



NoPass

CADASTRAMENTO E AUTENTICAÇÃO MULTIFATORES PARA FUNCIONÁRIOS

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

Tecnologia de autenticação NoPass™

O NoPass™ é um plug-in de autenticação multifatorial para usuários remotos. Além do nome e da senha do usuário, o NoPass™ executa dois fatores de autenticação adicionais: algo que possui e que é. Isso usa telefones inteligentes (smartphone) e não requer a compra de dispositivos de autenticação de hardware adicionais para cada usuário. Ele também não usa SMS, o que também pode ser caro.



O NoPass™ é um aplicativo de autenticação segura que fornece as duas coisas que você mais precisa: o mais alto nível de segurança de autenticação e a interface do usuário mais simples. Agora você pode ter certeza de nunca se preocupar em comprometer suas credenciais online.

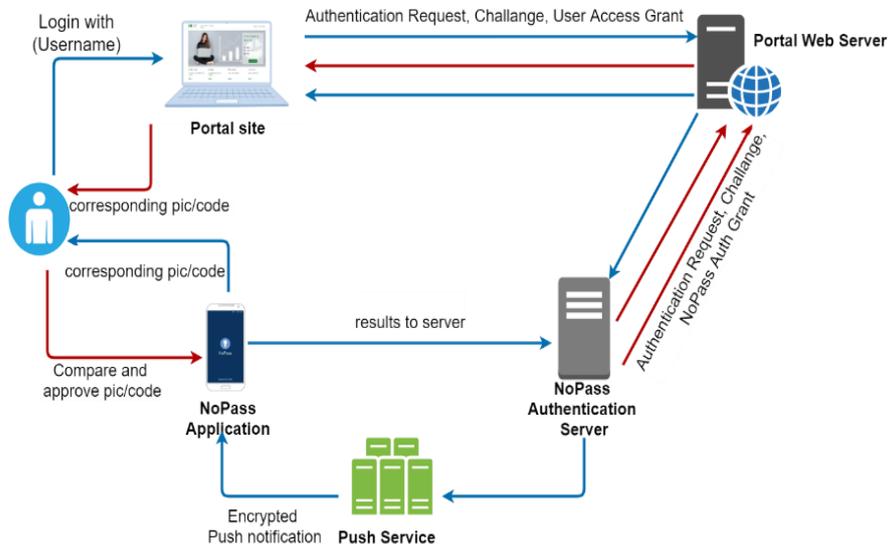
Juntamente com uma segurança muito forte, o usuário não precisa digitar uma senha. O servidor NoPass™ e o aplicativo no telefone cuidam de todo o link bidirecional e exigem que o usuário compare duas imagens (uma imagem e um número de 3 dígitos), depois toque no botão de aprovar e eles estão conectados.

Esse método fornece um milhão de combinações criptografadas e praticamente não pode ser comprometido por um hacker, pois os metadados são válidos por apenas alguns segundos e depois são inúteis. Mesmo se o usuário aprovar a transação por engano, podemos detectar a intrusão e bloquear a entrada no servidor.

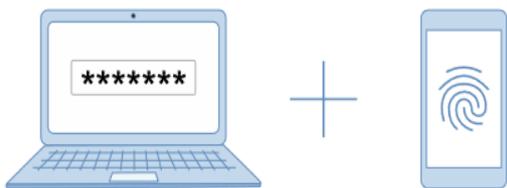
Tecnologia de AUTENTICAÇÃO FULL DUPLEX™

O processo de autenticação NoPass™, Full Duplex™ segue um modelo de autenticação descentralizado. Isso nos permite trabalhar com qualquer tipo de tecnologia tradicional de autenticação de usuário, como PIN, OTP, PKI e biometria. O NoPass™ possui uma arquitetura flexível para integrar-se facilmente a qualquer solução de autenticação de usuário.

Ao combinar a criptografia de chave pública com a rápida autenticação OTP, a autenticação NoPass™ Full Duplex™ MFA permite o login da sessão iniciado em dispositivos móveis, direto para as estações de trabalho através do seu dispositivo móvel. É rápido e seguro.



NoPass™ MFA (Fator Duplo)

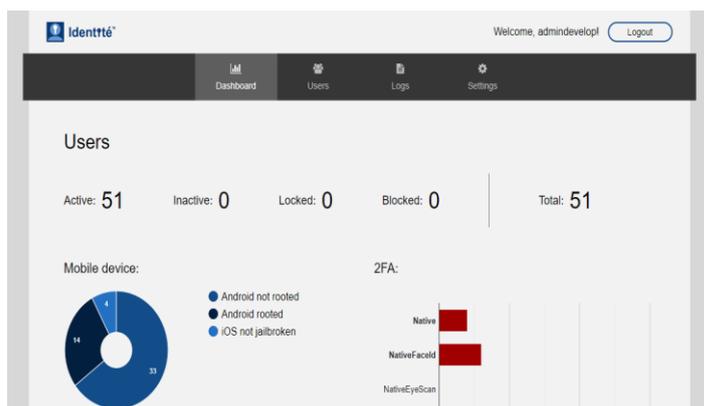


Com o aumento dos ataques de phishing e outras identidades atualmente, a autenticação que requer um nome de usuário e senha (como RADIUS) pode estar em risco. Esquemas sofisticados de engenharia social e táticas inteligentes podem enganar até os usuários mais inteligentes. Para combater isso, o NoPass™ lançou sua solução de fator duplo, um recurso leve que melhora a segurança geral e pode ser adaptado aos principais protocolos de autenticação do mercado.

NoPass™ Painel de administração

Obtenha uma visão geral completa da administração: usando o painel de administração do NoPass™. Garantia de confiança do dispositivo - verifique se todos os dispositivos atendem aos padrões de segurança. Políticas de acesso adaptável estabelecem políticas para conceder ou bloquear tentativas de acesso. Acesso remoto, acesso seguro a todos os aplicativos e servidores.

Todos os aspectos do seu sistema de autenticação NoPass™ podem ser gerenciados no painel de administração do NoPass™. Isso inclui criar e gerenciar aplicativos, registrar e ativar usuários, gerenciar dispositivos móveis, ajustar a experiência do usuário da instalação do NoPass™ e muito mais.



Requisitos de infraestrutura

Interno (servidor da empresa)

- Implantação altamente disponível
- Suporte para Docker e Kubernetes
- proxy reverso
- Agrupamento e HA

Nuvem

- Implantação em nuvem privada (ou seja, AWS, Azure, IBM) Implantação de alta disponibilidade
- Alta escalabilidade
- Implementar em quase todos os países
- Suporte para auto-registro para teste e produção

Características do produto

- Experiência do usuário simples e clara para cadastrar, autenticação e restauração
- Imagem e código OTP inovadores, conveniência do usuário e segurança contra ataques da força bruta
- Painel de administração fácil de usar para definir políticas e restrições
- Controlar a higiene do dispositivo e verificar se há dispositivos liberados ou enraizados que possam comprometer a segurança
- Integração flexível com qualquer autenticação de usuário existente
- Compatível com Android e iOS
- Backups criptografados de contas na nuvem acessíveis para iOS e Android

Benefícios NoPass™

Segurança

As credenciais de login são únicas em todos os sites, nunca saem do dispositivo do usuário e nunca são armazenadas em um servidor.

Conveniencia

Os usuários desbloqueiam credenciais de login com métodos internos simples, como leitores de impressões digitais ou digitalizações faciais.

Escalabilidade

O uso extensivo de smartphones e nossa implementação em nuvem facilitam o dimensionamento de qualquer autenticação existente.

Eficiencia de Custo

Economize milhões em custos de suporte técnico e suporte de senha.

Privacidad

Proteja seus usuários contra vazamentos de credenciais e phishing de senha