CionSystems

Compliance and Active Directory

Active Directory plays an important role in establishing a compliance initiative and maintaining the regulatory requirements

COMPLIANCE PRODUCTS

- Active Directory Manager
- Active Directory Self Service
- Active Directory Reporter
- Active Directory Change Notifier

Compliance- Why is it important?

The compliance activities especially in IT organizations represent a challenge for enterprises both from a technical and organizational standpoint. The scope of each regulation varies, however there is considerable overlap in areas of monitoring, information security and information management. Some of the most common regulations that companies have to comply with are HIPAA, SOX, and PCI. We will focus on SOX compliance because of its wider use across many verticals.

SOX is the Sarbanes-Oxley Act that was enacted by the US Congress in 2002. Some of the key components in this Act have to do with corporate governance, adding strong internal controls, organizational transparencies and disclosure accuracy- especially financial.

If you are a public company, you are required to comply with SOX regulations. It is not optional, and the penalties for non-compliance are quite severe: multi-million dollar fines, stock market delisting and even prison sentences. No matter what the penalties are, the net effect of non-compliance on your business is disastrous.

IT Compliance

Businesses rely on the IT organization to implement the afore-mentioned strong internal controls by providing a secure environment, and employing scalable monitoring and auditing solutions so as to comply with the SOX guidelines. Access and Identity management has become a very important aspect of any compliance policy, and consequently, the administration of such initiatives has become more complex.

To the CIO and other executives, compliance monitoring has two important aspects. A compliant organization has to be able to confirm that controls required to maintain compliance are in place and functioning. Also, a compliant organization must also monitor those systems, to detect and respond in timely fashion to incidents that could place protected information at risk. The Sarbanes-Oxley sections 404 and 302 directly shape IT's involvement in compliance.

IT Compliance initiatives must involve Active Directory

According to Microsoft, Active Directory is a central component of the Windows platform that provides the means to manage the identities and relationships that make up network environments. Active Directory offers significant assistance in the implementation of compliance standards, such as: control over the identities and access permissions within the enterprise, central repository for tracking access, regular and central authentication of users, delegation tools, provisioning access to specific resources for each user, etc.

Although Active Directory is important in ensuring the components are present, it cannot satisfy the compliance requirements by itself. Utilizing third party monitoring, auditing and administration tools such as the Active Directory Reporter or Active Directory Manager is equally important to a company's compliance efforts.

Compliance solutions from CionSystems

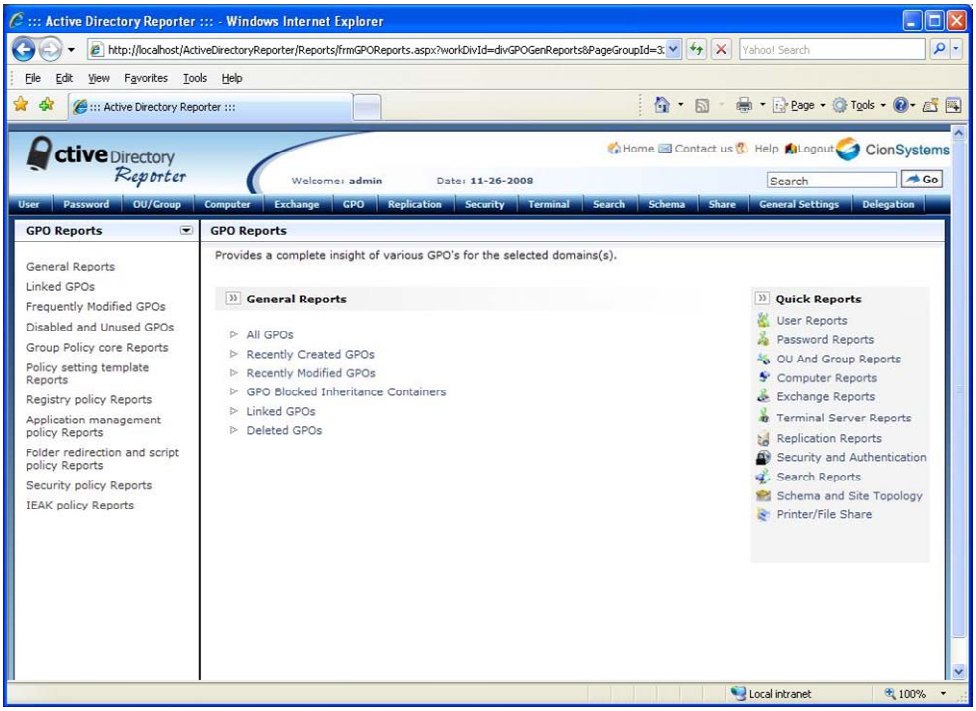
CionSystems offers intuitive web-based applications that facilitate centralized Active Directory administration and reporting/auditing. The easy to use browser based interface enhances the management capabilities and extends the tools found natively in Active Directory. The reporting features help administrators save a lot of time and effort and make compliance a snap.

For monitoring and auditing, the Active Directory Reporter has over 200 out-of-the-box reports. The Active Directory Reporter extracts vital information about Windows Active Directory infrastructure and objects quickly and displays it in a clear and logical format. All of these reports are customizable so you can tailor them to your needs. Furthermore, they are available on demand, or can be scheduled for distribution at preset times. This flexibility allows administrators to reduce security risks by eliminating stale users and groups, outline password and account policy gaps, and verify user permissions. The reporting capabilities also help with Risk Analysis and Management and track changes for auditing.

The standard reports are divided into the following categories:

Active Directory User Reports
Active Directory Logon Reports
Active Directory Password Reports
Active Directory Computer Reports
Active Directory Security Reports
Active Directory Exchange Reports
Active Directory GPO Reports
Active Directory File and Printer Reports

Active Directory Site Reports
Active Directory Replication Reports
Active Directory OU Reports
Active Directory Group Reports
Active Directory Policy Reports
Active Directory Terminal Server Reports
Active Directory Schema Reports
Active Directory Trust reports



On the administration side, the Active Directory Manager helps enterprises meet the compliance requirements by providing the same reporting capabilities and browser-based UI as the Active Directory Reporter. Additionally, by implementing this solution, companies have a centralized access point for easy role delegation, template-based User creation, auto generation of reports, and Exchange management. Other features include the intuitive Dashboard, Password and ACL management, Notifications features, and Search and Replace functions.

CionSystems provides complete web-based solutions to meet the Active Directory management requirements with a specialized set of reports and tools useful for regulatory compliance audits. Implementing our solutions, companies can meet the requirements of Enterprise Wide Security Policy, Risk Analysis, Disaster Recovery, and prove compliance with ease.

For more information on any of our products or services please visit us on the Web at: www.CionSystems.com

CionSystems Inc.
16625 Redmond Way,
Ste. M106
Redmond, WA. 98052
425.605.5325

Microsoft CERTIFIED Partner