

NetIQ Advanced Authentication Connector for z/OS

Information Security is a significant requirement in the digital age. All organizations must manage and protect business-critical corporate and customer data. Increasingly sophisticated means of unauthorized data access need to be met with greater rigor across all data locations.

Product Highlights

Organizations taking advantage of robust authentication security software have to manage multiple infrastructures for each data source location. Typically, this requires additional solutions that provide secure connectivity to the IBM mainframe environment.

The NetIQ Advanced Authentication by OpenText™ Connector for z/OS integrates directly with the NetIQ Advanced Authentication server to provide a single framework for adding the strong level of authentication (Multi-Factor or two-Factor) required to meet regulatory, industry, and client needs across the enterprise. It streamlines the effort to provide a robust security protocol across all core enterprise data locations, including the IBM mainframe.

Key Benefits

- It establishes a single, centralized enterprise-wide framework for access authentication, including z/OS, by integrating directly into NetIQ Advanced Authentication facility
- Provides the scalability to support very large and complex mainframe environments
- Enables rapid conformance with security requirements through a simple mainframe implementation and rollout process

Key Features

- Support for any client tool connecting through to your IBM z/OS environment, whether this is TSO, CICS, z/OSMF, Eclipse, or any user applications that requires specific log-on authentication.
- Works with IBM RACF and CA Top Secret and ACF2 access control systems
- Integration with the OpenText Advanced Authentication Server that provides
 - Wide integration capabilities and the latest authentication methods and devices. This gives you the freedom to use the right security in the right scenario throughout your environment.
 - An Open standards-based solution so you can protect against security breaches while protecting against the risk of vendor lock-in.
 - Broad platform coverage available from Windows, OS X, Linux, iOS, Windows Mobile, Android, and now z/OS.

For full details of the NetIQ Advanced Authentication platform, visit [here](#).

NetIQ Advanced Authentication Connector for z/OS at a Glance:

- Enterprise-wide access authentication now includes critical mainframe apps and data
- Easy to install and rollout
- Supports all major mainframe security access methods
- Plugs directly into the OpenText advanced authentication facility

Connect with Us



System Requirements

NetIQ Advanced Authentication Connector for z/OS

- IBM z/OS V2.2 or above
- Configured IBM Integrated Cryptographic Service Facility (ICSF), IBM CP Assist for Cryptographic Function (CPACF) and IBM z/OS Client Web Enablement Toolkit

NetIQ Advanced Authentication Server

NetIQ Advanced Authentication Server 6.2 or later is a pre-requisite for enabling the z/OS Connector.

Appliance Requirements

Minimum Configuration:

- 40 GB disk space
- 2 Cores CPU
- SSE 4.2 instructions must be supported by processor
- 4 GB RAM

Recommended Configuration:

- 60 GB disk space
- 8 Cores CPU
- SSE 4.2 instructions must be supported by processor
- 8 GB RAM

NetIQ Advanced Authentication Appliance runs a 64-bit operating system on x86-64 hardware supported by SLES 12 SP3.

Learn more at

www.opentext.com