

Hardware and Software Requirements NEXIS Bridge

System prerequisites for operating the NEXIS Bridge

As of: October 22, 2026 | **Status:** Confirmed

Table of Contents

1. General	1
2. Hardware Requirements	2
3. Software Requirements	2

1. General

The NEXIS Platform is delivered as a SaaS solution and integrates with both cloud services and on-premises applications. Cloud services are typically reachable directly through their public APIs. On-premises applications – such as an IGA solution – also expose APIs, but the customer's network boundary prevents the NEXIS Platform from initiating inbound connections to systems inside it.

The NEXIS Bridge resolves this. It is a lightweight component deployed within the customer network that establishes an outbound WebSocket Secure (WSS) connection to the NEXIS Platform. Because the connection originates inside the network, no inbound firewall ports are required.

Once established, the connection serves as a persistent, bidirectional communication channel. Although the channel is initiated by the bridge, the NEXIS Platform acts as the logical initiator of all operations: it pulls data from on-premises systems and pushes changes to them over the same connection.

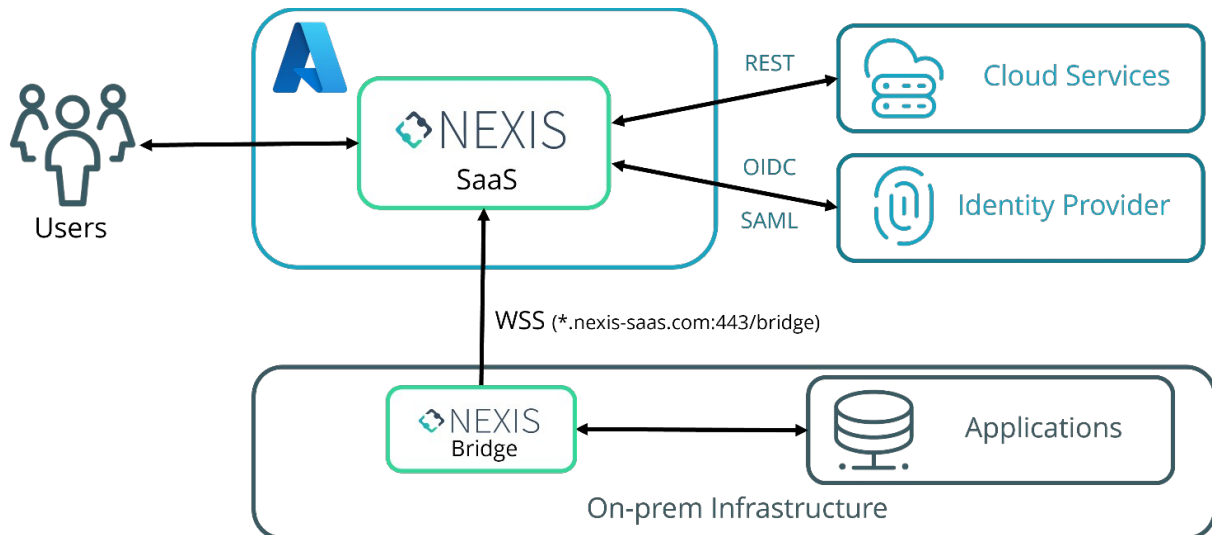


Figure 1: Integration of the NEXIS Bridge into the on-premises infrastructure

2. Hardware Requirements

Hardware requirements vary with the volume of data processed by the bridge – primarily the number of managed objects (employees, accounts, system entitlements, and business roles) transferred per synchronization, the frequency of synchronization, and the number of connected target systems. Deployments with large object volumes or frequent reconciliation may require resources toward the upper end of the range.

Objects per synchronization	Requirements
0 – 60,000	1-core processor 4 GB memory 10 GB hard disk
more than 60,000	2-core processor 6 GB memory 10 GB hard disk

Table 1: Hardware requirements of the NEXIS Bridge

3. Software Requirements

The NEXIS Bridge is a Java application that connects to the NEXIS Platform over secure WebSockets (WSS). The connection is always established outbound by the bridge; no inbound connection into the on-premises infrastructure is required. The following network paths must be permitted:

- Outbound TCP 443 (WSS) from the bridge to the NEXIS SaaS endpoint.
- Outbound connectivity from the bridge to each target system (e.g., database, LDAP/Active Directory, file path), as configured in the connection allowlist.

The bridge does not support connection through an outbound HTTP/HTTPS proxy; direct outbound access to the NEXIS endpoint on TCP 443 is required. The NEXIS SaaS TLS certificate chain must be trusted by the bridge's Java runtime (added to the JDK trust store) for the WSS handshake to succeed.

Component	Supported products
Operating system	Windows Server 2025 / 2022 / 2019, Ubuntu 20 / 22 / 24, RHEL 8 / 9
Java	OpenJDK 25 (Eclipse Temurin)

Table 2: Supported software of the NEXIS Bridge