NetIQ Access Management

NetIQ Access Platform Capabilities

Single Sign-on – SSO minimizes disruption to your users by allowing them to log in just once to gain access to all their applications, services, and resources across all of your environments, both cloud and legacy. This allows you to optimize the access experience for your employees and consumers. This simplified experience also allows you to increase your security without sacrificing user satisfaction.

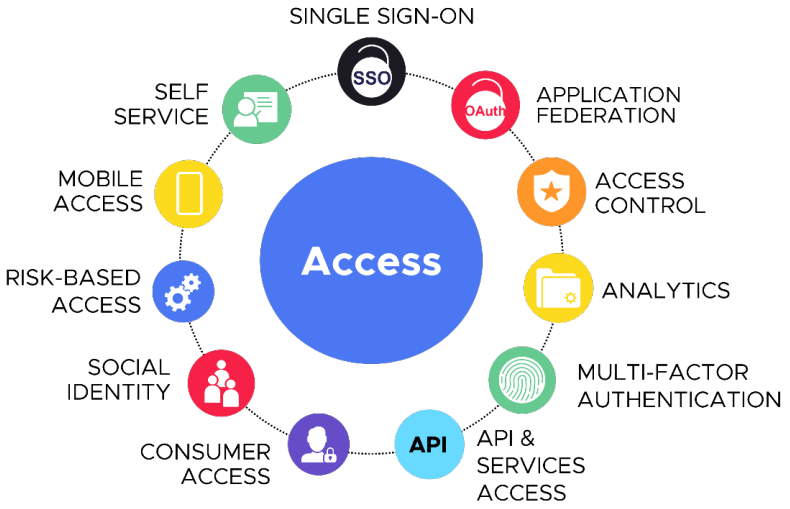
Passwordless authentication – Protect against the number one attack method against passwords (phishing) while providing a user-friendly approach to verifying claimed identities with passwordless authentication. NetIQ's integration framework provides an extensive set of different methods so that you can offer your users the right authentication that fits their situation.

Multi-factor authentication – the NetIQ authentication framework allows you to use different authentication types (what you know, have, or are) to raise confidence that users are who they say they are. You can implement simple 2FA up to chained MFA methods based on the risk at hand. Beyond the traditional MFA methods used, for those focused on optimizing their user's experience, Advanced Authentication offers a variety of passive authentication options.

Secure web service delivery – The NetIQ access gateway does more than just access control. It can bring together disparate web services together into a simplified or single-user experience when needed. Your web-based resources don't need to have their own access security infrastructure for the gateway to invoke corporate access security policies on them. The gateway works equally well for cloud-based or legacy services as well as traditional, OIDC, or other federated credentials.

Self-service onboarding and credential management – Allow users to onboard their identities into your environment using their social credentials or some other trusted IdP. Graduate user identities from social to verified based on the level of risk of the information they store or access. Offer users self-service credential management when users get locked out. NetIQ offers advanced identity and credential management capabilities at scale needed for B2C, G2C, and other large environments.

Comprehensive Platform



API access management – extends your access and authentication environment to include secure API delivery for all your secure integration needs. NetIQ Secure API Manager is an essential core component for your access security layer.

Recognizing high risk access – effectively measure risk according to your security policies based on a user's contextual information about their location and device. Additionally, identify risk beyond your security blind spots using powerful behavior heuristics.

Inherent risk of protected resources – feed resource risk information onboarded on to NetIQ Identity Governance catalog into the Risk Service for a more accurate view of the potential risk at hand.

Continuous authentication and authorization – Adaptive access management goes beyond invoking a multi-factor authentication at the beginning of a session. But instead initiates additional actions as needed when risk thresholds have been crossed at any time within a session. This dynamic approach to access management empowers organizations to deliver the best user experience while raising security levels when needed.

NetIQ Access Management

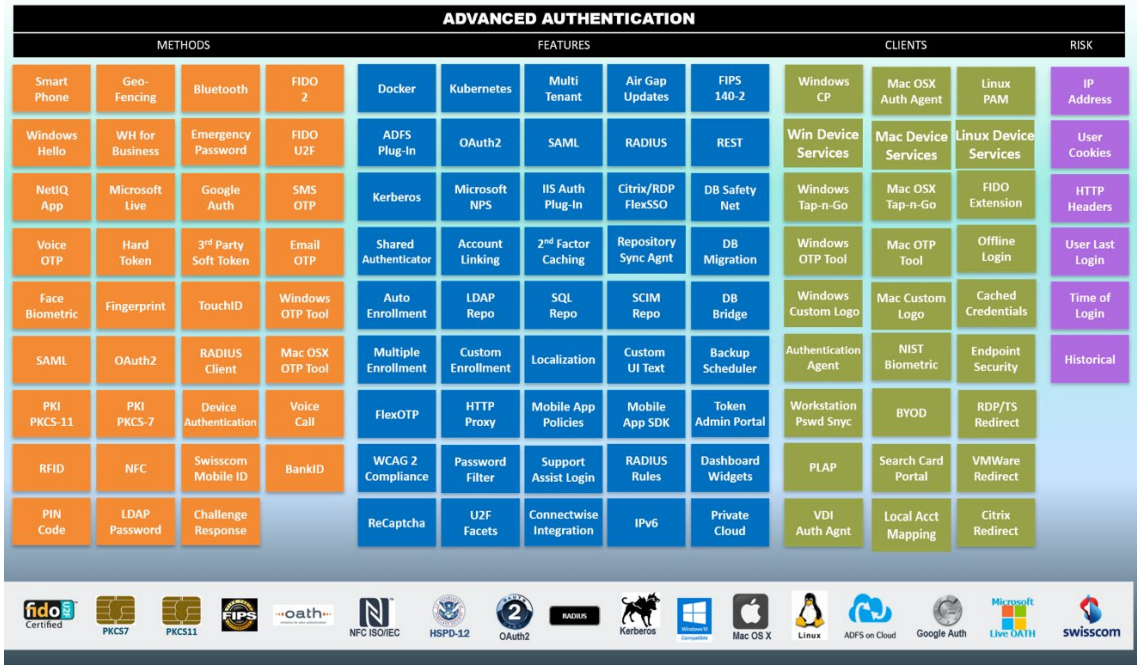
NetIQ by opentext™

Why having the Best Authentication Framework Matters

As authentication technologies advance, the way organizations leverage them will continue to diversify. Giving users more authentication options allow them to enroll in the types they're most comfortable with. You may also find that in your quest to drive down friction of digital interactions, multiple passive authentications are needed in place of a disruptive one. The more options you can access, the greater your flexibility in applying them.

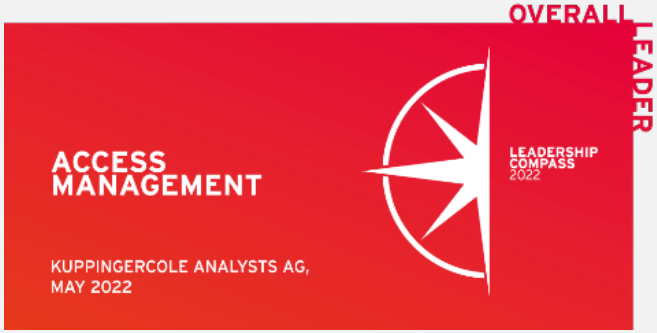
If you're like other organizations, you have multiple authentication infrastructures across different parts of your business. These siloed environments raise your administration costs and create space for disjointed authentication policies. The exposure is greatest when users leave or changes roles. The best way to maintain consistency during these changes is to have a single library of authentication policies to apply.

Comprehensive Library of Authentication Methods



NetIQ is an Overall Leader

Analyst firm KuppingerCole names NetIQ (as Micro Focus) an Overall Leader for Access Management.



OpenText has completed the purchase of Micro Focus, including CyberRes.

Trusted by some of the largest deployments in the world for Workforce, B2B, and B2C.

vodacom · BANCOMEXT · helvetia · VINCI ENERGIES · Carante Groep · ELKJOP · ARCOR · Medica

More Info

- NetIQ Unplugged YouTube Channel: https://www.youtube.com/c/NetIQUnplugged
- Website: NetIQ home page
- Community: Join the conversation