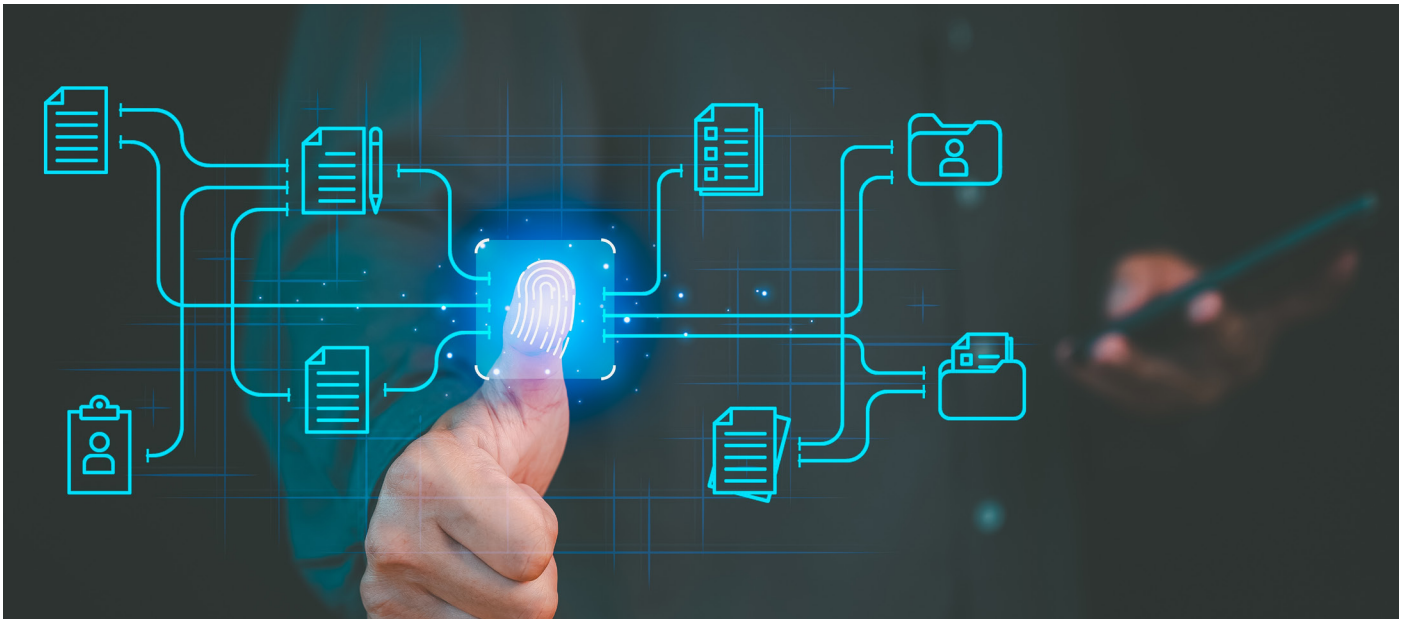
OpenText NetIQ Advanced Authentication

Enable passwordless and multi-factor authentication for simple, organization-wide protection



Benefits

- **Protect** against phishing
- **Eliminate** uneven authentication policies
- **Enhance** Microsoft Active Directory® and Entra® ID authentication
- **Avoid** vendor lock-in

If you're like many other organizations, your security infrastructure likely has a variety of disparate authentication techniques, including any number and combinations of IDs and passwords, building access badges, challenge-response phrases, and PINs.

OpenText™ NetIQ Advanced Authentication lets you centralize all of that, making it easier for you to deliver a strong level of authentication (multi-factor or other passwordless implementations) to meet regulatory and internal security requirements. It gives organizations the flexibility they need to tailor their security levels and user experience to meet their specific needs.

Modernize your authentication to be more adaptive to risk. Consolidate your authentication silos into one set of application integrations and authentication policies.

Protect against phishing

Cyberthieves are well aware that users choose the same passwords across multiple platforms and services, including transversing them from their personal accounts into their professional ones. While user security training helps, the stronger protection is implementing multi-factor authentication and other passwordless technologies, such as fingerprint or facial recognition, that create a unique token. This same approach can be applied to system and data administrators, who create the greatest risk to an organization due to their high level of permissions. If their credential is hacked, the outsider has the greatest amount of access.

"Leveraging Access and Identity Manager and Advanced Authentication, we quickly secured VPN remote access for everyone who needed it, across both on-premises and cloud-based applications."

José Luis Rodríguez
COO and Co-Founder of ITechGrup

Eliminate uneven authentication policies

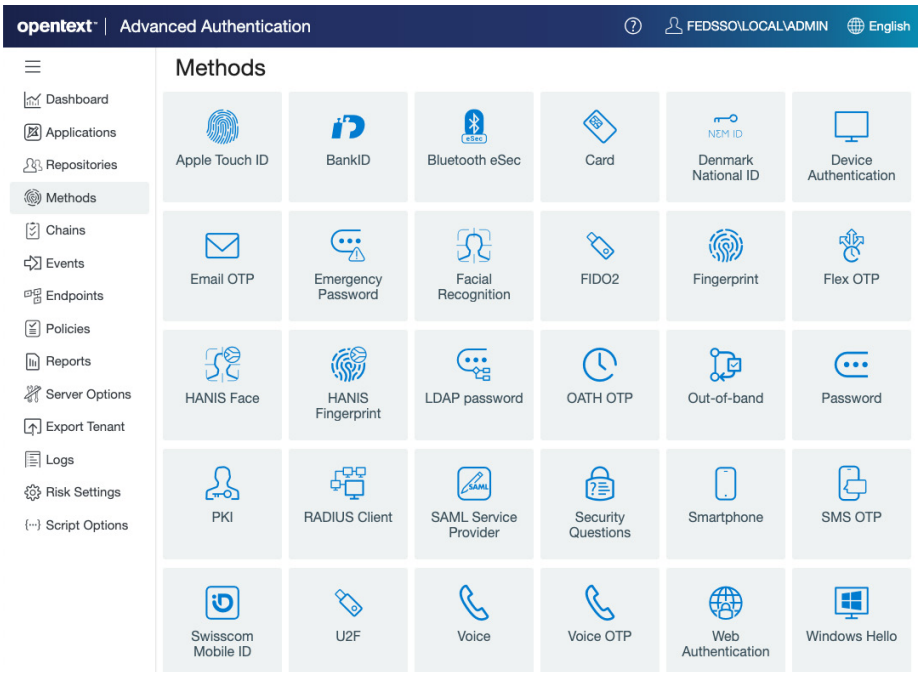
Authentication silos built up over time as tactical deployments multiply your exposure to unwanted outsiders breaching your digital environment's security. Advanced Authentication allows you to centralize your authentication into a single framework where you can manage them with a single policy console, not just increasing security but decreasing administration costs. We provide wide integration capabilities and the latest authentication methods and devices, making it easier to consolidate your silos into a single authentication framework.

Enhance Microsoft Active Directory® and Entra® ID authentication

Entra ID continues to grow as organizations expand their adoption of Microsoft Enterprise solutions, as well as other services that use Active Directory and Entra ID as its data repository. It is important to update the strength of your authentication to match the risk of these offerings. Advanced Authentication protects access to your environment through consolidation and integration across all identity stores in a way that is easy for users to consume. Its added method flexibility allows organizations to offer authentication options that best fit the user. So, regardless of whether your applications are running on-premises or in a cloud environment, Advanced Authentication can strengthen your ADFS-centric systems from unauthorized access.

Avoid vendor lock-in

CTOs and architects have long understood the benefits of open standards. Standards are foundational to achieving interoperability between application and platform independence, as well as foundational to maintaining long-term architecture integrity. However, when an organization implements an authentication solution built on proprietary protocols, they no longer have the freedom to shop across the industry for the devices that best fit their needs at the best price. OpenText also supports FIDO (Fast Identity Online) Alliance. FIDO U2F (Universal 2nd Factor) enables organizations to support an environment where users manage their own authentication devices. FIDO2 combines the W3C's Web Authentication (WebAuthn) specification and the FIDO Client to Authenticator Protocol (CTAP) to enable passwordless authentications across websites and apps using public-key cryptography.



OpenText authentication framework offers a robust set of integrations and interfaces.

Resources

Cybersecurity blog: The State of Passwordless Authentication

Read the blog ›

OpenText NetIQ Advanced Authentication

Watch the video ›

Remote Work Security Infographic

Read the infographic ›

Rather than use the management software that comes with your authentication appliances, OpenText protects you from authentication silos. You will gain greater security by enforcing consistent authentication policies and your administration overhead will go down as well. The OpenText authentication framework is designed to be your single integration point for all your applications and methods.

Unlike competing products, OpenText offers client-specific strong authentication clients for Windows®, Mac OS®, Linux®, and mobile. The mobile client allows geofencing-based authentication; meaning, when security administrators can leverage the user's GPS location, or other risk-based metrics, to help determine the authentication strength that they should enforce.

Product features	Description
Standards-based integration	Centralize your application and authentication into a single framework – HSPD11, PKI12, OAuth, FIDO, OATH, RADIUS, FIPS 140, NFC ISO/IEC and others). Also support for some proprietary solutions.
Geo-fencing	You may be familiar with IP based GeoLocation. We have taken this to a new level, using global positioning (GPS) technology. Our Geo-Fencing allows authentication policies based on a user's specific location (such as a building or campus).
Mobile offline login	Travelers on-the-go required to perform second-factor authentication can now do so anytime they need, even without connectivity.
FIPS 140-2 inside	National Institute of Standards (NIST)x` Federal Information Processing Standard (FIPS) 140-2 encryption.
Built-in, risk-based authentication	Built-in, risk-based authentication engine provides risk scoring to authentication type based on score.
Helpdesk module	Provides the capabilities to ensure a good end-to-end customer experience (enroll, re-enroll, token assignment emergency password, etc.).
Mobile SDKs for iOS and Android	APIs and tools for native iOS and Android authentication services.

Copyright © 2026 Open Text • 05.26 | 240-000103-002

opentext™