NetIQ Access Manager

OpenText is a leading provider of web single sign-on solutions that deliver transparent, secure access to applications and services. Supporting federation standards, NetIQ Access Manager enables organizations to share private information across web, cloud and mobile securely and conveniently. Because granting secure access is more than just knowing who needs it, NetIQ Access Manager adapts to the right level of user identification based on measured risk to the business.

Product Overview

NetIQ Access Manager by OpenText delivers user single sign-on and secure access to intranet and cloud-based applications from wherever the user is located: the office, remote, on the road; or for consumers, from whatever device they are using. NetIQ Access Manager does this by supporting federation standards for today's modern applications and services while still keeping its best-of-breed gateway capabilities for everything else. In addition to single sign-on and access control, NetIQ Access Manager includes a built-in, risk-based engine and two-factor authentication, so organizations can keep access simple when risk is low and adapt user verification when risk is high or in between. It's designed to use less hardware, deploy faster, and require less maintenance, giving you faster time to value and lower cost of ownership.

For organizations that don't already have one, NetIQ Access Manager includes a customizable login page and mini application portal, so organizations can brand them as needed. The application icons are configurable and adapt to the form factor from which they are consumed, all of which requires minimal time and expertise. From beginning to end, NetIQ Access Manager is designed for simplicity and low cost of ownership.

Key Benefits

NetIQ Access Manager is the right fit for delivering single sign-on and secure access to web-based applications. With its rich set of features built right into the product and its simplified design and integration with other OpenText identity and access solutions, you can avoid complex and siloed configurations. NetIQ Access Manager empowers organizations to do more with less, delivering quick and convenient access for users while keeping private information secure. With NetIQ Access Manager, your organization can:

- Deliver secure access across the organization—NetIQ Access Manager is a full-featured access solution that delivers single sign-on for modern federated services that support SAML, WS-Federation, WS-Trust, OAuth and OpenID, as well as applications and services without federation support.

- Score quick wins for your mobile strategy— Whether you need single sign-on for your internally developed corporate mobile apps or for your legacy web apps, NetIQ Access Manager has the solution. It comes with an SDK that enables application federation for developers, as well as a mobile gateway that delivers one-touch access to legacy web apps on mobile form factors in just hours. Either way, you're able to implement identity and access control without touching your back-end applications.

System Requirements

Admin Console, Identity Server and Access Gateway Service
- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk
  - SUSE Linux Enterprise Server (SLES) 11 SP4

    Or
  - SLES 12 with 64-bit operating system x86-64 hardware (physical or virtual)

    Or
  - Red Hat Enterprise Linux (RHEL) 6.7 and 7.1 (64-bit) (physical or virtual)

    Or
  - Windows Server 2012 R2, 64-bit (physical or virtual)

Access Gateway Appliance and NetIQ Access Manager Appliance
- 8 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk

The appliance runs 64bit operating system on x86-64 hardware supported by SLES 11 SP4.

For a list of x86-64 hardware with SLES 11 SP4 and SLES 12 support, see the YES CERTIFIED Bulletin at: **www.suse.com/yessearch/Search.jsp**

- Increase security and convenience together—NetIQ Access Manager has a built-in, risk-based authentication engine that allows organizations to adapt their user's authentication experience based on measured risk, allowing users frictionless access for low risk environments and a step-up authentication for higher risk situations.
- Integrates with other OpenText identity, access, and security products that equip organizations to deliver convenient access to those who need it while protecting organizations from those who don't, both inside and out

Key Features

Enterprises use NetIQ Access Manage to integrate access to their applications and services across all of their business units, regardless of who owns the user repositories. Its federation and gateway capabilities allow you to bridge together cloud and Intranet applications into a seamless single sign-on and access experience.

- Full support for federation implementations using SAML, OAuth, OpenID Connect, WS-Federation, and others
- UI designer for login and portal pages allows custom branding and icon configuration
- Optional virtual appliance-ready form factor, which is hypervisor agnostic (deploy in almost any environment)
- Out-of-the-box integration with Microsoft SharePoint and Office 365 Enterprise
- Software development kit for iOS devices
- Built-in, risk-based authentication engine that provides risk scoring and selective authentication based on score
- Out-of-the-box integration with Advanced Authentication Framework that supports a wide range of authentication methods
- Centralized policy engine (for role-based access enforcement)

- Built-in mobile gateway for users on smartphones (iOS and Android) who need access to legacy applications
- Access Authorization, single sign-on, and personalization through built-in Access Gateway

Why NetIQ Access Manager

NetIQ Access Manager enables organizations to integrate modern as well as legacy web-based applications. In addition to providing multiple federation options, it also allows single sign-on access for applications through its GUI without the need to modify applications or write complex code.

NetIQ Access Manager includes a built-in risk engine that's free of complex configuration or setup while providing a way to customize the user's authentication experience based on a wide variety of parameters, including context, historical pattern, location, time, or even device.

The Wizard-based code promotion utility allows you to bring up a new server, make a backup, or migrate your policies from your test environment to your production environment in a matter of minutes.

With its pluggable architecture and default integration with Identity Manager and Sentinel security, NetIQ Access Manager provides comprehensive identity, access and security for your intranet, cloud and mobile applications.

Its flexible and compact design and superior performance make NetIQ Access Manager easier to get up and running, using notably less hardware and simplified configuration. And as part of a product line that secures, monitors, and governs access to your valued resources, NetIQ Access Manager can serve as a component of an integrated IAM strategy.

Connect with Us
www.CyberRes.com

opentext | Cybersecurity