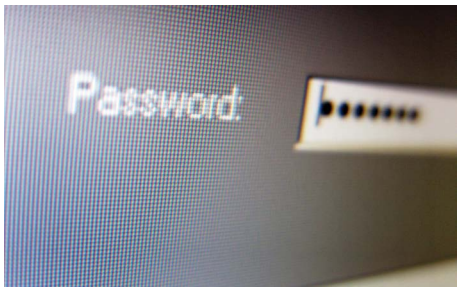
Product Flyer
Security



NetIQ Identity Manager

How do enterprises ensure efficient, consistent and secure access to corporate assets within and beyond their firewalls? With increasing demands on resources, the expanding workplace brought on by mobility and BYOD, internal and external audit controls, and cloud computing, enterprises need Identity Manager.

Identity Manager at a Glance:
The foundation for identity-powered solutions, Identity Manager is designed to manage the complete identity lifecycle in a modular yet integrated manner so you can address current and future needs as they come.

With Growth Comes Complexity and Security Challenges

As enterprises evolve, they are constantly challenged to provide timely access to new applications and services. With the explosion of devices, ease of access brought on by the consumerization of IT and connectivity everywhere you go, enterprises are challenged to meet the demand for a consumer experience at work while maintaining adequate management of access to applications and data. Enterprises implement various processes to handle this challenge, but to be successful, a robust and effective management of identity is foundational to provide the flexibility needed to adjust to changing business needs.

With constant connectivity being the new norm, the workplace is now anywhere and business user preferences have shifted towards mobile device interfaces. Users wonder, "why can't I have access to what I need now" or "why can't I just download an app" and "why am I being asked for another password?" These consumerization trends toward convenience are dictating technology choices.

An equal, if not greater, challenge is ensuring the protection of corporate assets, data and compliance with internal and external controls. Preventing unauthorized access to sensitive information is enormously challenging when cloud applications and mobile devices are outside of the control of IT.

Striking the balance of ease of use with adequate controls can be a formidable task. To answer these challenges, your organization needs a comprehensive solution that manages user identities and their associated attributes in various applications. Those applications may be on-premises, partner-delivered or software as a service. An identity foundation supports appropriate access and can enrich security data to understand how and when users are utilizing corporate assets. An integrated approach to identity, access and security can provide users with that consumer-like experience while efficiently and effectively responding to threats and answering auditors.

Identity Manager Provides a Comprehensive Approach to Complex Requirements

NetIQ® Identity Manager powers the entire identity management lifecycle, managing identities and their associated attributes to minimize privileges. This enables your organization to reduce the costs of manual account management and demonstrate compliance while reducing the risk of unauthorized access. It delivers benefits for all critical stakeholders in your organization. For example, it allows your:

- CIO to decrease the costs of compliance and offer more convenient access, so the business can take advantage of new opportunities
- CISO to enforce enterprise-wide access compliance and security
- Line of business managers to keep their teams productive by providing immediate, role-based access to resources

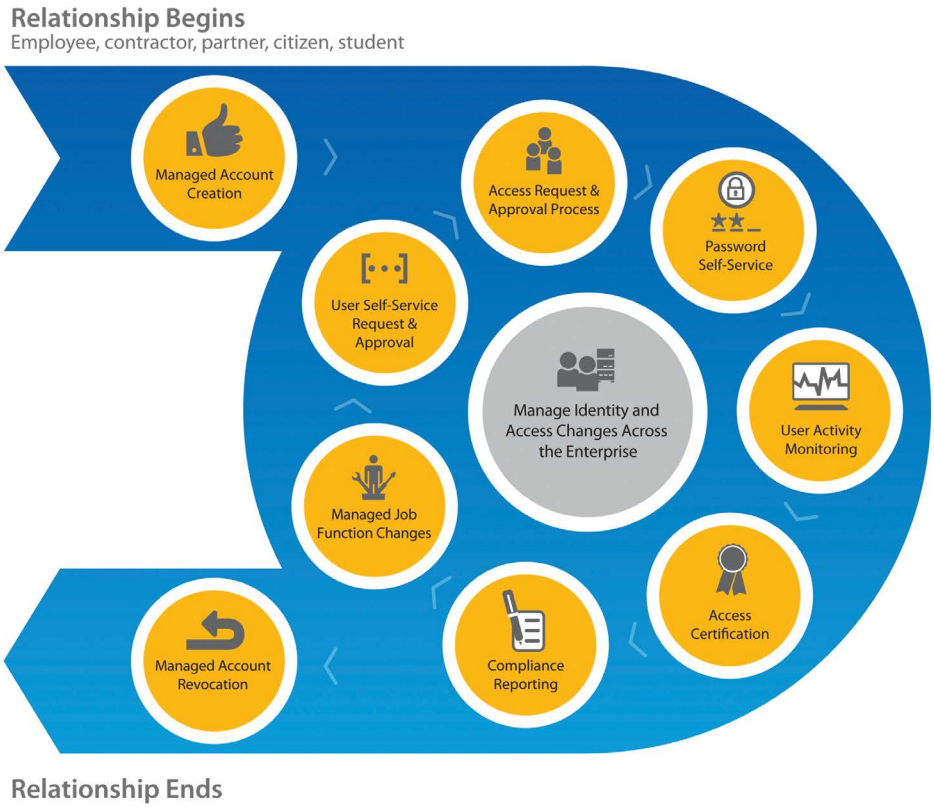


Figure 1. The Identity Management Lifecycle, Powered by Identity Manager

- IT managers to better manage resources and provide identity rich usage data to key stakeholders

Identity Manager manages the complete identity lifecycle in a modular yet integrated manner so you can address current and future needs as they come. Capabilities include:

Managed Account Creation, Revocation and Job Changes—Identity Manager offers an integrated roles-rules-workflow engine that provides the most efficient solution on the market today. Automate as much or as little provisioning as makes sense for your organization. The engine matches the way your organization does business by combining business rules with the efficiency of optional roles-based provisioning, allowing the workflow engine to handle standard approvals and exceptions such as separation-of-duties conflicts.

Managed Identity and Access Changes across the Enterprise—Identity Manager leverages an event-based architecture and enforces identity authority across all connected systems, ensuring identities are created only from appropriate sources. Additionally, Identity Manager enforces attributes authority, meaning systems that "own" components of the identity are the only ones that can change them, and if changed in non-authoritative sources, they can be automatically re-set to the value in the authoritative source. Both are critical when basing provisioning and access policies on attributes. Identity Manager uses an event-based architecture to respond in real time when a user-lifecycle event, such as a hire, termination, promotion or role change occurs, its data-management engine triggers policy-based processes with little-to-no human intervention.

Additionally, various applications, such as Microsoft SharePoint and SAP systems, have their own policy controls. Identity Manager makes it easy to integrate different entitlements into a consolidated catalog, leveraging the Identity Manager resource reconciliation service. This capability allows you to automatically discover permissions and use visual operations to map resources to appropriate roles or Identity Manager resources.

Seamlessly integrating different policy controls into one system quickly creates a unified governing mechanism that gives the right individuals a complete view of users' privileges, and empowers them to make informed decisions to evaluate and ensure the right people have access to the right resources. Not only does it deliver ease-of-use for initial setup but ongoing entitlement maintenance provides your organization with an agile system for managing resources and entitlements across all connected

With constant connectivity being the new norm, the workplace is now anywhere and business user preferences have shifted towards mobile device interfaces. Users wonder, "why can't I have access to what I need now" or "why can't I just download an app" and "why am I being asked for another password?"

systems, no matter where the systems are located—on premise or in the cloud.

Designer for Identity Manager offers the ability to produce access-request workflows that can dramatically reduce human error with no programming or customization required. In the graphical interface, your administrators can manage the entire project lifecycle, including designing and simulating various account management configurations without any scripting. As you expand Identity Manager to applications throughout your environment, the challenge of "data clean-up" can be time consuming. Analyzer for Identity Manager, a feature in Designer, efficiently displays and compares data from the identity vault and in connected systems, minimizing the time required to prepare applications for integration into the identity infrastructure, thereby minimizing the time and costs required to connect new systems.

User Self-Service Access Request and Approval Process—Using an intuitive, business-user friendly dashboard, business users can make and track access requests, and manage approval tasks all from one location. This self-service capability gives users control over their own identity information, so they can remain productive while reducing the workload on IT to handle requests. Full integration with the provisioning system means that users can get the access they need almost immediately, rather than waiting on manual fulfilment.

Approvers are typically business managers who travel for business and are on the go. Productivity is lost when requests from users have to wait on an approver to be in the office. In today's world, work is an activity and not a location. The Mobile Approval Application for Identity Manager is a native and secure mobile application that can be easily installed on any mobile device allowing approvers to be immediately alerted and respond to requests from anywhere.

Password Self-Service—One of the largest helpdesk costs is borne by helping users reset their passwords. Self Service Password Reset (SSPR) can virtually eliminate the helpdesk's involvement by allowing users to manage and reset their own passwords and even re-enable locked accounts while still maintaining the security your company requires.

With self-service password reset, users confirm who they are through methods before they're allowed to securely reset their passwords. Whatever method is selected for identification reflects the appropriate level of security your organization requires, and new passwords always adhere to requirements with as-you-type password rule enforcement. That way, there's no danger of replacing a strong password with a weaker one that doesn't meet the specified requirements. New passwords and unlocked accounts are effective instantly, so users can gain immediate access to their systems and applications.

User Activity Monitoring—Knowing and managing who has access to what is only part of the picture. Knowing what people are doing with their access—both historically and in real time—is equally important. Inadvertently allowing noncompliant, malicious or improper behavior could result in hefty fines, failed audits and severe damage to your enterprise's information stores and business reputation. The available Identity Tracking for Identity Manager combines the powerful information and provisioning capabilities of Identity Manager with a real-time correlation engine to give you a complete picture of who has access to what and what people are doing with their access. This user-activity monitoring and remediation solution works across all systems that Identity Manager provisions, significantly reducing the risks of non-compliant, malicious or improper behavior harming your enterprise.

Access Certification—Periodic access reviews are a compliance requirement and can consume significant time. IT wastes time compiling access entitlements and too much effort is required of the business to certify those entitlements. Identity Governance, a complementary solution to Identity Manager, automates much of that process by enabling organizations to review and certify user access to applications and systems across the enterprise. Identity Governance allows review of managed and un-managed applications, enables periodic and event-driven reviews, allows supervisor reviews, supports both application and permission owner reviews, streamlines reviews based on risk, and fulfills review decisions automatically or manually.

Compliance Reporting—Identity Manager is equipped with the comprehensive reporting capabilities that your organization needs to prove access compliance. The reports not only provide visibility into which systems users can currently access, but also into which systems they could access on specific dates or between two points in time. The reporting framework also allows users to create custom reports to suit their specific requirements, and to save the reports for future use. The policy-based data collection and storage capabilities provide strong compliance support so that your organization is always ready for its next audit.

Conclusion

The time-tested and award-winning Identity Manager delivers a complete solution to control who has access to what across your enterprise—both inside the firewall and in the cloud. It enables you to provide secure and convenient access to critical information for business users, while meeting compliance demands. You can be confident in knowing that it has achieved Common Criteria Certification at Evaluation Assurance Level 3 with augmented assurance (EAL3+).

> **"With centralized user identity management, we can present our company in a seamless fashion. Customers no longer need to remember multiple IDs and passwords to access their many different services with us."**
>
> **KANON COZAD**
> Senior Vice President and Director of Application Development
> UMB Financial Corporation

Contact us at:
www.microfocus.com

Like what you read? Share it.

Deployed by thousands of customers worldwide, Micro Focus® delivers a highly-scalable, differentiated identity management foundation, ensuring your organization can stay competitive, agile and secure—at low cost. It offers an integrated approach to deploying enterprise-wide solutions, or individual identity and access management products to address the most pressing needs first. With our products, and solutions, your enterprise gets the most value from its past, present and future IT investments.