FOLHETO

Cloud Access Manager

Unificação e proteção do acesso para seus desafios mais urgentes

Benefícios

- Acesso simples e seguro a aplicativos locais e baseados em cloud
- Satisfação do usuário e produtividade aprimoradas
- Permite que a equipe de TI proteja e gerencie vários modos de acesso e aplicativos
- Um nível extra de garantia de login com autenticação de múltiplos fatores
- Economia com provisionamento no momento certo para Salesforce, Google Apps e Office 365
- Administração simples com interface da Web baseada em assistente
- Aproveita todas as capacidades dos padrões OAuth 2.0 e OpenID Connect

Requisitos do sistema

Para obter uma lista completa dos requisitos do sistema, acesse oneidentity.com/cloud-access-manager

Anos atrás, quando todos os usuários e aplicativos de uma organização estavam no local, o controle de acesso era simples. Hoje, funcionários, parceiros e clientes acessam aplicativos de locais no mundo todo com uma variedade crescente de dispositivos. Aplicativos relevantes incluem não apenas aqueles desenvolvidos e/ou hospedados internamente, mas também aplicativos baseados em cloud, como Salesforce.com®, serviço Google® Apps™ e Microsoft® Office 365®. Enquanto isso, as exigências de segurança crescem no mesmo ritmo, se não mais rapidamente, que as expectativas do usuário de acesso ininterrupto.

É responsabilidade da equipe de TI conceder de maneira eficiente aos usuários o acesso necessário e no momento certo, além de garantir que todo o acesso seja adequado, seguro e compatível com as políticas de segurança. É necessária uma maneira de colocar todo o acesso, independentemente do tipo de usuário, da localização ou do tipo de aplicativo, sob a mesma proteção de gerenciamento e segurança.

Com o Cloud Access Manager, parte da família de produtos One Identity, é possível atender às necessidades dos seus usuários quanto ao acesso baseado em navegador para recursos internos, aplicativos móveis

ONE IDENTITY

personalizados e aplicativos da Web baseados em cloud, ao mesmo tempo que aprimora a eficiência da TI e da segurança. O Cloud Access Manager fornece login único (SSO), segurança com reconhecimento de contexto (ou adaptável), provisionamento de cloud no momento certo, federação, autorização e auditoria para uma ampla gama de tipos de aplicativos e cenários de acesso.

Recursos

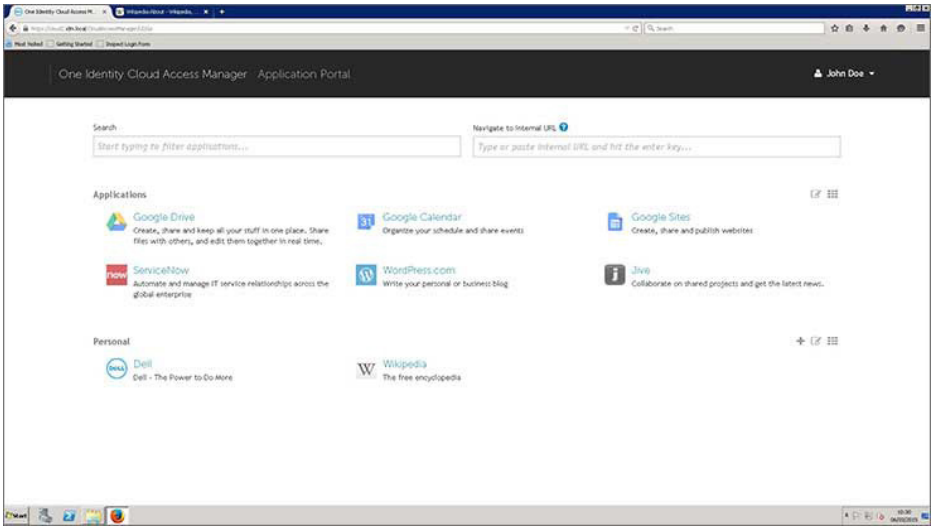
Autenticação centralizada, SSO e recuperação de atributos

Não dependa dos diretórios dedicados centrados em aplicativo e da carga administrativa que eles representam. Conecte-se a múltiplos aplicativos e diretórios de usuário em um hub de autenticação centralizado. Agora, um evento de login único (e senha) pode criar uma sessão com múltiplos aplicativos da Web, hospedados localmente ou por fornecedores de SaaS, assim como seus próprios aplicativos móveis personalizados, por meio do protocolo OpenID Connect. Os aplicativos podem ser integrados por meio de uma variedade de tecnologias, inclusive injeção de credenciais, cabeçalhos HTTP, tokens de segurança Security Assertion Markup Language (SAML) e login social compatível com OAuth via Google, Microsoft Live ID, Facebook e Twitter. Com o uso de um mecanismo eficiente e baseado em regras, o Cloud Access Manager pode oferecer dados adicionais sobre os usuários para aplicativos protegidos para controle de acesso detalhado.

Segurança com reconhecimento de contexto

Ao considerar os aspectos de quem, o quê, quando e onde para a aplicação de segurança, o Mecanismo de Análise de Segurança (SAE), que está incluído no Cloud Access Manager, coleta informações de várias fontes para fornecer contexto sobre quais decisões de acesso podem ser tomadas e aplicadas. As informações contextuais disponíveis por meio do SAE incluem:

- Navegador utilizado: inclui a análise do histórico de uso do navegador que desvia do comportamento normal do usuário
- Padrão de localização geográfica: detecta se uma atividade de acesso é originada de um local anormal
- Localização geográfica específica: impede acessos iniciados de regiões geográficas específicas, conhecidas por promover atividade mal-intencionada
- Associação em grupo
- Tentativa/histórico de autenticação com falha
- Horário: detecta atividades de acesso que ocorrem fora dos padrões normais do usuário
- Lista negra: lista redes ou endereços de rede proibidos
- Lista branca: lista redes ou endereços de rede aprovados



O Cloud Access Manager fornece uma experiência de login unificada para qualquer aplicativo desenvolvido internamente e baseado em navegador, aplicativos da Web, aplicativos móveis OpenID Connect e aplicativos SaaS.

Autenticação de múltiplos fatores

O Cloud Access Manager oferece suporte à autenticação de múltiplos fatores como uma fonte principal de login e para autenticação progressiva conforme indicado pelas pontuações de risco geradas pelo Mecanismo de análise de segurança. As opções para a autenticação de múltiplos fatores incluem o Defender no local e o Defender como uma implantação de serviço baseada em SaaS.

Controles de acesso baseados em políticas

Elimine a segurança ad hoc inconsistente e garanta que os usuários possam acessar somente os recursos autorizados com base em funções do usuário definidas pela equipe de TI. As funções e as associações da função podem ser atribuídas dinamicamente com base nas políticas avaliadas em tempo real com os dados de identidade. O controle de acesso baseado em regras pode ser aplicado a sub-regiões de um aplicativo da Web para permitir uma autorização granular.

Federação de identidade

Ative cenários de acesso que abranjam limites de segurança (como aplicativos baseados em cloud, colaboração de múltiplas forests, plataformas heterogêneas e extranets de parceiros) sem a necessidade de senhas de usuário redundantes. As alegações do Cloud Access Manager também podem ser associadas aos recursos do SharePoint. Com o suporte à federação em funções de fornecedor de identidade e prestador de serviços, ele facilita o acesso do usuário aos aplicativos da Web, independentemente de onde os usuários e/ou aplicativos estejam localizados.

Atenda às necessidades dos seus usuários de acesso com login único a aplicativos da Web baseados em cloud, ao mesmo tempo que melhora a segurança e a eficiência da TI.

Provisionamento de acesso a cloud

Para SSOs federados para aplicativos em cloud, como Salesforce.com, Google Apps ou Office 365 funcionarem, as contas de usuário precisam ser provisionadas no aplicativo de cloud. O Cloud Access Manager centraliza as funções de provisionamento de acesso e de SSO em uma única ferramenta para maior eficiência da equipe de TI. O provisionamento no momento certo economiza dinheiro ao ativar as licenças somente quando o acesso é realmente utilizado.

Agregação de espaço de trabalho e acesso remoto

Com a habilidade de personalizar seu portal do Cloud Access Manager, é possível simplificar a maneira como os usuários encontram todos os aplicativos necessários para trabalhar com o Portal de aplicativos do Cloud Access Manager.

Os usuários encontram uma coleção de links fácil de ler e baseada em funções para os aplicativos aos quais eles têm direito. Por meio do proxy do Cloud Access Manager, os usuários podem acessar qualquer aplicativo via navegador da Web.

Auditoria de acesso

O Cloud Access Manager permite que os profissionais de segurança aproveitem sua função como uma solução centralizada de autenticação e de controle de acesso para auditoria e relatórios sobre eventos de acesso para fins forenses, de conformidade e de repúdio.

Os tipos de login com suporte do Cloud Access Manager incluem cabeçalho HTTP, federação/confiança de WS, SAML, preenchimento de formulário, federado como um fornecedor de identidade e federado como um prestador de serviços, assim como cenários OpenID Connect e OAuth.

Sobre o One Identity

A família One Identity de soluções de gerenciamento de identidades e acessos (IAM) oferece IAM para o mundo real, inclusive soluções centradas nos negócios, modulares e integradas preparadas para o futuro para governança de identidades, gerenciamento de acesso e gerenciamento privilegiado.

Saiba mais em OneIdentity.com

Datasheet-CloudAccessManager-US-KJ-pt_BR-WL-27053

ONE IDENTITY