



eTrust® Access Control r 8

eTrust® Access Control protects business critical infrastructure and minimizes security risks by regulating access to confidential business data and mission critical services. This powerful solution provides policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. eTrust Access Control can be deployed in phases, and policies can be created, managed and distributed on an enterprise-wide basis.

Key Features at a Glance

- Role-Based Granular Access Control
- Superuser Containment and Rights Delegation
- Server Intrusion Prevention
- Automated Policy Distribution
- Self Protection Mechanism
- Centralized and Delegated Administration
- Strong Password Management and Policies
- Complete Audit Trail
- Phased Deployment
- Broad Platform Coverage

What's New

- eTrust Identity and Access Management Integration
- Web-Based Administration Console
- External LDAP Support
- Policy Management System
- Application Policy Generator
- Operational Enhancements
- Maintenance Mode Security

Safeguarding Electronic Assets and Enforcing Security Compliance

In most organizations, critical information and processes — such as business transactions, Web services, customer information and confidential financial records — reside on distributed servers. Protecting this data and restricting access to these services presents a major challenge since the native operating systems do not provide adequate data security. As processing power grows and more business applications leverage internet technology, the risk to business assets from these threats has increased exponentially.

According to annual CSI/FBI reports, unregulated internal access is one major contributing security threat to data confidentiality and electronic financial losses. This issue is compounded with superuser account sharing that leads to lack of accountability and expanded single point of

failure. A strong access management system must be deployed to protect valuable electronic assets, remove critical security holes and help ensure compliance with complying regulatory requirements.

The other major threat is malicious-code attacks to mission-critical servers. Cyber attacks, like “Worms”, have moved to the application level, circumventing network-based firewalls, and rendering signature-based antivirus protection and latent patch management ineffective. Businesses are moving away from a reliance on risk avoidance strategies. Proactive business application security is essential.

Secure Computing

To address these challenges, CA offers eTrust® Identity and Access Management.

A critical component of Identity and Access Management is managing access to enterprise critical resources. Award-winning eTrust Access Control enables

organizations to centrally manage user access privileges and allow deployment of baseline security policies so that the right people have access to the right information. It proactively secures access to data and applications located on Linux, UNIX and Windows system servers throughout the enterprise.

eTrust Access Control supplies advanced intrusion prevention technology for everything from Web servers to RDBMS applications. It can be deployed in phases and can scale from a department to the largest enterprise. It strengthens protection against malicious code attacks with the automated rule generator and customizable security policies for any enterprise application.

Access control is especially crucial in supporting regulatory compliance as well as security certifications. Many privacy protection and confidentiality regulations like SOX, HIPAA, or security certifications like BS 7799, require strong user access control to confidential data, which includes superuser containment and strict access rights granting, accompanied with high integrity auditing records. eTrust Access Control provides regulated access that can help organizations comply with regulation requirements and auditing.

Distinctive Features and Functionalities

Role-based Access Control. eTrust Access Control gives users access to the information they need and prevents and logs all unauthorized information requests.

• **Fine-grained Access Control.** eTrust Access Control provides individual access controls for system logons, and regulates access to resources, programs, files and processes through a series of stringent criteria including time, login method, network attributes and access program.

• **Superuser Containment.** eTrust Access Control can reduce and delegate the privileges associated with superuser accounts:

- "Administrator" for Windows
- "root" for UNIX/Linux

This native, single point of failure on every distributed platform can be removed to prevent internal abuse or external exploits.

• **Delegated Administration and Accountability.** eTrust Access Control eliminates privilege creep through delegation of access rights to designated systems operators.

• **Program Pathing.** Users can be regulated to access resources only through a designated program. This is particularly valuable to backup operators, database managers that use a few specific programs to perform their operations.

Server Intrusion Prevention. eTrust Access Control provides stack overflow protection, denial of Trojan Horse attacks, best practices security baseline, and soft-firewall capabilities, that prevent system intrusion or most worm attacks.

• **Stack Overflow Protection (STOP).** STOP prevents hackers from using stack overflow exploits, which can enable them to execute arbitrary commands to break into other networked systems.

• **Out-of-Box Best Practices Policies.** eTrust Access Control provides out-of-box security best practices samples that can be installed on most popular applications, including web servers, database servers and enterprise servers.

• **Host-based Firewall Protection.** eTrust Access Control regulates both incoming and outgoing network connection based on ports, connection method, access sources, network attributes and time.

Policy Management. eTrust Access Control allows administrators to define access policies to be applied to multiple, disparate servers across multiple domains, ensuring that access policies are consistently enforced across platforms.

• **Automated Policy Distribution.** eTrust Access Control uses its Policy Model Database (PMDb) infrastructure to automatically propagate policies to a hierarchy of server nodes.

• **Multi-Master Policy Inheritance.** Policies may be defined to draw from a combination of other policies (e.g. system policies, application policies and web server policies.) Changes to a parent policy are automatically synchronized to subscribers.

• **Native Policy Management.** Security administrators can use eTrust Access Control to manage the security on both native user accounts and ACLs, greatly reducing the need to use two sets of management tools.

• **Profile Groups.** eTrust Access Control provides easy-to-implement password policy template function that allows users to be added to groups with predefined password rules.

Enhanced Security. eTrust Access Control integrates closely into the operating system to prohibit the bypassing of authorization checks and to ensure its own integrity.

• **Self-protection.** It is virtually impossible for users to attack, change or erase eTrust Access Control core services and data. It protects itself against hacking and constantly monitors its protected processes and audit logs to ensure its security service integrity.

• **Customizable Encryption Libraries.** Enterprises can substitute an alternate encryption algorithm by replacing the module used to secure eTrust Access Control administrative communications.

- **B1 Security Features.** eTrust Access Control can define and enforce access based on security label and security level as defined in the National Computer Security Council B1 (Department of Defense) clearance levels.

Administration. When managing a diverse server environment, the ability to have a central security management console is crucial for reducing costs and consolidating redundant operations. It empowers the security manager to set policy centrally and to perform urgent tasks like suspending a user in real time.

- **Centralized Administration.** eTrust Access Control enables administrative users to centrally manage policies, users and passwords across departments and platforms.
- **Administration Console.** User account and access rules management can be performed through various interfaces by choices, including Web-based, graphical and command-line.

User and Password Management. When access to critical servers that host enterprise applications, user account and password policies must be consistently defined and enforced to ensure proper access is assigned.

- **User Account Management.** eTrust Access Control can synchronize user creation, update, suspension and revocation across different flavors of UNIX/Linux and Windows and can be extended to Mainframe security packages. It is fully compatible with NIS, NIS+ and Active Directory systems.
- **Password Quality.** eTrust Access Control allows an organization to create and enforce password quality including password composition, minimum and maximum length, repetition and custom dictionary.

- **Mainframe Password Synchronization.** User passwords can be synchronized across mainframe security packages (eTrust® ACF2 Security, eTrust® Top Secret Security, IBM RACF).

Extensibility. eTrust Access Control includes features that support an extended heterogeneous environment and adapt to the specific needs of the business.

- **Phased Deployment.** eTrust Access Control can be installed on a single server with full functionality and can grow to large scale deployment. It also integrates seamlessly with eTrust Identity and Access Management infrastructure for a full Identity and Access Management configuration.
- **Cross-platform Support.** Administrators can define a single policy that can be applied to any mix of Windows, UNIX or Linux systems plus applications.
- **Pluggable Authentication Module (PAM).** Organizations can install a custom mechanism for authentication of eTrust Access Control administrators.

Secure and Flexible Auditing.

Comprehensive security must include a complete and reliable record of individuals' activities. eTrust Access Control can audit all security-sensitive events and activate immediate alerts and actions in case of an security incident.

- **Identity Audit Trail.** eTrust Access Control has a separate secure audit log and can track the original user identity even after the user performs a surrogate operation. The log pre-serves the full user action trail from login to logout.
- **Log File Integrity.** eTrust Access Control secure its audit logs and event logs against any tampering. Only individuals participating in the auditor role can access the files and only in read-only mode, ensuring forensic quality of log files.

- **Log Routing.** eTrust Access Control can route logs from different eTrust Access Control sources to a remote server for integrity protection and analysis.
- **Integration with eTrust® Security Command Center.** Logging access events is an important plank in a security access management strategy. eTrust Access Control events can be monitored and managed by eTrust Security Command Center and consolidated into a complete identity audit across network, security, application and operating auditing sources.

Broad Platform Coverage. eTrust Access Control protects a wide spectrum of distributed server platforms in the industry.

- **Linux.** Linux RedHat and SuSE are supported on a wide range of platforms: x86, AMD64/EM64T, Itanium, s390, s390x.
- **UNIX.** AIX, HP-UX, HP-UX on Itanium, Solaris, Solaris on AMD64/EM64T, HP Tru64 and SCO/UNIXWare.
- **Windows.** Windows NT, Windows 2000, Windows 2003 and XP platforms.

What's New in Release 8

eTrust Identity and Access Management Integration. Organizations need complete end-to-end management of identities. eTrust Access Control, a component of the eTrust Identity and Access Management platform, protects enterprise-critical data and applications, and tracks users access to data and applications. eTrust Access Control is integrated with enterprise class provisioning and auditing for total identity and access management.

Web-Based Administration Console.

eTrust Access Control adds a web-based management interface in addition to existing Windows, Motif and Command-Line consoles. It is fully integrated into eTrust Identity and Access Management administration portal.

External LDAP Support. Many organizations are moving to centralize their user data stores to LDAP-based repositories. eTrust Access Control can use an external LDAP user repository as source user database and perform user account creation, update, suspend and revocation.

Policy Management System. The new eTrust Access Control stand-alone policy management system helps administrators to easily manage departmental security policies with policy set versioning, distribution and remote download abilities, to ensure all subscription servers obtain the latest security policies and easy version controls.

Application Policy Generator. An automated policy generator program is provided to profile application behaviors and generate security policies accordingly. It creates a security envelope around the applications and greatly reduces the deployment efforts required to construct these rules.

Operational Enhancements.

- **Fast and reliable database backup.** The eTrust Access Control database can be backed up to an alternate directory without terminating processing.
- **Native Installation Package.** The new RPM format of installation files of eTrust Access Control allows flexible software installation, query and update methods.

Maintenance Mode Security. When eTrust Access Control is in maintenance mode, all access events are denied to ensure full security restriction when eTrust Access Control is not active.

As a leader in the Identity and Access Management market, eTrust Access Control provides enterprise-level server security against both internal and external threats, and helps organizations comply with auditing and regulatory compliance.

For more information,
call 1-800-875-9659
or visit ca.com

