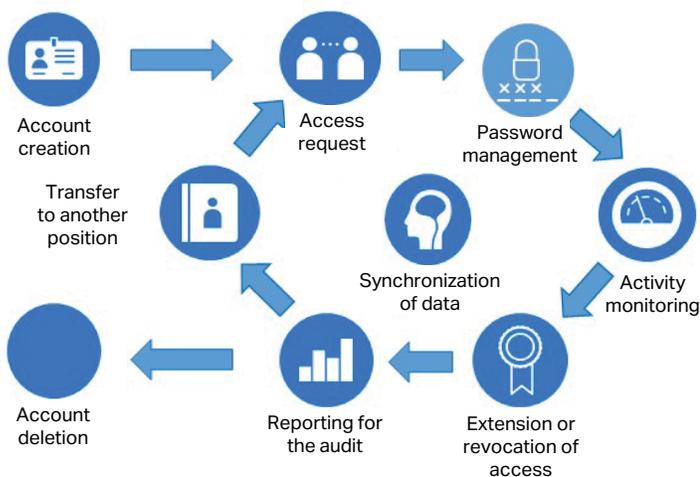


# NetIQ Identity Governance and Administration

A NetIQ identity governance and administration (IGA) solution that helps organizations manage the lifecycle of accounts and access rights to information resources.



The global digitalization of business and the spread of hybrid IT infrastructures have made managing user credentials and access to information systems one of the most important—and at the same time challenging—tasks to solve. NetIQ by OpenText™ solutions offers a set of integrated components for the complete, automated management of user credentials and access. From the moment the account is initially created, and throughout its lifecycle, user attributes are synchronized across all the organization's information systems. Authorized employees may periodically check users' access rights. Current rights can be extended, and unnecessary rights can be revoked with a single click. When deleting an account, all access rights for the employee are revoked from all information systems in a matter of seconds. This reduces the risks associated with the misuse of credentials belonging to dismissed employees.



## Main Possibilities of the Solution

### Synchronization of Credentials

Starting from the moment when employees are hired and their data is entered into the HR system, NetIQ Identity Manager by OpenText creates a corresponding record in its centralized account information storage system, Identity Vault. Users' credentials are then transferred automatically to all systems connected to NetIQ Identity Manager, and accounts are created in these systems. As a result, new employees can start performing their full duties on the first day of work, with access to all the necessary information resources within the organization. If it is necessary to make changes to the user's credentials in the future (for example, in the event of periodic password changes), NetIQ Identity Manager will make sure that these changes are correctly reflected in all connected systems. When employees transfer to another position, a review of their access levels may be required. [NetIQ Identity Manager](#) automates

the process of granting new permissions to a user and, if necessary, revoking old privileges. When employees are dismissed, their credentials are either deleted from the HR system or marked as inactive. NetIQ Identity Manager automatically makes the appropriate changes in all connected systems, revoking the access rights of the employees. As a result, the relevant users will no longer have access to the organization's critical systems within a few seconds of the management decision. This avoids the risks associated with dismissed employees gaining access to important corporate information.

### Role-Based Administration

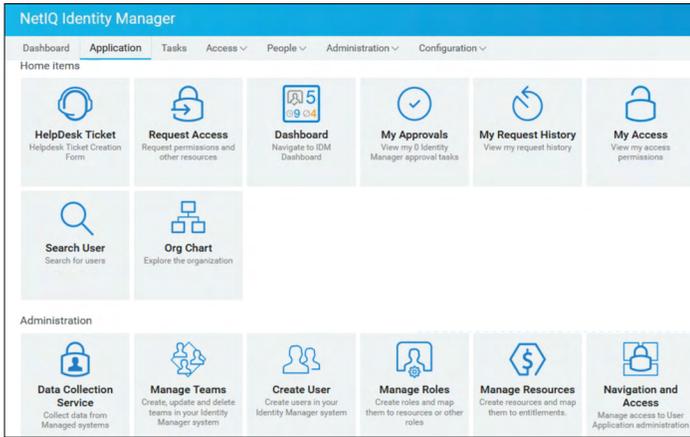
To increase the flexibility of the solution, NetIQ Identity Manager assigns user access rights to resources through specific roles rather than applying them directly. The list of roles can either reflect the organizational structure of the company (departments, units, etc.) or have a special structure (for example, associated with the organization's key projects). An individual user can have one or several roles in NetIQ Identity Manager. Access rights are granted to a particular role. This ensures transparency for auditors and ease of managing access to the information resources of the organization.

### User Self Service

The NetIQ Identity Governance and Administration (IGA) by OpenText minimizes routine management work while meeting the needs of organizations with complex business logic when providing access. NetIQ offers built-in tools for creating approval workflows, allowing approvals for privileges to be obtained from stakeholders. The system also supports delegation of roles and powers in accordance with the described procedure.

The NetIQ Self Service Password Reset by OpenText module included in NetIQ Identity Manager reduces the load on the IT Service Department. Using the module, the organization can implement mandatory policies related to user passwords, including the frequency of password changes and password complexity.

Users can view and edit their personal information in the corporate directory through the self-service portal. The information entered in the directory will be reflected in all systems that NetIQ Identity Manager is synchronized with. This reduces the administrative load on company staff and allows users to keep their corporate profiles up to date. In addition to updating their profile, the self-service portal allows employees to request access to the necessary resources in the organization's resource catalog for themselves or their reports. Once created, the request will be sent along the pre-defined approval workflow in NetIQ Identity Manager.



An additional benefit of NetIQ IGA is the possibility of performing a comparative review of existing user access rights. This simplifies the process of granting and changing permissions and also provides a visual representation of a given sample of employees.

The NetIQ IGA solution allows policies to be configured for separation of duties, a process in which more than one person must perform critical business actions. This minimizes the risks of both intentional abuse and basic human error. The requirement to share powers is in many regulatory documents, and auditors check compliance often. Depending on the NetIQ IGA settings, the system either generates a refusal or requires special approval for requests for excessive powers.

### Reporting System

NetIQ IGA offers Identity Intelligence and Identity Reporting modules for visual analytics and reporting in the embedded IGA solution.

Identity Intelligence is designed for analyzing NetIQ IGA processes in an organization. Typical examples of its use include:

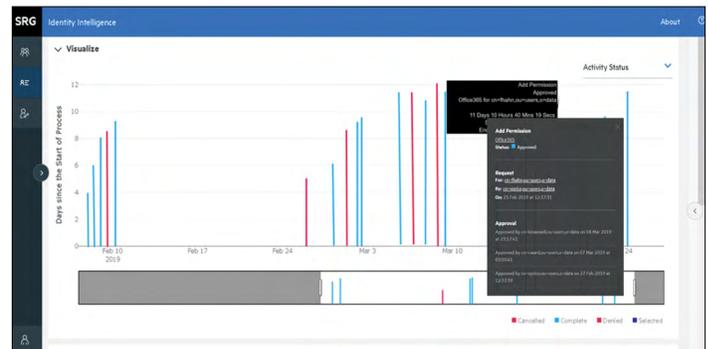
- **Detecting and responding to process violations.** Monitoring and detecting unexpected events and exceptions.
- **Preparing for audits.** Collecting information and demonstrating compliance with industry requirements and business rules to inspection bodies.
- **Fine-tuning NetIQ IGA processes.** Analyzing the similarity of assigned roles and trends in granting access levels. Identifying bottlenecks and potential problems.
- **Supporting internal investigations.** Identifying who had access to what at a certain point in time.

### Auditing of Access Rights

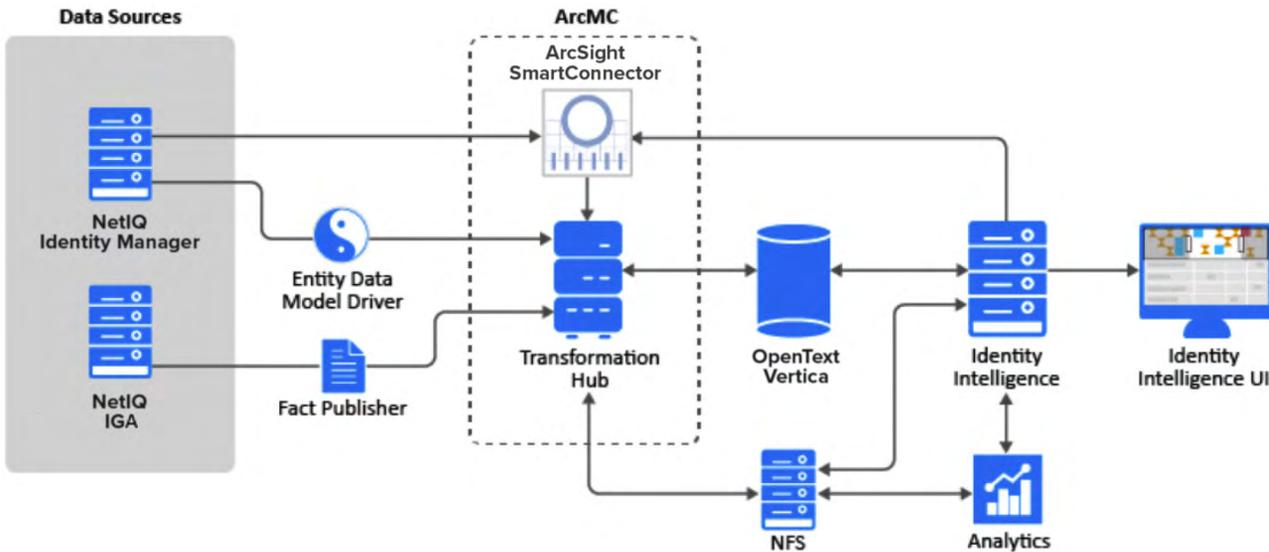
The NetIQ IGA module is designed for centralized auditing of access rights. It makes it possible to gain a clear picture of who has access to what within the organization. With the help of periodic certifications, authorized employees can renew existing employee access rights to various resources, as well as revoke them if necessary. This makes it possible to implement the principle of least privilege in the organization, giving users only minimum access rights to corporate resources.

User access comparison	Sam Oliver	Elise Grace	Anil Patel	Carly Cox
Google apps	X	X	X	X
Adobe creative cloud				
GotoMeeting	X		X	X
GotoTraining	X		X	X
GotoWebinar		X		
NSS Forums		X		
SAP User Access Report				
SAP Account ownership				
SalesForce Community Cloud	X	X		
Salesforce Sales Cloud				
VersionOne	X	X	X	
MicroFocus intranet	X	X	X	
Google Analytics				
Security Senses				X
Harvard Business Review				X
Travelflow 360				
Leadership dashboard				
Weekly KPI review				
Identity Governance overview report	X	X	X	

[Request Changes](#)



The Identity Intelligence architecture is based on the OpenText™ Vertica™ analytical database. This ensures high performance when creating analytical reports, through optimal use of computing resources.



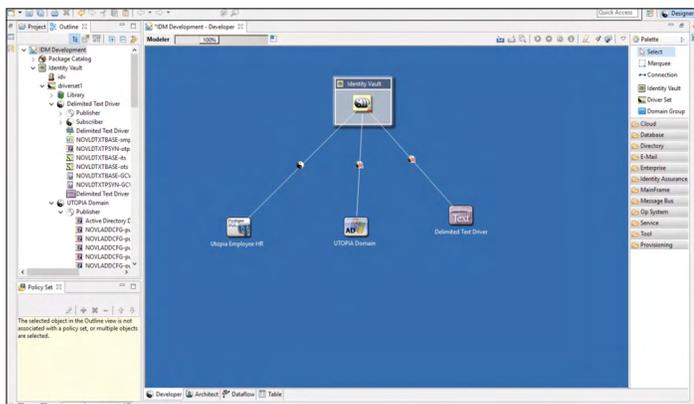
The Identity Reporting module is designed for creating and sending reports about the NetIQ IGA system configuration: a list of synchronized attributes, what is associated with what in connected systems, settings policies for passwords, and much more.

### Solution Design

NetIQ Identity Manager contains utilities to simplify planning, configuration, and implementation of the NetIQ IGA solution in an organization. NetIQ Identity Manager Designer is one of these utilities. It is designed for architects and allows all the components of an IGA

solution to be visualized, with a diagram of their interaction. Designer also makes it possible to document and pre-test a solution before implementing it in a production environment within an enterprise.

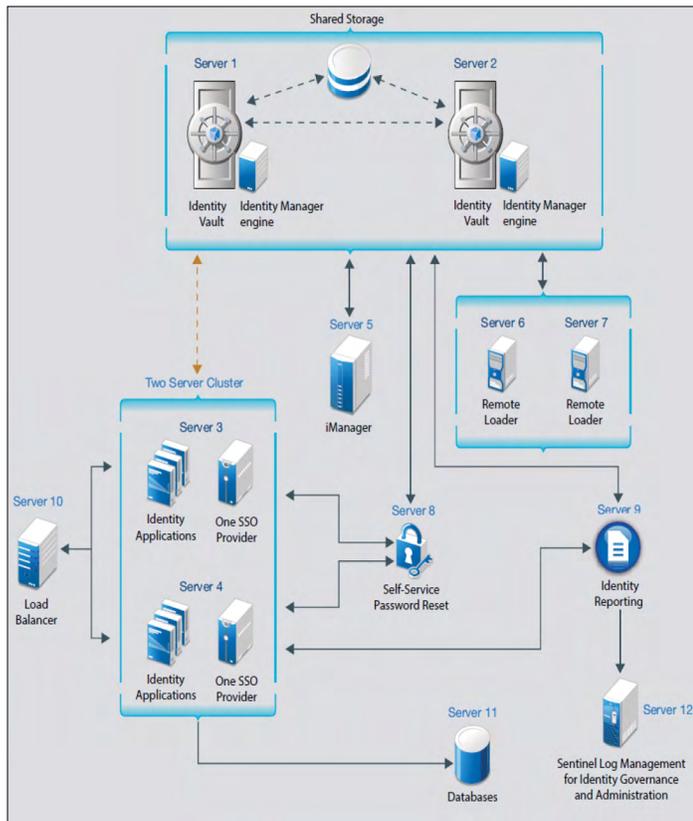
Leverage data from another utility, NetIQ Analyzer by OpenText for NetIQ Identity Manager, when preparing an IGA solution: create a data diagram, determine business logic for collecting data, configure the correspondence of fields between connected systems, etc.



### Scalability and Fault Tolerance

All critical components of the solution are supported in fault-tolerant mode. This means that if one of the cluster nodes of an IGA service fails at some point in time, the corresponding service is automatically started on the backup node. First of all, the NetIQ IGA solution provides a high level of scalability, thanks to the organizational features of a centralized credential storage system—NetIQ Identity Vault by OpenText. This can manage billions of objects. Secondly, the NetIQ IGA solution supports horizontal power build-up and load balancing between the key components.

It is also worth noting that most components offer cross-platform support. For more information about the supported platforms and their versions, see the technical documentation at [www.microfocus.com/documentation/identity-governance-and-administration/](http://www.microfocus.com/documentation/identity-governance-and-administration/).



Depending on the NetIQ Identity Governance settings, the system either generates a refusal or requires special approval for requests for excessive powers.

### Localization

As a global company, OpenText™ offers localized user interfaces for many of its products. In particular, the interfaces of the following components of NetIQ Identity Manager are available in Russian: iManager, Identity Dashboard, Identity Applications Administration, Identity Reporting, Identity Approvals, User Application. In addition, the “Identity App User Guide” is available in Russian.



The Identity Reporting module is designed for creating and sending reports about the IGA system configuration: a list of synchronized attributes, what is associated with what in connected systems, settings policies for passwords, and much more.

### About NetIQ by OpenText

OpenText has completed the purchase of Micro Focus, including CyberRes. Our combined expertise expands our security offerings to help customers protect sensitive information by automating privilege and access control to ensure appropriate access to applications, data, and resources. NetIQ Identity and Access Management is part of OpenText Cybersecurity, which provides comprehensive security solutions for companies and partners of all sizes.

**Connect with Us**

[www.opentext.com](http://www.opentext.com)



**opentext™** | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.