

ECC ECAR™ Enterprise Compliance Auditing & Reporting

Automates measurable, sustainable and repeatable assessment of 175 Microsoft Windows security events for demonstrable compliance to IT-related regulations and standards

Background

The ECC Enterprise Compliance Auditing & Reporting aligns 175 Microsoft® Windows Server security events with specific regulatory requirements and best standards recommendations. Easily customized and extensive, IT-related security data is gathered and organized in a fashion that is immediately useable for internal review and external audits. Nearly 100 reports are mapped directly to individual regulations and may be output to a large number of file/archive formats.

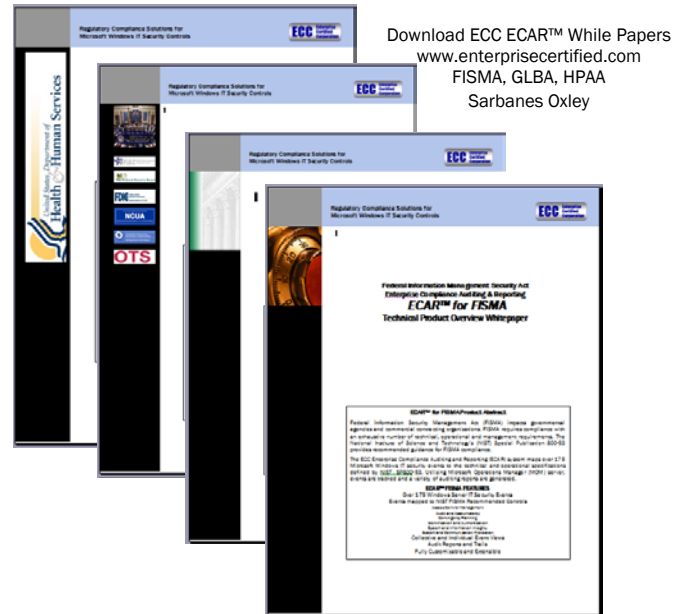
ECAR™ Solution for Today

ECC ECAR™ is designed to more rapidly facilitate the audit process associated with IT security assessment and regulatory compliance auditing/reporting. Versions are available for the Federal Information Security Management Act (FISMA), Gramm Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes Oxley Act. Each version ties directly to the expectations associated with the individual legislative and associated agency initiatives. In addition, knowledgebase support for specific auditing and reporting functions is associated with best standards such as those from the National Institute of Science and Technology (NIST), COSO, and the Federal Financial Institutions Examination Council (FFIEC).

ECC recognizes that among the estimated expenditure of over \$15 billion associated with compliance organizations will need to apply a variety of tools and approaches. As it relates to Windows IT security issues, ECC ECAR™ clearly is the robust and cost effective solution of choice.

Key Benefits

ECC ECAR™ unique mapping of IT security events to regulations and standards streamlines the assessment process and provides greater assurance of producing meaningful audits and reports. The unified approach is sustainable, repeatable and measurable. The web-based report generator provides the administrator to set parameters and IT events that are most applicable for security assessment and regulatory auditing of a particular organization. Utilizing the infrastructure afforded Microsoft Operations Manager and SQL Reporting Services, ECC ECAR™ provides regulatory aligned rules groups and definable event views.



On demand, continuous and customized analysis – ECC ECAR™ automatically collects IT security information for predefined events, rules and computer group associations that have a direct relation to a regulation or standard. This activity remains continuous for all enabled functions. In addition, special reports can be output based upon very granular administrator defined on-demand requirements. Whether standard or customized configuration is desired, audit integrity is maintained so longevity and “slice of time” information is readily available.

Centralized and inherently useful information – ECC ECAR™ was designed to provide IT security event information that would be useful for a variety of user audiences. IT management is provided a variety of levels of formatted data that permit summary and in depth analysis. Columnar, group and graphical reports make review by non-technical management something that is viable and readily available. For external auditors or government examination teams, IT security events are assembled in a fashion that maps to their regulatory inspection guidelines. Where disputes should occur, the alignment of ECC ECAR™ to best practice standards provides greater justification for current and proposed policies and procedures. All is centralized and secure.

ECC ECAR™ Enterprise Compliance Auditing & Reporting

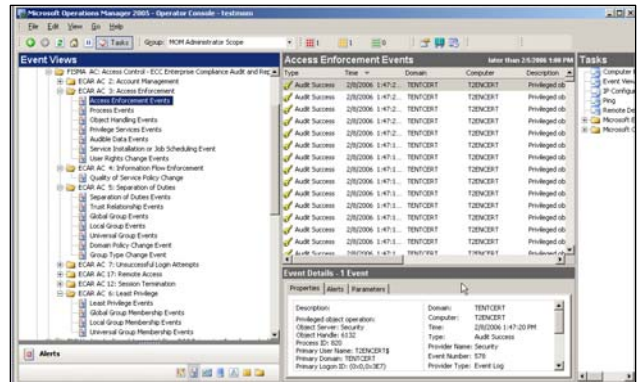
Technical Features

Over 175 Windows Server IT Security Events Administrator and User Event Interfaces
 Collective and Individual Event Views
 100 Audit Reports and Templates
 Fully Customizable and Extensible
 Compliance by regulation
 Compliance by event, rule and computer group
 Historic and on-demand defined analysis
 Events mapped to NIST Recommended Controls:

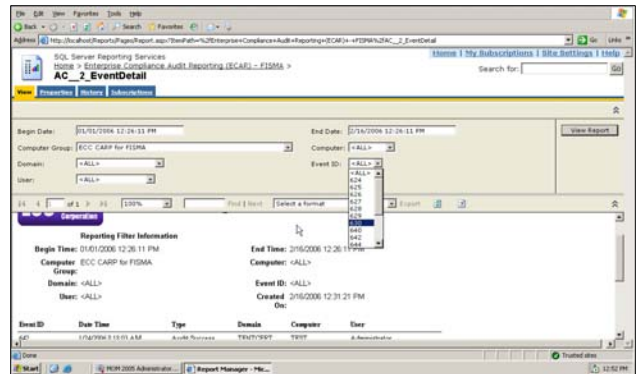
- Access Control Management
- Audit and Accountability
- Contingency Planning
- Identification and Authentication
- System and Information Integrity
- System and Communication Protection

System Requirements

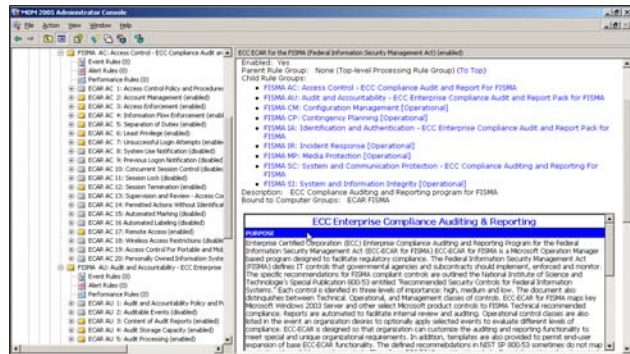
Windows Server 2003 or higher
 SQL Server 2000, SP 2
 SQL Report Server
 Microsoft Operations Manager 2005
 Internet Explorer 6.0 or higher



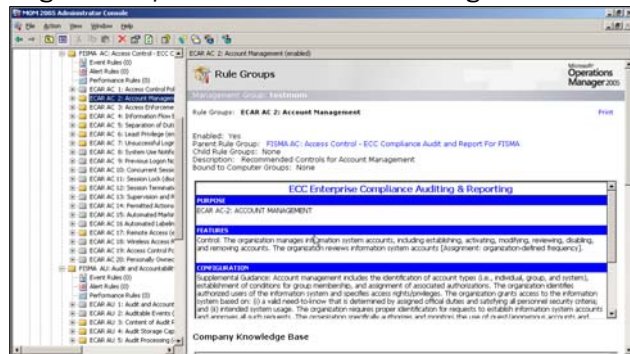
On demand security event standard and custom views



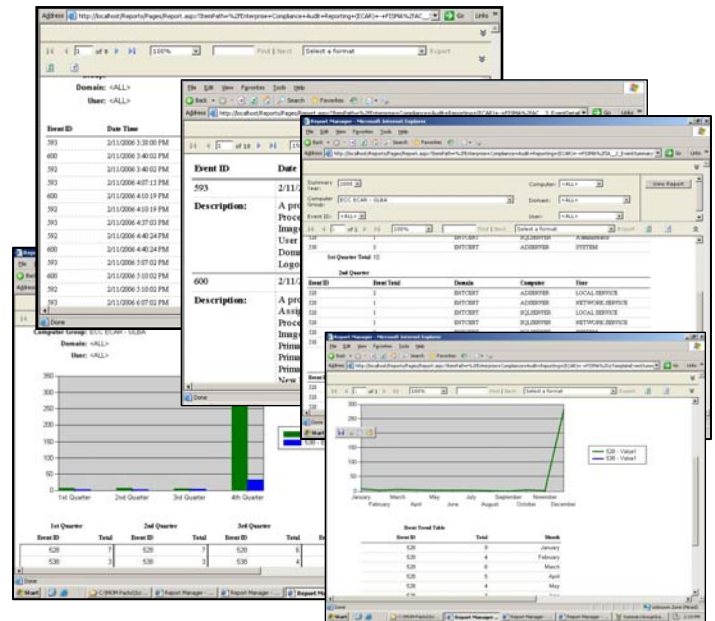
Definable Report Parameter Settings



Regulation Specific Administrative Management



Standards Based Knowledgebase and Guidance



Detail, Expanded, Summary, Group Graphical and Trend Analysis Reports defined by Regulation, Rule and/or Event