

ecora

Security Compliance & Control Made Easy

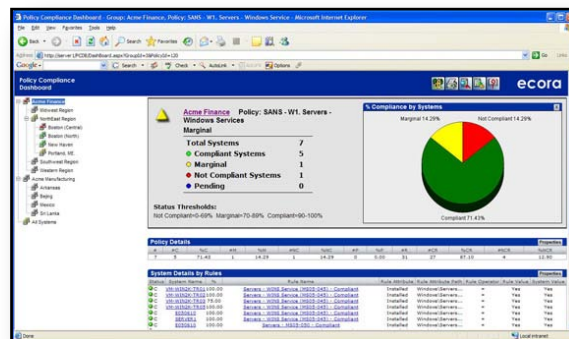
Control Your Enterprise for Maximum Performance and Availability

IT Control

In information technology, the only constant is change. Industry analysts estimate that configuration errors are responsible for up to 80 percent of network outages. These errors are often caused by unauthorized changes which remain hidden until critical downtime has occurred.

Without accurate, up-to-date, audit reports of what's happening in your environment, unscheduled downtime and the associated business costs become a significant expense. Extra staff time must be dedicated to finding and correcting the error. Downtime also subjects businesses to lost revenue, increased vulnerability to attack, and damaged customer relations. Automating configuration reporting, gaining at a glance visibility to configuration policy compliance, and automated change-making capability can efficiently and affordably ensure control over your environment.

Maintain availability standards by monitoring changes in compliance status with Ecora's executive dashboard



Do you know what's actually happening on critical business systems?

How quickly can you change improper configurations once discovered?

Ecora can tell you what's changed, automate corrections, and report results – before downtime occurs.

The Ecora Solution

With Ecora, you will reduce the cost of downtime and meet or exceed your service level agreements. By capturing accurate, cross-platform system configuration information, comparing it against established policy, then displaying your level of compliance in a web-accessible graphical dashboard, organizations can audit changes occurring in their environment. Businesses benefit from significantly fewer errors and maximum system and network uptime. When problematic changes are found and configuration settings fall outside of compliance standards, Ecora automates the deployment of corrective changes – saving additional time and resources.

How Ecora Benefits You

- Know what changed and when
- Measure configuration policy compliance based on leading industry standards or your own criteria
- View policy compliance status at a glance on a web-accessible dashboard
- Validate and remediate changes, authorized and unauthorized
- Control configuration drift to sustain compliance
- Generate audit-ready reports that demonstrate compliance
- Automate change-making to reduce the time and cost of troubleshooting

"Ecora helps us prove to auditors that we're prepared. From reducing the time to troubleshoot problems to the information we need to quickly recover our databases, Ecora is extremely valuable."

Chuck Lewis, Senior Database Analyst
U.S. Coast Guard Finance Center

Ecora Change and Configuration Management Solution Suite

Ecora Auditor Professional is a powerful configuration and change reporting solution that collects over a million asset, security, and configuration settings from nearly every operating system, database management system, application, and network device found in an IT infrastructure. The configuration settings are stored in a centralized Configuration Management Database (CMDB) for on-demand, accurate auditing, reporting and change control. Ecora Auditor Professional eliminates the resource-intensive, error-prone manual process of managing enterprise-wide configurations and simplifies ongoing compliance with IT security standards and regulations.

Ecora Auditor Professional includes a web-accessible executive dashboard providing at-a-glance validation of compliance to established IT controls, security policies, and configuration standards. The dashboard evaluates configuration information from the CMDB to generate an easy-to-understand pie graph displaying compliant and non-compliant systems as either green (compliant) or red (non-compliant). This enables IT managers to quickly identify non-compliant systems and direct the appropriate personnel to remediate any non-compliant configurations. Dozens of out-of-the-box report and policy templates are included for Sarbanes Oxley, HIPAA, GLBA, 21 CFR Part 11, VISA PCI, FISMA, and NIST IT requirements. You can also create your own reports and policies or customize existing ones.

"When one of our servers lost all of its permissions, we had the necessary documentation reports right at our fingertips to rapidly restore those permissions and significantly minimize what could have been hours of potential downtime."

Randy Samora, Network Systems Engineer
Landata Systems



www.ecora.com

ecora Software | 2 International Drive, Suite 150, Portsmouth, NH 03801 | p: 877.92.ECORA or 603.436.1616 | f: 603.436.4344 | sales@ecora.com

The Ecora Auditor Professional family also includes:

Ecora Auditor Lite - A free application that collects and reports on hundreds of configuration settings from nearly every system and device in the IT infrastructure. The audit-ready documentation is generated on demand, and archived reports provide an easily accessible audit trail for effective disaster recovery, IT audits, troubleshooting, and consolidations.

Ecora Auditor Basic - An upgrade from Auditor Lite that provides additional functionality by offering dozens of ready-made fact-finding report templates for quick, simplified analysis of critical configuration data such as access rights, NTFS permissions, and password settings.

The Auditor product family supports VMware ESX servers; Microsoft Windows and Exchange servers, SQL Server databases, Active Directory, and workstations; HP-UX, AIX, Solaris, RedHat Linux, and Novell NetWare servers; Oracle databases, Citrix and IIS applications; Lotus Domino servers; and Cisco routers.



Track and change critical configurations with Auditor Professional's automated reporting and change-making capabilities.