nevisAuth – Authentication Service

Teaser

nevisAuth provides a highly secure, most flexible and adjustable, easy-to-integrate and user-friendly authentication service, which protects your web applications against unauthorized access.

Benefits

nevisAuth is NEVIS' *modular and highly flexible* authentication service. It supports a wide range of authentication methods, data exchange protocols and token formats (including the NEVIS proprietary SecToken). This makes it possible to *integrate the product in almost every existing IT landscape*. nevisAuth is also able to *adjust authentication strengths*, thus *substantially improving the security* of your web applications. The highly customizable product allows you to *implement exactly the kind of authentication you need* to protect your applications in an optimal way: *as strong as required and as user-friendly as possible*.

What is it about?

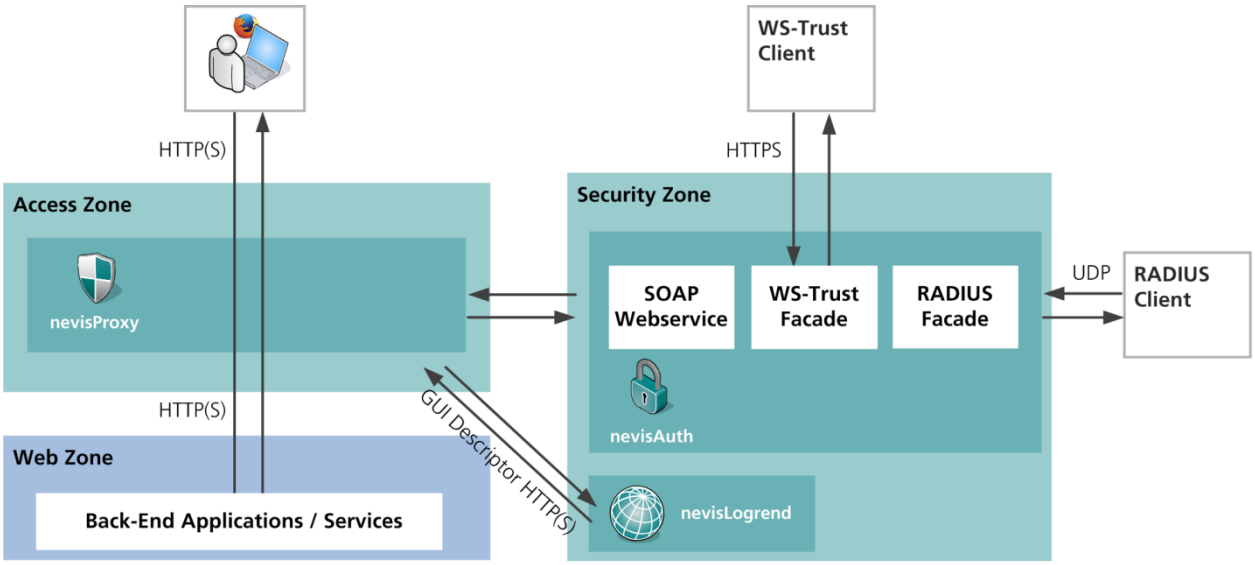

Figure 1 nevisAuth overview

nevisAuth implements strong user and system authentication for the NEVIS identity and access management solution. The product complements nevisProxy, NEVIS' entry gateway and web application firewall. Where nevisProxy filters the *content* of user requests to protect your company's online applications against internal and external threats, nevisAuth focusses on the user's *identity*. Its task is to verify whether the user is who he claims to be, in order to prevent unauthorized users from accessing your applications.

In this context, identification, authentication and authorization play a central role. *Identification* means claiming that you are user X, e.g., by entering your username "userX". *Authentication* is how the system proves if you really are user X. For this, the system can use up to three authentication factors, either separately or combined: something you know (e.g., password or PIN), something you own (e.g., grid card or a third-party token) and something you are (refers to biometrics, e.g., your fingerprint or your typing habits). *Authorization* takes place after the system has successfully identified and authenticated you as really being user X. It is the step that determines what you are allowed to do in the application, your roles and permissions.

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

nevisAuth covers the whole process of identification, authentication and authorization. If the authentication was successful, nevisAuth copies all relevant security data on a signed security token, the SecToken. This token is the user's *Proof of Authentication* towards nevisProxy and the business applications in the back end.

To be able to perform its tasks, nevisAuth works closely together with nevisProxy. For the verification of the user credentials and retrieval of user roles and permissions, the ideal partner of nevisAuth is nevisIDM, NEVIS' product for identity management. However, nevisAuth can also cooperate with LDAP-based directory servers or other authentication services.

Also, a request to authenticate a user must not necessarily enter nevisAuth via nevisProxy. nevisAuth provides several other interfaces (APIs), such as the RADIUS or the WS-Trust API, to integrate VPN gateways or specific Microsoft services.

Additionally, nevisAuth supports other token formats besides NEVIS' proprietary SecToken, such as the SAML assertion, the X509 user certificate or the JWT claim (OpenID Connect). Thus, nevisAuth enables identity federations with external networks or security domains.

Main features

- Modular and customizable setup
- Support of a wide range of authentication methods, such as user name/password authentication, X.509 client certificates, security questions, challenge/response procedures, one-time passwords
- Integration of identity federation protocols, such as SAML2, WS-Federation and OpenID Connect
- Support of various token formats, e.g., SAML assertion, the X509 user certificate or the JWT claim (OpenID Connect)
- Availability of flexible interfaces, such as RADIUS and the WS-Trust facade, to easily integrate external systems
- Possibility to create realms/domains in order to enable single sign-on
- Dynamic adjustment/upgrade of authentication strength to improve security
- Facility to include user roles and permissions to establish a detailed and fine-grained authentication system

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