opentext™ | Cybersecurity

Solution Flyer

Workday and NetIQ Identity Governance and Administration Integration

Accelerate business, govern access to resources, and adapt to risk with a Workday connector that detects identity lifecycle changes as they happen.

Workday with NetIQ Identity Governance and Administration Integration at a Glance

Enhanced Productivity

Automate business processes to provide timely access to resources.

Real-time Change Detection

Detect and respond to identity lifecycle changes as they happen in Workday.

Continuous Compliance

Identify and remediate risk through governance policies and access reviews.

The Importance of Real-Time Synchronization

As the authoritative source of HR information, your cloud-based Workday system contains critical information to support provisioning and governance processes across your organization. However, communicating and synchronizing this information effectively across your enterprise can be a challenge.

When Workday and other systems manage identity information in silos, efficiency and security are impacted. IT teams spend too much time managing disconnected systems through periodic reconciliations and manual processes. Users wait too long for access to applications and data, resulting in lost productivity. And approvers do not have the right data to make accurate review decisions, leading to rubber-stamping and far more access than is appropriate.

For effective identity governance and administration (IGA), a new approach is needed.

Adaptive Identity Governance and Administration

Your organization needs the ability to detect changes as they happen in Workday. Rather than waiting for point-in-time, periodic reconciliations, policies should be evaluated against a near real-time view of your environment. This enables you to automate access to resources, with interventions needed only for exceptions. Business users can focus on high-risk items, closing the gaps that result in too much access.

The Workday connector for NetIQ Identity Governance and Administration by OpenText enables a near real-time view of how Workday identity lifecycle changes impact access in other systems. As changes are made in Workday, you can initiate powerful workflows in connected systems to streamline access while protecting resources. You can also identify and respond to changes that impact risk, taking immediate action to adapt security controls.

By integrating Workday with NetIQ Identity Governance and Administration, your organization can support use cases across connected systems, including:

- Removing a privileged user's administrative access in Active Directory after termination in Workday.
- Reassigning expense approval responsibilities after a manager leaves the organization.
- Triggering a micro-certification for a user who is in a transition period between roles but has outlier access that does not fit into either role.

How it Works

NetIQ Identity Governance and Administration provides connectors to a wide variety of systems, including on-premises and cloud-based applications, directories, and databases. A real-time, event-driven security architecture enables automatic, two-way changes throughout the ecosystem, eliminating the need for periodic reconciliation and closing gaps that lead to abuse.

Connect with Us
www.opentext.com

With the Workday and NetIQ Identity Governance and Administration integration, your organization can:

- **Detect Workday changes in real time** for an up-to-date, unified view of identity and access across your environment.
- **Achieve continuous compliance** by automatically adjusting access to resources, sending alerts to managers, or submitting access changes to ITSM systems.
- **Free up IT resources** by translating even the most complex identity processes into automated workflows for provisioning and fulfillment.
- **Enforce governance controls**, including the remediation of excessive access, orphaned accounts, and separation of duties violations.

As part of a comprehensive identity governance and administration program, the Workday and NetIQ now by OpenText™ certified integration enables your organization to accelerate business, govern access to resources, and adapt to risk. This flexible, scalable, and powerful foundation enables you to manage identities and govern access across your enterprise landscape.

Learn more at
www.microfocus.com/en-us/cyberres/identity-access-management/identity-governance-administration

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.

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.