OpenText NetIQ Advanced Authentication for Your Business

Implementing an authentication framework has the power to drive down costs, increase security, and offer more authentication options across your organization.

NetIQ Advanced Authentication at a Glance

- A single framework for all your authentication needs
- Provides mix-and-match authentication method chaining flexibility
- Supports a broad variety of integrations: RADIUS, VPN, OpenID, OATH, FIDO, RACF Windows, Mac OS, Linux, Citrix, VMware, etc.

Standards-Based Authentication Framework

In today's connected world, fraught with persistent cyberthreats, authentication strategies have become a core component of protecting against them. These initiatives, typically driven by risk management and government mandates, are usually driven by specific business requirements where identity verification is both simple and strong.

When done right, authentication can:

- Contribute to or cement customer trust, where they feel digitally secure interacting with organizations.
- Make organizations easy to do business with by providing identity verification that is highly resistant to breaches while minimizing inconvenience or friction for their users.
- Be part of a services architecture designed to simplify and optimize business processes, regardless of where the employee, contractor, or partner is located.

Single sign-on continues to be an essential element of convenient access, adding even more dependence on strong authentication for security.

Why a Framework?

Because new authentication purchases typically originate within a business unit, they are often solved from a specific tactical perspective. This approach leaves organizations with multiple authentication silos (building access, remote access,

compliance requirements, etc.). These disjointed implementations impose higher administrative overhead and inefficient processes. But, more importantly, they create vulnerabilities due to inconsistent authentication policies.

In short, authentication frameworks have the power to:

- Drive down costs through consolidation.
- Increase security through one universal library of policies.
- Offer more authentication options across the organization.

It's not easy building a framework that can meet the broad set of organizational needs. For example:

- It must offer simplicity of deployment and administration for small organizations, while meeting the scalability requirements of large ones.
- It needs to be moldable to the shape of the organization, whether it's concentrated within a specific region or is highly distributed across the globe. Regardless of the shape of the organization, the framework must deliver quick response to authentication requests.
- The more methods a framework can support, the more flexibility organizations will have as they consolidate their authentication silos into one. The framework must also be able to easily expand as new authentication technologies are introduced into the market.

Standards-Based Open Architecture

CTOs and architects have long understood the benefits of open standards. The intrinsic interoperability offers application and platform independence, as well as 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. They are also subject to vendor lock-in.

The Cybersecurity line of business from OpenText™ is a member and strong supporter of the FIDO (Fast Identity Online) Alliance. FIDO U2F (Universal 2nd Factor) enables organizations to support an environment where users manage their own authentication devices. OpenText™ NetIQ™ Advanced Authentication provides a solid framework to deliver that support to your applications without the need for development. Not only do you benefit from deferring token costs, but your users are able to incorporate a higher level of security across other aspects of their digital life.

With the deep level of support provided by NetIQ Advanced Authentication, there is no better framework from which to provide a U2F authentication environment:

- FIPS 140.2 ready
- OAuth2 integration
- OATH authentication
- Google Authenticator
- Microsoft OATH
- Support NFC ISO/IEC
- RADIUS integration
- Kerberos integration
- Support for PKSCS7 & PKCS11

IT groups should be cautious about selecting solutions that offer minimal support for today's modern authentication standards.

Maximum Application Coverage with the Most Native Methods

Beyond the authentication types available in RADIUS, NetIQ Advanced Authentication offers more native methods than any other solution on the market. Why does that matter? Because both your internal and external users access sensitive information from a wide range of situations and from multiple devices. With its collection of ready-to-go application integrations (RADIUS, OpenID, OATH, FIDO, RACF, z/OS, Windows, Mac OS, Linux, Citrix, VMware, and more), NetIQ Advanced Authentication offers wide applicability for your environment. In addition, its broad support for a variety of authentication readers and methods provides a new level of flexibility.

SaaS, Docker, or Appliance—No Compromises on Any Platform

The NetIQ Advanced Authentication framework is designed for high availability and internal load balancing for continuous uninterrupted operations, regardless of how large or small your environment. Replication between primary and secondary servers provides data integrity and disaster recovery (over LAN or WAN).

NetIQ Advanced Authentication is available in multiple form factors:

- Traditional on premises
- Soft appliance
- Docker containers
- Software-as-a-service provided directly from OpenText

Simplicity of the Appliance

The NetIQ Advanced Authentication soft appliance edition is the perfect fit for SMB environments. With all of its components consolidated into a single package,the appliance eliminates many of the configuration tasks that are otherwise required. Just load the virtual image and it’s ready to go. Additionally, because the appliance is a condensed, hardened virtual appliance environment, it does just what is needed and no more. This protects it from the exposure of unwanted and unneeded services that could be exploited by hackers or malware. For many, it’s the best option for those who don’t have Docker experience.

Docker Containers for Manageability

As organizations continue to evolve their architecture across complex hybrid environments, ease of application deployment and distribution is more important than ever. That’s why NetIQ Advanced Authentication is now available as Docker containers. Because all of the dependencies are bundled into a small set of Docker containers, they can be transferred as needed without any compatibility issues. And it’s that ability to avoid compatibility issues that makes Docker containers a form factor of choice for cloud environments such as Amazon Web Services (AWS). Deployed as containers, NetIQ Advanced Authentication can run on top of a variety of virtualization, hypervisor, and cloud-based technologies that best fit your needs. You can also configure it in specialized models optimized for performance or availability (with version 6 and later).

Strong Authentication for Your Office 365 and Azure Environments

Active Directory Federation Services (ADFS) continues to grow as organizations migrate to Office 365 and Microsoft's Azure platforms. It is important to update the strength of your authentication to match the risk of these offerings. NetIQ Advanced Authentication protects access to your environment through consolidation and integration in a way that is easy for users to consume, while providing a higher level of user verification through MFA (multi-factor authentication). This means, regardless of whether your applications are running on premises or in a cloud environment, NetIQ Advanced Authentication can strengthen your ADFS-centric systems from unauthorized access.

The Best Framework for Your Passwordless Strategy

While passwordless solutions have been available for decades, both cost and complexity of implementation have created barriers to widespread adoption. However, in recent years, we've seen a shift in the market. The incorporation of smartphones for both business and pleasure have made fingerprint readers commonplace. Similarly, mobile apps that use the smartphone's camera for eye scans are also gaining traction.

But the biggest boost to passwordless technologies has been the ubiquitous push for multi-factor authentication. A variety of government mandates across key industries have forced organizations to onboard authentication technologies that go beyond passwords. The authentication market continues to evolve as organizations keep a constant lookout for technologies that lower user friction as they access protected resources.

Support for Almost Any Authentication Type

In addition to multi-factor authentication, these same passwordless technologies (what you are, what you have, and even what you are doing) are also strong options for single-factor authentication. They are highly resistant to phishing—the weapon of choice for criminals to hack credentials. Different types of authentication include card, biometric, Bluetooth, behavioral (such as typing, gesture, and others), etc. The passwordless authentication market currently stands at around $35B, but is forecast to grow over twelve-fold to $450B by 2030[1]. As such, a framework that is designed to handle a broad variety of authentication needs—now and into the future—protects your investment.

As you evolve your organization's identity verification strategy, it's good to know that OpenText is aggressively incorporating new methods into our offerings to support emerging technologies as they come onto the market.

Offers the Most Flexibility for Zero Trust Environments

When applying zero trust to an environment from an identity perspective at the application layer, key capabilities are continuous authentication and authorization:[2]

- Continuous authentication is the ability to re-verify an identity as many times as needed in response to a risk score that has spiked within a session. Depending on the strength of the method, one or more successful authentications might be needed to lower the risk score.
- In response to a rise in risk score at any time within a session, an access request is subject to potential restriction, or even a termination.

1 www.nextmsc.com/report/passwordless-authentication-market
2 https://community.opentext.com/cybersec/b/cybersecurity-blog/posts/achieving-zero-trust-without-driving-your-users-crazy

> **"Even when you can't solve your authentication "Even when you can't solve your authentication."**
>
> Senior Director of a specialized security deployment team

The more methods that security and IT teams have at their disposal (especially passive ones), the better able they are to design a zero trust environment that doesn't slow down their workforce. This same model can be applied to B2B, B2C, or G2C interactions where highly sensitive information is being protected. In addition, several passive authentication methods could possibly be chained together to equal the strength of a highly disruptive one. Passwordless authentication has the power to be much more than a play for convenience—it can increase security as well.

NetIQ Advanced Authentication Teleworkers

Organizations have long faced the challenge of securing remote users who are accessing highly sensitive information. These have typically been personae such as road warriors, finance professionals, executives, and those who access regulated data. However, the pandemic dramatically accelerated an already growing trend of teleworkers. So, the teleworkers that used to be a relatively small subset of the workforce has, for many, spread across the entire organization.

This evolution of the remote user model has changed fundamental authentication requirements:

- Now that the user count is much higher, it will be a primary factor in shortlisting options.
- The entire paradigm of user enrollment must change. More than ever, having remote access to simple self-service enrollment tools is a must; anything complicated will overrun IT's support capability.
- The cost overhead and security vulnerabilities of authentication are multiplied.
- Greater due diligence is needed to verify passwordless coverage of services and resources.

For organizations that haven't yet evolved their authentication approach from tactical to strategic, the accelerated teleworking trend will push them in that direction.

Why Us

With a consolidated MFA approach, NetIQ Advanced Authentication is less complex to configure and maintain than other solutions. Our strength also lies in out-of-the box integrations that provide a wealth of configurable authentication options. Your entire organization benefits from the increased security and usability. You also have the freedom to build new or replace and consolidate MFA infrastructures, enabling your organization to control costs and maximize investments. Lower costs and increased security are what make NetIQ Advanced Authentication a market-leading solution.

To learn more about the NetIQ Advanced Authentication framework, or to start a trial.

Check out our NetIQ Unplugged channel.

opentext™