Multi-Factor Authentication

Protect identities and corporate resources with secure and user-friendly authentication.

Overview

Securing access to corporate networks, protecting the identities of users, and ensuring that the users are who they claim to be is vital for any organization. With the increasing use of cloud applications and mobile devices while at the same time reducing costs are challenges many organizations face today.

Features

- Activate users easy and quickly
- Product includes several verifying methods
- High availability solution
- Mobile apps included
- Easy to install and integrate

Integrates easily

Please visit our website to find a number of products we integrate with. Here you will also find step-by-step documents on how to easily configure integration with different products. With our flexible API´s it is also possible to add above to your custom applications. phenixid.se/integrations/

Reduce TCO

Web interfaces are included to activate mobile apps and edit personal information such as mobile phone number or email address. This can be done by the user or by assigned administrators.

Several methods included

PhenixID Multi-Factor Authentication includes several methods to strengthen the user login process:

- One-time passwords (otp) delivered via SMS, Voice or email. (PhenixID also provides a message gateway for delivering SMS and Voice)

- Generate otps via mobile apps or hardware tokens

- Generate temporary otps to consultants or to employees that have lost or forgot their token device

- Use x.509 certificates

Integration

By integrating your existing solutions with products from PhenixID you can easily add strong multi-factor authentication and simplify login user experience. With our flexible API´s it is also possible to add above to your custom applications.
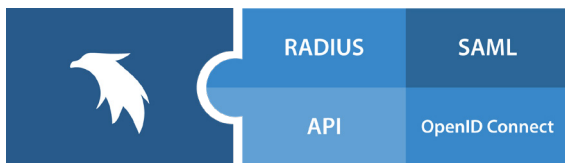
Why PhenixID?

We are a Swedish company based in Stockholm. Our focus is to create applications that solves customer challenges while at the same time keep the cost at a low level.

All our products are built on open standards. All methods for delivering one-time passwords are included in the license. Technical training is available at request. Third line support, with highly experienced technicians.

Web-based tools included to simplify and reduce TCO

Included are two web-based tools to help users and administrators manage MFA related tasks. End-user use Self Service manage themselves. Delegated administrators use MFA Admin to perform tasks on other users. Tasks that can be performed in Self Service or in MFA Admin are:

- Managing mobile phone number or email address

- Add PIN Code

- Generate temporary tokens

- Enable PhenixID Pocket Pass per user

- Enable PhenixID One Touch per user

PhenixID One Touch

With the One Touch app a user will receive a notification on their device prompting for interaction. The user will approve or deny the authentication request by simply answer "Approve" or "Decline". Add PIN code or iOS TouchID for additional security. The mobile app PhenixID One Touch is included in the product and available on iOS and Android.

PhenixID Pocket Pass

Pocket Pass is a mobile app where user can generate one-time passwords when needed during login. Add PIN code or iOS TouchID for additional security. The mobile app PhenixID Pocket Pass is included in the product and available on iOS and Android.

Platforms

Runs on Windows and Linux

High availability

Redundant and scalable for high availability.