Authentication methods

This article describes authentication methods available in Nexus Hybrid Access Gateway. Authentication methods are used as requirements in access rules for authentication. Different authentication methods provide various levels of security.

How does authentication work?

When a user uses a web browser to access a resource, the request flows through a web of specialized services: the access point, the policy service, the authentication service, and back again. But for the user, the single point of contact is the web browser. The access point verifies the identity of the user by forwarding the user credentials via the policy service to the authentication service, which in turn compares the information with credentials stored in the user storage. When the control is completed, a request accept is sent to the access point which allows the user to enter.

What authentication methods are supported?

Hybrid Access Gateway supports many authentication methods. Some of the most common ones are listed below.

To choose the right authentication method for your business, consider your users’ needs when it comes to mobility, device flexibility and level of security. It is possible to specify multiple authentication methods for each resource.

Some common authentication methods

For a complete list, see the user interface in Hybrid Access Gateway admin interface.

Expand/Collapse All

Nexus Personal Mobile

Nexus Personal Mobile is a mobile app that makes two-factor authentication (2FA) easier and more cost efficient. It is used together with the Nexus Personal Service that is consumed by, for example, Nexus Hybrid Access Gateway, which provides user authentication and access to applications, information and cloud services.

Read more...

Nexus Personal Desktop

Nexus Personal Desktop is a smart card middleware integrating smart cards and security tokens and provides your users with intuitive two-factor authentication (2FA), digital signing, email encryption etc.

Read more...

OpenID Connect

OpenID Connect is a federation technology, comparable with SAML 2.0, that is implemented as an identity layer on top of the OAuth 2.0 protocol.

Several digital identities, such as Norwegian BankID and Verimi, are based on OpenID Connect.

Related information

- Set up authentication method
- Access point, add, set up and configure
- Access rules
- Authentication service, add, set up and configure
- Policy service, add, set up and configure
- Resources
- User storage

Read more...

Nexus TruID

Nexus TruID is a mobile two-factor (2FA) software token that is installed on a hardware device that the user already has, such as a smart phone, PC (Linux/Windows) or a Mac. The user enters a pin code into the soft token to generate a one-time password, OTP. This OTP is used to logon to the application or service.

Read more...

Nexus Mobile Text

Nexus Mobile Text uses the mobile phone and a mobile text-distribution service such as SMS to distribute the one-time password. By using SMS, any mobile phone can be used for this two-factor authentication (2FA) method, and smart phones are not required.

Read more...

Nexus Invisible Token

The Nexus Invisible Token is a unique on-demand solution that combines the strength of passwords and tokens for two-factor authentication (2FA). It is secure, convenient, easy to deploy, and most importantly easy to use. Invisible Token is based on HTML5 and transforms your browser into an OTP-token that is independent of the platform you are using.

Read more...

Nexus OATH

With Nexus Hybrid Access Gateway Authentication Server, any OATH (Open Authentication) compliant software or hardware security token may be used to provide user authentication. OATH provides an open architecture enabling customers to replace disparate and proprietary security solutions to increase flexibility.

Read more...

Nexus Password

Nexus Password can be used for environments with lower security demands.

Read more...

Swedish national eID - BankID and Mobile BankID

Nexus Hybrid Access Gatway support authentication using the Swedish national eID BankID. With Hybrid Access Gateway you can let your users authenticate with BankID on smartcard, file or by using a smartphone with Mobile BankID. There are multiple ways to connect Hybrid Access Gateway to the service for validation of BankID and Mobile BankID. By using a national eID such as BankID you can easily and securely enable your services for a large number of customers without the burden of managing their credentials and authentication methods.

Read more...

Freja eID

Freja eID is an electronic identity on your mobile device that allows you to log in, sign and approve transactions and agreements with your fingerprint or PIN. With Freja eID+, you will get an eID officially approved by the Swedish authority DIGG with the quality mark Svensk e-legitimation. You can configure Hybrid Access Gateway to only accept Freja eID+.

Read more...