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, such as push-to-authenticate, SMS texts and phone calls
- Enables rapid helpdesk response to user-authentication issues from any web browser
- Mitigates the risk of a security breach from compromised or stolen authentication credentials
- Provides a comprehensive audit trail to meet compliance requirements

Overview

No matter how passwords are compromised, whether it's by questionable user behavior, use of weak passwords or they are just stolen, it's going to be bad for your organization's reputation and bottom line. There's a simple way to enhance security and prevent a data breach by requiring two-factor authentication to gain access to your network resources.

With Starling Two-Factor Authentication, a SaaS-based solution, you can secure your organization, make users more productive and drastically reduce the volume of password-reset calls to your help desk.

Make User Access Secure and Simple

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. You should consider how your organization operates, how authentication processes could be made more efficient, what token form factors you will need and what will work with your existing application stack and infrastructure.

Starling Two-Factor Authentication solves the password problem without the capital costs that come with traditional on-premises solutions. Its easy-to-use admin dashboard and flexible authentication options for end users enables organizations to quickly and easily verify a user's identity.

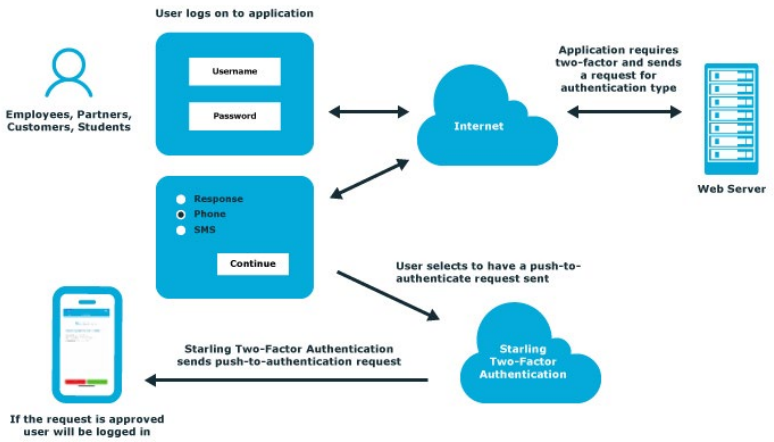

Figure 1. Starling Two-Factor Authentication architecture and modules.

Features

Easy-to-use Admin 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 for iOS, Android and Chrome 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.

HTTP Agent

Implement two-factor authentication protection to IIS websites.

Desktop Login

Enhance your environment - add two-factor authentication to users' computers and servers by unifying user logons and strengthening authentication.

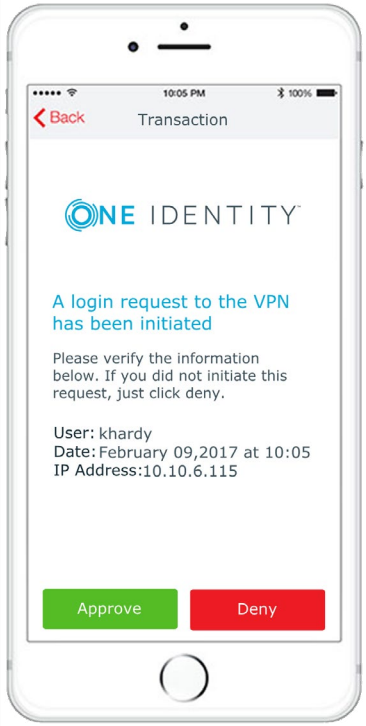

Figure 2. Push-to-Authenticate simplifies and secures the user login process.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com