

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 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:

- ♦ [“Server Requirements” on page 1](#)
- ♦ [“Client Components Requirements” on page 4](#)
- ♦ [“Plug-Ins Requirements” on page 7](#)
- ♦ [“Smartphone Applications Requirement” on page 8](#)

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 SP5.
RAM	Minimum: 8 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 .

NOTE: It is recommended to increase the number of processors and amount of RAM if the user traffic is high.

For example, if you have more than a million users, then you can increase the number of processors to 12 cores and the amount of RAM to 128GB.

Hard Disk space	Minimum: 60 GB Recommended: 100 GB with 40% free space IMPORTANT: For large deployments, you may require more disk space than the recommended above. To verify the available disk space, login to the Appliance Configuration Console and run the command <code>df -h /dev/sda1</code> on the command prompt. Ensure that you are not utilizing more than 40% of the available disk space. If you are utilizing more than 40% of your free space, increase your disk space to the value listed below before performing an upgrade: ♦ Minimum: 120 GB ♦ Recommended: 200 GB with 40% free space
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 NOTE: While running the Advanced Authentication appliance on VMware ESXi, ensure that the Boot Options for the virtual machine is configured to the BIOS mode.

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 NOTE: The Bluetooth method has been deprecated from Advanced Authentication 6.4 Service Pack 1. ♦ Bluetooth eSec NOTE: The Bluetooth eSec method is available from Advanced Authentication 6.4 Service Pack 2. ♦ Card ♦ Device Authentication ♦ Email OTP ♦ Facial Recognition ♦ FIDO U2F ♦ Fingerprint ♦ Flex OTP ♦ 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 Open Text: ◆ 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 Edge 123 and later ◆ Google Chrome 123 and later ◆ Mozilla Firefox 124 and later ◆ Safari 17 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 5](#)
- ◆ [“Device Service” on page 6](#)
- ◆ [“Desktop OTP Tool” on page 6](#)

- ♦ [“Windows Authentication Agent” on page 7](#)
- ♦ [“Virtual Desktop Authentication Agent” on page 7](#)

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 11 v23H2 and 24H2 (64-bit) ♦ Microsoft Windows 10 v22H2 (32-bit and 64-bit) ♦ Microsoft Windows Server 2016 ♦ Microsoft Windows Server 2019 ♦ Microsoft Windows Server 2022 NOTE: Advanced Authentication Windows Client is not supported on Windows Server Core editions.

Mac OS X Client

Operating System	♦ macOS 13 Ventura in the emulation mode ♦ macOS 14 Sonoma in the emulation mode ♦ macOS 15 Sequoia in the emulation mode
-------------------------	---

Linux PAM Client

Operating System	Supported on the following operating systems: ♦ SUSE Linux Enterprise Server 15 Service Pack6 ♦ SUSE Linux Enterprise Server 12 Service Pack5 ♦ Red Hat Enterprise Linux 8, 8.10, 9.2, 9.3, and 9.4 ♦ Ubuntu 20.04 LTS, 22.04 LTS, and 24.04 LTS ♦ Advanced Interactive eXecutive (AIX) 7.2 and 7.3
Login Setting	Set Gnome Display Manager (GDM) as the login manager in CentOS.

Device Service

NOTE: For detailed information on the system requirements of the Device Service and the list of supported devices, see [System Requirements](#).

Operating System	♦ Windows ♦ Microsoft Windows 11 v23H2 and 24H2 (64-bit) ♦ Microsoft Windows 10 v22H2 (32-bit and 64-bit) ♦ Microsoft Windows Server 2016 ♦ Microsoft Windows Server 2019 ♦ Microsoft Windows Server 2022 ♦ Apple ♦ macOS 13 Ventura in the emulation mode ♦ macOS 14 Sonoma in the emulation mode ♦ macOS 15 Sequoia in the emulation mode ♦ Linux ♦ SUSE Linux Enterprise Server 15 Service Pack6 ♦ SUSE Linux Enterprise Server 12 Service Pack5 ♦ Red Hat Enterprise Linux Client 8, 8.10, 9.2, 9.3, and 9.4 ♦ Ubuntu 20.04 LTS, 22.04 LTS, and 24.04 LTS NOTE: Advanced Authentication Device Service is not supported on Windows Server Core editions.
Browsers	♦ Google Chrome 123 and later ♦ Mozilla Firefox 124 and later ♦ Safari 17 and later ♦ Microsoft Edge 123 and later

Desktop OTP Tool

Operating System	♦ Windows ♦ Microsoft Windows 11 v23H2 and 24H2 (64-bit) ♦ Microsoft Windows 10 v22H2 (32-bit and 64-bit) ♦ Microsoft Windows Server 2016 ♦ Microsoft Windows Server 2019 ♦ Microsoft Windows Server 2022 ♦ Apple ♦ macOS 13 Ventura in the emulation mode ♦ macOS 14 Sonoma in the emulation mode ♦ macOS 15 Sequoia in the emulation mode
-------------------------	---

Windows Authentication Agent

Operating System	♦ Microsoft Windows 11 v23H2 and 24H2 (64-bit) ♦ Microsoft Windows 10 v22H2 (32-bit and 64-bit) ♦ Microsoft Windows Server 2016 ♦ Microsoft Windows Server 2019 ♦ Microsoft Windows Server 2022
-------------------------	---

Virtual Desktop Authentication Agent

Operating System	♦ Microsoft Windows 11 v24H2 (64-bit) ♦ Microsoft Windows Server 2016 ♦ Microsoft Windows Server 2019 ♦ Microsoft Windows Server 2022
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 2016 ♦ Microsoft Windows Server 2019 ♦ Microsoft Windows Server 2022
	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 2016 ♦ Microsoft Windows Server 2019 ♦ Microsoft Windows Server 2022
	Software Requirement	♦ Microsoft IIS Manager ♦ Microsoft .NET Framework 4.5 ♦ Microsoft SQL
Logon Filter	Operating System	Domain controllers based one of the following: ♦ Microsoft Windows Server 2016 ♦ Microsoft Windows Server 2019 ♦ Microsoft Windows Server 2022

Remote Desktop Gateway	Operating System	◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2022
	Software Requirement	Microsoft Remote Desktop Gateway role

Smartphone Applications Requirement

Android	◆ Supported versions are: ◆ Android 10 ◆ Android 11 ◆ Android 12 ◆ Android 13 NOTE: NetIQ Advanced Authentication smartphone application supports Android 10 and later versions. Google does not provide any security updates for the versions prior to Android 10. ◆ 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 15 ◆ iOS 16 ◆ iOS 17 NOTE: The NetIQ Advanced Authentication application installation is supported on iPad.