



eTrust® SiteMinder®

eTrust® SiteMinder® is a security and management foundation for enterprise web applications with a centralized security infrastructure for managing user authentication and access. eTrust SiteMinder delivers the market's most advanced security management capabilities and enterprise-class site administration, reducing overall IT operational cost and complexity. eTrust SiteMinder enables the secure delivery of essential information and applications to employees, partners, suppliers and customers, and scales with growing business needs.

Key Features at a Glance

- Single Sign-On
- Centralized Policy-Based Server
- Enterprise Manageability
- Federated Identity Support
- Open and Extensible
- Scalable and Reliable
- Dynamic Authorization

Business In, Risk Out

The web provides organizations with unparalleled opportunities to increase revenues, lower costs and deepen relationships with customers, partners and employees. But for all its promise the web presents a host of security and management challenges. How do you manage who is entitled to access which resources? How do you let business in while keeping risk out?

Distinctive Features and Functionalities

Single Sign-On. Single sign-on (SSO) across multiple heterogeneous applications, platforms and Internet domains provides a richer user experience, increased security and reduced customer support costs due to forgotten passwords.

Centralized Policy-Based Server.

Centralized security policy enforcement of user entitlements reduces application development and administration costs enterprise-wide.

Enterprise Manageability. Enterprise-class system management tools enable security architects to monitor, manage and maintain multiple environments more efficiently for development, testing and production, assuring cost-effective management of sophisticated security systems.

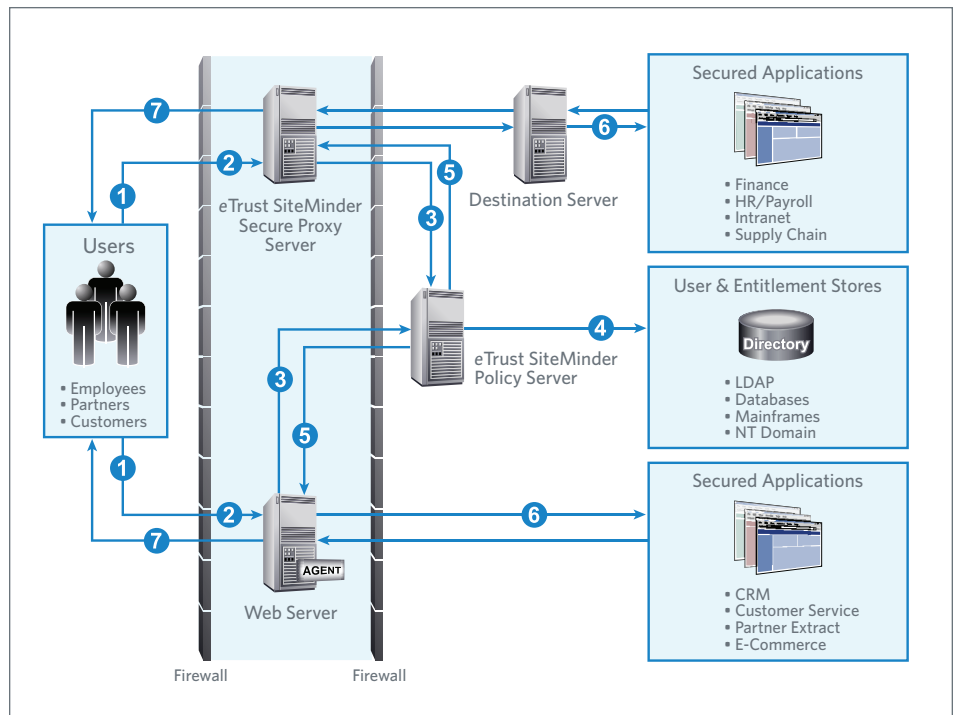
- Key management
- Unattended installs
- Operational monitoring
- Rolling upgrades
- Centralized web agent management
- Security policy migration
- Scripting interface capabilities

Federated Identity Support. Support for SAML, Liberty Alliance, .Net Passport and Kerberos enable SSO and session management across federated business networks. Secure federated networks allow the delivery of customized products and services, enhancing the user experience and improving customer retention.

Integration with eTrust® Single Sign-On. eTrust Single Sign-On is the market leading solution for enterprise SSO. Integration between the two products enables eTrust Single Sign-On and eTrust® SiteMinder® users to authenticate only once and have access to resources in both security domains. For customer environments using both solutions, integration significantly improves user satisfaction and productivity, while also improving product manageability and efficiency.

Open and Extensible. The heterogeneous cross platform support for authentication systems, operating systems, user stores, web servers, J2EE application servers, enterprise applications and wide API support of eTrust SiteMinder leverages existing infrastructure to help reduce deployment time and costs while increasing ROI.

Scalable and Reliable. Advanced load balancing, fully tunable two-level caching, cluster-to-cluster failover, dynamic load balancing, Agent, Policy Server and user store replication, clustering, automatic fail-over and support for 4&8-way SMP servers. Confidently deploy mission-critical applications to multi-million user populations knowing that eTrust SiteMinder performance has been verified through independent testing, proving deployment support to 100 million users and thousands of applications.



Dynamic Authorization. Real-time transactional security and integrated Web services with eTrust SiteMinder eTelligent Rules creates security policies that evaluate dynamic data from a variety of local or external sources, including Web services and databases in real time. Reduce cost and complexity by eliminating advanced security logic from web applications and centralizing it within eTrust SiteMinder Policies.

How it Works

1. User attempts to access a protected resource.
2. User is challenged for his credentials and presents them to the web agent or to the Secure Proxy Server.
3. The user's credentials are passed to the Policy Server.
4. The user is authenticated against the appropriate user store.
5. The Policy Server evaluates the user's entitlements and grants access.
6. User profile and entitlement information is passed to the application.
7. The user gets access to the secured application which delivers customized content.

Supported Platforms

Authentication Methods	Enterprise Applications SSO	User Directories	Operating Systems
Password Forms-based Forms and/or Certificates Password Over SSL Two Factor Tokens X.509 Certificates Smart Cards Biometric Devices CRL and OCSP Support Combinations of Methods Custom Methods Security Assertions Markup Language (SAML) Liberty Alliance (ID-FF)	Siebel PeopleSoft Oracle SAP	Sun Java System Directory Server Novell eDirectory Microsoft Active Directory Microsoft AD/AM Microsoft SQL Server Microsoft NT Domain Oracle Internet Directory Oracle RDBMS Lotus Domino LDAP Critical Path Directory Server Siemens DirX, DirXEE IBM Directory Server IBM DB2 CA eTrust	NT/Win2000/Win 2003 Sun Solaris HP-UX Red Hat Enterprise Linux
	Application Servers		Web Agents
	BEA WebLogic IBM WebSphere		Microsoft IIS Sun Java System Web Server Stronghold Apache Covalent Apache IBM HTTP Server Domino Oracle HTTP Server HP Apache

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

