Advanced Authentication System Requirements

NetIQ Corporation recommends the fully tested and certified platforms described in this page. 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 polices, 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:

- "Server Requirements" on page 1
- "Client Components Requirements" on page 4
- "Plug-Ins Requirements" on page 8
- "Smartphone Applications Requirement" on page 9

Server Requirements

- Appliance
- Advanced Authentication Server on Public Cloud
- Common Specifications for Appliance and Server on Cloud

Appliance

NOTE: It is not recommended to install any third-party software on the Advanced Authentication Appliance.

Platform	Advanced Authentication Appliance runs 64-bit operating system on x86-64 hardware supported by SLES 12 SP4.
RAM	Minimum: 6 GB Recommended: 12 GB
Processor	Minimum: 4 Cores Recommended: 8 Cores Processor must support SSE 4.2 instructions. For more information about how to check whether the CPU supports SSE 4.2 instructions, see Verifying SSE 4.2 Instructions on CPU.
Hard Disk space	Minimum: 60 GB Recommended: 100 GB

Virtual System	Supported Virtual systems are: ◆ Citrix XenServer 7.1, 7.5 ◆ Citrix Hypervisor 8.0 ◆ Hyper-V Server 2016 or later ◆ VMware ESX 5.5 or later

Advanced Authentication Server on Public Cloud

AWS	Node requirements are as follows: ◆ **Node Type**: T3 large ◆ **Node Volume Size**: 60 GB
Azure	**Node Size**: DS3_V2 Standard

Common Specifications for Appliance and Server on Cloud

Authentication Methods	Supported Authentication Methods are: ◆ Apple Touch ID ◆ Bluetooth ◆ Card ◆ Device Authentication ◆ Email OTP ◆ Facial Recognition ◆ FIDO U2F ◆ Fingerprint ◆ HOTP ◆ LDAP Password ◆ Password ◆ PKI ◆ RADIUS Client ◆ Security Questions ◆ Smartphone ◆ SMS OTP ◆ Swedish BankID ◆ Swisscom Mobile ID ◆ TOTP ◆ Voice ◆ Voice OTP ◆ Windows Hello It is possible to combine more than one authentication method to form an authentication chain.

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

RADIUS Server	Advanced Authentication can act as a RADIUS Server or a RADIUS Client. Only PAP validations are supported with Advanced Authentication RADIUS Server.
Ports	Ensure that the default ports for the Advanced Authentication appliance are open in your firewall. For more information, see Configuring the Firewall (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/firewall.html).
Browsers	Any one of the following browsers: ◆ Microsoft Internet Explorer 11 ◆ Microsoft Edge 20.0 and later ◆ Google Chrome 65 and later ◆ Mozilla Firefox 58 and later ◆ Safari 11 and later
LDAP Repositories	Any one of the following repositories: ◆ Microsoft Active Directory Services ◆ Microsoft Active Directory Lightweight Directory Services ◆ NetIQ eDirectory ◆ OpenLDAP ◆ OpenDJ ◆ Microsoft SQL Server 2016

Client Components Requirements

This section lists the system requirements of the following components:

- "Windows Client" on page 5
- "Mac OS X Client" on page 5
- "Linux PAM Client" on page 6
- "Device Service" on page 7

- "Desktop OTP Tool" on page 8
- "Windows Authentication Agent" on page 8
- "Virtual Desktop Authentication Agent" on page 8

Windows Client

Processor	Minimum: 2 Cores Recommended: 4 Cores
Hard Disk	Minimum: 100 MB Recommended: 1 GB
Memory	Minimum: 2 GB Recommended: 4 GB
Operating System	Any one of the following operating systems: ◆ Microsoft Windows 8.1 (32-bit or 64-bit) ◆ Microsoft Windows 10 v1903, v1909, v2004, 20H2, 21H2 (32-bit and 64-bit) ◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019 **NOTE:** Advanced Authentication Windows Client is not supported on Windows Server Core editions.

Mac OS X Client

Operating System	◆ macOS Catalina ◆ macOS Big Sur including M1 chip in the emulation mode ◆ macOS Monterey including M1 chip in the emulation mode

Linux PAM Client

Operating System	Supported on the following operating systems: ◆ CentOS 7, 8 ◆ SUSE Linux Enterprise Desktop 12 Service Pack4 ◆ SUSE Linux Enterprise Server 12 Service Pack4 ◆ SUSE Linux Enterprise Server 12 Service Pack5 **NOTE:** This version is supported since Advanced Authentication 6.3 Service Pack7. ◆ SUSE Linux Enterprise Server 15 Service Pack1 ◆ SUSE Linux Enterprise Server 15 Service Pack2 ◆ SUSE Linux Enterprise Server 15 Service Pack3 **NOTE:** This version is supported since Advanced Authentication 6.3 Service Pack7. ◆ Red Hat Enterprise Linux Client 7, 8 ◆ Red Hat Enterprise Linux Server 7, 8 ◆ Debian 9, 10 ◆ Ubuntu 16, or Ubuntu 18
Login Setting	Set Gnome Display Manager (GDM) as the login manager in CentOS.

Device Service

Operating System	◆ Windows
	  ◆ Microsoft Windows 8.1 (32-bit and 64-bit)
	  ◆ Microsoft Windows 10 v1903, v1909, v2004, 21H2 (32-bit and 64-bit)
	  ◆ Microsoft Windows Server 2012 R2
	  ◆ Microsoft Windows Server 2016
	  ◆ Microsoft Windows Server 2019
	◆ Apple
	  ◆ macOS Catalina
	  ◆ macOS Big Sur including M1 chip in the emulation mode
	  ◆ macOS Monterey including M1 chip in the emulation mode
	◆ Linux
	  ◆ CentOS 7, 8
	  ◆ SUSE Linux Enterprise Server 12 Service Pack4
	  ◆ SUSE Linux Enterprise Server 12 Service Pack5
	  NOTE: This version is supported since Advanced Authentication 6.3 Service Pack7.
	  ◆ SUSE Linux Enterprise Server 15 Service Pack1
	  ◆ SUSE Linux Enterprise Server 15 Service Pack2
	  ◆ SUSE Linux Enterprise Server 15 Service Pack3
	  NOTE: This version is supported since Advanced Authentication 6.3 Service Pack7.
	  ◆ Red Hat Enterprise Linux Client 7, 8
	  ◆ Red Hat Enterprise Linux Server 7, 8
	  ◆ Debian 9, 10
	  ◆ Ubuntu 16, 18
	NOTE: Advanced Authentication Device Service is not supported on Windows Server Core editions.

Browsers	◆ Microsoft Internet Explorer 11 ◆ Google Chrome 65 and later ◆ Mozilla Firefox 58 and later ◆ Safari 11 and later ◆ Microsoft Edge 20.0 and later

Desktop OTP Tool

Operating System	◆ Windows
	  ◆ Microsoft Windows 8.1 (32-bit and 64-bit)
	  ◆ Microsoft Windows 10 v1903, v1909, v2004, 20H2, 21H2 (32-bit and 64-bit)
	  ◆ Microsoft Windows Server 2012 R2
	  ◆ Microsoft Windows Server 2016
	  ◆ Microsoft Windows Server 2019
	◆ Apple
	  ◆ macOS Catalina
	  ◆ macOS Big Sur including M1 chip in the emulation mode
	  ◆ macOS Monterey including M1 chip in the emulation mode

Windows Authentication Agent

Operating System	◆ Microsoft Windows 8.1 (32-bit and 64-bit) ◆ Microsoft Windows 10 v1903, v1909, v2004, 20H2, 21H2 (32-bit and 64-bit) ◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019

Virtual Desktop Authentication Agent

Operating System	◆ Microsoft Windows 8.1 (32-bit or 64-bit) ◆ Microsoft Windows 10 v1903, v1909, v2004, 21H2 (32-bit and 64-bit) ◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019
Virtual Client Software	◆ Citrix Receiver v4.12 ◆ Citrix Workspace app 2002 ◆ VMware Horizon Client v5 ◆ Microsoft Remote Desktop

Plug-Ins Requirements

ADFS MFA plug-in	Operating System	◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019

	Software Requirement	◆ Microsoft .NET Framework 4.5 ◆ ADFS role installed and configured. It must work correctly without the ADFS MFA plug-in
IIS Authentication plug-in	Operating System	◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019
	Software Requirement	◆ Microsoft IIS Manager ◆ Microsoft .NET Framework 4.5
Logon Filter	Operating System	Domain controllers based one of the following: ◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019
Remote Desktop Gateway	Operating System	◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 20H2
	Software Requirement	Microsoft Remote Desktop Gateway role

Smartphone Applications Requirement

Android	◆ Supported versions are: ◆ Android 8.1 ◆ Android 9 ◆ Android 10 ◆ Android 11 **NOTE:** NetIQ Advanced Authentication smartphone application supports Android 8.1. It is recommended to upgrade to version 8.1 because Google does not provide any security updates for the versions before 8.1. ◆ 3 megapixel camera with the auto-focus feature. ◆ The fingerprint scanner to use the fingerprint sensor to access the app.
Apple	Supported versions are: ◆ iOS 12 ◆ iOS 13 ◆ iOS 14 ◆ iOS 15 **NOTE:** The NetIQ Advanced Authentication application installation is supported on iPad.