NoPass

AUTENTICAÇÃO E REGISTRO SEM SENHA

Contate-Nos
sales@identite.us
www.identite.us

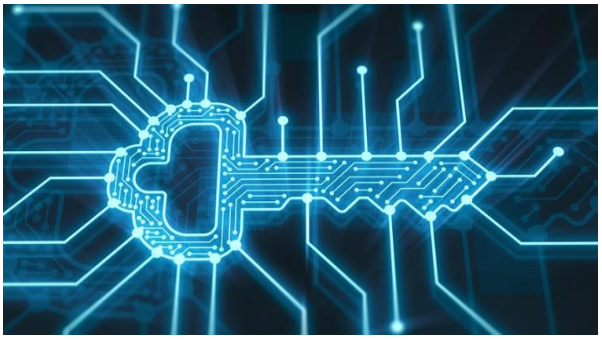
Tecnologia Single-Sign-On

Hoje, as organizações desejam fornecer aos usuários finais acesso aos aplicativos aprovados pela empresa de forma rápida e segura. Eles querem garantir que as pessoas certas (ou seja, funcionários, funcionários de meio período, contratados, etc.) tenham acesso às informações corretas da empresa. Na verdade, se houver uma oportunidade de reduzir ou eliminar o uso de senha, tanto as organizações quanto os usuários finais irão gostar disso. Quando a produtividade do funcionário e a experiência do usuário são as principais prioridades, o logon único em aplicativos corporativos é fundamental.

NoPass™ SSO multifator para funcionarios sem senha garante que apenas usuários autorizados tenham acesso a dados confidenciais a traveis de todos os seus sistemas. Com NoPass™ SSO para empregados obtenha todos os recursos do NoPass™ MFA cpm recursos adicionais, como suporte de Federação/SAML/OIDC e Identity Brokering.

NoPass™ é um aplicativo de autenticação seguro que oferece as duas coisas que você mais precisa: o mais alto nível de segurança de autenticação e a interface de usuário mais simples. Agora você pode ter a confiança de nunca se preocupar com o comprometimento de suas credenciais online.

NoPass™ Single-Sign-On

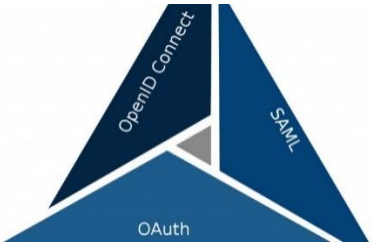


Aumente a produtividade enquanto mantém os dados seguros. Com NoPass™ SSO para empregados, os usuários só precisam se autenticar uma vez para acessar seus aplicativos da web na nuvem. Essa medida básica de gerenciamento de identidade e acesso (IAM) é a primeira etapa na construção de experiências confiáveis para sua força de trabalho, clientes e parceiros. A autenticação multifator sem senha de SSO do funcionário NoPass™ garante que apenas usuários autorizados tenham acesso a dados confidenciais. NoPass™ SSO para empregados incorpora todos os recursos que são oferecidos no NoPass™ Employee MFA com recursos adicionais para Single-Sign-on, como:

Login Único

Com o NoPass™ SSO, os usuários só precisam inserir um nome de usuário para acessar com segurança seus aplicativos da web na nuvem e atrás do firewall - via desktops, smartphones e tablets. Isso aumenta muito a produtividade, mantendo os dados seguros. O SSO NoPass™ usa autenticação integrada do Windows (IWA) para conectar usuários ao NoPass™ automaticamente depois que eles entrarem no domínio do Active Directory ou no portal da empresa.

Suporte para Federação/SAML/OIDC



NoPass™ pode se integrar com aplicativos em nuvem e locais usando SAML, WS-Federation, OpenID Connect, e serviços da web para fornecer logon único, simples e rápido para qualquer dispositivo e servir como o provedor de identidade para provedores de serviços externos de modo que quando o usuário fizer login em um serviço, em vez de fornecer credenciais ao provedor de serviços, o provedor de serviços confie no provedor de identidade para validar as credenciais.
O servidor de autenticação NoPass ™ tem a capacidade de aceitar tokens de autenticação SAML e OIDC e responder a cada um, respectivamente.

Corretagem de Identidade

NoPass™ SSO para empregados pode atuar como um serviço intermediário que conecta vários provedores de serviços com diferentes provedores de identidade. Como um serviço intermediário, o NoPass™ SSO para empregados é responsável por criar uma relação de confiança com um provedor de identidade externo, a fim de permitir o acesso de suas identidades a serviços internos expostos por provedores de serviços. NoPass™ SSO para empregados tem a capacidade de adicionar fatores adicionais de autenticação além da autenticação do usuário dos provedores de identidade. Quando um provedor de identidade envia um token de autenticação via NoPass™, a identidade do usuário é registrada em NoPass™. Você pode configurar fatores de autenticação adicionais para este usuário após NoPass™ receber um token de federação válido.

Experiência perfeita para o usuários/Usuário temporário

Com NoPass™ SSO para empregado, você agora tem a capacidade de adicionar usuários temporários à sua força de trabalho e conceder a eles a possibilidade de usar os serviços que seus outros funcionários estão acessando. Você pode adicionar restrições como o período em que eles têm acesso aos recursos, quais recursos estão disponíveis e quais ainda são restritos e o horário durante o dia em que eles podem acessar esses serviços. Essa opção é muito importante para empresas que recebem visitantes frequentes ou terceirizam parte de seus serviços para fornecedores terceirizados. Permita que seus usuários finais acessem rapidamente aplicativos corporativos aprovados com um clique. Elimine a inconveniência de gerenciar, lembrar e redefinir várias senhas para usuários finais.

Requisitos de Infraestructura

No Local

- Implantação altamente disponível
- Suporte a Docker e Kubernetes
- Proxy reverso
- Clustering e HA

Nuvem

- Nuvem privada implantável (ou seja, AWS, Azure, IBM)
- Alta escalabilidade
- Implante em quase todos os países
- Suporte para autoinscrição para testes e produção

Características do Produto

- Produto de autenticação sem senha full-duplex simples, seguro e conveniente
- O processo NoPass ™, Full Duplex Authentication ™ segue um modelo de autenticação descentralizado. Funciona em conjunto com qualquer tecnologia de autenticação de usuário tradicional, como PIN, OTP, PKI e biometria
- SSO totalmente sem senha, fácil de instalar, gerenciar e escalar para atender às necessidades de qualquer tamanho de organização
- Imagem inovadora e código OTP, conveniente para o usuário e segurança de força bruta muito maior
- Visão geral completa da administração - usando o painel de administração, defina políticas e restrições, como dispositivos e requisitos geográficos
- Arquitetura flexível para fácil integração com qualquer autenticação de usuário existente

Benefícios de NoPass™

Seguridade
As credenciais de login são únicas em cada site, nunca saem do dispositivo do usuário e nunca são armazenadas em um servidor.

Conveniência
Os usuários desbloqueiam credenciais de login com métodos integrados simples, como leitores de impressão digital ou varreduras de rosto.

Escalabilidade
O amplo uso de smartphones e nossa implantação na nuvem tornam muito fácil dimensionar qualquer autenticação existente.

Eficiência de custos
Economize milhões em custos de helpdesk e suporte de senha.

Privacidade
Proteja os usuários contra vazamentos de credenciais e phishing de senha.