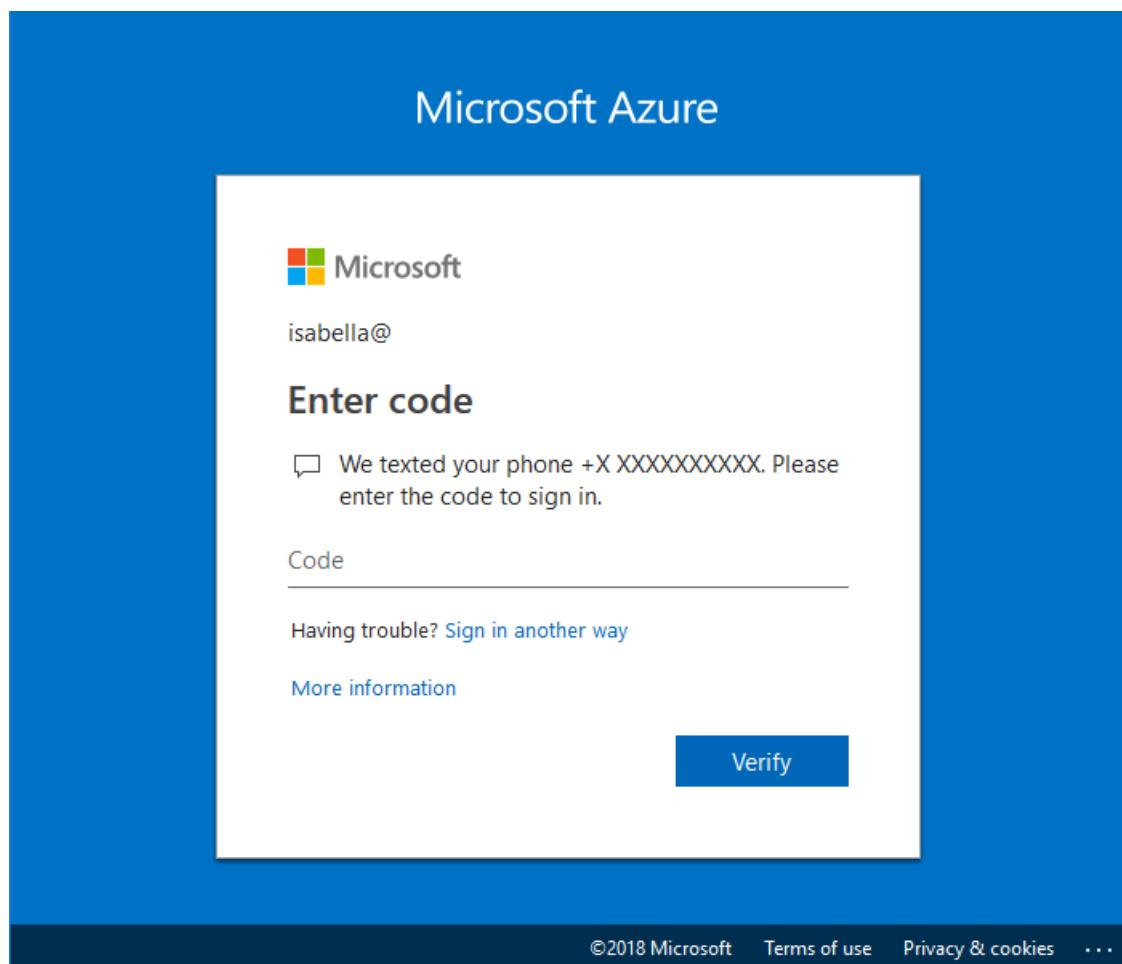
Activate Cancel

6. Se sua função exigir autenticação multifator, selecione **Verificar sua identidade antes de prosseguir**.

Você só precisa se autenticar uma vez por sessão.

The screenshot shows two overlapping windows. The left window is titled 'Activate' and has a yellow header bar with the text 'Verify your identity before proceeding →'. It contains fields for 'Assignment details', 'Scope' (set to 'Pay-As-You-Go'), 'Start time' (set to 2018-08-31 at 12:43:06 PM), 'duration (hours)' (set to 8), and 'Reason (max 500 characters)'. A red error message at the bottom states: 'Activation reason is required. Maximum supported text is 500 characters. The value should not be empty.' The right window is titled 'Verify my identity' and has the subtitle 'BizTalk Contributor'. It contains the text: 'Before you activate this role, verify your identity with Azure Multi-Factor Authentication. If you haven't registered with Azure MFA yet, we'll help you do that.' Below this is a button labeled 'Verify my identity' with an exclamation mark icon.

7. Selecione **verificar minha identidade** e siga as instruções para fornecer verificação de segurança adicional.

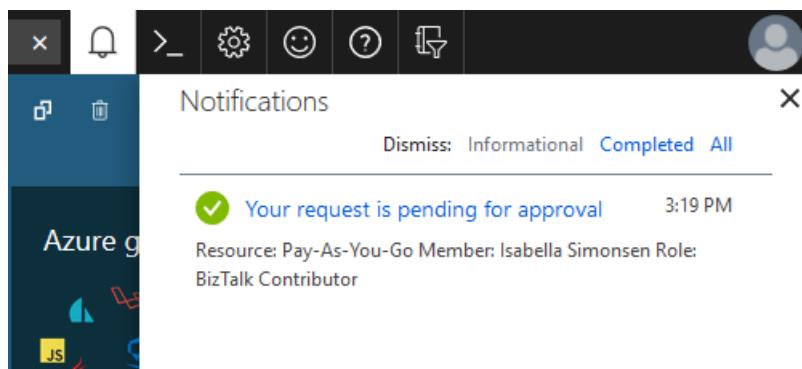


8. Se você quiser especificar um escopo reduzido, selecione **escopo** para abrir o painel de filtro. No painel filtro, você pode especificar os recursos do Azure AD aos quais você precisa acessar. É uma prática

recomendada solicitar acesso apenas aos recursos de que você precisa.

9. Se necessário, especifique uma hora de início de ativação personalizada. A função do Azure AD seria ativada após a hora selecionada.
10. Na caixa **Motivo**, insira o motivo da solicitação de ativação.
11. Selecione **Ativar**.

Se a [função exigir aprovação](#) para ser ativada, uma notificação será exibida no canto superior direito do seu navegador informando que a solicitação está com a aprovação pendente.



## Exibir o status de suas solicitações

Você pode exibir o status das suas solicitações pendentes a serem ativadas.

1. Abra o Azure AD Privileged Identity Management.
2. Selecione **minhas solicitações** para ver uma lista de suas funções do Azure AD e das solicitações de função de recurso do Azure.

A screenshot of the Microsoft Azure portal. At the top, there is a navigation bar with "Microsoft Azure" and a search bar. Below the navigation bar, the URL shows "Home > Privileged Identity Management > My requests - Azure AD roles".

**My requests - Azure AD roles**

Privileged Identity Management - My requests

**My requests**

- Azure AD roles**
- Azure resources

**Troubleshooting + Support**

- Troubleshoot
- New support request

**Role**      **Group**      **Member**

|                              |  |  |
|------------------------------|--|--|
| Authentication Administrator |  |  |
|------------------------------|--|--|

3. Role para a direita para exibir o **Status da solicitação** coluna.

## Cancelar uma solicitação pendente

Caso não precise da ativação de uma função que requer aprovação, você pode cancelar uma solicitação pendente a qualquer momento.

1. Abra o Azure AD Privileged Identity Management.
2. Selecione **minhas solicitações**.
3. Para a função que você deseja cancelar, selecione o link **Cancelar**.

Quando você selecionar cancelar, a solicitação será cancelada. Para ativar a função novamente, você precisará enviar uma nova solicitação de ativação.

The screenshot shows a table with three columns: START TIME, REQUEST STATUS, and ACTION. There is one row of data. The 'REQUEST STATUS' column contains the text 'PendingApproval'. The 'ACTION' column contains a blue button labeled 'Cancel', which is highlighted with a red rectangular border. A horizontal scrollbar is visible below the table.

| START TIME             | REQUEST STATUS  | ACTION        |
|------------------------|-----------------|---------------|
| 8/31/2018, 3:19:36 ... | PendingApproval | <b>Cancel</b> |

## Solucionar problemas

### As permissões não são concedidas depois de ativar uma função

Quando você ativa uma função no Privileged Identity Management, a ativação pode não ser propagada instantaneamente para todos os portais que exigem a função privilegiada. Às vezes, mesmo quando a alteração é propagada, o cache da web em um portal pode fazer com que a alteração não entre em vigor de imediato. Se a ativação estiver atrasada, aqui está o que você deve fazer.

1. Saia do portal do Azure e entre novamente.
2. Em Privileged Identity Management, verifique se você está listado como o membro da função.

## Próximas etapas

- [Ativar minhas funções do Azure AD no Privileged Identity Management](#)

# Ativar minhas funções de recurso do Azure no Privileged Identity Management

22/07/2020 • 5 minutes to read • [Edit Online](#)

Use o Privileged Identity Management (PIM) para permitir que membros de função qualificados de recursos do Azure agendem a ativação para uma data e hora futuras. Eles também podem selecionar uma duração de ativação específica até o valor máximo (configurado pelos administradores).

Este artigo é para membros que precisam ativar sua função de recurso do Azure no Privileged Identity Management.

## Ativar uma função

Quando precisar tomar uma função de recurso do Azure, você poderá solicitar a ativação usando a opção de navegação **minhas funções** no Privileged Identity Management.

1. Entre no [portal do Azure](#).
2. Abra **Azure ad Privileged Identity Management**. Para obter informações sobre como adicionar o bloco Privileged Identity Management ao seu painel, consulte [começar a usar o Privileged Identity Management](#).
3. Selecione **minhas funções**.

The screenshot shows the Azure portal interface with the following details:

- Left Sidebar:** Shows various navigation icons and the current path: Dashboard > Privileged Identity Management > My roles - Azure resource roles.
- Left Panel (Tasks):** Includes links for Quick start, My roles (which is selected), My requests, Approve requests, Review access, Manage (with Azure AD roles and Azure resources), Activity (with My audit history), Troubleshooting + Support (with Troubleshoot and New support request), and a general Troubleshooting link.
- Center Content Area:**
  - Activate:** Submenu with options for Azure AD roles and Azure resource roles (which is selected).
  - Troubleshooting + Support:** Submenu with options for Troubleshoot and New support request.
- Right Panel (My roles - Azure resource roles):**
  - Header:** Refresh button and tabs for Eligible roles (selected), Active roles, and Expired roles. A search bar is also present.
  - Table:** A list of roles and their corresponding resources. The table has two columns: ROLE and RESOURCE.

| ROLE                                   | RESOURCE     |
|--|--------------|
| Owner                                  | Wingtip Toys |
| Lab Creator                            | Wingtip Toys |
| EventGrid EventSubscription Contrib... | Wingtip Toys |
| Contributor                            | Wingtip Toys |
| Website Contributor                    | Wingtip Toys |

4. Selecione **funções de recurso do Azure** para ver uma lista de suas funções de recurso do Azure qualificadas.

The screenshot shows the Microsoft Azure interface. On the left, there's a sidebar with various navigation options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'Shared dashboards', 'All resources', and 'Resource groups'. The main content area is titled 'My roles - Azure resource roles'. It has sections for 'Activate', 'Azure AD roles', and 'Azure resource roles'. The 'Azure resource roles' section is highlighted with a red box. Below it are 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'.

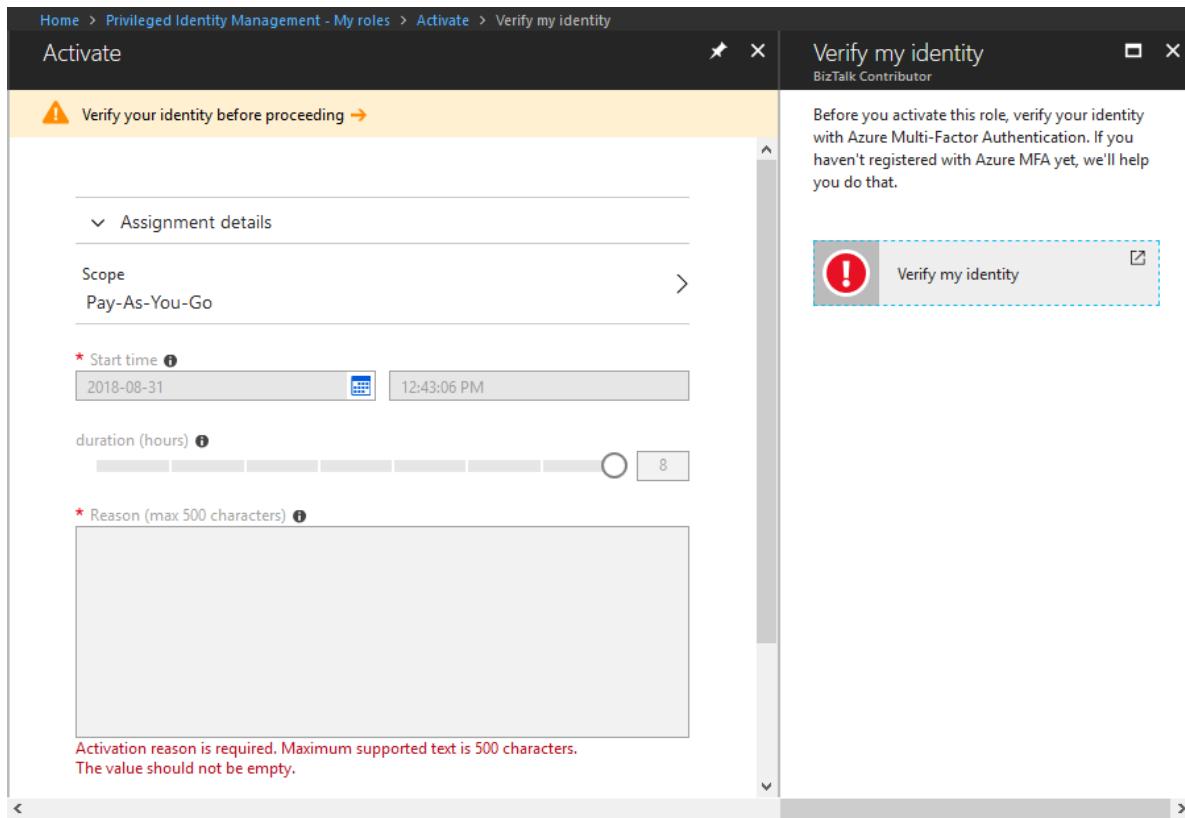
5. Na lista **Funções de recursos do Azure**, encontre a função que você deseja ativar.

This screenshot shows the 'Azure resource roles' list page. It has tabs for 'Eligible roles', 'Active roles', and 'Expired roles'. There's a 'Refresh' button. A table lists roles with columns for 'ROLE', 'RESOURCE', 'RESOURCE TYPE', 'MEMBERSHIP TYPE', 'END TIME', and 'ACTION'. One row shows 'BizTalk Contributor' with 'Pay-As-You-Go' as the resource type, 'Subscription' as the membership type, and an end time of '8/31/2018, 9:48:45 PM'. The 'ACTION' column contains 'Activate' and 'Extend' buttons, with 'Activate' highlighted with a red box.

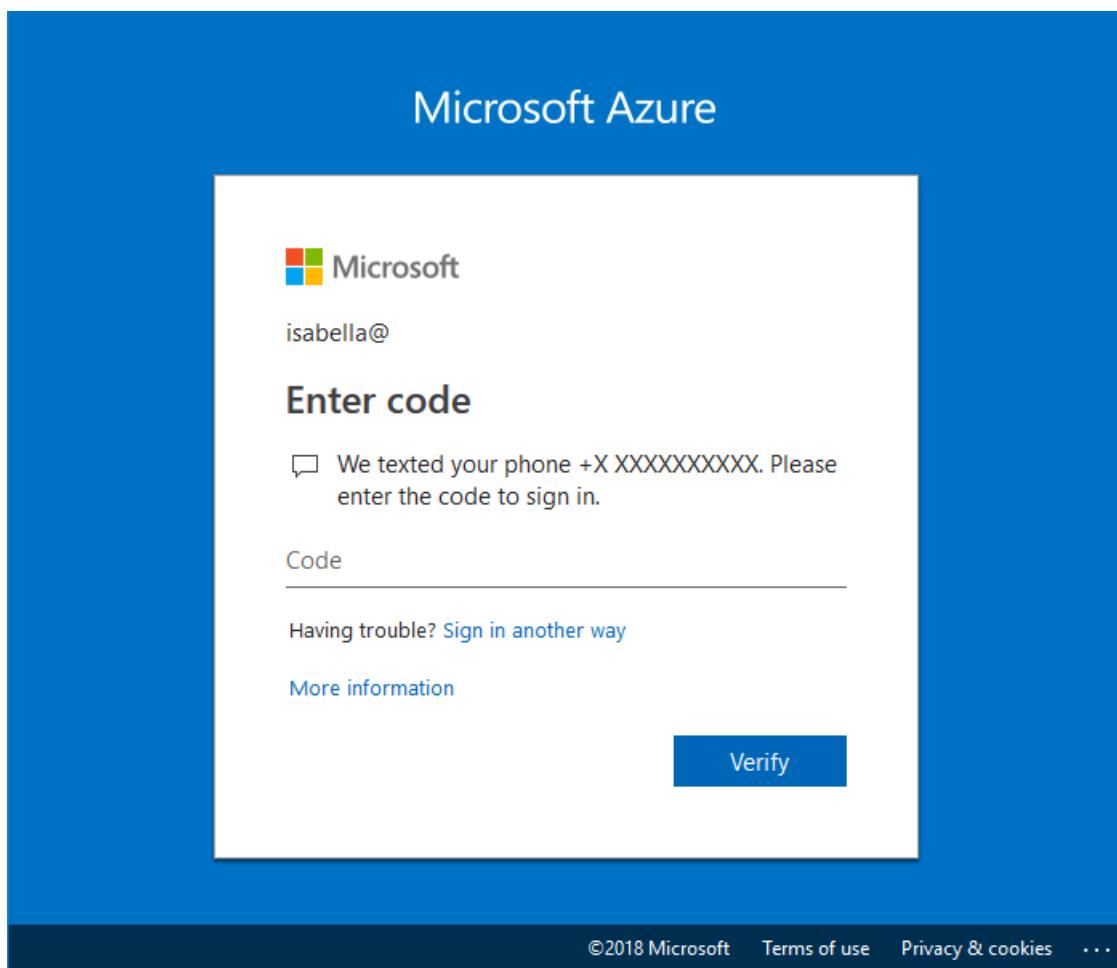
6. Selecione **Ativar** para abrir a página ativar.

This screenshot shows the 'Activate - Owner' dialog box. It has tabs for 'Roles', 'Activate', 'Scope', and 'Status'. Under 'Activate', there's a checkbox for 'Custom activation start time' and a slider for 'Duration (hours)' set to 8. There's also a note about the reason being limited to 500 characters. At the bottom are 'Activate' and 'Cancel' buttons, with 'Activate' highlighted with a red box.

7. Se sua função exigir autenticação multifator, selecione **Verificar sua identidade antes de prosseguir**. Você só precisa se autenticar uma vez por sessão.



8. Selecione **verificar minha identidade** e siga as instruções para fornecer verificação de segurança adicional.



9. Se você quiser especificar um escopo reduzido, selecione **escopo** para abrir o painel Filtro de recursos.

É uma prática recomendada solicitar apenas o acesso aos recursos de que você precisa. No painel de filtro Recursos, você pode especificar os grupos de recursos ou recursos aos quais você precisa acessar.

Home > Activate > Resource filter

## Activate

Assignment details

Scope  
Pay-As-You-Go

\* Start time !  
2018-08-31   12:53:56 PM

duration (hours) !  
 8

\* Reason (max 500 characters) !

Activation reason is required. Maximum supported text is 500 characters.  
The value should not be empty.

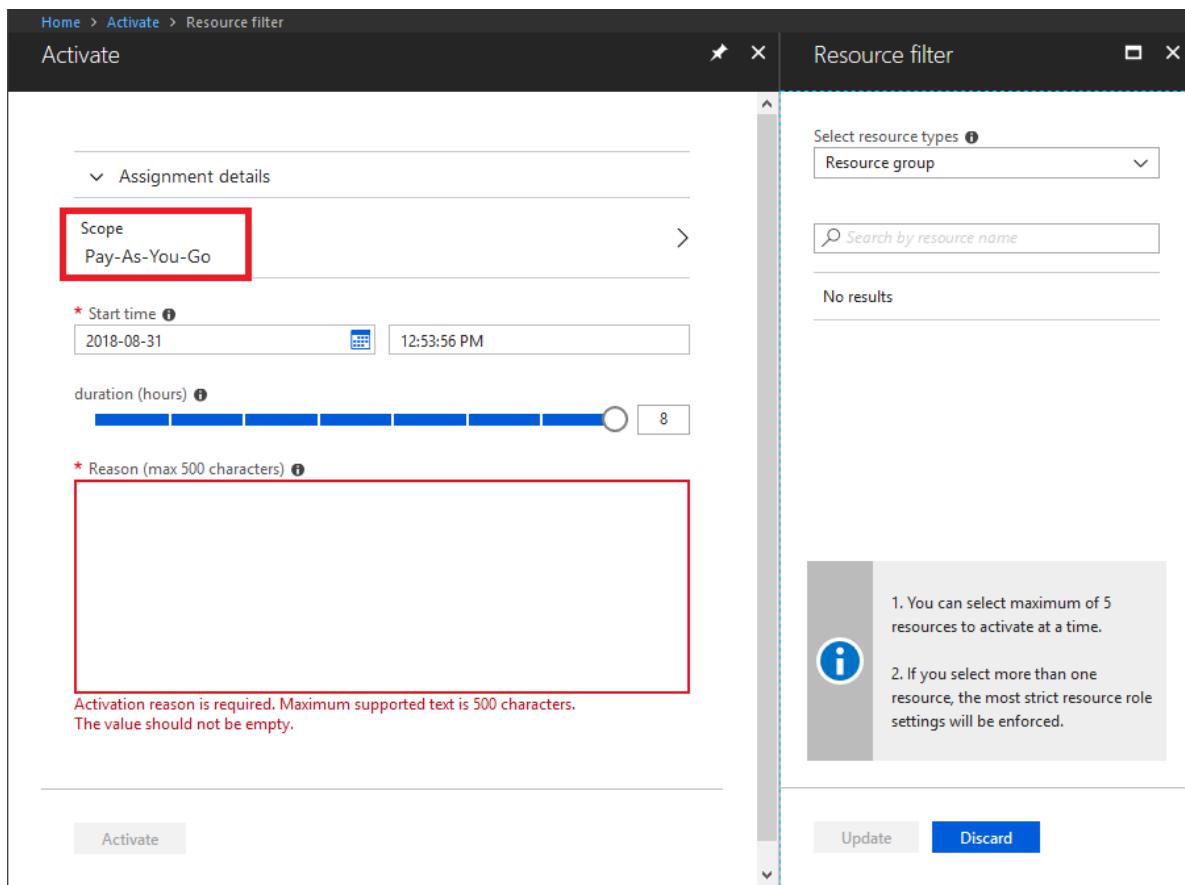
Select resource types !  
Resource group

Search by resource name

No results

i 1. You can select maximum of 5 resources to activate at a time.  
2. If you select more than one resource, the most strict resource role settings will be enforced.

Activate Update Discard



10. Se necessário, especifique uma hora de início de ativação personalizada. O membro seria ativado após o horário selecionado.
11. Na caixa **Motivo**, insira o motivo da solicitação de ativação.

Home > Activate

## Activate

Assignment details

Scope  
Pay-As-You-Go

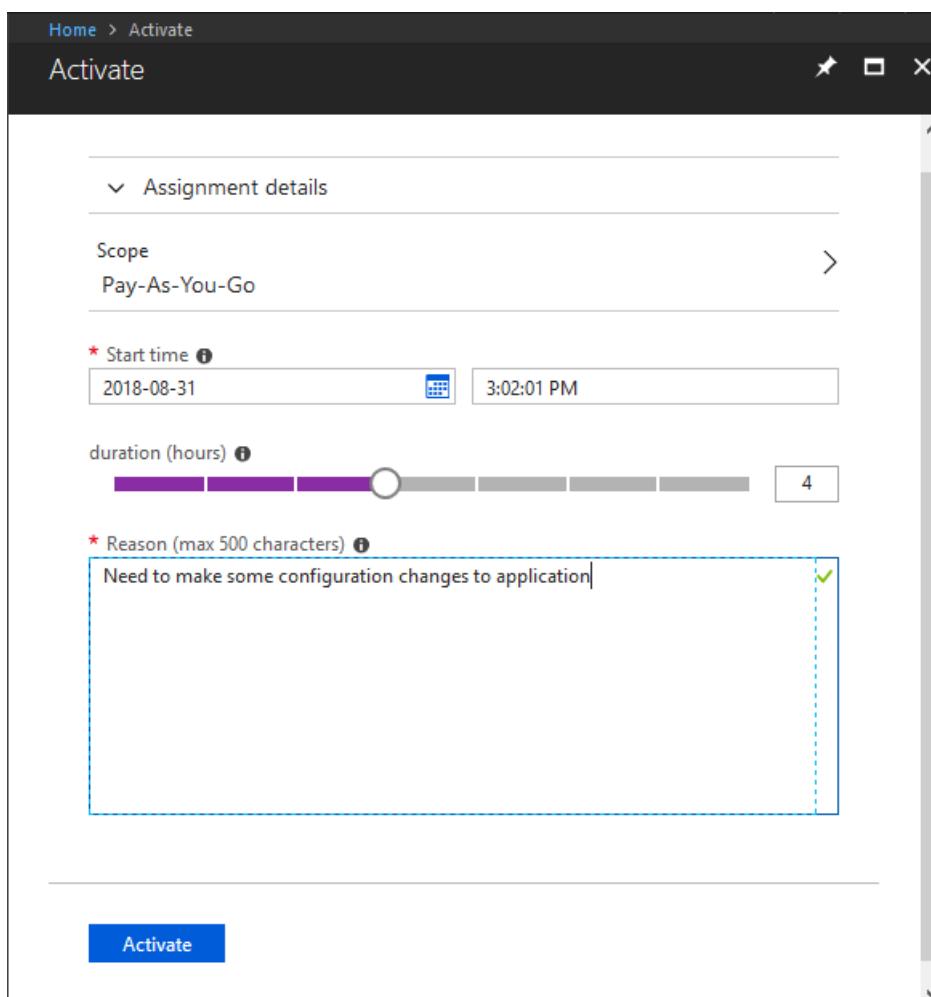
\* Start time !  
2018-08-31   3:02:01 PM

duration (hours) !  
 4

\* Reason (max 500 characters) !

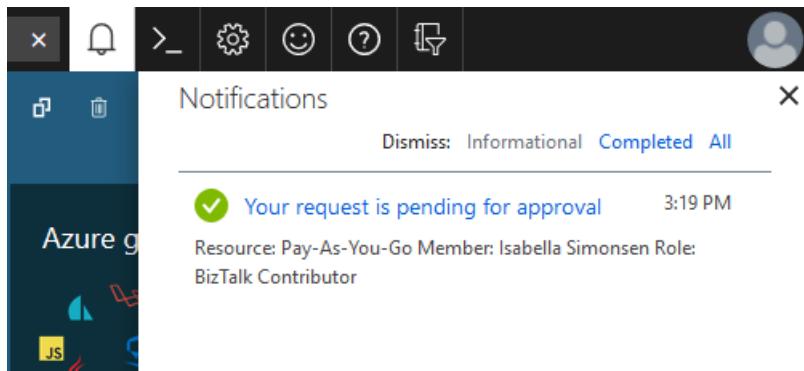
Need to make some configuration changes to application

Activate Update



## 12. Selecione Ativar.

Se a função exigir aprovação para ser ativada, uma notificação será exibida no canto superior direito do seu navegador informando que a solicitação está com a aprovação pendente.



## Exibir o status de suas solicitações

Você pode exibir o status das suas solicitações pendentes a serem ativadas.

1. Abra o Azure AD Privileged Identity Management.
2. Selecione **minhas solicitações** para ver uma lista de suas funções do Azure AD e das solicitações de função de recurso do Azure.

A screenshot of the Azure AD Privileged Identity Management interface. On the left, there is a sidebar with various icons and links. The 'My requests' link under the 'Tasks' section is highlighted. The main content area is titled 'My requests - Azure resources'. It shows a list of items: 'My requests', 'Azure AD roles', 'Azure resources' (which is selected and highlighted in blue), 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. To the right, there is a table titled 'My requests' with columns 'ROLE', 'RESOURCE', and 'MEMBER'. Two rows are listed:

| ROLE                | RESOURCE     | MEMBER |
|---------------------|--------------|--------|
| Billing Reader      | Wingtip Toys | Shaun  |
| Automation Operator | Wingtip Toys | Shaun  |

3. Role para a direita para exibir o **Status da solicitação** coluna.

## Cancelar uma solicitação pendente

Caso não precise da ativação de uma função que requer aprovação, você pode cancelar uma solicitação pendente a qualquer momento.

1. Abra o Azure AD Privileged Identity Management.
2. Selecione **minhas solicitações**.
3. Para a função que você deseja cancelar, selecione o link **Cancelar**.

Quando você selecionar cancelar, a solicitação será cancelada. Para ativar a função novamente, você precisará enviar uma nova solicitação de ativação.

| START TIME             | REQUEST STATUS  | ACTION                 |
|------------------------|-----------------|------------------------|
| 8/31/2018, 3:19:36 ... | PendingApproval | <a href="#">Cancel</a> |

## Solucionar problemas

### As permissões não são concedidas depois de ativar uma função

Quando você ativa uma função no Privileged Identity Management, a ativação pode não ser propagada instantaneamente para todos os portais que exigem a função privilegiada. Às vezes, mesmo quando a alteração é propagada, o cache da web em um portal pode fazer com que a alteração não entre em vigor de imediato. Se a ativação estiver atrasada, aqui está o que você deve fazer.

1. Saia do portal do Azure e entre novamente.
2. Em Privileged Identity Management, verifique se você está listado como o membro da função.

## Próximas etapas

- [Estender ou renovar funções de recurso do Azure no Privileged Identity Management](#)
- [Ativar minhas funções do Azure AD no Privileged Identity Management](#)

# Recursos de gerenciamento para funções do Azure AD no Privileged Identity Management

22/07/2020 • 6 minutes to read • [Edit Online](#)

A experiência de gerenciamento das funções do Azure AD no Privileged Identity Management foi atualizada para unificar a forma como as funções do Azure AD e as funções de recurso do Azure são gerenciadas. Anteriormente, Privileged Identity Management para as funções de recursos do Azure tinham alguns recursos principais que não estavam disponíveis para as funções do Azure AD.

Com a atualização sendo distribuída no momento, estamos mesclando as duas em uma única experiência de gerenciamento e, nela, você obtém a mesma funcionalidade para as funções do Azure AD como as funções de recursos do Azure. Este artigo informa sobre os recursos atualizados e quaisquer requisitos.

## Atribuições de limite de tempo

Anteriormente, havia dois Estados possíveis para as atribuições de função: *elegíveis* e *permanentes*. Agora você também pode definir uma hora de início e de término para cada tipo de atribuição. Essa adição oferece quatro Estados possíveis em que você pode fazer uma atribuição:

- Qualificado permanentemente
- Ativo permanentemente
- Qualificado, com datas de início e de término especificadas para atribuição
- Ativo, com datas de início e de término especificadas para atribuição

Em muitos casos, mesmo que você não queira que os usuários tenham funções qualificadas de atribuição e ativação todas as vezes, você ainda pode proteger sua organização do Azure AD definindo um tempo de expiração para atribuições. Por exemplo, se você tiver alguns usuários temporários qualificados, considere definir uma expiração para removê-los automaticamente da atribuição de função quando seu trabalho for concluído.

## Novas configurações de função

Também estamos adicionando novas configurações para as funções do Azure AD.

- **Anteriormente**, você podia definir apenas as configurações de ativação por função. Ou seja, as configurações de ativação, como requisitos de autenticação multifator e requisitos de incidente/solicitação de tíquete, foram aplicadas a todos os usuários qualificados para uma função específica.
- **Agora**, você pode configurar se um usuário individual precisa executar a autenticação multifator antes de poder ativar uma função. Além disso, você pode ter controle avançado sobre seus emails de Privileged Identity Management relacionados a funções específicas.

## Estender e renovar atribuições

Assim que você descobrir a atribuição de tempo limite, a primeira pergunta que você pode fazer é o que acontece se uma função tiver expirado? Nesta nova versão, fornecemos duas opções para este cenário:

- **Estender**: quando uma atribuição de função se aproxima de sua expiração, o usuário pode usar Privileged Identity Management para solicitar uma extensão para essa atribuição de função
- **Renovar**: quando uma atribuição de função tiver expirado, o usuário poderá usar Privileged Identity Management para solicitar uma renovação para essa atribuição de função

As duas ações iniciadas pelo usuário exigem uma aprovação de um administrador global ou de um administrador de função com privilégios. Os administradores não precisarão mais estar no negócio de gerenciar essas expirações. Eles só precisam aguardar as solicitações de extensão ou renovação e aprová-las se a solicitação for válida.

## Alterações de API

Quando os clientes tiverem a versão atualizada distribuída para sua organização do Azure AD, a API do Graph existente deixará de funcionar. Você deve fazer a transição para usar o [API do Graph para funções de recurso do Azure](#). Para gerenciar funções do Azure AD usando essa API, troque `/azureResources` com `/aadroles` na assinatura e use a ID de diretório para o `resourceId`.

Nós experimentamos o nosso melhor para entrar em contato com todos os clientes que estão usando a API anterior para que eles saibam sobre essa alteração antes do tempo. Se a sua organização do Azure AD foi movida para a nova versão e você ainda depende da API antiga, entre em contato com a equipe em [pim\\_preview@microsoft.com](mailto:pim_preview@microsoft.com).

## Alteração do PowerShell

Para clientes que estão usando o módulo Privileged Identity Management PowerShell para funções do Azure AD, o PowerShell deixará de funcionar com a atualização. No lugar dos cmdlets anteriores, você deve usar os cmdlets Privileged Identity Management dentro do módulo PowerShell de visualização do Azure AD. Instale o módulo do PowerShell do Azure AD da [Galeria do PowerShell](#). Agora você pode ler a [documentação e os exemplos de operações do PIM neste módulo do PowerShell](#).

## Próximas etapas

- [Atribuir uma função personalizada do Azure AD](#)
- [Remover ou atualizar uma atribuição de função personalizada do Azure AD](#)
- [Configurar uma atribuição de função personalizada do Azure AD](#)
- [Definições de função no Azure AD](#)

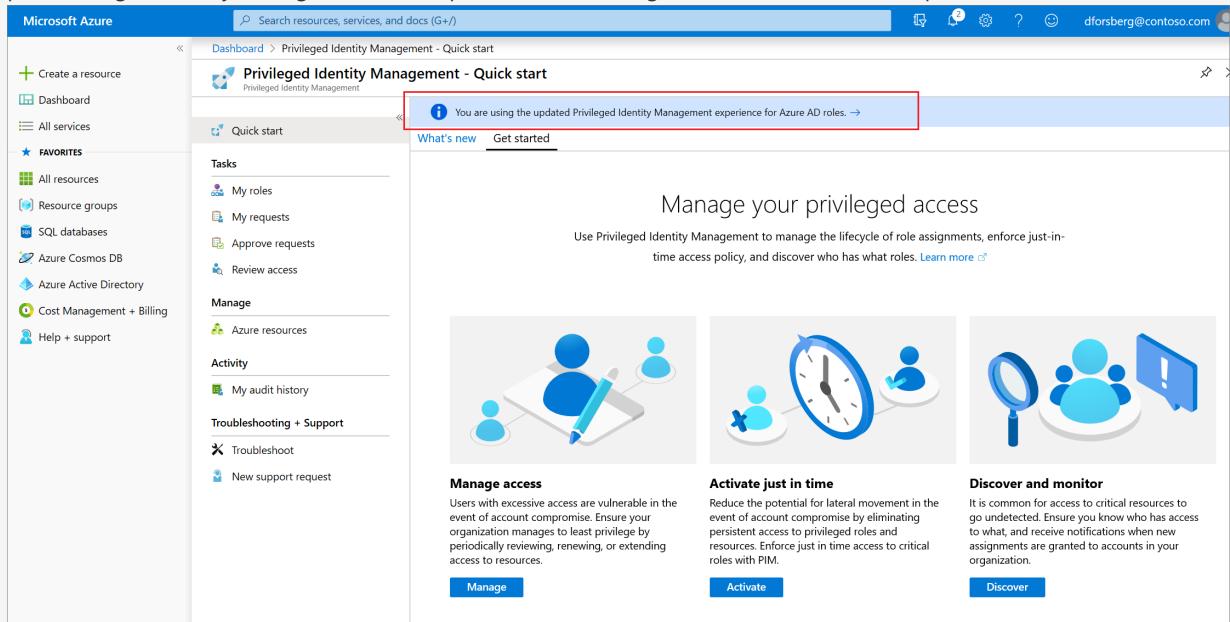
# PowerShell para funções do Azure AD no Privileged Identity Management

22/07/2020 • 10 minutes to read • [Edit Online](#)

Este artigo contém instruções para usar os cmdlets do PowerShell do Azure Active Directory (AD do Azure) para gerenciar funções do Azure AD no Privileged Identity Management (PIM). Ele também explica como configurar usando o módulo PowerShell do Azure AD.

## NOTE

Nosso PowerShell oficial só terá suporte se você estiver na nova versão do Azure AD Privileged Identity Management. Vá para Privileged Identity Management e verifique se você tem a seguinte faixa na folha início rápido.



Se você não tiver essa faixa, aguarde, pois estamos atualmente no processo de distribuir essa experiência atualizada nas próximas semanas. Os cmdlets Privileged Identity Management PowerShell têm suporte por meio do módulo de visualização do Azure AD. Se você estiver usando um módulo diferente e esse módulo agora estiver retornando uma mensagem de erro, comece a usar esse novo módulo. Se você tiver sistemas de produção criados com base em um módulo diferente, entre em contato compim\_preview@microsoft.com

## Instalação e configuração

### 1. Instalar o módulo de visualização do Azure AD

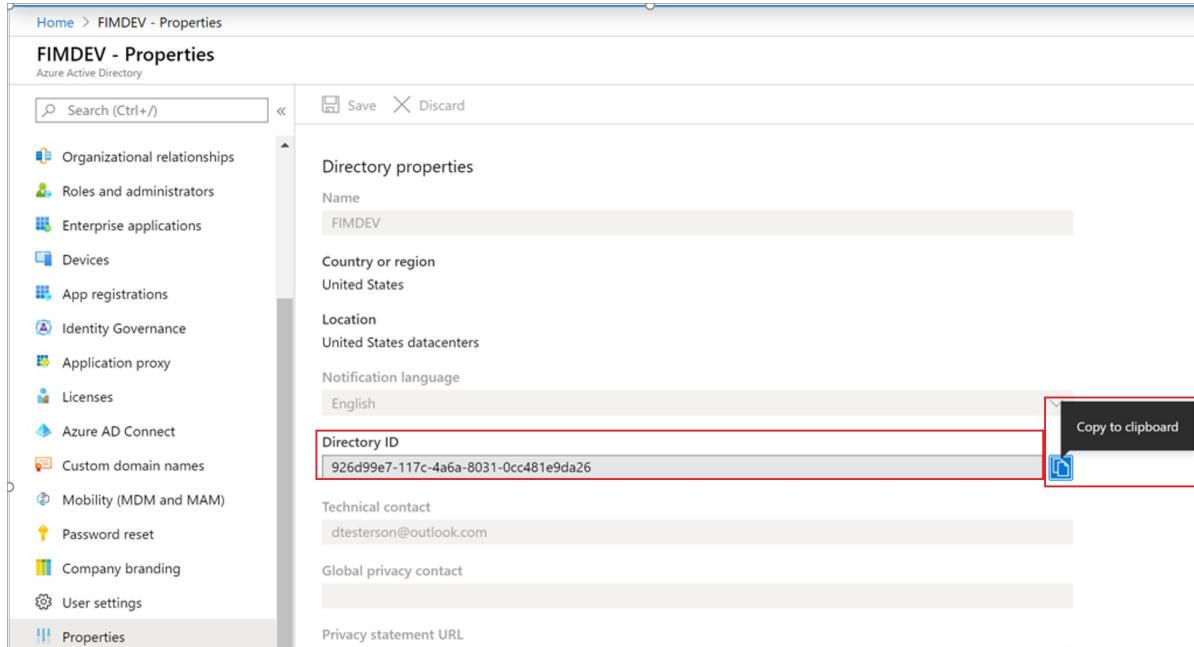
```
Install-Module AzureADPreview
```

### 2. Verifique se você tem as permissões de função necessárias antes de continuar. Se você estiver tentando executar tarefas de gerenciamento como atribuir uma atribuição de função ou atualizar a configuração de função, verifique se você tem a função de administrador global ou de administrador de função privilegiada. Se você estiver apenas tentando ativar sua própria atribuição, nenhuma permissão além das permissões de usuário padrão será necessária.

### 3. Conecte-se ao Azure AD.

```
$AzureAdCred = Get-Credential  
Connect-AzureAD -Credential $AzureAdCred
```

4. Localize a ID de locatário da sua organização do Azure ad acessando **Azure Active Directory > Properties > ID do diretório** de propriedades. Na seção cmdlets, use essa ID sempre que precisar fornecer o resourceld.



The screenshot shows the 'Properties' page for a directory named 'FIMDEV' in the Azure Active Directory. The 'Directory properties' section includes fields for Name (set to 'FIMDEV'), Country or region (set to 'United States'), Location (set to 'United States datacenters'), and Notification language (set to 'English'). A red box highlights the 'Directory ID' field, which contains the value '926d99e7-117c-4a6a-8031-0cc481e9da26'. To the right of this field is a blue 'Copy to clipboard' button. On the left side of the page, there is a navigation menu with links to various Azure services such as Organizational relationships, Roles and administrators, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, and Properties.

#### NOTE

As seções a seguir são exemplos simples que podem ajudar você a colocar em funcionamento. Você pode encontrar uma documentação mais detalhada sobre os seguintes cmdlets em [https://docs.microsoft.com/powershell/module/azuread/?view=azureadps-2.0-preview#privileged\\_role\\_management](https://docs.microsoft.com/powershell/module/azuread/?view=azureadps-2.0-preview#privileged_role_management). No entanto, será necessário substituir "azureResources" no parâmetro ProviderID por "aadRoles". Você também precisará se lembrar de usar a ID da organização para sua organização do Azure AD como o parâmetro Resourceld.

## Recuperando definições de função

Use o cmdlet a seguir para obter todas as funções internas e personalizadas do Azure AD na sua organização do Azure AD. Essa etapa importante fornece o mapeamento entre o nome da função e o roleDefinitionId. O roleDefinitionId é usado em todos esses cmdlets para fazer referência a uma função específica.

O roleDefinitionId é específico para sua organização do Azure AD e é diferente do roleDefinitionId retornado pela API de gerenciamento de função.

```
Get-AzureADMSPrivilegedRoleDefinition -ProviderId aadRoles -ResourceId 926d99e7-117c-4a6a-8031-0cc481e9da26
```

Resultado:

```

Id : 4ca61808-25be-4ba7-b1ec-3b0e35fb9679
ResourceId : 926d99e7-117c-4a6a-8031-0cc481e9da26
ExternalId : 5d6b6bb7-de71-4623-b4af-96380a352509
DisplayName : Security Reader
SubjectCount :
EligibleAssignmentCount :
ActiveAssignmentCount :

Id : 4cad2863-8986-4c0c-9492-3aa15bf96247
ResourceId : 926d99e7-117c-4a6a-8031-0cc481e9da26
ExternalId : de517428-0238-42dc-9b0b-93fd3df5ecb0
DisplayName : applicationsauthenticationupdate
SubjectCount :
EligibleAssignmentCount :
ActiveAssignmentCount :

Id : 50d41cad-1c1d-4861-8b01-4f1bf9a9386d
ResourceId : 926d99e7-117c-4a6a-8031-0cc481e9da26
ExternalId : e8611ab8-c189-46e8-94e1-60213ab1f814
DisplayName : Privileged Role Administrator
SubjectCount :
EligibleAssignmentCount :
ActiveAssignmentCount :

Id : 51d871b2-7133-42c8-bd8b-dc883ea75944
ResourceId : 926d99e7-117c-4a6a-8031-0cc481e9da26
ExternalId : 4a5d8f65-41da-4de4-8968-e035b65339cf
DisplayName : Reports Reader
SubjectCount :
EligibleAssignmentCount :
ActiveAssignmentCount :

```

## Recuperando atribuições de função

Use o cmdlet a seguir para recuperar todas as atribuições de função em sua organização do Azure AD.

```
Get-AzureADMSPrivilegedRoleAssignment -ProviderId "aadRoles" -ResourceId "926d99e7-117c-4a6a-8031-0cc481e9da26"
```

Use o cmdlet a seguir para recuperar todas as atribuições de função para um usuário específico. Essa lista também é conhecida como "minhas funções" no portal do AD do Azure. A única diferença aqui é que você adicionou um filtro para a ID da entidade. A ID do assunto neste contexto é a ID de usuário ou a ID do grupo.

```
Get-AzureADMSPrivilegedRoleAssignment -ProviderId "aadRoles" -ResourceId "926d99e7-117c-4a6a-8031-0cc481e9da26" -Filter "subjectId eq 'f7d1887c-7777-4ba3-ba3d-974488524a9d'"
```

Use o cmdlet a seguir para recuperar todas as atribuições de função para uma função específica. O roleDefinitionId aqui é a ID que é retornada pelo cmdlet anterior.

```
Get-AzureADMSPrivilegedRoleAssignment -ProviderId "aadRoles" -ResourceId "926d99e7-117c-4a6a-8031-0cc481e9da26" -Filter "roleDefinitionId eq '0bb54a22-a3df-4592-9dc7-9e1418f0f61c'"
```

Os cmdlets resultam em uma lista de objetos de atribuição de função mostrados abaixo. A ID de assunto é a ID de usuário para a qual a função é atribuída. O estado de atribuição pode estar ativo ou qualificado. Se o usuário estiver ativo e houver uma ID no campo LinkedEligibleRoleAssignmentId, isso significa que a função está ativada no momento.

Resultado:

|                                       |   |   |
|---------------------------------------|---|---|
| <b>Id</b>                             | : | LJnv8vs6uUa3z6Em7nTEUXyI0fd3d6NLuj2XRIhSSp0-1 |
| <b>ResourceId</b>                     | : | 926d99e7-117c-4a6a-8031-0cc481e9da26          |
| <b>RoleDefinitionId</b>               | : | 8ce75876-f760-42be-b2a2-3a080f2df068          |
| <b>SubjectId</b>                      | : | f7d1887c-7777-4ba3-ba3d-974488524a9d          |
| <b>LinkedEligibleRoleAssignmentId</b> | : |   |
| <b>ExternalId</b>                     | : | LJnv8vs6uUa3z6Em7nTEUXyI0fd3d6NLuj2XRIhSSp0-1 |
| <b>StartDateTime</b>                  | : | 2/13/2020 12:14:15 AM                         |
| <b>EndDateTime</b>                    | : |   |
| <b>AssignmentState</b>                | : | Active  |
| <b>MemberType</b>                     | : | Direct  |

## Atribuir uma função

Use o cmdlet a seguir para criar uma atribuição qualificada.

```
Open-AzureADMSPrivilegedRoleAssignmentRequest -ProviderId 'aadRoles' -ResourceId '926d99e7-117c-4a6a-8031-0cc481e9da26' -RoleDefinitionId 'ff690580-d1c6-42b1-8272-c029ded94dec' -SubjectId 'f7d1887c-7777-4ba3-ba3d-974488524a9d' -Type 'adminAdd' -AssignmentState 'Eligible' -schedule $schedule -reason "dsasdsas"
```

O agendamento, que define a hora de início e de término da atribuição, é um objeto que pode ser criado como o exemplo a seguir:

```
$schedule = New-Object Microsoft.Open.MSGraph.Model.AzureADMSPrivilegedSchedule
$schedule.Type = "Once"
$schedule.StartDateTime = (Get-Date).ToUniversalTime().ToString("yyyy-MM-ddTHH:mm:ss.fffZ")
$schedule.endDateTime = "2020-07-25T20:49:11.770Z"
```

### NOTE

Se o valor de EndDateTime for definido como NULL, ele indicará uma atribuição permanente.

## Ativar uma atribuição de função

Use o cmdlet a seguir para ativar uma atribuição qualificada.

```
Open-AzureADMSPrivilegedRoleAssignmentRequest -ProviderId 'aadRoles' -ResourceId '926d99e7-117c-4a6a-8031-0cc481e9da26' -RoleDefinitionId 'f55a9a68-f424-41b7-8bee-cee6a442d418' -SubjectId 'f7d1887c-7777-4ba3-ba3d-974488524a9d' -Type 'UserAdd' -AssignmentState 'Active' -schedule $schedule -reason "dsasdsas"
```

Esse cmdlet é quase idêntico ao cmdlet para criar uma atribuição de função. A principal diferença entre os cmdlets é que, para o parâmetro – Type, a ativação é "userAdd" em vez de "adminAdd". A outra diferença é que o parâmetro – Assignmentstate é "ativo" em vez de "elegível".

## NOTE

Há dois cenários de limitação para a ativação de função por meio do PowerShell.

1. Se você precisar de um número de tíquete/sistema de tíquete em sua configuração de função, não será possível fornecê-lo como um parâmetro. Portanto, não seria possível ativar a função além da portal do Azure. Este recurso está sendo distribuído para o PowerShell nos próximos meses.
2. Se você precisar de autenticação multifator para ativação de função, atualmente não há como o PowerShell desafiar o usuário quando ele ativar sua função. Em vez disso, os usuários precisarão disparar o desafio de MFA quando se conectarem ao Azure AD seguindo [esta postagem de blog](#) de um de nossos engenheiros. Se você estiver desenvolvendo um aplicativo para PIM, uma implementação possível será desafiar os usuários e reconectá-los ao módulo depois que eles receberem um erro de "MfaRule".

## Recuperando e atualizando configurações de função

Use o cmdlet a seguir para obter todas as configurações de função em sua organização do Azure AD.

```
Get-AzureADMSPrivilegedRoleSetting -ProviderId 'aadRoles' -Filter "ResourceId eq '926d99e7-117c-4a6a-8031-0cc481e9da26'"
```

Há quatro objetos principais na configuração. Somente três desses objetos são usados atualmente pelo PIM. As UserMemberSettings são configurações de ativação, AdminEligibleSettings são configurações de atribuição para atribuições qualificadas e o AdminmemberSettings são configurações de atribuição para atribuições ativas.

```
Id          : e19a3999-1dc5-4f7b-81f5-fc78e3ed00af
ResourceId  : 926d99e7-117c-4a6a-8031-0cc481e9da26
RoleDefinitionId : e228f5e5-1ef3-451a-a08b-e82ffa0e5c35
IsDefault   : True
LastUpdatedDateTime :
LastUpdatedBy :
AdminEligibleSettings : {class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: ExpirationRule
    Setting: {"maximumGrantPeriod": "365.00:00:00", "maximumGrantPeriodInMinutes": 525600, "permanentAssignment": false}
  }
  , class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: MfaRule
    Setting: {"mfaRequired": false}
  }
}
AdminMemberSettings : {class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: ExpirationRule
    Setting: {"maximumGrantPeriod": "180.00:00:00", "maximumGrantPeriodInMinutes": 259200, "permanentAssignment": false}
  }
  , class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: MfaRule
    Setting: {"mfaRequired": false}
  }
  , class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: JustificationRule
    Setting: {"required": true}
  }
}
UserEligibleSettings : {}
UserMemberSettings : {class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: ExpirationRule
    Setting: {"maximumGrantPeriod": "08:00:00", "maximumGrantPeriodInMinutes": 480, "permanentAssignment": false}
  }
  , class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: MfaRule
    Setting: {"mfaRequired": false}
  }
  , class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: JustificationRule
    Setting: {"required": true}
  }
  , class AzureADMSPrivilegedRuleSetting {
    RuleIdentifier: ApprovalRule
    Setting: {"enabled": false, "isCriteriaSupported": false, "approvers": null, "businessFlowId": null, "hasNotificationPolicy": false}
  }
}
...
```

Para atualizar a configuração de função, você deve obter o objeto de configuração existente para uma função específica e fazer alterações nele:

```
$setting = Get-AzureADMSPrivilegedRoleSetting -ProviderId 'aadRoles' -Filter "roleDefinitionId eq 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'"
$setting.UserMemberSetting.justificationRule = '{"required": false}'
```

Em seguida, você pode aplicar a configuração a um dos objetos para uma função específica, conforme mostrado abaixo. A ID aqui é a ID de configuração de função que pode ser recuperada do resultado do cmdlet `List role Settings`.

```
Set-AzureADMSPrivilegedRoleSetting -ProviderId 'aadRoles' -Id 'ff518d09-47f5-45a9-bb32-71916d9aeadf' -  
ResourceId '3f5887ed-dd6e-4821-8bde-c813ec508cf9' -RoleDefinitionId '2387ced3-4e95-4c36-a915-73d803f93702' -  
UserMemberSettings $setting
```

## Próximas etapas

- [Atribuir uma função personalizada do Azure AD](#)
- [Remover ou atualizar uma atribuição de função personalizada do Azure AD](#)
- [Configurar uma atribuição de função personalizada do Azure AD](#)
- [Definições de função no Azure AD](#)

# Atribuir funções do Azure AD no Privileged Identity Management

22/07/2020 • 11 minutes to read • [Edit Online](#)

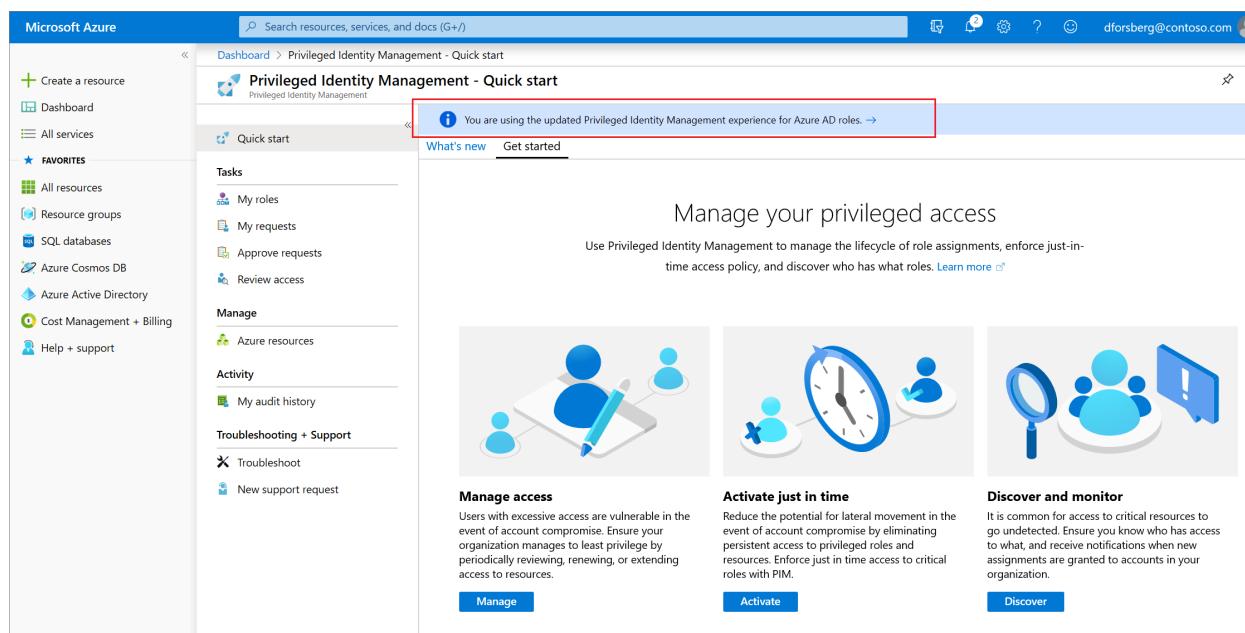
Com o Azure Active Directory (AD do Azure), um administrador global pode fazer atribuições de função de administrador do Azure AD **permanentes**. Essas atribuições de função podem ser criadas usando o [portal do Azure](#) ou usando [comandos do PowerShell](#).

O serviço PIM (Azure AD Privileged Identity Management) também permite que administradores de função com privilégios façam atribuições de função de administrador permanentes. Além disso, os administradores de função com privilégios podem tornar os usuários **qualificados** para as funções de administrador do Azure AD. Um administrador qualificado pode ativar a função quando necessário e suas permissões expirarão assim que forem feitas.

## Determinar sua versão do PIM

A partir de novembro de 2019, a parte das funções do Azure AD da Privileged Identity Management está sendo atualizada para uma nova versão que corresponde às experiências de funções de recurso do Azure. Isso cria recursos adicionais, bem como [as alterações na API existente](#). Enquanto a nova versão está sendo distribuída, os procedimentos que você seguir neste artigo dependem da versão do Privileged Identity Management que você tem atualmente. Siga as etapas nesta seção para determinar qual versão do Privileged Identity Management você tem. Depois de saber sua versão do Privileged Identity Management, você pode selecionar os procedimentos neste artigo que correspondem a essa versão.

1. Entre no [portal do Azure](#) com um usuário que esteja na função de [administrador de função com privilégios](#).
2. Abra [Azure ad Privileged Identity Management](#). Se você tiver uma faixa na parte superior da página Visão geral, siga as instruções na [nova guia versão](#) deste artigo. Caso contrário, siga as instruções na guia [versão anterior](#).



- [Nova versão](#)
- [Versão anterior](#)

# Atribuir uma função

Siga estas etapas para tornar um usuário qualificado para uma função de administrador do Azure AD.

1. Entre no [portal do Azure](#) com um usuário que seja membro da função de [administrador de função com privilégios](#).

Para obter informações sobre como conceder a outro administrador acesso para gerenciar Privileged Identity Management, consulte [conceder acesso a outros administradores para gerenciar Privileged Identity Management](#).

2. Abra **Azure ad Privileged Identity Management**.
3. Selecione **funções do Azure ad**.
4. Selecione **funções** para ver a lista de funções para permissões do Azure AD.

| Role                                       | Description  | Count |
|--|--|-------|
| Authentication Administrator               | Can access to view, set and reset authentication method information for any non-a...<br>4    | 5     |
| Azure DevOps Administrator                 | Can manage Azure DevOps organization policy and settings.<br>3                               | 2     |
| Azure Information Protection Administrator | Users with this role have user rights only on the Azure Information Protection service.<br>2 | 0     |
| B2C IEF Keyset Administrator               | Manage secrets for federation and encryption in the Identity Experience Framework.<br>2      | 0     |
| B2C IEF Policy Administrator               | Create and manage trust framework policies in the Identity Experience Framework.<br>1        | 0     |
| Billing Administrator                      | Makes purchases, manages subscriptions, manages support tickets, and monitors s...<br>11     | 8     |
| Cloud Application Administrator            | Users with this role can create and manage all aspects of app registrations and ente...<br>3 | 2     |
| Cloud Device Administrator                 | Full access to manage devices in Azure AD.<br>4  | 3     |
| Compliance Administrator                   | Users with this role have management permissions within the Office 365 Security...<br>2      | 3     |
| Compliance Data Administrator              | Creates and manages compliance content.<br>4   | 5     |
| Conditional Access Administrator           | Users with this role have the ability to manage Azure Active Directory conditional a...<br>2 | 2     |
| Dynamics 365 Administrator                 | Users with this role have global permissions within Microsoft CRM Online<br>4                | 1     |
| Customer LockBox Access Approver           | Can approve Microsoft support requests to access customer organizational data<br>0           | 1     |
| CustomRole-1                               | <br>3  | 3     |
| Desktop Analytics Administrator            | Users in this role will have access to manage Desktop Analytics and Office Customiz...<br>0  | 3     |
| Device Administrators                      | Users with this role become local machine administrators on all Windows 10 device...<br>2    | 3     |
| Directory Readers                          | Allows access to various read only tasks in the directory.<br>21                             | 7     |
| Exchange Administrator                     | Users with this role have global permissions within Microsoft Exchange Online<br>1           | 3     |

5. Selecione **Adicionar atribuições** para abrir a página **Adicionar atribuições**.

6. Selecione **selecionar uma função** para abrir a página **selecionar uma função**.

Microsoft Azure Search resources, services, and docs (G+)

Home > FIMDEV | Roles >

## Add assignments

Privileged Identity Management | Azure AD roles

Membership Setting

Resource FIMDEV

Resource type Directory

Select role ⓘ

Search role

Search role by name

anujcRole11111

Application Administrator

Application Developer

Application Helpdesk Administrator

Applications Basic Update

applicationsallpropertiesupdate

applicationsaudienceupdate

applicationsauthenticationupdate

applicationscreate

applicationscreateasowner

applicationscredentialsupdate

applicationsmyorganizationallpropertiesupdate

Next > Cancel

The screenshot shows the 'Add assignments' step in the Microsoft Azure Privileged Identity Management interface. It's a 'Membership' configuration screen for a resource named 'FIMDEV'. A dropdown menu titled 'Select role' is open, listing various Azure AD roles. The 'Next >' button at the bottom of the dropdown is highlighted with a red box.

7. Selecione uma função que você deseja atribuir, selecione um membro a quem você deseja atribuir à função e, em seguida, selecione **Avançar**.
8. Na lista **tipo de atribuição**, no painel **configurações de associação**, selecione **qualificado** ou **ativo**.
  - Atribuições **qualificadas** exigem que o membro da função execute uma ação para usar a função. As ações podem incluir a execução de uma verificação de MFA (Autenticação Multifator), fornecimento de uma justificativa comercial ou solicitação de aprovação dos aprovadores designados.
  - As atribuições **ativas** não exigem que o membro execute qualquer ação para usar a função. Membros atribuídos como ativos sempre possuem privilégios atribuídos pela função.
9. Para especificar uma duração de atribuição específica, adicione as caixas de data e hora de início e término. Quando terminar, selecione **atribuir** para criar a nova atribuição de função.

Microsoft Azure Search resources, services, and docs (G+)

Home > FIMDEV | Roles >

## Add assignments

Privileged Identity Management | Azure AD roles

Membership Setting

**Assignment type** ⓘ

Eligible

Active

Maximum allowed eligible duration is 1 month(s).

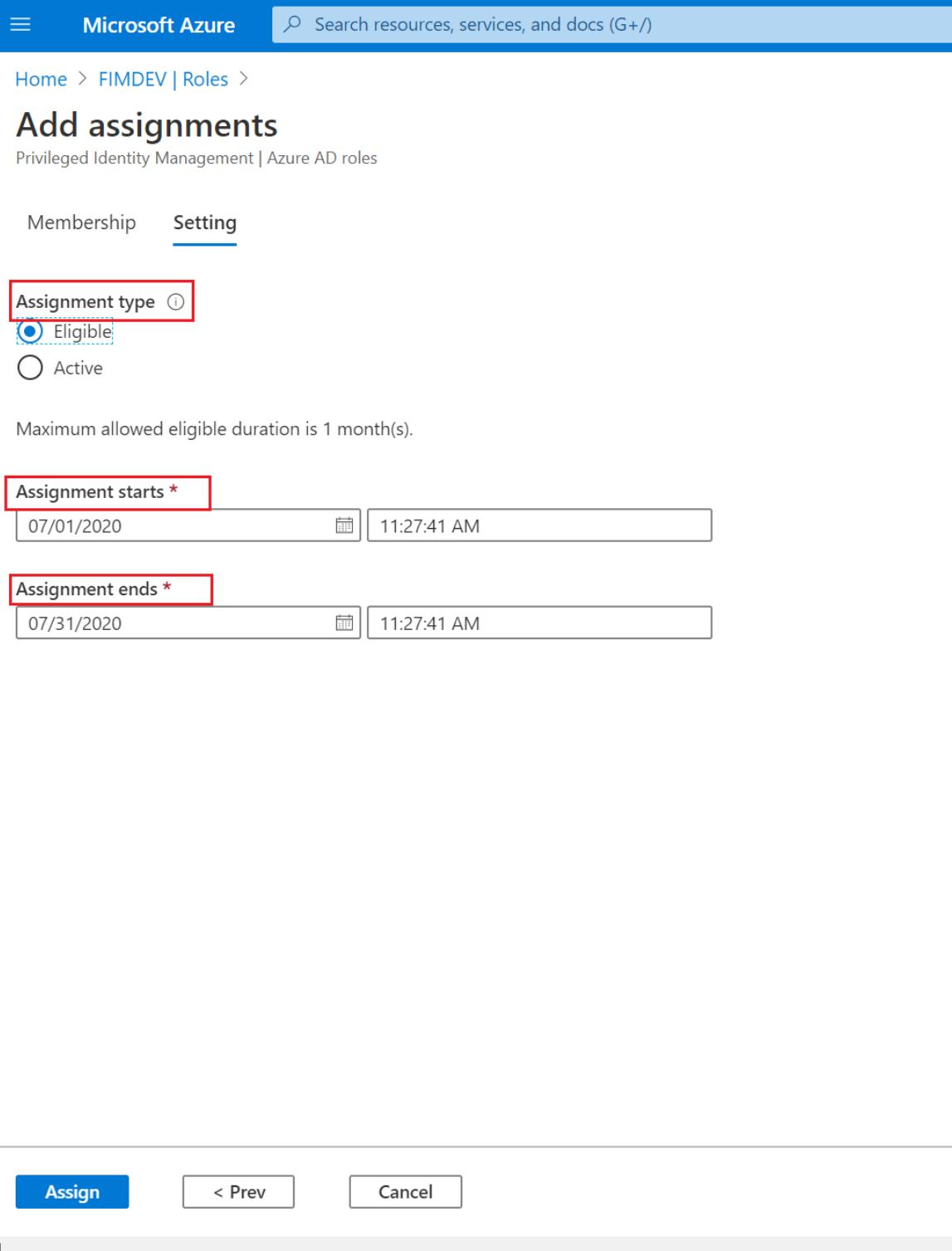
**Assignment starts \***

07/01/2020 11:27:41 AM

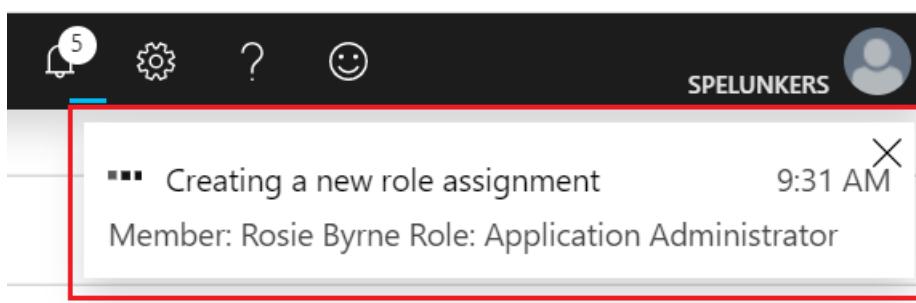
**Assignment ends \***

07/31/2020 11:27:41 AM

Assign < Prev Cancel



10. Depois que a função é atribuída, uma notificação de status de atribuição é exibida.



Atualizar ou remover uma atribuição de função existente

Siga estas etapas para atualizar ou remover uma atribuição de função existente.

1. Abra Azure ad Privileged Identity Management.
2. Selecione funções do Azure ad.
3. Selecione funções para ver a lista de funções do Azure AD.
4. Selecione a função que você deseja atualizar ou remover.
5. Localize a atribuição de função nas guias **Funções qualificadas** ou **Funções ativas**.

| Name              | Principal name    | Type  | Scope     | Membership | Start time             | End time               | Action                          |
|-------------------|-------------------|-------|-----------|------------|------------------------|------------------------|---------------------------------|
| Dritan Kodra      | dritan@fimdev.net | User  | Directory | Direct     | 12/5/2019, 8:56:15 AM  | 3/30/2021, 4:22:52 PM  | <a href="#">Remove   Update</a> |
| Nihad Samaha      | nihad@fimdev.net  | User  | Directory | Direct     | 4/15/2020, 12:28:26 PM | 3/30/2021, 4:22:52 PM  | <a href="#">Remove   Update</a> |
| Rabeh Záher       | rabeh@fimdev.net  | User  | Directory | Direct     | 3/30/2020, 4:23:06 PM  | 3/30/2021, 4:22:52 PM  | <a href="#">Remove   Update</a> |
| AAA_AAA_Test_Grou | -                 | Group | Directory | Direct     | 6/2/2020, 9:25:00 AM   | 7/2/2020, 9:24:49 AM   | <a href="#">Remove   Update</a> |
| Lisha Daher       | lisha@fimdev.net  | User  | Directory | Direct     | 3/14/2020, 11:20:35 PM | 3/30/2021, 4:22:52 PM  | <a href="#">Remove   Update</a> |
| 006-Exchange Admi | -                 | Group | Directory | Direct     | 7/1/2020, 11:48:57 AM  | 7/31/2020, 11:27:41 AM | <a href="#">Remove   Update</a> |

6. Selecione **Atualizar** ou **Remover** para atualizar ou remover a atribuição de função.

## Próximas etapas

- Definir as configurações de função do administrador do Azure AD no Privileged Identity Management
- Atribuir funções de recurso do Azure no Privileged Identity Management

# Aprovar ou negar solicitações para funções do Azure AD no Privileged Identity Management

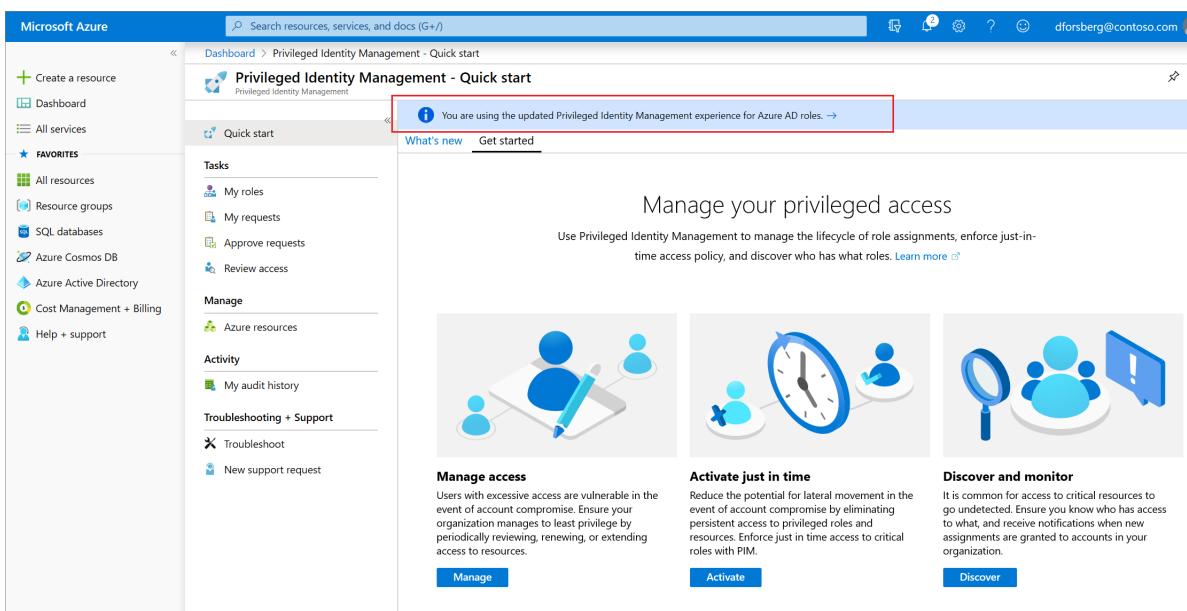
22/07/2020 • 6 minutes to read • [Edit Online](#)

Com o Azure Active Directory (Azure AD) Privileged Identity Management (PIM), você pode configurar funções para exigir aprovação para ativação e escolher um ou vários usuários ou grupos como aprovadores delegados. Os aprovadores representantes têm 24 horas para aprovar as solicitações. Se a solicitação não for aprovada dentro de 24 horas, o usuário qualificado deverá enviar outra. A janela de tempo de aprovação de 24 horas não é configurável.

## Determinar sua versão do PIM

A partir de novembro de 2019, a parte das funções do Azure AD da Privileged Identity Management está sendo atualizada para uma nova versão que corresponde às experiências para funções do Azure. Isso cria recursos adicionais, bem como [as alterações na API existente](#). Enquanto a nova versão está sendo distribuída, os procedimentos que você seguir neste artigo dependem da versão do Privileged Identity Management que você tem atualmente. Siga as etapas nesta seção para determinar qual versão do Privileged Identity Management você tem. Depois de saber sua versão do Privileged Identity Management, você pode selecionar os procedimentos neste artigo que correspondem a essa versão.

1. Entre no [portal do Azure](#) com um usuário que esteja na função de **administrador de função com privilégios**
2. Abra **Azure ad Privileged Identity Management**. Se você tiver uma faixa na parte superior da página Visão geral, siga as instruções na **nova guia versão** deste artigo. Caso contrário, siga as instruções na guia **versão anterior**.



Siga as etapas neste artigo para aprovar ou negar solicitações para funções do Azure AD.

- [Nova versão](#)
- [Versão anterior](#)

## Exibir solicitações pendentes

Como um Aprovador delegado, você receberá uma notificação por email quando uma solicitação de função do Azure AD estiver aguardando sua aprovação. Você pode exibir essas solicitações pendentes no Privileged Identity Management.

1. Entre no [portal do Azure](#).
2. Abra Azure ad Privileged Identity Management.
3. Selecione **aprovar solicitações**.

The screenshot shows the Azure Privileged Identity Management interface. The left sidebar has sections for Quick start, Tasks (My roles, My requests, Approve requests, Review access), Manage (Azure AD roles, Azure resources), and Activity (My audit history). The main content area is titled 'Approve requests - Azure AD roles' and shows a list of requests under 'Requests to renew or extend role assignments'. One item is listed: 'Cloud Application Ad...' by 'Priyank User' for 'FIMDEV'. Below this is another section for 'No requests pending approval'.

| Role                    | Requestor    | Resource |
|-------------------------|--------------|----------|
| Cloud Application Ad... | Priyank User | FIMDEV   |

Na seção **Solicitações para ativações de função** você verá uma lista de solicitações aguardando a aprovação.

## Aprovar solicitações

1. Localize e selecione a solicitação que você deseja aprovar. Uma página aprovar ou negar é exibida.

Home > Privileged Identity Management > Approve requests - Azure AD roles

**Approve requests - Azure AD roles**

Requests to renew or extend role assignments

| Role                    | Requestor    | Resource |
|-------------------------|--------------|----------|
| Cloud Application Ad... | Priyank User | FIMDEV   |

No requests pending approval

2. Na caixa de justificação , insira a justificativa comercial.
3. Selecione **Aprovar**. Você receberá uma notificação do Azure de sua aprovação.

- Approve requests

Approval requests for Azure AD directory role

| Approve                      | Deny | Refresh |
|------------------------------|------|---------|
| ROLE                         |      |         |
| No requests pending approval |      |         |

Approval requests for Azure RBAC resources

^ Requests to renew or extend role assignments

| Refresh                      |           |          |
|------------------------------|-----------|----------|
| ROLE                         | REQUESTOR | RESOURCE |
| No requests pending approval |           |          |

^ Requests for role activations

| ROLE                | REQUESTOR         |
|---------------------|-------------------|
| BizTalk Contributor | Isabella Simonsen |

\* Justification

Approve Deny

## Negar solicitações

1. Localize e selecione a solicitação que você deseja negar. Uma página aprovar ou negar é exibida.

The screenshot shows the Azure portal interface for managing approval requests. On the left, there's a sidebar with navigation options like 'My requests', 'Approve requests', and 'Pending approvals'. The main area displays two sections: 'Approval requests for Azure AD directory roles' and 'Approval requests for Azure RBAC resources'. Under the first section, it says 'No requests pending approval'. Under the second section, it says 'Requests to renew or extend role assignments' and 'Requests for role activations'. Both sections show a table with columns 'ROLE', 'REQUESTOR', and 'RESOURCE'. In the 'ROLE' column, 'BizTalk Contributor' is listed. In the 'REQUESTOR' column, 'Isabella Simonsen' is listed. At the bottom of the main area, there are 'Approve' and 'Deny' buttons. A modal dialog box is overlaid on the page, providing detailed information about a specific request:

| Role          | BizTalk Contributor                                    |
|---------------|--|
| Requestor     | Isabella Simonsen                                      |
| Request Time  | 8/31/2018 3:19 PM                                      |
| Resource      | Pay-As-You-Go  |
| Resource Type | subscription   |
| Reason        | Need to make some configuration changes to application |
| Start Time    | 8/31/2018 10:02 PM                                     |
| End Time      | 9/1/2018 2:02 AM                                       |

\* Justification !

Approve Deny

2. Na caixa de justificação , insira a justificativa comercial.

3. Selecione negar. Uma notificação é exibida com a negação.

## Notificações de fluxo de trabalho

Veja algumas informações sobre notificações de fluxo de trabalho:

- Os aprovadores são notificados por email quando uma solicitação de uma função está aguardando sua revisão. As notificações por email incluem um link direto para a solicitação no qual o aprovador pode aprovar ou negar.
- As solicitações são resolvidas pelo primeiro aprovador que aprova ou nega.
- Quando um Aprovador responde à solicitação, todos os aprovadores são notificados sobre a ação.
- Administradores globais e administradores de função privilegiada são notificados quando um usuário aprovado se torna ativo em sua função.

**NOTE**

Um administrador global ou administrador de função com privilégios que acredita que um usuário aprovado não deve estar ativo pode remover a atribuição de função ativa em Privileged Identity Management. Embora os administradores não sejam notificados sobre solicitações pendentes, a menos que sejam um aprovador, eles podem exibir e cancelar quaisquer solicitações pendentes para todos os usuários exibindo solicitações pendentes no Privileged Identity Management.

## Próximas etapas

- [Notificações por email no Privileged Identity Management](#)
- [Aprovar ou negar solicitações para funções de recurso do Azure no Privileged Identity Management](#)

# Definir as configurações de função do Azure AD no Privileged Identity Management

22/07/2020 • 14 minutes to read • [Edit Online](#)

Um administrador de função com privilégios pode personalizar Privileged Identity Management (PIM) em sua organização do Azure Active Directory (Azure AD), incluindo a alteração da experiência de um usuário que está ativando uma atribuição de função qualificada.

## Determinar sua versão do PIM

A partir de novembro de 2019, a parte das funções do Azure AD da Privileged Identity Management está sendo atualizada para uma nova versão que corresponde às experiências de funções de recurso do Azure. Isso cria recursos adicionais, bem como [as alterações na API existente](#). Enquanto a nova versão está sendo distribuída, os procedimentos que você seguir neste artigo dependem da versão do Privileged Identity Management que você tem atualmente. Siga as etapas nesta seção para determinar qual versão do Privileged Identity Management você tem. Depois de saber sua versão do Privileged Identity Management, você pode selecionar os procedimentos neste artigo que correspondem a essa versão.

1. Entre no [portal do Azure](#) com um usuário que esteja na função de [administrador de função com privilégios](#).
2. Abra **Azure ad Privileged Identity Management**. Se você tiver uma faixa na parte superior da página Visão geral, siga as instruções na **nova guia versão** deste artigo. Caso contrário, siga as instruções na **guia versão anterior**.

Siga as etapas neste artigo para aprovar ou negar solicitações para funções do Azure AD.

- [Nova versão](#)
- [Versão anterior](#)

## Abrir configurações de função

Siga estas etapas para abrir as configurações de uma função do Azure AD.

- Entre no [portal do Azure](#) com um usuário na função de [administrador de função com privilégios](#).
- Abra **Azure ad Privileged Identity Management** > configurações de função de função de **Azure ad** > **Role settings**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. Below the navigation is a breadcrumb trail: Home > Privileged Identity Management > Settings. The main content area is titled 'Settings' and 'Privileged Identity Management - Azure AD roles'. On the left, there's a sidebar with sections like 'Quick start', 'Tasks' (My roles, Pending requests, Approve requests, Review access), 'Manage' (Roles, Members, Alerts, Access reviews, Settings), and 'Activity' (Resource audit, My audit). The 'Settings' link in the sidebar is highlighted with a red box. The main pane displays a table of roles with columns for Role, Modified, Last updated, and Last updated by. Roles listed include Application Administrator, Cloud Application Administrator, Privileged Role Administrator, Privileged Authentication Administrator, Groups Administrator, Message Center Reader, Application Developer, Security Administrator, External Identity Provider Administrator, User Account Administrator, Security Operator, Device Join, Reports Reader, and Directory Readers.

- Selecione a função cujas configurações você deseja configurar.

The screenshot shows the 'Role setting details - Application Administrator' page. The top navigation bar and breadcrumb trail are identical to the previous screenshot. The main content area is titled 'Role setting details - Application Administrator'. It features a 'Edit' button highlighted with a red box. The page is divided into sections: 'Activation' and 'Assignment'. The 'Activation' section contains settings for activation maximum duration (8 hours), require justification, ticket information, approval, and approvers. The 'Assignment' section contains settings for permanent eligible assignment, expiration, active assignment, and multi-factor authentication requirements. At the bottom, there's a note about sending notifications for member assignments.

- Selecione **Editar** para abrir a página Configurações da função.

Microsoft Azure  Search resources, services, and docs (G+/)

Home > Privileged Identity Management > Settings > Role setting details - Application Administrator >

## Edit role setting - Application Administrator

Privileged Identity Management - Azure AD roles

Activation Assignment Notification

Activation maximum duration (hours)

-----  8

On activation, require  Azure MFA  None

Require justification on activation  
 Require ticket information on activation  
 Require approval to activate

---

Select approver(s) >  
No approver selected

---

**Update** **Next: Assignment**

No painel Configurações de função de cada função, há várias configurações que podem ser configuradas.

## Duração dae atribuição

É possível escolher entre duas opções de duração de atribuição para cada tipo de atribuição (qualificada e ativa) ao definir as configurações de uma função. Essas opções se tornam a duração máxima padrão quando um usuário é atribuído à função no Privileged Identity Management.

Você pode escolher uma destas opções de duração de atribuição **qualificadas** :

|   |   |
|---|---|
| <b>Permitir atribuição qualificada permanente</b> | Administradores globais e administradores de função com privilégios podem atribuir atribuição qualificada permanente.   |
| <b>Expirar atribuição qualificada após</b>        | Administradores globais e administradores de função com privilégios podem exigir que todas as atribuições qualificadas tenham uma data de início e de término especificada. |

E, você pode escolher uma destas opções de duração da atribuição **ativa**:

|   |   |
|---|---|
| <b>Permitir atribuição ativa permanente</b> | Administradores globais e administradores de função com privilégios podem atribuir uma atribuição ativa permanente.   |
| <b>Expirar atribuição ativa após</b>        | Administradores globais e administradores de função com privilégios podem exigir que todas as atribuições ativas tenham uma data de início e de término especificada. |

#### **NOTE**

Todas as atribuições que têm uma data de término especificada podem ser renovadas por administradores globais e administradores de função com privilégios. Além disso, os usuários podem iniciar solicitações de autoatendimento para [estender ou renovar atribuições de função](#).

## Exigir autenticação multifator

O Privileged Identity Management fornece imposição opcional da Autenticação Multifator do Azure para dois cenários diferentes.

### **Exigir Autenticação Multifator na atribuição ativa**

Em alguns casos, talvez você queira atribuir um usuário a uma função por uma duração curta (um dia, por exemplo). Nesse caso, os usuários atribuídos não precisam solicitar ativação. Nesse cenário, Privileged Identity Management não pode impor a autenticação multifator quando o usuário usa sua atribuição de função porque eles já estão ativos na função a partir do momento em que são atribuídos.

Para garantir que o administrador que está atendendo à atribuição seja quem dizem que eles são, você pode impor a autenticação multifator na atribuição ativa marcando a caixa de **atribuição exigir autenticação multifator no Active**.

### **Exigir a Autenticação Multifator na ativação**

Você pode exigir que os usuários qualificados para uma função comprovem quem estão usando a autenticação multifator do Azure antes que possam ser ativados. A autenticação multifator garante que o usuário seja quem dizem que eles estão com certeza razoável. A aplicação dessa opção protege recursos críticos em situações em que a conta do usuário pode ter sido comprometida.

Para exigir a autenticação multifator antes da ativação, marque a caixa **exigir autenticação multifator no modo de ativação** na guia atribuição da configuração **Editar função**.

Para saber mais, confira [Autenticação multifator e Privileged Identity Management](#).

## Duração máxima de ativação

Use o controle deslizante **Duração máxima da ativação** para definir o tempo máximo, em horas, que uma função permanecerá ativa antes de expirar. Esse valor pode ser de uma a 24 horas.

## Exigir justificativa

Você pode exigir que os usuários insiram uma justificativa de negócios ao serem ativados. Para exigir justificativa, marque a caixa **\*\*Exigir justificativa na atribuição ativa \*\*** ou a caixa **Exigir justificativa na ativação**.

## Exigir aprovação para ativar

Se definir vários Aprovadores, a aprovação será concluída assim que um deles for aprovado ou negado. Você não pode exigir aprovação de pelo menos dois usuários. Para exigir aprovação para ativar uma função, siga estas etapas.

1. Marque a caixa de seleção **Exige aprovação para ativar**.

2. Selecione **selecionar aprovadores**.

The screenshot shows the 'Role settings' page for a specific role in the Azure portal. In the 'Activation' section, the 'Activation maximum duration (hours)' is set to 8. Under the 'Select approvers' section, there is a note stating 'No member or group selected'. A modal window titled 'Select a member or group' is open, listing five users: Admin, Admin 2, Alain Charon, Alain Team, and Ann Mack. The 'Selected' status is shown as 'None'.

3. Selecione pelo menos um usuário e clique em **selecionar**. É necessário selecionar pelo menos um aprovador. Não há nenhum aprovador padrão.

Suas seleções serão exibidas na lista de aprovadores selecionados.

4. Depois de especificar todas as suas configurações de função, selecione **Atualizar** para salvar suas alterações.

## Próximas etapas

- [Atribuir funções do Azure AD no Privileged Identity Management](#)
- [Configurar alertas de segurança para funções do Azure AD no Privileged Identity Management](#)

# Configurar alertas de segurança para funções do Azure AD no Privileged Identity Management

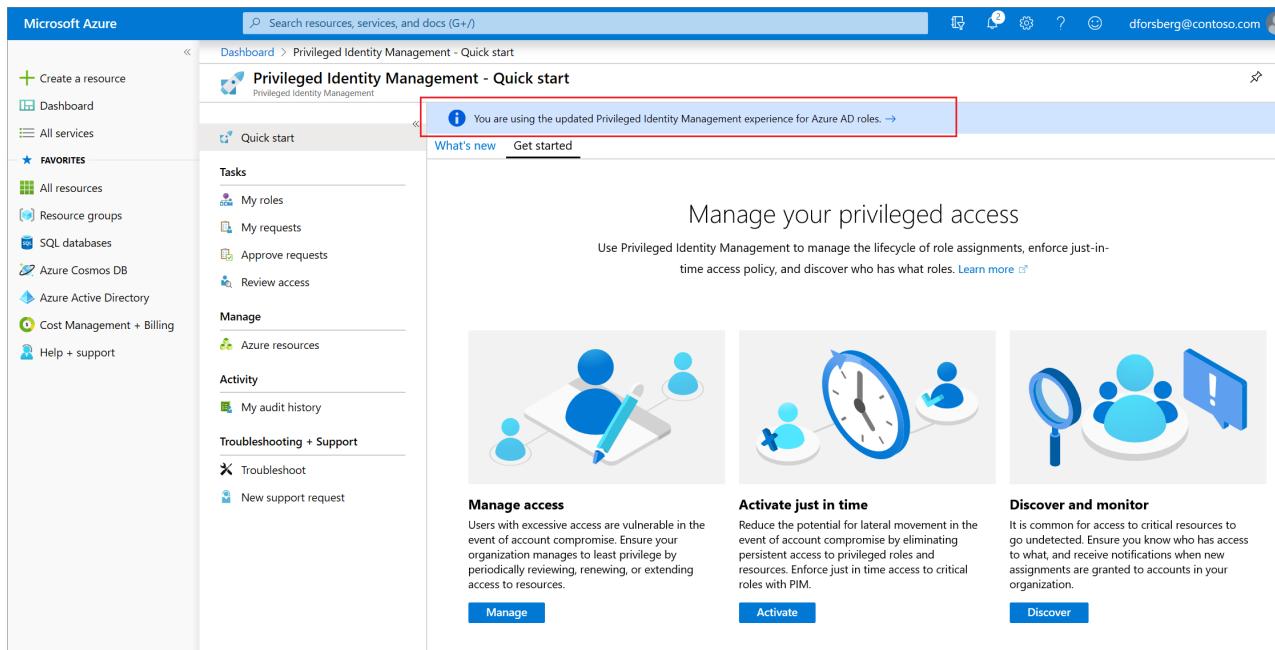
22/07/2020 • 24 minutes to read • [Edit Online](#)

Privileged Identity Management (PIM) gera alertas quando há atividade suspeita ou não segura em sua organização do Azure Active Directory (AD do Azure). Quando um alerta é disparado, ele aparece no painel Privileged Identity Management. Selecione o alerta para ver um relatório que lista os usuários ou as funções que dispararam o alerta.

## Determinar sua versão do PIM

A partir de novembro de 2019, a parte das funções do Azure AD da Privileged Identity Management está sendo atualizada para uma nova versão que corresponde às experiências de funções de recurso do Azure. Isso cria recursos adicionais, bem como [as alterações na API existente](#). Enquanto a nova versão está sendo distribuída, os procedimentos que você seguir neste artigo dependem da versão do Privileged Identity Management que você tem atualmente. Siga as etapas nesta seção para determinar qual versão do Privileged Identity Management você tem. Depois de saber sua versão do Privileged Identity Management, você pode selecionar os procedimentos neste artigo que correspondem a essa versão.

1. Entre no [portal do Azure](#) com um usuário que esteja na função de [administrador de função com privilégios](#).
2. Abra **Azure ad Privileged Identity Management**. Se você tiver uma faixa na parte superior da página Visão geral, siga as instruções na [nova guia versão](#) deste artigo. Caso contrário, siga as instruções na guia **versão anterior**.



Siga as etapas neste artigo para investigar alertas de segurança para funções do Azure AD.

- [Nova versão](#)
- [Versão anterior](#)

| Alert  | Count | Risk level |
|--|-------|------------|
| Roles don't require multi-factor authentication for activation | 12    | Medium     |
| Administrators aren't using their privileged roles             | 15    | Low        |
| Roles are being activated too frequently                       | 1     | Medium     |
| Potential stale accounts in a privileged role                  | 29    | Medium     |

## Alertas de segurança

Esta seção lista todos os alertas de segurança para funções do Azure AD, juntamente com como corrigir e como evitar. Severidade tem o seguinte significado:

- **Alta:** exige ação imediata devido a uma violação da política.
- **Média:** não exige ação imediata, mas sinaliza uma possível violação da política.
- **Baixa:** não requer ação imediata, mas sugere uma alteração de política preferencial.

### Os administradores não estão usando suas funções privilegiadas

|                                    |   |
|------------------------------------|---|
| <b>Severidade</b>                  | Baixo   |
| <b>Por que recebo este alerta?</b> | Os usuários que receberam papéis privilegiados que não precisam aumentam a chance de um ataque. Também é mais fácil para os invasores permanecerem despercebidos nas contas que não estão sendoativamente usadas. |
| <b>Como corrigir?</b>              | Examine os usuários na lista e remova-os das funções privilegiadas que eles não precisam.   |
| <b>Prevenção</b>                   | Atribua funções privilegiadas somente a usuários que têm uma justificativa comercial.<br>Agende revisões de <a href="#">acesso regulares</a> para verificar se os usuários ainda precisam de acesso.              |
| <b>Ação de mitigação no portal</b> | Remove a conta da sua função privilegiada.  |
| <b>Gatilho</b>                     | Disparado se um usuário passar por um número especificado de dias sem ativar uma função.  |
| <b>Número de dias</b>              | Essa configuração especifica o número máximo de dias, de 0 a 100, que um usuário pode ir sem ativar uma função.   |

### Funções não exigem autenticação multifator para ativação

|                                    |  |
|------------------------------------|--|
| <b>Severidade</b>                  | Baixo  |
| <b>Por que recebo este alerta?</b> | Sem a autenticação multifator, os usuários comprometidos podem ativar funções privilegiadas.   |
| <b>Como corrigir?</b>              | Examine a lista de funções e <a href="#">exija a autenticação multifator</a> para cada função. |
| <b>Prevenção</b>                   | <a href="#">Exigir MFA</a> para cada função.   |
| <b>Ação de mitigação no portal</b> | Torna necessária a autenticação multifator para a ativação da função com privilégios.          |

#### A organização não tem Azure AD Premium P2

|                                    |  |
|------------------------------------|--|
| <b>Severidade</b>                  | Baixo  |
| <b>Por que recebo este alerta?</b> | A organização do Azure AD atual não tem Azure AD Premium P2.   |
| <b>Como corrigir?</b>              | Revise informações sobre <a href="#">edições do Microsoft Azure Active Directory</a> . Atualizar para o Microsoft Azure Active Directory Premium P2. |

#### Contas obsoletas possíveis em uma função com privilégios

|                                    |  |
|------------------------------------|--|
| <b>Severidade</b>                  | Médio  |
| <b>Por que recebo este alerta?</b> | As contas em uma função privilegiada não alteraram sua senha nos últimos 90 dias. Essas contas podem ser de serviço ou compartilhadas, que não estejam passando por manutenção e estejam vulneráveis aos invasores.  |
| <b>Como corrigir?</b>              | Examine as contas na lista. Se eles não precisarem mais de acesso, remova-os de suas funções privilegiadas.  |
| <b>Prevenção</b>                   | Certifique-se de que as contas compartilhadas estejam girando senhas fortes quando houver uma alteração nos usuários que conhecem a senha.<br>Examine regularmente as contas com funções privilegiadas usando <a href="#">revisões de acesso</a> e remova as atribuições de função que não são mais necessárias. |
| <b>Ação de mitigação no portal</b> | Remove a conta da sua função privilegiada.   |

|                                     |   |
|-------------------------------------|---|
| <p><b>Práticas recomendadas</b></p> | <p>As contas de acesso compartilhado, de serviço e de emergência que se autenticam usando uma senha e são atribuídas a funções administrativas altamente privilegiadas, como administrador global ou administrador de segurança, devem ter suas senhas giradas para os seguintes casos:</p> <ul style="list-style-type: none"> <li>• Após um incidente de segurança envolvendo uso indevido ou comprometimento de direitos de acesso administrativo</li> <li>• Depois que os privilégios de qualquer usuário são alterados para que eles não sejam mais administradores (por exemplo, depois que um funcionário que era administrador deixa a TI ou deixa a organização)</li> <li>• Em intervalos regulares (por exemplo, trimestral ou anual), mesmo que não haja nenhuma violação ou alteração conhecida na equipe de TI</li> </ul> <p>Como várias pessoas têm acesso às credenciais dessas contas, as credenciais devem ser rotacionadas para garantir que as pessoas que deixaram suas funções não possam mais acessar as contas. <a href="#">Saiba mais sobre como proteger contas</a></p> |
|-------------------------------------|---|

### As funções estão sendo atribuídas fora do Privileged Identity Management

|                             |   |
|-----------------------------|---|
| Severidade                  | Alta  |
| Por que recebo este alerta? | As atribuições de função com privilégios feitas fora do Privileged Identity Management não são monitoradas corretamente e podem indicar um ataque ativo.        |
| Como corrigir?              | Examine os usuários na lista e remova-os das funções privilegiadas atribuídas fora do Privileged Identity Management.   |
| Prevenção                   | Investigue onde os usuários estão sendo atribuídos a funções privilegiadas fora do Privileged Identity Management e proíba as atribuições futuras a partir daí. |
| Ação de mitigação no portal | Remove o usuário de sua função privilegiada.  |

### Há muitos administradores globais

|                             |   |
|-----------------------------|---|
| Severidade                  | Baixo   |
| Por que recebo este alerta? | O administrador global é a função com privilégios mais altos. Se um administrador global estiver comprometido, o invasor ganhará acesso a todas as suas permissões, o que coloca todo o sistema em risco. |
| Como corrigir?              | Examine os usuários na lista e remova qualquer que não precise absolutamente da função de administrador global. Em vez disso, atribua funções com privilégios inferiores a esses usuários.                |

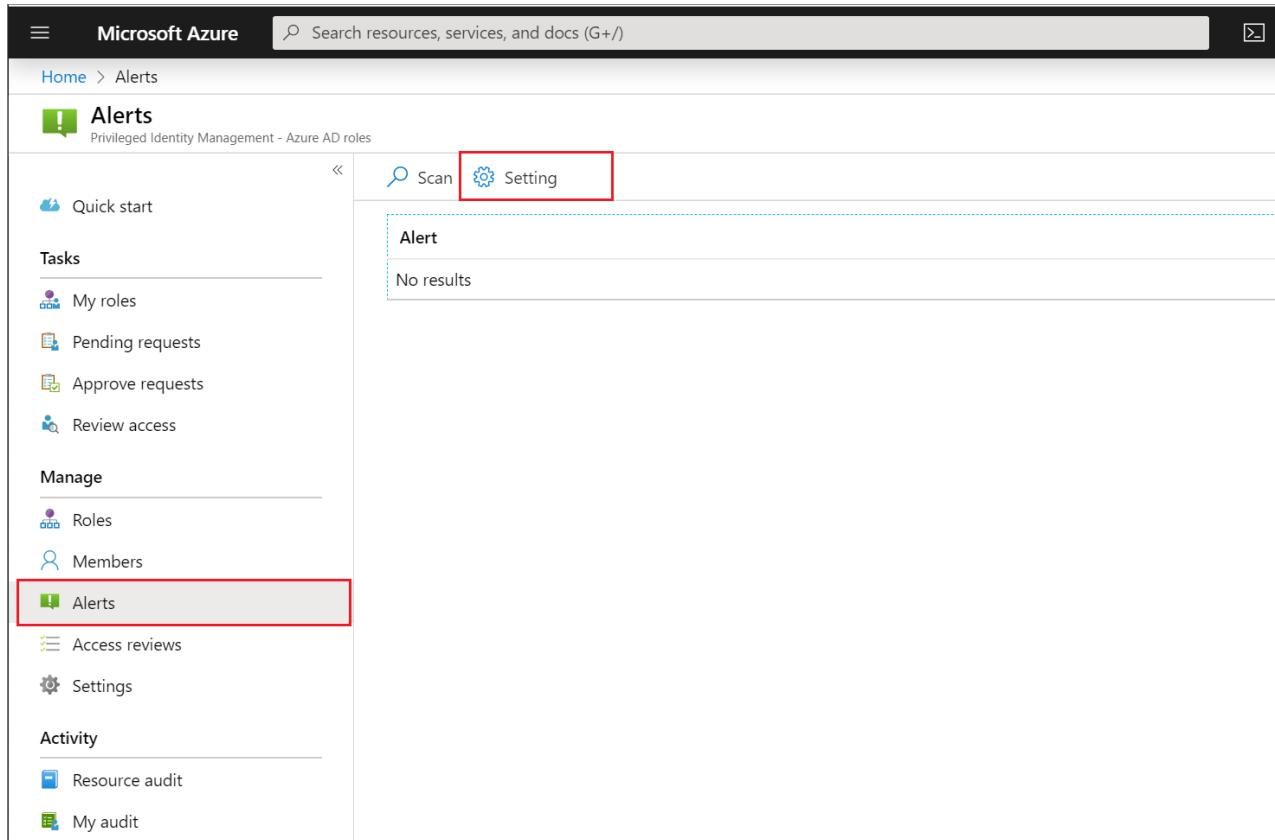
|   |  |
|---|--|
| <b>Prevenção</b>                                | Designe aos usuários a função menos privilegiada de que precisam.  |
| <b>Ação de mitigação no portal</b>              | Remove a conta da sua função privilegiada.   |
| <b>Gatilho</b>                                  | Acionado se dois critérios diferentes forem atendidos e você puder configurar ambos. Primeiro, você precisa alcançar um certo limite de administradores globais. Em segundo lugar, um determinado percentual de suas atribuições de função total deve ser administradores globais. Se você atender apenas a uma dessas medidas, o alerta não será exibido. |
| <b>Número mínimo de administradores globais</b> | Essa configuração especifica o número de administradores globais, de 2 a 100, que você considera muito poucos para sua organização do Azure AD.  |
| <b>Percentual de administradores globais</b>    | Essa configuração especifica o percentual mínimo de administradores que são administradores globais, de 0% a 100%, abaixo do qual você não deseja que sua organização do Azure AD seja DIP.  |

#### As funções estão sendo ativadas com muita frequência

|  |   |
|--|---|
| <b>Severidade</b>                                | Baixo   |
| <b>Por que recebo este alerta?</b>               | Múltiplas ativações para o mesmo papel privilegiado pelo mesmo usuário é um sinal de um ataque.   |
| <b>Como corrigir?</b>                            | Revise os usuários na lista e assegure-se de que a <a href="#">duração da ativação</a> para sua função privilegiada esteja definida por tempo suficiente para que eles executem suas tarefas.   |
| <b>Prevenção</b>                                 | Assegure-se de que a <a href="#">duração da ativação</a> para funções privilegiadas esteja definida por tempo suficiente para que os usuários executem suas tarefas.<br><a href="#">Exigir autenticação multifator</a> para funções privilegiadas que têm contas compartilhadas por vários administradores. |
| <b>Ação de mitigação no portal</b>               | N/D   |
| <b>Gatilho</b>                                   | Disparado se um usuário ativar a mesma função privilegiada várias vezes dentro de um período especificado. Você pode configurar o período e o número de ativações.  |
| <b>Período de tempo de renovação de ativação</b> | Essa configuração especifica em dias, horas, minutos e segundos o período de tempo que você deseja usar para rastrear renovações suspeitas.   |
| <b>Número de renovações de ativação</b>          | Essa configuração especifica o número de ativações, de 2 a 100, em que você deseja ser notificado, dentro do período de tempo escolhido. Você pode mudar essa configuração movendo o controle deslizante ou digitando um número na caixa de texto.  |

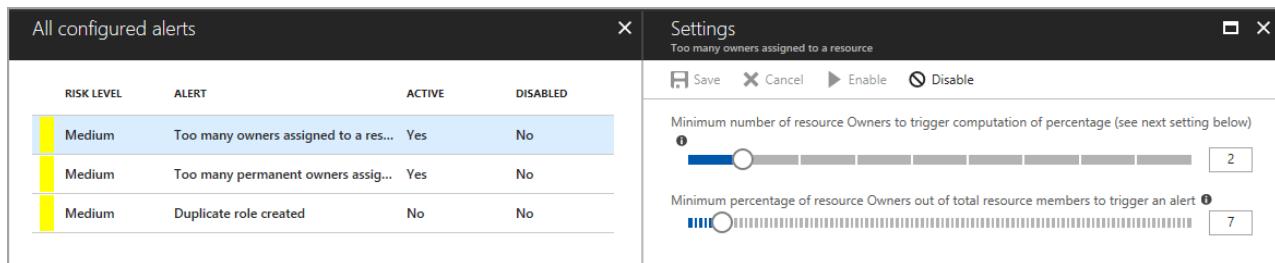
# Definir configurações de alerta de segurança

Na página Alertas, vá para Configurações.



The screenshot shows the Microsoft Azure Privileged Identity Management - Azure AD roles interface. On the left, there's a sidebar with sections like 'Tasks', 'Manage', and 'Activity'. Under 'Manage', the 'Alerts' item is selected and highlighted with a red box. At the top right, there are two buttons: 'Scan' and 'Setting', with 'Setting' also highlighted with a red box. The main area is titled 'Alert' and displays the message 'No results'.

Personalize configurações nos diferentes alertas para trabalhar com seu ambiente e as metas de segurança.



The screenshot shows the 'All configured alerts' table. It has columns for RISK LEVEL, ALERT, ACTIVE, and DISABLED. There are three rows, all of which are highlighted with a blue background. The first row contains: Medium, Too many owners assigned to a res..., Yes, No. The second row contains: Medium, Too many permanent owners assig..., Yes, No. The third row contains: Medium, Duplicate role created, No, No. To the right of the table is a 'Settings' dialog box for the first alert. It has tabs for 'Save', 'Cancel', 'Enable', and 'Disable'. It includes settings for 'Minimum number of resource Owners to trigger computation of percentage' (set to 2) and 'Minimum percentage of resource Owners out of total resource members to trigger an alert' (set to 7).

## Próximas etapas

- Definir as configurações de função do Azure AD no Privileged Identity Management

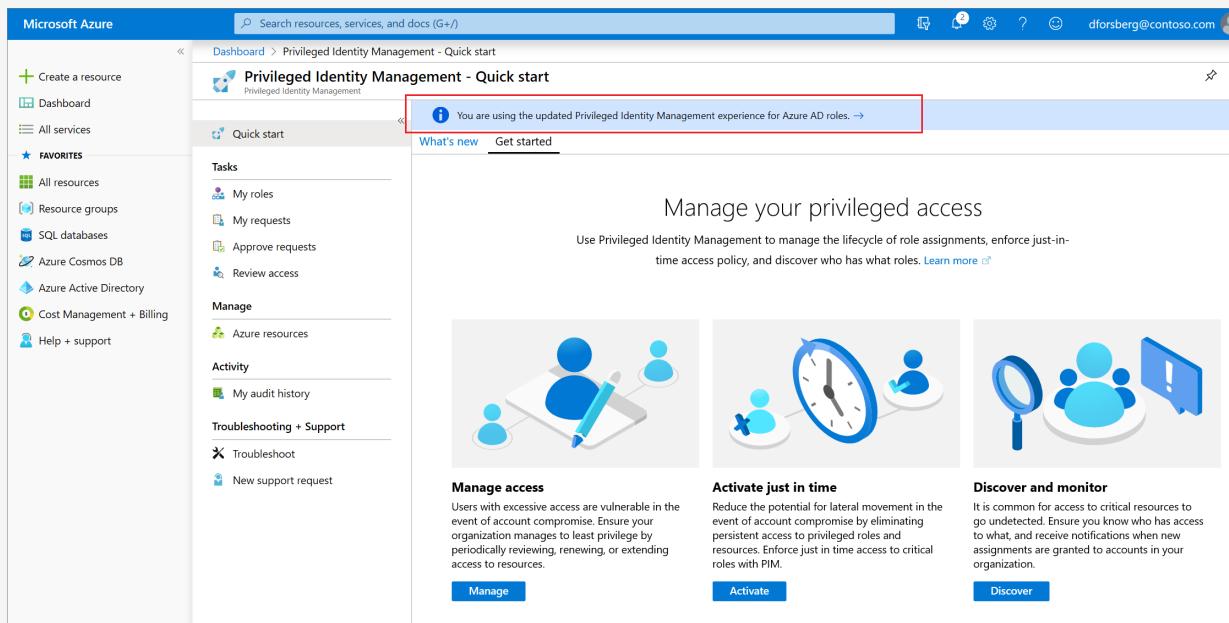
# Ativar uma função personalizada do Azure AD no PIM (Privileged Identity Management)

22/07/2020 • 4 minutes to read • [Edit Online](#)

O Privileged Identity Management no Azure AD (Active Directory) agora dá suporte à atribuição Just-In-Time e de limite de tempo a funções personalizadas criadas para Gerenciamento de Aplicativos na experiência administrativa de Gerenciamento de Identidades e Acesso. Para saber mais sobre como criar funções personalizadas para delegar o gerenciamento de aplicativos no Azure AD, confira [Funções Administrador personalizadas no Azure Active Directory \(versão prévia\)](#).

## NOTE

As funções personalizadas do Azure AD não são integradas às funções de diretório internas durante a versão prévia. Depois que a funcionalidade estiver em disponibilidade geral, o gerenciamento de função ocorrerá na experiência de funções internas. Se você vir a seguinte faixa, essas funções deverão ser gerenciadas [na experiência de funções internas](#) e este artigo não se aplicará:



## Ativar uma função

Quando precisar ativar uma função personalizada do Azure AD, solicite a ativação selecionando a opção de navegação minhas funções em Privileged Identity Management.

1. Entre no [portal do Azure](#).
2. Abra o Azure AD [Privileged Identity Management](#).
3. Selecione **funções personalizadas do Azure AD** para ver uma lista de atribuições de função personalizadas do Azure AD elegíveis.

**Página inicial > Fotografia f/128 - Visão geral > Privileged Identity Management - Início rápido**

## Privileged Identity Management - Início rápido

**Início rápido**

**Tarefas**

- Minhas funções
- Minhas solicitações
- Aprovar solicitações
- Análise de acesso

**Gerenciar**

- Funções do Azure AD
  - Funções personalizadas do Azure Active Directory ...
  - Recursos do Azure

**Atividade**

**Introdução**  
→ Proteja sua empresa. Gerencie e restrinja o acesso privilegiado

[Azure AD Privileged Identity Management](#)  
Módulo PowerShell do Azure AD Privileged Identity Management  
Azure AD Privileged Identity Management para funções de recursos do Azure

**Novidades do Privileged Identity Management**

Todos os serviços  
 Azure Active Directory  
 Recursos do Azure

**Atualização de recursos**  
Azure Active Directory

**Experiência de ativação aprimorada**  
Sexta-feira, 22 de março de 2019

#### NOTE

Antes de atribuir uma função, você deve criar/configurar uma função. Para obter mais informações sobre como configurar funções personalizadas do AAD, consulte [aqui] (<https://docs.microsoft.com/azure/active-directory/privileged-identity-management/azure-ad-custom-roles-configure>)

1. Na página **funções personalizadas do Azure AD (versão prévia)**, localize a atribuição de que você precisa.
2. Selecione **Ativar sua função** para abrir a página **Ativar**.
3. Se sua função exigir autenticação multifator, selecione **Verificar sua identidade antes de prosseguir**. Você precisa se autenticar apenas uma vez por sessão.
4. Selecione **Verificar minha identidade** e siga as instruções para fornecer qualquer verificação de segurança adicional.
5. Para especificar um escopo de aplicativo personalizado, selecione **Escopo** para abrir o painel de filtro. Você deve solicitar acesso a uma função no escopo mínimo necessário. Se sua atribuição estiver em um escopo de aplicativo, você poderá ativar somente nesse escopo.

Página inicial > Privileged Identity Management > Contoso - Funções > Administrador de credenciais de registro de aplicativo

|   |   |
|---|---|
| <p><b>Nova atribuição</b></p> <p>Administrador de credenciais de registro de aplicativo</p> <p><b>Escopo</b></p> <p>Amazon Web Services (AWS)</p> <p>* Seleccionar uma função &gt;</p> <p>Credencial de registro do aplicativo...</p> <p>* Seleccionar um membro &gt;</p> <p>Timothy Perkins</p> <p>* Definir configurações de associação &gt;</p> <p>Configurações personalizadas selecio...</p> <p><b>Adicionar</b></p> | <p><b>Escopo</b></p> <p>Pesquisar por nome de recurso</p> <p>Amazon Web Services (AWS)</p> <p>ztest</p> <p>Declaração de grupo</p> <p><b>Recursos selecionados (1)</b></p> <p>Amazon Web Services (AWS) <b>Remover</b></p> <p><b>Selecionar</b></p> |
|---|---|

6. Se necessário, especifique uma hora de início de ativação. Quando usado, o membro da função é ativado na hora especificada.
7. Na caixa **Motivo**, insira o motivo da solicitação de ativação. Eles podem ser tornados obrigatórios ou não na configuração da função.
8. Selecione **Ativar**.

Se a função não exigir aprovação, ela já estará ativada de acordo com suas configurações e será adicionada à lista de funções ativas. Se desejar usar a função ativada, comece com as etapas em [Atribuir uma função personalizada do Azure AD no Privileged Identity Management](#).

Se a função exigir aprovação para ser ativada, você receberá uma notificação do Azure informando-o de que a solicitação está com aprovação pendente.

## Próximas etapas

- [Atribuir uma função personalizada do Azure AD](#)
- [Remover ou atualizar uma atribuição de função personalizada do Azure AD](#)
- [Configurar uma atribuição de função personalizada do Azure AD](#)
- [Definições de função no Azure AD](#)

# Atribuir uma função personalizada do Azure AD no PIM (Privileged Identity Management)

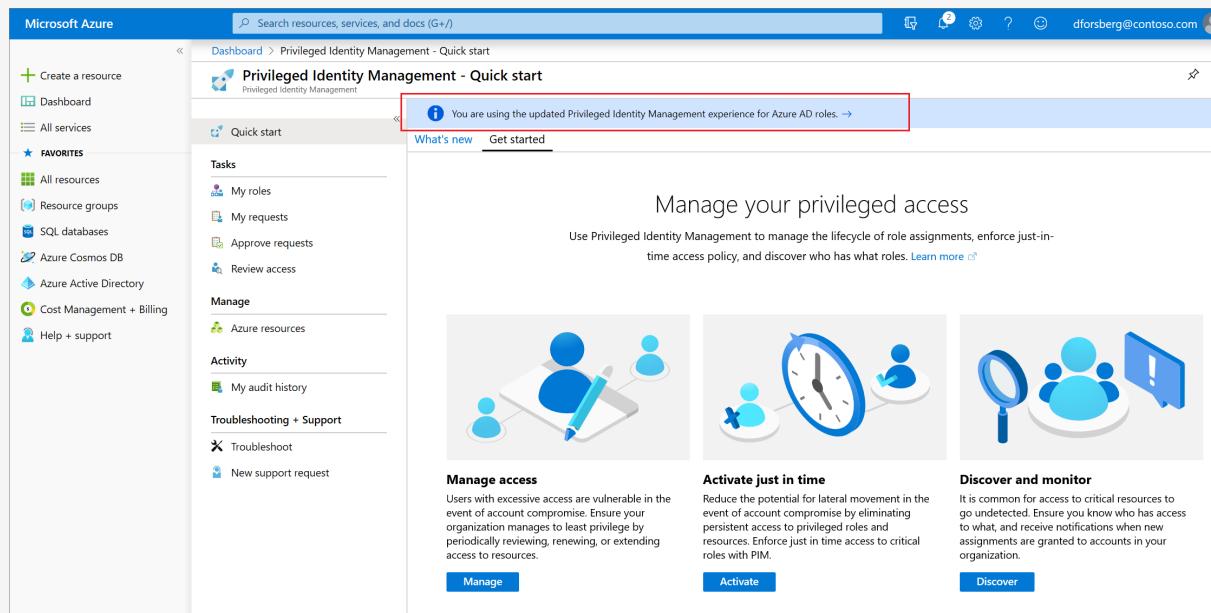
22/07/2020 • 5 minutes to read • [Edit Online](#)

Este artigo informa como usar o PIM (Privileged Identity Management) para criar a atribuição Just-In-Time e com limite de tempo a funções personalizadas criadas para gerenciar aplicativos na experiência administrativa do Azure AD (Azure Active Directory).

- Para saber mais sobre como criar funções personalizadas para delegar o gerenciamento de aplicativos no Azure AD, confira [Funções Administrador personalizadas no Azure Active Directory \(versão prévia\)](#).
- Se você ainda não usou o Privileged Identity Management, obtenha mais informações em [Começar a usar o Privileged Identity Management](#).
- Para obter informações sobre como conceder a outro administrador acesso para gerenciar Privileged Identity Management, consulte [conceder acesso a outros administradores para gerenciar Privileged Identity Management](#).

## NOTE

As funções personalizadas do Azure AD não são integradas às funções de diretório internas durante a versão prévia. Depois que a funcionalidade estiver em disponibilidade geral, o gerenciamento de função ocorrerá na experiência de funções internas. Se você vir a seguinte faixa, essas funções deverão ser gerenciadas [na experiência de funções internas](#) e este artigo não se aplicará:



## Atribuir uma função

O Privileged Identity Management pode gerenciar funções personalizadas que você cria no gerenciamento de aplicativos do Azure AD (Active Directory). As etapas a seguir fazem uma atribuição qualificada para uma função do diretório personalizada.

1. Entre no [Privileged Identity Management](#) no portal do Azure com uma conta de usuário atribuída à função de administrador de funções com privilégios.
2. Selecione [funções personalizadas do Azure AD \(versão prévia\)](#).

**Privileged Identity Management - Início rápido**

**Tarefas**

- Minhas funções
- Minhas solicitações
- Aprovar solicitações
- Análise de acesso

**Gerenciar**

- Funções do Azure AD
  - Funções personalizadas do Azure Active Directory ...
  - Recursos do Azure

**Atividade**

**Introdução**  
Proteja sua empresa. Gerencie e restrinja o acesso privilegiado

[Azure AD Privileged Identity Management](#)  
Módulo PowerShell do Azure AD Privileged Identity Management  
Azure AD Privileged Identity Management para funções de recursos do Azure

**Novidades do Privileged Identity Management**

Todos os serviços  
 Azure Active Directory  
 Recursos do Azure

**Atualização de recursos**  
Azure Active Directory  
[Experiência de ativação aprimorada](#)  
Sexta-feira, 22 de março de 2019

3. Selecione **Funções** para ver a lista de funções personalizadas para aplicativos do Azure AD.

**Contoso - Funções**

**Tarefas**

- Minhas funções
- Solicitações pendentes
- Aprovar solicitações

**Gerenciar**

- Funções
- Membros
- Configurações

**Atividade**

**Adicionar membro**

| FUNÇÃO   | Descrição |
|--|-----------|
| Administrador de credenciais de registro de aplicativo |           |
| Administrador de suporte do aplicativo                 |           |
| Administrador Contoso                                  |           |

4. Selecione **Adicionar membro** para abrir a página de atribuição.

5. Para restringir o escopo da atribuição de função para um único aplicativo, selecione **Escopo** para especificar um escopo de aplicativo.

Painel > Privileged Identity Management > FIMDEV - Funções > Nova atribuição > Escopo

**Nova atribuição**

**Escopo**

Escopo  
Diretório (Padrão)

Selecionar uma função  
Nenhuma função selecionada

Selecionar um membro  
Nenhum membro selecionado

Definir configurações de associação  
Configuração padrão selecionada

**Test Deb**

**example-app**

**ExpenseReport Single-Tenant App**

**Liebersoft**

**anujitest1**

**t-pado-autoroleassign**

**AADIGI Tester**

**test3 pls**

**Recursos selecionados (0)**

Nenhum recurso selecionado

6. Selecione Selecionar uma função para abrir a lista Selecionar uma função.

**Nova atribuição**

**Selecionar uma função**

Selecionar função única a partir da lista

Escopo  
example-app

Selecionar uma função  
Nenhuma função selecionada

Selecionar um membro  
Nenhum membro selecionado

Definir configurações de associação  
Configuração padrão selecionada

**FUNÇÃO**

anujcRole11111

Administrador de Assistência técnica ...

applicationsallpropertiesupdate

applicationsaudienceupdate

applicationsauthenticationupdate

applicationsbasicupdate

applicationscreate

applicationscreateasowner

applicationscredentialsupdate

7. Selecione uma função que você deseja atribuir e clique em Selecionar. A lista Selecionar um membro é aberta.

**Microsoft Azure**

Página inicial > Contoso - Funções > Nova atribuição > Selecionar um membro

**Nova atribuição**

- Escopo >
- Selecionar uma função >
- Selecionar um membro** > **Nenhum membro selecionado**
- Definir configurações de associação > *Configuração padrão selecionada*

**Selecionar um membro**

Selecionar ⓘ  
tper ✓

Timothy Perkins  
tperkins@contoso.com

Membro selecionado:  
Nenhum membro selecionado

**Selecionar**

8. Selecione um usuário a quem você deseja atribuir a função e, em seguida, clique em **Selecionar**. A lista **Configurações de Associação** é aberta.

Página inicial > Contoso - Funções > Nova atribuição > Configurações de associação

**Nova atribuição**

- Escopo >
- Selecionar uma função >
- Administrador de credenciais de ...
- Selecionar um membro > Timothy Perkins
- Definir configurações de associação > *Configuração padrão selecionada*

**Configurações de associação**

Tipo de atribuição

- Qualificado
- Qualificado
- Ativo

\* Início da atribuição  
09-08-2019 08:25:24

\* Fim da atribuição  
08-08-2020 08:25:24

**Salvar**

9. Na página **Configurações de associação**, selecione **Qualificada** ou **Ativa**:

- Atribuições **Qualificadas** exigem que o usuário atribuído à função execute uma ação antes de poder usar a função. As ações podem incluir a passagem de uma verificação de autenticação multifator, o fornecimento de uma justificativa comercial ou a solicitação da aprovação de aprovadores designados.
- Atribuições **Ativas** não exigem que o usuário atribuído execute nenhuma ação para usar a função. Usuários ativos têm os privilégios atribuídos à função sempre.

10. Se a caixa de seleção **Permanente** estiver presente e disponível (dependendo das configurações de função), você poderá especificar se a atribuição é permanente. Marque a caixa de seleção para tornar a atribuição permanentemente qualificada ou permanentemente atribuída. Desmarque a caixa de seleção

para especificar a duração de uma atribuição.

11. Para criar a atribuição de função, clique em **Salvar** e, em seguida, em **Adicionar**. Uma notificação do status do processo da atribuição é exibida.

Para verificar a atribuição de função, em uma função aberta, selecione **atribuições** > **atribuir** e verifique se a atribuição de função está corretamente identificada como qualificada ou ativa.

Página inicial > Contoso - Funções > Administrador de credenciais de registro de aplicativo - Atribuições

Administrador de credenciais de registro de aplicativo - Atribuições

Gerenciar

Atribuições

Adicionar membro Configurações Atualizar Exportar

Funções qualificáveis Funções ativas **Funções expiradas**

Pesquisar por nome de membro

| NOME   | NOME UPN                            | SCOPO     | ASSOCIAÇÃO | ESTADO    |
|--|-------------------------------------|-----------|------------|-----------|
| ADMINISTRADOR DE CREDENCIAIS DE REGISTRO DE APLICATIVO | Timothy Perkins tperkins@contoso.cc | Directory | Direto     | Atribuído |

## Próximas etapas

- [Ativar uma função personalizada do Azure AD](#)
- [Remover ou atualizar uma atribuição de função personalizada do Azure AD](#)
- [Configurar uma atribuição de função personalizada do Azure AD](#)
- [Definições de função no Azure AD](#)

# Atualizar ou remover uma função personalizada do Azure AD atribuída no Privileged Identity Management

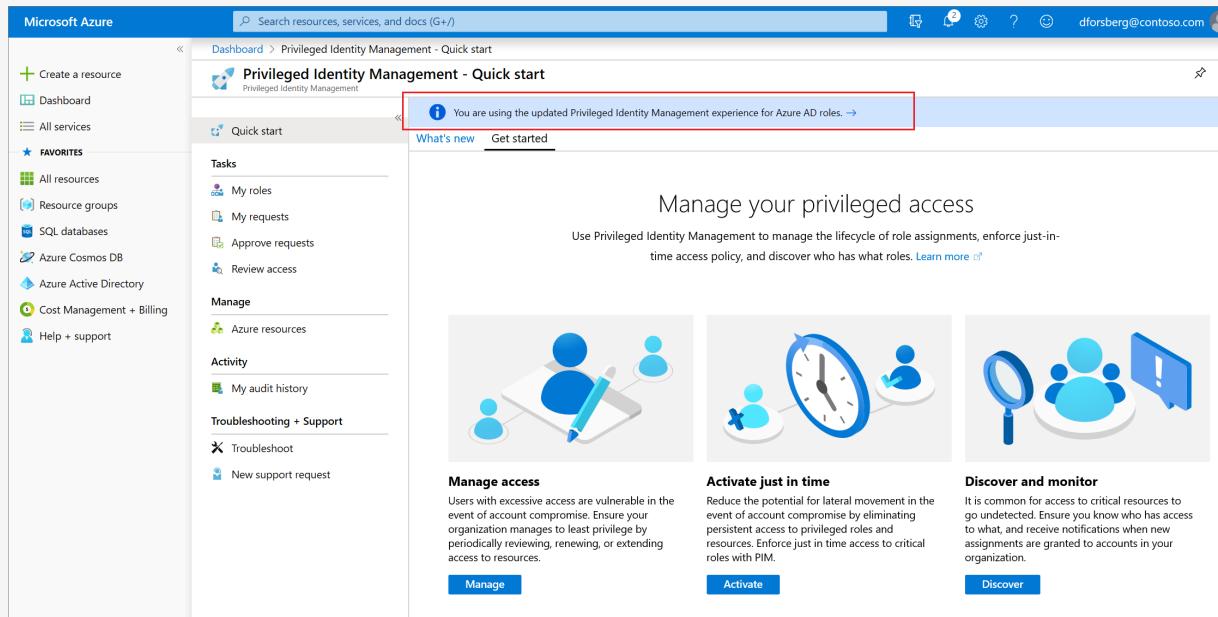
22/07/2020 • 2 minutes to read • [Edit Online](#)

Este artigo informa como usar o PIM (Privileged Identity Management) para atualizar ou remover a atribuição Just-In-Time e com limite de tempo a funções personalizadas criadas para gerenciamento de aplicativos na experiência administrativa do Azure AD (Azure Active Directory).

- Para saber mais sobre como criar funções personalizadas para delegar o gerenciamento de aplicativos no Azure AD, confira [Funções Administrador personalizadas no Azure Active Directory \(versão prévia\)](#).
- Se você ainda não usou o Privileged Identity Management, obtenha mais informações em [Começar a usar o Privileged Identity Management](#).

## NOTE

As funções personalizadas do Azure AD não são integradas às funções de diretório internas durante a versão prévia. Depois que a funcionalidade estiver em disponibilidade geral, o gerenciamento de função ocorrerá na experiência de funções internas. Se você vir a seguinte faixa, essas funções deverão ser gerenciadas [na experiência de funções internas](#) e este artigo não se aplicará:



## Atualizar ou remover uma atribuição

Siga estas etapas para atualizar ou remover uma atribuição de função personalizada existente.

1. Entre no [Privileged Identity Management](#) no portal do Azure com uma conta de usuário atribuída à função de administrador de funções com privilégios.
2. Selecione [funções personalizadas do Azure AD \(versão prévia\)](#).

**Privileged Identity Management - Início rápido**

**Tarefas**

- Minhas funções
- Minhas solicitações
- Aprovar solicitações
- Análise de acesso

**Gerenciar**

- Funções do Azure AD
  - Funções personalizadas do Azure Active Directory ...
- Recursos do Azure

**Atividade**

**Introdução**  
Proteja sua empresa. Gerencie e restrinja o acesso privilegiado

[Azure AD Privileged Identity Management](#)  
Módulo PowerShell do Azure AD Privileged Identity Management  
Azure AD Privileged Identity Management para funções de recursos do Azure

**Novidades do Privileged Identity Management**

- Todos os serviços
- Azure Active Directory
- Recursos do Azure

[Atualização de recursos](#)  
Azure Active Directory  
[Experiência de ativação aprimorada](#)  
Sexta-feira, 22 de março de 2019

- Selecione **Funções** para ver a lista de **Atribuições** de funções personalizadas para aplicativos do Azure AD.

| NOME          | NOME UPN          | ESCOPO      |
|---------------|-------------------|-------------|
| ANUJCROLE1111 |                   |             |
| Tom Smith     | tsmith@fimdev.net | example-app |
| Tom Smith     | tsmith@fimdev.net | Liebersoft  |

- Selecione a função que você deseja atualizar ou remover.
- Localize a atribuição de função nas guias **Funções qualificadas** ou **Funções ativas**.
- Selecione **Atualizar** ou **Remover** para atualizar ou remover a atribuição de função.

| Funções qualificáveis        | Funções ativas                   | Funções expiradas |            |                      |                          |  |
|------------------------------|----------------------------------|-------------------|------------|----------------------|--------------------------|--|
| Pesquisar por nome de membro |                                  |                   |            |                      |                          |  |
| NOME                         | NOME UPN                         | ESCOPO            | ASSOCIAÇÃO | HORA DE INÍCIO       | HORA DE TÉRMINO          | AÇÃO   |
| <b>ANUJROLE11111</b>         |                                  |                   |            |                      |                          |  |
| Tom Smith                    | tsmith@fimdev.net                | example-app       | Direto     | 07/06/2019, 12:48:15 | 05/09/2019, 12:48:02     | <a href="#">Remover</a>   <a href="#">Atualizar</a>   Estender |
| Tom Smith                    | tsmith@fimdev.net                | Liebersoft        | Direto     | 07/06/2019, 13:17:46 | 05/09/2019, 13:17:37     | <a href="#">Remover</a>   <a href="#">Atualizar</a>   Estender |
| nawu                         | nawu@fimdev.net                  | Directory         | Direto     | 17/07/2019, 14:34:37 | 30/09/2019, 13:15:35     | <a href="#">Remover</a>   <a href="#">Atualizar</a>   Estender |
| Lizhang Sun                  | lizsun@fimdev.net                | Directory         | Direto     | 25/07/2019, 21:09:59 | Permanente               | <a href="#">Remover</a>   <a href="#">Atualizar</a>   Estender |
| anajcuser                    | anujcuser@fimdev.net             | anujtest1         | Direto     | 17/07/2019, 12:38:46 | 15/10/2019, 12:38:37 ... | <a href="#">Remover</a>   <a href="#">Atualizar</a>   Estender |
| Bhaskar                      | vikama@fimdev.net                | Directory         | Direto     | 25/07/2019, 21:15:48 | Permanente               | <a href="#">Remover</a>   <a href="#">Atualizar</a>   Estender |
| Gaurav Mishra                | gmish@fimdev.net                 | example-app       | Direto     | 06/06/2019, 20:23:07 | 04/09/2019, 20:22:56     | <a href="#">Remover</a>   <a href="#">Atualizar</a>   Estender |
| 312steve                     | 321steve_gmailcom#EXT#@fimdev.on | example-app       | Direto     | 27/06/2019, 13:27:02 | 25/09/2019, 13:26:55     | <a href="#">Remover</a>   <a href="#">Atualizar</a>   Estender |

## Próximas etapas

- [Ativar uma função personalizada do Azure AD](#)
- [Atribuir uma função personalizada do Azure AD](#)
- [Configurar uma atribuição de função personalizada do Azure AD](#)

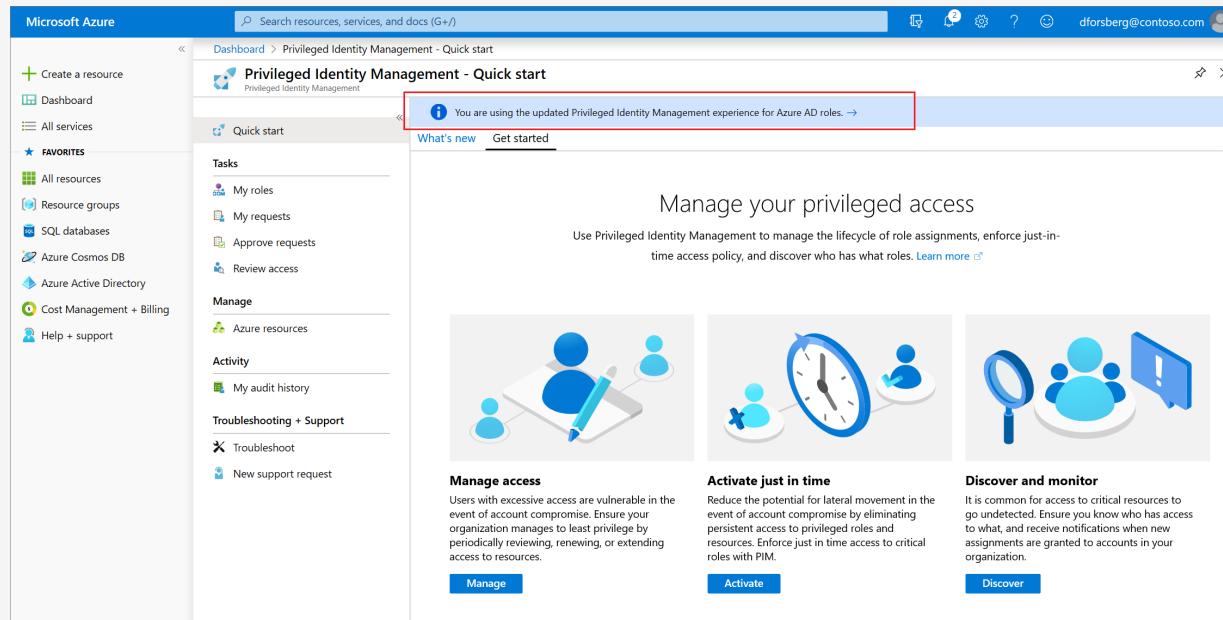
# Configurar funções personalizadas do Azure AD no Privileged Identity Management

22/07/2020 • 6 minutes to read • [Edit Online](#)

Um administrador de funções com privilégios pode alterar as configurações de função que se aplicam a um usuário quando eles ativam sua atribuição a uma função personalizada e a outros administradores de aplicativo que estão atribuindo funções personalizadas.

## NOTE

As funções personalizadas do Azure AD não são integradas às funções de diretório internas durante a versão prévia. Depois que a funcionalidade estiver em disponibilidade geral, o gerenciamento de função ocorrerá na experiência de funções internas. Se você vir a seguinte faixa, essas funções deverão ser gerenciadas [na experiência de funções internas](#) e este artigo não se aplicará:



## Abrir configurações de função

Siga estas etapas para abrir as configurações de uma função do Azure AD.

1. Entre no [Privileged Identity Management](#) no portal do Azure com uma conta de usuário atribuída à função de administrador de funções com privilégios.
2. Selecione **funções personalizadas do Azure AD (versão prévia)**.

## Contoso - Configurações

« Atualizar

Pesquisar por nome de função

| FUNÇÃO   | MODIFICADO | ÚLTIMA ATUALIZAÇÃO |
|--|------------|--------------------|
| Administrador de suporte do aplicativo                 | Não        | -                  |
| Administrador de credenciais de registro de aplicativo | Não        | -                  |
| Administrador Contoso                                  | Não        | -                  |

3. Selecione **Configuração** para abrir a página **Configurações**. Selecione a função para as configurações que você deseja definir.
4. Selecione **Editar** para abrir a página **Configurações da função**.

## Detalhes da configuração da função

applicationsmyorganizationauthenticationupdate



Editar

### Atribuição

| CONFIGURAÇÃO  | ESTADO  |
|---|---------|
| Permitir atribuição permanente qualificável                           | Não     |
| Expirar atribuições qualificáveis depois                              | 3 meses |
| Permitir atribuição permanente ativa                                  | Não     |
| Expirar atribuições ativas depois                                     | 1 mês   |
| Exigir Autenticação Multifator do Microsoft Azure na atribuição ativa | Não     |
| Exigir justificativa na atribuição ativa                              | Sim     |

### Ativação

| CONFIGURAÇÃO  | ESTADO  |
|---|---------|
| Duração máxima da ativação (horas)                            | 8 horas |
| Exigir Autenticação Multifator do Microsoft Azure na ativação | Não     |
| Exigir justificativa na ativação                              | Sim     |
| Exigir informações de tíquete na ativação                     | Sim     |
| Exigir aprovação para ativar esta função                      | Não     |
| Aprovadores   | Nenhum  |

## Configurações de função

Há várias configurações que você pode definir.

### Duração da atribuição

É possível escolher entre duas opções de duração de atribuição para cada tipo de atribuição (qualificada ou ativa) ao definir as configurações de uma função. Essas opções passam a ter a duração máxima padrão quando um membro é atribuído à função no Privileged Identity Management.

É possível escolher uma destas opções de duração de atribuição *qualificada*.

- **Permitir atribuição qualificada permanente:** os administradores podem atribuir uma associação qualificada permanente.
- **Expirar atribuição qualificada após:** os administradores podem exigir que todas as atribuições qualificadas tenham uma data de início e de término especificada.

Além disso, você pode escolher uma destas opções de duração da atribuição *ativa*:

- **Permitir atribuição ativa permanente:** os administradores podem atribuir uma associação ativa permanente.
- **Expirar atribuição ativa após:** os administradores podem exigir que todas as atribuições ativas tenham uma data de início e de término especificada.

#### **Exigir autenticação multifator do Azure**

O Privileged Identity Management fornece imposição opcional da Autenticação Multifator do Azure para dois cenários diferentes.

- **Exigir Autenticação Multifator na atribuição ativa**

Se você quiser atribuir um membro a uma função por uma curta duração (por exemplo, um dia), poderá demorar muito para exigir que os membros atribuídos solicitem a ativação. Nesse cenário, o Privileged Identity Management não pode impor a autenticação multifator quando o usuário ativa sua atribuição de função, pois já está ativo na função desde o momento em que ele é atribuído. Para verificar se o administrador que atende à atribuição é quem ele diz que é, marque a caixa **Exigir Autenticação Multifator na atribuição ativa**.

- **Exigir a Autenticação Multifator na ativação**

Você pode exigir que usuários qualificados atribuídos a uma função se inscrevam na Autenticação Multifator do Azure antes de poderem ativar. Esse processo garante que o usuário solicitando ativação seja quem diz ser com uma certeza razoável. A imposição dessa opção protege funções críticas em situações em que a conta do usuário pode ter sido comprometida. Para solicitar que um membro qualificado execute a Autenticação Multifator do Azure antes da ativação, marque a caixa **Exigir Autenticação Multifator na ativação**.

Para saber mais, confira [Autenticação multifator e Privileged Identity Management](#).

#### **Duração máxima de ativação**

Use o controle deslizante **Duração máxima da ativação** para definir o tempo máximo, em horas, que uma função permanecerá ativa antes de expirar. Esse valor pode ser de 1 a 24 horas.

#### **Exigir justificativa**

É possível exigir que os membros insiram uma justificativa na atribuição ativa ou quando são ativados. Para exigir justificativa, marque a caixa de seleção **Exigir justificativa na atribuição ativa** ou a caixa **Exigir justificativa na ativação**.

#### **Exigir aprovação para ativar**

Se você quiser exigir aprovação para ativar uma função, siga estas etapas.

1. Marque a caixa de seleção **Exigir aprovação para ativar**.
2. Selecione **Selecionar aprovadores** para abrir a lista **Selecionar um membro ou grupo**.

Página inicial > Pay-As-You-Go - Configurações de função > Detalhes da configuração da função > Configurações de função > Selecionar um membro ou grupo

Configurações de função

Selecionar um membro ou grupo

Exigir Autenticação Multifator na atribuição ativa

Exigir justificativa na atribuição ativa

**Ativação**

Duração máxima da ativação (horas)

8

Exigir Autenticação Multifator na ativação

Exigir justificativa na ativação

Exigir aprovação para ativar esta função

**Selecionar aprovadores**

Nenhum membro ou grupo selecionado

**Selecionar**

Convidar

Selecionar

Pesquisar por nome ou endereço de email

AD Admin admin@

A2 Admin 2 admin2@

AC Alain Charon alain@

AT Alain Team

AM Ann Mack annm@

Selecionado Nenhum

Atualizar

3. Selecione pelo menos um membro ou grupo e clique em **Selecionar**. É necessário selecionar pelo menos um aprovador. Não há nenhum aprovador padrão. Suas seleções serão exibidas na lista de aprovadores selecionados.
4. Após especificar as configurações de função, selecione **Atualizar** para salvar suas alterações.

## Próximas etapas

- [Ativar uma função personalizada do Azure AD](#)
- [Atribuir uma função personalizada do Azure AD](#)
- [Remover ou atualizar uma atribuição de função personalizada do Azure AD](#)
- [Definições de função no Azure AD](#)

# Exibir histórico de auditoria para funções do Azure AD no Privileged Identity Management

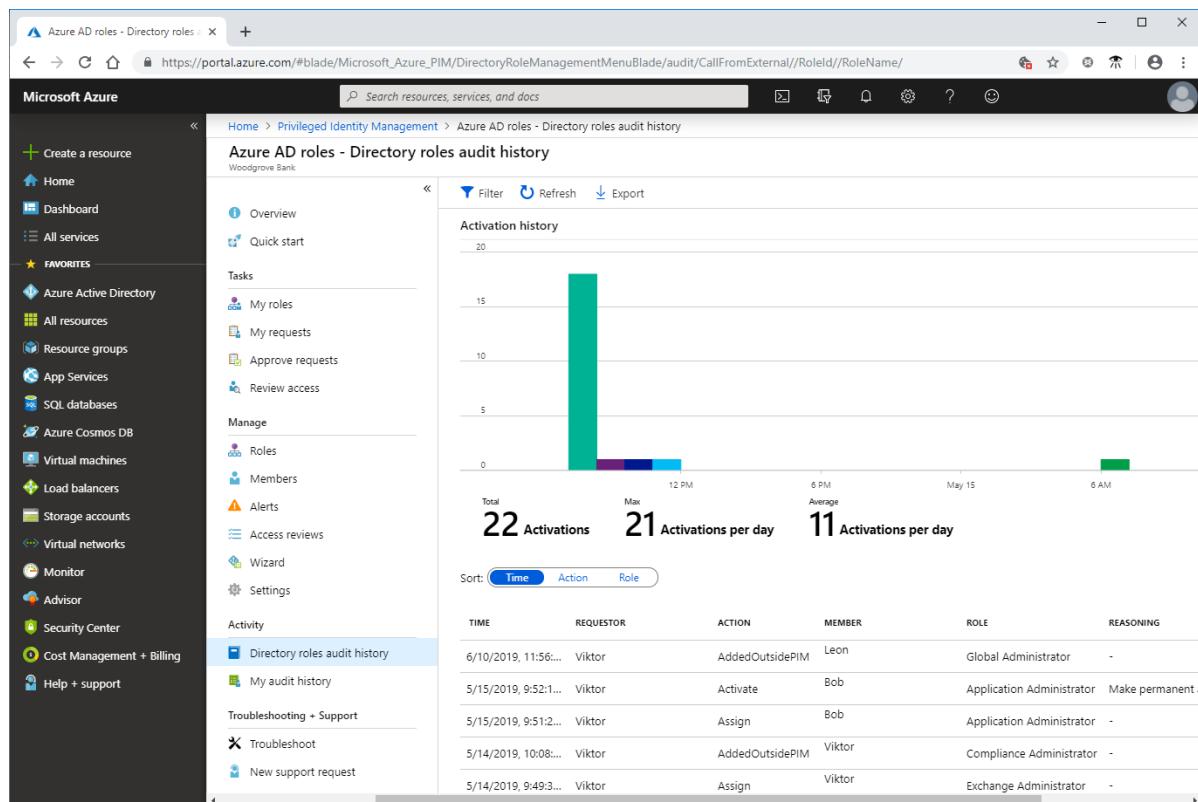
22/07/2020 • 8 minutes to read • [Edit Online](#)

Você pode usar o histórico de auditoria de Privileged Identity Management (PIM) para ver todas as atribuições de função e ativações nos últimos 30 dias para todas as funções privilegiadas. Se você quiser ver o histórico de auditoria completo de atividade na organização do Azure Active Directory (Azure AD), incluindo o administrador, o usuário final e a atividade de sincronização, poderá usar os [relatórios de segurança e atividade do Azure Active Directory](#).

## Determinar sua versão do PIM

A partir de novembro de 2019, a parte das funções do Azure AD da Privileged Identity Management está sendo atualizada para uma nova versão que corresponde às experiências de funções de recurso do Azure. Isso cria recursos adicionais, bem como [as alterações na API existente](#). Enquanto a nova versão está sendo distribuída, os procedimentos que você seguir neste artigo dependem da versão do Privileged Identity Management que você tem atualmente. Siga as etapas nesta seção para determinar qual versão do Privileged Identity Management você tem. Depois de saber sua versão do Privileged Identity Management, você pode selecionar os procedimentos neste artigo que correspondem a essa versão.

1. Entre no [portal do Azure](#) com um usuário que esteja na função de [administrador de função com privilégios](#).
2. Abra **Azure ad Privileged Identity Management**. Se você tiver uma faixa na parte superior da página Visão geral, siga as instruções na **nova guia versão** deste artigo. Caso contrário, siga as instruções na guia **versão anterior**.



- [Nova versão](#)
- [Versão anterior](#)

Siga estas etapas para exibir o histórico de auditoria para funções do Azure AD.

## Exibir o histórico de auditoria de recursos

A auditoria de recursos fornece uma exibição de todas as atividades associadas às suas funções do Azure AD.

1. Abra **Azure ad Privileged Identity Management**.
2. Selecione **funções do Azure ad**.
3. Selecione **auditoria de recurso**.
4. Filtre o histórico usando uma data predefinida ou um intervalo personalizado.

| TIME                  | REQUESTOR | ACTION  | RESOURCE NAME | PRIMARY TARGET                    | SUBJECT | SUBJECT TYPE | STATUS |
|-----------------------|-----------|---|---------------|-----------------------------------|---------|--------------|--------|
| 4/4/2019, 2:31:29 PM  | Shaun     | Add eligible member to role in PIM complete       | Wingtip Toys  | Automation Operator               | Shaun   | Member       | ✓      |
| 4/4/2019, 2:31:29 PM  | Shaun     | Add eligible member to role in PIM requested      | Wingtip Toys  | Automation Operator               | Shaun   | Member       | ✓      |
| 4/4/2019, 2:30:56 PM  | Shaun     | Remove member from role in PIM completed          | Wingtip Toys  | Automation Operator               | Shaun   | Member       | ✓      |
| 4/4/2019, 2:18:32 PM  | Shaun     | Remove eligible member from role in PIM completed | Wingtip Toys  | Automation Operator               | Tom     | Member       | ✓      |
| 4/4/2019, 2:18:32 PM  | Shaun     | Add eligible member to role in PIM complete       | Wingtip Toys  | Automation Operator               | Tom     | Member       | ✓      |
| 4/4/2019, 2:18:31 PM  | Shaun     | Add eligible member to role in PIM requested      | Wingtip Toys  | Automation Operator               | Tom     | Member       | ✓      |
| 4/4/2019, 11:02:53 AM |           | Add member to role canceled (PIM activation)      | Wingtip Toys  | EventGrid EventSubscription Co... |         | Member       | ✓      |
| 4/4/2019, 11:01:12 AM |           | Add member to role approval requested (PIM)       | Wingtip Toys  | EventGrid EventSubscription Co... |         | Member       | ✓      |
| 4/4/2019, 11:01:04 AM |           | Add member to role requested (PIM activation)     | Wingtip Toys  | EventGrid EventSubscription Co... |         | Member       | ✓      |
| 4/4/2019, 11:00:50 AM |           | Add member to role canceled (PIM activation)      | Wingtip Toys  | EventGrid EventSubscription Co... |         | Member       | ✓      |
| 4/4/2019, 10:34:14 AM | Shaun     | Add eligible member to role in PIM requested      | Wingtip Toys  | Billing Reader                    | Shaun   | Member       | ✓      |
| 4/4/2019, 10:31:08 AM | Shaun     | Add member to role completed (PIM activation)     | Wingtip Toys  | Owner                             | Shaun   | Member       | ✓      |
| 4/4/2019, 10:31:05 AM | Shaun     | Add member to role requested (PIM activation)     | Wingtip Toys  | Owner                             | Shaun   | Member       | ✓      |
| 4/4/2019, 9:16:10 AM  | Kelly     | Add member to role completed (PIM activation)     | Wingtip Toys  | Owner                             | Kelly   | Member       | ✓      |

## Exibir minha auditoria

A opção Minha auditoria permite que você exiba sua atividade de função pessoal.

1. Abra **Azure ad Privileged Identity Management**.
2. Selecione **funções do Azure ad**.
3. Selecione o recurso para o qual você deseja exibir o histórico de auditoria.
4. Selecione **minha auditoria**.
5. Filtre o histórico usando uma data predefinida ou um intervalo personalizado.

Dashboard > Privileged Identity Management - Azure resources > Wingtip Toys - My audit

### Wingtip Toys - My audit

Overview Tasks My roles Pending requests Approve requests Review access Manage Roles Members Alerts Access reviews Role settings Activity Resource audit My audit

Export

| Time span  | Audit type | Subject type |       |
|------------|------------|--------------|-------|
| Last day   | All        | All          | Apply |
| Last day   |            |              |       |
| Last week  |            |              |       |
| Last month |            |              |       |
| Custom     |            |              |       |

|                       | ACTION | RESOURCE NAME   | PRIMARY TARGET                    | SUBJECT                           | SUBJECT TYPE | STATUS |
|-----------------------|--------|---|-----------------------------------|-----------------------------------|--------------|--------|
| 4/4/2019, 2:31:29 PM  | Shaun  | Add eligible member to role in PIM completed: Wingtip Toys      | Automation Operator               | Shaun                             | Member       | ✓      |
| 4/4/2019, 2:31:29 PM  | Shaun  | Add eligible member to role in PIM requested: Wingtip Toys      | Automation Operator               | Shaun                             | Member       | ✓      |
| 4/4/2019, 2:30:56 PM  | Shaun  | Remove member from role in PIM completed: Wingtip Toys          | Automation Operator               | Shaun                             | Member       | ✓      |
| 4/4/2019, 2:18:32 PM  | Shaun  | Remove eligible member from role in PIM completed: Wingtip Toys | Automation Operator               | Tom                               | Member       | ✓      |
| 4/4/2019, 2:18:32 PM  | Shaun  | Add eligible member to role in PIM completed: Wingtip Toys      | Automation Operator               | Tom                               | Member       | ✓      |
| 4/4/2019, 2:18:31 PM  | Shaun  | Add eligible member to role in PIM requested: Wingtip Toys      | Automation Operator               | Tom                               | Member       | ✓      |
| 4/4/2019, 10:34:14 AM | Shaun  | Add eligible member to role in PIM requested: Wingtip Toys      | Billing Reader                    | Shaun                             | Member       | ✓      |
| 4/4/2019, 10:31:08 AM | Shaun  | Add member to role completed (PIM activation): Wingtip Toys     | Owner                             | Shaun                             | Member       | ✓      |
| 4/4/2019, 10:31:05 AM | Shaun  | Add member to role requested (PIM activation): Wingtip Toys     | Owner                             | Shaun                             | Member       | ✓      |
| 4/4/2019, 1:57:55 AM  | Shaun  | Remove member from role (PIM activation): Wingtip Toys          | Owner                             | Shaun                             | Member       | ✓      |
| 4/3/2019, 6:01:52 PM  | Shaun  | Add eligible member to role in PIM completed: Wingtip Toys      | EventGrid EventSubscription Co... | Shaun                             | Member       | ✓      |
| 4/2/2019, 6:01:52 PM  | Shaun  | Add eligible member to role in PIM requested: Wingtip Toys      | EventGrid EventSubscription Co... | Shaun                             | Member       | ✓      |
| 4/3/2019, 5:59:56 PM  | Shaun  | Add eligible member to role in PIM completed: Wingtip Toys      | EventGrid EventSubscription Co... |                                   | Member       | ✓      |
| 4/3/2019, 5:59:54 PM  | Shaun  | Add eligible member to role in PIM requested: Wingtip Toys      | EventGrid EventSubscription Co... |                                   | Member       | ✓      |
| 4/3/2019, 5:58:56 PM  | Shaun  | Update role setting in PIM                                      | Wingtip Toys                      | EventGrid EventSubscription Co... | -            | ✓      |

## Próximas etapas

- Exibir a atividade e o histórico de auditoria das funções de recurso do Azure no Privileged Identity Management

# Atribuir funções de recurso do Azure no Privileged Identity Management

22/07/2020 • 5 minutes to read • [Edit Online](#)

O Azure Active Directory (Azure AD) Privileged Identity Management (PIM) pode gerenciar as funções de recurso internas do Azure, bem como as funções personalizadas, incluindo (mas não se limitando a):

- Proprietário
- Administrador de Acesso do Usuário
- Colaborador
- Administrador de Segurança
- Gerenciador de Segurança

## NOTE

Os usuários ou membros de um grupo atribuído ao proprietário ou às funções de assinatura do administrador de acesso do usuário e aos administradores globais do Azure AD que habilitam o gerenciamento de assinaturas no Azure AD têm permissões de administrador de recursos por padrão. Esses administradores podem atribuir funções, definir configurações de função e revisar o acesso usando Privileged Identity Management para recursos do Azure. Um usuário não pode gerenciar Privileged Identity Management para recursos sem permissões de administrador de recursos. Exiba a lista de [funções internas para recursos do Azure](#).

## Atribuir uma função

Siga estas etapas para tornar um usuário qualificado para uma função de recurso do Azure.

1. Entre no [portal do Azure](#) com um usuário que seja membro da função de [administrador de função com privilégios](#).

Para obter informações sobre como conceder a outro administrador acesso para gerenciar Privileged Identity Management, consulte [conceder acesso a outros administradores para gerenciar Privileged Identity Management](#).

2. Abra [Azure ad Privileged Identity Management](#).
3. Selecione [recursos do Azure](#).
4. Use o filtro de recursos para localizar os recursos gerenciados que você está procurando.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > FIMDEV | Overview >

## Privileged Identity Management | Azure resources

Privileged Identity Management

Quick start

Tasks

- My roles
- My requests
- Approve requests
- Review access

Manage

- Azure AD roles
- Groups (Preview)
- Azure resources

Activity

- My audit history

Troubleshooting + Support

- Troubleshoot
- New support request

Resource filter: Subscription

| Resource     | Parent resource |
|--------------|-----------------|
| Wingtip Toys |                 |

Search by resource name:

Wingtip Toys

5. Selecione o recurso que você deseja gerenciar para abrir a página Visão geral do recurso.

6. Em gerenciar, selecione funções para ver a lista de funções para recursos do Azure.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Privileged Identity Management | Azure resources >

## Wingtip Toys | Roles

Privileged Identity Management | Azure resources

Add assignments Refresh

Overview

Tasks

- My roles
- Pending requests
- Approve requests
- Review access

Manage

- Roles
- Assignments
- Alerts
- Access reviews
- Settings

Activity

- Resource audit
- My audit

Search by role name:

| Role                                       | Active | Eligible |
|--|--------|----------|
| AcrDelete                                  | 0      | 3        |
| AcrImageSigner                             | 0      | 2        |
| AcrPull                                    | 1      | 4        |
| AcrPush                                    | 0      | 0        |
| AcrQuarantineReader                        | 0      | 5        |
| AcrQuarantineWriter                        | 0      | 1        |
| AnujCustomRoleOnSubscription               | 0      | 0        |
| API Management Service Contributor         | 0      | 5        |
| API Management Service Operator Role       | 0      | 0        |
| API Management Service Reader Role         | 0      | 5        |
| App Configuration Data Owner               | 0      | 0        |
| App Configuration Data Reader              | 1      | 0        |
| Application Insights Component Contributor | 0      | 0        |
| Application Insights Snapshot Debugger     | 0      | 0        |
| Attestation Contributor                    | 0      | 0        |
| Attestation Reader                         | 0      | 0        |
| Automation Job Operator                    | 0      | 0        |
| Automation Operator                        | 1      | 0        |

7. Selecione Adicionar atribuições para abrir o painel Adicionar atribuições .

8. Selecione selecionar uma função para abrir a página selecionar uma função .

[Home](#) > [Wingtip Toys | Roles](#) >

## Add assignments

[Privileged Identity Management](#) | [Azure resources](#)[Membership](#) [Setting](#)**Resource**

Wingtip Toys

**Resource type**

subscription

**Select role** ⓘ Search role Search role by name

AcrDelete

AcrlImageSigner

AcrPull

AcrPush

AcrQuarantineReader

AcrQuarantineWriter

AnujCustomRoleOnSubscription

API Management Service Contributor

API Management Service Operator Role

API Management Service Reader Role

App Configuration Data Owner

App Configuration Data Reader

[Next >](#)[Cancel](#)

9. Selecione uma função que você deseja atribuir e clique em **Selecionar**.

O painel **selecionar um membro ou grupo** é aberto.

10. Selecione um membro ou grupo que você deseja atribuir à função e, em seguida, clique em **selecionar**.

# Select a member or group

X

Privileged Identity Management | Azure resources

 Search

0G

0Group  
Selected

A3

a3a386d5-adbc-4ee9-aec9-e913b35f792c  
12488fb8-8a55-46e6-af0d-007cad7c6672@fimdev.net

AA

aadmigration\_0  
aadmigration\_0@fimdev.net

AA

aadmigration\_1  
aadmigration\_1@fimdev.net

AA

aadmigration\_2  
aadmigration\_2@fimdev.net

AA

aadmigration\_3  
aadmigration\_3@fimdev.net

## Selected items

0G

0Group

 Remove

 Select

11. Na guia **configurações** , na lista tipo de atribuição , selecione qualificado ou ativo.

[Home](#) > [Wingtip Toys | Roles](#) >

## Add assignments

Privileged Identity Management | Azure resources

Membership

Setting

**Assignment type** ⓘ

- Eligible  
 Active

Maximum allowed eligible duration is 1 year(s).

**Assignment starts \***

07/01/2020



1:56:41 PM

**Assignment ends \***

07/01/2021



1:56:41 PM

**Assign**

&lt; Prev

Cancel

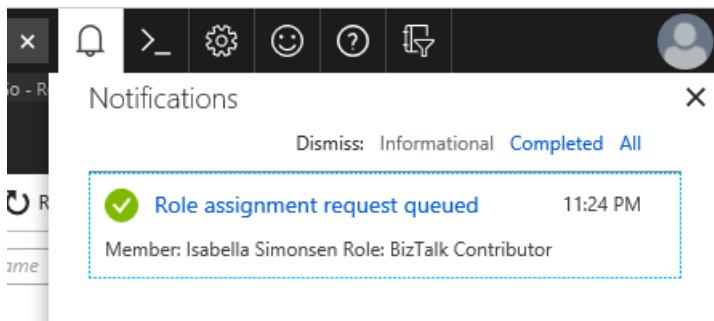
Privileged Identity Management para recursos do Azure fornece dois tipos distintos de atribuição:

- Atribuições **qualificadas** exigem que o membro da função execute uma ação para usar a função. As ações podem incluir a execução de uma verificação de MFA (Autenticação Multifator), fornecimento de uma justificativa comercial ou solicitação de aprovação dos aprovadores designados.
- As atribuições **ativas** não exigem que o membro execute qualquer ação para usar a função. Membros atribuídos como ativos sempre possuem privilégios atribuídos pela função.

12. Para especificar uma duração de atribuição específica, altere as datas e horários de início e término.

13. Quando terminar, selecione **atribuir**.

14. Depois que a nova atribuição de função é criada, uma notificação de status é exibida.



## Atualizar ou remover uma atribuição de função existente

Siga estas etapas para atualizar ou remover uma atribuição de função existente.

1. Abra **Azure ad Privileged Identity Management**.
2. Selecione **recursos do Azure**.
3. Selecione o recurso que você deseja gerenciar para abrir sua página de visão geral.
4. Em **gerenciar**, selecione **funções** para ver a lista de funções para recursos do Azure.

A screenshot of the Microsoft Azure Privileged Identity Management interface. The left sidebar shows navigation sections like Overview, Tasks (My roles, Pending requests, Approve requests, Review access), Manage (Roles, Assignments, Alerts, Access reviews, Settings), and Activity (Resource audit, My audit). The 'Manage' section has 'Roles' selected and highlighted with a red box. The main content area shows a list of roles with a search bar at the top. The list includes:

| Role                                       |
|--|
| AcrDelete                                  |
| AcrImageSigner                             |
| AcrPull                                    |
| AcrPush                                    |
| AcrQuarantineReader                        |
| AcrQuarantineWriter                        |
| AnujCustomRoleOnSubscription               |
| API Management Service Contributor         |
| API Management Service Operator Role       |
| API Management Service Reader Role         |
| App Configuration Data Owner               |
| App Configuration Data Reader              |
| Application Insights Component Contributor |
| Application Insights Snapshot Debugger     |
| Attestation Contributor                    |
| Attestation Reader                         |

5. Selecione a função que você deseja atualizar ou remover.

6. Localize a atribuição de função nas guias **Funções qualificadas** ou **Funções ativas**.

The screenshot shows the Microsoft Azure Privileged Identity Management interface. The top navigation bar includes 'Microsoft Azure', a search bar, and user information ('curtis@fimdev.net FIMDEV'). Below the navigation is a breadcrumb trail: Home > FIMDEV | Overview > Privileged Identity Management | Azure resources > Wingtip Toys | Roles > API Management Service Contributor.

The main content area displays a table of roles:

| Name                               | Principal name               | Type  | Membership | Start time             | End time               | Action   |
|------------------------------------|------------------------------|-------|------------|------------------------|------------------------|--|
| API Management Service Contributor |                              |       |            |                        |                        |  |
| Dritan Kodra                       | dritan@fimdev.net            | User  | Direct     | 4/21/2020, 1:51:17 PM  | Permanent              | <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Extend</a> |
| Nihad Samaha                       | nihad@fimdev.net             | User  | Direct     | 4/21/2020, 1:51:15 PM  | Permanent              | <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Extend</a> |
| Suman                              | surod@fimdev.net             | User  | Direct     | 1/30/2020, 11:38:18 AM | 1/20/2021, 11:35:07 AM | <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Extend</a> |
| 637123797428461961                 | -                            | Group | Direct     | 3/18/2020, 10:31:52 AM | Permanent              | <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Extend</a> |
| Rabeh Zaher                        | rabeh@fimdev.onmicrosoft.com | User  | Direct     | 10/4/2019, 11:02:42 AM | 10/3/2020, 11:02:18 AM | <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Extend</a> |
| 0Group                             | -                            | Group | Direct     | 7/1/2020, 2:08:44 PM   | 7/1/2021, 1:56:41 PM   | <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Extend</a> |

7. Selecione **Atualizar** ou **Remover** para atualizar ou remover a atribuição de função.

Para obter informações sobre como estender uma atribuição de função, consulte [estender ou renovar funções de recurso do Azure no Privileged Identity Management](#).

## Próximas etapas

- [Estender ou renovar funções de recurso do Azure no Privileged Identity Management](#)
- [Definir configurações de função de recurso do Azure no Privileged Identity Management](#)
- [Atribuir funções do Azure AD no Privileged Identity Management](#)

# Convide usuários convidados e atribua funções de recursos do Azure no Privileged Identity Management

22/07/2020 • 9 minutes to read • [Edit Online](#)

Os usuários convidados do Azure Active Directory (Azure AD) fazem parte dos recursos de colaboração B2B (entre empresas) no Azure AD para que você possa gerenciar usuários e fornecedores externos convidados como convidados no Azure AD. Ao combinar a colaboração B2B com o Azure AD Privileged Identity Management (PIM), você pode estender seus requisitos de conformidade e governança para convidados. Por exemplo, você pode usar esses recursos de Privileged Identity Management para tarefas de identidade do Azure com convidados:

- Atribuir acesso a recursos específicos do Azure
- Habilite acesso Just-In-Time
- Especifique a data de duração e de término da atribuição
- Exigir autenticação multifator na atribuição ou ativação ativa
- Realizar as revisões de acesso
- Usar alertas e logs de auditoria

Este artigo descreve como convidar um convidado para sua organização e gerenciar o acesso aos recursos do Azure usando Privileged Identity Management.

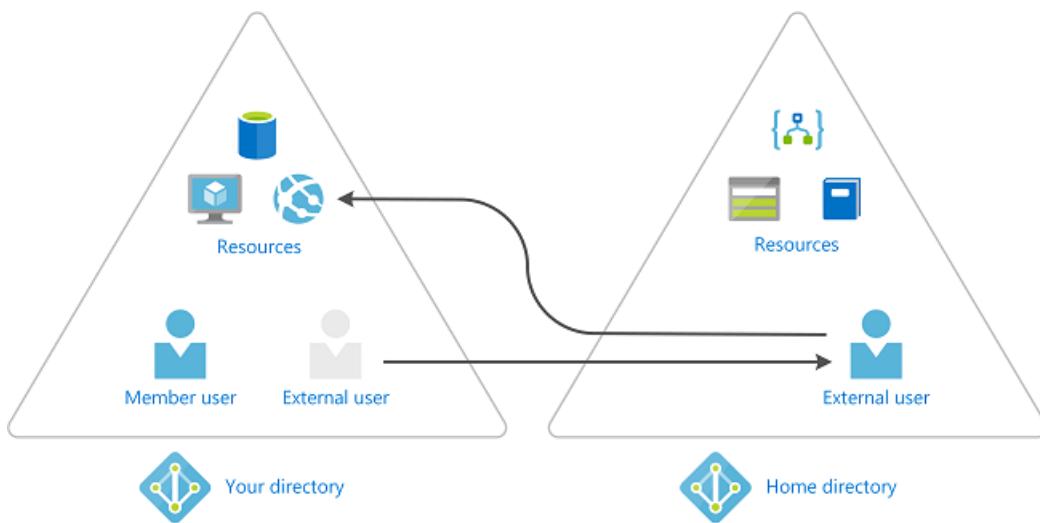
## Quando você convidar convidados?

Aqui estão alguns exemplos de quando você pode convidar convidados para sua organização:

- Permitir que um fornecedor externo autônomo tenha apenas uma conta de email para acessar os recursos do Azure para um projeto.
- Permitir que um parceiro externo em uma grande organização que usa Serviços de Federação do Active Directory (AD FS) local para acessar o aplicativo de despesas.
- Permitir que os engenheiros de suporte que não são da sua organização (como o suporte da Microsoft) acessem temporariamente o recurso do Azure para solucionar problemas.

## Como funciona a colaboração usando os convidados B2B?

Ao usar a colaboração B2B, você pode convidar um usuário externo para sua organização como um convidado. O convidado pode ser gerenciado como um usuário em sua organização, mas um convidado precisa ser autenticado em sua organização inicial e não em sua organização do Azure AD. Isso significa que, se o convidado não tiver mais acesso à sua organização inicial, eles também perderão o acesso à sua organização. Por exemplo, se o convidado deixar sua organização, ele perderá automaticamente o acesso a todos os recursos que você compartilhou com eles no Azure AD sem precisar fazer nada. Para obter mais informações sobre a colaboração B2B, consulte [o que é acesso de usuário convidado em Azure Active Directory B2B?](#)



## Verificar as configurações de colaboração do convidado

Para garantir que você possa convidar convidados para sua organização, verifique suas configurações de colaboração de convidado.

1. Entre no [Portal do Azure](#).
2. Selecione **Azure Active Directory > configurações do usuário**.
3. Selecione **gerenciar configurações de colaboração externas**.

4. Verifique se os **Administradores e usuários na função de convite do emissor de convidado** podem **convidar** o comutador está definido como Sim.

## Convidar um convidado e atribuir uma função

Usando Privileged Identity Management, você pode convidar um convidado e torná-lo qualificado para uma função de recurso do Azure.

1. Entre no [portal do Azure](#) com um usuário que seja membro da função Administrador de [função privilegiada](#) ou [administrador de usuário](#).

2. Abra Azure ad Privileged Identity Management.
  3. Selecione recursos do Azure.
  4. Use o Filtro de recurso para filtrar a lista de recursos gerenciados.
  5. Selecione o recurso que você deseja gerenciar, como um recurso, grupo de recursos, assinatura ou grupo de gerenciamento.
- Você deve definir o escopo para apenas o que o convidado precisa.
6. Em gerenciar, selecione funções para ver a lista de funções para recursos do Azure.

| ROLE                       | ACTIVE | ELIGIBLE |
|----------------------------|--------|----------|
| Owner                      | 3      | 0        |
| Reader                     | 2      | 0        |
| Billing Reader             | 1      | 0        |
| User Access Administrator  | 1      | 0        |
| Virtual Machine Operator   | 0      | 0        |
| Virtual Machine Operator 2 | 0      | 0        |
| Virtual Machine Operator 3 | 0      | 0        |
| AcrImageSigner             | 0      | 0        |
| AcrPull                    | 0      | 0        |
| AcrPush                    | 0      | 0        |
| AcrQuarantineReader        | 0      | 0        |
| AcrQuarantineWriter        | 0      | 0        |

7. Selecione a função mínima que será necessária para o usuário.

| NAME       | EMAIL | MEMBERSHIP TYPE | START TIME | END TIME | ACTION |
|------------|-------|-----------------|------------|----------|--------|
| No results |       |                 |            |          |        |

8. Na página função, selecione Adicionar membro para abrir o painel nova atribuição.
9. Clique em Selecionar um membro ou grupo.

roles > resource-group-hr - Roles > Contributor > New assignment > Select a member or group

New assignment X

Contributor

\* User Select a role >  
Contributor

\* User Select a member or group >  
No member or group selected

\* User Set membership settings >  
Default setting is selected

Select a member or group X

+ Invite

Select ?

Search by name or email address ✓

AAD Request Verification Service - PROD

AADPremiumService

aciapi

AD Admin admin

A2 Admin 2 admin2

AIGraphClient

Selected 🔒

None

Add Select

10. Para convidar um convidado, clique em **convidar**.

Invite a guest X

Enter email address of the external user  
user@contoso.com ✓

Include a personal message with the invitation  
Can you help with the HR App deployment?

Invite >

11. Depois de selecionar um convidado, clique em **convidar**.

O convidado deve ser adicionado como um membro selecionado.

12. No painel **selecionar um membro ou grupo**, clique em **selecionar**.

13. No painel configurações de associação , selecione o tipo de atribuição e a duração.

The screenshot shows two adjacent panels. The left panel, titled 'New assignment' under 'Contributor', contains three steps: 'Select a role' (Contributor), 'Select a member or group' (user), and 'Set membership settings' (Default setting is selected). The right panel, titled 'Membership settings', shows the 'Assignment type' set to 'Eligible'. It also displays the start and end times for the assignment: 'Assignment starts' on 2018-11-14 at 4:30:36 PM and 'Assignment ends' on 2018-11-21 at 4:30:36 PM. At the bottom are 'Add', 'Done', and 'Reset' buttons.

14. Para concluir a atribuição, selecione **concluído** e, em seguida, **Adicionar**.

A atribuição de função de convidado aparecerá na sua lista de funções.

The screenshot shows the 'Contributor' page in the Azure portal. The top navigation bar includes 'Home', 'Privileged Identity Management - Azure resources', 'resource-group-hr - Roles', and 'Contributor'. Below the navigation is a toolbar with 'Add member', 'Group by', 'Role settings', 'Export', and 'Refresh' buttons. A search bar allows searching by member name. The main area is divided into tabs: 'Eligible roles' (selected), 'Active roles', and 'Expired roles'. A table lists the assigned role: 'user' with email 'user\_contoso.com#E...' under 'CONTRIBUTOR'. The table columns are NAME, EMAIL, MEMBERSHIP TYPE, START TIME, END TIME, and ACTION. The 'ACTION' column for the user row contains 'Remove | Update | Extend'.

## Ativar a função como um convidado

Se você for um usuário externo, deverá aceitar o convite para ser convidado na organização do Azure AD e possivelmente ativar sua atribuição de função.

1. Abra o email com seu convite. O email se parecerá com o seguinte.

You're invited to the Default Directory organization



Microsoft Invitations <invites@microsoft.com>

Wed 11/14/2018, 5:25 PM

You ▾



## Azure Active Directory

You've been invited to access applications in the

### Default Directory organization

by



User

Can you help with the HR App deployment?

**Get Started**

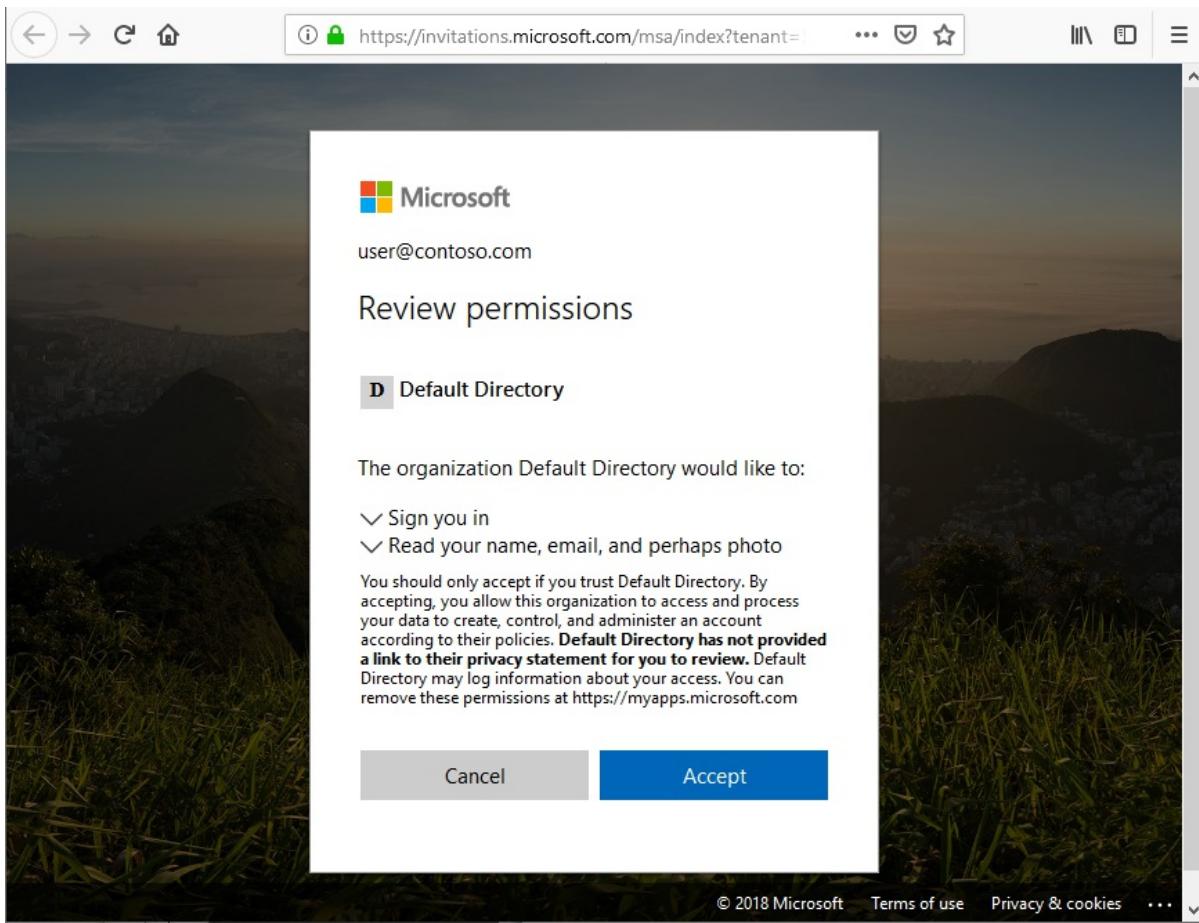
Return to the above link at any time for access.

This email has been sent on behalf of the Default Directory organization. Please act on this email only if you trust the Default Directory organization. This email may have advertising content. You can [unsubscribe](#) from future invitations from the Default Directory organization at any time. See [Microsoft organization privacy statement](#) to learn more about how Microsoft handles your data.

Facilitated by : Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



2. Selecione o **link de introdução** no email.
3. Depois de revisar as permissões, clique em **Aceitar**.



4. Você pode ser solicitado a aceitar os termos de uso e especificar se deseja permanecer conectado. No portal do Azure, se você estiver *qualificado* para uma função, ainda não terá acesso aos recursos.
5. Para ativar a atribuição de função, abra o email com o link ativar função. O email se parecerá com o seguinte.

## PIM: You now have the Contributor role

Microsoft Azure  <azure-noreply@microsoft.com>  
Wed 11/14/2018, 5:40 PM  
You ↘

Default Directory

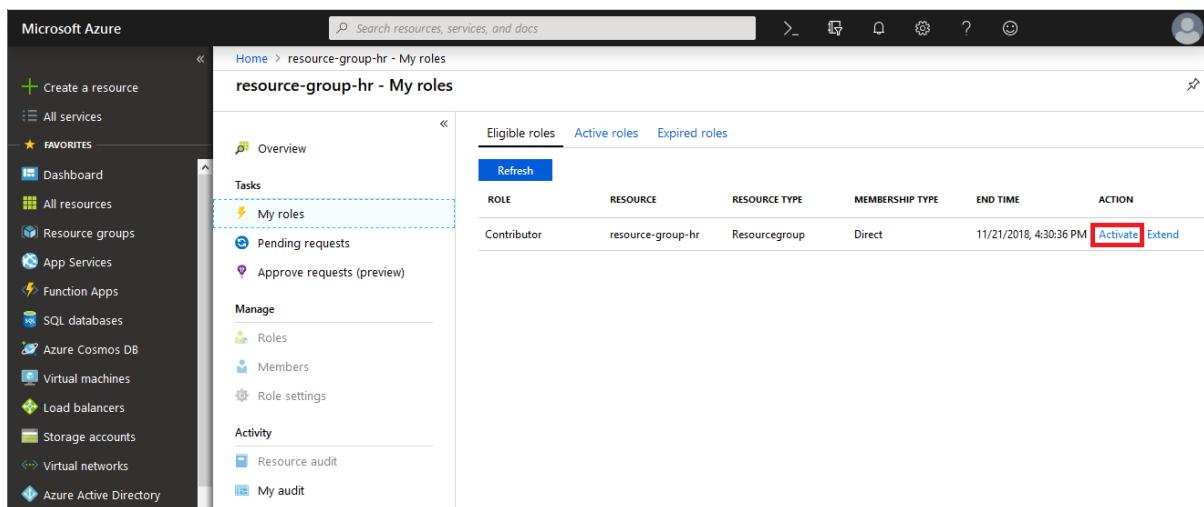
Admin assigned you the Contributor role in the resource-group-hr resourcegroup

[Activate role >](#)

| Settings         | Value                      |
|------------------|----------------------------|
| User or Group    | user                       |
| Role             | Contributor                |
| Resource         | resource-group-hr          |
| Resource type    | resourcegroup              |
| Assigned by      | Admin                      |
| Assignment type  | Eligible                   |
| Assignment start | November 15, 2018 0:39 UTC |
| Assignment end   | November 22, 2018 0:30 UTC |
| Justification    | -                          |

Privileged Identity Management protects your organization from accidental or malicious activity by reducing persistent access to Azure resources, providing just-in-time or time-limited access when needed.

6. Selecione Ativar função para abrir suas funções qualificadas no Privileged Identity Management.



| ROLE        | RESOURCE          | RESOURCE TYPE | MEMBERSHIP TYPE | END TIME               | ACTION  |
|-------------|-------------------|---------------|-----------------|------------------------|---|
| Contributor | resource-group-hr | Resourcegroup | Direct          | 11/21/2018, 4:30:36 PM | <a href="#">Activate</a> <a href="#">Extend</a> |

7. Em ação, selecione o link Ativar .

Dependendo das configurações de função, você precisará especificar algumas informações para ativar a função.

8. Depois de especificar as configurações para a função, clique em Ativar para ativar a função.

Home > resource-group-hr - My roles > Activate

## Activate

Assignment details

Scope  
resource-group-hr 

\* Start time   

duration (hours)  

\* Reason (max 500 characters)   

**Activate**

A menos que o administrador seja necessário para aprovar sua solicitação, você deve ter acesso aos recursos especificados.

## Exibir atividade para um convidado

Você pode exibir os logs de auditoria para controlar o que os convidados estão fazendo.

1. Como administrador, abra Privileged Identity Management e selecione o recurso que foi compartilhado.
2. Selecione **auditoria de recurso** para exibir a atividade para esse recurso. O exemplo a seguir mostra um exemplo da atividade para um grupo de recursos.

Dashboard > Privileged Identity Management - Azure resources > Wingtip Toys - Resource audit

## Wingtip Toys - Resource audit

- [Overview](#)
- [Tasks](#)
- [My roles](#)
- [Pending requests](#)
- [Approve requests](#)
- [Review access](#)
- [Manage](#)
  - [Roles](#)
  - [Members](#)
  - [Alerts](#)
  - [Access reviews](#)
  - [Role settings](#)
- [Activity](#)
  - [Resource audit](#)
  - [My audit](#)

Export
Time span
Audit type

Last day
All

| TIME                 | REQUESTOR | ACTION            |
|----------------------|-----------|-------------------|
| 4/9/2019, 3:11:16 PM | Gaurav    | Remove            |
| 4/9/2019, 3:11:14 PM | Gaurav    | Remove            |
| 4/9/2019, 3:09:56 PM | Gaurav    | Add member        |
| 4/9/2019, 3:09:54 PM | Gaurav    | Add member        |
| 4/9/2019, 3:09:17 PM | Gaurav    | Add eligible user |
| 4/9/2019, 3:09:16 PM | Gaurav    | Add eligible user |
| 4/9/2019, 3:08:10 PM | Gaurav    | Add member        |
| 4/9/2019, 3:08:02 PM | Gaurav    | Add member        |
| 4/9/2019, 3:07:52 PM | Gaurav    | Add member        |
| 4/9/2019, 2:55:24 PM |           | Update resource   |
| 4/9/2019, 2:54:30 PM |           | Update resource   |

3. Para exibir a atividade para o convidado, selecione **Azure Active Directory** > nome de convidados **usuários** > *guest name*.
4. Selecione **logs de auditoria** para ver os logs de auditoria da organização. Se necessário, você pode especificar os filtros.

Home > Default Directory - Audit logs

## Default Directory - Audit logs

- [Overview \(Preview\)](#)
- [Identity Secure Score \(Preview\)](#)
- [Conditional Access](#)
- [MFA](#)
- [Users flagged for risk](#)
- [Risk events](#)
- [Authentication methods](#)
- [Audit logs](#)
- [Logs](#)
- [Diagnostic settings](#)
- [Troubleshooting + Support](#)
- [Troubleshoot](#)
- [New support request](#)

Search (Ctrl+J)
Columns
Refresh
Download
Troubleshoot
Export Data Settings

Category
All
Activity Resource Type
All
Activity
All

Date Range
1 Month
Target
Enter target name or URL

Initiated By (Actor)
Enter actor name or URL

| DATE                   | TARGET(S)                           | INITIATED BY (ACTOR)            | ACTIVITY                    |
|------------------------|-------------------------------------|---------------------------------|-----------------------------|
| 11/14/2018, 5:34:59 PM | Policy : Contoso Official Tenant    | user                            | Accept Terms Of Use         |
| 11/14/2018, 5:34:45 PM | User : user_contoso.com#EXXXXXXXXXX | Microsoft Invitation Acceptance | Update user                 |
| 11/14/2018, 5:34:45 PM | Other : UPN: user_contoso.com       | user@contoso.com                | Redeem external user invite |
| 11/14/2018, 5:27:59 PM | ServicePrincipal : Microsoft ...    | Microsoft Azure AD Internal...  | Add service principal       |
| 11/14/2018, 4:25:39 PM | ServicePrincipal : Microsoft ...    | Microsoft Azure AD Internal...  | Add service principal       |
| 11/14/2018, 4:25:37 PM | Other : UPN: user@contoso.com       | example.com#Admin@example...    | Invite external user        |
| 11/14/2018, 4:25:37 PM | User : user_contoso.com#EXXXXXXXXXX | Microsoft B2B Admin Worker      | Add user                    |
| 11/14/2018, 4:25:37 PM | ServicePrincipal : Microsoft ...    | Microsoft Azure AD Internal...  | Add service principal       |
| 11/3/2018, 7:48:25 PM  | ServicePrincipal : aciapi           | Windows Azure Service Ma...     | Add service principal       |

## Próximas etapas

- [Atribuir funções de administrador do Azure AD no Privileged Identity Management](#)
- [O que é o acesso de usuário convidado na colaboração B2B do Azure AD?](#)

# Aprovar ou negar solicitações para funções de recurso do Azure no Privileged Identity Management

22/07/2020 • 4 minutes to read • [Edit Online](#)

Com o Privileged Identity Management (PIM) no Azure Active Directory (Azure AD), você pode configurar funções para exigir aprovação para ativação e escolher usuários ou grupos da sua organização do Azure AD como aprovadores delegados. É recomendável selecionar dois ou mais aprovadores para cada função para reduzir a carga de trabalho para o administrador da função com privilégios. Os aprovadores representantes têm 24 horas para aprovar as solicitações. Se a solicitação não for aprovada dentro de 24 horas, o usuário qualificado deverá enviar outra. A janela de tempo de aprovação de 24 horas não é configurável.

Siga as etapas neste artigo para aprovar ou negar solicitações de funções de recursos do Azure.

## Exibir solicitações pendentes

Como um aprovador delegado, você receberá uma notificação por email quando uma solicitação de função de recurso do Azure estiver aguardando a aprovação. Você pode exibir essas solicitações pendentes no Privileged Identity Management.

1. Entre no [portal do Azure](#).
2. Abra Azure ad Privileged Identity Management.
3. Selecione **aprovar solicitações**.

The screenshot shows the Azure Privileged Identity Management interface. On the left, there's a sidebar with various icons and links like 'Quick start', 'My roles', 'My requests', 'Approve requests', 'Review access', 'Manage', 'Azure AD roles', 'Azure resources', 'Activity', 'My audit history', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The 'Approve requests' link is highlighted. The main area has a title 'Approve requests - Azure resources'. Below it, there's a sidebar with 'Approve requests', 'Azure AD roles', 'Azure resources' (which is selected and highlighted in blue), 'Azure managed applications', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main content area shows two sections: 'Requests to renew or extend role assignments' and 'Requests for role activations'. Under 'Requests to renew or extend role assignments', there are two entries:

| ROLE                | REQUESTOR | RESOURCE     |
|---------------------|-----------|--------------|
| Automation Operator | Tom       | Wingtip Toys |
| Automation Operator | Shaun     | Wingtip Toys |

Under 'Requests for role activations', there is one entry:

| RESOURCE                     | ROLE | REQUESTOR TENANT |
|------------------------------|------|------------------|
| No requests pending approval |      |                  |

Na seção **Solicitações para ativações de função** você verá uma lista de solicitações aguardando a aprovação.

## Aprovar solicitações

1. Localize e selecione a solicitação que você deseja aprovar. Uma página aprovar ou negar é exibida.

- Approve requests

Approval requests for Azure AD directory role

Approve Deny Refresh

ROLE

No requests pending approval

Approval requests for Azure RBAC resources

^ Requests to renew or extend role assignments

Refresh

ROLE REQUESTOR RESO

No requests pending approval

^ Requests for role activations

ROLE REQUESTOR

BizTalk Contributor Isabella Simonsen

Approve Deny

Isabella Simonsen  
isabella@

Role BizTalk Contributor

Requestor Isabella Simonsen

Request Time 8/31/2018 3:19 PM

Resource Pay-As-You-Go

Resource Type subscription

Reason Need to make some configuration changes to application

Start Time 8/31/2018 10:02 PM

End Time 9/1/2018 2:02 AM

\* Justification ⓘ

2. Na caixa de **justificação**, insira a justificativa comercial.
  3. Selecione **Aprovar**. Você receberá uma notificação do Azure de sua aprovação.

The screenshot shows the Microsoft Teams Notifications page. At the top, there are several icons: a close button (X), a bell icon, a gear icon, a smiley face icon, a question mark icon, a split screen icon, and a user profile icon. Below the icons, the word "Notifications" is displayed. To the right of "Notifications" is another close button (X). Underneath, there is a list of notifications. The first notification is highlighted with a blue dashed border. It contains a green checkmark icon, the text "Update request status", the time "6:00 PM", and the message "Isabella Simonsen is approved". Above this list, there are buttons for "Dismiss", "Informational", "Completed", and "All".

## Negar solicitações

1. Localize e selecione a solicitação que você deseja negar. Uma página aprovar ou negar é exibida.

2. Na caixa de justificação , insira a justificativa comercial.
3. Selecione negar. Uma notificação é exibida com a negação.

## Notificações de fluxo de trabalho

Veja algumas informações sobre notificações de fluxo de trabalho:

- Os aprovadores são notificados por email quando uma solicitação de uma função está aguardando sua revisão. As notificações por email incluem um link direto para a solicitação no qual o aprovador pode aprovar ou negar.
- As solicitações são resolvidas pelo primeiro aprovador que aprova ou nega.
- Quando um Aprovador responde à solicitação, todos os aprovadores são notificados sobre a ação.
- Os administradores de recursos são notificados quando um usuário aprovado se torna ativo em sua função.

### NOTE

Um administrador de recursos que acredita que um usuário aprovado não deve estar ativo pode remover a atribuição de função ativa em Privileged Identity Management. Embora os administradores de recursos não sejam notificados sobre solicitações pendentes, a menos que sejam um aprovador, eles podem exibir e cancelar solicitações pendentes para todos os usuários exibindo solicitações pendentes no Privileged Identity Management.

## Próximas etapas

- Estender ou renovar funções de recurso do Azure no Privileged Identity Management
- Notificações por email no Privileged Identity Management
- Aprovar ou negar solicitações para funções do Azure AD no Privileged Identity Management

# Estender ou renovar atribuições de função de recurso do Azure no Privileged Identity Management

22/07/2020 • 11 minutes to read • [Edit Online](#)

O Azure Active Directory (Azure AD) Privileged Identity Management (PIM) fornece controles para gerenciar o acesso e o ciclo de vida de atribuição para recursos do Azure. Os administradores podem atribuir funções usando as propriedades de data e hora de início e término. Quando a extremidade de atribuição se aproxima, Privileged Identity Management envia notificações por email aos usuários ou grupos afetados. Ele também envia notificações por e-mail aos administradores do recurso para garantir que o acesso apropriado seja mantido. As atribuições podem ser renovadas e permanecer visíveis em um estado expirado por até 30 dias, mesmo que o acesso não seja estendido.

## Quem pode estender e renovar?

Somente os administradores do recurso podem estender ou renovar atribuições de função. O usuário ou grupo afetado pode solicitar a extensão das funções que estão prestes a expirar e a solicitação para renovar as funções que já expiram.

## Quando as notificações são enviadas?

Privileged Identity Management envia notificações por email para administradores e usuários afetados ou grupos de funções que estão expirando em 14 dias e um dia antes da expiração. Ele envia um e-mail adicional quando uma atribuição expira oficialmente.

Os administradores recebem notificações quando um usuário ou grupo atribuiu solicitações de função expiradas ou expiradas para estender ou renovar. Quando um administrador específico resolve a solicitação, todos os outros administradores são notificados da decisão de resolução (aprovada ou recusada). Em seguida, o usuário ou grupo solicitante é notificado sobre a decisão.

## Estender atribuições de função

As etapas a seguir descrevem o processo de solicitação, resolução ou administração de uma extensão ou renovação de uma atribuição de função.

### Estender automaticamente as atribuições de expiração

Os usuários ou grupos atribuídos a uma função podem estender as atribuições de função de expiração diretamente da guia **qualificada** ou **ativa** na página **minhas funções** de um recurso e na página **minhas funções** de nível superior do portal de Privileged Identity Management. Os usuários ou grupos podem solicitar a extensão de funções qualificadas e ativas (atribuídas) que expiram nos próximos 14 dias.

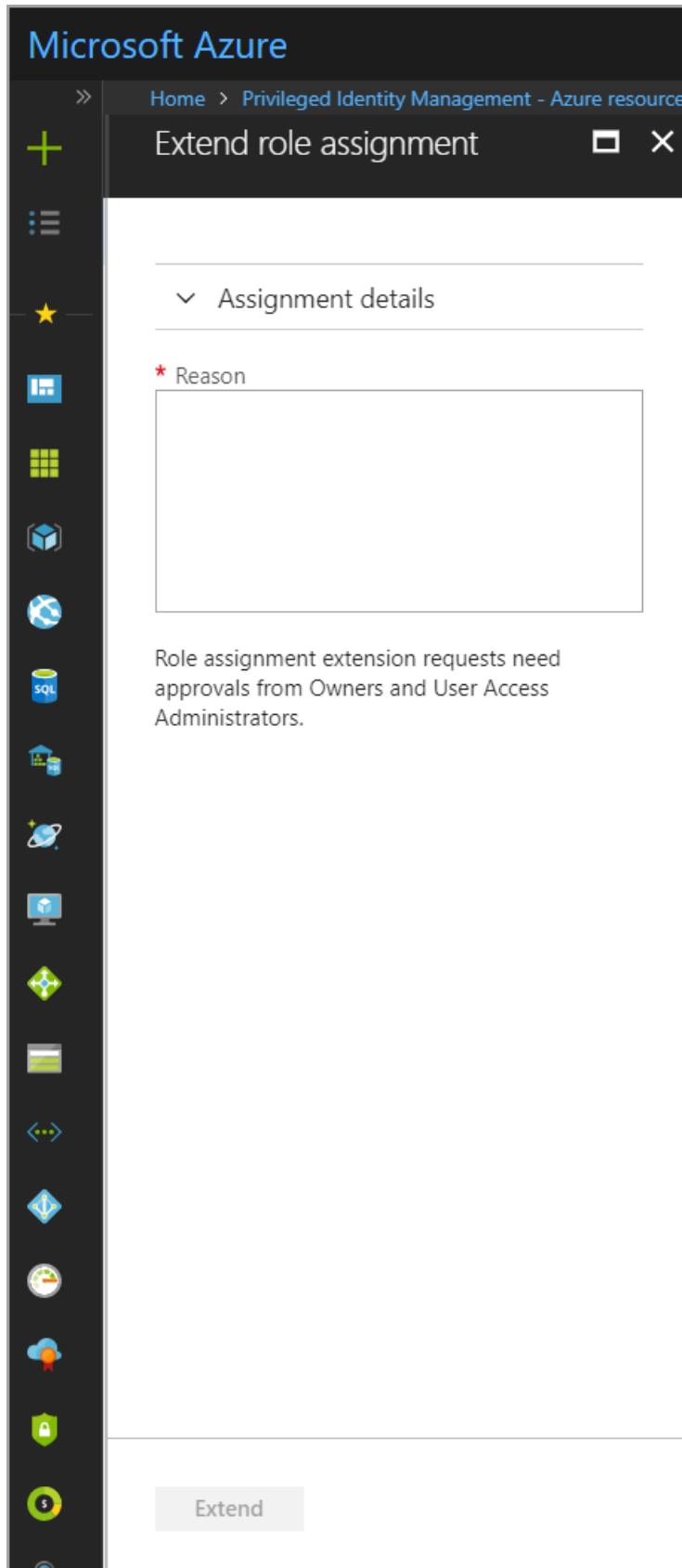
The screenshot shows the Azure portal interface for 'Wingtip Toys - My roles'. On the left, there's a sidebar with icons for Overview, Tasks, Manage, and other settings. The main area displays a table of roles. The 'Active roles' tab is selected. A red arrow points from the 'Active roles' tab to the 'Action' column for the 'Owner' role row.

| ROLE                                   | RESOURCE     | RESOURCE TYPE | MEMBERSHIP TYPE | END TIME              | ACTION                            |
|--|--------------|---------------|-----------------|-----------------------|-----------------------------------|
| Automation Operator                    | Wingtip Toys | Subscription  | Direct          | 4/5/2019, 2:31:08 PM  | <a href="#">Activate   Extend</a> |
| Owner                                  | Wingtip Toys | Subscription  | Direct          | 5/7/2019, 6:07:10 PM  | <a href="#">Activate   Extend</a> |
| Lab Creator                            | Wingtip Toys | Subscription  | Direct          | 6/25/2019, 7:54:44 AM | <a href="#">Activate   Extend</a> |
| EventGrid EventSubscription Contrib... | Wingtip Toys | Subscription  | Direct          | 7/2/2019, 6:01:47 PM  | <a href="#">Activate   Extend</a> |
| Contributor                            | Wingtip Toys | Subscription  | Direct          | 5/27/2019, 4:22:07 PM | <a href="#">Activate   Extend</a> |

Quando a data e a hora de término da atribuição estiverem dentro de 14 dias, o botão para \*\* Estender \*\* se tornará um link ativo na interface do usuário. No exemplo a seguir, suponha que a data atual seja 27 de março.

| END TIME               | ACTION                            |
|------------------------|-----------------------------------|
| 9/15/2018, 12:47:46 PM | <a href="#">Activate   Extend</a> |
| 4/2/2018, 10:33:05 AM  | <a href="#">Activate   Extend</a> |
| 4/25/2018, 6:03:02 PM  | <a href="#">Activate   Extend</a> |

Para solicitar uma extensão dessa atribuição de função, selecione \*\* Estender \*\* para abrir o formulário de solicitação.



Para visualizar informações sobre a atribuição original, expanda \*\* Detalhes da atribuição \*\*. Digite uma razão para a solicitação de extensão e, em seguida, selecione \*\* Estender \*\*.

## NOTE

Recomendamos incluir os detalhes de por que a extensão é necessária e por quanto tempo a extensão deve ser concedida (se você tiver essa informação).

Microsoft Azure

Home > Privileged Identity Management - Azure resources

## Extend role assignment

Assignment details

Resource name: Wingtip Toys - Prod

Role: Owner

User: Tom Smith

Start time: 10/4/2017, 10:33:21 AM

End time: 4/2/2018, 10:33:05 AM

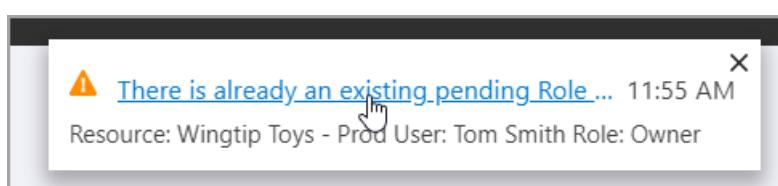
Activation required: Yes

\* Reason: I'll need another month to complete the networking configuration. Please extend my access until 4/27. -Thanks! ✓

Role assignment extension requests need approvals from Owners and User Access Administrators.

**Extend**

Em questão de minutos, os administradores de recursos recebem uma notificação por email solicitando que eles revisem a solicitação de extensão. Se uma solicitação para estender já tiver sido enviada, uma notificação do Azure aparecerá no Portal.



Vá para a página **solicitações pendentes** para exibir o status de sua solicitação ou para cancelá-la.

| ROLE                | RESOURCE     | MEMBER | REQUEST TYPE | REASON                     | REQUEST TIME         | START TIME | REQUEST STATUS       | ACTION                 |
|---------------------|--------------|--------|--------------|----------------------------|----------------------|------------|----------------------|------------------------|
| Automation Operator | Wingtip Toys | Tom    | Member renew | I need to finish this proj | 4/4/2019, 2:21:27 PM | -          | PendingAdminDecision | <a href="#">Cancel</a> |

## Extensão aprovada pelo administrador

Quando um usuário ou grupo envia uma solicitação para estender uma atribuição de função, os administradores de recursos recebem uma notificação por email que contém os detalhes da atribuição original e o motivo da solicitação. A notificação inclui um link direto com a solicitação para o administrador aprovar ou negar.

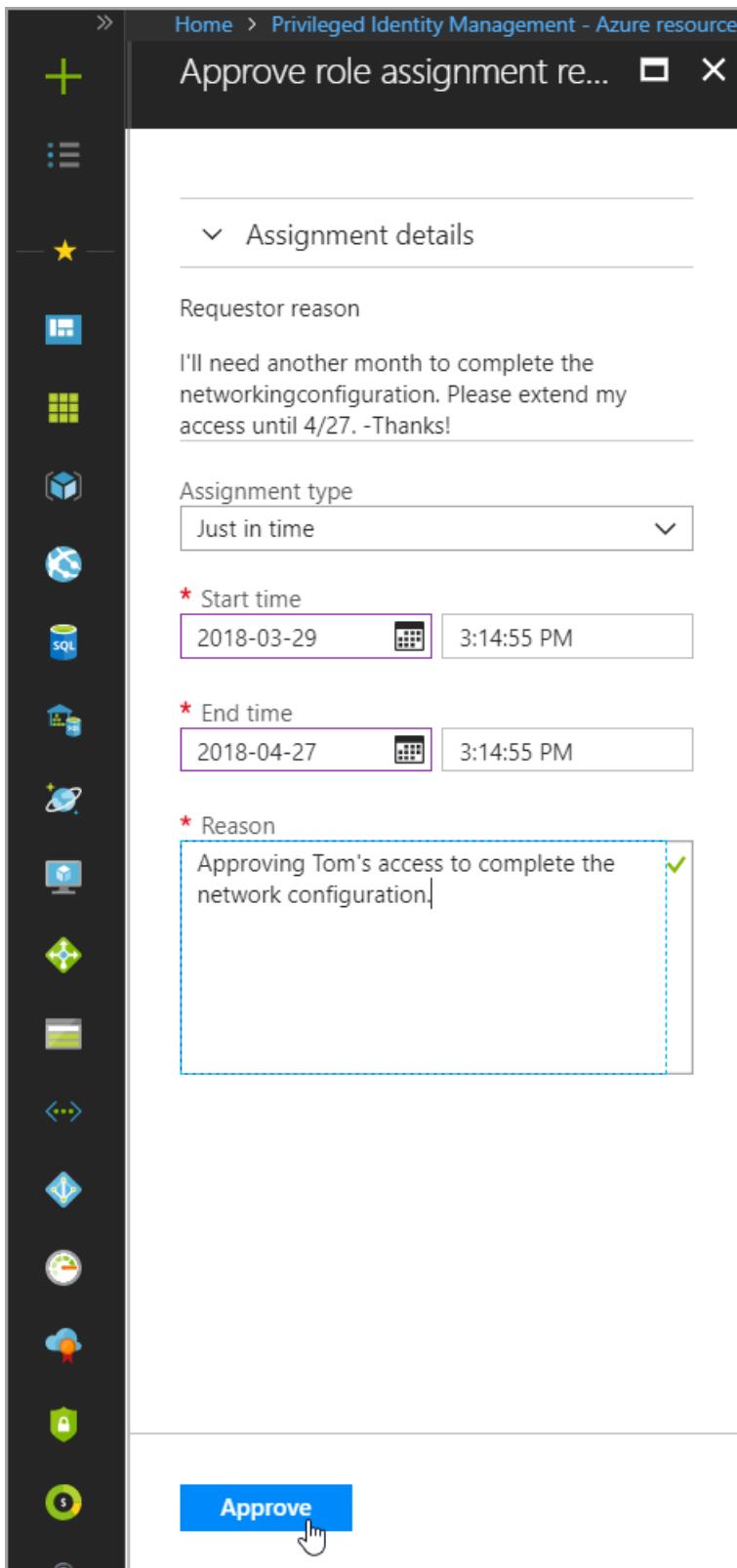
Além de usar o link do email a seguir, os administradores podem aprovar ou negar solicitações acessando o portal de administração do Privileged Identity Management e selecionando **aprovar solicitações** no painel esquerdo.

| ROLE                | REQUESTOR | RESOURCE     | RESOURCE TYPE | REQUEST TYPE | ASSIGNMENT TYPE | START TIME           | END TIME             | ACTION                                       |
|---------------------|-----------|--------------|---------------|--------------|-----------------|----------------------|----------------------|--|
| Automation Operator | Tom       | Wingtip Toys | subscription  | Member renew | Eligible        | 4/4/2019, 2:18:32 PM | 4/4/2019, 2:18:03 PM | <a href="#">Approve</a> <a href="#">Deny</a> |

| ROLE                                  | REQUESTOR | REQUEST TIME       | REASON | START TIME         | END TIME          |
|---------------------------------------|-----------|--------------------|--------|--------------------|-------------------|
| EventGrid EventSubscription Contri... |           | 4/4/2019, 11:01 AM | S      | 4/4/2019, 11:01 AM | 4/4/2019, 7:01 PM |

Quando um administrador seleciona **aprovar** ou **negar**, os detalhes da solicitação são mostrados, juntamente com um campo para fornecer uma justificativa de negócios para os logs de auditoria.

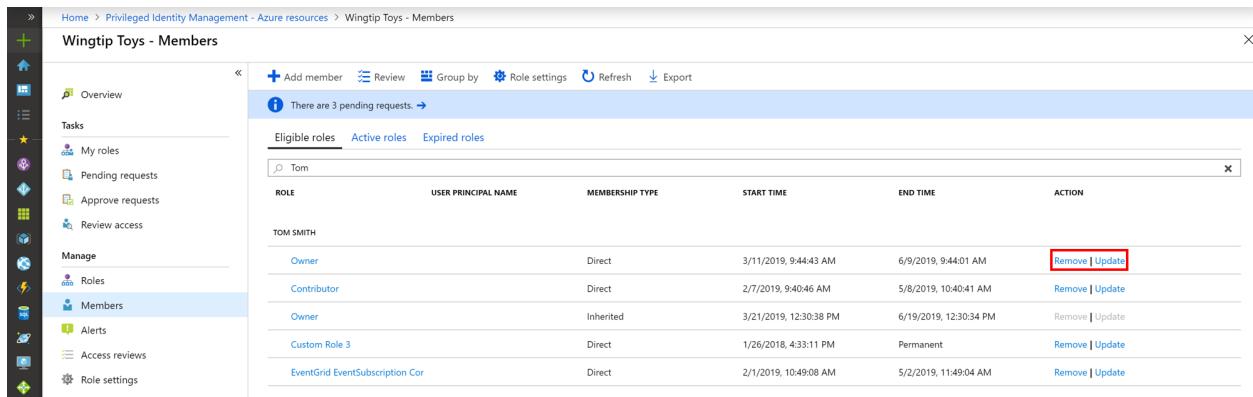


Ao aprovar uma solicitação para estender a atribuição de função, os administradores de recursos podem escolher uma nova data de início, uma data de término e um tipo de atribuição. Alterar o tipo de atribuição pode ser necessário se o administrador quiser fornecer acesso limitado para concluir uma tarefa específica (um dia, por exemplo). Neste exemplo, o administrador pode alterar a atribuição de \*\* Qualificado \*\* para \*\* Ativo \*\*. Isso significa que eles podem fornecer acesso ao solicitante sem precisar que eles sejam ativados.

#### Extensão iniciada pelo administrador

Se um usuário atribuído a uma função não solicitar uma extensão para a atribuição de função, um administrador poderá estender uma atribuição em nome do usuário. As extensões administrativas da atribuição de função não exigem aprovação, mas as notificações são enviadas a todos os outros administradores após a extensão da função.

Para estender uma atribuição de função, navegue até a função de recurso ou exibição de atribuição em Privileged Identity Management. Localize a atribuição que requer uma extensão. Em seguida, selecione **estender** na coluna ação.



| ROLE                            | USER PRINCIPAL NAME | MEMBERSHIP TYPE | START TIME             | END TIME               | ACTION                          |
|---------------------------------|---------------------|-----------------|------------------------|------------------------|---------------------------------|
| Owner                           |                     | Direct          | 3/11/2019, 9:44:43 AM  | 6/9/2019, 9:44:01 AM   | <a href="#">Remove   Update</a> |
| Contributor                     |                     | Direct          | 2/7/2019, 9:40:46 AM   | 5/8/2019, 10:40:41 AM  | <a href="#">Remove   Update</a> |
| Owner                           |                     | Inherited       | 3/21/2019, 12:30:38 PM | 6/19/2019, 12:30:34 PM | <a href="#">Remove   Update</a> |
| Custom Role 3                   |                     | Direct          | 1/26/2018, 4:33:11 PM  | Permanent              | <a href="#">Remove   Update</a> |
| EventGrid EventSubscription Cor |                     | Direct          | 2/1/2019, 10:49:08 AM  | 5/2/2019, 11:49:04 AM  | <a href="#">Remove   Update</a> |

## Renovar atribuições de função

Embora seja conceitualmente semelhante ao processo para solicitar uma extensão, o processo para renovar uma atribuição de função expirada é diferente. Usando as etapas, as atribuições e os administradores a seguir podem renovar o acesso às funções expiradas quando necessário.

### Renovação automática

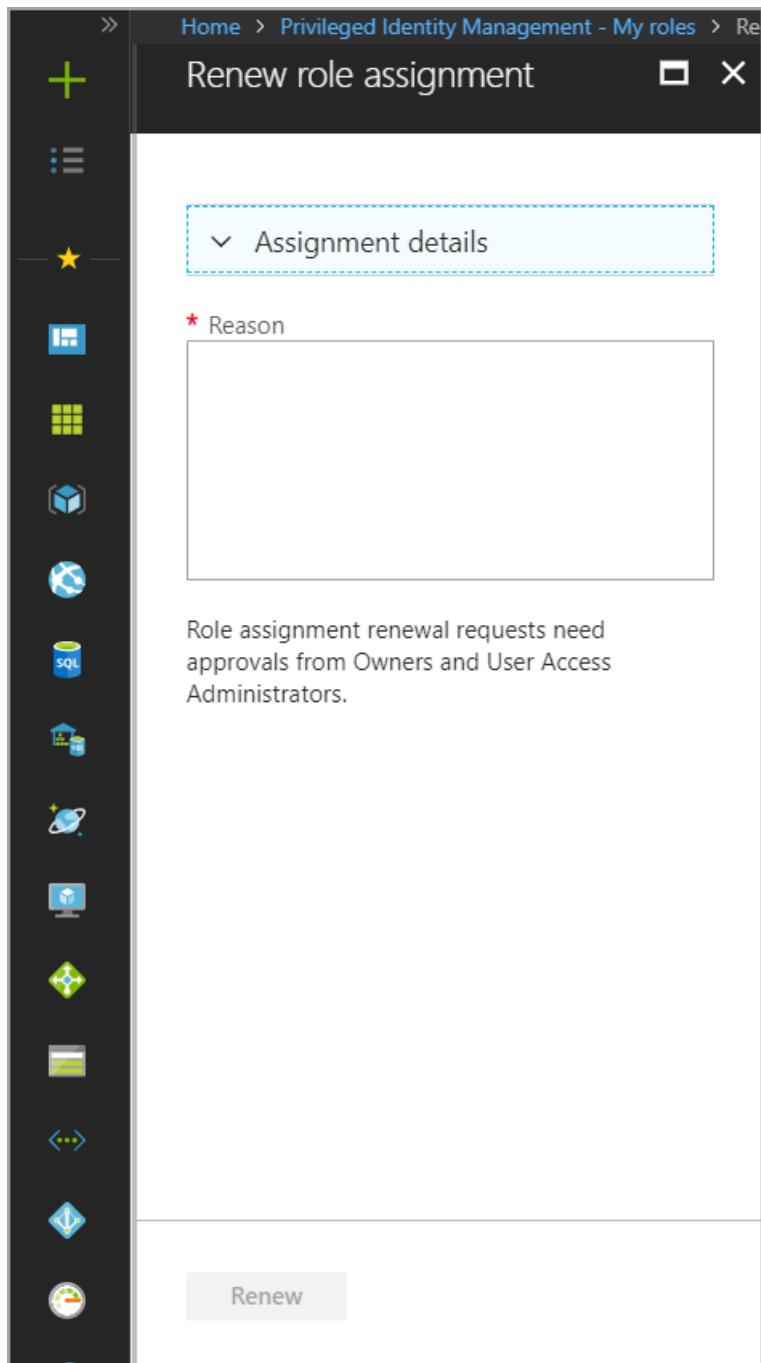
Os usuários que não podem mais acessar recursos podem acessar até 30 dias de histórico de atribuição expirado. Para fazer isso, navegue até **funções Meus** no painel esquerdo e, em seguida, selecione o **expirado funções** guia na seção de funções de recurso do Azure.



| ROLE        | RESOURCE            |
|-------------|---------------------|
| Contributor | Wingtip Toys - Prod |

A lista de papéis mostrada é padronizada para \*\* Funções elegíveis \*\*. Use o menu suspenso para alternar entre as funções atribuídas Elegíveis e Ativas.

Para solicitar a renovação de qualquer uma das atribuições de função na lista, selecione a ação \*\* Renovar \*\*. Em seguida, forneça um motivo para a solicitação. É útil fornecer uma duração além de qualquer contexto adicional ou uma justificativa de negócios que possa ajudar o administrador de recursos a decidir aprovar ou negar.



Depois que a solicitação é enviada, os administradores de recursos são notificados sobre uma solicitação pendente para renovar uma atribuição de função.

#### Aprovação pelo administrador

Os administradores de recursos podem acessar a solicitação de renovação por meio do link na notificação por email ou acessando Privileged Identity Management na portal do Azure e selecionando **aprovar solicitações** no painel esquerdo.

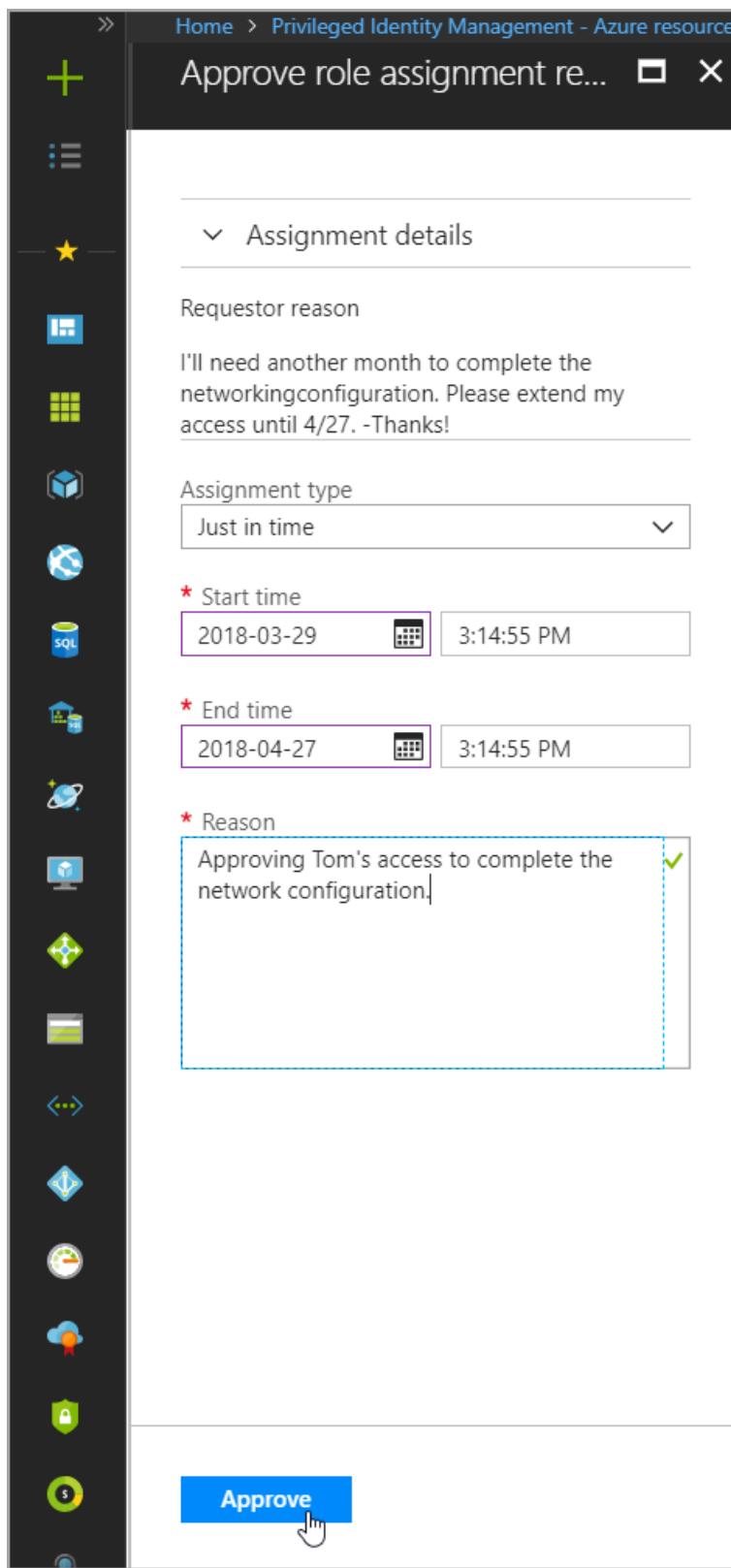
The screenshot shows the Azure portal interface for managing role assignments. The left sidebar has a dark theme with various icons and links. The main content area is titled 'Wingtip Toys - Approve requests'. It contains two tables:

- Requests to renew or extend role assignments:**

| ROLE                | REQUESTOR | RESOURCE     | RESOURCE TYPE | REQUEST TYPE | ASSIGNMENT TYPE | START TIME           | END TIME             | ACTION                                       |
|---------------------|-----------|--------------|---------------|--------------|-----------------|----------------------|----------------------|--|
| Automation Operator | Tom       | Wingtip Toys | subscription  | Member renew | Eligible        | 4/4/2019, 2:18:32 PM | 4/4/2019, 2:18:03 PM | <a href="#">Approve</a> <a href="#">Deny</a> |
- Requests for role activations:**

| ROLE                                 | REQUESTOR          | REQUEST TIME | REASON             | START TIME        | END TIME |
|--------------------------------------|--------------------|--------------|--------------------|-------------------|----------|
| EventGrid EventSubscription Contr... | 4/4/2019, 11:01 AM | S            | 4/4/2019, 11:01 AM | 4/4/2019, 7:01 PM |          |

Quando um administrador seleciona **aprovar** ou **negar**, os detalhes da solicitação são mostrados junto com um campo para fornecer uma justificativa de negócios para os logs de auditoria.



Ao aprovar uma solicitação para renovar a atribuição de função, os administradores de recursos devem inserir uma nova data de início, uma data de término e um tipo de atribuição.

### Renovação pelo administrador

Os administradores de recursos podem renovar atribuições de função expiradas da guia \*\* Members \*\* no menu de navegação à esquerda de um recurso. Eles também podem renovar atribuições de função expiradas de dentro do **expirado** guia funções de uma função de recurso.

Para visualizar uma lista de todas as atribuições de funções expiradas, na tela \*\* Members \*\*, selecione \*\* Expired roles \*\*.

The screenshot shows the Azure Privileged Identity Management - Azure resources dashboard. The left sidebar has a tree view with nodes like Overview, Tasks, My roles, Pending requests, Approve requests, Review access, Manage, Roles, and Members. The 'Members' node is selected. The main content area has a header with 'Add member', 'Review', 'Group by', 'Role settings', 'Refresh', and 'Export' buttons. A message says 'There are 4 pending requests.' Below is a table with columns: ROLE, SUBJECT, START TIME, END TIME, and ACTION. The table lists the following data:

| ROLE                        | SUBJECT | START TIME             | END TIME               | ACTION |
|-----------------------------|---------|------------------------|------------------------|--------|
| Automation Operator         | Tom     | 4/4/2019, 2:18:32 PM   | 4/4/2019, 2:18:03 PM   | Renew  |
| Owner                       | asg     | 2/28/2019, 5:59:39 PM  | 5/29/2019, 6:59:35 PM  | Renew  |
| Owner                       | asg     | 2/27/2019, 1:20:28 PM  | 5/28/2019, 2:20:20 PM  | Renew  |
| Contributor                 | Naren   | 4/2/2018, 12:43:55 PM  | 3/20/2019, 12:42:22 PM | Renew  |
| Reader                      | Priyank | 12/11/2018, 4:36:27 PM | 3/11/2019, 3:26:02 PM  | Renew  |
| Data Box Contributor        | anu     | 12/11/2018, 4:36:27 PM | 3/11/2019, 3:25:49 PM  | Renew  |
| Classic Network Contributor | anu     | 12/11/2018, 4:36:27 PM | 3/11/2019, 2:59:46 PM  | Renew  |
| Owner                       | Tom     | 12/9/2018, 8:45:09 PM  | 3/9/2019, 8:45:00 PM   | Renew  |

## Próximas etapas

- Aprovar ou negar solicitações para funções de recurso do Azure no Privileged Identity Management
- Definir configurações de função de recurso do Azure no Privileged Identity Management

# Definir configurações de função de recurso do Azure no Privileged Identity Management

22/07/2020 • 9 minutes to read • [Edit Online](#)

Ao definir as configurações de função de recurso do Azure, você define as configurações padrão que são aplicadas às atribuições de função de recurso do Azure no Azure Active Directory (Azure AD) Privileged Identity Management (PIM). Use os procedimentos a seguir para configurar o fluxo de trabalho de aprovação e especifique quem pode aprovar ou negar solicitações.

## Abrir configurações de função

Siga estas etapas para abrir as configurações de uma função de recursos do Azure.

1. Entre no [portal do Azure](#) com um usuário na função de [administrador de função com privilégios](#).
2. Abra **Azure ad Privileged Identity Management**.
3. Selecione **recursos do Azure**.
4. Selecione o recurso que você deseja gerenciar, como uma assinatura ou grupo de gerenciamento.

The screenshot shows the Azure Privileged Identity Management - Azure resources interface. On the left, there's a sidebar with various icons and a list of tasks and manage options. The 'Azure resources' option is highlighted with a red box. The main pane shows a 'Resource filter' for 'Subscription' and a search bar. A single resource, 'Wingtip Toys', is listed under the 'RESOURCE' section.

5. Selecione **configurações de função**.

| ROLE                                    | MODIFIED |
|---|----------|
| MultiActions                            | Yes      |
| AcrPull                                 | Yes      |
| Automation Job Operator                 | Yes      |
| EventGrid EventSubscription Contributor | Yes      |
| Cognitive Services User                 | Yes      |
| AcrDelete                               | Yes      |
| Traffic Manager Contributor             | Yes      |
| Site Recovery Contributor               | Yes      |
| Managed Application Operator Role       | Yes      |
| Avere Operator                          | Yes      |
| Automation Operator                     | Yes      |
| Storage Account Contributor             | Yes      |

6. Selecione a função cujas configurações você deseja configurar.

| SETTING  | STATE      |
|--|------------|
| Allow permanent eligible assignment                      | No         |
| Expire eligible assignments after                        | 3 month(s) |
| Allow permanent active assignment                        | No         |
| Expire active assignments after                          | 1 month(s) |
| Require Multi-Factor Authentication on active assignment | No         |
| Require justification on active assignment               | Yes        |

| SETTING   | STATE     |
|---|-----------|
| Activation maximum duration (hours)               | 8 hour(s) |
| Require Multi-Factor Authentication on activation | No        |
| Require justification on activation               | Yes       |
| Require approval to activate                      | No        |
| Approvers   | None      |

7. Selecione **Editar** para abrir o painel configurações de função . A primeira guia permite que você atualize a configuração de ativação de função no Privileged Identity Management.

Edit role setting - BizTalk Contributor

Privileged Identity Management - Azure resources

Activation **Assignment** Notification

Activation maximum duration (hours)

8

On activation, require

Azure MFA  None

Require justification on activation

Require ticket information on activation

Require approval to activate

Select approver(s) >

No approver selected

Update **Next: Assignment**

8. Selecione a guia **atribuição** ou o botão **próximo: atribuição** na parte inferior da página para abrir a guia Configuração de atribuição. Essas configurações controlam as atribuições de função feitas dentro da interface Privileged Identity Management.

Edit role setting - BizTalk Contributor

Privileged Identity Management - Azure resources

Activation **Assignment** **Notification**

Allow permanent eligible assignment

Expire eligible assignments after

3 Months

Allow permanent active assignment

Expire active assignments after

1 Month

Require Azure Multi-Factor Authentication on active assignment

Require justification on active assignment

Update **Prev: Activation** **Next: Notification**

9. Use a guia **notificação** ou o botão **Avançar: ativação** na parte inferior da página para acessar a guia Configuração de notificação para essa função. Essas configurações controlam todas as notificações por email relacionadas a essa função.

**Edit role setting - BizTalk Contributor**  
Privileged Identity Management - Azure resources

**Activation Assignment Notification**

**Send notifications when members are assigned as eligible to this role:**

| Type   | Default recipients                           | Additional recipients              | Critical emails only ⓘ   |
|--|--|------------------------------------|--------------------------|
| Role assignment alert                                  | <input checked="" type="checkbox"/> Admin    | Email Ids separated by semicolon() | <input type="checkbox"/> |
| Notification to the assigned user (assignee)           | <input checked="" type="checkbox"/> Assignee | Email Ids separated by semicolon() | <input type="checkbox"/> |
| Request to approve a role assignment renewal/extension | <input checked="" type="checkbox"/> Approver | Email Ids separated by semicolon() | <input type="checkbox"/> |

**Send notifications when members are assigned as active to this role:**

| Type   | Default recipients                           | Additional recipients              | Critical emails only ⓘ   |
|--|--|------------------------------------|--------------------------|
| Role assignment alert                                  | <input checked="" type="checkbox"/> Admin    | Email Ids separated by semicolon() | <input type="checkbox"/> |
| Notification to the assigned user (assignee)           | <input checked="" type="checkbox"/> Assignee | Email Ids separated by semicolon() | <input type="checkbox"/> |
| Request to approve a role assignment renewal/extension | <input checked="" type="checkbox"/> Approver | Email Ids separated by semicolon() | <input type="checkbox"/> |

**Send notifications when eligible members activate this role:**

| Type                                       | Default recipients                            | Additional recipients                            | Critical emails only ⓘ   |
|--|---|--|--------------------------|
| Role activation alert                      | <input checked="" type="checkbox"/> Admin     | Email Ids separated by semicolon()               | <input type="checkbox"/> |
| Notification to activated user (requestor) | <input checked="" type="checkbox"/> Requestor | Email Ids separated by semicolon()               | <input type="checkbox"/> |
| Request to approve an activation           | <input checked="" type="checkbox"/> Approver  | Only designated approvers can receive this email | <input type="checkbox"/> |

**Buttons:** [Update](#) | [Prev: Assignment](#)

Na guia **notificações** da página Configurações de função, Privileged Identity Management habilita o controle granular sobre quem recebe notificações e quais notificações elas recebem.

- **Desligando um email**

Você pode desativar emails específicos desmarcando a caixa de seleção destinatário padrão e excluindo destinatários adicionais.

- **Limitar emails a endereços de email especificados**

Você pode desativar os emails enviados aos destinatários padrão desmarcando a caixa de seleção destinatário padrão. Em seguida, você pode adicionar endereços de email adicionais como destinatários adicionais. Se você quiser adicionar mais de um endereço de email, separe-os usando um ponto-e-vírgula (;).

- **Enviar emails para destinatários padrão e destinatários adicionais**

Você pode enviar emails para o destinatário padrão e para o destinatário adicional, marcando a caixa de seleção destinatário padrão e adicionando endereços de email para destinatários adicionais.

- **Somente emails críticos**

Para cada tipo de email, você pode marcar a caixa de seleção para receber emails críticos apenas. Isso significa que Privileged Identity Management continuará a enviar emails para os destinatários configurados somente quando o email exigir uma ação imediata. Por exemplo, emails solicitando que os usuários estendam suas atribuições de função não serão disparados enquanto um email que exigir que os administradores aprovem uma solicitação de extensão será disparado.

10. Selecione o botão **Atualizar** a qualquer momento para atualizar as configurações de função.

## Duração dae atribuição

É possível escolher entre duas opções de duração de atribuição para cada tipo de atribuição (qualificada e ativa) ao definir as configurações de uma função. Essas opções se tornam a duração máxima padrão quando um usuário é atribuído à função no Privileged Identity Management.

Você pode escolher uma destas opções de duração de atribuição **qualificadas** :

|   |   |
|---|---|
| <b>Permitir atribuição qualificada permanente</b> | Os administradores de recursos podem atribuir uma atribuição qualificada permanente.  |
| <b>Expirar atribuição qualificada após</b>        | Os administradores de recursos podem exigir que todas as atribuições qualificadas tenham uma data de início e de término especificadas. |

E, você pode escolher uma destas opções de duração da atribuição **ativa**:

|   |   |
|---|---|
| <b>Permitir atribuição ativa permanente</b> | Os administradores de recursos podem atribuir uma atribuição ativa permanente.  |
| <b>Expirar atribuição ativa após</b>        | Os administradores de recursos podem exigir que todas as atribuições ativas tenham uma data de início e de término especificadas. |

#### NOTE

Todas as atribuições que têm uma data de término especificada poderão ser renovadas por administradores de recursos. Além disso, os usuários podem iniciar solicitações de autoatendimento para [estender ou renovar atribuições de função](#).

## Exigir autenticação multifator

O Privileged Identity Management fornece imposição opcional da Autenticação Multifator do Azure para dois cenários diferentes.

### Exigir Autenticação Multifator na atribuição ativa

Em alguns casos, talvez você queira atribuir um usuário ou grupo a uma função por uma duração curta (um dia, por exemplo). Nesse caso, os usuários atribuídos não precisam solicitar ativação. Nesse cenário, Privileged Identity Management não pode impor a autenticação multifator quando o usuário usa sua atribuição de função porque eles já estão ativos na função a partir do momento em que são atribuídos.

Para garantir que o administrador de recursos que está atendendo à atribuição seja quem eles dizem que eles são, você pode impor a autenticação multifator na atribuição ativa marcando a caixa de **atribuição exigir autenticação multifator no Active**.

### Exigir a Autenticação Multifator na ativação

Você pode exigir que os usuários qualificados para uma função comprovem quem estão usando a autenticação multifator do Azure antes que possam ser ativados. A autenticação multifator garante que o usuário seja quem dizem que eles estão com certeza razoável. A aplicação dessa opção protege recursos críticos em situações em que a conta do usuário pode ter sido comprometida.

Para exigir a autenticação multifator antes da ativação, marque a caixa de seleção **exigir autenticação multifator no modo de ativação**.

Para saber mais, confira [Autenticação multifator e Privileged Identity Management](#).

## Duração máxima de ativação

Use o controle deslizante **Duração máxima da ativação** para definir o tempo máximo, em horas, que uma função permanecerá ativa antes de expirar. Esse valor pode ser de uma a 24 horas.

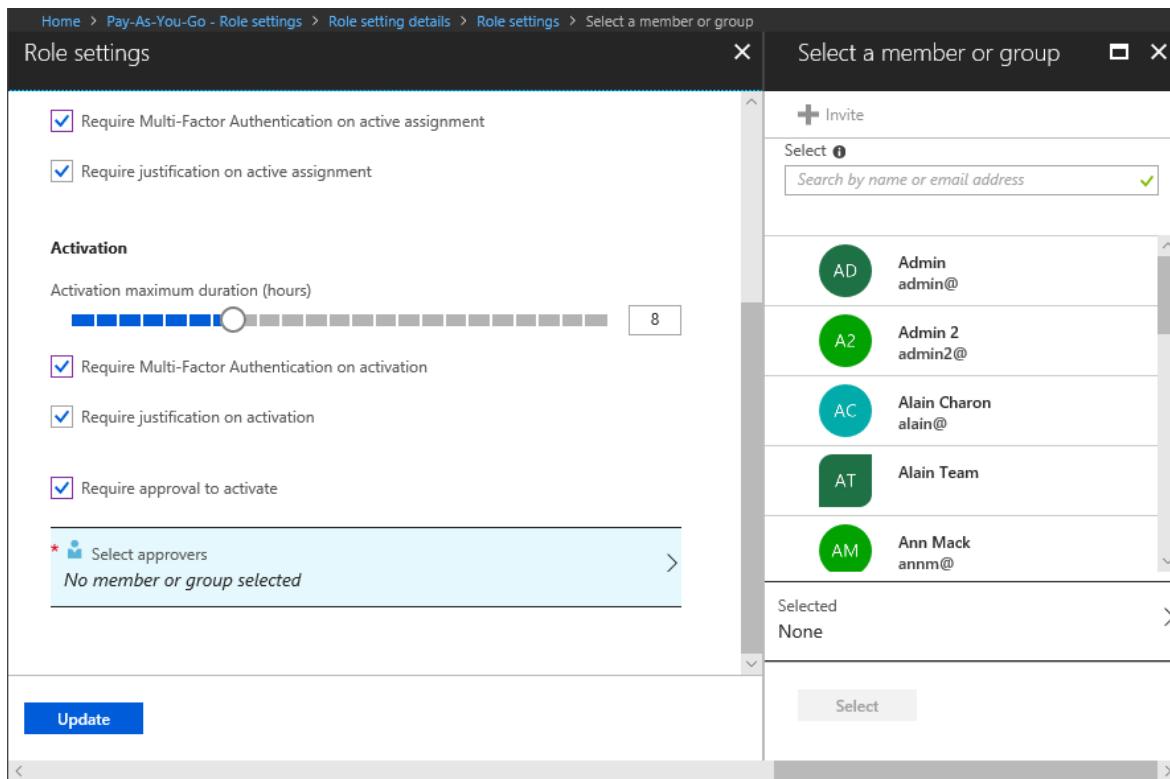
## Exigir justificativa

Você pode exigir que os usuários insiram uma justificativa de negócios ao serem ativados. Para exigir justificativa, marque a caixa **\*\*Exigir justificativa na atribuição ativa\*\*** ou a caixa **Exigir justificativa na ativação**.

## Exigir aprovação para ativar

Se você quiser exigir aprovação para ativar uma função, siga estas etapas.

1. Marque a caixa de seleção **Exige aprovação para ativar**.
2. Selecione **selecionar aprovadores** para abrir a página **selecionar um membro ou grupo**.



3. Selecione pelo menos um usuário ou grupo e clique em **selecionar**. Você pode adicionar qualquer combinação de usuários e grupos. É necessário selecionar pelo menos um aprovador. Não há nenhum aprovador padrão.  
Suas seleções serão exibidas na lista de aprovadores selecionados.
4. Depois de especificar todas as suas configurações de função, selecione **Atualizar** para salvar suas alterações.

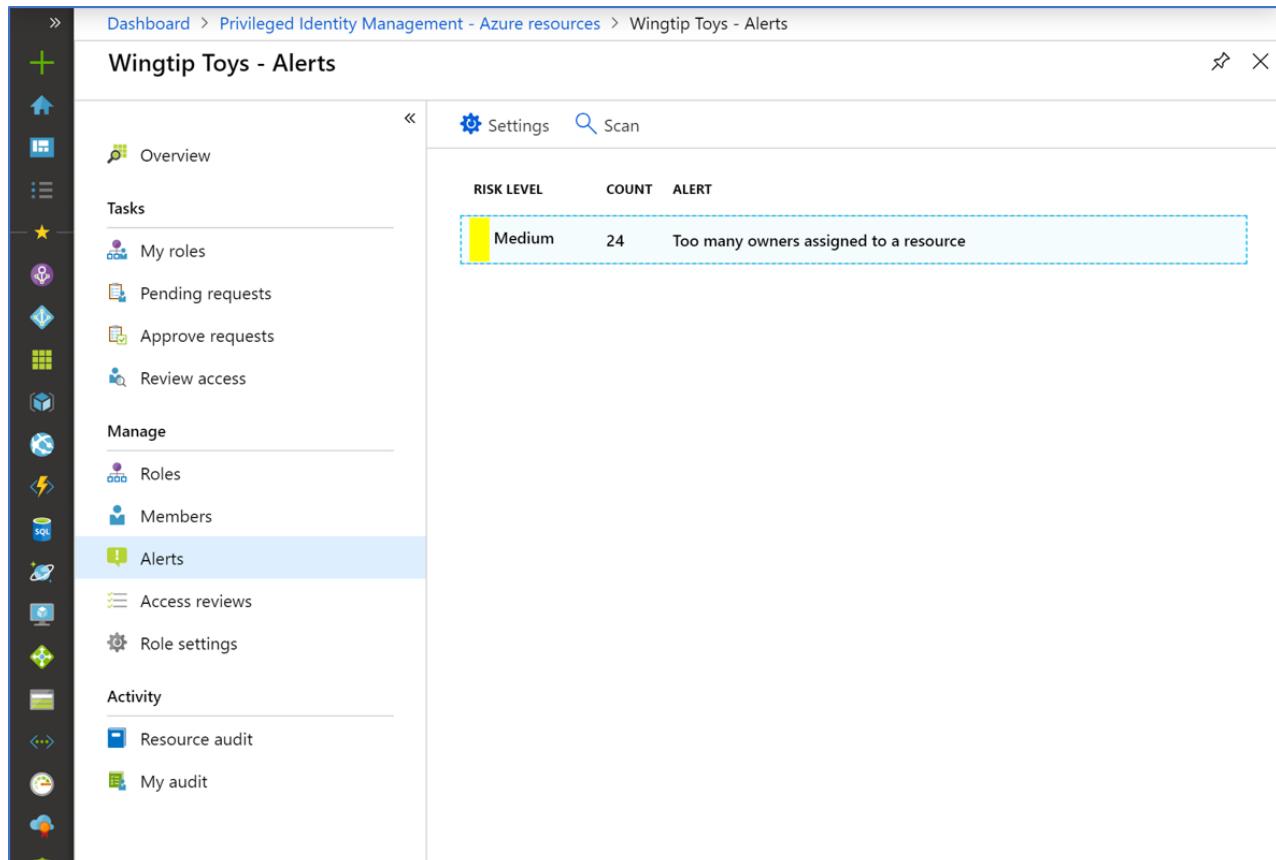
## Próximas etapas

- [Atribuir funções de recurso do Azure no Privileged Identity Management](#)
- [Configurar alertas de segurança para funções de recurso do Azure no Privileged Identity Management](#)

# Configurar alertas de segurança para funções de recurso do Azure no Privileged Identity Management

22/07/2020 • 2 minutes to read • [Edit Online](#)

Privileged Identity Management (PIM) gera alertas quando há atividade suspeita ou não segura em sua organização do Azure Active Directory (AD do Azure). Quando um alerta é disparado, ele aparece na página Alerts.



The screenshot shows the 'Wingtip Toys - Alerts' page in the Azure PIM interface. The left sidebar lists various management tasks like 'My roles', 'Pending requests', and 'Alerts'. The main area displays a single alert card:

| RISK LEVEL | COUNT | ALERT                                  |
|------------|-------|--|
| Medium     | 24    | Too many owners assigned to a resource |

## Revisar alertas

Selecione um alerta para ver um relatório que lista os usuários ou funções que dispararam o alerta, juntamente com diretrizes de correção.

Too many owners assigned to a resource

Fix  Dismiss  Settings

Last scan time  
3/29/2018 3:44:02 PM

Description  
The number of users with the Owner role is too high. We recommend assigning these individuals to less privileged roles or roles more suitable to their daily needs. Take a moment to review the current assignments, and suggested changes here.

Mitigation steps  
To mitigate this issue, reduce the number of users in the Owner role. Review the list of users in the list, and reassign them to a less privileged role such as Contributor.  
Click "Fix" button above to automatically apply these mitigation steps

Type  
Vulnerability

Severity  
Medium

Security impact  
As the number of users with the owner role increases, so does the potential for malicious or mistaken actions affecting your resource.

How to prevent next time  
Choose a role that provides the fewest privileges necessary for a user or group to complete their tasks.

| ASSIGNEE NAME | ASSIGNEE TYPE    |
|---------------|------------------|
| Albert Almora | User             |
| anujcuser     | User             |
| APRJ-VM-01-T  | ServicePrincipal |
| Binbin Hu     | User             |

## Alertas

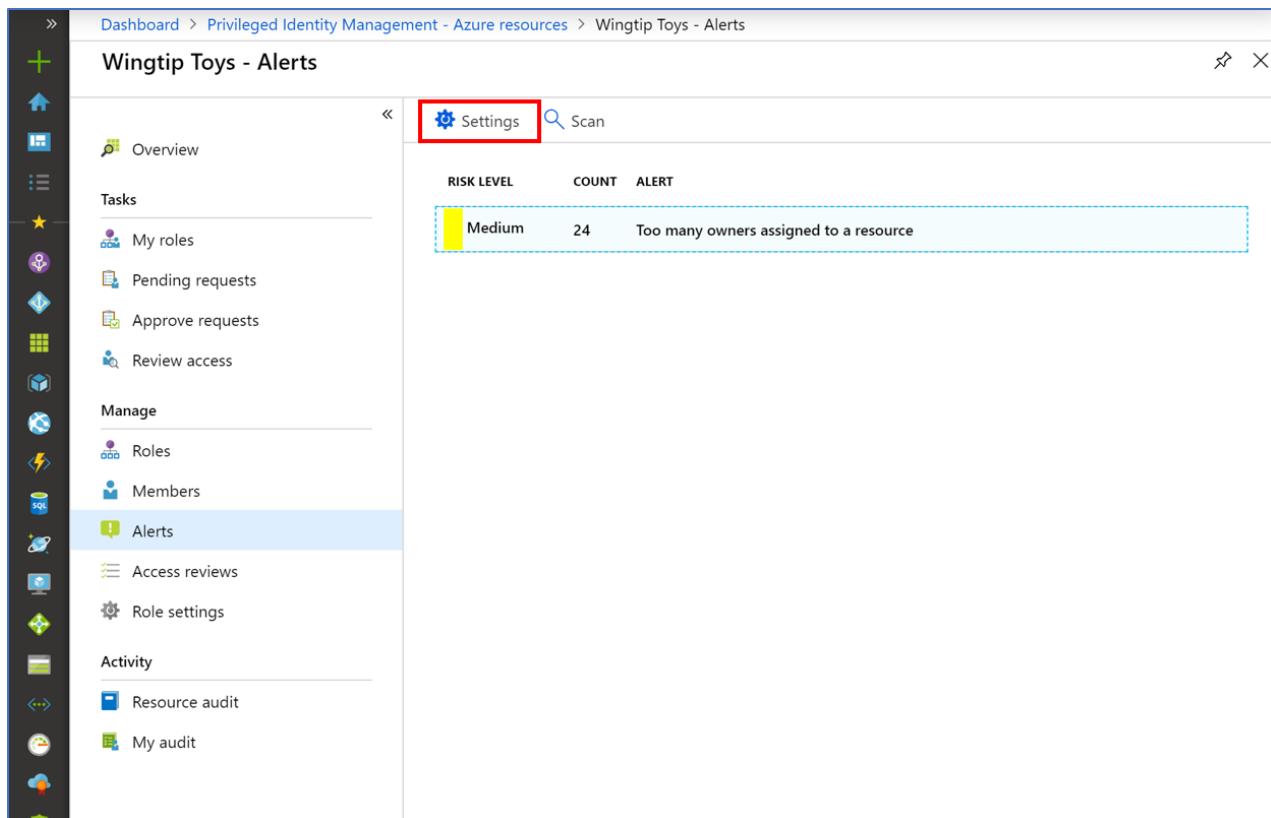
| ALERTA   | SEVERITY | GATILHO  | RECOMENDAÇÃO  |
|--|----------|--|---|
| Muitos proprietários atribuídos a um recurso             | Médio    | Muitos usuários têm a função de proprietário.                | Examine os usuários na lista e reatribua alguns a funções menos privilegiadas.            |
| Muitos proprietários permanentes atribuídos a um recurso | Médio    | Muitos usuários são permanentemente atribuídos a uma função. | Revise os usuários na lista e reatribua alguns para exigir ativação para o uso da função. |
| Duplicar função criada                                   | Médio    | Várias funções têm os mesmos critérios.                      | Use apenas uma dessas funções.  |

### Severity

- Alta: exige ação imediata devido a uma violação da política.
- Média: não exige ação imediata, mas sinaliza uma possível violação da política.
- Baixa: não exige ação imediata, mas sugere uma alteração preferencial da política.

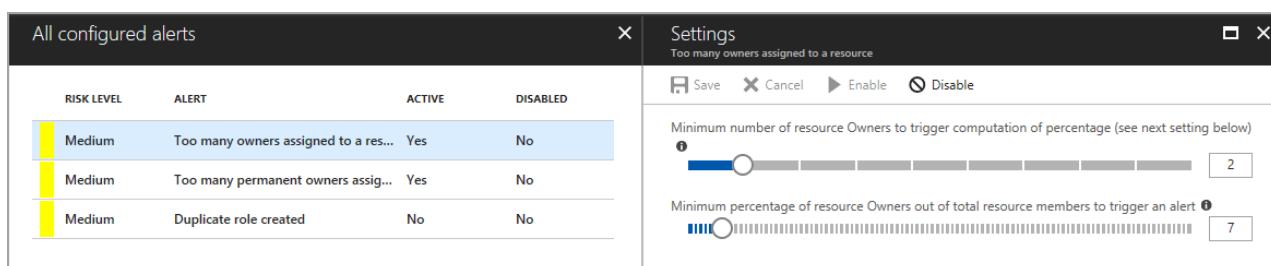
## Definir configurações de alerta de segurança

Na página Alertas, vá para Configurações.



The screenshot shows the Azure Privileged Identity Management - Azure resources blade. In the top navigation bar, the path is: Dashboard > Privileged Identity Management - Azure resources > Wingtip Toys - Alerts. On the left sidebar, under the 'Alerts' section, the 'Alerts' item is selected and highlighted with a blue background. At the top of the main content area, there are three tabs: 'Overview', 'Settings' (which is highlighted with a red box), and 'Scan'. Below the tabs, there is a table with three columns: RISK LEVEL, COUNT, and ALERT. One row is visible, showing 'Medium' risk level, '24' count, and the alert message 'Too many owners assigned to a resource'.

Personalize configurações nos diferentes alertas para trabalhar com seu ambiente e as metas de segurança.



The screenshot shows two windows side-by-side. On the left is a table titled 'All configured alerts' with four columns: RISK LEVEL, ALERT, ACTIVE, and DISABLED. It lists three rows, all of which are 'Medium' risk level and 'Active'. The first row has the alert message 'Too many owners assigned to a resource'. On the right is a 'Settings' dialog for this specific alert. The title bar says 'Settings' and the alert message 'Too many owners assigned to a resource'. The dialog includes buttons for 'Save', 'Cancel', 'Enable', and 'Disable'. Below these are two slider controls. The first slider is labeled 'Minimum number of resource Owners to trigger computation of percentage (see next setting below)' and has a value of 2. The second slider is labeled 'Minimum percentage of resource Owners out of total resource members to trigger an alert' and has a value of 7.

## Próximas etapas

- Definir configurações de função de recurso do Azure no Privileged Identity Management

# Exibir a atividade e o histórico de auditoria das funções de recurso do Azure no Privileged Identity Management

22/07/2020 • 7 minutes to read • [Edit Online](#)

Com o Azure AD (Azure Active Directory) PIM (Privileged Identity Management), você pode exibir a atividade, as ativações e o histórico de auditoria para funções de recursos do Azure em sua organização. Isso inclui assinaturas, grupos de recursos e até mesmo máquinas virtuais. Qualquer recurso dentro do portal do Azure que aproveita a funcionalidade de controle de acesso baseado em função do Azure pode aproveitar os recursos de segurança e gerenciamento do ciclo de vida no Privileged Identity Management.

## NOTE

Se sua organização tiver funções de gerenciamento terceirizadas para um provedor de serviços que usa o [Gerenciamento de recursos delegado do Azure](#), as atribuições de função autorizadas por esse provedor de serviços não serão mostradas aqui.

## Exibir a atividade e as ativações

Para ver as ações que um usuário específico realizou em vários recursos, você pode exibir a atividade do recurso do Azure associada a um período de ativação especificado.

1. Abra **Azure ad Privileged Identity Management**.
2. Selecione **recursos do Azure**.
3. Selecione o recurso para o qual você deseja exibir a atividade e as ativações.
4. Selecione **funções ou Membros**.
5. Selecione um usuário.

Você verá um resumo das ações do usuário nos recursos do Azure por data. Ele também mostra as ativações de função recentes nesse mesmo período.

User details

[Remove](#) [Change settings](#)

Essentials ^

|  |  |
|--|--|
| User name<br>Angelina Berggren                 | User email<br>bergg@fimdev.net               |
| Role<br>Contributor                            | Status<br>Eligible                           |
| Assignment start time<br>9/15/2017 12:48:21 PM | Assignment end time<br>9/15/2018 12:47:46 PM |

\* Start date [i](#) \* End date [i](#)  
 [Calendar](#)  [Calendar](#) [Apply](#)

Resource activity summary

Role activations

| ACTIVATION TIME       | ACTION                          |
|-----------------------|---------------------------------|
| 2/28/2018 6:51:53 AM  | Activate role <a href="#">🔗</a> |
| 2/27/2018 10:13:05 AM | Activate role                   |
| 2/26/2018 4:28:13 PM  | Activate role                   |
| 2/23/2018 9:01:27 AM  | Activate role                   |
| 2/22/2018 7:52:11 AM  | Activate role                   |
| 2/21/2018 2:46:22 PM  | Activate role                   |

6. Selecione uma ativação de função específica para ver detalhes e a atividade de recurso do Azure correspondente que ocorreu enquanto esse usuário estava ativo.

Dashboard > Privileged Identity Management - Azure resources > Wingtip Toys - Members

Wingtip Toys - Members

Overview [+ Add member](#) [Review](#) [Group by](#) [Role settings](#) [Refresh](#) [Export](#)

There are 4 pending requests. [→](#)

Eligible roles Active roles Expired roles

Assignee type: Eligible

| ROLE                        | SUBJECT | START TIME             | END TIME               |
|-----------------------------|---------|------------------------|------------------------|
| Automation Operator         | Tom     | 4/4/2019, 2:18:32 PM   | 4/4/2019, 2:18:32 PM   |
| Owner                       | asg     | 2/28/2019, 5:59:39 PM  | 5/29/2019, 6:59        |
| Owner                       | asg     | 2/27/2019, 1:20:28 PM  | 5/28/2019, 2:20        |
| Contributor                 | Naren   | 4/2/2018, 12:43:55 PM  | 3/20/2019, 12:43:55 PM |
| Reader                      | Priyank | 12/11/2018, 4:36:27 PM | 3/11/2019, 3:26        |
| Data Box Contributor        | anu     | 12/11/2018, 4:36:27 PM | 3/11/2019, 3:25        |
| Classic Network Contributor | anu     | 12/11/2018, 4:36:27 PM | 3/11/2019, 2:59        |
| Owner                       | Tom     | 12/9/2018, 8:45:09 PM  | 3/9/2019, 8:45:09 PM   |

Export membership

Export membership information for everyone with role assignments inside this subscription.

Export members only in this subscription

Export membership information for everyone with role assignments inside this subscription as well as its child resources (resource groups, resources etc.)

[Export all members](#)

## Exportar as atribuições de função com filhos

Talvez você tenha um requisito de conformidade no qual precisa fornecer uma lista completa de atribuições de função para auditores. Privileged Identity Management permite consultar atribuições de função em um recurso

específico, que inclui atribuições de função para todos os recursos filho. Anteriormente, era difícil para os administradores obter uma lista completa das atribuições de função para uma assinatura e eles precisavam exportar as atribuições de função para cada recurso específico. Usando Privileged Identity Management, você pode consultar todas as atribuições de função ativas e qualificadas em uma assinatura, incluindo atribuições de função para todos os grupos de recursos e recursos.

1. Abra Azure ad Privileged Identity Management.
  2. Selecione **recursos** do Azure.
  3. Selecione o recurso para o qual você deseja exportar atribuições de função, como uma assinatura.
  4. Selecione **Membros**.
  5. Selecione **Exportar** para abrir o painel Exportar associação.

Dashboard > Privileged Identity Management - Azure resources > Wingtip Toys - Members

### Wingtip Toys - Members

Overview Tasks Manage Activity

Add member Review Group by Role settings Refresh Export

There are 4 pending requests.

Eligible roles Active roles Expired roles

Assignee type Eligible

| ROLE                        | SUBJECT | START TIME             | END TIME               |
|-----------------------------|---------|------------------------|------------------------|
| Automation Operator         | Tom     | 4/4/2019, 2:18:32 PM   | 4/4/2019, 2:18:32 PM   |
| Owner                       | asg     | 2/28/2019, 5:59:39 PM  | 5/29/2019, 6:59 PM     |
| Owner                       | asg     | 2/27/2019, 1:20:28 PM  | 5/28/2019, 2:20 PM     |
| Contributor                 | Naren   | 4/2/2018, 12:43:55 PM  | 3/20/2019, 12:43:55 PM |
| Reader                      | Priyank | 12/11/2018, 4:36:27 PM | 3/11/2019, 3:26 PM     |
| Data Box Contributor        | anu     | 12/11/2018, 4:36:27 PM | 3/11/2019, 3:25 PM     |
| Classic Network Contributor | anu     | 12/11/2018, 4:36:27 PM | 3/11/2019, 3:59 PM     |
| Owner                       | Tom     | 12/9/2018, 8:45:09 PM  | 3/9/2019, 8:45:09 PM   |

Export membership

Export membership information for everyone with role assignments inside this subscription.

Export members only in this subscription

Export membership information for everyone with role assignments inside this subscription as well as its child resources. (resource groups, resources etc.)

**Export all members**

6. Selecione **exportar todos os membros** para exportar todas as atribuições de função em um arquivo CSV.

| Assignment | User Group Name             | Resource Name          | Role Name                  | Resource Type                    | Email | Member Type | Assignment Start Time (UTC) | Assignment End Time (UTC) |
|------------|-----------------------------|------------------------|----------------------------|----------------------------------|-------|-------------|-----------------------------|---------------------------|
| Active     | anu                         | Subscription1          | Contributor                | subscription                     |       | Direct      | 2018-12-13 23:33:12Z        | Permanent                 |
| Eligible   | anu                         | Subscription1          | Owner                      | subscription                     |       | Direct      | 2018-11-06 00:41:15Z        | 2019-02-04 00:40:55Z      |
| Eligible   | anu                         | Subscription1          | Owner                      | subscription                     |       | Direct      | 2018-11-06 00:49:55Z        | 2019-02-04 00:49:43Z      |
| Active     | Ashish                      | Subscription1          | Owner                      | subscription                     |       | Direct      | 2018-11-19 19:16:13Z        | Permanent                 |
| Eligible   | anu                         | RG                     | API Manager resourcegroup  | resourcegroup                    |       | Direct      | 2018-12-07 00:33:10Z        | 2019-03-07 00:32:49Z      |
| Active     | anu                         | RG                     | Cost Manager resourcegroup | resourcegroup                    |       | Direct      | 2018-12-14 20:05:00Z        | 2019-01-13 19:58:40Z      |
| Active     | MS-PIM                      | Subscription1          | User Access Ai             | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | administrator               | Subscription1          | Cost Manager               | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | administrator               | Subscription1          | API Manager                | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | nan                         | Subscription1          | Owner                      | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | Subscription1          | Owner                      | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | ves                         | Subscription1          | Owner                      | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | anu                         | Subscription1          | Owner                      | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | Qi                          | Subscription1          | Owner                      | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | euc                         | Subscription1          | Owner                      | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | Nar                         | Subscription1          | Owner                      | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | ma                          | Subscription1          | Contributor                | subscription                     |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | appMrg7                | Owner                      | resourcegroup                    |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | AppMRG4                | Owner                      | resourcegroup                    |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | JitManualApprove2      | Owner                      | resourcegroup                    |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | app7                   | Owner                      | microsoft.solutions/applications |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | AppAutoApprove3        | Owner                      | microsoft.solutions/applications |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | AppManualApprove11     | Owner                      | microsoft.solutions/applications |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | AppManualApprove10     | Owner                      | microsoft.solutions/applications |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | JitManualApproveND1    | Owner                      | resourcegroup                    |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | AppMRG2                | Owner                      | resourcegroup                    |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | AppMRG11               | Owner                      | resourcegroup                    |       | Direct      |                             | Permanent                 |
| Active     | Appliance Resource Provider | JitManualApprovelocked | Owner                      | resourcegroup                    |       | Direct      |                             | Permanent                 |

## Exibir o histórico de auditoria de recursos

A auditoria de recursos fornece uma exibição de todas as atividades de função para um recurso.

1. Abra Azure ad Privileged Identity Management.
  2. Selecione **recursos do Azure**.
  3. Selecione o recurso para o qual você deseja exibir o histórico de auditoria.
  4. Selecione **auditoria de recurso**.

5. Filtre o histórico usando uma data predefinida ou um intervalo personalizado.

| TIME                  | REQUESTOR | ACTION   | RESOURCE NAME | PRIMARY TARGET                    | SUBJECT | SUBJECT TYPE | STATUS |
|-----------------------|-----------|--|---------------|-----------------------------------|---------|--------------|--------|
| 4/4/2019, 2:31:29 PM  | Shaun     | Add eligible member to role in PIM complete            | Wingtip Toys  | Automation Operator               | Shaun   | Member       | ✓      |
| 4/4/2019, 2:31:29 PM  | Shaun     | Add eligible member to role in PIM requested           | Wingtip Toys  | Automation Operator               | Shaun   | Member       | ✓      |
| 4/4/2019, 2:30:56 PM  | Shaun     | Remove member from role in PIM completed               | Wingtip Toys  | Automation Operator               | Shaun   | Member       | ✓      |
| 4/4/2019, 2:18:32 PM  | Shaun     | Remove eligible member from role in PIM completed      | Wingtip Toys  | Automation Operator               | Tom     | Member       | ✓      |
| 4/4/2019, 2:18:32 PM  | Shaun     | Add eligible member to role in PIM complete            | Wingtip Toys  | Automation Operator               | Tom     | Member       | ✓      |
| 4/4/2019, 2:18:31 PM  | Shaun     | Add eligible member to role in PIM requested           | Wingtip Toys  | Automation Operator               | Tom     | Member       | ✓      |
| 4/4/2019, 11:02:53 AM |           | Add member to role canceled (PIM activation)           | Wingtip Toys  | EventGrid EventSubscription Co... |         | Member       | ✓      |
| 4/4/2019, 11:01:12 AM |           | Add member to role approval requested (PIM activation) | Wingtip Toys  | EventGrid EventSubscription Co... |         | Member       | ✓      |
| 4/4/2019, 11:01:04 AM |           | Add member to role requested (PIM activation)          | Wingtip Toys  | EventGrid EventSubscription Co... |         | Member       | ✓      |
| 4/4/2019, 11:00:50 AM |           | Add member to role canceled (PIM activation)           | Wingtip Toys  | EventGrid EventSubscription Co... |         | Member       | ✓      |
| 4/4/2019, 10:34:14 AM | Shaun     | Add eligible member to role in PIM requested           | Wingtip Toys  | Billing Reader                    | Shaun   | Member       | ✓      |
| 4/4/2019, 10:31:08 AM | Shaun     | Add member to role completed (PIM activation)          | Wingtip Toys  | Owner                             | Shaun   | Member       | ✓      |
| 4/4/2019, 10:31:05 AM | Shaun     | Add member to role requested (PIM activation)          | Wingtip Toys  | Owner                             | Shaun   | Member       | ✓      |
| 4/4/2019, 9:16:10 AM  | Kelly     | Add member to role completed (PIM activation)          | Wingtip Toys  | Owner                             | Kelly   | Member       | ✓      |

6. Em Tipo de auditoria, selecione Ativar (Atribuído + Ativado).

| TIME                  | REQUESTOR     | ACTION                   | RESOURCE NAME       | PRIMARY TARGET         | SUBJECT       | SUBJECT TYPE | STATUS |
|-----------------------|---------------|--------------------------|---------------------|------------------------|---------------|--------------|--------|
| 3/29/2018 2:54:47 PM  | Phoebe Garner | Activate role (activity) | Wingtip Toys - Prod | Owner                  | Phoebe Garner | User         | ✓      |
| 3/29/2018 12:37:05 PM | Phoebe Garner | Activate role (activity) | Wingtip Toys - Prod | Owner                  | Phoebe Garner | User         | ✓      |
| 3/29/2018 11:13:07 AM | vijag         | Activate role (activity) | Wingtip Toys - Prod | Monitoring Reader      | vijag         | User         | ✓      |
| 3/29/2018 11:09:30 AM | vijayuser     | Activate role (activity) | Wingtip Toys - Prod | Reader and Data Access | vijag         | User         | ✓      |
| 3/29/2018 10:57:00 AM | vijag         | Activate role (activity) | Wingtip Toys - Prod | Owner                  | vijag         | User         | ✓      |

| TIME                  | REQUESTOR     | ACTION                   | RESOURCE NAME       | PRIMARY TARGET         | SUBJECT       | SUBJECT TYPE | STATUS |
|-----------------------|---------------|--------------------------|---------------------|------------------------|---------------|--------------|--------|
| 3/29/2018 2:54:47 PM  | Phoebe Garner | Activate role (activity) | Wingtip Toys - Prod | Owner                  | Phoebe Garner | User         | ✓      |
| 3/29/2018 12:37:05 PM | Phoebe Garner | Activate role (activity) | Wingtip Toys - Prod | Owner                  | Phoebe Garner | User         | ✓      |
| 3/29/2018 11:13:07 AM | vijag         | Activate role (activity) | Wingtip Toys - Prod | Monitoring Reader      | vijag         | User         | ✓      |
| 3/29/2018 11:09:30 AM | vijayuser     | Activate role (activity) | Wingtip Toys - Prod | Reader and Data Access | vijag         | User         | ✓      |
| 3/29/2018 10:57:00 AM | vijag         | Activate role (activity) | Wingtip Toys - Prod | Owner                  | vijag         | User         | ✓      |

7. Em Ação, clique em (atividade) de um usuário para ver os detalhes da atividade desse usuário em recursos do Azure.

Activity details - 3/29/2018 11:09:30 AM - vijag

Wingtip Toys - Prod - subscription

User activities

| TIME                  | ACTION                                  | ROLE                   | TARGET        | STATUS |
|-----------------------|---|------------------------|---------------|--------|
| 3/29/2018 12:38:32 PM | Admin remove eligible role assign...    | DevTest Labs User      | Phoebe Garner | ✓      |
| 3/29/2018 12:38:31 PM | Create request for eligible role re...  | DevTest Labs User      | Phoebe Garner | ✓      |
| 3/29/2018 12:37:52 PM | Request approval for role activation    | DevTest Labs User      | vijag         | ✓      |
| 3/29/2018 12:37:48 PM | Create request for role activation      | DevTest Labs User      | vijag         | ✓      |
| 3/29/2018 12:37:10 PM | Add eligible role assignment            | DevTest Labs User      | Phoebe Garner | ✓      |
| 3/29/2018 12:37:09 PM | Create request for eligible role ass... | DevTest Labs User      | Phoebe Garner | ✓      |
| 3/29/2018 12:36:49 PM | Update role settings                    | DevTest Labs User      | -             | ✓      |
| 3/29/2018 11:13:40 AM | Create request for permanent elig...    | Monitoring Reader      | Phoebe Garner | ✓      |
| 3/29/2018 11:13:07 AM | Activate role                           | Monitoring Reader      | vijag         | ✓      |
| 3/29/2018 11:13:01 AM | Create request for role activation      | Monitoring Reader      | vijag         | ✓      |
| 3/29/2018 11:12:26 AM | Add permanent eligible role assig...    | Monitoring Reader      | Phoebe Garner | ✓      |
| 3/29/2018 11:12:23 AM | Create request for permanent elig...    | Monitoring Reader      | Phoebe Garner | ✓      |
| 3/29/2018 11:10:36 AM | Create request for eligible role re...  | Reader and Data Access | Phoebe Garner | ✓      |
| 3/29/2018 11:09:30 AM | Activate role                           | Reader and Data Access | vijag         | ✓      |

Resource activities

| TIME       | RESOURCE | ACTION | STATUS |
|------------|----------|--------|--------|
| No results |          |        |        |

## Exibir minha auditoria

A opção Minha auditoria permite que você exiba sua atividade de função pessoal.

1. Abra Azure ad Privileged Identity Management.
2. Selecione recursos do Azure.
3. Selecione o recurso para o qual você deseja exibir o histórico de auditoria.
4. Selecione minha auditoria.
5. Filtre o histórico usando uma data predefinida ou um intervalo personalizado.

| Time span  | Audit type | Subject type | Action                | Resource Name | Primary Target                                    | Subject      | Subject Type                      | Status |        |   |
|------------|------------|--------------|-----------------------|---------------|---|--------------|-----------------------------------|--------|--------|---|
| Last day   | All        | All          | 4/4/2019, 2:31:29 PM  | Shaun         | Add eligible member to role in PIM completed      | Wingtip Toys | Automation Operator               | Shaun  | Member | ✓ |
| Last day   | All        | All          | 4/4/2019, 2:31:29 PM  | Shaun         | Add eligible member to role in PIM requested      | Wingtip Toys | Automation Operator               | Shaun  | Member | ✓ |
| Last week  | All        | All          | 4/4/2019, 2:30:56 PM  | Shaun         | Remove member from role in PIM completed          | Wingtip Toys | Automation Operator               | Shaun  | Member | ✓ |
| Last month | All        | All          | 4/4/2019, 2:18:32 PM  | Shaun         | Remove eligible member from role in PIM completed | Wingtip Toys | Automation Operator               | Tom    | Member | ✓ |
| Custom     | All        | All          | 4/4/2019, 2:18:32 PM  | Shaun         | Add eligible member to role in PIM completed      | Wingtip Toys | Automation Operator               | Tom    | Member | ✓ |
| Custom     | All        | All          | 4/4/2019, 2:18:31 PM  | Shaun         | Add eligible member to role in PIM requested      | Wingtip Toys | Automation Operator               | Tom    | Member | ✓ |
| Custom     | All        | All          | 4/4/2019, 10:34:14 AM | Shaun         | Add eligible member to role in PIM requested      | Wingtip Toys | Billing Reader                    | Shaun  | Member | ✓ |
| Custom     | All        | All          | 4/4/2019, 10:31:08 AM | Shaun         | Add member to role completed (PIM active...)      | Wingtip Toys | Owner                             | Shaun  | Member | ✓ |
| Custom     | All        | All          | 4/4/2019, 10:31:05 AM | Shaun         | Add member to role requested (PIM activation ex)  | Wingtip Toys | Owner                             | Shaun  | Member | ✓ |
| Custom     | All        | All          | 4/4/2019, 1:57:55 AM  | Shaun         | Remove member from role (PIM activation ex)       | Wingtip Toys | Owner                             | Shaun  | Member | ✓ |
| Custom     | All        | All          | 4/3/2019, 6:01:52 PM  | Shaun         | Add eligible member to role in PIM completed      | Wingtip Toys | EventGrid EventSubscription Co... | Shaun  | Member | ✓ |
| Custom     | All        | All          | 4/3/2019, 6:01:52 PM  | Shaun         | Add eligible member to role in PIM requested      | Wingtip Toys | EventGrid EventSubscription Co... | Shaun  | Member | ✓ |
| Custom     | All        | All          | 4/3/2019, 5:59:56 PM  | Shaun         | Add eligible member to role in PIM completed      | Wingtip Toys | EventGrid EventSubscription Co... | -      | Member | ✓ |
| Custom     | All        | All          | 4/3/2019, 5:59:54 PM  | Shaun         | Add eligible member to role in PIM requested      | Wingtip Toys | EventGrid EventSubscription Co... | -      | Member | ✓ |
| Custom     | All        | All          | 4/3/2019, 5:58:56 PM  | Shaun         | Update role setting in PIM                        | Wingtip Toys | EventGrid EventSubscription Co... | -      | -      | ✓ |

#### NOTE

O acesso ao histórico de auditoria requer uma função de administrador global ou de administrador de função privilegiada.

## Obter motivo, Aprovador e número do tíquete para eventos de aprovação

- Entre no [portal do Azure](#) com permissões de função de administrador de função com privilégios e abra o Azure AD.
- Selecione **Logs de Auditoria**.
- Use o filtro de **serviço** para exibir apenas eventos de auditoria para o serviço Privileged Identity Management. Na página **logs de auditoria**, você pode:
  - Consulte o motivo de um evento de auditoria na coluna **razão do status**.
  - Consulte o aprovador na coluna **iniciado por (ator)** do evento "Adicionar membro à solicitação de função aprovada".

The screenshot shows the Azure Active Directory Audit logs interface. The left sidebar has a tree view with sections like App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Notifications settings, Security, Monitoring, Sign-ins, Audit logs (selected), Provisioning logs (Preview), Logs, Diagnostic settings, Workbooks, Usage & insights, Troubleshooting + Support, and New support request. The main area displays a table of audit logs. The columns are Date, Service, Category, Activity, Status, Status reason, and Target(s). A red box highlights the 'Service' column header and the first event row, which is for PIM activation.

4. Selecione um evento de log de auditoria para ver o número do tiquete na guia **atividade** do painel de **detalhes**.

The screenshot shows the detailed view of an audit log entry. The left sidebar is identical to the previous screenshot. The main area shows a table of audit logs with a red box highlighting the 'Details' tab. Under 'Details', there are tabs for 'Activity', 'Target(s)', and 'Modified Properties'. The 'Activity' tab shows information like DATE (1/3/2020, 10:27:59 AM), ACTIVITY TYPE (Add member to role completed (PIM activation)), and STATUS (Success). The 'Modified Properties' tab shows INITIATED BY (ACTOR) and ADDITIONAL DETAILS. A red box highlights the 'TicketSystem' and 'TicketNumber' fields under 'Modified Properties'.

5. Você pode exibir o solicitante (pessoa ativando a função) na guia **destinos** do painel de **detalhes** para um evento de auditoria. Há três tipos de destino para as funções de recurso do Azure:

- A função (**Type** = Role)
- O solicitante (**tipo** = outro)
- O aprovador (**tipo** = usuário)

The screenshot shows the FIMDEV - Audit logs interface. On the left, there's a navigation sidebar with various options like Overview, Getting started, Diagnose and solve problems, Manage (Users, Groups, Organizational relationships, Roles and administrators, Enterprise application, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Notifications settings, Security, Monitoring), and Monitoring.

The main area displays a table of audit logs. The table has columns: Date, Service, Category, Activity, Status, Status reason, Target(s), and Initiated by (actor). The table shows several entries, with one specific entry highlighted by a red box. This highlighted entry details an 'Add member to role request approved (PIM activation)' event. The 'TARGET' section of this entry is also highlighted with a red box, showing 'TYPE: Role', 'ID: fc8eb205-c0c4-4b5c-a3e4-04cbd6a48bf6', and 'DISPLAY NAME: Teams Service Administrator'. Below this, another row in the table is also highlighted with a red box, showing 'TARGET: TYPE: Other' and 'ID: 74487eb5-1630-4fa8-9581-0bb076ea5de'.

Normalmente, o evento de log imediatamente acima do evento de aprovação é um evento para "Adicionar membro à função concluído", onde o iniciado por (ator) é o solicitante. Na maioria dos casos, você não precisará localizar o solicitante na solicitação de aprovação de uma perspectiva de auditoria.

## Próximas etapas

- Atribuir funções de recurso do Azure no Privileged Identity Management
- Aprovar ou negar solicitações para funções de recurso do Azure no Privileged Identity Management
- Exibir histórico de auditoria para funções do Azure AD no Privileged Identity Management

# Usar funções personalizadas para recursos do Azure no Privileged Identity Management

22/07/2020 • 2 minutes to read • [Edit Online](#)

Talvez seja necessário aplicar configurações de PIM (Privileged Identity Management estrita) a alguns usuários em uma função privilegiada em sua organização do Azure Active Directory (Azure AD), fornecendo, ao mesmo tempo, autonomia maior para outras pessoas. Considere, por exemplo, um cenário em que sua organização contrata vários associados de contrato para auxiliar no desenvolvimento de um aplicativo que será executado em uma assinatura do Azure.

Como administrador de recursos, você quer que os funcionários sejam qualificados para o acesso sem a necessidade de aprovação. No entanto, todos os colaboradores contratados devem ser aprovados quando solicitam acesso aos recursos da organização.

Siga as etapas descritas na próxima seção para definir as configurações de Privileged Identity Management direcionadas para funções de recurso do Azure.

## Criar a função personalizada

Para criar uma função personalizada para um recurso, siga as etapas descritas em [Criar funções personalizadas para o Controle de Acesso Baseado em Função do Azure](#).

Ao criar uma função personalizada, inclua um nome descritivo para que você possa facilmente se lembrar de qual função interna você pretende duplicar.

### NOTE

Certifique-se de que a função personalizada seja uma duplicação da função interna que você quer duplicar e que seu escopo corresponda à função interna.

## Aplicar configurações de PIM

Depois que a função for criada em sua organização do Azure AD, vá para a página **Privileged Identity Management-recursos do Azure** no portal do Azure. Selecione o recurso ao qual a função se aplica.

| RESOURCE     | RESOURCE TYPE | ROLE | MEMBER |
|--------------|---------------|------|--------|
| Wingtip Toys | Subscription  | 116  | 160    |

Defina Privileged Identity Management configurações de função que devem ser aplicadas a esses membros da função.

Por fim, atribua funções ao grupo distinto de membros que você deseja ter como destino com essas configurações.

## Próximas etapas

- Definir configurações de função de recurso do Azure no Privileged Identity Management
- Funções personalizadas no Azure

# Solucionar um problema com Privileged Identity Management

22/07/2020 • 2 minutes to read • [Edit Online](#)

Você está tendo um problema com Privileged Identity Management (PIM) no Azure Active Directory (Azure AD)? As informações a seguir podem ajudá-lo a fazer as coisas funcionarem novamente.

## Acesso aos recursos do Azure negado

### Problema

Como proprietário ativo ou administrador de acesso do usuário para um recurso do Azure, você pode ver seu recurso dentro de Privileged Identity Management, mas não pode executar ações como fazer uma atribuição qualificada ou exibir uma lista de atribuições de função na página Visão geral do recurso. Qualquer uma dessas ações resulta em um erro de autorização.

### Causa

Esse problema pode ocorrer quando a função Administrador de acesso do usuário para a entidade de serviço PIM foi acidentalmente removida da assinatura. Para que o serviço de Privileged Identity Management seja capaz de acessar recursos do Azure, a entidade de serviço do MS-PIM sempre deve ter atribuído a [função de administrador de acesso do usuário](#) pela assinatura do Azure.

### Resolução

Atribua a função de administrador de acesso do usuário ao nome da entidade de serviço do Privileged Identity Management (MS – PIM) no nível da assinatura. Essa atribuição deve permitir que o serviço Privileged Identity Management acesse os recursos do Azure. A função pode ser atribuída em um nível de grupo de gerenciamento ou no nível de assinatura, dependendo de seus requisitos. Para obter mais informações sobre entidades de serviço, consulte [atribuir um aplicativo a uma função](#).

## Próximas etapas

- [Requisitos de licença para usar o Privileged Identity Management](#)
- [Protegendo o acesso privilegiado para implantações de nuvem e híbridos no Azure AD](#)
- [Implantar o Privileged Identity Management](#)

# Criar uma revisão de acesso das funções do Azure AD no Privileged Identity Management

22/07/2020 • 10 minutes to read • [Edit Online](#)

Para reduzir o risco associado a atribuições de função obsoletas, você deve examinar o acesso regularmente. Você pode usar o Azure AD Privileged Identity Management (PIM) para criar revisões de acesso para funções privilegiadas do Azure AD. Você também pode configurar revisões de acesso recorrentes que ocorrem automaticamente.

Este artigo descreve como criar uma ou mais revisões de acesso para funções privilegiadas do Azure AD.

## Pré-requisitos

[Administrador de Função com Privilégios](#)

## Abrir revisões de acesso

1. Entre no [portal do Azure](#) com um usuário que seja membro da função de administrador de função com privilégios.
2. Abra Azure ad Privileged Identity Management.
3. Selecione **funções do Azure ad**.
4. Em gerenciar, selecione **revisões de acesso**, em seguida, selecione **novo**.

The screenshot shows the 'Create an access review' page in the Microsoft Azure (Preview) portal. The URL in the address bar is highlighted with a red box: 'Home > Microsoft | Access reviews > Create an access review'. The page contains fields for 'Review name' (mandatory), 'Description', 'Start date' (set to 04/24/2020), 'Frequency' (set to 'One time'), 'Duration (in days)' (set to 1), 'End' (set to 'Never'), 'Number of times' (set to 0), 'End date' (set to 05/24/2020), 'Users' (set to 'Everyone'), and 'Scope' (set to 'Everyone'). Below these fields is a section for 'Review role membership' with a 'Select privileged role(s)' link. At the bottom left is a 'Start' button, which is also highlighted with a red box.

## Criar uma ou mais revisões de acesso

1. Clique em **Novo** para criar uma revisão de acesso.
2. Nomeie a revisão de acesso. Opcionalmente, forneça uma descrição à revisão. O nome e a descrição são mostrados aos revisores.

**Create an access review**

Access reviews allow reviewers to attest to whether users still need to be in a role. [Learn more about access reviews here.](#)

|               |  |   |
|---------------|--|---|
| * Review name | Role review for May                    | ✓ |
| Description ⓘ | Review access for all privileged roles | ✓ |

3. Defina a **Data de início**. Por padrão, uma revisão de acesso ocorre uma vez, inicia na mesma hora em que é criada e termina em um mês. Você pode alterar as datas de início e de término para iniciar uma análise de acesso em uma data futura e que dure quantos dias você desejar.

|                      |            |                    |
|----------------------|------------|--------------------|
| * Start date         | 2019-04-27 | 📅                  |
| Frequency            | One time   | ▼                  |
| Duration (in days) ⓘ | 1          | 🕒                  |
| End ⓘ                | Never      | End by Occurrences |
| * Number of times    | 0          |                    |
| * End date           | 2019-05-27 | 📅                  |

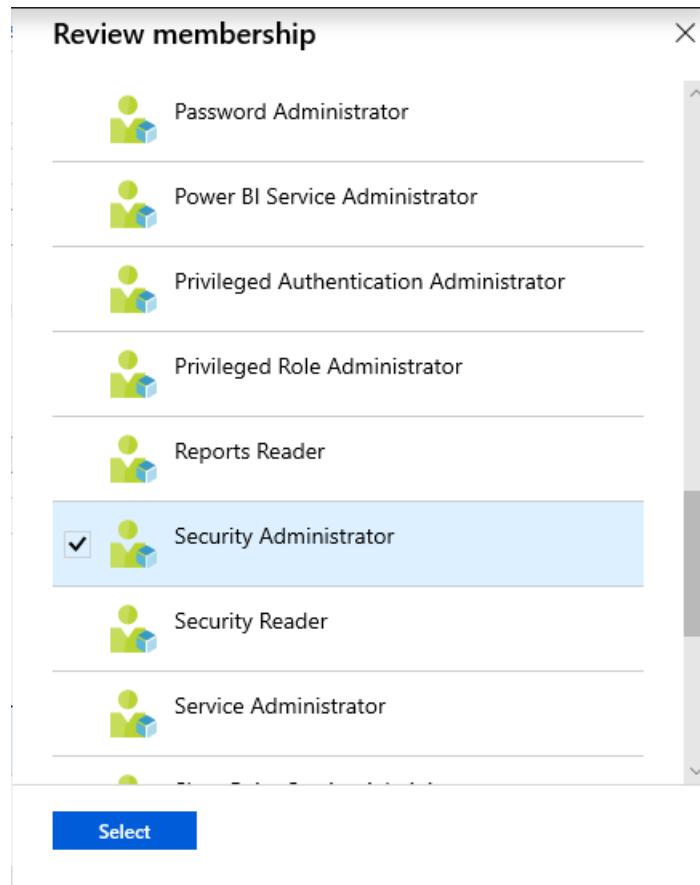
4. Para fazer com que a revisão de acesso seja recorrente, altere a configuração **Frequência** de **Uma vez** para **Semanal, Mensal, Trimestral, Anual ou Semestral**. Use o controle deslizante **Duração** ou caixa de texto para definir por quantos dias cada revisão da série recorrente será aberta para entrada de revisores. Por exemplo, a duração máxima que você pode definir para uma revisão mensal é de 27 dias, para evitar revisões sobrepostas.
5. Use a configuração **Final** para especificar como terminar a série de revisão de acesso recorrente. A série pode terminar de três maneiras: ela é executada continuamente para iniciar revisões indefinidamente, até uma data específica ou após a conclusão de um número definido de ocorrências. Você, outro usuário administrador ou outro administrador global pode interromper a série após a criação, alterando a data em **Configurações** para que ela encerre nessa data.
6. Na seção **Usuários**, selecione uma ou mais funções das quais você deseja examinar a associação.

|                           |          |
|---------------------------|----------|
| <b>Users</b>              |          |
| Scope                     | Everyone |
| <hr/>                     |          |
| * Review role membership  | >        |
| Select privileged role(s) |          |

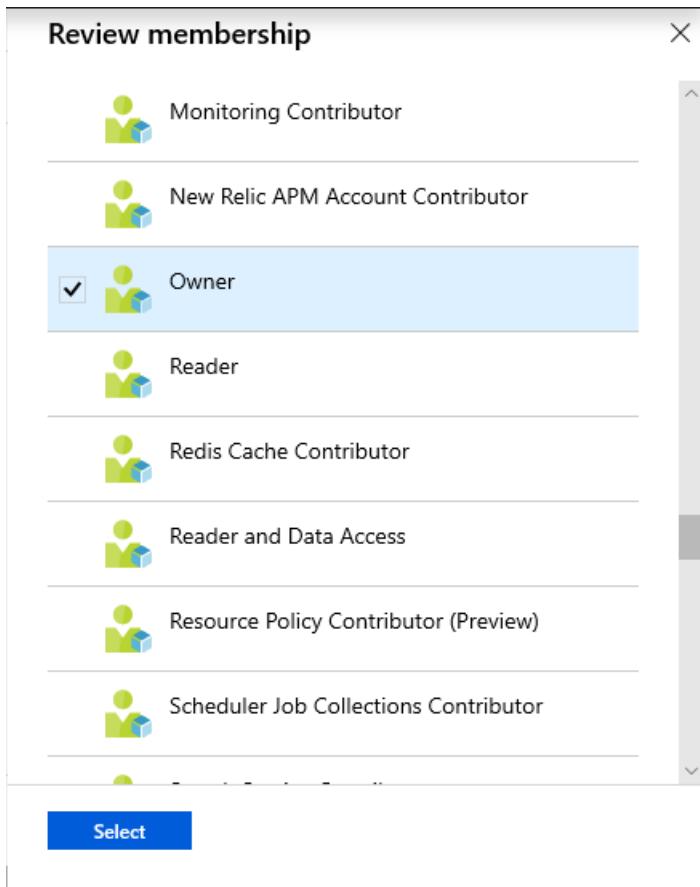
**NOTE**

- As funções selecionadas aqui incluem [funções permanentes e qualificadas](#).
- A seleção de mais de uma função criará várias revisões de acesso. Por exemplo, a seleção de cinco funções criará cinco revisões de acesso separadas.

Se você estiver criando uma revisão de acesso de **funções do Azure AD**, a imagem a seguir mostra um exemplo da lista Examinar associação.



Se você estiver criando uma revisão de acesso de **funções de recurso do Azure**, a imagem a seguir mostra um exemplo da lista Examinar associação.



7. Na seção **Revisores**, selecione uma ou mais pessoas para examinar todos os usuários no escopo. Ou você pode selecionar para que os membros examinem seus próprios acessos.

A screenshot of a "Reviewers" configuration section. It shows a dropdown menu with two options: "Selected users" and "Members (self)". Below the dropdown, a note states "0 users selected".

- **Usuários selecionados** – Use essa opção quando você não souber quem precisa de acesso. Com essa opção, você pode atribuir a revisão a um proprietário de recurso ou ao gerente do grupo para conclusão.
- **Membros (próprio)** – Use essa opção para fazer com que os usuários examinem suas próprias atribuições de função.

#### Após configurações de conclusão

1. Para especificar o que acontece após a conclusão de uma revisão, expanda a seção **Após configurações de conclusão**.

Upon completion settings

Auto apply results to resource [Enable](#) [Disable](#)

Should reviewer not respond [?](#)

- No change
- Remove access
- Approve access
- Take recommendations

[Start](#)

2. Se você quiser remover automaticamente o acesso para usuários que foram negados, defina **Resultados de aplicação automática ao recurso** para **Habilitar**. Se você deseja aplicar manualmente os resultados quando a revisão for concluída, defina a opção para **Desabilitar**.
3. Use a lista **Se o revisor não responder** para especificar o que acontece para usuários que não foram examinados pelo revisor dentro do período de revisão. Essa configuração não afeta os usuários que foram revisados pelos revisores manualmente. Se a decisão do revisor final for negar o acesso do usuário será removido.
  - **Nenhuma alteração** - deixar o acesso do usuário inalterado
  - **Remover o acesso** - remover o acesso do usuário
  - **Aprovar o acesso** - aprovar o acesso do usuário
  - **Fazer recomendações** - levar a recomendação do sistema ao negar ou aprovar o acesso contínuo do usuário

## Configurações avançadas

1. Para especificar configurações adicionais, expanda a seção **Configurações avançadas**.

Advanced settings

Show recommendations [?](#) [Enable](#) [Disable](#)

Require reason on approval [?](#) [Enable](#) [Disable](#)

Mail notifications [?](#) [Enable](#) [Disable](#)

Reminders [?](#) [Enable](#) [Disable](#)

[Start](#)

2. Definir **Mostrar recomendações** à **Habilitar** para mostrar aos revisores as recomendações do sistema com base nas informações de acesso do usuário.
3. Definir **Requer motivo sob aprovação** para **Habilitar** para exigir que o revisor forneça um motivo para aprovação.
4. Definir **Notificações por email** para **Habilitar** para que o Azure Active Directory envie notificações por email para os revisores quando uma revisão de acesso começar e para os administradores quando uma revisão terminar.
5. Defina **Lembretes** para **Habilitar** para que o Azure Active Directory envie lembretes de análises de acesso em andamento para os revisores que não concluíram a sua análise.

## Inicie a revisão de acesso

Depois de especificar as configurações para uma revisão de acesso, selecione **Iniciar**. A revisão de acesso será exibida na sua lista com um indicador de seu status.

The screenshot shows the 'Access reviews for Azure AD directory roles' section. It includes a search bar and a table with columns: ROLE, OWNER, START DATE, END DATE, and STATUS. Two rows are listed:

| ROLE                   | OWNER | START DATE | END DATE  | STATUS |
|------------------------|-------|------------|-----------|--------|
| User Administrator     | Admin | 4/27/2019  | 5/27/2019 | Active |
| Security Administrator | Admin | 4/27/2019  | 5/27/2019 | Active |

Por padrão, o Azure AD envia um email para os revisores logo após o início da análise. Se você optar pelo não envio do email pelo Azure AD, certifique-se de informar aos revisores que eles devem concluir uma análise de acesso pendente. Você pode mostrar as instruções sobre como [revisar o acesso às funções do Azure ad](#).

## Gerenciar a análise de acesso

Você pode acompanhar o progresso à medida que os revisores concluírem suas revisões na página [visão geral](#) da revisão de acesso. Nenhum direito de acesso é alterado no diretório até que a [revisão seja concluída](#).

The screenshot shows the 'Role review for May' page. On the left, there's a sidebar with sections for Overview, Current (Results, Reviewers, Settings), and Series (Reviewers, Settings, Scheduled review, Review history). The main area displays review details and a summary chart.

**Role review for May**

**Overview**

**Current**

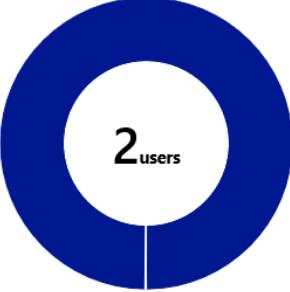
**Series**

**Role review for May**

**Delete series**

|                           |   |                        |                    |   |  |
|---------------------------|---|------------------------|--------------------|---|--|
| Owner                     | : | Admin                  | Scope              | : | Everyone                                     |
| Role                      | : | Security Administrator | Review status      | : | Active                                       |
| Require reason on appr... | : | true                   | Selected reviewers | : | Selected users                               |
| Access review period      | : | 4/27/2019 - 5/27/2019  | Description        | : | Review access to security administrator role |
| Remaining                 | : | NA                     | Recurrence type    | : | Monthly                                      |

**Current**



| Status       | Count |
|--------------|-------|
| Not reviewed | 2     |
| Approved     | 0     |
| Denied       | 0     |
| Don't know   | 0     |

Se esta for uma revisão única, depois que o período de revisão de acesso for concluído ou o administrador parar a revisão de acesso, siga as etapas em [concluir uma revisão de acesso das funções do Azure ad](#) para ver e aplicar os resultados.

Para gerenciar uma série de revisões de acesso, navegue até a revisão de acesso e você encontrará ocorrências

futuras nas revisões agendadas e edite a data de término ou adicione/remova revisores adequadamente.

Com base em suas seleções nas **configurações de conclusão**, a aplicação automática será executada após a data de término da revisão ou quando você interromper manualmente a revisão. O status da revisão será alterado de **concluído** por meio de Estados intermediários, como **aplicar** e, por fim, o estado **aplicado**. Você deve esperar que os usuários negados, se houver, sejam removidos das funções em alguns minutos.

## Próximas etapas

- [Examinar o acesso às funções do Azure AD](#)
- [Concluir uma revisão de acesso das funções do Azure AD](#)
- [Criar uma revisão de acesso das funções de recurso do Azure](#)

# Examinar o acesso às funções do Azure AD no Privileged Identity Management

22/07/2020 • 3 minutes to read • [Edit Online](#)

O Privileged Identity Management (PIM) simplifica o modo como as empresas gerenciam o acesso privilegiado a recursos no Azure Active Directory (AD) e outros serviços online da Microsoft, como o Office 365 ou Microsoft Intune. Siga as etapas neste artigo para revisar com êxito as funções atribuídas.

Se você for atribuído a uma função administrativa, o administrador de função com privilégios de sua organização poderá solicitar que você confirme regularmente que ainda precisa da função para seu trabalho. Você pode receber um email que inclui um link ou pode ir diretamente para a [portal do Azure](#) e começar.

Se você for um administrador com privilégios de função ou um administrador global interessado em revisões de acesso, obtenha mais detalhes em [Como iniciar uma revisão de acesso](#).

## Adicionar um bloco do painel PIM

Se você não tiver o serviço Privileged Identity Management fixado ao seu painel no seu portal do Azure, siga estas etapas para começar.

1. Entre no [portal do Azure](#).
2. Selecione seu nome de usuário no canto superior direito do portal do Azure e selecione a organização do Azure AD na qual você estará operando.
3. Selecione **Todos os serviços** e use a caixa de texto Filtrar para pesquisar o **Azure AD Privileged Identity Management**.
4. Marque **Fixar no painel** e então clique em **Criar**. O aplicativo Privileged Identity Management será aberto.

## Aprovar ou negar acesso

Ao aprovar ou negar o acesso, você está apenas dizendo ao revisor se ainda usa essa função ou não. Escolha **Aprovar** se você quiser manter a função ou **Negar** se não precisar mais do acesso. Seu status não mudará imediatamente até que o revisor aplique os resultados. Siga estas etapas para localizar e concluir a análise de acesso:

1. No serviço Privileged Identity Management, selecione **revisar acesso privilegiado**. Se você tiver quaisquer revisões de acesso pendentes, elas aparecerão na página de **revisões de acesso** do Azure AD.
2. Selecione a análise que deseja concluir.
3. A menos que tenha criado a análise, você aparece como o único usuário na análise. Selecione a marca de seleção ao lado de seu nome.
4. Escolha **Aprovar** ou **Negar**. Talvez seja necessário incluir um motivo para a sua decisão na caixa de texto **Fornecer um motivo**.
5. Feche a folha **Funções de análise do AD do Azure**.

## Próximas etapas

- [Realizar uma revisão de acesso das minhas funções de recurso do Azure no PIM](#)

# Concluir uma revisão de acesso das funções do Azure AD no Privileged Identity Management

22/07/2020 • 3 minutes to read • [Edit Online](#)

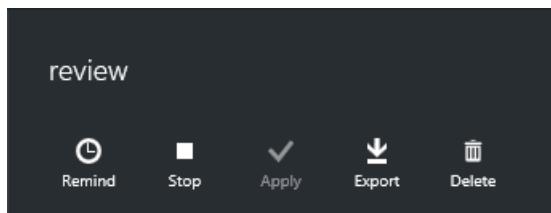
Os administradores de função com privilégios podem examinar o acesso privilegiado quando uma [revisão de acesso tiver sido iniciada](#). Privileged Identity Management (PIM) enviará automaticamente um email aos usuários em sua organização do Azure Active Directory (Azure AD) solicitando que eles revisem seu acesso. Se um usuário não tiver recebido um email, você poderá enviar para ele as instruções sobre [como executar uma revisão de acesso](#).

Depois do fim do período da revisão de acesso, ou quando todos os usuários tiverem terminado a autorrevisão, siga as etapas neste artigo para gerenciar a revisão e ver os resultados.

## Gerenciar revisões de acesso

1. Vá para a [portal do Azure](#) e selecione o serviço de **Azure ad Privileged Identity Management** em seu painel.
2. Clique na seção **Revisões de acesso** do painel.
3. Selecione a análise de acesso que você deseja gerenciar.

Na folha de detalhes da revisão de acesso, há várias opções para gerenciar essa revisão.



### Lembrar

Se uma análise de acesso é configurada para que os usuários examinem a si mesmos, o botão **Lembrar** envia uma notificação.

### Stop

Todas as revisões de acesso têm uma data de término, mas você pode usar o botão **Parar** para concluí-las mais cedo. Se quaisquer usuários ainda não tiverem sido examinados até este momento, eles não poderão ser após você parar a análise. Não é possível reiniciar uma análise após ela ter sido interrompida.

### Aplicar

Após uma análise de acesso ser concluída, seja porque você atingiu a data de término ou a interrompeu manualmente, o botão **Aplicar** implementa o resultado da análise. Se o acesso de um usuário foi negado na análise, esta é a etapa que removerá sua atribuição de função.

### Exportação

Se você quiser aplicar os resultados da revisão de acesso manualmente, poderá exportar a revisão. O botão **Exportar** começará a baixar um arquivo CSV. Você pode gerenciar os resultados no Excel ou em outros programas que abrem arquivos CSV.

### Excluir

Se você não estiver mais interessado na revisão, exclua-a. O botão **excluir** remove a revisão do serviço de

**IMPORTANT**

Não será necessário confirmar essa alteração destrutiva, portanto, verifique se você deseja excluir essa revisão.

## Próximas etapas

- [Iniciar uma revisão de acesso para as funções do Azure AD no Privileged Identity Management](#)
- [Executar uma revisão de acesso das minhas funções do Azure AD no Privileged Identity Management](#)

# Criar uma revisão de acesso das funções de recurso do Azure no Privileged Identity Management

22/07/2020 • 10 minutes to read • [Edit Online](#)

O acesso a funções privilegiadas de recursos do Azure para funcionários muda ao longo do tempo. Para reduzir o risco associado a atribuições de função obsoletas, você deve examinar o acesso regularmente. Você pode usar o Azure Active Directory (Azure AD) Privileged Identity Management (PIM) para criar revisões de acesso para funções de recursos do Azure com privilégios. Você também pode configurar revisões de acesso recorrentes que ocorrem automaticamente.

Este artigo descreve como criar uma ou mais revisões de acesso para funções privilegiadas de recursos do Azure.

## Pré-requisitos

[Administrador de Função com Privilégios](#)

## Abrir revisões de acesso

1. Entre no [portal do Azure](#) com um usuário que seja membro da função Administrador de Funções com Privilégios.
2. Abra [Azure ad Privileged Identity Management](#).
3. No menu à esquerda, selecione **recursos do Azure**.
4. Selecione o recurso que você deseja gerenciar, como uma assinatura ou grupo de gerenciamento.
5. Em gerenciar, selecione **revisões de acesso**.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a dark theme with various service icons. The main content area is titled 'Pay-As-You-Go - Access reviews'. On the left, there's a navigation pane with 'Overview', 'Tasks' (containing 'My roles', 'Pending requests', 'Approve requests', and 'Review access'), 'Manage' (containing 'Roles', 'Members', 'Alerts', and 'Access reviews' which is highlighted), and 'Role settings' and 'Activity'. The main right panel is titled 'Access reviews for Azure resource roles' and contains a table header with columns 'ROLE', 'OWNER', and 'START DATE'. Below the table, a message says 'No access reviews to display. Click 'New' above to create a new review'.

## Criar uma ou mais revisões de acesso

1. Clique em **Novo** para criar uma revisão de acesso.
2. Nomeie a revisão de acesso. Opcionalmente, forneça uma descrição à revisão. O nome e a descrição são mostrados aos revisores.

**Create an access review**

Access reviews allow reviewers to attest to whether users still need to be in a role. [Learn more about access reviews here.](#)

|               |  |   |
|---------------|--|---|
| * Review name | Role review for May                    | ✓ |
| Description   | Review access for all privileged roles | ✓ |

3. Defina a **Data de início**. Por padrão, uma revisão de acesso ocorre uma vez, inicia na mesma hora em que é criada e termina em um mês. Você pode alterar as datas de início e de término para iniciar uma análise de acesso em uma data futura e que dure quantos dias você desejar.

|                    |            |                    |
|--------------------|------------|--------------------|
| * Start date       | 2019-04-27 | 📅                  |
| Frequency          | One time   | ▼                  |
| Duration (in days) | 1          | 🕒                  |
| End                | Never      | End by Occurrences |
| * Number of times  | 0          |                    |
| * End date         | 2019-05-27 | 📅                  |

4. Para fazer com que a revisão de acesso seja recorrente, altere a configuração **Frequência de Uma vez para Semanal, Mensal, Trimestral, Anual ou Semestral**. Use o controle deslizante **Duração** ou caixa de texto para definir por quantos dias cada revisão da série recorrente será aberta para entrada de revisores. Por exemplo, a duração máxima que você pode definir para uma revisão mensal é de 27 dias, para evitar revisões sobrepostas.
5. Use a configuração **Final** para especificar como terminar a série de revisão de acesso recorrente. A série pode terminar de três maneiras: ela é executada continuamente para iniciar revisões indefinidamente, até uma data específica ou após a conclusão de um número definido de ocorrências. Você, outro usuário administrador ou outro administrador global pode interromper a série após a criação, alterando a data em **Configurações** para que ela encerre nessa data.
6. Na seção **Usuários**, selecione uma ou mais funções das quais você deseja examinar a associação.

**Users**

Scope  Everyone

---

\* Review role membership >  
Select privileged role(s)

**NOTE**

- As funções selecionadas aqui incluem [funções permanentes e qualificadas](#).
- A seleção de mais de uma função criará várias revisões de acesso. Por exemplo, a seleção de cinco funções criará cinco revisões de acesso separadas.

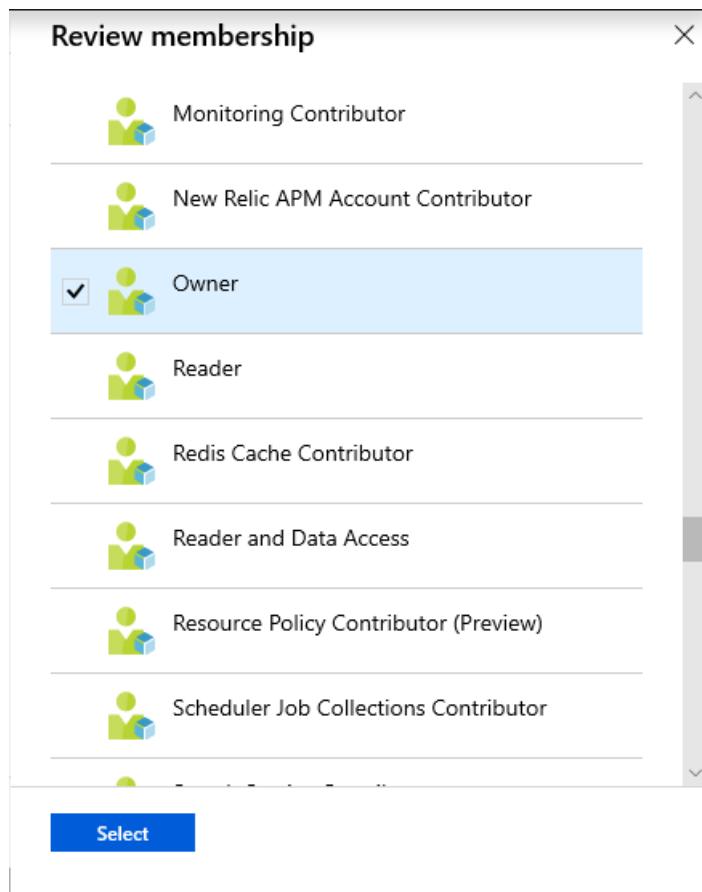
Se você estiver criando uma revisão de acesso de **funções do Azure AD**, a imagem a seguir mostra um exemplo da lista Examinar associação.

The screenshot shows a modal window titled "Review membership". It lists several Azure AD roles, each with a small green user icon. The "Security Administrator" role is selected, indicated by a checked checkbox to its left and a blue background. Other roles listed include "Password Administrator", "Power BI Service Administrator", "Privileged Authentication Administrator", "Privileged Role Administrator", "Reports Reader", "Security Reader", and "Service Administrator". At the bottom of the list is a "Select" button.

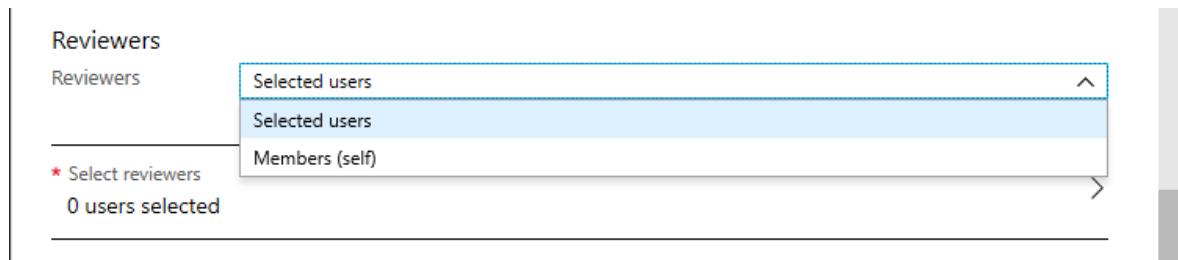
| Role   |
|--|
| Password Administrator                                     |
| Power BI Service Administrator                             |
| Privileged Authentication Administrator                    |
| Privileged Role Administrator                              |
| Reports Reader   |
| <input checked="" type="checkbox"/> Security Administrator |
| Security Reader  |
| Service Administrator                                      |

Select

Se você estiver criando uma revisão de acesso de **funções de recurso do Azure**, a imagem a seguir mostra um exemplo da lista Examinar associação.



7. Na seção **Revisores**, selecione uma ou mais pessoas para examinar todos os usuários no escopo. Ou você pode selecionar para que os membros examinem seus próprios acessos.



- **Usuários selecionados** – Use essa opção quando você não souber quem precisa de acesso. Com essa opção, você pode atribuir a revisão a um proprietário de recurso ou ao gerente do grupo para conclusão.
- **Membros (próprio)** – Use essa opção para fazer com que os usuários examinem suas próprias atribuições de função.

#### Após configurações de conclusão

1. Para especificar o que acontece após a conclusão de uma revisão, expanda a seção **Após configurações de conclusão**.

The screenshot shows the 'Upon completion settings' section of a configuration interface. It includes a dropdown menu for 'Should reviewer not respond' with options: 'No change', 'Remove access', 'Approve access', and 'Take recommendations'. A 'Start' button is at the bottom.

2. Se você quiser remover automaticamente o acesso para usuários que foram negados, defina **Resultados de aplicação automática ao recurso** para **Habilitar**. Se você deseja aplicar manualmente os resultados quando a revisão for concluída, defina a opção para **Desabilitar**.
3. Use a lista **Se o revisor não responder** para especificar o que acontece para usuários que não foram examinados pelo revisor dentro do período de revisão. Essa configuração não afeta os usuários que foram revisados pelos revisores manualmente. Se a decisão do revisor final for negar o acesso do usuário será removido.
  - **Nenhuma alteração** - deixar o acesso do usuário inalterado
  - **Remover o acesso** - remover o acesso do usuário
  - **Aprovar o acesso** - aprovar o acesso do usuário
  - **Fazer recomendações** - levar a recomendação do sistema ao negar ou aprovar o acesso contínuo do usuário

### Configurações avançadas

1. Para especificar configurações adicionais, expanda a seção **Configurações avançadas**.

The screenshot shows the 'Advanced settings' section of a configuration interface. It includes four toggle buttons: 'Show recommendations' (Enable), 'Require reason on approval' (Enable), 'Mail notifications' (Enable), and 'Reminders' (Enable). A 'Start' button is at the bottom.

2. Definir **Mostrar recomendações** à **Habilitar** para mostrar aos revisores as recomendações do sistema com base nas informações de acesso do usuário.
3. Definir **Requer motivo sob aprovação** para **Habilitar** para exigir que o revisor forneça um motivo para aprovação.
4. Definir **Notificações por email** para **Habilitar** para que o Azure Active Directory envie notificações por email para os revisores quando uma revisão de acesso começar e para os administradores quando uma revisão terminar.
5. Defina **Lembretes** para **Habilitar** para que o Azure Active Directory envie lembretes de análises de

acesso em andamento para os revisores que não concluíram a sua análise.

## Inicie a revisão de acesso

Depois de especificar as configurações para uma revisão de acesso, clique em **Iniciar**. A revisão de acesso será exibida na sua lista com um indicador de seu status.

| ROLE  | OWNER | START DATE | END DATE  | STATUS |
|-------|-------|------------|-----------|--------|
| Owner | Admin | 4/29/2019  | 5/29/2019 | Active |

Por padrão, o Azure AD envia um email para os revisores logo após o início da análise. Se você optar pelo não envio do email pelo Azure AD, certifique-se de informar aos revisores que eles devem concluir uma análise de acesso pendente. Você pode mostrar as instruções sobre como [revisar o acesso às funções de recurso do Azure](#).

## Gerenciar a análise de acesso

Você pode acompanhar o progresso à medida que os revisores concluírem suas revisões na página **visão geral** da revisão de acesso. Nenhum direito de acesso é alterado no diretório até que a [revisão seja concluída](#).

|                            |   |                       |                    |   |                       |
|----------------------------|---|-----------------------|--------------------|---|-----------------------|
| Owner                      | : | Admin                 | Scope              | : | Everyone              |
| Role                       | : | Owner                 | Review status      | : | Active                |
| Require reason on approval | : | true                  | Selected reviewers | : | Selected users        |
| Access review period       | : | 4/29/2019 - 5/29/2019 | Description        | : | Review access for May |
| Remaining                  | : | 2                     | Recurrence type    | : | One time              |

Se esta for uma revisão única, depois que o período de revisão de acesso for concluído ou o administrador parar a revisão de acesso, siga as etapas em [concluir uma revisão de acesso das funções de recurso do Azure](#) para ver e aplicar os resultados.

Para gerenciar uma série de revisões de acesso, navegue até a revisão de acesso e você encontrará ocorrências futuras nas revisões agendadas e edite a data de término ou adicione/remova revisores adequadamente.

Com base em suas seleções nas **configurações de conclusão**, a aplicação automática será executada após a data de término da revisão ou quando você interromper manualmente a revisão. O status da revisão será alterado de **concluído** por meio de Estados intermediários, como **aplicar** e, por fim, o estado **aplicado**. Você deve esperar que os usuários negados, se houver, sejam removidos das funções em alguns minutos.

## Próximas etapas

- [Examinar o acesso às funções de recurso do Azure](#)
- [Concluir uma revisão de acesso das funções de recurso do Azure](#)
- [Criar uma revisão de acesso das funções do Azure AD](#)

# Examinar o acesso às funções de recurso do Azure no Privileged Identity Management

22/07/2020 • 2 minutes to read • [Edit Online](#)

As revisões de acesso do Privileged Identity Management (PIM) podem ajudar a proteger o acesso a funções com privilégios no Azure Active Directory (AD do Azure). Este artigo as etapas para concluir uma análise das atribuições de função com privilégios em uma revisão de acesso do Azure AD.

Se você estiver atribuído a uma função administrativa, talvez seja necessário concluir uma análise de acesso por seu administrador para confirmar a necessidade de uma função. A solicitação de confirmação pode vir um email que inclui um link ou você pode confirmar na [portal do Azure](#).

Se você for um administrador com privilégios de função interessado em revisões de acesso, obtenha mais detalhes em [Como iniciar uma revisão de acesso](#).

## Aprovar ou negar acesso

Você pode aprovar ou negar o acesso com base em se você ainda usa essa função ou não. Escolha **Aprovar** se você quiser manter a função ou **Negar** se não precisar mais do acesso. Seu status será alterado somente depois que o revisor aplicar os resultados.

Siga estas etapas para localizar e concluir a análise de acesso:

1. Entre no [portal do Azure](#).
2. Selecione **Azure Active Directory** e abra **Privileged Identity Management**.
3. Selecione **examinar acesso**.

| REVIEW NAME                 | ROLE  | SUBSCRIPTION | END DATE             | REMAINING ITEMS |
|-----------------------------|-------|--------------|----------------------|-----------------|
| 06_28 Recurring Review test | Owner | Wingtip Toys | 4/9/2019<br>5 day(s) | 1               |

4. Selecione a análise que deseja concluir.
5. Escolha **aprovar** ou **negar**. Na caixa **fornecer um motivo**, insira uma justificativa de negócios para sua decisão, se necessário.

Filter Group

## Essentials ^

|                              |                            |
|------------------------------|----------------------------|
| Owner                        | Role                       |
| Leon Dinh[ledinh@fimdev.net] | Reader                     |
| Subscription                 | Require reason on approval |
| Wingtip Toys - Prod          | false                      |
| Start date                   | End date                   |
| 3/19/2018                    | 4/18/2018                  |
| Description                  | Remaining                  |
| 123                          | 1                          |

Select the user(s) from the list, and approve or deny their role membership using the buttons below

Search

USER ↑ USER EMAIL ↑ REVIEW DATE ↑

## NOT REVIEWED

Hana Kim hanki@fimdev.net

\* Reason

Approve

Deny

Reset

## Próximas etapas

- Executar uma revisão de acesso das minhas funções do Azure AD no Privileged Identity Management

# Concluir uma revisão de acesso das funções de recurso do Azure no Privileged Identity Management

22/07/2020 • 3 minutes to read • [Edit Online](#)

Os administradores de função com privilégios podem revisar o acesso privilegiado depois de [iniciarem uma revisão de acesso](#). O Privileged Identity Management (PIM) no Azure Active Directory (Azure AD) envia automaticamente um email que solicita aos usuários que revisem seu acesso. Se um usuário não receber um email, você poderá enviar para ele as instruções de [como executar uma revisão de acesso](#).

Depois do fim do período da revisão de acesso, ou após todos os usuários terminarem a autorrevisão, siga as etapas neste artigo para gerenciar a revisão e ver os resultados.

## Gerenciar revisões de acesso

1. Vá para o [Portal do Azure](#). No painel, selecione o serviço **recursos do Azure**.
2. Selecione seu recurso.
3. Clique na seção **Revisões de acesso** do painel.

| ROLE                        | OWNER                       | START DATE | END DATE   | STATUS         |
|-----------------------------|-----------------------------|------------|------------|----------------|
| 04_02 OWNER ROLE REVIEW     | Owner                       | 4/2/2018   | 4/2/2018   | Result applied |
| 04_02 REVIEW                | Contributor                 | 4/2/2018   | 5/2/2018   | Result applied |
| 04_02 REVIEW                | Traffic Manager Contributor | 4/2/2018   | 4/2/2018   | Result applied |
| 04_06 REVIEW                | Owner                       | 4/6/2018   | 4/6/2018   | Result applied |
| 05_28 RECURRING REVIEW TEST | Owner                       | 6/28/2018  | 12/31/9999 | Active         |
| 1031                        | Reader                      | 10/31/2018 | 11/30/2018 | Initializing   |

4. Selecione a análise de acesso que você deseja gerenciar.

Na página de detalhes da revisão de acesso, há várias opções para gerenciar essa revisão. As opções são as descritas a seguir:



### Stop

Todas as revisões de acesso têm uma data de término. Selecione **parar** para concluir o início. Todos os usuários que não concluíram sua revisão neste momento não poderão concluir-lo depois que você parar a revisão. Não é possível reiniciar uma revisão após ela ter sido interrompida.

### Redefinir

Você pode redefinir uma revisão de acesso para remover todas as decisões feitas nela. Depois de redefinir uma revisão de acesso, todos os usuários serão marcados como não revisados novamente.

## Aplicar

Após a conclusão de uma revisão de acesso, selecione **aplicar** para implementar o resultado da revisão. Se o acesso de um usuário foi negado na análise, esta etapa remove sua atribuição de função.

## Excluir

Se você não estiver mais interessado na revisão, exclua-a. Selecione **excluir** Yo remover a revisão do serviço de Privileged Identity Management.

## Resultados

Na página **resultados**, exiba e Baixe uma lista de seus resultados de revisão.

The screenshot shows a table of results from a review. The columns are: USER, OUTCOME, REASON, REVIEWED BY, APPLIED BY, and APPLY RESULT. There are 10 rows, each representing a user with a blue profile icon. All users have an 'OUTCOME' of 'Not reviewed'. The 'REASON' column is empty. The 'APPLIED BY' and 'APPLY RESULT' columns are also empty. The 'REVIEWED BY' column shows the email addresses of the reviewers: aamora@fimdev.net, anujuser@fimdev.net, bhu@fimdev.net, danminert@fimdev.net, davidhou@fimdev.net, debabchoudhury@fimdev.net, dituma@fimdev.net, ericliu@fimdev.net, gauravmishra@fimdev.net, and gopi@fimdev.net. The bottom right corner of the table has a navigation bar with numbers 1, 2, 3, 4, <, and >.

## Revisores

Exiba e adicione revisores à sua revisão de acesso existente. Lembre os revisores de concluir suas revisões.

The screenshot shows a table of reviewers. The columns are: NAME and USER PRINCIPAL NAME. There is one row for 'Qi Cao' with the value 'qicao@fimdev.net' in both columns. The bottom right corner of the table has a navigation bar with numbers 1, 2, 3, 4, <, and >.

## Próximas etapas

- Iniciar uma revisão de acesso para funções de recurso do Azure no Privileged Identity Management
- Executar uma revisão de acesso das minhas funções de recurso do Azure no Privileged Identity Management

# Restrições e limites de serviço do AD do Azure

22/07/2020 • 9 minutes to read • [Edit Online](#)

Este artigo contém as restrições de uso e outros limites de serviço para o serviço Azure AD (Azure Active Directory). Se você estiver procurando o conjunto completo de limites de serviço do Microsoft Azure, veja [Assinatura do Azure e limites de serviços, cotas e restrições](#).

Aqui estão as restrições de uso e outros limites de serviço para o serviço Microsoft Azure Active Directory (Azure AD).

| CATEGORIA  | LIMITE  |
|------------|---|
| Diretórios | <p>Um único usuário pode pertencer a um máximo de 500 diretórios do Microsoft Azure Active Directory como um membro ou convidado.</p> <p>Um único usuário pode criar no máximo 200 diretórios.</p>  |
| Domínios   | <p>É possível adicionar no máximo 900 nomes de domínio gerenciados. Ao configurar todos os domínios para a federação com o Active Directory local, você poderá adicionar no máximo 450 nomes de domínio em cada diretório.</p>  |
| Recursos   | <ul style="list-style-type: none"><li>Um máximo de 50.000 recursos do Azure AD pode ser criado em um único diretório por usuários da edição gratuita do Azure Active Directory por padrão. Se você tiver pelo menos um domínio verificado, a cota de serviço do Azure AD padrão para sua organização será estendida para os recursos 300.000 do Azure AD. Esse limite de serviço não está relacionado ao limite do tipo de preço de 500.000 recursos na página de preços do Azure AD. Para ir além da cota padrão, você deve entrar em contato com Suporte da Microsoft.</li><li>Um usuário não administrador pode criar no máximo 250 recursos do Azure AD. Recursos ativos e excluídos que estão disponíveis para restaurar a contagem em direção a essa cota. Somente os recursos do Azure AD excluídos que foram excluídos há menos de 30 dias estão disponíveis para restauração. Recursos do Azure AD excluídos que não estão mais disponíveis para restaurar a contagem em direção a essa cota em um valor de um trimestre por 30 dias. Se você tiver os desenvolvedores que provavelmente excederão repetidamente essa cota no decorrer de suas tarefas regulares, você poderá <a href="#">criar e atribuir uma função personalizada</a> com permissão para criar um número ilimitado de registros de aplicativo.</li></ul> |

| CATEGORIA               | LIMITE  |
|-------------------------|---|
| Extensões de esquema    | <ul style="list-style-type: none"> <li>As extensões do tipo cadeia de caracteres podem ter no máximo 256 caracteres.</li> <li>As extensões do tipo binário são limitadas a 256 bytes.</li> <li>Somente os valores de extensão 100, em <i>todos os tipos e todos os</i> aplicativos, podem ser gravados em qualquer recurso único do AD do Azure.</li> <li>Somente as entidades Grupo, TenantDetail, Dispositivo, Aplicativo e ServicePrincipal podem ser estendidas com atributos de valor único do tipo cadeia de caracteres ou binário.</li> <li>As extensões de esquema estão disponíveis somente na API do Graph versão 1.21 – versão prévia. O aplicativo precisa obter acesso de gravação para registrar uma extensão.</li> </ul> |
| Aplicativos             | Um máximo de 100 usuários podem ser proprietários de um único aplicativo.   |
| Manifesto do aplicativo | Um máximo de 1200 entradas pode ser adicionado no manifesto do aplicativo.  |

| CATEGORIA           | LIMITE  |
|---------------------|---|
| Grupos              | <ul style="list-style-type: none"> <li>Um usuário pode criar no máximo 250 grupos em uma organização do Azure AD.</li> <li>Uma organização do Azure AD pode ter um máximo de 5000 grupos dinâmicos.</li> <li>Um máximo de 100 usuários podem ser proprietários de um único grupo.</li> <li>Qualquer número de recursos do AD do Azure pode ser membros de um único grupo.</li> <li>Um usuário pode ser um membro de qualquer número de grupos.</li> <li>O número de membros em um grupo que podem ser sincronizados do Active Directory local para o Azure Active Directory usando o Azure AD Connect é limitado a 50 mil membros.</li> <li>Não há suporte para grupos aninhados no Azure AD em todos os cenários</li> </ul> <p>Neste momento, os cenários com suporte com grupos aninhados são os seguintes.</p> <ul style="list-style-type: none"> <li>Um grupo pode ser adicionado como membro de outro grupo e você pode obter aninhamento de grupo.</li> <li>Declarações de associação de grupo (quando um aplicativo é configurado para receber declarações de associação de grupo no token, grupos aninhados ou o usuário conectado é um membro de estes estão incluídos)</li> <li>Acesso condicional (ao definir o escopo de uma política de acesso condicional para um grupo)</li> <li>Restringindo o acesso à redefinição de senha de autoatendimento</li> <li>Restringir quais usuários podem fazer o ingresso no Azure AD e o registro do dispositivo</li> </ul> <p>Os seguintes cenários não têm suporte para grupos aninhados:</p> <ul style="list-style-type: none"> <li>A atribuição de função de aplicativo (atribuindo grupos a um aplicativo tem suporte, mas os grupos aninhados dentro do grupo atribuído diretamente não terão acesso), tanto para acesso quanto para provisionamento</li> <li>Licenciamento baseado em grupo (atribuindo uma licença automaticamente a todos os membros de um grupo)</li> <li>Grupos do Office 365.</li> </ul> |
| Proxy do Aplicativo | <ul style="list-style-type: none"> <li>Um máximo de 500 de transações por segundo por aplicativo de proxy de aplicativo</li> <li>Um máximo de 750 de transações por segundo para a organização do Azure AD</li> </ul> <p>Uma transação é definida como uma única solicitação HTTP e uma resposta para um recurso exclusivo. Quando limitado, os clientes receberão uma resposta de 429 (muitas solicitações).</p>   |
| Painel de acesso    | Não há limite para o número de aplicativos que podem ser vistos no painel de acesso por usuário, independentemente das licenças atribuídas.   |

| CATEGORIA                             | LIMITE  |
|---------------------------------------|---|
| Relatórios                            | Um máximo de 1.000 linhas podem ser exibidas ou baixadas em qualquer relatório. Todos os dados adicionais serão truncados.  |
| Unidades administrativas              | Um recurso do Azure AD pode ser um membro de no máximo 30 unidades administrativas.   |
| Funções e permissões do administrador | <ul style="list-style-type: none"> <li>• Um grupo não pode ser adicionado como <a href="#">proprietário</a>.</li> <li>• Um grupo não pode ser atribuído a uma <a href="#">função</a>.</li> <li>• A capacidade dos usuários de ler informações de diretório de outros usuários não pode ser restrita fora do comutador de toda a organização do Azure AD para desabilitar o acesso de todos os usuários não administradores a todas as informações de diretório (não recomendado). Mais informações sobre as permissões padrão <a href="#">aqui</a>.</li> <li>• Pode levar até 15 minutos ou sair/entrar antes que as adições e as revogações de associação de função de administrador entrem em vigor.</li> </ul> |

## Próximas etapas

- [Inscrever-se no Azure como uma organização](#)
- [Como as assinaturas do Azure estão associadas ao Azure AD](#)