

Advanced Authentication System Requirements



NetIQ Corporation recommends the fully tested and certified platforms described in this page. However, customers running on other platforms or with untested configurations will be supported until the point NetIQ Corporation determines that the root cause is the uncertified platform or configuration. Issues that can be reproduced on the certified platforms will be prioritized and fixed according to standard defect-handling policies. For more information about support policies, see [Support Policies](#). For more information about installation or hardware requirements, see the [Advanced Authentication-Server Installation and Upgrade](#) guide.

Choose a category in the below list to learn about the technical specifications:

- ♦ [Section 1, "Appliance Requirements," on page 1](#)
- ♦ [Section 2, "Integrations," on page 2](#)
- ♦ [Section 3, "RADIUS Server," on page 3](#)
- ♦ [Section 4, "ADFS Plug-In," on page 3](#)
- ♦ [Section 5, "Ports," on page 3](#)
- ♦ [Section 6, "Smartphone Applications," on page 3](#)
- ♦ [Section 7, "Enrollment," on page 3](#)
- ♦ [Section 8, "Client Components," on page 4](#)

1 Appliance Requirements

The following are the requirements for Advanced Authentication appliance:

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

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

Supported Authentication Methods:

- ♦ Bluetooth
- ♦ Card
- ♦ Email OTP
- ♦ Facial Recognition
- ♦ Fingerprint
- ♦ HOTP
- ♦ LDAP Password
- ♦ Password
- ♦ PKI
- ♦ RADIUS Client
- ♦ Security Questions
- ♦ Smartphone
- ♦ SMS OTP
- ♦ Swedish BankID
- ♦ Swisscom Mobile ID
- ♦ TOTP
- ♦ FIDO U2F
- ♦ Voice
- ♦ Voice OTP
- ♦ Windows Hello

It is possible to combine more than one authentication method to form an authentication chain.

2 Integrations

- ♦ Provides in-built RADIUS server functionalities
- ♦ Integration with third-parties using SAML 2.0 and OAuth 2.0
- ♦ Two ways to integrate with ADFS:
 - ♦ SAML 2.0
 - ♦ ADFS Plug-in
- ♦ Provides REST API for third-party integrations
- ♦ In-house integration with the other products of Micro Focus:
 - ♦ Access Manager
 - ♦ Secure Login
 - ♦ iPrint
 - ♦ Filr
 - ♦ Privileged Account Manager
 - ♦ Management and Security Server

3 RADIUS Server

Advanced Authentication can act as a RADIUS Server or a RADIUS Client

- ♦ Only PAP validations are supported with Advanced Authentication RADIUS Server.

4 ADFS Plug-In

ADFS MFA plug-in provides you with the ability to integrate NetIQ Advanced Authentication with Active Directory Federation Services 3.0 (Windows Server 2012 R2) or Active Directory Federation Services 4.0 (Windows Server 2016) for the use of strong authentication to access the secured systems and applications.

Requirements

- ♦ Microsoft Windows Server 2012 R2 or Microsoft Windows Server 2016
- ♦ Microsoft .NET Framework 4.5
- ♦ ADFS role installed and configured. It must work correctly without the ADFS MFA plug-in

5 Ports

To view the ports that Advanced Authentication uses, see <https://www.netiq.com/documentation/advanced-authentication-60/install-upgrade-guide/data/firewall.html#t465zfece2s9>

6 Smartphone Applications

Requirements

- ♦ Apple iOS 10/11/12 is installed for iPhone.
- ♦ Google Android 7.0/8.0, or 9.0. 3 megapixel camera with the autofocus function is supported on an Android Smartphone.
 - ♦ The Android phone must have a fingerprint scanner to use fingerprint sensor to access the application. The minimum version is Android 6 and later. The Android device must support Google Fingerprint Authentication API. For example, Samsung Galaxy Note 4 on Android 6 does not support Google Fingerprint Authentication API and fingerprint does not work in the application. Fingerprint is mostly supported for Android devices that were released after 2015.

7 Enrollment

Automatically enrolled: SMS, email, RADIUS and LDAP Password (based on repository object data).

Enrollment by Administrator: OATH Tokens can be assigned by administrator (or claimed by users).

Enrollment by Helpdesk: A Helpdesk administrator can perform assisted enrollment of authentication methods from the Helpdesk Portal.

Enrollment by Users: Users can enroll permitted methods at the User Self-Service portal.

8 Client Components

The following are the requirements for the Clients.

- ♦ **Windows Client:** Microsoft Windows 7 (x64 or x86) / Microsoft Windows 8.1 (x64 or x86) / Microsoft Windows 10 (v1709, v1803, v1809 or v1903 x64 or x86) / Microsoft Windows Server 2012 R2 / Microsoft Windows Server 2016.
- ♦ **Mac OS X Client:** Apple Mac OS 10.12 (Sierra), 10.13 (High Sierra).
- ♦ **Linux Client:** CentOS 7 with KDE or Gnome desktop environment / SUSE Linux Enterprise Desktop 11 Service Pack4 / SUSE Linux Enterprise Desktop 12 Service Pack3 / SUSE Linux Enterprise Desktop 15 / SUSE Linux Enterprise Server 11 Service Pack4 / SUSE Linux Enterprise Server 12 Service Pack3 / SUSE Linux Enterprise Server 15 / Red Hat Enterprise Linux Client 7.5 / Red Hat Enterprise Linux Server 7.5 / Debian 9.5 / Ubuntu 16, 18. Gnome Display Manager (GDM) should be set as the login manager.