**Proteger o acesso aos seus aplicativos usando os serviços de identidade do Azure**

Saiba como o Azure Active Directory ajuda a gerenciar e proteger identidades. Além disso, veja como o logon único, a autenticação multifator e o Acesso Condicional permitem que os usuários acessem com segurança recursos e aplicativos na intranet e em redes públicas.

## Objetivos de aprendizagem

Depois de concluir este módulo, você poderá:

* Explicar a diferença entre autenticação e autorização.
* Descrever como o Azure Active Directory fornece gerenciamento de identidade e acesso.
* Explicar a função que o SSO (logon único), a autenticação multifator e o Acesso Condicional desempenham no gerenciamento da identidade do usuário.

# Comparar autenticação e autorização

Lembre-se de que a Tailwind Traders precisa garantir que somente os funcionários possam entrar em aplicativos de negócios e acessá-los.

A Tailwind Traders também precisa garantir que os funcionários possam acessar apenas os aplicativos autorizados. Por exemplo, todos os funcionários podem acessar o software de inventário e de preços, mas somente os gerentes de lojas podem acessar a folha de pagamento e determinados softwares de contabilidade.

Dois conceitos fundamentais que você precisa entender ao falar sobre identidade e acesso são autenticação (AuthN) e autorização (AuthZ).

A autenticação e a autorização dão suporte a todo o restante. Elas ocorrem em sequência no processo de identidade e acesso.

Vamos dar uma olhada rápida em cada uma.

## O que é a autenticação?

Autenticação é o processo de estabelecer a identidade de uma pessoa ou serviço que deseja acessar um recurso. Ela envolve o ato de solicitar credenciais legítimas de uma parte e fornece a base para criação de uma entidade de segurança para controle de acesso e identidade. Estabelece se o usuário é quem diz ser.

## O que é autorização?

A autenticação estabelece a identidade do usuário, enquanto a autorização é o processo de estabelecer o nível de acesso que uma pessoa ou um serviço autenticado tem. Especifica quais dados podem ser acessados e que a pessoa ou serviço pode fazer com eles.

## Como a autenticação e a autorização estão relacionadas?

Este é um diagrama que mostra a relação entre a autenticação e a autorização:



O cartão de identificação representa as credenciais de que o usuário precisa para provar a identidade dele. Você aprenderá mais sobre os tipos de credenciais mais adiante neste módulo. Após a autenticação, a autorização define quais tipos de aplicativos, recursos e dados podem ser acessados pelo usuário.

# O que é o Azure Active Directory?

Nesta parte, você saberá como o Azure AD (Azure Active Directory) fornece serviços de identidade que permitem que os usuários entrem e acessem aplicativos em nuvem da Microsoft e aplicativos de nuvem que você desenvolve. Você também saberá como o Azure AD dá suporte ao SSO (logon único).

A Tailwind Traders já usa o Active Directory para proteger os ambientes locais. A empresa não quer que seus usuários tenham nomes de usuário e senhas diferentes dos quais precisarão se lembrar para acessar aplicativos e dados na nuvem. Eles podem integrar a instância existente do Active Directory aos serviços de identidade na nuvem para criar uma experiência simplificada para os usuários?

Vamos começar comparando o Azure AD com o Active Directory.

## **Como o Azure AD se compara com Active Directory?**

O Active Directory está relacionado ao Azure AD, mas há algumas diferenças importantes.

A Microsoft introduziu o Active Directory no Windows 2000 para permitir às organizações gerenciar vários sistemas e componentes de infraestrutura local usando uma única identidade por usuário.

Para ambientes locais, o Active Directory em execução no Windows Server fornece um serviço de gerenciamento de identidade e acesso gerenciado pela própria organização. O Azure AD é o serviço de gerenciamento de acesso e identidade baseado em nuvem da Microsoft. Com o Azure AD, você controla as contas de identidade, mas a Microsoft garante que o serviço esteja disponível globalmente. Se você já trabalhou com o Active Directory, o Azure AD lhe será familiar.

Quando você protege identidades locais com o Active Directory, a Microsoft não monitora tentativas de conexão. Quando você conecta o Active Directory ao Azure AD, a Microsoft pode ajudar a protegê-lo detectando tentativas de conexão suspeitas sem custo adicional. Por exemplo, o Azure AD pode detectar tentativas de conexão de locais inesperados ou dispositivos desconhecidos.

## Quem usa o Azure AD?

O Azure AD é para:

* **Administradores de TI**

Os administradores podem usar o Azure AD para controlar o acesso a aplicativos e recursos com base em seus requisitos de negócios.

* **Desenvolvedores de aplicativos**

Os desenvolvedores podem usar o Azure AD para fornecer uma abordagem baseada em padrões para adicionar funcionalidade a aplicativos que eles criam, como adicionar a funcionalidade de SSO a um aplicativo ou habilitar um aplicativo para trabalhar com as credenciais existentes de um usuário.

* **Usuários**

Os usuários podem gerenciar suas identidades. Por exemplo, a redefinição de senha por autoatendimento permite que os usuários alterem ou redefinam a senha sem envolvimento de um administrador de TI nem do suporte técnico.

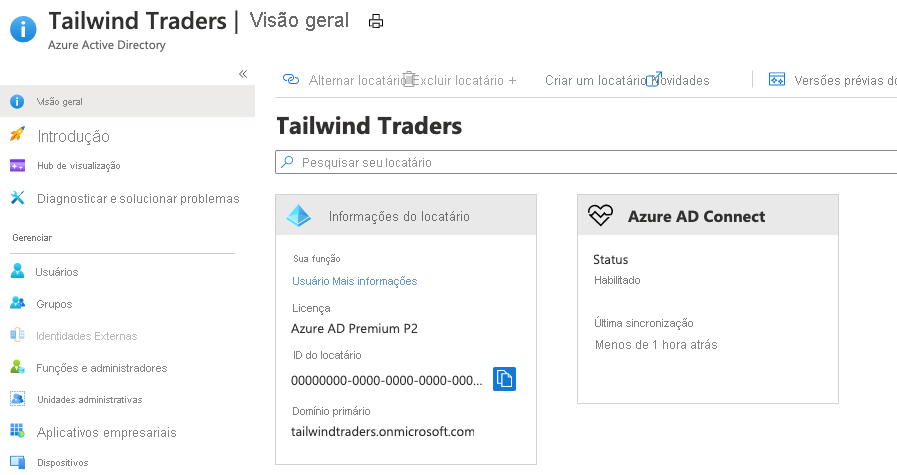
* **Assinantes do serviço online**

Os assinantes do Microsoft 365, do Microsoft Office 365, do Azure e do Microsoft Dynamics CRM Online já estão usando o Azure AD.

Um locatário é uma representação de uma organização. Normalmente, um locatário é separado de outros locatários e tem a própria identidade.

Cada locatário do Microsoft 365, do Office 365, do Azure e do Dynamics CRM Online é automaticamente um locatário do Azure AD.

Veja uma captura de tela mostrando o que um administrador de TI pode ver no portal do Azure ao trabalhar com o Active Directory:



## Que serviços o Azure AD fornece?

O Azure AD fornece serviços como:

* **Autenticação**

Inclui verificar a identidade para acessar aplicativos e recursos. Também inclui fornecer funcionalidades como redefinição de senha por autoatendimento, autenticação multifator, uma lista personalizada de senhas banidas e serviços de bloqueio inteligente.

* **Logon Único**

O SSO permite que você se lembre de apenas um nome de usuário e uma senha para acessar vários aplicativos. Uma única identidade é vinculada a um usuário, o que simplifica o modelo de segurança. À medida que os usuários trocam de funções ou saem de uma organização, as modificações de acesso são vinculadas àquela identidade, o que reduz consideravelmente o esforço necessário para alterar ou desabilitar contas.

* **Gerenciamento de aplicativos**

Você pode gerenciar seus aplicativos de nuvem e locais usando o Azure AD. Recursos como Proxy de Aplicativo, aplicativos SaaS, o portal Meus Aplicativos (também conhecido como Painel de Acesso) e o logon único proporcionam uma experiência do usuário aprimorada.

* **Gerenciamento de dispositivos**

Além das contas de pessoas individuais, o Azure AD dá suporte ao registro de dispositivos. O registro permite que os dispositivos sejam gerenciados por meio de ferramentas como o Microsoft Intune. Também permite que políticas de Acesso Condicional baseadas no dispositivo restrinjam tentativas de acesso somente às provenientes de dispositivos conhecidos, independentemente da conta de usuário solicitante.

## Quais tipos de recursos o Azure AD pode ajudar a proteger?

O Azure AD ajuda os usuários a acessar recursos internos e externos.

Os recursos externos podem incluir Microsoft Office 365, o portal do Azure e milhares de outros aplicativos SaaS (software como serviço).

Os recursos internos podem incluir aplicativos em sua rede corporativa e intranet, juntamente com qualquer aplicativo de nuvem desenvolvido em sua organização.

## O que é o logon único?

O logon único permite que um usuário entre uma vez e use essa credencial para acessar vários recursos e aplicativos de provedores diferentes.

Um número maior de identidades significa mais senhas para se lembrar e alterar. As políticas de senha podem variar entre aplicativos. À medida que os requisitos de complexidade aumentam, fica cada vez mais difícil para os usuários se lembrarem delas. Quanto mais senhas um usuário precisa gerenciar, maior o risco de um incidente de segurança relacionado às credenciais.

Considere o processo de gerenciamento de todas essas identidades. Um esforço adicional é colocado no suporte técnico, pois eles lidam com bloqueios de conta e solicitações de redefinição de senha. Se um usuário sai de uma organização, o rastreamento de todas essas identidades e a garantia de que elas estão desabilitadas podem ser um desafio. Quando uma identidade é negligenciada, isso pode permitir o acesso quando ele deveria ter sido eliminado.

Com o SSO, você precisa se lembrar apenas de uma ID e uma senha. O acesso entre aplicativos é concedido a uma única identidade vinculada ao usuário, o que simplifica o modelo de segurança. À medida que os usuários mudam de função ou deixam a organização, o acesso fica vinculado a uma só identidade. Essa alteração reduz consideravelmente o esforço necessário para alterar ou desabilitar contas. Usar SSO para contas torna mais fácil para os usuários gerenciar suas identidades e aumenta as funcionalidades de segurança.

Você encontrará recursos no final deste módulo sobre como habilitar SSO por meio do Azure AD.

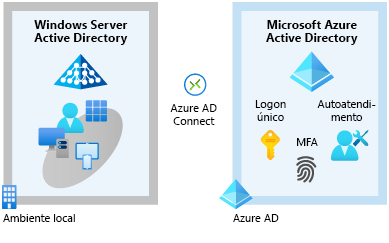
## Como posso conectar o Active Directory ao Azure AD?

Conectar o Active Directory ao Azure AD permite que você proporcione uma experiência de identidade consistente para seus usuários.

Há algumas maneiras de conectar sua instalação existente do Active Directory ao Azure AD. Talvez o método mais popular seja usar o Azure AD Connect.

O Azure AD Connect sincroniza identidades de usuário entre o Active Directory local e o Azure AD. O Azure AD Connect sincroniza alterações entre os dois sistemas de identidade, o que permite que você use recursos como SSO, autenticação multifator e redefinição de senha por autoatendimento em ambos. A redefinição de senha por autoatendimento impede que os usuários usem senhas comprometidas conhecidas.

Veja um diagrama que mostra como o Azure AD Connect se encaixa entre o Active Directory local e o Azure AD:



Conforme integra sua instância existente do Active Directory ao Azure AD, a Tailwind Traders cria um modelo de acesso consistente em toda a organização. Isso simplifica muito a capacidade de entrar em aplicativos diferentes, gerenciar alterações nas identidades e no controle do usuário e monitorar e bloquear tentativas de acesso incomuns.

# O que são a autenticação multifator e o Acesso Condicional?

A Tailwind Traders permite que os drivers de entrega usem os próprios dispositivos móveis para acessar aplicativos de agendamento e logística. Alguns motoristas de entrega são funcionários permanentes da Tailwind Traders. Outros trabalham com contratos de curto prazo. Como o departamento de TI pode garantir que uma tentativa de acesso seja realmente de um funcionário válido da Tailwind Traders?

Nesta parte, você aprenderá sobre dois processos que habilitam a autenticação segura: Autenticação Multifator do Azure AD e Acesso Condicional. Vamos começar com uma breve visão do que é a autenticação multifator de modo geral.

## **O que é a autenticação multifator?**

Autenticação multifator é um processo em que o usuário deve fornecer uma forma adicional de identificação durante o processo de entrada. Exemplos incluem um código no telefone celular ou uma verificação de impressão digital.

Pense em como você entra em sites, email ou serviços de jogos online. Além de seu nome de usuário e senha, você alguma vez precisou inserir um código enviado para seu telefone? Se sim, você usou a autenticação multifator para entrar.

A autenticação multifator fornece segurança adicional para as identidades, exigindo dois ou mais elementos para a autenticação completa.

Esses elementos se enquadram em três categorias:

* **Algo que o usuário sabe**

Pode ser um endereço de email e uma senha.

* **Algo que o usuário tem**

Pode ser um código enviado para o telefone celular do usuário.

* **Algo que o usuário é**

Normalmente é algum tipo de propriedade biométrica, como uma impressão digital ou verificação de detecção facial usada em muitos dispositivos móveis.



A autenticação multifator aumenta a segurança de identidade, limitando o impacto da exposição da credencial (por exemplo, nomes de acesso e senhas roubados). Com a autenticação multifator habilitada, um invasor que tenha uma senha de usuário também precisará ter em mãos o telefone ou a impressão digital desse usuário para se autenticar por completo.

Comparação da autenticação multifator com a autenticação de fator único. Na autenticação de fator único, um invasor precisaria apenas de um nome de usuário e senha para se autenticar. A autenticação multifator deve ser habilitada sempre que possível, pois traz enormes benefícios à segurança.

## O que é a Autenticação Multifator do Azure AD?

A Autenticação Multifator do Azure AD é um serviço da Microsoft que fornece funcionalidades de autenticação multifator. A Autenticação Multifator do Azure AD permite que os usuários escolham uma forma adicional de autenticação durante a conexão, como uma chamada telefônica ou uma notificação no aplicativo móvel.

Esses serviços fornecem funcionalidades de Autenticação Multifator do Azure AD:

* **Azure Active Directory**

A edição gratuita do Azure Active Directory habilita a Autenticação Multifator do Azure AD para administradores com o nível de acesso de administrador global por meio do aplicativo Microsoft Authenticator, de chamada telefônica ou de código SMS. Você também pode impor a Autenticação Multifator do Azure AD para todos os usuários por meio apenas do aplicativo Microsoft Authenticator habilitando padrões de segurança em seu locatário do Azure AD.

O Azure Active Directory Premium (licenças P1 ou P2) permite uma configuração abrangente e granular da Autenticação Multifator do Azure AD por meio de políticas de Acesso Condicional s(explicadas em breve).

* **Autenticação multifator para o Office 365**

Um subconjunto de funcionalidades da Autenticação Multifator do Azure AD faz parte da sua assinatura do Office 365.

Para obter mais informações sobre licenças e funcionalidades da Autenticação Multifator do Azure AD, confira [Versões disponíveis da Autenticação Multifator do Azure AD](https://docs.microsoft.com/pt-br/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-multi-factor-authentication?azure-portal=true).

## O que é Acesso Condicional?

O Acesso Condicional é uma ferramenta que o Azure Active Directory usa para permitir (ou negar) o acesso a recursos com base em sinais de identidade. Esses sinais incluem quem é o usuário, onde ele está e de qual dispositivo está solicitando acesso.

O acesso condicional ajuda os administradores de TI a:

* Capacitar os usuários a serem produtivos em qualquer lugar e sempre.
* Proteger os ativos da organização.

O Acesso Condicional também proporciona uma experiência de autenticação multifator mais granular para os usuários. Por exemplo, um segundo fator de autenticação poderá não ser solicitado se o usuário estiver em uma localização conhecida. No entanto, ele poderá ser solicitado se os sinais de conexão do usuário forem incomuns ou se o usuário estiver em uma localização inesperada.

Durante a conexão, o acesso condicional coleta sinais do usuário, toma decisões com base nesses sinais e impõe essa decisão, permitindo ou negando a solicitação de acesso ou solicitando uma resposta de autenticação multifator.

Aqui está um diagrama que ilustra esse fluxo:



Aqui, o sinal pode ser a localização do usuário, o dispositivo do usuário ou o aplicativo que o usuário está tentando acessar.

Com base nesses sinais, a decisão poderá ser permitir acesso completo se o usuário estiver entrando de seu local usual. Se o usuário estiver entrando de uma localização incomum ou que esteja marcada como de alto risco, o acesso poderá ser totalmente bloqueado ou possivelmente concedido depois que o usuário fornecer uma segunda forma de autenticação.

A imposição é a ação que executa a decisão. Por exemplo, permitir o acesso ou exigir que o usuário forneça uma segunda forma de autenticação.

### Quando posso usar o acesso condicional?

O acesso condicional é útil quando você precisa:

* Exigir autenticação multifator para acessar um aplicativo.

Você pode configurar se todos os usuários precisam de autenticação multifator ou apenas determinados usuários, como administradores.

Você também pode configurar se a autenticação multifator se aplica ao acesso de todas as redes ou apenas de redes não confiáveis.

* Exigir acesso a serviços somente por meio de aplicativos cliente aprovados.

Por exemplo, talvez você queira permitir que os usuários acessem os serviços do Office 365 usando um dispositivo móvel, desde que usem aplicativos cliente aprovados, como o aplicativo móvel do Outlook.

* Exigir que os usuários acessem seu aplicativo somente de dispositivos gerenciados.

Um dispositivo gerenciado é um dispositivo que atende aos seus padrões de segurança e conformidade.

* Bloquear o acesso de fontes não confiáveis, como o acesso de locais desconhecidos ou inesperados.

O acesso condicional vem com uma ferramenta What If, que ajuda a planejar e solucionar problemas de suas políticas de acesso condicional. Você pode usar essa ferramenta para modelar as políticas de Acesso Condicional propostas em tentativas de conexão recentes de seus usuários para ver qual teria sido o impacto se essas políticas tivessem sido habilitadas. A ferramenta What If permite que você teste as políticas de Acesso Condicional propostas antes de implementá-las.

### Onde o acesso condicional está disponível?

Para usar o acesso condicional, você precisa de uma licença do Azure AD Premium P1 ou P2. Se você tiver uma licença do Microsoft 365 Business Premium, também terá acesso aos recursos de Acesso Condicional.

# Verificação de conhecimentos

Considere este cenário. Depois, escolha a melhor resposta para cada pergunta a seguir e selecione **Verificar suas respostas**.

Na Tailwind Traders, lembre-se de que os funcionários de varejo recebem dispositivos Tablet dos quais eles podem controlar pedidos e planejar suas agendas de trabalho.

A Tailwind Traders também permite que os drivers de entrega usem os próprios dispositivos móveis para acessar aplicativos de agendamento e logística.

Uma senha roubada pode permitir o acesso não autorizado aos dados da empresa e do cliente. A Tailwind Traders quer estender seus investimentos no Active Directory para proteger todos os seus aplicativos, tanto acessados pela intranet e quanto por redes públicas.

A empresa está analisando como o Azure AD (Azure Active Directory), o SSO (logon único), a autenticação multifator e o Acesso Condicional podem ajudar a conquistar essas metas.

## Verificar seus conhecimentos

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamenteParte superior do formulário

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

# Resumo

Parte inferior do formulário

A Tailwind Traders precisa garantir que apenas suas equipes possam acessar seu conjunto crescente de aplicativos em nuvem, de qualquer localização e de qualquer dispositivo.

Ao desenvolver seu plano, a Tailwind Traders aprende que:

* A AuthN (autenticação) estabelece a identidade do usuário.
* A AuthZ (autorização) estabelece o nível de acesso que um usuário autenticado tem.
* O SSO (logon único) permite que um usuário entre uma vez e use essa credencial para acessar vários recursos e aplicativos.
* O Azure AD (Azure Active Directory) é um serviço de gerenciamento de identidade e acesso baseado em nuvem. O Azure AD permite que a organização controle o acesso a aplicativos e recursos com base em seus requisitos empresariais.
* A Autenticação Multifator do Azure AD fornece segurança adicional para as identidades, exigindo dois ou mais elementos para a autenticação completa. De modo geral, a autenticação multifator pode incluir algo que o usuário sabe, algo que o usuário tem e algo que o usuário é.
* O Acesso Condicional é uma ferramenta usada pelo Azure AD para permitir ou negar o acesso a recursos com base em sinais de identidade, como a localização do usuário.

Com essas ideias em vigor, as equipes de desenvolvimento de software e o administrador de TI podem começar a substituir os sistemas de autenticação atuais por sistemas que usam vários fatores e permitem o acesso a vários aplicativos.