

Strong User Authentication for Corporate Networks without the Need for Expensive Hardware

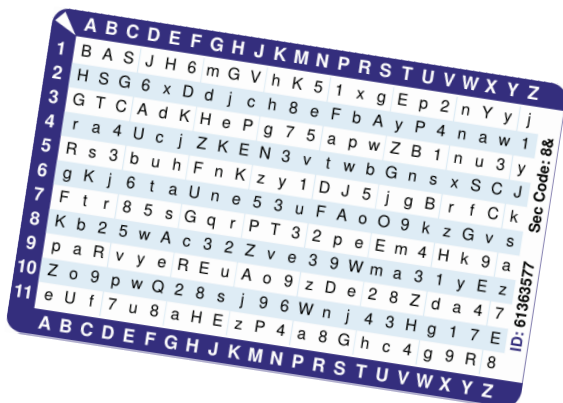
What is SAVERNOVA Network ID?

SAVERNOVA Network ID is a client-server application with its own administration console. The console and associated SQL database and services are installed on a Windows domain controller.

User information is retrieved from Active Directory. In the administration console, the administrator determines the security level for each user individually or for user groups. Each active user is stored in encrypted form in the SQL database along with his password card and secret reading method. No information on this is stored in Active Directory nor is Active Directory modified in any way.

How does it work?

Step 1: The user activates his own unique password card and defines his secret reading method. This user data is stored in encrypted form in SAVERNOVA Network ID along with the virtual copy of the card. This data is not accessible to the administrator.



Step 2: Every time the user logs onto the network, he is given a unique starting point on his password card. Starting in this point, the user must apply his secret reading method. Immediately after typing the password from the given starting point, the correct and only possible password is stored in Active Directory and the user is registered.

network ID

Server Components

Administration console

- Administration tool for defining and implementing a security policy using the SavernoVA password card
- Application of the security policy to different users and groups retrieved from Active Directory
- Import, overview and administration of virtual cards
- Configuration of general settings for the entire software

Database

- MS SQL database
- Stores the individual settings and user profile with an active card, reading method and number of starting points
- All information is stored in encrypted form

NIM service

- Communication with the database and Active Directory
- Upon request, sends the starting point to the client with SN-Gina installed

SN-Gina (Windows logon)

- Replaces the normal Windows logon
- Gives the user the starting point from which to apply his secret reading method when he logs on
- Activates the SN password card and creates a user profile
- Displays general company or administrator information to the user before he reaches his desktop.

How the programme works

Once the server and client components have been installed, the card file supplied by Savernova is installed in the software. This file contains all the SN password cards available for the given licence.

Via the administration console, individual users or entire organisational groups from Active Directory may be enabled to use a SAVERNOVA password card. The users are then assigned to various security groups, in which various security levels may be set for use of the SN password card (e.g. card displayed during logon or printed card required; number of possible logons with a single card; period of validity of the card etc.)

After all the various settings have been made, the user is prompted, when he first logs on, to activate his card and choose a secret reading method.

Once he has completed this procedure, the Windows logon takes place and the user reaches his desktop.

From this moment on, every time the user logs on, he must apply his secret reading method from the given starting point on his SN password card and enter the corresponding password.

Companies today protect themselves very well against external threats. However, many are unaware that around 70% of attacks are carried out by their own employees.

Contact

Savernova Ltd
info@savernova.com

Technical description of the components

Administration console

- Software administration console
- All information, settings and virtual cards are retrieved from the SQL database
- The user overview shows only one visual import from AD

Database

- Microsoft SQL database (works with SQL Server or SQL Express)
- Only when a user is enabled to use the SN password card is he registered in the database
- The content of the card and the user's secret reading method are stored in encrypted form in the database
- The administrator does not have access to the user's chosen reading method

NIM service

- Service installed in Windows Services
- Must be installed on a domain controller
- Communicates with the SQL database
- Sends a unique starting point to the client requesting it
- Compares the password in Active Directory with the password entered by the user using the password card

SN-Gina

- Installed on client PCs (Windows 2000/XP Pro)
- Changes the Windows logon on the client
- Communicates via SSL with the NIM service on the domain controller