opentext™ | Cybersecurity

Data Sheet

NetIQ Advanced Authentication

NetIQ Advanced Authentication gives organizations the flexibility they need to tailor the security and the user experience to the level of authentication needed. Your organization likely has a variety of techniques that are already used for security, any number and combinations of IDs and passwords, building access badges, challenge response phrases and PINs. All serve basic access needs. NetIQ Advanced Authentication framework adds the strong level of authentication (MFA or 2 Factor) you require to meet regulatory, industry and client forces.

Key Benefits

NetIQ Advanced Authentication by OpenText allows you to centralize your authentication into a single framework where you can manage them with a single policy console, decreasing costs and increasing security. We provide wide integration capabilities and the latest authentication methods and devices. This affords you the freedom to use the right security in the right scenario throughout your environment. With our open standards based solution, you can protect against security breaches while protecting against the risk of vendor lock-in. You choose the best option to use to fit your needs.

Authentication flexibility is more than just which methods are supported, platform support matters as well. NetIQ Advanced Authentication gives you the broadest platform coverage available with support for Windows, OS X, and Linux, iOS, Windows Mobile and Android.

All of this means that OpenText™ is committed to enabling you to shape NetIQ Advanced Authentication to fit your environment. Large organizations will appreciate NetIQ Advanced Authentication's ability to scale to the largest, more complicated environments, while small organizations will appreciate its simplicity.

Key Features

Multi-Site Support
We have you covered with support for organizations with geographically diverse and multi-site location requirements.

Multi-Tenant Support
If your organization has multiple divisions or business units with vastly different requirements, we support those individualized configurations.

High Availability: Redundancy and Load Balancing
Reliability and performance are ensured with our design for High Availability including internal load balancing and replication.

NetIQ Advanced Authentication for Active Directory Federation Services (ADFS)
IT security teams have the option to use NetIQ Advanced Authentication's ADFS plug-in to extend access to more methods and application integrations.

FIPS 140-2 Inside
We include National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 inside encryption so you can deploy with confidence.

Appliance Requirements

Minimum Configuration
- 2 Cores
- 2 GB RAM
- 40 GB disk space

Recommended Configuration
- 4 Cores
- 4 GB RAM
- 60 GB disk space

RADIUS Server
A RADIUS server is included in product. Currently only PAP validations are supported with it.

Client Components
- Windows Credential Provider, Linux PAM and MacOS Authentication Plug-In
- Microsoft Windows 7 (x64/x86) SP1/Microsoft Windows 8.1 (x64/x86)/Microsoft Windows 10 (x64/x86)
- Apple MacOS X 10.10.5
- Linux Pluggable Authentication Module (CentOS 7, SUSE Linux Enterprise Desktop 12, SUSE Linux Enterprise Server 12, Red Hat Enterprise Linux Client 7.2, or Red Hat Enterprise Linux Server 7.2)

Smartphone Application
- Apple iOS 8/ 9
- Google Android 4.2/ 4.3/ 4.4/ 5.1/ 6.0, with 3 mega pixels (or greater) camera with the autofocus function
- Windows Phone 8.1/ 10, with 3 mega pixels (or greater) camera with the autofocus function

Geo-Fencing
You may be familiar with IP based Geo-Location. 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).

2nd-Factor Skipping
If you need to balance speed-of-access with security needs. You can configure a grace period between authentications where a 2nd factor isn't required. The user is still required to fulfill the complete authentication requirement initially. Separately, your organization may choose to use NetIQ Access Manager by OpenText™'s risk based authentication engine to define when 2-factor authentication is required.

Mobile Workforce Support—Offline Login
Travelers on-the-go required to perform 2nd factor authentication to access private information can now do so anytime they need. Meaning, that even without connectivity users are able to get work done.

Broad Platform Support
We specialize in providing security across a broad number of platforms (Windows, OS X, Linux and Mobile). You can use many methods such as those based on iOS, Android and Windows Mobile along with RADIUS, cards and biometrics to authenticate.

Standards-Based Application Integration
Our solution is standards (HSPD11, PKI12, OAuth, FIDO, OATH, RADIUS, FIPS 140, NFC ISO/IEC and others) based. We support some proprietary solutions but we will always build based on providing you the highest flexibility.

Help Desk Module
Help Desk module provides the capabilities to ensure a good end-to-end customer experience (enroll, re-enroll, token assignment emergency password, etc.).

Emergency Password
What do you do when a user has no available enrolled authentication method? As a backup, when your users still need access, the Help Desk can generate an Emergency password for use.

External Proxy
HTTP Proxy provides flexible routing between the Internet and your authentication servers.

Support for Non-Domain Clients
Support for those users who have their own devices (BYOD) and are not part of your corporate domain. We do not limit your use of multi-factor authentication to just corporate devices by requiring domain membership.

On-Prem, Cloud, or SaaS
The authentication framework is offered as a portable Docker container that gives you the flexibility to incorporate throughout your environment in whatever form best fits your needs. The docker format allows the options between cloud, on-prem, or as a SaaS offering delivered by OpenText. All of these options work well for your cloud and hybrid environments. The Docker platform also allows you to leverage a mature and capable management toolset, making it the perfect platform for your configuration and maintenance needs. Our authentication framework is also offered as-a-Service which provides a fast, powerful way for you to incorporate passwordless authentication across your environment.

Connect with Us
www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.