

nevisIDM – Identity Management

Teaser

The NEVIS identity management solution nevisIDM offers a flexible, customizable and centralized management of users, applications, roles and permissions.

Benefits

nevisIDM manages the users, roles and permissions of your business applications in a centralized way. This **central control and administration of data** makes your system **more secure** and **reduces costs**. It also paves the way for a **company-wide single sign-on**. Together with the support for a broad range of user credentials, the **implementation of strong authentication mechanisms** is possible.

The sophisticated data model enables a **fine-grained authorization concept** that supports the separation of powers and thus **enhances the security of your system**. The additional nevisWorkflow component further facilitates the division of tasks. It also gives your users the possibility of self-service, e.g., to reset their passwords or view their profiles themselves.

The full audit trail allows for **complete traceability of all user actions**, which helps **fulfill compliance requirements**. An additional feature is the ability of nevisIDM to **handle multi-tenant setups with completely separated user groups**. As such, you need only one identity management solution to cover several user populations at once.

What is it about?

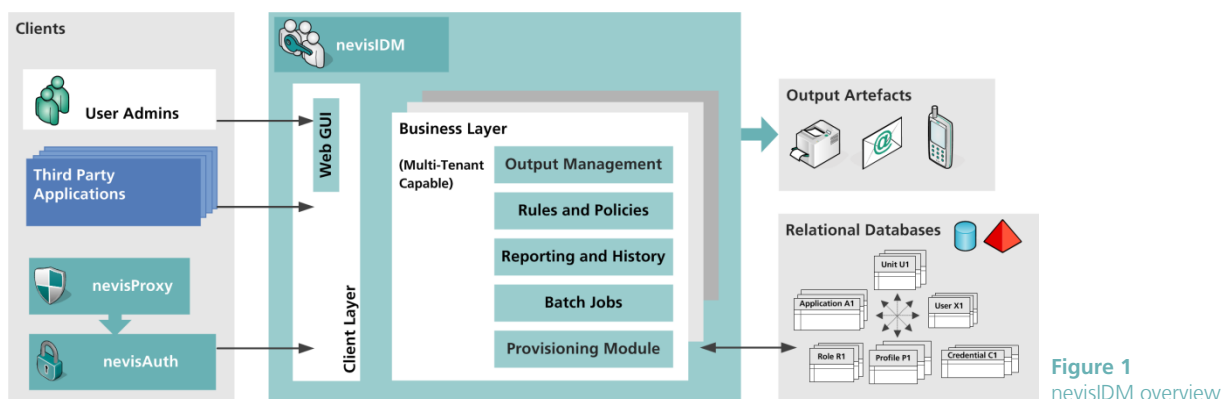


Figure 1
nevisIDM overview

Identity Management (IM) describes the management of individual identities, their authentication, authorization, roles and privileges within or across system and enterprise boundaries. The goal of identity management is to increase security and productivity while decreasing costs, downtime, and repetitive tasks.

Together with nevisProxy and nevisAuth, nevisIDM enables the implementation of a highly sophisticated, state-of-the-art identity and access management system. Within this system, *nevisProxy* builds one single point of access to your business applications in the back end and as such controls all incoming and outgoing HTTP traffic. *nevisAuth* takes care of the user identification and authentication. This is where nevisIDM comes in: it offers all the information that nevisAuth needs to identify and authenticate the user. This also includes user

authorization: assigning users the correct permissions and roles they need to be able to work with the desired application.

nevisIDM contains all processes and supporting tools required to manage your application and user data, including roles and permissions. The product can deal with a wide range of user credentials, such as (one-time) passwords, certificates, URL tickets, security questions, mTAN or Kerberos. This makes it possible to use strong authentication mechanisms for your business applications.

nevisIDM stores all user and application data in a reliable database based on a sophisticated data model. This data model defines all available data entities with their attributes as well as the relations between the entities. You can use a bundled, or your own database facility for the data storage.

Additionally, nevisIDM supports the provisioning of user data to external data storages such as LDAP directories.

The application's web layer provides the necessary interfaces to create and update the data. These interfaces support, among others, the Simple Object Access Protocol (SOAP) to exchange information

with (third-party) applications. Support of Representational State Transfers (REST) is coming soon. It is already possible to perform full-text searches by means of the Query REST Service.

The access control functionality in the business core layer guarantees that the user can only perform operations for which he is authorized.

Web user interface

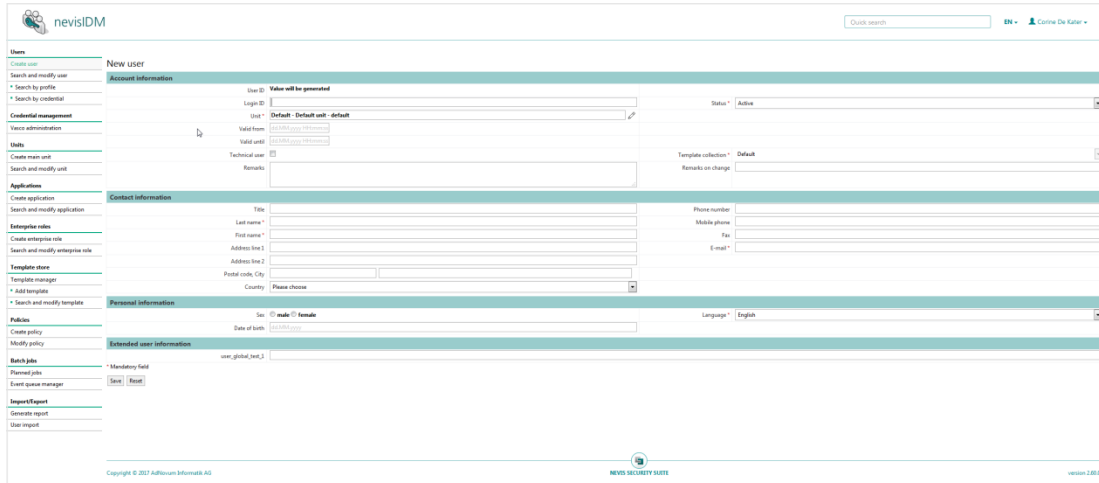


Figure 2
nevisIDM
web application

By means of nevisIDM's powerful graphical user interface, application administrators can manage the entities within nevisIDM. This includes not only the creation and modification of user and application entities, but a number of other features:

- The *Unit* entities help you shape the management of user data according to your organization's structure. This facilitates the assignment of roles and permissions and enables the delegation of user administration.
- The possibility of specifying credential policies allows for a fine-grained authentication system. You could, for example, determine a *simple password* policy and a *strong password* policy, with different requirements regarding the length of the password, the used characters, the allowed number of resets, and so on. Which of the two

password policies is valid for an application in the back end depends on the application's requirements regarding security.

- Customizable mail- and SMS templates enable you to notify users if, e.g., a password reset is due. If set accordingly, messages in several languages can be created.
- The search field facilitates full-text searches through all User, Application, Unit and Client entities stored within nevisIDM.

The web GUI also provides a self-administration facility, allowing the users of your application(s) to view their profiles or change their passwords themselves.

If desired, you can adjust the look of the web interface to your company's corporate design in regard to the (background) colors, fonts and logos.

Other features

- Remote administration via the web interface.
- Implementation of your authorization concept via user associations with profiles and roles.
- Implementation of complex processes by means of a workflow engine (nevisWorkflow).
- Bulk import of user data via Excel files.
- Powerful output management (mail, SMS, letters).
- Facilitates auditability with versioned storage of documents and security relevant events. All access rights are fully auditable at any time.