DATASHEET

Starling Two-Factor Authentication

Secure and simple identity verification

Benefits

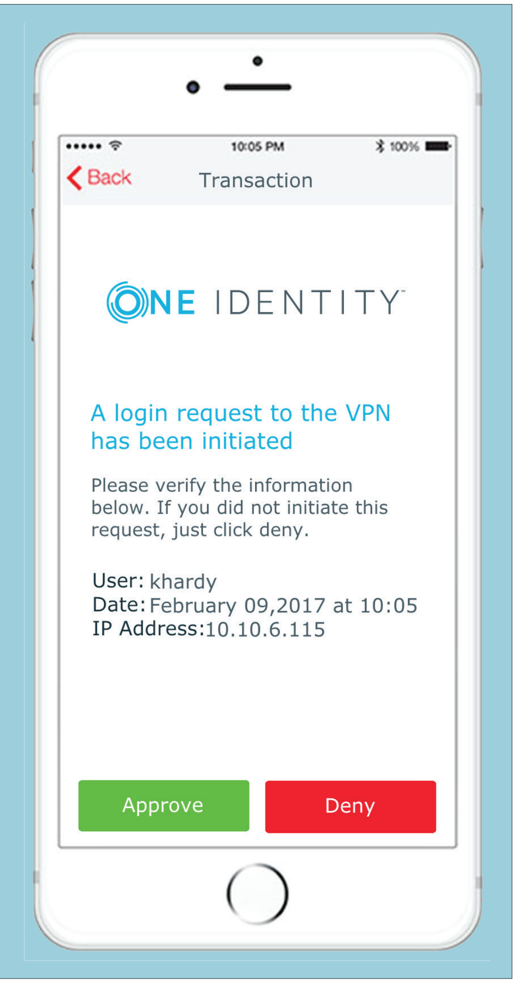
- Heightens security for virtually any system or application
- Simplifies ongoing management by not requiring the infrastructure costs and headache of on-premises solutions
- Eases users' adoption by providing simple to use authentication options like push to authenticate, SMS texts, and phone calls.
- Enables rapid help-desk response to user authentication issues from any Web browser
- Mitigates the risk of a security breach using lost or stolen authentication credentials
- Provides a comprehensive audit trail that enables compliance

Make user access secure and simple

The use of weak, default or stolen passwords is major contributor to many of today's high-profile data breaches. Compounding this issue is that when organizations attempt to strengthen passwords by requiring more frequent password changes and the use of special characters, users are more likely to use the same password for multiple accounts, write the password down, or forget it altogether. When any of these behaviors result the value of the strengthened password is negated and expensive password-reset calls to your helpdesk increase.

What to look for in TFA

The simplest and most secure way to address the password problem is two-factor authentication (TFA). However, not all two-factor solutions are the same. Organizations should consider a solution's architecture, ease of deployment and administration, available tokens, and overall cost.



A login request to the VPN has been initiated

Please verify the information below. If you did not initiate this request, just click deny.

User: khardy
Date: February 09,2017 at 10:05
IP Address:10.10.6.115

Push-to-Authenticate simplifies and secures the user login process.

Starling Two-Factor Authentication solves the password problem securing your organization and keeping your users productive. It does this all without a capital investment or the increased infrastructure and management costs that you might incur with traditional on-premises solutions. With an easy to use dashboard for administrators and flexible authentication options for end users, Starling Two-Factor Authentication enables organizations to quickly and easily verify a user's identity.

Features

Role-based Dashboard

The role-based administrator dashboard with approval workflow ensures that administrators and helpdesk associates receive the appropriate tasks/rights while making it easy for them to manage end-user accounts, generate temporary response codes, and run health checks to verify the mobile app is working correctly.

Multiple authentication methods

Users can generate one-time passwords with the Starling 2FA mobile app or receive a one-time password via SMS or phone call.

Push-to-Authenticate

Make two-factor authentication even easier for your users: They can skip the one-time password by choosing to push-to-authenticate after entering their username and password into an application. This will send a SMS verification to their mobile app asking if they approve or deny the logon request to the application. Once approved, they will be automatically logged into the application.

Tokens

Starling two-factor authentication has several options, including mobile apps for iOS and Android, Chrome; SMS text; or phone call.

Token Branding

Via Starling's dashboard, administrators can easily customize the look of the token on the mobile app to match company branding.

ADFS Adapter

Enables organizations to implement two-factor authentication to applications that use Microsoft WS-Federation protocol, such as Office 365. Plus, it is compatible with other federation protocols, including SAML 2.0 to support logons for cloud apps like Google Apps and salesforce.com.

Radius Agent

Enables organizations to support two-factor authentication on anything that uses the radius protocol for authentication.

RESTful API

Enables quick and easy integration with most application-development languages.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

Learn more at OneIdentity.com