

OpenText NetIQ AD Bridge

Use Active Directory to manage and secure Linux, extending privilege and policy tools for better security, governance, and compliance

Benefits

- Extend Active Directory control to Linux resources
- Unify environments for simplified compliance
- Leverage existing tools for enhanced security and future readiness

Managing and securing both Windows® and Linux® resources can be complex, especially in diverse IT environments. Inconsistent policies and inefficient tools create challenges for IT and security teams, increasing administrative overhead and security risks.

Simplified Linux management with Active Directory

OpenText™ NetIQ™ AD Bridge extends Active Directory (AD) controls to Linux systems, unifying management and security across your infrastructure. By leveraging existing AD investments, it streamlines administration, strengthens policy enforcement, and improves compliance. IT teams can ensure consistent security policies, reduce manual effort, and seamlessly prepare for future cloud and SaaS integrations—all while maximizing their current AD setup.

Comprehensive IAM coverage

Integrating with OpenText's identity-powered privileged management and delegation tools, AD Bridge consolidates identity and access management under a single vendor. This unified approach eliminates redundant tools, reduces complexity, and provides complete visibility across Windows and Linux environments.

Consistent policy enforcement

Extend AD policies to Linux, ensuring security and compliance across on-premises, hybrid, and cloud environments. This eliminates the need for duplicate policies or additional tools while maintaining a uniform security posture.

Reduced security risks

By integrating native firewall services into IPTables, AD Bridge automates firewall management and minimizes vulnerabilities. This proactive approach reduces human error and strengthens overall security.

Granular privilege control

The ActiveView model enables precise privilege management, ensuring only authorized users access sensitive resources. This fine-tuned control enhances security while simplifying compliance efforts.

Privileged session monitoring

Non-intrusive monitoring provides real-time visibility into privileged activities without disrupting workflows. IT teams can detect anomalies, mitigate risks, and maintain compliance seamlessly.

Efficient workflow automation

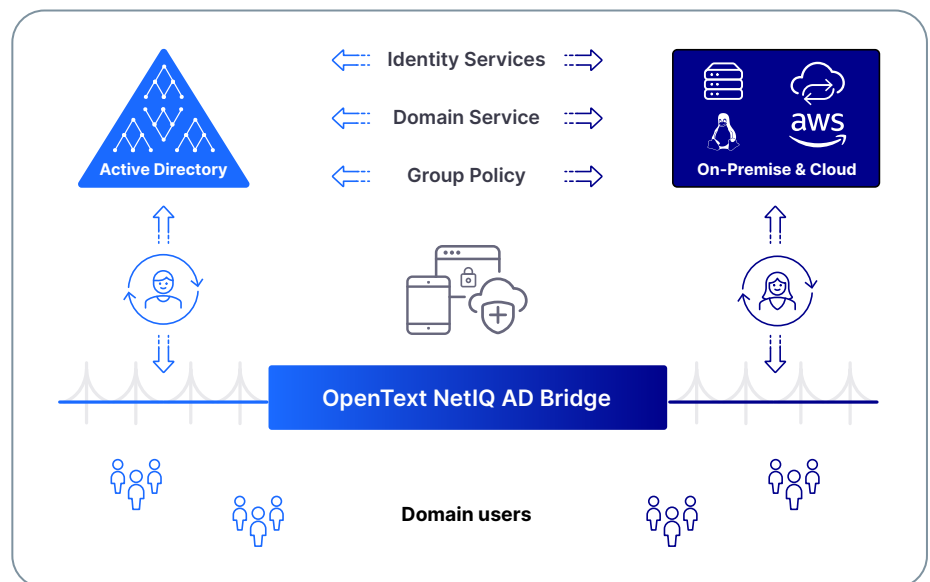
Built-in workflow automation streamlines administrative tasks, reducing manual intervention and improving operational efficiency. IT teams can enforce security measures more effectively while enhancing productivity.

Complete audit coverage

Comprehensive audit and reporting capabilities consolidate access and activity data across Windows and Linux environments. This simplifies compliance management and provides clear insights into security trends.

A streamlined, secure approach

AD Bridge simplifies Linux management by integrating seamlessly with Active Directory, enabling centralized control, real-time security enforcement, and consistent policy application. Unlike fragmented solutions, it unifies policy enforcement across hybrid environments, reducing complexity and ensuring compliance. With near real-time updates and proactive security enforcement, OpenText delivers a streamlined, secure approach to Linux administration.



AD Bridge brings everything together under one management system. It installs an agent on non-Windows devices, letting you manage them all in one place.

It mainly does three things:

1. **Identity Services:** Integrates these devices into Active Directory for unified user management and authentication.
2. **Domain Services:** Extends Active Directory domain services to non-Windows devices, allowing them to be managed as part of the domain.
3. **Group Policy:** Applies and enforces group policies on these devices through a single interface, ensuring consistent configuration and security settings.

In short, AD Bridge extends your familiar Active Directory tools to new areas, allowing you to use existing Windows policies and management practices in new environments.

Features and components	Benefits
Identity Services	Integrates non-Windows devices into Active Directory for unified user management and authentication.
Domain Services	Extends Active Directory domain services to non-Windows devices, making them part of the domain.
Group Policy	Applies and enforces group policies on non-Windows devices through a single interface.
Unified Management Console	Provides a centralized interface to manage all devices, both Windows and non-Windows.
Configuration Management	Manages and enforces configurations on endpoints through a common interface.