

# 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.

---

<b>Platform</b>	Advanced Authentication Appliance runs 64-bit operating system on x86-64 hardware supported by SLES 12 SP5.
<b>RAM</b>	Minimum: 8 GB Recommended: 12 GB
<b>Processor</b>	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 <a href="#">Verifying SSE 4.2 Instructions on CPU</a> .

**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.

<b>Hard Disk space</b>	<p>Minimum: 60 GB</p> <p>Recommended: 100 GB with 40% free space</p> <p><b>IMPORTANT:</b> For large deployments, you may require more disk space than the recommended above. To verify the available disk space, login to the <b>Appliance Configuration Console</b> and run the command <code>df -h /dev/sda1</code> on the command prompt.</p> <p>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:</p> <ul style="list-style-type: none"><li>◆ Minimum: 120 GB</li><li>◆ Recommended: 200 GB with 40% free space</li></ul>
<b>Virtual System</b>	<p>Supported Virtual systems are:</p> <ul style="list-style-type: none"><li>◆ Citrix XenServer 7.1, 7.5</li><li>◆ Citrix Hypervisor 8.0</li><li>◆ Hyper-V Server 2016 or later</li><li>◆ VMware ESX 5.5 or later</li></ul> <p><b>NOTE:</b> While running the Advanced Authentication appliance on VMware ESXi, ensure that the <b>Boot Options</b> for the virtual machine is configured to the <b>BIOS</b> mode.</p>

## Advanced Authentication Server on Public Cloud

<b>AWS</b>	<p>Node requirements are as follows:</p> <ul style="list-style-type: none"><li>◆ <b>Node Type:</b> T3 large</li><li>◆ <b>Node Volume Size:</b> 60 GB</li></ul>
<b>Azure</b>	<p><b>Node Size:</b> DS3_V2 Standard</p>

## Common Specifications for Appliance and Server on Cloud

<b>Authentication Methods</b>	<p>Supported Authentication Methods are:</p> <ul style="list-style-type: none"><li>◆ Apple Touch ID</li><li>◆ Bluetooth <b>NOTE:</b> The Bluetooth method has been deprecated from Advanced Authentication 6.4 Service Pack 1.</li><li>◆ Bluetooth eSec <b>NOTE:</b> The Bluetooth eSec method is available from Advanced Authentication 6.4 Service Pack 2.</li><li>◆ Card</li><li>◆ Device Authentication</li><li>◆ Email OTP</li><li>◆ Facial Recognition</li><li>◆ FIDO U2F</li><li>◆ Fingerprint</li><li>◆ Flex OTP</li><li>◆ HOTP</li><li>◆ LDAP Password</li><li>◆ Password</li><li>◆ PKI</li><li>◆ RADIUS Client</li><li>◆ Security Questions</li><li>◆ Smartphone</li><li>◆ SMS OTP</li><li>◆ Swedish BankID</li><li>◆ Swisscom Mobile ID</li><li>◆ TOTP</li><li>◆ Voice</li><li>◆ Voice OTP</li><li>◆ Windows Hello</li></ul> <p>It is possible to combine more than one authentication method to form an authentication chain.</p>
-------------------------------	---

<b>Integrations</b>	<ul style="list-style-type: none"> <li>◆ Provides in-built RADIUS server functionalities</li> <li>◆ Integration with third-parties using SAML 2.0 and OAuth 2.0</li> <li>◆ Two ways to integrate with ADFS: <ul style="list-style-type: none"> <li>◆ SAML 2.0</li> <li>◆ ADFS Plug-in</li> </ul> </li> <li>◆ Provides REST API for third-party integrations</li> <li>◆ In-house integration with the other products of Open Text: <ul style="list-style-type: none"> <li>◆ Access Manager</li> <li>◆ Secure Login</li> <li>◆ iPrint</li> <li>◆ Filr</li> <li>◆ Privileged Account Manager</li> <li>◆ Management and Security Server</li> </ul> </li> </ul>
<b>RADIUS Server</b>	Advanced Authentication can act as a RADIUS Server or a RADIUS Client. Only PAP validations are supported with Advanced Authentication RADIUS Server.
<b>Ports</b>	Ensure that the default ports for the Advanced Authentication appliance are open in your firewall. For more information, see <a href="https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/firewall.html">Configuring the Firewall (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/firewall.html)</a> .
<b>Browsers</b>	Any one of the following browsers: <ul style="list-style-type: none"> <li>◆ Microsoft Edge 123 and later</li> <li>◆ Google Chrome 123 and later</li> <li>◆ Mozilla Firefox 124 and later</li> <li>◆ Safari 17 and later</li> </ul>
<b>LDAP Repositories</b>	Any one of the following repositories: <ul style="list-style-type: none"> <li>◆ Microsoft Active Directory Services</li> <li>◆ Microsoft Active Directory Lightweight Directory Services</li> <li>◆ NetIQ eDirectory</li> <li>◆ OpenLDAP</li> <li>◆ OpenDJ</li> <li>◆ Microsoft SQL Server 2016</li> </ul>

## 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

<b>Processor</b>	Minimum: 2 Cores Recommended: 4 Cores
<b>Hard Disk</b>	Minimum: 100 MB Recommended: 1 GB
<b>Memory</b>	Minimum: 2 GB Recommended: 4 GB
<b>Operating System</b>	Any one of the following operating systems: <ul style="list-style-type: none"> <li>◆ Microsoft Windows 11 v21H2, 22H2, and 23H2 (64-bit)</li> <li>◆ Microsoft Windows 10 21H2 and 22H2 (32-bit and 64-bit)</li> <li>◆ Microsoft Windows Server 2016</li> <li>◆ Microsoft Windows Server 2019</li> </ul> <p><b>NOTE:</b> Advanced Authentication Windows Client is not supported on Windows Server Core editions.</p>

## Mac OS X Client

<b>Operating System</b>	<ul style="list-style-type: none"> <li>◆ macOS 12 Monterey in the emulation mode</li> <li>◆ macOS 13 Ventura in the emulation mode</li> </ul>
-------------------------	---

## Linux PAM Client

<b>Operating System</b>	Supported on the following operating systems: <ul style="list-style-type: none"> <li>◆ CentOS 7</li> <li>◆ SUSE Linux Enterprise Server 12 Service Pack5</li> <li>◆ Red Hat Enterprise Linux Workstation 7, 8, 9.2, and 9.3</li> <li>◆ Red Hat Enterprise Linux Server 7, 8, 9.2, and 9.3</li> <li>◆ Debian 10</li> <li>◆ Ubuntu 20.04 LTS</li> <li>◆ Advanced Interactive eXecutive (AIX) 7.2 and 7.3</li> </ul>
<b>Login Setting</b>	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](#).

<b>Operating System</b>	<ul style="list-style-type: none"><li>◆ Windows<ul style="list-style-type: none"><li>◆ Microsoft Windows 11 v21H2, 22H2, and 23H2 (64-bit)</li><li>◆ Microsoft Windows 10 21H2 and 22H2 (32-bit and 64-bit)</li><li>◆ Microsoft Windows Server 2016</li><li>◆ Microsoft Windows Server 2019</li></ul></li><li>◆ Apple<ul style="list-style-type: none"><li>◆ macOS 12 Monterey in the emulation mode</li><li>◆ macOS 13 Ventura in the emulation mode</li></ul></li><li>◆ Linux<ul style="list-style-type: none"><li>◆ CentOS 7</li><li>◆ SUSE Linux Enterprise Server 12 Service Pack5</li><li>◆ Red Hat Enterprise Linux Client 7, 8, 9.2, and 9.3</li><li>◆ Red Hat Enterprise Linux Server 7, 8, 9.2, and 9.3</li><li>◆ Debian 10</li><li>◆ Ubuntu 20.04 LTS</li></ul></li></ul> <p><b>NOTE:</b> Advanced Authentication Device Service is not supported on Windows Server Core editions.</p>
<b>Browsers</b>	<ul style="list-style-type: none"><li>◆ Google Chrome 123 and later</li><li>◆ Mozilla Firefox 124 and later</li><li>◆ Safari 17 and later</li><li>◆ Microsoft Edge 123 and later</li></ul>

## Desktop OTP Tool

<b>Operating System</b>	<ul style="list-style-type: none"><li>◆ Windows<ul style="list-style-type: none"><li>◆ Microsoft Windows 11 v21H2, 22H2, and 23H2 (64-bit)</li><li>◆ Microsoft Windows 10 21H2 and 22H2 (32-bit and 64-bit)</li><li>◆ Microsoft Windows Server 2016</li><li>◆ Microsoft Windows Server 2019</li></ul></li><li>◆ Apple<ul style="list-style-type: none"><li>◆ macOS 12 Monterey in the emulation mode</li><li>◆ macOS 13 Ventura in the emulation mode</li></ul></li></ul>
-------------------------	---

## Windows Authentication Agent

<b>Operating System</b>	<ul style="list-style-type: none"> <li>◆ Microsoft Windows 11 v21H2, 22H2, and 23H2 (64-bit)</li> <li>◆ Microsoft Windows 10 21H2 and 22H2 (32-bit and 64-bit)</li> <li>◆ Microsoft Windows Server 2016</li> <li>◆ Microsoft Windows Server 2019</li> </ul>
-------------------------	---

## Virtual Desktop Authentication Agent

<b>Operating System</b>	<ul style="list-style-type: none"> <li>◆ Microsoft Windows 11 v21H2 and 22H2 (64-bit)</li> <li>◆ Microsoft Windows Server 2016</li> <li>◆ Microsoft Windows Server 2019</li> </ul>
<b>Virtual Client Software</b>	<ul style="list-style-type: none"> <li>◆ Citrix Receiver v4.12</li> <li>◆ Citrix Workspace app 2002</li> <li>◆ VMware Horizon Client v5</li> <li>◆ Microsoft Remote Desktop</li> </ul>

## Plug-Ins Requirements

<b>ADFS MFA plug-in</b>	Operating System	<ul style="list-style-type: none"> <li>◆ Microsoft Windows Server 2016</li> <li>◆ Microsoft Windows Server 2019</li> </ul>
	Software Requirement	<ul style="list-style-type: none"> <li>◆ Microsoft .NET Framework 4.5</li> <li>◆ ADFS role installed and configured. It must work correctly without the ADFS MFA plug-in</li> </ul>
<b>IIS Authentication plug-in</b>	Operating System	<ul style="list-style-type: none"> <li>◆ Microsoft Windows Server 2016</li> <li>◆ Microsoft Windows Server 2019</li> </ul>
	Software Requirement	<ul style="list-style-type: none"> <li>◆ Microsoft IIS Manager</li> <li>◆ Microsoft .NET Framework 4.5</li> <li>◆ Microsoft SQL</li> </ul>
<b>Logon Filter</b>	Operating System	Domain controllers based one of the following: <ul style="list-style-type: none"> <li>◆ Microsoft Windows Server 2016</li> <li>◆ Microsoft Windows Server 2019</li> </ul>
<b>Remote Desktop Gateway</b>	Operating System	<ul style="list-style-type: none"> <li>◆ Microsoft Windows Server 2016</li> <li>◆ Microsoft Windows Server 2019</li> </ul>
	Software Requirement	Microsoft Remote Desktop Gateway role

# Smartphone Applications Requirement

<b>Android</b>	<ul style="list-style-type: none"><li>◆ Supported versions are:<ul style="list-style-type: none"><li>◆ Android 10</li><li>◆ Android 11</li><li>◆ Android 12</li><li>◆ Android 13</li></ul></li></ul> <p><b>NOTE:</b> 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.</p> <ul style="list-style-type: none"><li>◆ 3 megapixel camera with the auto-focus feature.</li><li>◆ The fingerprint scanner to use the fingerprint sensor to access the app.</li></ul>
<b>Apple</b>	<p>Supported versions are:</p> <ul style="list-style-type: none"><li>◆ iOS 15</li><li>◆ iOS 16</li><li>◆ iOS 17</li></ul> <p><b>NOTE:</b> The NetIQ Advanced Authentication application installation is supported on iPad.</p>