Technical Requirements for Identity Governance

24.3 (v4.3.1)

We recommend the verified components described in the following sections. However, customers running on any component not provided in this list or with untested configurations will be supported until the point our Support team determines that the root cause is the untested component or configuration.

Issues that can be reproduced on the verified component will be prioritized and fixed according to standard defect-handling policies. For more information about support polices, see Support Policies.

Ensure that the systems you install and use with Identity Governance meet the hardware and software requirements and supported paths and product versions listed here.

For additional documentation, see the Identity Governance and Administration Documentation (https://www.microfocus.com/documentation/identity-governance-and-administration/) website.

Identity Governance Server System Requirements

This section provides the minimum requirements for the servers where you want to install Identity Governance. You can install Identity Governance and the required components in different configurations. For more information, see Recommended Production Environment Installation Scenarios in the *Identity Governance 24.3 (v4.3.1) Installation and Configuration Guide*.

These system requirements provide server settings according to the size of your Identity Governance catalog. In a small catalog, you might collect fewer than 100,000 identities with 100,000 permissions and 80,000 groups.

Category	Minimum Requirement
Processor	◆ 4.0 GHz, single processor (small catalog) ◆ 4 physical cores of 2.0 GHz or higher per processor
Disk Space	50 GB
Memory	◆ 16 GB (small catalog) ◆ 32 GB
Utilities	Identity Governance Configuration Update utility (ConfigUpdate) 5.0
Operating System	◆ Red Hat Enterprise Linux 8.8 (64-bit) or later patched versions of 8.*x* ◆ SUSE Linux Enterprise Server 15.4 or later patched version of 15.*x* ◆ Microsoft Windows Server 2022 or later patched versions of Windows Server 2022 **IMPORTANT:** Before installing Identity Governance, apply the latest operating system patches.
Virtual Systems	We support Identity Governance on enterprise-class virtual systems that provide official support for the operating systems where our products are running. As long as the vendors of the virtual systems officially support these operating systems, we support Identity Governance running on them. **IMPORTANT:** Ensure to configure the virtual machines running Identity Governance as Thick Provisioned.
Java	Azul JDK 11.0.24 or later respective patched versions of 11.0.*xx*
Application Server	Apache Tomcat 9.0.91 and later patched versions of 9.0.*xx* **NOTE:** (Conditional) For guaranteed delivery of email notifications, your application server must include support for Apache ActiveMQ Java Message Service (JMS) and clustering.
LDAP Identity Service	◆ Microsoft Active Directory that comes with Windows Server 2022 ◆ eDirectory 9.2.8 or later patched versions of 9.2.*x* ◆ Identity Manager 4.8.7 and 4.9 or later patched versions of 4.8.*x* or 4.9.*x*
Authentication Service	◆ OSP 6.6.7 only when deployed with Identity Manager 4.8.7 ◆ OSP 6.7.6 or later versions of 6.7.x when deployed with Identity Governance 4.3.1 or Identity Manager 4.9 ◆ Access Manager 5.0.4, or later patched versions of 5.0.*x*
Secure Communication	TLS 1.2 for secure communication

Category	Minimum Requirement
Third-Party Connector Libraries	(Optional) The Identity Governance JDBC Collectors and SAP User Management Collector use third-party client connector software that is not distributed with the product. Find and download the appropriate JDBC driver file for your database from the database vendor. ◆ DB2: `com.ibm.db2.jcc.DB2Driver` ◆ Generic jTDS: `net.sourceforge.jtds.jdbc.Driver` ◆ Microsoft SQL Server: `com.microsoft.sqlserver.jdbc.SQLServerDriver` ◆ MySQL: `com.mysql.jdbc.Driver` ◆ Oracle Thin Client: `oracle.jdbc.driver.OracleDriver` ◆ PostgreSQL: `org.postgresql.Driver` ◆ SAP: `sapjco3.jar` **NOTE:** Ensure that all required SAP Java Connector Native library components are installed on the host system. For more information, refer to the vendor documentation. ◆ Sybase: `com.sybase.jdbc3.jdbc.SybDriver` To gather identity and application data from one of these sources, put one or more of the these client `.jar` files into the Apache Tomcat `/lib` folder, then restart the Apache Tomcat server. The default installation location is: ◆ **Linux:** `/opt/netiq/idm/apps/tomcat/lib` ◆ **Windows:** `c:\netiq\idm\apps\tomcat\lib`

Database Requirements

This section provides the additional minimum requirements for the server where you want to install the databases for Identity Governance and the supported versions of the databases. The databases for Identity Governance are required for the product to work.

These system requirements provide server settings according to the size of your Identity Governance catalog. In a small catalog, you might collect fewer than 100,000 identities with 100,000 permissions and 80,000 groups.

On a virtual machine, set up the VM as Thick Provisioned.

Category	Minimum Requirement
Processor	◆ 4.0 GHz, single processor (small catalog) ◆ 4 physical cores of 2.0 GHz or higher per processor
Disk Space	◆ 60 GB (small catalog) ◆ 100 GB
Memory	◆ 16 GB (small catalog) ◆ 32 GB

Category	Minimum Requirement
Operating System	◆ Red Hat Enterprise Linux 8.8 (64-bit) or later patched versions of 8.*x* ◆ SUSE Linux Enterprise Server 15.4 or later patched version of 15.*x* ◆ Microsoft Windows Server 2022 or later patched versions of Windows Server 2022 **IMPORTANT:** Before installing Identity Governance, apply the latest operating system patches.
Virtual Systems	We support the databases for Identity Governance on enterprise-class virtual systems that provide official support for the operating systems where our products are running. As long as the vendors of the virtual systems officially support these operating systems, we support Identity Governance running on them. **IMPORTANT:** Ensure to configure the virtual machines running Identity Governance as Thick Provisioned.

Database	One of the following:
	
	◆ Microsoft SQL Server
	  ◆ Microsoft SQL Server 2019 or later patched versions of the SQL Server 2019
	  ◆ Microsoft SQL JDBC driver 10.2 or later patched versions of the Microsoft SQL JDBC driver
	◆ Oracle
	  ◆ Oracle 19c, or later patched versions of 19*x*
	  ◆ Oracle JDBC driver `ojdbc8.jar`
	◆ PostgreSQL
	  ◆ PostgreSQL 14.13, or later patched versions of 14.*x*
	  ◆ PostgreSQL JDBC driver 42.6.0 or later patched versions of the PostgreSQL JDBC driver
	◆ Vertica
	
	NOTE: Identity Governance supports Vertica as an Identity Governance custom metrics data store and as an external archive. You cannot use Vertica as a runtime database for Identity Governance, Identity Reporting, or Workflow Service.
	  ◆ Vertica 12.0 or later patched versions of 12.0..*x*
	  ◆ Vertica JDBC driver 12.0.*x*

Secure Communication	TLS 1.2 for secure communication

For information about the different options on how to create and populate the different Identity Governance databases, see Creating Databases for Identity Governance and Components in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

Identity Reporting Server System Requirements

Servers that host Identity Reporting when installing only for Identity Governance need to meet the same minimum requirements as for the Identity Governance server and databases.

Identity Reporting is a separate product that comes with Identity Governance that provides detailed reports about your business-critical processes and systems. It is optional to install Identity Reporting. If you determine that you will install Identity Reporting, you install it after you have completed the Identity Governance installation.

For more information about whether to install the components on the same server, see Recommended Production Environment Installation Scenarios in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

Identity Reporting also comes with Identity Manager, however, the reports provided are different if you install the version that comes with Identity Manager than the version of Identity Reporting that comes with Identity Governance. There are different requirements if you want to install Identity Reporting in an Identity Manager environment. For more information about the system requirements for installing in an Identity Manager environment that includes Identity Governance, see *System Requirements for Identity Manager*.

To see how to install Identity Reporting that comes with Identity Governance, see Installing Identity Reporting in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

Workflow Engine Server System Requirements

The Workflow Engine runs the workflows at runtime and manages the approval tasks for approvers. It comes with Identity Governance but it is optional to install the Workflow Engine.

IMPORTANT: Installing Workflow Engine on a remote server will be supported in a future release. If installing Workflow Engine, install it on the same Tomcat Server as Identity Governance.

Browser Requirements for Identity Governance and its Components

To log in to Identity Governance on their local devices, users must have one of the following browser versions, at a minimum:

Computers

- Apple Safari 17.6
- Google Chrome 128.0.6613.119
- Microsoft Edge Browser 128.0.2739.42
- Mozilla Firefox 129.0.2

IMPORTANT: The browser must have cookies enabled. If cookies are disabled, the product does not work.

Audit Server System Requirements

Identity Governance generates the common event format (CEF) events which you can forward to an audit server to generate audit logs that can help prove compliance with regulations. Enabling auditing in Identity Governance is optional.

If you decide to use auditing, you must have your audit server installed and running. Identity Governance does not install the third-party audit servers for you. This section provides the minimum version of the audit servers where you want to send audit events from Identity Governance. We support the following audit servers using `syslogger` for use with Identity Governance:

- ArcSight Enterprise Security Manager Suite 7.6 (Including ArcSight Enterprise SmartConnector 8.4)
- Sentinel 8.5
- Sentinel Log Manager 8.5
- Splunk 9.0.80

To determine where you should install the audit server, see Recommended Production Environment Installation Scenarios. You can enable auditing during the installation of the components or you can enable auditing after you have installed the components. It depends on your environment and your needs.

Email Notification Server System Requirements

Identity Governance can send email notifications to managers, reviewers, administrators, or other people who must receive notifications about events or processes occurring. To be able to send emails and ensure that there are not any lapses in communication, you can install Apache ActiveMQ to guarantee that Identity Governance sends notifications using SMTP. Enabling email notifications is optional. If you choose to enable email notifications, Identity Governance supports the following:

- Apache ActiveMQ 5.17.6

You can enable email notification during the installation of Identity Governance or Identity Reporting or you can enable email notifications after the installation. It depends on your environment and your needs.

Supported Upgrade Paths and Integrated Components

This section outlines the supported upgrade paths and integrated component versions.

Supported Upgrade Paths

Supported upgrade paths for Identity Governance and related products are listed below.

- Identity Governance 3.7, 3.7.3, or 4.2 to 4.3.1
- Identity Reporting 6.7, 6.7.2, or 7.2 to 7.3.1

Integrated Components

- Form Builder 1.5.2.0000
- Identity Reporting 7.3.1
- Workflow Console 1.0.8.0100
- Workflow Engine 1.0.8.0100 on the same Tomcat server as Identity Governance

Supported Identity Manager Drivers and Packages

Identity Governance provides IDM entitlement application definition and application templates to collect account and permission entitlements from an on-premises Identity Manager environment. To successfully collect all accounts and permissions, the supported drivers must be running. Find below a list of the Identity Manager and Identity Governance supported drivers.

- Drivers in Identity Manager 4.8.4 (https://www.netiq.com/documentation/identity-manager-48-drivers/) and later patched versions
- Identity Governance Assignment collection: MFIGASGMTCOL_1.0.0.20220110104142

Driver	Minimum Driver Version	Minimum Package Version
Active Directory	4.1.3.0	• NOVLADENTEX_2.5.7.20190610155012
Azure AD	5.1.7	• MFAZUREENTL_1.0.2.20211118165327 • MFAZUREXROLE_1.0.2.20211125114229
Bidirectional	4.0.4.0	• NOVLEDIR2ENT_2.2.7.20211118165416
Groupwise REST	4.0.1.1	• NOVLGRPWRAEN_3.1.1.202112091738838
JDBC	4.2.2.0000	• NOVLJDBCBISN_2.0.0.20211208134901 • NOVLJDBCENTI_2.4.4.20211208135336 • NOVLORAINSYN_2.1.0.20211208135824 • NOVLSQSIDSYN_2.1.1.20211220115351 • NOVLPGSINSYN_2.1.1.20211220124959
Lotus Notes	4.1.2.0	• NOVLNOTEENT_2.4.1.20211118113748
SAP User Management	4.0.4.0	• NOVLSAPUFENT_2.3.5.20211217153914 • NOVLSAPUMIG_1.0.0.20211217153953
SCIM	1.0.1.0200	• NETQSCIMENT_1.0.1.20211223151040 • NETQSCIMBASE_1.0.1.20211223151032
Workday	1.3.0.0100	• NETIQWDENT_1.0.0.20210505165701

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment link on each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com (mailto:Documentation-Feedback@microfocus.com).

Legal Notices