Identity Tracking: An Extension of Identity Management

Your organization’s identity management, access management and security information and event management (SIEM) systems are indispensable components of its efforts to comply with policies and regulations. As essential as these systems are, however, they could do much more for your organization than they do now. Each of these systems uses its own data store, creating silos of information. Integrating the information from these systems would enhance their security and compliance benefits, separately and collectively. This white paper reviews the separate functions of identity management, access management and SIEM systems, and explains the benefits of integrating identity and security information using NetIQ® Identity Tracking for Identity Manager™.
This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

Copyright © 2012 NetIQ Corporation and its affiliates. All Rights Reserved.

Access Manager, ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Cloud Manager, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PlateSpin, PlateSpin Forge, Privileged User Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its affiliates in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.
# Table of Contents

Identity, Access and Security—How do I Manage All of These? ................................................................. 1

Identity Management ................................................................................................................................... 2

The Components of an Identity Infrastructure ......................................................................................... 5

The Identity Vault and Integration Modules .............................................................................................. 5

Rules, Roles and Requests ....................................................................................................................... 8

Security Management ............................................................................................................................. 10

Security Integration with Identity Management ...................................................................................... 11

Next Steps: Integrating Access Management ......................................................................................... 13

Conclusion ................................................................................................................................................ 15

About NetIQ .............................................................................................................................................. 16
Identity, Access and Security–How do I Manage All of These?

IT has become the cornerstone of most organizations’ efforts to achieve compliance. With never-ending requirements to cut costs, maintain business agility and mitigate risks, IT departments are finding ways to automate enforcement processes for policies they originally developed on paper. To achieve this goal, they are relying on identity management, access management and security information and event management (SIEM) technologies. Identity and access management products determine users’ identities and appropriately grant and revoke access to your organization’s resources. SIEM provides an enterprise-wide view of who is accessing what. In short, identity and access management defines who should have access to your organization’s resources, and an important function of SIEM identifies who is accessing these resources—both functions are integral components of policy and regulatory compliance.

Modern identity and access management products are extremely adept at validating identities, provisioning resources and enforcing access roles; and security information management solutions do an excellent job of aggregating security data from across the organization. But these technologies contain siloed data that would be invaluable if it were integrated. Unfortunately, in most organizations one silo holds identity and access management policies (which define who gets access to corporate applications) and another contains security data (which indicates who is accessing corporate applications).

Bridging the gap between identity and security, NetIQ® Identity Tracking for Identity Manager provides a real-time, holistic view of the organization and its compliance posture. NetIQ Identity Tracking for Identity Manager cross-validates identity and security information in real time, so your organization always knows which users are accessing what, when they are doing it and if they are authorized. If situations arise that are out of the norm, you can take appropriate actions in real time—by sending simple notifications or initiating full remediation (revoking user access), for example. Your organization’s policies and processes can determine one or several remedies for violations.

By combining user provisioning and security monitoring, NetIQ Identity Tracking for Identity Manager delivers business-process automation that gives users the appropriate resources, validated in real time, to ensure compliance with organizational policies—eliminating the gaps that have left so many organizations at risk. Rather than a piecemeal solution made of complex (and expensive) product silos, NetIQ Identity Tracking for Identity Manager integrates these silos to deliver an organization-wide view and governance-defined policy enforcement.
Identity Management

Who has access to what? Why? Who granted the access, and when? These are just a few of many standard questions IT administrators and security personnel must answer during any audit process. Identity management is intended to reduce the complexities of provisioning, automate the provisioning process and electronically maintain the policies that determine how resources are provisioned. Identity Manager uniquely addresses provisioning complexities by automating the provisioning processes in real time. As changes occur throughout the organization, the changes are replicated across all the sources that house identity data instantaneously. The result: Systems consistently and correctly provision access to corporate resources without synchronization delays.

Figure 1: Integrated identity management, access management and SIEM
Figures 2: Identity Manager high-level architecture
Figure 3: High Level Architecture for a combined NetIQ Identity and Access Management and SIEM solution.
The Components of an Identity Infrastructure

One of the most critical components of an identity management deployment is the ability to connect to disparate identity stores throughout the enterprise. To achieve this, you need a robust policy-definition engine that you can easily configure to stringently maintain the integrity of identities and their attributes. This engine must also be flexible enough to match the nuances of your organization’s policies.

The Identity Vault and Integration Modules

At the center of Identity Manager is the Identity Vault, which maintains all of the rules, roles and workflow-request definitions that determine how your system provisions applications to users throughout the organization. The core of this technology is an industry-unique event bus, patented replication technology and rich access control list (ACL) support for ease of management and execution. The event bus allows for distributed management and authoritative control while providing centralized policy and process governance.

Each application is connected by an Identity Manager Integration Module, which allows bi-directional communication between the Identity Vault and the remote identity store. The Integration Module consists of the policies that determine user-account management on the target system and various entitlements (for example, group memberships). Managing the data flow from remote identity stores to the Identity Vault, along with various user attributes throughout systems, ensures that only the proper sources can initiate a provisioning activity, and that the proper systems maintain authority over user attributes (Figures 2 and 3).

A human resource (HR) system such as SAP stores basic employee information, and therefore generally acts as the authoritative source for initiating the provisioning process. Since the HR department is usually responsible for knowing when users are hired, when their attributes change (because the users change departments or move to new physical locations, for example) and when they leave the organization, the HR system becomes the default source for basic provisioning actions. (See Figure 4)

As the identity management system provisions resources to users, it appends additional information to their identities. For example, when IT creates a user’s email account, the identity management system adds a new component to the user’s identity profile—the user’s Internet email address. The identity management system would most likely share this additional piece of information with the HR system. However, a challenge of bi-directionally synchronizing identity data stores is maintaining authority for each attribute so that a non-authoritative source cannot inadvertently update users’ identities. What if an HR employee modified a shared email attribute in SAP? Propagating this bad data to the email system could cause a serious issue. Similarly, if a directory administrator changed the user’s department in the corporate directory, this change would propagate back to the HR system, causing more problems.

You can avoid these problems with Identity Manager by creating a policy for each connected system. Identity Manager allows administrators to define which systems are authoritative for each shared attribute, and how the system should react when someone changes an attribute. When someone changes an identity attribute, the Filter Policy determines how to handle the change. The Filter Policy (shown in Figure 5) enforces how Identity Manager shares the data. If a non-authoritative source initiates the change, Identity Manager automatically resets the data to the value in the Identity Vault, which the authoritative source populates.
Figure 4: Bi-directional policy-based connectivity
Figure 5: Filter Policy
Rules, Roles and Requests

Rules, roles and requests underpin most provisioning deployments, but depending solely on one of these provisioning methodologies can lead to an ineffective or incomplete provisioning solution. The ability to seamlessly intermix the capabilities of rules-, roles- and request-based provisioning enables organizations to use the right methodology for each job (See Figure 7).

Figure 7: Rules-, roles- and request-based provisioning
Rules allow users to seamlessly and easily access appropriate applications with automated provisioning based on pre-defined criteria. When users meet proper conditions, provisioning processes occur automatically.

However, some provisioning processes require human interaction: For example, it may be necessary for application owners or managers to approve access to certain resources. Defining how workflow and approval requests function in provisioning processes is easy with Identity Manager. It includes a graphically driven development environment, which allows your administrators to easily define the flows, approvers and audit components of workflow processes. (See Figure 8) The same flexibility for creating workflow definitions is available for defining approval processes. Identity Manager includes serial, parallel, individual, group and quorum approval capabilities in addition to support for digital signatures.

Roles based provisioning can be very effective when a subsection of users need similar entitlements to applications. Identity Manager (Advanced Edition) allows organizations to define:

- Roles
- Segregation of duty (SoD) violations between roles
- Attestation processes for users’ identity attributes
- Possible roles for particular users
- Possible roles and members that Identity Manager can use for validation, certification and re-certification

Identity Manager has the capability to provision users based upon one or more of these methodologies using a single, intuitive policy-based engine. By incorporating rules, roles and requests into a common provisioning engine, Identity Manager reduces the administrative burden and end-user confusion by eliminating multiple, potentially overlapping or conflicting products, and consolidating multiple product interfaces into one.
Performing IT audits and meeting standards and regulatory requirements are mandatory for most organizations. In fact, organizations are spending significant time and energy scrutinizing their security and event logs to track who has accessed which systems, what activity took place and whether it was appropriate. Organizations are increasingly looking toward data-driven automation to help ease this administrative burden. The security management market has taken shape to provide focused solutions to the problem.

Security management automates the process of analyzing security, network and application logs. When coupled with identity and access management, a security management solution provides the ability to link system access to individual users (See Figure 9). According to most of today’s regulations, tracking and reviewing access is a primary audit requirement, especially for access granted with administrative privileges.
The combination of these two technologies—identity management and security management—provides a framework that enables your organization’s policies to drive IT policies, and to deliver the evidence it needs to demonstrate compliance with internal policies, industry standards and government regulations—including Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Federal Information Security Management Act of 2002 (FISMA) and others.

Security Integration with Identity Management

1. The security management system gathers security events from applications and systems spread across your organization. The integrated system analyzes and correlates events in the iScale Message Bus for potential policy violations, then stores the events in a central data repository for historical analysis.

2. As the integrated system identifies security events in various applications, network devices and other stores, Identity Manager provides identity context, inserting user-specific information into the security events.

3. The integrated system collects and stores operational events in Identity Manager, NetIQ® Access Manager and the Identity Vault.

Figure 9: Integrated security and identity management systems
4. The integrated system analyzes all events. If event correlation detects suspicious activities or policy violations, the integrated system triggers remediation activities to protect your organization from the potential security threat. This can take the form of provisioning activities or approval workflow processes automated by Identity Manager.

By mapping security information to identity profiles, NetIQ Identity Tracking for Identity Manager enables your organization to improve its ability to identify and investigate security breaches. Without this integration, if a user attempted to access a sensitive customer database he was provisioned to by overriding security protocols, database administrators would only know that someone tried to break in. With identity-enabled security information, these same administrators could refer to an easy-to-read, real-time dashboard showing who attempted the security breach (Figure 10), what else he or she has been doing recently and what other accounts the user has across the enterprise (Figure 11). This clear, graphical overview of identity and security throughout your organization enables administrators make sense of mountains of security data, identifying legitimate threats while eliminating false positives.

Identity management systems can identify which users have access to which applications. But are these employees actually using the applications? You can answer this question only when identity management and security management are integrated through NetIQ Identity Tracking for Identity Manager. Administrators gain an additional level of inspection and validation—providing visibility into not just which users have access to corporate applications, but also how often they log in to and use the applications. Tracking application usage is an excellent way to gauge whether your corporate policies and role definitions actually line up with day-to-day operations.

Providing identity context to security events significantly enhances your ability to act on security data. For example, using the identity data in NetIQ Identity Tracking for Identity Manager, your administrators can review user-specific security records that provide real-time and historical identity information.
Automating identity-driven policies and processes and continually monitoring your IT environment allows for immediate notification when out-of-policy or non-compliant behavior occurs. Further, the ability to correlate device-based event logs with the activities of individual users allows your administrators to take timely action.

To illustrate, consider the example of an IT administrator who provisions an employee with access to the accounts receivable invoicing system. Security personnel soon detect that, unbeknownst to the IT department, the employee is attempting to generate payments, a clear violation of the segregation of duties. The ability to correlate the authorization attempts with the user’s identity provides the information security personnel need to manage the risk. When problems are uncovered, organizations can remediate them based on policies and processes. The actual remedy can range from simply notifying appropriate individuals, thus alerting them to the violation, to automatically removing a user’s access rights to all systems. Tightly coupling identity management and security management capabilities makes a range of responses possible.

For an example of a more proactive approach, imagine the same user attempting to access an application to complete a job assignment. This time the system requires approval, which has not been granted. Integrated security events and identity information enables the access management system to automatically interpret the user’s action in the context of his or her identity profile, and the identity management system then enables the user to request access. This proactive approach is much more user friendly than an approach that merely tells users they’ve been denied access.

Next Steps: Integrating Access Management

Granting users access to resources should be automatic and seamless. Identity-enabled access management fulfills this requirement by dynamically provisioning users with access to needed corporate resources.

Under ideal circumstances, provisioning resources to users automatically updates access policies. However, in some circumstances, users legitimately attempt to access resources that fall outside of their defined roles. When this happens, they generally receive a very IT-centric “access denied” error message, which leaves them wondering what to do next.

The following scenario illustrates a common use case for integrating identity and access management.

Josh, an employee in the Finance department has access to basic corporate applications and some financial applications. In the course of his daily work activities, Josh attempts to access the accounts payable system. As defined in a NetIQ Access Manager policy, Josh is a Finance employee and, based on his role, does not have the appropriate rights to access this system. So, when Josh attempts to access the resource, NetIQ Access Manager presents him with an “access denied” message (See Figure 12). However, since NetIQ Access Manager understands the identity context of Josh’s request, it provides Josh with instructions for getting access to the system. By clicking a link within the message, NetIQ Access Manager seamlessly links Josh to the Identity Manager request tool, where he can request his manager’s and the system owner’s approvals to access the accounts payable system (See Figure 13).
Figure 12: NetIQ Access Manager message to Josh

Make a Request

Complete resource request.
* indicates required.

<table>
<thead>
<tr>
<th>Resource:</th>
<th>Vendor Payment Role Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient:</td>
<td>Josh Kelley</td>
</tr>
<tr>
<td>Type of Request:</td>
<td>Roles</td>
</tr>
<tr>
<td>Description:</td>
<td>Request Access to the Vendor Payment Role</td>
</tr>
</tbody>
</table>

Form Detail

Vendor Payment Role Request
Press "Submit" to initiate the request.

[Input fields for Recipient and Reason for request]

Submit Cancel

Figure 13: The Identity Manager request tool
If Allison, a marketing employee, attempts to access the same accounts payable resource, NetIQ Access Manager determines that she is not in the Finance department and therefore should not have access. Instead of the typical “access denied” message, NetIQ Access Manager informs Allison that based on her role in the marketing department, she cannot access this resource (see Figure 14).

![Figure 14: NetIQ Access Manager notification message about why access was denied](image)

**Conclusion**

Organizations around the world continue to struggle with policy-compliance issues. Security and business policy violations continue to multiply and evolve, even as spending increases—leaving many organizations with a feeling that they have little recourse but to spend more. NetIQ Identity Tracking for Identity Manager integrates two silos of data, providing a rich context for user activities throughout the organization. By blending its award-winning identity and security technologies, NetIQ has delivered the ultimate governance solution that provides a real-time, holistic view to mitigate the risks posed by internal and external threats—and ultimately, to ensure your organization’s image, brand and reputation are safe.

NetIQ is an established leader in identity and security management, providing solutions to thousands of organizations around the globe. NetIQ Identity Tracking for Identity Manager allows your organization to combine powerful technology with pre-configured policies and documented best practices to provide a comprehensive approach to policy compliance—plus the most impressive return on investment available anywhere.
About NetIQ

NetIQ is a global, IT enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly-distributed business applications.

Our portfolio includes scalable, automated solutions for Identity, Security and Governance and IT Operations Management that help organizations securely deliver, measure and manage computing services across physical, virtual and cloud computing environments. These solutions and our practical, customer-focused approach to solving persistent IT challenges ensure organizations are able to reduce cost, complexity and risk.

To learn more about our industry-acclaimed software solutions, visit www.netiq.com.

Worldwide Headquarters
1233 West Loop South, Suite 810
Houston, Texas 77027 USA
Worldwide: +713.548.1700
U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com
http://community.netiq.com

For a complete list of our offices
In North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit www.netiq.com/contacts.