nevisIDM – Google Authenticator Support with OATH

Benefits

With Google Authenticator, Authy, FreeOTP and other OATH smartphone applications, users benefit from **strong authentication with little additional effort** – a smartphone is all you need.

Strong two-factor authentication with nevisIDM and OATH **reduces the risk and impact of identity theft**. The one-time passwords (OTPs) used as part of the authentication process can only be used once. Therefore, attackers cannot reuse the login information even if they manage to steal it.

What is it about?

We value your applications. Secure access to them is crucial and must be ensured by reliable authentication methods.

Common authentication methods are passwords and security questions, for example. However, these types of authentication are insecure. Once an attacker knows the password or the answer to the security question, he has direct access to the system.

With strong authentication, malicious access is much less likely. OATH, the Initative for Open Authentication, promotes the adoption of strong authentication.

nevisIDM supports two OATH algorithms: HOTP and TOTP. HOTP is a HMAC-based one-time password. HMAC stands for keyed-hash message authentication code. HOTPs are counter-based, which means the password generation happens upon request (e.g., clicking a button). TOTP is also a one-time password, but it is time-based. That means a password is only valid for a set amount of time.

In combination with an OATH app like Google Authenticator, you can log in to your applications with safe two-factor OATH authentication.
Two-factor authentication requires pieces of evidence from two of the following three categories: something you know, something you own, something you are. Something you know could be a password or PIN. Something you own might be a grid card or a third-party token. Something you are refers to biometrics. It could be your fingerprint, your voice, your typing habits, etc.

With OATH authentication, satisfying the category "something you own" becomes much more convenient. Your smartphone serves as something you own, with the benefit that you are most likely carrying it with you already anyways.

The process is easy. First, download an OATH application (e.g., Google Authenticator). You can enable two-factor authentication by scanning the QR code shown on the screen.

From now on, you will be asked for an OTP in addition to your standard login information (e.g., user name and password) every time you want to log in to your NEVIS-protected application. OTP generation does not require internet access. Additionally, the OTP changes often as it is re-generated automatically for TOTPs or upon request for HOTPs. This means that even if attackers manage to steal your login information, it will not be of any use to them as it cannot be reused.

Main features

- Strong two-factor authentication with little additional effort
- Access to all your applications via Google Authenticator, Authy, FreeOTP and other authentication apps
- Automatic re-generation of passwords
- One-time use of passwords
- No need to carry around an additional device for strong authentication – your smartphone suffices
- Choice between time-based one-time password (TOTP) and HMAC-based one-time password (HOTP)

Switzerland ▪ AdNovum Informatik AG ▪ Roentgenstrasse 22 ▪ 8005 Zurich ▪ Switzerland ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapore ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Germany ▪ NEVIS Office Germany ▪ Hubenstein 11 ▪ 84416 Taufkirchen ▪ Germany ▪ +49 8084 41 33 10 ▪ info@nevis-security.de ▪ www.nevis-security.de

Onboarding Process

The user wants to access an application (target application) but has never used OATH authentication before. Therefore, the user's mobile phone and nevisIDM do not share a secret key yet, which is necessary for generating an OTP.

To start the onboarding process (i.e., enable two-factor authentication), the user needs to be authenticated, e.g., by a user name / password combination (1). The server then generates a secret key, which is presented to the user in the form of a QR code (2). The user scans/enters the secret key with the OATH application (e.g., Google Authenticator) on his mobile phone (3). The secret key is now shared between the OATH application and nevisIDM (4).

Optionally, the user can make sure the secret key is imported correctly. To do so, the user enters a one-time password (6) generated by the OATH application (5) in the browser. If the OTP was entered correctly, the user successfully enabled two-factor authentication and the onboarding process is complete.

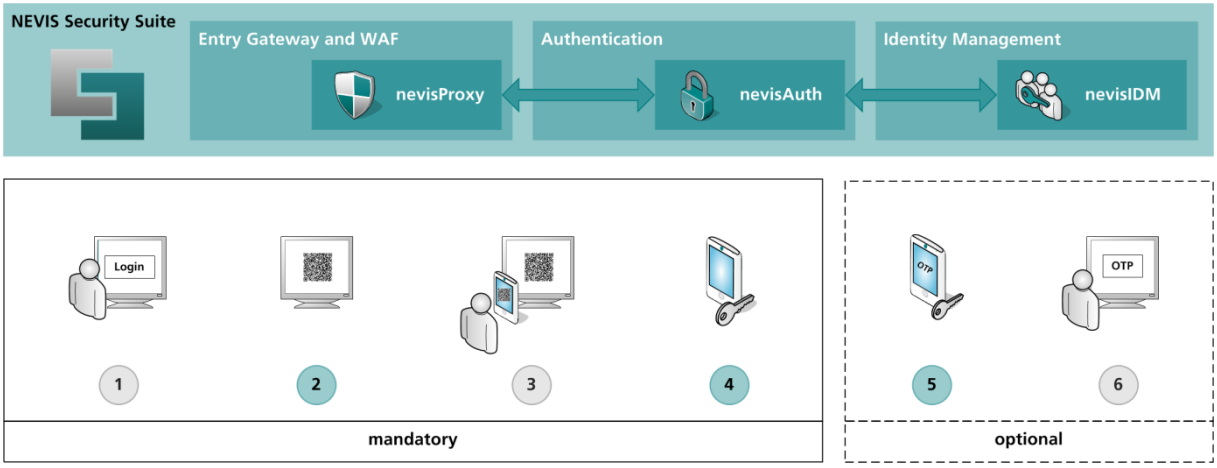

Figure 1 Onboarding Process

Login Process

The user requests access to his target application in the browser (1). nevisProxy and nevisAuth communicate and ask the user for his login information, e.g., user name and password (2). If the correct information was entered, nevisAuth asks for the OTP (3). The user checks the OATH application (e.g., Google Authenticator) on his mobile phone, which generates an OTP by using the stored secret key obtained during the onboarding process (4). The user then enters this OTP in the browser (5). nevisIDM verfies the OTP and, upon success, the user is redirected to his target application (6).

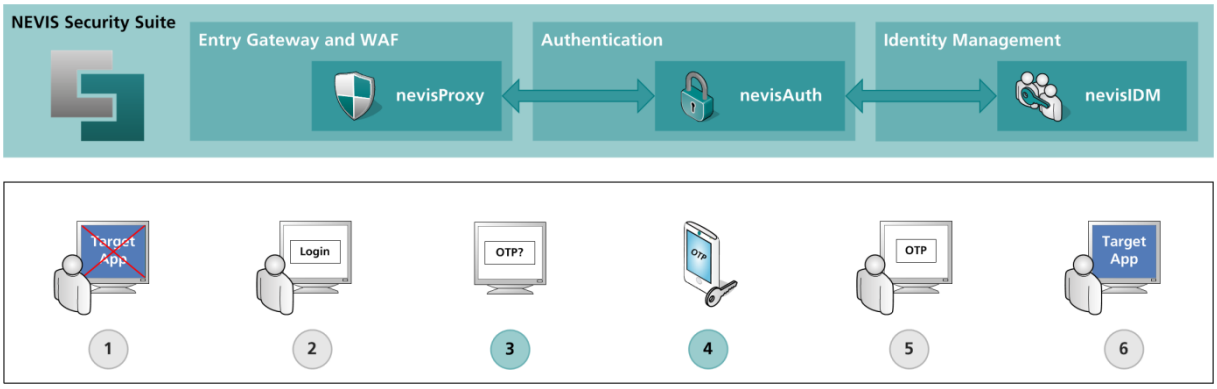

Figure 2 Login Process

Switzerland ▪ AdNovum Informatik AG ▪ Roentgenstrasse 22 ▪ 8005 Zurich ▪ Switzerland ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapore ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Germany ▪ NEVIS Office Germany ▪ Hubenstein 11 ▪ 84416 Taufkirchen ▪ Germany ▪ +49 8084 41 33 10 ▪ info@nevis-security.de ▪ www.nevis-security.de