PRIME requirements and interoperability

This article provides installation requirements and interoperability data for Nexus PRIME.

This article is valid for Nexus PRIME 3.10.

Expand/Collapse All

Requirements

PRIME application server

	Minimum	Recommended
Hard disk storage	5 GB ⚠ The application generates log files, which consumes additional hard disk space.	
CPU	2 GHz	> 2 GHz
RAM	8 GB	16 GB

The sizing requirements listed above are only recommendations for a default setup. The sizing may differ, for example depending on the following things:

- Number of concurrent users in the PRIME applications.
- System architecture: for example high availability setup, combined or distributed setup of the PRIME applications.
- OS footprint: different operating systems consume different RAM/CPU loads.

⚠ It is recommended to host the application server and the database server in the same data center (but on separated servers). Connecting a PRIME application server to a database server via a WAN connection would mean higher latencies and would affect the performance of the system.

The following operating systems are supported:

- Windows 10 (Client OS not recommended for production environment)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Linux and others on request

The following software is supported:

- Oracle Java JDK/JRE:
  - Version 8.0 (32-bit and 64-bit) , Update 191 or higher
- OpenJDK
  - Version 11 (6-4bit), Tested on OpenJDK 11.0.1
- Application Server:
  - Apache Tomcat 8.5 and 8.0

Related information

- Card SDK requirements and interoperability
- PRIME installation and upgrade

- IBM Websphere 8.5.5.11 (we expect Websphere expertise at the customer, Nexus does not offer integration services for deployment Websphere)

Required ports for Tomcat

On the Apache Tomcat at least two ports are required, one for HTTP and one for HTTPS. Tomcat default ports are 8080 (HTTP) and 8443 (HTTPS). To avoid port collisions, the PRIME distribution package is preconfigured with 18080/18443. The port numbers can be configured in the configuration file `server.xml`. Technically, it is not necessary to use HTTPS, but it is highly recommended.

PRIME database server

	Minimum	Recommended
Hard disk storage	~ 1 MB per person record with photo	
CPU	2 GHz	> 2 GHz
RAM	4 GB	8 GB

It is recommended to host the application server and the database server in the same data center (but on separated servers). Connecting a PRIME application server to a database server via a WAN connection would mean higher latencies and would affect the performance of the system.

The following databases are supported:

- SQL Server 2012 and 2012 R2
- SQL Server 2014 and 2014 R2
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- Azure SQL
- Oracle Database 11g
- Oracle Database 12c
- PostgreSQL 9.2 – 9.6
- IBM DB2 10.5

All operating systems that can host the above databases are supported.

PRIME client workstation

All PRIME applications (Designer, Explorer, Tenant and Self-Service) are executed in up-to-date HTML5 web browsers such as:

- Mozilla Firefox
- Google Chrome
- Internet Explorer 11
- Safari
- Microsoft Edge (Edge HTML engine)

PRIME releases are always tested with the latest browser versions.

	Minimum	Recommended
Hard disk storage	~ 100 MB for Nexus Card SDK installation ⚠ Nexus Card SDK is only necessary on a capture or production client.	
CPU	2 GHz	> 2 GHz
RAM	4 GB	> 4 GB

The following operating systems are supported:

- Windows 10
- Linux (for clients without image capture, printing and encoding)

Mobile device platforms

Platforms of mobile devices, for example iOS, Android, and Windows RT, are only supported by certain functions of the browser-based Nexus PRIME Self-Service, but cannot be used with Nexus PRIME Designer and Nexus PRIME Explorer.

The following version of JasperReports is supported:

- Templates in JasperReports format (.jrxml) version 6.5.1 are supported

If a workstation is used as a capture client or production client, the Nexus Card SDK application must be installed and licensed.

This requires a Windows-based workstation (PC). For complete installation requirements for Card SDK, see the Nexus Card SDK documentation.

The following version is required:

- Nexus Card SDK Version >= 5.4.0.22

For PKI cryptochip encoding the following is also required:

- A PKCS#11 compliant smart card middleware.
  - For a list of supported smart card middleware, see Smartcards and smartcard middleware.
- Oracle Java JDK/JRE or OpenJDK
  - Version: 8 or 11, Tested on JRE 8 Update 191 and OpenJDK 11.0.2
  - Architecture: 32-bit (for any smart card middleware) or 64-bit (for any smart card middleware except Nexus Personal)
- The smart card middleware and client-side Java must have the same OS architecture, either 32-bit or 64-bit, since PRIME Explorer's encoding component connectors from the client-side Java to the middleware.

The following requirements apply for the use of PKI cryptochip encoding features on PRIME Self-Service clients:

- A PKCS#11 compliant smart card middleware.
  - For a list of supported smartcard middleware, see Smartcards and smartcard middleware.
- Nexus Personal Desktop App version 1.2.

Interoperability

Data connectors

PRIME supports connection to directories compliant with the following standard:

- LDAP v3

Microsoft Active Directory is a typical example of a supported directory.

PRIME supports connection to databases based on Java database connectivity (JDBC).

The following databases are supported:

- SQL Server 2012 and 2012 R2
- SQL Server 2014 and 2014 R2
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- Azure SQL
- Oracle Database 11g
- Oracle Database 12c
- PostgreSQL 9.2 – 9.6
- IBM DB2 10.5
- H2

The following certificate authority (CA) products and services are supported:

- Nexus Certificate Manager 7.18
- Microsoft Active Directory Certificate Services (ADCS) 2012 / 2012 R2 / 2016
- D-Trust Managed PKI
- IDNomic version 4.8.1
- EJBCA Version 6.3 (without Key Backup / Key Recovery)
- DFN Managed PKI
- QuoVadis PKI

Other CAs can be integrated on demand.

These are the different levels of PACS integration in PRIME:

Basic PACS integration

- Integration via standard data connectors, such as CSV files, JDBC, LDAP, and SCIM
- Export of card data to PACS at card activation and deactivation

All PACS systems that can use any of the standard data connectors are supported.

Full entitlement PACS integration

Full entitlement PACS integration is included as part of the Physical Entitlement Management module in PRIME:

- Integration via standard connectors in PACS backend
- Online sync of card data and access profiles
- Virtual access profile groups on top of PACS access profiles
- Updates of access profiles can be separated from card issuing

The following PACS systems are supported:

Vendor	System	Supported versions
ASSA	Arx	4.1
Siemens	Bewator 2010 Omnis	6.2
Bravida	Integra	7.0
Evva Salto	SALTO	12.2
dormakaba	KABA Exos 9300	4.0
Lenel	OnGuard	6.6
Pacom	Unison	5.8.6
RCO	RCARD M5	5.x
Stanley	Stanley Security Manager (SSM)	8.0, 8.1
Stanley	Niscayah Integration Manager (NIM3)	3.40
Unitek	Unilock	2.0

For some PACS systems you need an additional license to do this integration. Contact your PACS vendor for more information.

Contact us!

Is your PACS system not on the list? Provide the details of your PACS system in this form and we will contact you.

The following mobile device management (MDM) product is supported:

- MobileIron 9.1

Other MDM systems can be integrated on demand.

Smartcards and smartcard middleware

Supported smart cards depend on the smart card middleware. Smart card middleware is not part of the Nexus PRIME product.

PRIME connects to a smart card via the PKCS#11 library provided by the middleware. For a list of supported cryptochips and smart cards, please refer to the corresponding technical specification of the middleware.

CardOS 4.4 and CardOS 5.0 are our reference cards for testing. Other cards listed in the middleware specification also normally work, but must be tested individually for the specific requirement.

The following smart card middleware products are supported:

Vendor/ Product	Version	Reference Card
Nexus Personal Desktop Client	4.30.2 and 5.1	CardOS 4.4 + 5.0

AET SafeSign	3.0.93	CardOS 4.4 Neowave Weneo
Atos CardAPI	5.4 (1)	CardOS 4.2C + 4.4 + 5.0 + 5.3
Charismathics CSSI	5.4	CardOS 4.4 + 5.0 TPM
Cryptovision cv act sc/interface	7.0.5	CardOS 4.4
Gemalto IDGo800 Pkcs#11 Library	1.2.4	IDPrime MD 830
Morpho Ypsid	7.0.1	Ypsid S3
Oberthur AWP	5.1.1	V 7.0.1
Safenet Authentication Client	10.2	IDPrime MD 840
T-Systems TCOS3 NetKey	1.8.2.2 (2)	TeleSec Signature Card V2.0, TeleSec IDKey 1.0

(1) 5.4W14 or later is required for certain features

(2) 1.8.2.2 is the minimum compatible version, we recommend 1.8.2.4 or later

Virtual smartcards

The following virtual smartcard is supported:

Vendor/ Product	Version
Nexus Personal Desktop App	1.2

Language support

The following languages are supported:

- English
- French
- German
- Swedish