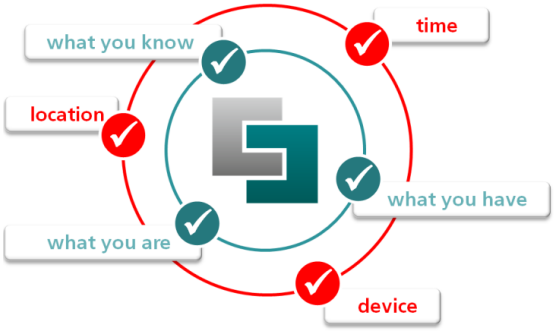
nevisAuth – Adaptive Context-Aware Authentication Plug-In

Benefits

The adaptive context-aware authentication (ACAA) plug-in of nevisAuth uses behavioral context data to decide how to authenticate a user during login. Thus, the ACAA plug-in at the same time **enhances security** and **increases usability** of your system. The plug-in enhances security by preventing unauthorized end users or unknown client devices from accessing your corporate data. It increases usability by allowing selective use of strong authentication.



What is it about?

As of Q3/Q4 2016, nevisAuth supports context-aware authentication. By means of the adaptive context-aware authentication (ACAA) plug-in, NEVIS can decide whether to grant a user access to an application based on the user's context data.

Context-aware security is "the use of supplemental information to improve security decisions at the time they are made, resulting in more accurate security decisions capable of supporting dynamic business and IT environments" (Gartner IT Glossary).
The goal is to prevent unauthorized end users or unknown client devices from accessing your corporate data.

To decide whether the login of a certain user is trustworthy, the ACAA plug-in makes use of user login profiles based on behavioral context data. During a login attempt, the plug-in compares the established login profile of the user with the context data of the user's actual login.

Currently, the ACAA plug-in considers the login time, the client device as well as the location (country) from which the user logs in. Depending on the discrepancy between the user's current login characteristics and the established profile, the plug-in decides how to continue with the authentication process.

For example: User X normally logs in between 8 and 9 in the morning, always using the same private device that is well-known by NEVIS, from a location somewhere in Zurich, Switzerland. If this user suddenly tries to log in from Belgium at midnight, the ACAA plug-in will recognize this login as being abnormal (or anomalistic), and reacts accordingly.

Context-aware authentication is an effective means against threats such as credential theft. In case of credential theft, the attacker uses stolen username/password combinations, smartcards, tokens, smartphones, etc., to get unauthorized access to applications. Because the attacker tries to log in with the credentials of an authorized user, the system may not identify this login as malicious. Context-aware authentication helps you to detect such evil invasions, since it recognizes all context-related abnormalities and peculiarities that accompany the attacker's login.

Main features

The ACAA plug-in offers the following features:

- Long-term storage of user behavioral context data (in the form of login profiles).
- Dynamic adaptation of the plug-in to the user's environment, also over time, by continuously storing context data in the long-term storage after every successful login of the user.
- Possibility to ramp up the plug-in before starting to trigger additional authentication mechanisms, in order to avoid an overreaction in the initial production phase.
- An "emergency stop" to avoid overreaction in the enforcement phase.
- Support of both passive and active reactions to risky logins. Passive means that the user is not aware of the reaction. E.g., nevisAuth sends a warning via e-mail to the system administrator. Active means: The user is involved in the reaction. E.g., nevisAuth asks the user to solve a CAPTCHA.
- Multiple options to dynamically configure the plug-in (without having to restart nevisAuth):
  - Risk weight for each type of context data.
  - Anomaly scores for each deviation from the established context information.
  - The next step in the authentication process, based on the risk score.
- Possibility to integrate the findings of the ACAA plug-in in nevisReports' dashboards and reports.

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